Exam SAA-C03

AWS Certified Solutions Architect - Associate (SAA-C03)

Version: 19.0

[Total Questions: 677]

Topic 1, Exam Pool A

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. Use an Application Load Balancer to distribute the incoming requests.

B. Use two Amazon EC2 instances to host the containerized web application. Use an Application Load Balancer to distribute the incoming requests

C. Use AWS Lambda with a new code that uses one of the supported languages. Create multiple Lambda functions to support the load. Use Amazon API Gateway as an entry point to the Lambda functions.

D. Use a high performance computing (HPC) solution such as AWS ParallelClusterto 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.

2. - (Topic 1)

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

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

A. Store the credentials as secrets in AWS Secrets Manager. Use multi-Region secret replication for the required Regions Configure Secrets Manager to rotate the secrets on a schedule

B. Store the credentials as secrets in AWS Systems Manager by creating a secure string parameter Use multi-Region secret replication for the required Regions Configure Systems Manager to rotate the secrets on a schedule

C. Store the credentials in an Amazon S3 bucket that has server-side encryption (SSE) enabled Use Amazon EventBridge (Amazon CloudWatch Events) to invoke an AWS Lambda function to rotate the credentials

D. Encrypt the credentials as secrets by using AWS Key Management Service (AWS KMS) multi-Region customer managed keys Store the secrets in an Amazon DynamoDB global table Use an AWS Lambda function to retrieve the secrets from DynamoDB Use the RDS API to rotate the secrets.

Answer: A

Explanation:

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

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. Use human review for low- confidence

predictions.

B. Use Amazon Rekognition to detect inappropriate content. Use human review for low- confidence predictions.

C. Use Amazon SageMaker to detect inappropriate content. Use ground truth to label low- confidence predictions.

D. Use AWS Fargate to deploy a custom machine learning model to detect inappropriate content. Use ground truth to label low-confidence predictions.

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

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. Other applications can consume the data stored in Amazon S3

C. Stream the transactions data into Amazon Kinesis Data Streams Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions

data in Amazon DynamoDB Other applications can consume the transactions data off the Kinesis data stream.

D. Store the batched transactions data in Amazon S3 as files. Use AWS Lambda to process every file and

remove sensitive data before updating the files in Amazon S3 The Lambda function then stores the data in Amazon DynamoDB Other applications can consume transaction files stored in Amazon S3.

Answer: C

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.

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

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

C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for each SaaS source to send output data. Configure the S3 bucket as the rule's target. Create a second EventBridge (CloudWatch Events) rule to send events when the upload to the S3 bucket is complete. Configure an Amazon Simple Notification Service (Amazon SNS) topic as the second rule's target.

D. Create a Docker container to use instead of an EC2 instance. Host the containerized application on Amazon Elastic Container Service (Amazon ECS). Configure Amazon CloudWatch Container Insights to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.

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/

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 Mm from S3 Standard to S3 Glacier 30 days from object

creation Delete the Tiles 4 years after object creation

B. Create an S3 bucket lifecycle policy to move tiles from S3 Standard to S3 One Zone- infrequent Access (S3 One Zone-IA] 30 days from object creation. Delete the fees 4 years after object creation

C. Create an S3 bucket lifecycle policy to move files from S3 Standard-infrequent Access (S3 Standard -IA) 30 from object creation. Delete the ties 4 years after object creation

D. Create an S3 bucket Lifecycle policy to move files from S3 Standard to S3 Standard- Infrequent Access (S3 Standard-IA) 30 days from object creation Move the files to S3 Glacier 4 years after object carton.

Answer: B

Explanation:

https://aws.amazon.com/s3/storage-classes/?trk=66264cd8-3b73-416c-9693-ea7cf4fe846a&sc_channel=ps&s_kwcid=AL!4422!3!536452716950!p!!g!!aws%20s3%20pri cing&ef_id=Cj0KCQjwnbmaBhD-ARIsAGTPcfVHUZN5_BMrzl5zBcaC8KnqpnNZvjbZzqPkH6k7q4JcYO5KFLx0YYgaAm6nEALw_wcB:G:s&s_kwcid=AL!4422!3!536452716950!p!!g!!aws%20s3%20pricing

7. - (Topic 1)

A company hosts its web applications in the AWS Cloud. The company configures Elastic Load Balancers to use certificate that are imported into AWS Certificate Manager (ACM). The company's security team must be notified 30 days before the expiration of each certificate.

What should a solutions architect recommend to meet the requirement?

A. Add a rule m ACM to publish a custom message to an Amazon Simple Notification Service (Amazon SNS) topic every day beginning 30 days before any certificate will expire.

B. Create an AWS Config rule that checks for certificates that will expire within 30 days. Configure Amazon EventBridge (Amazon CloudWatch Events) to invoke a custom alert by way of Amazon Simple Notification Service (Amazon SNS) when AWS Config reports a noncompliant resource

C. Use AWS trusted Advisor to check for certificates that will expire within to days. Create an Amazon CloudWatch alarm that is based on Trusted Advisor metrics for check status changes Configure the alarm to send a custom alert by way of Amazon Simple rectification Service (Amazon SNS)

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

Answer: B

Explanation: https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate- expiration/

8. - (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

9. - (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. All the applications will read and process the messages.

B. Deploy the application on Amazon EC2 instances in an Auto Scaling group, which scales the number of EC2 instances based on CPU metrics.

C. Write the messages to Amazon Kinesis Data Streams with a single shard. All applications will read from the stream and process the messages.

D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with one or more Amazon Simple Queue Service (Amazon SQS) subscriptions. All applications then process the messages from the queues.

Answer: 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.

10. - (Topic 1)

A company has an application that provides marketing services to stores. The services are based on previous purchases by store customers. The stores upload transaction data to the company through SFTP, and the data is processed and analyzed to generate new marketing offers. Some of the files can exceed 200 GB in size.

Recently, the company discovered that some of the stores have uploaded files that contain personally identifiable information (PII) that should not have been included. The company wants administrators to be alerted if PII is shared again. The company also wants to automate remediation.

What should a solutions architect do to meet these requirements with the LEAST development effort?

A. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Inspector to scan me objects in the bucket. If objects contain Pll. trigger an S3 Lifecycle policy to remove the objects that contain Pll.

B. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Macie to scan the objects in the bucket. If objects contain Pll. Use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects mat contain Pll.

C. Implement custom scanning algorithms in an AWS Lambda function. Trigger the function when objects are loaded into the bucket. It objects contain Rll. use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain Pll.

D. Implement custom scanning algorithms in an AWS Lambda function. Trigger the function when objects are loaded into the bucket. If objects contain Pll. use Amazon Simple Email Service (Amazon STS) to trigger a notification to the administrators and trigger on S3 Lifecycle policy to remove the objects mot contain PII.

Answer: B

Explanation:

To meet the requirements of detecting and alerting the administrators when PII is shared and automating remediation with the least development effort, the best approach would be to use Amazon S3 bucket as a secure transfer point and scan the objects in the bucket with Amazon Macie. Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect sensitive data stored in Amazon S3. It can be used to classify sensitive data, monitor access to sensitive data, and automate remediation actions.

In this scenario, after uploading the files to the Amazon S3 bucket, the objects can be scanned for PII by Amazon Macie, and if it detects any PII, it can trigger an Amazon Simple Notification Service (SNS) notification to alert the administrators to remove the objects containing PII. This approach requires the least development effort, as Amazon Macie already has pre-built data classification rules that can detect PII in various formats. Hence, option B is the correct answer.

References:

- Amazon Macie User Guide: https://docs.aws.amazon.com/macie/latest/userguide/what-is-macie.html
- AWS Well-Architected Framework - Security Pillar: https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html

11. - (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 duster 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 tor analysis

C. Cache the data to Amazon CloudFron: 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 tor analysis.

D. Collect the data from Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to transmit the data to an Amazon S3 data lake Load the data in Amazon Redshift for analysis

Answer: D

Explanation:

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

12. - (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

13. - (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/

14. - (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.

15. - (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 completed. Restart the DB instance when required.

B. Use an Auto Scaling policy with the DB instance to automatically scale when tests are completed.

C. Create a snapshot when tests are completed. Terminate the DB instance and restore the snapshot when required.

D. Modify the DB instance to a low-capacity instance when tests are completed. Modify the DB instance again when required.

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)

16. - (Topic 1)

A company has a three-tier web application that is deployed on AWS. The web servers are deployed in a public subnet in a VPC. The application servers and database servers are deployed in private subnets in the same VPC. The company has deployed a third-party virtual firewall appliance from AWS Marketplace in an inspection VPC. The appliance is configured with an IP interface that can accept IP packets.

A solutions architect needs to Integrate the web application with the appliance to inspect all traffic to the application before the traffic teaches the web server. Which solution will moot these requirements with the LEAST operational overhead?

A. Create a Network Load Balancer the public subnet of the application's VPC to route the traffic lo the appliance for packet inspection

B. Create an Application Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection

C. Deploy a transit gateway m the inspection VPC Configure route tables to route the incoming pockets through the transit gateway

D. Deploy a Gateway Load Balancer in the inspection VPC Create a Gateway Load Balancer endpoint to receive the incoming packets and forward the packets to the appliance

Answer: D

Explanation:

https://aws.amazon.com/blogs/networking-and-content-delivery/scaling-network-traffic-inspection-using-aws-gateway-load-balancer/

17. - (Topic 1)

A global company hosts its web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The web application has static data and dynamic data. The company stores its static data in an Amazon S3 bucket. The company wants to improve performance and reduce latency for the static data and dynamic data. The company is using its own domain name registered with Amazon Route 53. What should a solutions architect do to meet these requirements?

A. Create an Amazon CloudFront distribution that has the S3 bucket and the ALB as origins Configure Route 53 to route traffic to the CloudFront distribution.

B. Create an Amazon CloudFront distribution that has the ALB as an origin Create an AWS Global Accelerator standard accelerator that has the S3 bucket as an endpoint. Configure Route 53 to route traffic to the CloudFront distribution.

C. Create an Amazon CloudFront distribution that has the S3 bucket as an origin Create an AWS Global Accelerator standard accelerator that has the ALB and the CloudFront distribution as endpoints Create a custom domain name that points to the accelerator DNS name Use the custom domain name as an endpoint for the web application.

D. Create an Amazon CloudFront distribution that has the ALB as an origin C. Create an AWS Global Accelerator standard accelerator that has the S3 bucket as an endpoint Create two domain names. Point one domain name to the CloudFront DNS name for dynamic content, Point the other domain name to the accelerator DNS name for static content Use the domain names as endpoints for the web application.

Answer: C

Explanation:

Static content can be cached at Cloud front Edge locations from S3 and dynamic content EC2 behind the ALB whose performance can be improved by Global Accelerator whose one endpoint is ALB and other Cloud front. So with regards to custom domain name endpoint is web application is R53 alias records for the custom domain point to web application

https://aws.amazon.com/blogs/networking-and-content-delivery/improving-availability-and-performance-for-application-load-balancers-using-one-click-integration- with-aws-global-accelerator/

18. - (Topic 1)

A company is migrating a distributed application to AWS The application serves variable workloads The

legacy platform consists of a primary server trial coordinates jobs across multiple compute nodes The company wants to modernize the application with a solution that maximizes resiliency and scalability. How should a solutions architect design the architecture to meet these requirements?

A. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure EC2 Auto Scaling to use scheduled scaling

B. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs Implement the compute nodes with Amazon EC2 Instances that are managed in an Auto Scaling group Configure EC2 Auto Scaling based on the size of the queue

C. Implement the primary server and the compute nodes with Amazon EC2 instances that are managed In an Auto Scaling group. Configure AWS CloudTrail as a destination for the fobs Configure EC2 Auto Scaling based on the load on the primary server

D. implement the primary server and the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group Configure Amazon EventBridge (Amazon CloudWatch Events) as a destination for the jobs Configure EC2 Auto Scaling based on the load on the compute nodes

Answer: B

Explanation:

To maximize resiliency and scalability, the best solution is to use an Amazon SQS queue as a destination for the jobs. This decouples the primary server from the compute nodes, allowing them to scale independently. This also helps to prevent job loss in the event of a failure. Using an Auto Scaling group of Amazon EC2 instances for the compute nodes allows for automatic scaling based on the workload. In this case, it's recommended to configure the Auto Scaling group based on the size of the Amazon SQS queue, which is a better indicator of the actual workload than the load on the primary server or compute nodes. This approach ensures that the application can handle variable workloads, while also minimizing costs by automatically scaling up or down the compute nodes as needed.

19. - (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. Query the tags to retrieve the files from S3 Glacier Instant Retrieval.

B. Store individual files in Amazon S3 Intelligent-Tiering. Use S3 Lifecycle policies to move the files to S3 Glacier Flexible Retrieval after 1 year. Query and retrieve the files that are in Amazon S3 by using Amazon Athena. Query and retrieve the files that are in S3 Glacier by using S3 Glacier Select.

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

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

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/

20. - (Topic 1)

A company is implementing a new business application. The application runs on two Amazon EC2 instances and uses an Amazon S3 bucket for document storage. A solutions architect needs to ensure that the EC2 instances can access the S3 bucket.

What should the solutions architect do to meet this requirement?

A. Create an IAM role that grants access to the S3 bucket. Attach the role to the EC2 instances.

B. Create an IAM policy that grants access to the S3 bucket. Attach the policy to the EC2 instances.

C. Create an IAM group that grants access to the S3 bucket. Attach the group to the EC2 instances.

D. Create an IAM user that grants access to the S3 bucket. Attach the user account to the EC2 instances.

Answer: A

Explanation:

https://aws.amazon.com/premiumsupport/knowledge-center/ec2-instance-access-s3- bucket/

21. - (Topic 1)

A company uses NFS to store large video files in on-premises network attached storage. Each video file ranges in size from 1MB to 500 GB. The total storage is 70 TB and is no longer growing. The company decides to migrate the video files to Amazon S3. The company must migrate the video files as soon as possible while using the least possible network bandwidth.

Which solution will meet these requirements?

A. Create an S3 bucket Create an IAM role that has permissions to write to the S3 bucket. Use the AWS CLI to copy all files locally to the S3 bucket.

B. Create an AWS Snowball Edge job. Receive a Snowball Edge device on premises. Use the Snowball Edge client to transfer data to the device. Return the device so that AWS can import the data into Amazon S3.

C. Deploy an S3 File Gateway on premises. Create a public service endpoint to connect to the S3 File Gateway Create an S3 bucket Create a new NFS file share on the S3 File Gateway Point the new file share to the S3 bucket. Transfer the data from the existing NFS file share to the S3 File Gateway.

D. Set up an AWS Direct Connect connection between the on-premises network and AWS. Deploy an S3 File Gateway on premises. Create a public virtual interlace (VIF) to connect to the S3 File Gateway. Create an S3 bucket. Create a new NFS file share on the S3 File Gateway. Point the new file share to the S3 bucket. Transfer the data from the existing NFS file share to the S3 File Gateway.

Answer: B

Explanation:

The basic difference between Snowball and Snowball Edge is the capacity they provide. Snowball provides a total of 50 TB or 80 TB, out of which 42 TB or 72 TB is available, while Amazon Snowball Edge provides 100 TB, out of which 83 TB is available.

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

23. - (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.

24. - (Topic 1)

A company is developing an application that provides order shipping statistics for retrieval by a REST API. The company wants to extract the shipping statistics, organize the data into an easy-to-read HTML format, and send the report to several email addresses at the same time every morning.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

A. Configure the application to send the data to Amazon Kinesis Data Firehose.

B. Use Amazon Simple Email Service (Amazon SES) to format the data and to send the report by email.

C. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Glue job to query the application's API for the data.

D. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Lambda function to query the application's API for the data.

E. Store the application data in Amazon S3. Create an Amazon Simple Notification Service (Amazon SNS) topic as an S3 event destination to send the report by

Answer: B,D

Explanation:

https://docs.aws.amazon.com/ses/latest/dg/send-email-formatted.html

* D. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Lambda function to query the application's API for the data. This step can be done using AWS Lambda to extract the shipping statistics and organize the data into an HTML format.

* B. Use Amazon Simple Email Service (Amazon SES) to format the data and send the report by email. This step can be done by using Amazon SES to send the report to multiple email addresses at the same time every morning.

Therefore, options D and B are the correct choices for this question. Option A is incorrect because Kinesis Data Firehose is not necessary for this use case. Option C is incorrect because AWS Glue is not required to query the application's API. Option E is incorrect because S3 event notifications cannot be used to send the

report by email.

25. - (Topic 1)

A development team needs to host a website that will be accessed by other teams. The website contents consist of HTML, CSS, client-side JavaScript, and images Which method is the MOST cost-effective for hosting the website?

A. Containerize the website and host it in AWS Fargate.

B. Create an Amazon S3 bucket and host the website there

C. Deploy a web server on an Amazon EC2 instance to host the website.

D. Configure an Application Loa d Balancer with an AWS Lambda target that uses the Express js framework.

Answer: B

Explanation:

In Static Websites, Web pages are returned by the server which are prebuilt. They use simple languages such as HTML, CSS, or JavaScript.

There is no processing of content on the server (according to the user) in Static Websites. Web pages are returned by the server with no change therefore, static Websites are fast.

There is no interaction with databases.

Also, they are less costly as the host does not need to support server-side processing with different languages.

==========

In Dynamic Websites, Web pages are returned by the server which are processed during runtime means they are not prebuilt web pages but they are built during runtime according to the user's demand.

These use server-side scripting languages such as PHP, Node.js, ASP.NET and many more supported by the server.

So, they are slower than static websites but updates and interaction with databases are possible.

26. - (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. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.

B. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production Use database cloning to create the staging database on-demand

C. Use Amazon RDS for MySQL with a Mufti AZ deployment and read replicas for production Use the standby instance tor the staging database.

D. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.

Answer: B

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

27. - (Topic 1)

A company uses 50 TB of data for reporting. The company wants to move this data from on premises to AWS A custom application in the company's data center runs a weekly data transformation job. The company plans to pause the application until the data transfer is complete and needs to begin the transfer process as soon as possible.

The data center does not have any available network bandwidth for additional workloads A solutions architect must transfer the data and must configure the transformation job to continue to run in the AWS Cloud

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

A. Use AWS DataSync to move the data Create a custom transformation job by using AWS Glue

B. Order an AWS Snowcone device to move the data Deploy the transformation application to the device

C. Order an AWS Snowball Edge Storage Optimized device. Copy the data to the device. Create a custom transformation job by using AWS Glue

D. Order an AWS D. Snowball Edge Storage Optimized device that includes Amazon EC2 compute Copy the data to the device Create a new EC2 instance on AWS to run the transformation application

Answer: D

Explanation:

AWS Snowball Edge is a type of Snowball device with on-board storage and compute power for select AWS capabilities. Snowball Edge can do local processing and edge- computing workloads in addition to transferring data between your local environment and the AWS Cloud1. Users can order an AWS Snowball Edge Storage Optimized device that includes Amazon EC2 compute to move 50 TB of data from on premises to AWS. The Storage Optimized device has 80 TB of usable storage and 40 vCPUs of compute power2. Users can copy the data to the device using the AWS OpsHub graphical user interface or the Snowball client command line tool3. Users can also create and run Amazon EC2 instances on the device using Amazon Machine Images (AMIs) that are compatible with the sbe1 instance type. Users can use the Snowball Edge device to transfer the data and run the transformation job locally without using any network bandwidth.

Users can also create a new EC2 instance on AWS to run the transformation application after the data transfer is complete. Amazon EC2 is a web service that provides secure, resizable compute capacity in the cloud. Users can launch an EC2 instance in the same AWS Region where they send their Snowball Edge device and choose an AMI that matches their application requirements. Users can use the EC2 instance to continue running the transformation job in the AWS Cloud.

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. Associate the target group with

the Auto Scaling group. Use the NLB as an AWS Global Accelerator endpoint in each Region.

B. Deploy an Application Load Balancer (ALB) and an associated target group. Associate the target group with the Auto Scaling group. Use the ALB as an AWS Global Accelerator endpoint in each Region.

C. Deploy a Network Load Balancer (NLB) and an associated target group. Associate the target group with the Auto Scaling group. Create an Amazon Route 53 latency record that points to aliases for each NLB. Create an Amazon CloudFront distribution that uses the latency record as an origin.

D. Deploy an Application Load Balancer (ALB) and an associated target group. Associate the target group with the Auto Scaling group. Create an Amazon Route 53 weighted record that points to aliases for each ALB. Deploy an Amazon CloudFront distribution that uses the weighted record as an origin.

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 Egde Locations – Cloutfront

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..

29. - (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/

30. - (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 NLB. supplying the URL of the company's application.

B. Add a cron job to the EC2 instances to check the local application's logs once each minute. If HTTP errors are detected, the application will restart.

C. Replace the NLB with an Application Load Balancer. Enable HTTP health checks by supplying the URL of the company's application. Configure an Auto Scaling action to replace unhealthy instances.

D. Create an Amazon Cloud Watch alarm that monitors the UnhealthyHostCount metric for the NLB. Configure an Auto Scaling action to replace unhealthy instances when the alarm is in the ALARM state.

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.

31. - (Topic 1)

A solutions architect is using Amazon S3 to design the storage architecture of a new digital media application. The media files must be resilient to the loss of an Availability Zone Some files are accessed frequently while other files are rarely accessed in an unpredictable pattern. The solutions architect must minimize the costs of storing and retrieving the media files.

Which storage option meets these requirements?

A. S3 Standard

B. S3 Intelligent-Tiering

C. S3 Standard-Infrequent Access {S3 Standard-IA)

D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: B

Explanation: S3 Intelligent-Tiering - Perfect use case when you don't know the frequency of access or irregular patterns of usage.

Amazon S3 offers a range of storage classes designed for different use cases. These include S3 Standard for general-purpose storage of frequently accessed data; S3 Intelligent-Tiering for data with unknown or changing access patterns; S3 Standard- Infrequent Access (S3 Standard-IA) and S3 One Zone-Infrequent Access (S3 One Zone- IA) for long-lived, but less frequently accessed data; and Amazon S3 Glacier (S3 Glacier) and Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive) for long-term archive and digital preservation. If you have data residency requirements that can't be met by an existing AWS Region, you can use the S3 Outposts storage class to store your S3 data on- premises. Amazon S3 also offers capabilities to manage your data throughout its lifecycle. Once an S3 Lifecycle policy is set, your data will automatically transfer to a different storage class without any changes to your application.

https://aws.amazon.com/getting-started/hands-on/getting-started-using-amazon-s3-intelligent-tiering/?nc1=h_ls

32. - (Topic 1)

A company needs the ability to analyze the log files of its proprietary application. The logs are stored in JSON format in an Amazon S3 bucket Queries will be simple and will run on- demand A solutions architect needs to perform the analysis with minimal changes to the existing architecture

What should the solutions architect do to meet these requirements with the LEAST amount of operational overhead?

A. Use Amazon Redshift to load all the content into one place and run the SQL queries as needed

B. Use Amazon CloudWatch Logs to store the logs Run SQL queries as needed from the Amazon CloudWatch console

C. Use Amazon Athena directly with Amazon S3 to run the queries as needed

D. Use AWS Glue to catalog the logs Use a transient Apache Spark cluster on Amazon EMR to run the

SQL queries as needed

Answer: C

Explanation:

Amazon Athena can be used to query JSON in S3

33. - (Topic 1)

A company wants to run its critical applications in containers to meet requirements tor 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)- op6mized 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

34. - (Topic 1)

A company is hosting a static website on Amazon S3 and is using Amazon Route 53 for DNS. The website is experiencing increased demand from around the world. The company must decrease latency for users who access the website.

Which solution meets these requirements MOST cost-effectively?

A. Replicate the S3 bucket that contains the website to all AWS Regions. Add Route 53 geolocation routing entries.

B. Provision accelerators in AWS Global Accelerator. Associate the supplied IP addresses with the S3 bucket. Edit the Route 53 entries to point to the IP addresses of the accelerators.

C. Add an Amazon CloudFront distribution in front of the S3 bucket. Edit the Route 53 entries to point to the CloudFront distribution.

D. Enable S3 Transfer Acceleration on the bucket. Edit the Route 53 entries to point to the new endpoint.

Answer: C

Explanation:

Amazon CloudFront is a content delivery network (CDN) that caches content at edge locations around the world, providing low latency and high transfer speeds to users accessing the content. Adding a CloudFront distribution in front of the S3 bucket will cache the static website's content at edge locations around the world, decreasing latency for users accessing the website. This solution is also cost-effective as it only charges for the data transfer and requests made by users accessing the content from the CloudFront edge locations. Additionally, this solution provides scalability and reliability benefits as CloudFront can automatically scale to handle increased demand and provide high availability for the website.

35. - (Topic 1)

A company hosts an application on AWS Lambda functions mat 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 me Lambda functions to the maximum Create a retry mechanism in the code that stores the customer data in the database

C. Persist the customer data to Lambda local storage. Configure new Lambda functions to scan the local storage to save the customer data to the database.

D. Store the customer data m an Amazon Simple Queue Service (Amazon SOS) 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 connection concurrently which can be taxing on DB compute resources, hence RDS proxy was introduced to manage and leverage these connections efficiently.

36. - (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. Subscribe an AWS Lambda function to the topic to perform processing.

B. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) FIFO queue when the application receives an order. Configure the SQS FIFO queue to invoke an AWS Lambda function for processing.

C. Use an API Gateway authorizer to block any requests while the application processes an order.

D. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) standard queue when the application receives an order. Configure the SQS standard queue to invoke an AWS Lambda function for processing.

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.

37. - (Topic 1)

A company maintains a searchable repository of items on its website. The data is stored in an Amazon RDS for MySQL database table that contains more than 10 million rows The database has 2 TB of General Purpose SSD storage There are millions of updates against this data every day through the company's website

The company has noticed that some insert operations are taking 10 seconds or longer The company has determined that the database storage performance is the problem

Which solution addresses this performance issue?

A. Change the storage type to Provisioned IOPS SSD

B. Change the DB instance to a memory optimized instance class

C. Change the DB instance to a burstable performance instance class

D. Enable Multi-AZ RDS read replicas with MySQL native asynchronous replication.

Answer: A

Explanation: https://aws.amazon.com/ebs/features/

"Provisioned IOPS volumes are backed by solid-state drives (SSDs) and are the highest performance EBS volumes designed for your critical, I/O intensive database applications.

These volumes are ideal for both IOPS-intensive and throughput-intensive workloads that require extremely low latency."

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

38. - (Topic 1)

A company recently migrated a message processing system to AWS. The system receives messages into an ActiveMQ queue running on an Amazon EC2 instance. Messages are processed by a consumer application running on Amazon EC2. The consumer application processes the messages and writes results to a MySQL database funning on Amazon EC2. The company wants this application to be highly available with tow operational complexity

Which architecture otters the HGHEST availability?

A. Add a second ActiveMQ server to another Availably Zone Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.

B. Use Amazon MO with active/standby brokers configured across two Availability Zones Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.

C. Use Amazon MO with active/standby blotters configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Use Amazon ROS tor MySQL with Multi-AZ enabled.

D. Use Amazon MQ with active/standby brokers configured across two Availability Zones Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use Amazon RDS for MySQL with Multi-AZ enabled.

Answer: D

Explanation:

Amazon S3 is a highly scalable and durable object storage service that can store and retrieve any amount of data from anywhere on the web1. Users can configure the application to upload images directly from each user's browser to Amazon S3 through the use of a presigned URL. A presigned URL is a URL that gives access to an object in an S3 bucket for a limited time and with a specific action, such as uploading an object2. Users can generate a presigned URL programmatically using the AWS SDKs or AWS CLI. By using a presigned URL, users can reduce coupling within the application and improve website performance, as they do not need to send the images to the web server first. AWS Lambda is a serverless compute service that runs code in response to events and automatically manages the underlying compute resources3. Users can configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded. S3 Event Notifications is a feature that allows users to receive notifications when certain events happen in an S3 bucket, such as object creation or deletion. Users can configure S3 Event Notifications to invoke a Lambda function that resizes the image and stores it back in the same or a different S3 bucket. This way, users can offload the image resizing task from the web server to Lambda.

39. - (Topic 1)

A company's containerized application runs on an Amazon EC2 instance. The application needs to download security certificates before it can communicate with other business applications. The company wants a highly secure solution to encrypt and decrypt the certificates in near real time. The solution also

needs to store data in highly available storage after the data is encrypted.

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

A. Create AWS Secrets Manager secrets for encrypted certificates. Manually update the certificates as needed. Control access to the data by using fine-grained IAM access.

B. Create an AWS Lambda function that uses the Python cryptography library to receive and perform encryption operations. Store the function in an Amazon S3 bucket.

C. Create an AWS Key Management Service (AWS KMS) customer managed key. Allow the EC2 role to use the KMS key for encryption operations. Store the encrypted data on Amazon S3.

D. Create an AWS Key Management Service (AWS KMS) customer managed key. Allow the EC2 role to use the KMS key for encryption operations. Store the encrypted data on Amazon Elastic Block Store (Amazon EBS) volumes.

Answer: D

40. - (Topic 1)

A company runs an ecommerce application on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales based on CPU utilization metrics. The ecommerce application stores the transaction data in a MySQL 8.0 database that is hosted on a large EC2 instance.

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

Which solution will meet these requirements?

A. Use Amazon Redshift with a single node for leader and compute functionality.

B. Use Amazon RDS with a Single-AZ deployment Configure Amazon RDS to add reader instances in a different Availability Zone.

C. Use Amazon Aurora with a Multi-AZ deployment. Configure Aurora Auto Scaling with Aurora Replicas.

D. Use Amazon ElastiCache for Memcached with EC2 Spot Instances.

Answer: C

Explanation: AURORA is 5x performance improvement over MySQL on RDS and handles more read requests than write,; maintaining high availability = Multi-AZ deployment

41. - (Topic 1)

A company has a website hosted on AWS. The website is behind an Application Load Balancer (ALB) that is configured to handle HTTP and HTTPS separately. The company wants to forward all requests to the website so that the requests will use HTTPS.

What should a solutions architect do to meet this requirement?

A. Update the ALB's network ACL to accept only HTTPS traffic

B. Create a rule that replaces the HTTP in the URL with HTTPS.

C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.

D. Replace the ALB with a Network Load Balancer configured to use Server Name Indication (SNI).

Answer: C

Explanation:

https://aws.amazon.com/premiumsupport/knowledge-center/elb-redirect-http-to-https- using-alb/

How can I redirect HTTP requests to HTTPS using an Application Load Balancer? Last updated: 2020-10-30 I want to redirect HTTP requests to HTTPS using Application Load Balancer listener rules. How can I do this? Resolution Reference:

https://aws.amazon.com/premiumsupport/knowledge-center/elb-redirect-http-to-https- using-alb/

42. - (Topic 1)

A company needs to store data in Amazon S3 and must prevent the data from being changed. The company wants new objects that are uploaded to Amazon S3 to remain unchangeable for a nonspecific amount of time until the company decides to modify the objects. Only specific users in the company's AWS account can have the ability to delete the objects. What should a solutions architect do to meet these requirements?

A. Create an S3 Glacier vault Apply a write-once, read-many (WORM) vault lock policy to the objects

B. Create an S3 bucket with S3 Object Lock enabled Enable versioning Set a retention period of 100 years Use governance mode as the S3 bucket's default retention mode for new objects

C. Create an S3 bucket Use AWS CloudTrail to (rack any S3 API events that modify the objects Upon notification, restore the modified objects from any backup versions that the company has

D. Create an S3 bucket with S3 Object Lock enabled Enable versioning Add a legal hold to the objects Add

the s3 PutObjectLegalHold permission to the IAM policies of users who need to delete the objects

Answer: D

Explanation:

"The Object Lock legal hold operation enables you to place a legal hold on an object version. Like setting a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed."

https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-legal-hold.html

43. - (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. Enter the product manager's email address, and complete the sharing steps. Provide a shareable link for the dashboard to the product manager.

B. Create an IAM user specifically for the product manager. Attach the CloudWatch Read Only Access managed policy to the user. Share the new login credential with the product manager. Share the browser URL of the correct dashboard with the product manager.

C. Create an IAM user for the company's employees, Attach the View Only Access AWS managed policy to the IAM user. Share the new login credentials with the product manager. Ask the product manager to navigate to the CloudWatch console and locate the dashboard by name in the Dashboards section.

D. Deploy a bastion server in a public subnet. When the product manager requires access to the dashboard, start the server and share the RDP credentials. On the bastion server, ensure that the browser is configured to open the dashboard URL with cached AWS credentials that have appropriate permissions to view the dashboard.

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.

44. - (Topic 1)

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

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

A. Copy the data so both EBS volumes contain all the documents.

B. Configure the Application Load Balancer to direct a user to the server with the documents

C. Copy the data from both EBS volumes to Amazon EFS Modify the application to save new documents to Amazon EFS

D. Configure the Application Load Balancer to send the request to both servers Return each document from the correct server.

Answer: C

Explanation:

https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html#how-it-works-ec2

45. - (Topic 1)

A company has a large Microsoft SharePoint deployment running on-premises that requires Microsoft Windows shared file storage. The company wants to migrate this workload to the AWS Cloud and is considering various storage options. The storage solution must be highly available and integrated with Active Directory for access control.

Which solution will satisfy these requirements?

A. Configure Amazon EFS storage and set the Active Directory domain for authentication

B. Create an SMB Me share on an AWS Storage Gateway tile gateway in two Availability Zones

C. Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume

D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication

Answer: D

46. - (Topic 1)

A company has created an image analysis application in which users can upload photos and add photo frames to their images. The users upload images and metadata to indicate which photo frames they want to add to their images. The application uses a single Amazon EC2 instance and Amazon DynamoDB to store the metadata.

The application is becoming more popular, and the number of users is increasing. The company expects the number of concurrent users to vary significantly depending on the time of day and day of week. The company must ensure that the application can scale to meet the needs of the growing user base.

Which solution meats these requirements?

A. Use AWS Lambda to process the photos. Store the photos and metadata in DynamoDB.

B. Use Amazon Kinesis Data Firehose to process the photos and to store the photos and metadata.

C. Use AWS Lambda to process the photos. Store the photos in Amazon S3. Retain DynamoDB to store the metadata.

D. Increase the number of EC2 instances to three. Use Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volumes to store the photos and metadata.

Answer: C

Explanation:

https://www.quora.com/How-can-I-use-DynamoDB-for-storing-metadata-for-Amazon-S3-objects

This solution meets the requirements of scalability, performance, and availability. AWS Lambda can process the photos in parallel and scale up or down automatically depending on the demand. Amazon S3 can store the photos and metadata reliably and durably, and provide high availability and low latency. DynamoDB can store the metadata efficiently and provide consistent performance. This solution also reduces the cost and complexity of managing EC2 instances and EBS volumes.

Option A is incorrect because storing the photos in DynamoDB is not a good practice, as it can increase the

storage cost and limit the throughput. Option B is incorrect because Kinesis Data Firehose is not designed for processing photos, but for streaming data to destinations such as S3 or Redshift. Option D is incorrect because increasing the number of EC2 instances and using Provisioned IOPS SSD volumes does not guarantee scalability, as it depends on the load balancer and the application code. It also increases the cost and complexity of managing the infrastructure.

References:

- https://aws.amazon.com/certification/certified-solutions-architect-professional/
- https://www.examtopics.com/discussions/amazon/view/7193-exam-aws-certified-solutions-architect-professional-topic-1/
- https://aws.amazon.com/architecture/

47. - (Topic 1)

An image-processing company has a web application that users use to upload images. The application uploads the images into an Amazon S3 bucket. The company has set up S3 event notifications to publish the object creation events to an Amazon Simple Queue Service (Amazon SQS) standard queue. The SQS queue serves as the event source for an AWS Lambda function that processes the images and sends the results to users through email.

Users report that they are receiving multiple email messages for every uploaded image. A solutions architect determines that SQS messages are invoking the Lambda function more than once, resulting in multiple email messages.

What should the solutions architect do to resolve this issue with the LEAST operational overhead?

A. Set up long polling in the SQS queue by increasing the ReceiveMessage wait time to 30 seconds.

B. Change the SQS standard queue to an SQS FIFO queue. Use the message deduplication ID to discard duplicate messages.

C. Increase the visibility timeout in the SQS queue to a value that is greater than the total of the function timeout and the batch window timeout.

D. Modify the Lambda function to delete each message from the SQS queue immediately after the message is read before processing.

Answer: C

48. - (Topic 1)

A company wants to migrate an on-premises data center to AWS. The data canter hosts an SFTP server that stores its data on an NFS-based file system. The server holds 200 GB of data that needs to be transferred. The server must be hosted on an Amazon EC2 instance that uses an Amazon Elastic File System (Amazon EFS) file system

When combination of steps should a solutions architect take to automate this task? (Select TWO)

A. Launch the EC2 instance into the same Avalability Zone as the EFS fie system

B. install an AWS DataSync agent m the on-premises data center

C. Create a secondary Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instance tor the data

D. Manually use an operating system copy command to push the data to the EC2 instance

E. Use AWS DataSync to create a suitable location configuration for the onprermises SFTP server

Answer: B,E

Explanation: AWS DataSync is an online data movement and discovery service that simplifies data migration and helps users quickly, easily, and securely move their file or object data to, from, and between AWS storage services1. Users can use AWS DataSync to transfer data between on-premises and AWS storage services. To use AWS DataSync, users need to install an AWS DataSync agent in the on-premises data center. The agent is a software appliance that connects to the source or destination storage system and handles the data transfer to or from AWS over the network2. Users also need to use AWS DataSync to create a suitable location configuration for the on-premises SFTP server. A location is a logical representation of a storage system that contains files or objects that users want to transfer using DataSync. Users can create locations for NFS shares, SMB shares, HDFS file systems, self-managed object storage, Amazon S3 buckets, Amazon EFS file systems, Amazon FSx for Windows File Server file systems, Amazon FSx for Lustre file systems, Amazon FSx for OpenZFS file systems, Amazon FSx for NetApp ONTAP file systems, and AWS Snowcone devices3.

49. - (Topic 1)

A company has a data ingestion workflow that consists the following:

- An Amazon Simple Notification Service (Amazon SNS) topic for notifications about new data deliveries

- An AWS Lambda function to process the data and record metadata

The company observes that the ingestion workflow fails occasionally because of network connectivity issues. When such a failure occurs, the Lambda function does not ingest the corresponding data unless the company manually reruns the job.

Which combination of actions should a solutions architect take to ensure that the Lambda function ingests all data in the future? (Select TWO.)

A. Configure the Lambda function In multiple Availability Zones.

B. Create an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe It to me SNS topic.

C. Increase the CPU and memory that are allocated to the Lambda function.

D. Increase provisioned throughput for the Lambda function.

E. Modify the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue

Answer: B,E

Explanation: To ensure that the Lambda function ingests all data in the future despite occasional network connectivity issues, the following actions should be taken:

- Create an Amazon Simple Queue Service (SQS) queue and subscribe it to the SNS topic. This allows for decoupling of the notification and processing, so that even if the processing Lambda function fails, the message remains in the queue for further processing later.
- Modify the Lambda function to read from the SQS queue instead of directly from SNS. This decoupling allows for retries and fault tolerance and ensures that all messages are processed by the Lambda function.

Reference:

AWS SNS documentation: https://aws.amazon.com/sns/ AWS SQS documentation: https://aws.amazon.com/sqs/

AWS Lambda documentation: https://aws.amazon.com/lambda/

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. Store the backup in an Amazon S3 bucket. Set an S3 Lifecycle configuration for the S3 bucket.

D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function. Configure the Lambda function to back up the table and to store the backup in an Amazon S3 bucket. Set an S3 Lifecycle configuration for the S3 bucket.

Answer: C

51. - (Topic 1)

An ecommerce company wants to launch a one-deal-a-day website on AWS. Each day will feature exactly one product on sale for a period of 24 hours. The company wants to be able to handle millions of requests each hour with millisecond latency during peak hours.

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

A. Use Amazon S3 to host the full website in different S3 buckets Add Amazon CloudFront distributions Set the S3 buckets as origins for the distributions Store the order data in Amazon S3

B. Deploy the full website on Amazon EC2 instances that run in Auto Scaling groups across multiple Availability Zones Add an Application Load Balancer (ALB) to distribute the website traffic Add another ALB for the backend APIs Store the data in Amazon RDS for MySQL

C. Migrate the full application to run in containers Host the containers on Amazon Elastic Kubernetes Service (Amazon EKS) Use the Kubernetes Cluster Autoscaler to increase and decrease the number of pods to process bursts in traffic Store the data in Amazon RDS for MySQL

D. Use an Amazon S3 bucket to host the website's static content Deploy an Amazon CloudFront distribution. Set the S3 bucket as the origin Use Amazon API Gateway and AWS Lambda functions for the backend APIs Store the data in Amazon DynamoDB

Answer: D

Explanation: To launch a one-deal-a-day website on AWS with millisecond latency during peak hours and with the least operational overhead, the best option is to use an Amazon S3 bucket to host the website's static content, deploy an Amazon CloudFront distribution, set the S3 bucket as the origin, use Amazon API Gateway and AWS Lambda functions for the backend APIs, and store the data in Amazon DynamoDB. This option requires minimal operational overhead and can handle millions of requests each hour with millisecond latency during peak hours. Therefore, option D is the correct answer.

Reference:

https://aws.amazon.com/blogs/compute/building-a-serverless-multi-player-game-with-aws-lambda-and-amazon-dynamodb/

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. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate IAM roles.

B. Create an analysis in Amazon OuickSighl. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate users and groups.

C. Create an AWS Glue table and crawler for the data in Amazon S3. Create an AWS Glue extract, transform, and load (ETL) job to produce reports. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.

D. Create an AWS Glue table and crawler for the data in Amazon S3. Use Amazon Athena Federated Query to access data within Amazon RDS for PoslgreSQL. Generate reports by using Amazon Athena. 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

53. - (Topic 1)

A company is implementing a shared storage solution for a media application that is hosted m the AWS Cloud The company needs the ability to use SMB clients to access data The solution must he fully managed.

Which AWS solution meets these requirements?

A. Create an AWS Storage Gateway volume gateway. Create a file share that uses the required client protocol Connect the application server to the file share.

B. Create an AWS Storage Gateway tape gateway Configure (apes to use Amazon S3 Connect the application server lo the tape gateway

C. Create an Amazon EC2 Windows instance Install and configure a Windows file share role on the instance. Connect the application server to the file share.

D. Create an Amazon FSx for Windows File Server tile system Attach the fie system to the origin server. Connect the application server to the file system

Answer: D

Explanation:

https://aws.amazon.com/fsx/lustre/

Amazon FSx has native support for Windows file system features and for the industry- standard Server Message Block (SMB) protocol to access file storage over a network.

https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html

54. - (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

55. - (Topic 1)

A company runs multiple Windows workloads on AWS. The company's employees use Windows file shares that are hosted on two Amazon EC2 instances. The file shares synchronize data between themselves and maintain duplicate copies. The company wants a highly available and durable storage solution that preserves how users currently access the files.

What should a solutions architect do to meet these requirements?

A. Migrate all the data to Amazon S3 Set up IAM authentication for users to access files

B. Set up an Amazon S3 File Gateway. Mount the S3 File Gateway on the existing EC2 Instances.

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

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

Answer: C

Explanation: https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/AmazonEFS.html Amazon FSx for Windows File Server provides fully managed Microsoft Windows file servers, backed by a fully native Windows file system. https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html

56. - (Topic 1)

A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon EC2 instance in a public subnet of a VPC A solutions architect needs to connect from the on-premises

network, through the company's internet connection to the bastion host and to the application servers The solutions architect must make sure that the security groups of all the EC2 instances will allow that access

Which combination of steps should the solutions architect take to meet these requirements? (Select TWO)

A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances

B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company

C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company

D. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host

E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host

Answer: C,D

Explanation: https://digitalcloud.training/ssh-into-ec2-in-private-subnet/

57. - (Topic 1)

A company wants to improve its ability to clone large amounts of production data into a test environment in the same AWS Region. The data is stored in Amazon EC2 instances on Amazon Elastic Block Store (Amazon EBS) volumes. Modifications to the cloned data must not affect the production environment. The software that accesses this data requires consistently high I/O performance.

A solutions architect needs to minimize the time that is required to clone the production data into the test environment.

Which solution will meet these requirements?

A. Take EBS snapshots of the production EBS volumes. Restore the snapshots onto EC2 instance store volumes in the test environment.

B. Configure the production EBS volumes to use the EBS Multi-Attach feature. Take EBS snapshots of the production EBS volumes. Attach the production EBS volumes to the EC2 instances in the test environment.

C. Take EBS snapshots of the production EBS volumes. Create and initialize new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment before restoring the volumes from the production EBS snapshots.

D. Take EBS snapshots of the production EBS volumes. Turn on the EBS fast snapshot restore feature on the EBS snapshots. Restore the snapshots into new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment.

Answer: C

Explanation:

To clone the production data into the test environment with high I/O performance and without affecting the production environment, the best option is to take EBS snapshots of the production EBS volumes and restore them onto new EBS volumes in the test environment. Then, attach the new EBS volumes to EC2 instances in the test environment. This option minimizes the time required to clone the data and ensures that modifications to the cloned data do not affect the production environment. Therefore, option C is the correct answer.

Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-restoring-volume.html

58. - (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 URL. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM).

B. Create Route 53 DNS records with the company's domain name. Point the alias record to the Regional API Gateway stage endpoint. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region.

C. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Region. Attach the certificate to the API Gateway endpoint. Configure Route 53 to route traffic to the API Gateway endpoint.

D. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region. Attach the certificate to the API Gateway APIs. Create Route 53 DNS records with the company's domain name. Point an A record to the company's domain name.

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.

59. - (Topic 1)

A company is running an SMB file server in its data center. The file server stores large files that are accessed frequently for the first few days after the files are created. After 7 days the files are rarely accessed.

The total data size is increasing and is close to the company's total storage capacity. A solutions architect must increase the company's available storage space without losing low-latency access to the most recently accessed files. The solutions architect must also provide file lifecycle management to avoid future storage issues.

Which solution will meet these requirements?

A. Use AWS DataSync to copy data that is older than 7 days from the SMB file server to AWS.

B. Create an Amazon S3 File Gateway to extend the company's storage space. Create an S3 Lifecycle policy to transition the data to S3 Glacier Deep Archive after 7 days.

C. Create an Amazon FSx for Windows File Server file system to extend the company's storage space.

D. Install a utility on each user's computer to access Amazon S3. Create an S3 Lifecycle policy to transition the data to S3 Glacier Flexible Retrieval after 7 days.

Answer: B

Explanation: Amazon S3 File Gateway is a hybrid cloud storage service that enables on- premises

applications to seamlessly use Amazon S3 cloud storage. It provides a file interface to Amazon S3 and supports SMB and NFS protocols. It also supports S3 Lifecycle policies that can automatically transition data from S3 Standard to S3 Glacier Deep Archive after a specified period of time. This solution will meet the requirements of increasing the company's available storage space without losing low-latency access to the most recently accessed files and providing file lifecycle management to avoid future storage issues.

Reference:

https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.ht ml

60. - (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 Add Permission API call to add appropriate permissions

C. Use the ReceiveMessage API call to set an appropriate wail 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 best suite & other Options ruled out [Option A - You can't intruduce one more Queue in the existing one; Option B - only Permission & Option C - Only Retrieves Messages] FIF O 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).

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 AM' 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 needs 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

62. - (Topic 1)

A company needs to review its AWS Cloud deployment to ensure that its Amazon S3 buckets do not have unauthorized configuration changes.

What should a solutions architect do to accomplish this goal?

A. Turn on AWS Config with the appropriate rules.

B. Turn on AWS Trusted Advisor with the appropriate checks.

C. Turn on Amazon Inspector with the appropriate assessment template.

D. Turn on Amazon S3 server access logging. Configure Amazon EventBridge (Amazon Cloud Watch Events).

Answer: A

Explanation:

To ensure that Amazon S3 buckets do not have unauthorized configuration changes, a solutions architect should turn on AWS Config with the appropriate rules. AWS Config is a service that allows users to audit and assess their AWS resource configurations for compliance with industry standards and internal policies. It provides a detailed view of the resources and their configurations, including information on how the resources are related to each other. By turning on AWS Config with the appropriate rules, users can identify and remediate unauthorized configuration changes to their Amazon S3 buckets.

63. - (Topic 1)

A company is storing sensitive user information in an Amazon S3 bucket The company wants to provide secure access to this bucket from the application tier running on Ama2on EC2 instances inside a VPC. Which combination of steps should a solutions architect take to accomplish this? (Select TWO.)

A. Configure a VPC gateway endpoint for Amazon S3 within the VPC

B. Create a bucket policy to make the objects to the S3 bucket public

C. Create a bucket policy that limits access to only the application tier running in the VPC

D. Create an IAM user with an S3 access policy and copy the IAM credentials to the EC2 instance

E. Create a NAT instance and have the EC2 instances use the NAT instance to access the S3 bucket

Answer: A,C

Explanation:

https://aws.amazon.com/premiumsupport/knowledge-center/s3-private-connection-no-authentication/

64. - (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. Use multipart uploads to directly upload site data to the destination bucket.

B. Upload site data to an Amazon S3 bucket in the closest AWS Region. Use S3 cross- Region replication to copy objects to the destination bucket.

C. Schedule AWS Snowball jobs daily to transfer data to the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.

D. Upload the data to an Amazon EC2 instance in the closest Region. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. Once a day take an EBS snapshot and copy it to the centralized Region. Restore the EBS volume in the centralized Region and run an analysis on the data daily.

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:

"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."

65. - (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: A,C

Explanation: (https://aws.amazon.com/cloudfront

66. - (Topic 1)

A company is building an application in the AWS Cloud. The application will store data in Amazon S3

buckets in two AWS Regions. The company must use an AWS Key Management Service (AWS KMS) customer managed key to encrypt all data that is stored in the S3 buckets. The data in both S3 buckets must be encrypted and decrypted with the same KMS key. The data and the key must be stored in each of the two Regions.

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

A. Create an S3 bucket in each Region Configure the S3 buckets to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) Configure replication between the S3 buckets.

B. Create a customer managed multi-Region KMS key. Create an S3 bucket in each Region. Configure replication between the S3 buckets. Configure the application to use the KMS key with client-side encryption.

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

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

Answer: B

Explanation:

From https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store- overview.html

For most users, the default AWS KMS key store, which is protected by FIPS 140-2 validated cryptographic modules, fulfills their security requirements. There is no need to add an extra layer of maintenance responsibility or a dependency on an additional service. However, you might consider creating a custom key store if your organization has any of the following requirements: Key material cannot be stored in a shared environment. Key material must be subject to a secondary, independent audit path. The HSMs that generate and store key material must be certified at FIPS 140-2 Level 3.

https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.html

https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-overview.html

67. - (Topic 1)

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

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

What is the effect of this policy?

A. Users can terminate an EC2 instance in any AWS Region except us-east-1.

B. Users can terminate an EC2 instance with the IP address 10 100 100 1 in the us-east-1 Region

C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.

D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100 100 254

Answer: C

Explanation: as the policy prevents anyone from doing any EC2 action on any region except us-east-1 and allows only users with source ip 10.100.100.0/24 to terminate instances. So user with source ip 10.100.100.254 can terminate instances in us-east-1 region.

68. - (Topic 1)

A company is planning to use an Amazon DynamoDB table for data storage. The company is concerned about cost optimization. The table will not be used on most mornings. In the evenings, the read and write traffic will often be unpredictable. When traffic spikes occur, they will happen very quickly.

What should a solutions architect recommend?

A. Create a DynamoDB table in on-demand capacity mode.

B. Create a DynamoDB table with a global secondary index.

C. Create a DynamoDB table with provisioned capacity and auto scaling.

D. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table.

Answer: A

69. - (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. Provision a second VPN tunnel for private connectivity and as a backup if the primary VPN connection fails.

C. Provision an AWS Direct Connect connection to a Region Provision a second Direct Connect connection to the same Region as a backup if the primary Direct Connect connection fails.

D. Provision an AWS Direct Connect connection to a Region Use the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails.

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/

70. - (Topic 1)

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

A. Deploy an Amazon EC2 instance to host an API that sends data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.

B. Deploy an Amazon EC2 instance to host an API that sends data to AWS Glue. Stop source/destination checking on the EC2 instance. Use AWS Glue to transform the data and to send the data to Amazon S3.

C. Configure an Amazon API Gateway API to send data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.

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

Answer: C

71. - (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: A,B

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

72. - (Topic 1)

A company has more than 5 TB of file data on Windows file servers that run on premises Users and applications interact with the data each day

The company is moving its Windows workloads to AWS. As the company continues this process, the company requires access to AWS and on-premises file storage with minimum latency The company needs a solution that minimizes operational overhead and requires no significant changes to the existing file access patterns. The company uses an AWS Site-to-Site VPN connection for connectivity to AWS

What should a solutions architect do to meet these requirements?

A. Deploy and configure Amazon FSx for Windows File Server on AWS. Move the on- premises file data to FSx for Windows File Server. Reconfigure the workloads to use FSx for Windows File Server on AWS.

B. Deploy and configure an Amazon S3 File Gateway on premises Move the on-premises file data to the S3 File Gateway Reconfigure the on-premises workloads and the cloud workloads to use the S3 File Gateway

C. Deploy and configure an Amazon S3 File Gateway on premises Move the on-premises file data to Amazon S3 Reconfigure the workloads to use either Amazon S3 directly or the S3 File Gateway, depending on each workload's location

D. Deploy and configure Amazon FSx for Windows File Server on AWS Deploy and configure an Amazon FSx File Gateway on premises Move the on-premises file data to the FSx File Gateway Configure the cloud workloads to use FSx for Windows File Server on AWS Configure the on-premises workloads to use the FSx File Gateway

Answer: D

Explanation:

https://docs.aws.amazon.com/filegateway/latest/filefsxw/what-is-file-fsxw.html

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/

73. - (Topic 1)

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

What should the solutions architect recommend?

A. Launch an Amazon EC2 instance in us-east-1 and migrate the site to it.

B. Move the website to Amazon S3. Use cross-Region replication between Regions.

C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.

D. Use an Amazon Route 53 geo-proximity routing policy pointing to on-premises servers.

Answer: C

Explanation: https://aws.amazon.com/pt/blogs/aws/amazon-cloudfront-support-for- custom-origins/

You can now create a CloudFront distribution using a custom origin. Each distribution will can point to an S3 or to a custom origin. This could be another storage service, or it could be something more interesting and more dynamic, such as an EC2 instance or even an Elastic Load Balancer

74. - (Topic 1)

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

What should a solutions architect do to accomplish this?

A. Use AWS Config rules to define and detect resources that are not properly tagged.

B. Use Cost Explorer to display resources that are not properly tagged. Tag those resources manually.

C. Write API calls to check all resources for proper tag allocation. Periodically run the code on an EC2 instance.

D. Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.

Answer: A

Explanation: To ensure all Amazon EC2 instances, Amazon RDS DB instances, and Amazon Redshift clusters are configured with tags, a solutions architect should use AWS Config rules to define and detect resources that are not properly tagged. AWS Config rules are a set of customizable rules that AWS Config uses to evaluate AWS resource configurations for compliance with best practices and company policies. Using AWS Config rules can minimize the effort of configuring and operating this check because it automates the process of identifying non-compliant resources and notifying the responsible teams.

Reference:

AWS Config Developer Guide: AWS Config Rules

(https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_use-managed- rules.html)

75. - (Topic 1)

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

Which solution will meet these requirements?

A. Migrate the application to run as containers on Amazon Elastic Container Service (Amazon ECS) Use Amazon S3 for storage

B. Migrate the application to run as containers on Amazon Elastic Kubernetes Service (Amazon EKS) Use Amazon Elastic Block Store (Amazon EBS) for storage

C. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic File System (Amazon EFS) for storage.

D. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic Block Store (Amazon EBS) for storage.

Answer: C

Explanation:

EFS is a standard file system, it scales automatically and is highly available.

76. - (Topic 1)

A company is developing a two-tier web application on AWS. The company's developers have deployed the application on an Amazon EC2 instance that connects directly to a backend Amazon RDS database. The company must not hardcode database credentials in the application. The company must also implement a solution to automatically rotate the database credentials on a regular basis.

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

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

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

C. Store the database credentials as a secret in AWS Secrets Manager. Turn on automatic rotation for the secret. Attach the required permission to the EC2 role to grant access to the secret.

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

Answer: C

Explanation: https://docs.aws.amazon.com/secretsmanager/latest/userguide/create_database_secret.ht ml

77. - (Topic 1)

A company needs to store its accounting records in Amazon S3. The records must be immediately accessible for 1 year and then must be archived for an additional 9 years. No one at the company, including administrative users and root users, can be able to delete the records during the entire 10-year period. The records must be stored with maximum resiliency.

Which solution will meet these requirements?

A. Store the records in S3 Glacier for the entire 10-year period. Use an access control policy to deny deletion of the records for a period of 10 years.

B. Store the records by using S3 Intelligent-Tiering. Use an IAM policy to deny deletion of the records. After 10 years, change the IAM policy to allow deletion.

C. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year. Use S3 Object Lock in compliance mode for a period of 10 years.

D. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 year. Use S3 Object Lock in governance mode for a period of 10 years.

Answer: C

Explanation: To meet the requirements of immediately accessible records for 1 year and then archived for an additional 9 years with maximum resiliency, we can use S3 Lifecycle policy to transition records from S3 Standard to S3 Glacier Deep Archive after 1 year. And to ensure that the records cannot be deleted by anyone, including administrative and root users, we can use S3 Object Lock in compliance mode for a period of 10 years. Therefore, the correct answer is option C.

Reference: https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html

78. - (Topic 1)

A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week.

What should the company do to guarantee the EC2 capacity?

A. Purchase Reserved instances that specify the Region needed

B. Create an On Demand Capacity Reservation that specifies the Region needed

C. Purchase Reserved instances that specify the Region and three Availability Zones needed

D. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed

Answer: D

Explanation: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity- reservations.html

Reserve instances: You will have to pay for the whole term (1 year or 3years) which is not cost effective

79. - (Topic 1)

A social media company allows users to upload images to its website. The website runs on Amazon EC2 instances. During upload requests, the website resizes the images to a standard size and stores the resized images in Amazon S3. Users are experiencing slow upload requests to the website.

The company needs to reduce coupling within the application and improve website performance. A solutions architect must design the most operationally efficient process for image uploads.

Which combination of actions should the solutions architect take to meet these requirements? (Choose two.)

A. Configure the application to upload images to S3 Glacier.

B. Configure the web server to upload the original images to Amazon S3.

C. Configure the application to upload images directly from each user's browser to Amazon S3 through the use of a presigned URL.

D. Configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded. Use the function to resize the image

E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function on a schedule to resize uploaded images.

Answer: C,D

Explanation: Amazon S3 is a highly scalable and durable object storage service that can store and retrieve any amount of data from anywhere on the web1. Users can configure the application to upload images directly from each user's browser to Amazon S3 through the use of a presigned URL. A presigned URL is a URL that gives access to an object in an S3 bucket for a limited time and with a specific action, such as uploading an object2. Users can generate a presigned URL programmatically using the AWS SDKs or AWS CLI. By using a presigned URL, users can reduce coupling within the application and improve website

performance, as they do not need to send the images to the web server first. AWS Lambda is a serverless compute service that runs code in response to events and automatically manages the underlying compute resources3. Users can configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded. S3 Event Notifications is a feature that allows users to receive notifications when certain events happen in an S3 bucket, such as object creation or deletion. Users can configure S3 Event Notifications to invoke a Lambda function that resizes the image and stores it back in the same or a different S3 bucket. This way, users can offload the image resizing task from the web server to Lambda.

80. - (Topic 1)

A company has several web servers that need to frequently access a common Amazon RDS MySQL Multi-AZ DB instance The company wants a secure method for the web servers to connect to the database while meeting a security requirement to rotate user credentials frequently.

Which solution meets these requirements?

A. Store the database user credentials in AWS Secrets Manager Grant the necessary IAM permissions to allow the web servers to access AWS Secrets Manager

B. Store the database user credentials in AWS Systems Manager OpsCenter Grant the necessary IAM permissions to allow the web servers to access OpsCenter

C. Store the database user credentials in a secure Amazon S3 bucket Grant the necessary IAM permissions to allow the web servers to retrieve credentials and access the database. D.

Store the database user credentials in files encrypted with AWS Key Management Service (AWS KMS) on the web server file system. The web server should be able to decrypt the files and access the database

Answer: A

Explanation: AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html

Secrets Manager enables you to replace hardcoded credentials in your code, including passwords, with an API call to Secrets Manager to retrieve the secret programmatically. This helps ensure the secret can't be compromised by someone examining your code, because the secret no longer exists in the code. Also, you can configure Secrets Manager to automatically rotate the secret for you according to a specified schedule.

This enables you to replace long-term secrets with short-term ones, significantly reducing the risk of compromise.

81. - (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 certificate. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.

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

C. Use AWS Certificate Manager (ACM) Private Certificate Authority to issue an SSL/TLS certificate from the root CA. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.

D. Use AWS Certificate Manager (ACM) to import an SSL/TLS certificate. Apply the certificate to the ALB. Use Amazon EventBridge (Amazon CloudWatch Events) to send a notification when the certificate is nearing expiration. Rotate the certificate manually.

Answer: D

Explanation:

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

82. - (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

83. - (Topic 1)

A company receives 10 TB of instrumentation data each day from several machines located at a single factory. The data consists of JSON files stored on a storage area network (SAN) in an on-premises data center located within the factory. The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-lime analytics. A secure transfer is important because the data is considered sensitive.

Which solution offers the MOST reliable data transfer?

A. AWS DataSync over public internet

B. AWS DataSync over AWS Direct Connect

C. AWS Database Migration Service (AWS DMS) over public internet

D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

Answer: B

Explanation: These are some of the main use cases for AWS DataSync: • Data migration – Move active datasets rapidly over the network into Amazon S3, Amazon EFS, or FSx for Windows File Server. DataSync includes automatic encryption and data integrity validation to help make sure that your data arrives securely, intact, and ready to use.

"DataSync includes encryption and integrity validation to help make sure your data arrives securely, intact, and ready to use." https://aws.amazon.com/datasync/faqs/

84. - (Topic 1)

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

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

A. Use Amazon Athena with Amazon S3

B. Use Amazon API Gateway with AWS Lambda

C. Use Amazon QuickSight with Amazon Redshift.

D. Use Amazon API Gateway with Amazon Kinesis Data Analytics

Answer: D

Explanation:

https://aws.amazon.com/solutions/implementations/aws-streaming-data-solution-for- amazon-kinesis/

85. - (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 available. Modify the CMK's key policy to allow the MSP Partner's AWS account to use the key

B. Modify the launchPermission property of the AMI. Share the AMI with the MSP Partner's AWS account only. Modify the CMK's key policy to allow the MSP Partner's AWS account to use the key.

C. Modify the launchPermission property of the AMI Share the AMI with the MSP Partner's AWS account only. Modify the CMK's key policy to trust a new CMK that is owned by the MSP Partner for encryption.

D. Export the AMI from the source account to an Amazon S3 bucket in the MSP Partner's AWS account. Encrypt the S3 bucket with a CMK that is owned by the MSP Partner Copy and launch the AMI in the MSP

Partner's AWS account.

Answer: 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

86. - (Topic 1)

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

How can the solutions architect meet this requirement?

A. Deploy Amazon API Gateway into a public subnet and adjust the route table to route S3 calls through It.

B. Deploy a NAT gateway into a public subnet and attach an end point policy that allows access to the S3 buckets.

C. Deploy the application Into a public subnet and allow it to route through an internet gateway to access the S3 Buckets

D. Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets.

Answer: D

Explanation:

The correct answer is Option D. Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets. By deploying an S3 VPC gateway endpoint, the application can access the S3 buckets over a private network connection within the VPC, eliminating the need for data transfer over the internet. This can help reduce data transfer fees as well as improve the performance of the application. The endpoint policy can be used to specify which S3 buckets the application has access to.

87. - (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

88. - (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 now route table that excludes the route to the public subnets' CIDR blocks. Associate the route table to the database subnets.

B. Create a security group that denies ingress from the security group used by instances in the public subnets. Attach the security group to an Amazon RDS DB instance.

C. Create a security group that allows ingress from the security group used by instances in the private subnets. Attach the security group to an Amazon RDS DB instance.

D. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database

subnets.

Answer: C

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#VPCSecurit yGroups

89. - (Topic 1)

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

A. Modify the DB instance to be a Multi-AZ deployment

B. Create a read replica of the database Configure the script to query only the read replica

C. Instruct the development team to manually export the entries in the database at the end of each day

D. Use Amazon ElastiCache to cache the common queries that the script runs against the database

Answer: B

90. - (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.

91. - (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 tables. For RPO recovery, point the application to a different AWS Region.

B. Configure DynamoDB point-in-time recovery. For RPO recovery, restore to the desired point in time.

C. Export the DynamoDB data to Amazon S3 Glacier on a daily basis. For RPO recovery, import the data from S3 Glacier to DynamoDB.

D. Schedule Amazon Elastic Block Store (Amazon EBS) snapshots for the DynamoDB table every 15 minutes. For RPO recovery, restore the DynamoDB table by using the EBS snapshot.

Answer: B

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

92. - (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. send an alert to an Amazon Simple Notification Service (Amazon SNS) topic with the application owner's email address for further processing

Answer: A,B

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.

93. - (Topic 1)

A survey company has gathered data for several years from areas m\ the United States. The company hosts the data in an Amazon S3 bucket that is 3 TB m size and growing. The company has started to share the data with a European marketing firm that has S3 buckets The company wants to ensure that its data transfer costs remain as low as possible

Which solution will meet these requirements?

A. Configure the Requester Pays feature on the company's S3 bucket

B. Configure S3 Cross-Region Replication from the company's S3 bucket to one of the marketing firm's S3 buckets.

C. Configure cross-account access for the marketing firm so that the marketing firm has access to the company's S3 bucket.

D. Configure the company's S3 bucket to use S3 Intelligent-Tiering Sync the S3 bucket to one of the marketing firm's S3 buckets

Answer: A

Explanation:

"Typically, you configure buckets to be Requester Pays buckets when you want to share data but not incur charges associated with others accessing the data. For example, you might use Requester Pays buckets when making available large datasets, such as zip code directories, reference data, geospatial information, or web crawling data."

https://docs.aws.amazon.com/AmazonS3/latest/userguide/RequesterPaysBuckets.html

94. - (Topic 1)

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

Which solution will meet these requirements?

A. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a one- way forest trust or a one-way domain trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.

B. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a two- way forest trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.

C. Use AWS Directory Service. Create a two-way trust relationship with the company's self- managed Microsoft Active Directory.

D. Deploy an identity provider (IdP) on premises. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.

Answer: A

Explanation: To provide single sign-on (SSO) across all the company's accounts while continuing to manage users and groups in its on-premises self-managed Microsoft Active Directory, the solution is to enable AWS Single Sign-On (SSO) from the AWS SSO console and create a one-way forest trust or a one-way domain trust to connect the company's self- managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory. This solution is described in the AWS documentation

95. - (Topic 1)

A company has an AWS Glue extract. transform, and load (ETL) job that runs every day at the same time. The job processes XML data that is in an Amazon S3 bucket.

New data is added to the S3 bucket every day. A solutions architect notices that AWS Glue is processing all the data during each run.

What should the solutions architect do to prevent AWS Glue from reprocessing old data?

A. Edit the job to use job bookmarks.

B. Edit the job to delete data after the data is processed

C. Edit the job by setting the NumberOfWorkers field to 1.

D. Use a FindMatches machine learning (ML) transform.

Answer: C

Explanation: This is the purpose of bookmarks: "AWS Glue tracks data that has already been processed during a previous run of an ETL job by persisting state information from the job run. This persisted state information is called a job bookmark. Job bookmarks help AWS Glue maintain state information and prevent the reprocessing of old data."

https://docs.aws.amazon.com/glue/latest/dg/monitor-continuations.html

96. - (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. Store the resulting JSON file in an Amazon Aurora DB cluster.

B. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue. Use Amazon EC2 instances to read from the queue and process the data. Store the resulting JSON file in Amazon DynamoDB.

C. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function to read from the queue and process the data. Store the resulting JSON file in Amazon DynamoDB. Most Voted

D. Configure Amazon EventBridge (Amazon CloudWatch Events) to send an event to Amazon Kinesis Data Streams when a new file is uploaded. Use an AWS Lambda function to consume the event from the stream and process the data. Store the resulting JSON file in Amazon Aurora DB cluster.

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

97. - (Topic 1)

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

What should a solutions architect do to secure the audit documents?

A. Enable the versioning and MFA Delete features on the S3 bucket.

B. Enable multi-factor authentication (MFA) on the IAM user credentials for each audit team IAM user account.

C. Add an S3 Lifecycle policy to the audit team's IAM user accounts to deny the s3:DeleteObject action during audit dates.

D. Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key.

Answer: A

98. - (Topic 1)

A company is preparing to store confidential data in Amazon S3 For compliance reasons the data must be encrypted at rest Encryption key usage must be logged tor auditing purposes. Keys must be rotated every year.

Which solution meets these requirements and «the MOST operationally efferent?

A. Server-side encryption with customer-provided keys (SSE-C)

B. Server-side encryption with Amazon S3 managed keys (SSE-S3)

C. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with manual rotation

D. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with automate rotation

Answer: D

Explanation: https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html When you enable automatic key rotation for a customer managed key, AWS KMS generates new cryptographic material for the KMS key every year. AWS KMS also saves the KMS key's older cryptographic material in perpetuity so it can be used to decrypt data that the KMS key encrypted.

Key rotation in AWS KMS is a cryptographic best practice that is designed to be transparent and easy to use. AWS KMS supports optional automatic key rotation only for customer managed CMKs. Enable and disable key rotation. Automatic key rotation is disabled by default on customer managed CMKs. When you enable (or re-enable) key rotation, AWS KMS automatically rotates the CMK 365 days after the enable date and every 365 days thereafter.

99. - (Topic 1)

An application allows users at a company's headquarters to access product data. The product data is stored in an Amazon RDS MySQL DB instance. The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic. A solutions architect needs to optimize the application's performance quickly.

What should the solutions architect recommend?

A. Change the existing database to a Multi-AZ deployment. Serve the read requests from the primary Availability Zone.

B. Change the existing database to a Multi-AZ deployment. Serve the read requests from the secondary Availability Zone.

C. Create read replicas for the database. Configure the read replicas with half of the compute and storage resources as the source database.

D. Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.

Answer: D

Explanation: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_MySQL.Replication.ReadReplicas.html

100. - (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 AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.

B. Create three NAT instances, one for each private subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.

C. Create a second internet gateway on one of the private subnets. Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.

D. Create an egress-only internet gateway on one of the public subnets. Update the route table for the private subnets that forward non-VPC traffic to the egress- only internet gateway.

Answer: A

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

101. - (Topic 1)

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

How should security groups be configured in this situation? (Select TWO)

A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.

B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.

C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.

D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.

E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

Answer: A,C

Explanation: "Security groups create an outbound rule for every inbound rule." Not completely right. Statefull does NOT mean that if you create an inbound (or outbound) rule, it will create an outbound (or inbound) rule. What it does mean is: suppose you create an inbound rule on port 443 for the X ip. When a request enters on port 443 from X ip, it will allow traffic out for that request in the port 443. However, if you look at the outbound rules, there will not be any outbound rule on port 443 unless explicitly create it. In ACLs, which are stateless, you would have to create an inbound rule to allow incoming requests and an outbound rule to allow your application responds to those incoming requests.

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#SecurityGro upRules

102. - (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

103. - (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 Logs. Export the logs to the S3 bucket.

C. Create an instance profile on Amazon EC2 to allow S3 access.

D. Create an Amazon API Gateway API with a private link to access the S3 endpoint.

Answer: A

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

104. - (Topic 1)

A company has thousands of edge devices that collectively generate 1 TB of status alerts each day. Each alert is approximately 2 KB in size. A solutions architect needs to implement a solution to ingest and store the alerts for future analysis.

The company wants a highly available solution. However, the company needs to minimize costs and does not want to manage additional infrastructure. Ad ditionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days.

What is the MOST operationally efficient solution that meets these requirements?

A. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days

B. Launch Amazon EC2 instances across two Availability Zones and place them behind an Elastic Load Balancer to ingest the alerts Create a script on the EC2 instances that will store tne alerts m an Amazon S3 bucket Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days

C. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon Elasticsearch Service (Amazon ES) duster Set up the Amazon ES cluster to take manual snapshots every day and delete data from the duster that is older than 14 days

D. Create an Amazon Simple Queue Service (Amazon SQS i standard queue to ingest the alerts and set the message retention period to 14 days Configure consumers to poll the SQS queue check the age of the message and analyze the message data as needed If the message is 14 days old the consumer should copy the message to an Amazon S3 bucket

and delete the message from the SQS queue

Answer: A

Explanation:

https://aws.amazon.com/kinesis/data-firehose/features/?nc=sn&loc=2#:~:text=into%20Amazon%20S3%2C%20Amazon%20Redshift%2C%20Amazon%20OpenSearch%20Service%2C%20Kinesis,Delivery%20streams

105. - (Topic 1)

A company has a production web application in which users upload documents through a web interlace or a mobile app. According to a new regulatory requirement, new documents cannot be modified or deleted after they are stored.

What should a solutions architect do to meet this requirement?

A. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled

B. Store the uploaded documents in an Amazon S3 bucket. Configure an S3 Lifecycle policy to archive the documents periodically.

C. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning enabled Configure an ACL to restrict all access to read-only.

D. Store the uploaded documents on an Amazon Elastic File System (Amazon EFS) volume. Access the data by mounting the volume in read-only mode.

Answer: A

Explanation:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html

106. - (Topic 1)

A company has an application that runs on Amazon EC2 instances and uses an Amazon Aurora database. The EC2 instances connect to the database by using user names and passwords that are stored locally in a file. The company wants to minimize the operational overhead of credential management.

What should a solutions architect do to accomplish this goal?

A. Use AWS Secrets Manager. Turn on automatic rotation.

B. Use AWS Systems Manager Parameter Store. Turn on automatic rotation.

C. Create an Amazon S3 bucket lo store objects that are encrypted with an AWS Key C. Management Service (AWS KMS) encryption key. Migrate the credential file to the S3 bucket. Point the application to the S3 bucket.

D. Create an encrypted Amazon Elastic Block Store (Amazon EBS) volume (or each EC2 instance. Attach the new EBS volume to each EC2 instance. Migrate the credential file to the new EBS volume. Point the application to the new EBS volume.

Answer: A

Explanation:

https://aws.amazon.com/cn/blogs/security/how-to-connect-to-aws-secrets-manager-service-within-a-virtual-private-cloud/

https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/

107. - (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 instances.

Connect the database by using native Java Database Connectivity (JDBC) drivers.

B. Change the platform from Aurora to Amazon DynamoDB. Provision a DynamoDB Accelerator (DAX) cluster. Use the DAX client SDK to point the existing DynamoDB API calls at the DAX cluster.

C. Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using Amazon Simple Notification Service (Amazon SNS).

D. Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using an Amazon Simple Queue Service (Amazon SQS) queue.

Answer: B

Explanation: bottlenecks can be avoided with queues (SQS).

108. - (Topic 1)

A company uses AWS Organizations to manage multiple AWS accounts for different departments. The management account has an Amazon S3 bucket that contains project reports. The company wants to limit access to this S3 bucket to only users of accounts within the organization in AWS Organizations.

Which solution meets these requirements with the LEAST amount of operational overhead?

A. Add the aws:PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy.

B. Create an organizational unit (OU) for each department. Add the aws:PrincipalOrgPaths global condition key to the S3 bucket policy.

C. Use AWS CloudTrail to monitor the CreateAccount, InviteAccountToOrganization, LeaveOrganization, and RemoveAccountFromOrganization events. Update the S3 bucket policy accordingly.

D. Tag each user that needs access to the S3 bucket. Add the aws:PrincipalTag global condition key to the S3 bucket policy.

Answer: A

Explanation:

https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-aws-organization-of-iam-principals/

The aws:PrincipalOrgID global key provides an alternative to listing all the account IDs for all AWS

accounts in an organization. For example, the following Amazon S3 bucket policy allows members of any account in the XXX organization to add an object into the

examtopics bucket.

{"Version": "2020-09-10",

"Statement": {

"Sid": "AllowPutObject", "Effect": "Allow",

"Principal": "*",

"Action": "s3:PutObject",

"Resource": "arn:aws:s3:::examtopics/*", "Condition": {"StringEquals":

{"aws:PrincipalOrgID":["XXX"]}}}}

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition- keys.html

109. - (Topic 1)

A company runs its Infrastructure on AWS and has a registered base of 700.000 users for res document management application The company intends to create a product that converts large pdf files to jpg Imago files. The .pdf files average 5 MB in size. The company needs to store the original files and the converted files. A solutions architect must design a scalable solution to accommodate demand that will grow rapidly over lime.

Which solution meets these requirements MOST cost-effectively?

A. Save the pdf files to Amazon S3 Configure an S3 PUT event to invoke an AWS Lambda function to convert the files to jpg format and store them back in Amazon S3

B. Save the pdf files to Amazon DynamoDB. Use the DynamoDB Streams feature to invoke an AWS Lambda function to convert the files to jpg format and store them hack in DynamoDB

C. Upload the pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances. Amazon Elastic Block Store (Amazon EBS) storage and an Auto Scaling group. Use a program In the EC2 instances to convert the files to jpg format Save the .pdf files and the .jpg files In the EBS store.

D. Upload the .pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic File System (Amazon EPS) storage, and an Auto Scaling group. Use a program in the EC2 instances to convert the file to jpg format Save the pdf files and the jpg files in the EBS store.

Answer: A

Explanation: Elastic BeanStalk is expensive, and DocumentDB has a 400KB max to upload files. So Lambda and S3 should be the one.

110. - (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 Regions. Use Amazon Route 53 health checks to redirect traffic. Use Aurora PostgreSQL Cross-Region Replication.

B. Configure the Auto Scaling group to use multiple Availability Zones. Configure the database as Multi-AZ. Configure an Amazon RDS Proxy instance for the database.

C. Configure the Auto Scaling group to use one Availability Zone. Generate hourly snapshots of the database. Recover the database from the snapshots in the event of a failure.

D. Configure the Auto Scaling group to use multiple AWS Regions. Write the data from the application to Amazon S3. Use S3 Event Notifications to launch an AWS Lambda function to write the data to the database.

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.

111. - (Topic 1)

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

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

A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services.

B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the server's peak utilization during the performance failures. Increase the size of the application server's Amazon EC2 instances to meet the peak requirements.

C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.

D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

Answer: A

Explanation:

https://aws.amazon.com/getting-started/hands-on/build-serverless-web-app-lambda-apigateway-s3-dynamodb-cognito/module-4/

Build a Serverless Web Application with AWS Lambda, Amazon API Gateway, AWS Amplify, Amazon DynamoDB, and Amazon Cognito. This example showed similar setup as question: Build a Serverless Web Application with AWS Lambda, Amazon API Gateway, AWS Amplify, Amazon DynamoDB, and Amazon Cognito

112. - (Topic 1)

A company recently launched a variety of new workloads on Amazon EC2 instances in its AWS account. The company needs to create a strategy to access and administer the instances remotely and securely. The company needs to implement a repeatable process that works with native AWS services and follows the AWS Well-Architected Framework.

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

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

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

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

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

Answer: B

Explanation:

https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-launch-managed-instance.html

113. - (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/

114. - (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 instances. Use Reserved Instances for the development and test EC2 instances.

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

C. Use Spot blocks for the production EC2 instances. Use Reserved Instances for the development and test EC2 instances.

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

Answer: B

Topic 2, Exam Pool B

115. - (Topic 2)

A company hosts a two-tier application on Amazon EC2 instances and Amazon RDS. The application's

demand varies based on the time of day. The load is minimal after work hours and on weekends. The EC2 instances run in an EC2 Auto Scaling group that is configured with a minimum of two instances and a maximum of five instances. The application must be available at all times, but the company is concerned about overall cost.

Which solution meets the availability requirement MOST cost-effectively?

A. Use all EC2 Spot Instances. Stop the RDS database when it is not in use.

B. Purchase EC2 Instance Savings Plans to cover five EC2 instances. Purchase an RDS Reserved DB Instance

C. Purchase two EC2 Reserved Instances Use up to three additional EC2 Spot Instances as needed. Stop the RDS database when it is not in use.

D. Purchase EC2 Instance Savings Plans to cover two EC2 instances. Use up to three additional EC2 On-Demand Instances as needed. Purchase an RDS Reserved DB Instance.

Answer: C

Explanation:

This solution meets the requirements of a two-tier application that has a variable demand based on the time of day and must be available at all times, while minimizing the overall cost. EC2 Reserved Instances can provide significant savings compared to On-Demand Instances for the baseline level of usage, and they can guarantee capacity reservation when needed. EC2 Spot Instances can provide up to 90% savings compared to On- Demand Instances for any additional capacity that the application needs during peak hours. Spot Instances are suitable for stateless applications that can tolerate interruptions and can be replaced by other instances. Stopping the RDS database when it is not in use can reduce the cost of running the database tier.

Option A is incorrect because using all EC2 Spot Instances can affect the availability of the application if there are not enough spare capacity or if the Spot price exceeds the maximum price. Stopping the RDS database when it is not in use can reduce the cost of running the database tier, but it can also affect the availability of the application. Option B is incorrect because purchasing EC2 Instance Savings Plans to cover five EC2 instances can lock in a fixed amount of compute usage per hour, which may not match the actual usage pattern of the application. Purchasing an RDS Reserved DB Instance can provide savings for the database tier, but it does not allow stopping the database when it is not in use. Option D is incorrect because purchasing EC2 Instance Savings Plans to cover two EC2 instances can lock in a fixed amount of

compute usage per hour, which may not match the

actual usage pattern of the application. Using up to three additional EC2 On-Demand Instances as needed can incur higher costs than using Spot Instances.

References:

- https://aws.amazon.com/ec2/pricing/reserved-instances/
- https://aws.amazon.com/ec2/spot/
- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_StopInstance.html

116. - (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/

117. - (Topic 2)

A medical records company is hosting an application on Amazon EC2 instances. The application processes customer data files that are stored on Amazon S3. The EC2 instances are hosted in public subnets. The EC2 instances access Amazon S3 over the internet, but they do not require any other network access.

A new requirement mandates that the network traffic for file transfers take a private route and not be sent over the internet.

Which change to the network architecture should a solutions architect recommend to meet this requirement?

A. Create a NAT gateway. Configure the route table for the public subnets to send traffic to Amazon S3 through the NAT gateway.

B. Configure the security group for the EC2 instances to restrict outbound traffic so that only traffic to the S3 prefix list is permitted.

C. Move the EC2 instances to private subnets. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets

D. Remove the internet gateway from the VPC. Set up an AWS Direct Connect connection, and route traffic to Amazon S3 over the Direct Connect connection.

Answer: C

Explanation: To meet the new requirement of transferring files over a private route, the EC2 instances should be moved to private subnets, which do not have direct access to the internet. This ensures that the traffic for file transfers does not go over the internet. To enable the EC2 instances to access Amazon S3, a VPC endpoint for Amazon S3 can be created. VPC endpoints allow resources within a VPC to communicate with resources in other services without the traffic being sent over the internet. By linking the

VPC endpoint to the route table for the private subnets, the EC2 instances can access Amazon S3 over a private connection within the VPC.

118. - (Topic 2)

A company has a Windows-based application that must be migrated to AWS. The application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances that are deployed across multiple Availability Zones.

What should a solutions architect do to meet this requirement?

A. Configure AWS Storage Gateway in volume gateway mode. Mount the volume to each Windows instance.

B. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx file system to each Windows instance.

C. Configure a file system by using Amazon Elastic File System (Amazon EFS). Mount the EFS file system to each Windows instance.

D. Configure an Amazon Elastic Block Store (Amazon EBS) volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.

Answer: B

Explanation:

This solution meets the requirement of migrating a Windows-based application that requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances that are deployed across multiple Availability Zones. Amazon FSx for Windows File Server provides fully managed shared storage built on Windows Server, and delivers a wide range of data access, data management, and administrative capabilities. It supports the Server Message Block (SMB) protocol and can be mounted to EC2 Windows instances across multiple Availability Zones.

Option A is incorrect because AWS Storage Gateway in volume gateway mode provides cloud-backed storage volumes that can be mounted as iSCSI devices from on-premises application servers, but it does not support SMB protocol or EC2 Windows instances. Option C is incorrect because Amazon Elastic File System (Amazon EFS) provides a scalable and elastic NFS file system for Linux-based workloads, but it does not support SMB protocol or EC2 Windows instances. Option D is incorrect because Amazon Elastic Block Store (Amazon EBS) provides persistent block storage volumes for use with EC2 instances, but it

does not support SMB protocol or attaching multiple instances to the same volume.

References:

- https://aws.amazon.com/fsx/windows/
- https://docs.aws.amazon.com/fsx/latest/WindowsGuide/using-file-shares.html

119. - (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. Add a static error page that is hosted in an Amazon S3 bucket to the records so that the traffic is sent to the most responsive endpoints.

B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page that is hosted in an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.

C. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance that hosts a static error page as endpoints. Configure Route 53 to send requests to the instance only if the health checks fail for the ALB.

D. Update the Route 53 records to use a multivalue answer routing policy. Create a health check. Direct traffic to the website if the health check passes. Direct traffic to a static error page that is hosted in Amazon S3 if the health check does not pass.

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

120. - (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 tune 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

121. - (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. Deny access to all AWS Regions except ap-northeast-3 in the AWS account settings.

C. Use AWS Organizations to configure service control policies (SCPS) that prevent VPCs from gaining internet access. Deny access to all AWS Regions except ap-northeast-3.

D. Create an outbound rule for the network ACL in each VPC to deny all traffic from 0.0.0.0/0. Create an IAM policy for each user to prevent the use of any AWS Region other than ap-northeast-3.

E. Use AWS Config to activate managed rules to detect and alert for internet gateways and to detect and alert for new resources deployed outside of ap-northeast-3.

Answer: A,C

Explanation:

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

122. - (Topic 2)

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

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

A. Create an Auto Scaling group that uses three Instances across each of tv/o Regions.

B. Modify the Auto Scaling group to use three instances across each of two Availability Zones.

C. Create an Auto Scaling template that can be used to quickly create more instances in another Region.

D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier.

Answer: B

Explanation:

High availability can be enabled for this architecture quite simply by modifying the existing Auto Scaling group to use multiple availability zones. The ASG will automatically balance the load so you don't actually need to specify the instances per AZ.

123. - (Topic 2)

A company produces batch data that comes from different databases. The company also produces live stream data from network sensors and application APIs. The company needs to consolidate all the data into one place for business analytics. The company needs to process the incoming data and then stage the data in different Amazon S3 buckets. Teams will later run one-time queries and import the data into a business intelligence tool to show key performance indicators (KPIs).

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

A. Use Amazon Athena foe one-time queries Use Amazon QuickSight to create dashboards for KPIs

B. Use Amazon Kinesis Data Analytics for one-time queries Use Amazon QuickSight to create dashboards for KPIs

C. Create custom AWS Lambda functions to move the individual records from me databases to an Amazon Redshift duster

D. Use an AWS Glue extract transform, and toad (ETL) job to convert the data into JSON format Load the data into multiple Amazon OpenSearch Service (Amazon Elasticsearch Service) dusters

E. Use blueprints in AWS Lake Formation to identify the data that can be ingested into a data lake Use AWS Glue to crawl the source extract the data and load the data into Amazon S3 in Apache Parquet format

Answer: A,E

Explanation:

Amazon Athena is the best choice for running one-time queries on streaming data. Although Amazon Kinesis Data Analytics provides an easy and familiar standard SQL language to analyze streaming data in real-time, it is designed for continuous queries rather than one-time queries[1]. On the other hand, Amazon Athena is a serverless interactive query service that allows querying data in Amazon S3 using SQL. It is optimized for ad-hoc querying and is ideal for running one-time queries on streaming data[2].AWS Lake Formation uses as a central place to have all your data for analytics purposes (E). Athena integrate perfect with S3 and can makes queries (A).

124. - (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: A,C

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

125. - (Topic 2)

A company wants to use the AWS Cloud to make an existing application highly available and resilient. The current version of the application resides in the company's data center. The application recently experienced data loss after a database server crashed because of an unexpected power outage.

The company needs a solution that avoids any single points of failure. The solution must give the application the ability to scale to meet user demand.

Which solution will meet these requirements?

A. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon RDS DB instance in a Multi-AZ configuration.

B. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group in a single Availability Zone. Deploy the database

on an EC2 instance. Enable EC2 Auto Recovery.

C. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling

group across multiple Availability Zones. Use an Amazon RDS DB instance with a read replica in a single Availability Zone. Promote the read replica to replace the primary DB instance if the primary DB instance fails.

D. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones Deploy the primary and secondary database servers on EC2 instances across multiple Availability Zones Use Amazon Elastic Block Store (Amazon EBS) Multi-Attach to create shared storage between the instances.

Answer: A

Explanation:

Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon RDS DB instance in a Multi-AZ configuration. To make an existing application highly available and resilient while avoiding any single points of failure and giving the application the ability to scale to meet user demand, the best solution would be to deploy the application servers using

Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones and use an Amazon RDS DB instance in a Multi-AZ configuration. By using an Amazon RDS DB instance in a Multi-AZ configuration, the database is automatically replicated across multiple Availability Zones, ensuring that the database is highly available and can withstand the failure of a single Availability Zone. This provides fault tolerance and avoids any single points of failure.

126. - (Topic 2)

An application runs on Amazon EC2 instances across multiple Availability Zones The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer The application performs best when the CPU utilization of the EC2 instances is at or near 40%.

What should a solutions architect do to maintain the desired performance across all instances in the group?

A. Use a simple scaling policy to dynamically scale the Auto Scaling group

B. Use a target tracking policy to dynamically scale the Auto Scaling group

C. Use an AWS Lambda function to update the desired Auto Scaling group capacity.

D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group

Answer: B

Explanation:

https://docs.aws.amazon.com/autoscaling/application/userguide/application-auto-scaling-target-tracking.html

127. - (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

128. - (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 anew solution. The website will be updated four times a year and does not need to have any dynamic content available. The solution must provide high scalability and enhanced security.

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

A. 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. Deploy the website by using an Auto Scaling group of Amazon EC2 instances behind an Application Load Balancer.

Answer: A,D

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)

129. - (Topic 2)

A company is migrating its on-premises PostgreSQL database to Amazon Aurora PostgreSQL. The on-premises database must remain online and accessible during the migration. The Aurora database must remain synchronized with the on-premises database.

Which combination of actions must a solutions architect take to meet these requirements? (Choose two.)

A. Create an ongoing replication task.

B. Create a database backup of the on-premises database

C. Create an AWS Database Migration Service (AWS DMS) replication server

D. Convert the database schema by using the AWS Schema Conversion Tool (AWS SCT).

E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to monitor the database synchronization

Answer: A,C

Explanation:

AWS Database Migration Service supports homogeneous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different database platforms, such as Oracle or Microsoft SQL Server to Amazon Aurora. With AWS Database Migration Service, you can also continuously replicate data with low latency from any supported source to any supported target. For example, you can replicate from multiple sources to Amazon Simple Storage Service (Amazon S3) to build a highly available and scalable data lake solution. You can also consolidate databases into a petabyte-scale data warehouse by streaming data to Amazon Redshift. Learn more about the supported source and target databases.

https://aws.amazon.com/dms/

130. - (Topic 2)

A security team wants to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there

must be a single point where permissions can be maintained.

What should a solutions architect do to accomplish this?

A. Create an ACL to provide access to the services or actions.

B. Create a security group to allow accounts and attach it to user groups.

C. Create cross-account roles in each account to deny access to the services or actions.

D. Create a service control policy in the root organizational unit to deny access to the services or actions.

Answer: D

Explanation: Service control policies (SCPs) are one type of policy that you can use to manage your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines.

See https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.ht

ml.

131. - (Topic 2)

A company is building a web-based application running on Amazon EC2 instances in multiple Availability Zones. The web application will provide access to a repository of text documents totaling about 900 TB in size. The company anticipates that the web application will experience periods of high demand. A solutions architect must ensure that the storage component for the text documents can scale to meet the demand of the application at all times. The company is concerned about the overall cost of the solution.

Which storage solution meets these requirements MOST cost-effectively?

A. Amazon Elastic Block Store (Amazon EBS)

B. Amazon Elastic File System (Amazon EFS)

C. Amazon Elasticsearch Service (Amazon ES)

D. Amazon S3

Answer: D

Explanation: Amazon S3 is cheapest and can be accessed from anywhere.

132. - (Topic 2)

A company runs an application using Amazon ECS. The application creates esi/ed versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3.

How can a solutions architect ensure that the application has permission to access Amazon S3?

A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.

B. Create an IAM role with S3 permissions, and then specify that role as the taskRoleAm in the task definition.

C. Create a security group that allows access from Amazon ECS to Amazon S3, and update the launch configuration used by the ECS cluster.

D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

Answer: B

Explanation:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ecs-taskdefinition.html

133. - (Topic 2)

An online retail company has more than 50 million active customers and receives more than 25,000 orders each day. The company collects purchase data for customers and stores this data in Amazon S3. Additional customer data is stored in Amazon RDS.

The company wants to make all the data available to various teams so that the teams can perform analytics. The solution must provide the ability to manage fine-grained permissions for the data and must minimize operational overhead.

Which solution will meet these requirements?

A. Migrate the purchase data to write directly to Amazon RDS. Use RDS access controls to limit access.

B. Schedule an AWS Lambda function to periodically copy data from Amazon RDS to Amazon S3. Create an AWS Glue crawler. Use Amazon Athena to query the data. Use S3 policies to limit access.

C. Create a data lake by using AWS Lake Formation. Create an AWS Glue JDBC connection to Amazon RDS. Register (he S3 bucket in Lake Formation. Use Lake Formation access controls to limit access.

D. Create an Amazon Redshift cluster. Schedule an AWS Lambda function to periodically copy data from Amazon S3 and Amazon RDS to Amazon Redshift. Use Amazon Redshift access controls to limit access.

Answer: C

Explanation:

To make all the data available to various teams and minimize operational overhead, the company can create a data lake by using AWS Lake Formation. This will allow the company to centralize all the data in one place and use fine-grained access controls to manage access to the data. To meet the requirements of the company, the solutions architect can create a data lake by using AWS Lake Formation, create an AWS Glue JDBC connection to Amazon RDS, and register the S3 bucket in Lake Formation. The solutions architect can then use Lake Formation access controls to limit access to the data. This solution will provide the ability to manage fine-grained permissions for the data and minimize operational overhead.

134. - (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.

135. - (Topic 2)

A company is concerned about the security of its public web application due to recent web attacks. The application uses an Application Load Balancer (ALB). A solutions architect must reduce the risk of DDoS attacks against the application.

What should the solutions architect do to meet this requirement?

A. Add an Amazon Inspector agent to the ALB.

B. Configure Amazon Macie to prevent attacks.

C. Enable AWS Shield Advanced to prevent attacks.

D. Configure Amazon GuardDuty to monitor the ALB.

Answer: C

Explanation:

AWS Shield Advanced provides expanded DDoS attack protection for your Amazon EC2 instances, Elastic Load Balancing load balancers, CloudFront distributions, Route 53 hosted zones, and AWS Global Accelerator standard accelerators.

https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html

136. - (Topic 2)

A reporting team receives files each day in an Amazon S3 bucket. The reporting team manually reviews and copies the files from this initial S3 bucket to an analysis S3 bucket each day at the same time to use with Amazon QuickSight. Additional teams are starting to send more files in larger sizes to the initial S3 bucket.

The reporting team wants to move the files automatically analysis S3 bucket as the files enter the initial S3 bucket. The reporting team also wants to use AWS Lambda functions to run pattern-matching code on the copied data. In addition, the reporting team wants to send the data files to a pipeline in Amazon SageMaker Pipelines.

What should a solutions architect do to meet these requirements with the LEAST operational overhead?

A. Create a Lambda function to copy the files to the analysis S3 bucket. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s30bjectCreated:Put as the event type.

B. Create a Lambda function to copy the files to the analysis S3 bucket. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge (Amazon CloudWatch Events). Configure an ObjectCreated rule in EventBridge (CloudWatch Events). Configure Lambda and SageMaker Pipelines as targets for the rule.

C. Configure S3 replication between the S3 buckets. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s30bjectCreated:Put as the event type.

D. Configure S3 replication between the S3 buckets. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge (Amazon CloudWatch Events). Configure an ObjectCreated rule in

EventBridge (CloudWatch Events). Configure Lambda and SageMaker Pipelines as targets for the rule.

Answer: D

Explanation:

This solution meets the requirements of moving the files automatically, running Lambda functions on the copied data, and sending the data files to SageMaker Pipelines with the least operational overhead. S3 replication can copy the files from the initial S3 bucket to the analysis S3 bucket as they arrive. The analysis S3 bucket can send event notifications to Amazon EventBridge (Amazon CloudWatch Events) when an object is created. EventBridge can trigger Lambda and SageMaker Pipelines as targets for the ObjectCreated rule. Lambda can run pattern-matching code on the copied data, and SageMaker Pipelines can execute a pipeline with the data files.

Option A is incorrect because creating a Lambda function to copy the files to the analysis S3 bucket is not necessary when S3 replication can do that automatically. It also adds operational overhead to manage the Lambda function. Option B is incorrect because creating a Lambda function to copy the files to the analysis S3 bucket is not necessary when S3 replication can do that automatically. It also adds operational overhead to manage the Lambda function. Option C is incorrect because using S3 event notification with multiple destinations can result in throttling or delivery failures if there are too many events. References:

➪ https://aws.amazon.com/blogs/machine-learning/automate-feature-engineering-pipelines-with-amazon-sagemaker/

➪ https://docs.aws.amazon.com/sagemaker/latest/dg/automating-sagemaker-with- eventbridge.html

➪ https://aws.amazon.com/about-aws/whats-new/2021/04/new-options-trigger-amazon-sagemaker-pipeline-executions/

137. - (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 bi 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 n Amazon S3

C. Store the files as large, single objects in Amazon S3.

D. Use Amazon Kinosis Data Analytics to run the Queries as pan of the batch processing operation

E. Use an AWS duo extract, transform, and load (ETL) process to convert the csv files into Apache Parquet format.

Answer: B,E

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 duo 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.

138. - (Topic 2)

A company has an ecommerce checkout workflow that writes an order to a database and calls a service to process the payment. Users are experiencing timeouts during the checkout process. When users resubmit the checkout form, multiple unique orders are created for the same desired transaction.

How should a solutions architect refactor this workflow to prevent the creation of multiple orders?

A. Configure the web application to send an order message to Amazon Kinesis Data Firehose. Set the payment service to retrieve the message from Kinesis Data Firehose and process the order.

B. Create a rule in AWS CloudTrail to invoke an AWS Lambda function based on the logged application path request Use Lambda to query the database, call the payment service, and pass in the order information.

C. Store the order in the database. Send a message that includes the order number to Amazon Simple Notification Service (Amazon SNS). Set the payment service to poll

Amazon SNS. retrieve the message, and process the order.

D. Store the order in the database. Send a message that includes the order number to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the payment service to retrieve the message and process the order. Delete the message from the queue.

Answer: D

Explanation: This approach ensures that the order creation and payment processing steps are separate and atomic. By sending the order information to an SQS FIFO queue, the payment service can process the order one at a time and in the order they were received. If the payment service is unable to process an order, it can be retried later, preventing the creation of multiple orders. The deletion of the message from the queue after it is processed will prevent the same message from being processed multiple times.

139. - (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 roof user credentials for performing AWS CloudFormation stack operations.

B. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached.

C. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the Administrate/Access IAM policy attached.

D. Create a new IAM User for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.

E. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using Dial IAM role.

Answer: D,E

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

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

140. - (Topic 2)

A company is building a containerized application on premises and decides to move the application to AWS. The application will have thousands of users soon after li is deployed. The company Is unsure how to manage the deployment of containers at scale. The company needs to deploy the containerized application in a highly available architecture that minimizes operational overhead.

Which solution will meet these requirements?

A. Store container images In an Amazon Elastic Container Registry (Amazon ECR) repository. Use an Amazon Elastic Container Service (Amazon ECS) cluster with the AWS Fargate launch type to run the containers. Use target tracking to scale automatically based on demand.

B. Store container images in an Amazon Elastic Container Registry (Amazon ECR) repository. Use an Amazon Elastic Container Service (Amazon ECS) cluster with the Amazon EC2 launch type to run the containers. Use target tracking to scale automatically based on demand.

C. Store container images in a repository that runs on an Amazon EC2 instance. Run the containers on EC2 instances that are spread across multiple Availability Zones. Monitor the average CPU utilization in Amazon CloudWatch. Launch new EC2 instances as needed

D. Create an Amazon EC2 Amazon Machine Image (AMI) that contains the container image Launch EC2 Instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon CloudWatch alarm to scale out EC2 instances when the average CPU utilization threshold is breached.

Answer: A

Explanation:

AWS Fargate is a serverless experience for user applications, allowing the user to concentrate on building applications instead of configuring and managing servers. Fargate also automates resource management, allowing users to easily scale their applications in response to demand.

141. - (Topic 2)

A company is running an online transaction processing (OLTP) workload on AWS. This workload uses an unencrypted Amazon RDS DB instance in a Multi-AZ deployment. Daily database snapshots are taken from this instance.

What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?

A. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted

snapshot

B. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it Enable encryption on the DB instance

C. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS) Restore encrypted snapshot to an existing DB instance

D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS)

Answer: A

Explanation: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_RestoreFromSnapshot.html#USER_RestoreFromSnapshot.CON

Under "Encrypt unencrypted resources" - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

142. - (Topic 2)

A company is planning to move its data to an Amazon S3 bucket. The data must be encrypted when it is stored in the S3 bucket. Additionally, the encryption key must be automatically rotated every year.

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

A. Move the data to the S3 bucket. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use the built-in key rotation behavior of SSE-S3 encryption keys.

B. Create an AWS Key Management Service {AWS KMS) customer managed key. Enable automatic key rotation. Set the S3 bucket's default encryption behavior to use the customer managed KMS key. Move the data to the S3 bucket.

C. Create an AWS Key Management Service (AWS KMS) customer managed key. Set the S3 bucket's default encryption behavior to use the customer managed KMS key. Move the data to the S3 bucket. Manually rotate the KMS key every year.

D. Encrypt the data with customer key material before moving the data to the S3 bucket. Create an AWS Key Management Service (AWS KMS) key without key material. Import the customer key material into the KMS key. Enable automatic key rotation.

Answer: B

Explanation:

SSE-S3 - is free and uses AWS owned CMKs (CMK = Customer Master Key). The encryption key is owned and managed by AWS, and is shared among many accounts. Its rotation is automatic with time that varies as shown in the table here. The time is not explicitly defined.

SSE-KMS - has two flavors:

AWS managed CMK. This is free CMK generated only for your account. You can only view it policies and audit usage, but not manage it. Rotation is automatic - once per 1095 days (3 years),

Customer managed CMK. This uses your own key that you create and can manage. Rotation is not enabled by default. But if you enable it, it will be automatically rotated every 1 year. This variant can also use an imported key material by you. If you create such key with an imported material, there is no automated rotation. Only manual rotation.

SSE-C - customer provided key. The encryption key is fully managed by you outside of AWS. AWS will not rotate it.

This solution meets the requirements of moving data to an Amazon S3 bucket, encrypting the data when it is stored in the S3 bucket, and automatically rotating the encryption key every year with the least operational overhead. AWS Key Management Service (AWS KMS) is a service that enables you to create and manage encryption keys for your data. A customer managed key is a symmetric encryption key that you create and manage in AWS KMS. You can enable automatic key rotation for a customer managed key, which means that AWS KMS generates new cryptographic material for the key every year. You can set the S3 bucket's default encryption behavior to use the customer managed KMS key, which means that any object that is uploaded to the bucket without specifying an encryption method will be encrypted with that key.

Option A is incorrect because using server-side encryption with Amazon S3 managed encryption keys (SSE-S3) does not allow you to control or manage the encryption keys. SSE-S3 uses a unique key for each object, and encrypts that key with a master key that is regularly rotated by S3. However, you cannot enable or disable key rotation for SSE-S3 keys, or specify the rotation interval. Option C is incorrect because manually rotating the KMS key every year can increase the operational overhead and complexity, and it may not meet the requirement of rotating the key every year if you forget or delay the rotation process. Option D is incorrect because encrypting the data with customer key material before moving the data to the S3 bucket can increase the operational overhead and complexity, and it may not provide consistent encryption for all objects in the bucket. Creating a KMS key without key material and importing

the customer key material into the KMS key can enable you to use your own source of random bits to generate your KMS keys, but it does not support automatic key rotation.

References:

- https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html
- https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html
- https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-encryption.html

143. - (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 AmazonEC2Ltnux 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 duster placement group. Attach a single Provisioned IOPS SSD Amazon Elastic Block Store (Amazon E BS) volume to all the instances by using Amazon EBS Multi-Attach

B. Use a cluster placement group. Create shared 'lie systems across the instances by using Amazon Elastic File System (Amazon EFS)

C. Use a partition placement group. Create shared tile systems across the instances by using Amazon Elastic File System (Amazon EFS).

D. Use a spread placement group. 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

144. - (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. Load the data into the new S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with AWS KMS multi-Region kays (SSE-KMS). Use Amazon Athena to query the data.

B. Create a new S3 bucket. Load the data into the new S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with AWS KMS multi-Region keys (SSE-KMS). Use Amazon RDS to query the data.

C. Load the data into the existing S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon Athena to query the data.

D. Load the data into the existing S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon RDS to query the data.

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/

145. - (Topic 2)

A media company is evaluating the possibility ot moving rts systems to the AWS Cloud The company needs at least 10 TB of storage with the maximum possible I/O performance for video processing. 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore

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

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

B. Amazon EBS for maximum performance, Amazon EFS for durable data storage and Amazon S3 Glacier for archival storage

C. Amazon EC2 instance store for maximum performance. Amazon EFS for durable data storage and Amazon S3 for archival storage

D. Amazon EC2 Instance store for maximum performance. Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

Answer: A

Explanation:

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

146. - (Topic 2)

A company runs its two-tier ecommerce website on AWS. The web tier consists of a load balancer that sends traffic to Amazon EC2 instances. The database tier uses an Amazon RDS DB instance. The EC2

instances and the RDS DB instance should not be exposed to the public internet. The EC2 instances require internet access to complete payment processing of orders through a third-party web service. The application must be highly available.

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

A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.

B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.

C. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones. Deploy an RDS Multi-AZ DB instance in private subnets.

D. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnet.

E. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnets.

Answer: A,E

Explanation:

Before you begin: Decide which two Availability Zones you will use for your EC2 instances. Configure your virtual private cloud (VPC) with at least one public subnet in each of these Availability Zones. These public subnets are used to configure the load balancer. You can launch your EC2 instances in other subnets of these Availability Zones instead.

147. - (Topic 2)

A solutions architect is creating a new Amazon CloudFront distribution for an application. Some of the information submitted by users is sensitive. The application uses HTTPS but needs another layer of security. The sensitive information should be protected throughout the entire application stack, and access to the information should be restricted to certain applications.

Which action should the solutions architect take?

A. Configure a CloudFront signed URL.

B. Configure a CloudFront signed cookie.

C. Configure a CloudFront field-level encryption profile.

D. Configure CloudFront and set the Origin Protocol Policy setting to HTTPS Only for the Viewer Protocol Policy.

Answer: C

Explanation: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html

"With Amazon CloudFront, you can enforce secure end-to-end connections to origin servers by using HTTPS. Field-level encryption adds an additional layer of security that lets you protect specific data throughout system processing so that only certain applications can see it."

148. - (Topic 2)

An entertainment company is using Amazon DynamoDB to store media metadata. The application is read intensive and experiencing delays. The company does not have staff to handle additional operational overhead and needs to improve the performance efficiency of DynamoDB without reconfiguring the application.

What should a solutions architect recommend to meet this requirement?

A. Use Amazon ElastiCache for Redis.

B. Use Amazon DynamoDB Accelerator (DAX).

C. Replicate data by using DynamoDB global tables.

D. Use Amazon ElastiCache for Memcached with Auto Discovery enabled.

Answer: B

Explanation:

https://aws.amazon.com/dynamodb/dax/

149. - (Topic 2)

A company runs workloads on AWS. The company needs to connect to a service from an external provider. The service is hosted in the provider's VPC. According to the company's security team, the connectivity must be private and must be restricted to the target service. The connection must be initiated only from the company's VPC.

Which solution will mast these requirements?

A. Create a VPC peering connection between the company's VPC and the provider's VPC. Update the

route table to connect to the target service.

B. Ask the provider to create a virtual private gateway in its VPC. Use AWS PrivateLink to connect to the target service.

C. Create a NAT gateway in a public subnet of the company's VPC. Update the route table to connect to the target service.

D. Ask the provider to create a VPC endpoint for the target service. Use AWS PrivateLink to connect to the target service.

Answer: D

Explanation:

AWS PrivateLink provides private connectivity between VPCs, AWS services, and your on-premises networks, without exposing your traffic to the public internet. AWS PrivateLink makes it easy to connect services across different accounts and VPCs to significantly simplify your network architecture. Interface **VPC endpoints**, powered by AWS PrivateLink, connect you to services hosted by AWS Partners and supported solutions available in AWS Marketplace. https://aws.amazon.com/privatelink/

150. - (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. Route the traffic from the Lambda function through the VPN.

C. Update the route tables in the VPC to allow the Lambda function to access the on- premises data center through Direct Connect.

D. Create an Elastic IP address. Configure the Lambda function to send traffic through the Elastic IP address without an elastic network interface.

Answer: A

Explanation:

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

151. - (Topic 2)

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

Which solution meets these requirements MOST cost-effectively?

A. Use Spot Instances exclusively to handle the maximum capacity required.

B. Use Reserved Instances exclusively to handle the maximum capacity required.

C. Use Reserved Instances for the baseline capacity and use Spot Instances to handle additional capacity.

D. Use Reserved Instances for the baseline capacity and use On-Demand Instances to handle additional capacity.

Answer: D

Explanation:

We recommend that you use On-Demand Instances for applications with short-term, irregular workloads that cannot be interrupted.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-on-demand-instances.html

152. - (Topic 2)

A company wants to manage Amazon Machine Images (AMIs). The company currently copies AMIs to the same AWS Region where the AMIs were created. The company needs to design an application that captures AWS API calls and sends alerts whenever the Amazon EC2 CreateImage API operation is called within the company's account.

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

A. Create an AWS Lambda function to query AWS CloudTrail logs and to send an alert when a CreateImage API call is detected.

B. Configure AWS CloudTrail with an Amazon Simple Notification Service {Amazon SNS) notification that

occurs when updated logs are sent to Amazon S3. Use Amazon Athena to create a new table and to query on CreateImage when an API call is detected.

C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for the CreateImage API call. Configure the target as an Amazon Simple Notification Service (Amazon SNS) topic to send an alert when a CreateImage API call is detected.

D. Configure an Amazon Simple Queue Service (Amazon SQS) FIFO queue as a target for AWS CloudTrail logs. Create an AWS Lambda function to send an alert to an Amazon Simple Notification Service (Amazon SNS) topic when a CreateImage API call is detected.

Answer: C

Explanation:

https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/monitor-ami-events.html#:~:text=For%20example%2C%20you%20can%20create%20an%20EventBridge%20rule%20that%20detects%20when%20the%20AMI%20creation%20process%20has%20completed%20and%20then%20invokes%20an%20Amazon%20SNS%20topic%20to% 20send%20an%20email%20notification%20to%20you.

Creating an Amazon EventBridge (Amazon CloudWatch Events) rule for the CreateImage API call and configuring the target as an Amazon Simple Notification Service (Amazon SNS) topic to send an alert when a CreateImage API call is detected will meet the requirements with the least operational overhead. Amazon EventBridge is a serverless event bus that makes it easy to connect applications together using data from your own applications, integrated Software as a Service (SaaS) applications, and AWS services. By creating an EventBridge rule for the CreateImage API call, the company can set up alerts whenever this operation is called within their account. The alert can be sent to an SNS topic, which can then be configured to send notifications to the company's email or other desired destination.

153. - (Topic 2)

A corporation has recruited a new cloud engineer who should not have access to the CompanyConfidential Amazon S3 bucket. The cloud engineer must have read and write permissions on an S3 bucket named AdminTools.

Which IAM policy will satisfy these criteria?

A.

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

B.

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

C.

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

D.

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

Answer: A

Explanation:

https://docs.amazonaws.cn/en_us/IAM/latest/UserGuide/reference_policies_examples_s3_ rw-bucket.html

The policy is separated into two parts because the ListBucket action requires permissions on the bucket while the other actions require permissions on the objects in the bucket. You must use two different

Amazon Resource Names (ARNs) to specify bucket-level and object-level permissions. The first Resource element specifies arn:aws:s3:::AdminTools for the ListBucket action so that applications can list all objects in the AdminTools bucket.

154. - (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 OB 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. Configure retry logic in the Lambda functions for attempts to connect to the database

B. Set up Amazon ElastiCache tor Redls to cache commonly read items from the database. Configure the Lambda functions to connect to ElastiCache for reads.

C. Add an Aurora Replica as a reader node. Configure the Lambda functions to connect to the reader endpoint of the OB cluster rather than lo the writer endpoint.

D. Use Amazon ROS Proxy to create a proxy. Set the DB cluster as the target database Configure the Lambda functions lo 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.

155. - (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

156. - (Topic 2)

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

What should the solutions architect recommend?

A. Implement EC2 Spot Instances

B. Purchase EC2 Reserved Instances

C. Implement EC2 On-Demand Instances

D. Implement the processing on AWS Lambda

Answer: A

Explanation:

EC2 Spot Instances allow users to bid on spare Amazon EC2 computing capacity and can be a cost-effective solution for stateless, interruptible workloads that can be started and stopped at any time. Since the batch processing job is stateless, can be started and stopped at any time, and typically takes upwards of 60 minutes to complete, EC2 Spot Instances would be a good fit for this workload.

157. - (Topic 2)

A company runs a web-based portal that provides users with global breaking news, local alerts, and weather updates. The portal delivers each user a personalized view by using mixture of static and dynamic content. Content is served over HTTPS through an API server running on an Amazon EC2 instance behind an Application Load Balancer (ALB). The company wants the portal to provide this content to its users across the world as quickly as possible.

How should a solutions architect design the application to ensure the LEAST amount of latency for all users?

A. Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve all static and dynamic content by specifying the ALB as an origin.

B. Deploy the application stack in two AWS Regions. Use an Amazon Route 53 latency routing policy to serve all content from the ALB in the closest Region.

C. Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve the static content. Serve the dynamic content directly from the ALB.

D. Deploy the application stack in two AWS Regions. Use an Amazon Route 53 geolocation routing policy to serve all content from the ALB in the closest Region.

Answer: A

Explanation:

https://aws.amazon.com/blogs/networking-and-content-delivery/deliver-your-apps-dynamic-content-using-amazon-cloudfront-getting-started-template/

158. - (Topic 2)

A hospital wants to create digital copies for its large collection of historical written records. The hospital will continue to add hundreds of new documents each day. The hospital's data team will scan the documents and will upload the documents to the AWS Cloud.

A solutions architect must implement a solution to analyze the documents, extract the medical information, and store the documents so that an application can run SQL queries on the data. The solution must maximize scalability and operational efficiency.

Which combination of steps should the solutions architect take to meet these requirements? (Select TWO.)

A. Write the document information to an Amazon EC2 instance that runs a MySQL database.

B. Write the document information to an Amazon S3 bucket. Use Amazon Athena to query the data.

C. Create an Auto Scaling group of Amazon EC2 instances to run a custom application that processes the scanned files and extracts the medical information.

D. Create an AWS Lambda function that runs when new documents are uploaded. Use Amazon Rekognition to convert the documents to raw text. Use Amazon Transcribe Medical to detect and extract relevant medical information from the text.

E. Create an AWS Lambda function that runs when new documents are uploaded. Use Amazon Textract to convert the documents to raw text. Use Amazon Comprehend Medical to detect and extract relevant medical information from the text.

Answer: B,E

Explanation:

This solution meets the requirements of creating digital copies for a large collection of historical written records, analyzing the documents, extracting the medical information, and storing the documents so that an application can run SQL queries on the data. Writing the document information to an Amazon S3 bucket can provide scalable and durable storage for the scanned files. Using Amazon Athena to query the data can provide serverless and interactive SQL analysis on data stored in S3. Creating an AWS Lambda function that runs when new documents are uploaded can provide event-driven and serverless processing of the scanned files. Using Amazon Textract to convert the documents to raw text can provide accurate optical character recognition (OCR) and extraction of structured data such as tables and forms from documents using artificial intelligence (AI). Using Amazon Comprehend Medical to detect and extract relevant medical information from the text can provide natural language processing (NLP) service that uses machine learning that has been pre-trained to understand and extract health data from medical text.

Option A is incorrect because writing the document information to an Amazon EC2 instance that runs a MySQL database can increase the infrastructure overhead and complexity, and it may not be able to handle large volumes of data. Option C is incorrect because creating an Auto Scaling group of Amazon

EC2 instances to run a custom application that processes the scanned files and extracts the medical information can increase the infrastructure overhead and complexity, and it may not be able to leverage existing AI and NLP services such as Textract and Comprehend Medical. Option D is incorrect because using Amazon Rekognition to convert the documents to raw text can provide image and video analysis, but it does not support OCR or extraction of structured data from documents. Using Amazon Transcribe Medical to detect and extract relevant medical information from the text can provide speech-to-text transcription service for medical conversations, but it does not support text analysis or extraction of health data from medical text.

References:

- https://aws.amazon.com/s3/
- https://aws.amazon.com/athena/
- https://aws.amazon.com/lambda/
- https://aws.amazon.com/textract/
- https://aws.amazon.com/comprehend/medical/

159. - (Topic 2)

A company stores its application logs in an Amazon CloudWatch Logs log group. A new policy requires the company to store all application logs in Amazon OpenSearch Service (Amazon Elasticsearch Service) in near-real time.

Which solution will meet this requirement with the LEAST operational overhead?

A. Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).

B. Create an AWS Lambda function. Use the log group to invoke the function to write the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).

C. Create an Amazon Kinesis Data Firehose delivery stream. Configure the log group as the delivery stream's source. Configure Amazon OpenSearch Service (Amazon Elasticsearch Service) as the delivery stream's destination.

D. Install and configure Amazon Kinesis Agent on each application server to deliver the logs to Amazon Kinesis Data Streams. Configure Kinesis Data Streams to deliver the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service)

Answer: B

Explanation: https://computingforgeeks.com/stream-logs-in-aws-from-cloudwatch-to- elasticsearch/

160. - (Topic 2)

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

Which solution will meet these requirements?

A. Migrate the Oracle database to an Amazon EC2 instance. Set up database replication to a different AWS Region.

B. Migrate the Oracle database to Amazon RDS for Oracle. Activate Cross-Region automated backups to replicate the snapshots to another AWS Region.

C. Migrate the Oracle database to Amazon RDS Custom for Oracle. Create a read replica for the database in another AWS Region.

D. Migrate the Oracle database to Amazon RDS for Oracle. Create a standby database in another Availability Zone.

Answer: C

Explanation:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-custom.html and https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/working-with-custom- oracle.html

161. - (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 OynamoDB 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/

162. - (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 WAR

How should the solutions architect comply with these requirements?

A. Configure an S3 bucket policy lo accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.

B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.

C. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only. Associate AWS WAF to CloudFront.

D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access

to the S3 bucket. Enable AWS WAF on the distribution.

Answer: D

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- awswaf.html

163. - (Topic 2)

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

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

A. Amazon CloudFront

B. AWS Global Accelerator

C. Amazon Route 53

D. Amazon S3 Transfer Acceleration

Answer: A

Explanation:

You can use CloudFront to deliver video on demand (VOD) or live streaming video using any HTTP origin. One way you can set up video workflows in the cloud is by using CloudFront together with AWS Media Services. https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streaming-video.html

164. - (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

165. - (Topic 2)

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

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

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

A. Add throttling on the API Gateway with server-side throttling limits.

B. Use DynamoDB Accelerator (DAX) and Lambda to buffer writes to DynamoDB.

C. Create a secondary index in DynamoDB for the table with the user requests.

D. Use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to

DynamoDB.

Answer: D

Explanation:

By using an SQS queue and Lambda, the solutions architect can decouple the API front end from the processing microservices and improve the overall scalability and availability of the system. The SQS queue acts as a buffer, allowing the API front end to continue accepting user requests even if the processing microservices are experiencing high workloads or are temporarily unavailable. The Lambda function can then retrieve requests from the SQS queue and write them to DynamoDB, ensuring that all user requests are stored and processed. This approach allows the company to scale the processing microservices independently from the API front end, ensuring that the API remains available to users even during periods of high demand.

166. - (Topic 2)

A company uses AWS Organizations to create dedicated AWS accounts for each business unit to manage each business unit's account independently upon request. The root email recipient missed a notification that was sent to the root user email address of one account. The company wants to ensure that all future notifications are not missed. Future notifications must be limited to account administrators.

Which solution will meet these requirements?

A. Configure the company's email server to forward notification email messages that are sent to the AWS account root user email address to all users in the organization.

B. Configure all AWS account root user email addresses as distribution lists that go to a few administrators who can respond to alerts. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.

C. Configure all AWS account root user email messages to be sent to one administrator who is responsible for monitoring alerts and forwarding those alerts to the appropriate groups.

D. Configure all existing AWS accounts and all newly created accounts to use the same root user email address. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.

Answer: B

Explanation: Use a group email address for the management account's root user

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html#best-practices_mgmt-acct_email-address

167. - (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/

168. - (Topic 2)

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

• An Amazon Simple Notation 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 tenure 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 me Lambda functions configuration to increase the CPU and memory allocations tor the (unction

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

169. - (Topic 2)

A company has two applications: a sender application that sends messages with payloads to be processed and a processing application intended to receive the messages with payloads. The company wants to implement an AWS service to handle messages between the two applications. The sender application can send about 1.000 messages each hour. The messages may take up to 2 days to be processed. If the messages fail to process, they must be retained so that they do not impact the processing of any remaining messages.

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

A. Set up an Amazon EC2 instance running a Redis database. Configure both applications to use the instance. Store, process, and delete the messages, respectively.

B. Use an Amazon Kinesis data stream to receive the messages from the sender application. Integrate the processing application with the Kinesis Client Library (KCL).

C. Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue. Configure a dead-letter queue to collect the messages that failed to process.

D. Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications to process. Integrate the sender application to write to the SNS topic.

Answer: C

Explanation:

https://aws.amazon.com/blogs/compute/building-loosely-coupled-scalable-c-applications-with-amazon-sqs-and-amazon-sns/

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html

170. - (Topic 2)

A gaming company has a web application that displays scores. The application runs on Amazon EC2 instances behind an Application Load Balancer. The application stores data in an Amazon RDS for MySQL database. Users are starting to experience long delays and interruptions that are caused by database read

performance. The company wants to improve the user experience while minimizing changes to the application's architecture.

What should a solutions architect do to meet these requirements?

A. Use Amazon ElastiCache in front of the database.

B. Use RDS Proxy between the application and the database.

C. Migrate the application from EC2 instances to AWS Lambda.

D. Migrate the database from Amazon RDS for MySQL to Amazon DynamoDB.

Answer: A

Explanation:

ElastiCache can help speed up the read performance of the database by caching frequently accessed data, reducing latency and allowing the application to access the data more quickly. This solution requires minimal modifications to the current architecture, as ElastiCache can be used in conjunction with the existing Amazon RDS for MySQL database.

171. - (Topic 2)

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

Which action should the solutions architect take to accomplish this?

A. Generate presigned URLs for the files.

B. Use cross-Region replication to all Regions.

C. Use the geoproximtty feature of Amazon Route 53.

D. Use Amazon CloudFront with the S3 bucket as its origin.

Answer: D

Explanation:

Amazon CloudFront is a content delivery network (CDN) that speeds up the delivery of static and dynamic web content, such as HTML pages, images, and videos. By using CloudFront, the HTML pages will be served to users from the edge location that is closest to them, resulting in faster delivery and a better user experience. CloudFront can also handle the high traffic and large number of requests expected for the global event, ensuring that the HTML pages are available and accessible to users around the world.

172. - (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. Create an AMI of the web application. Use the AMI to launch a second EC2 On-Demand Instance. Use an Application Load Balancer to distribute the load to each EC2 instance.

B. Migrate the database to an Amazon RDS for MySQL DB instance. Create an AMI of the web application. Use the AMI to launch a second EC2 On-Demand Instance. Use Amazon Route 53 weighted routing to distribute the load across the two EC2 instances.

C. Migrate the database to an Amazon Aurora MySQL DB instance. Create an AWS Lambda function to stop the EC2 instance and change the instance type. Create an Amazon CloudWatch alarm to invoke the Lambda function when CPU utilization surpasses 75%.

D. Migrate the database to an Amazon Aurora MySQL DB instance. Create an AMI of the web application. Apply the AMI to a launch template. Create an Auto Scaling group with the launch template Configure the launch template to use a Spot Fleet. Attach an Application Load Balancer to the Auto Scaling group.

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.

173. - (Topic 2)

A company has a service that produces event data. The company wants to use AWS to process the event data as it is received. The data is written in a specific order that must be maintained throughout processing The company wants to implement a solution that minimizes operational overhead.

How should a solutions architect accomplish this?

A. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages Set up an AWS Lambda function to process messages from the queue

B. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process Configure an AWS Lambda function as a subscriber.

C. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to hold messages. Set up an AWS Lambda function to process messages from the queue independently

D. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a subscriber.

Answer: A

Explanation: The details are revealed in below url:

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO- queues.html

FIFO (First-In-First-Out) queues are designed to enhance messaging between applications when the order of operations and events is critical, or where duplicates can't be tolerated. Examples of situations where you might use FIFO queues include the following: To make sure that user-entered commands are run in the right order. To display the correct product price by sending price modifications in the right order. To prevent a student from enrolling in a course before registering for an account.

174. - (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. Grant the user read permission to objects in the S3 bucket. Assign the user to CloudFront.

C. Write an S3 bucket policy that assigns the CloudFront distribution ID as the Principal and assigns the target S3 bucket as the Amazon Resource Name (ARN).

D. Create an origin access identity (OAI). Assign the OAI to the CloudFront distribution. Configure the S3 bucket permissions so that only the OAI has read permission.

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

175. - (Topic 2)

A business's backup data totals 700 terabytes (TB) and is kept in network attached storage (NAS) at its data center. This backup data must be available in the event of occasional regulatory inquiries and preserved for a period of seven years. The organization has chosen to relocate its backup data from its on-premises data center to Amazon Web Services (AWS). Within one month, the migration must be completed. The company's public internet connection provides 500 Mbps of dedicated capacity for data transport.

What should a solutions architect do to ensure that data is migrated and stored at the LOWEST possible cost?

A. Order AWS Snowball devices to transfer the data. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.

B. Deploy a VPN connection between the data center and Amazon VPC. Use the AWS CLI to copy the data from on premises to Amazon S3 Glacier.

C. Provision a 500 Mbps AWS Direct Connect connection and transfer the data to Amazon S3. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.

D. Use AWS DataSync to transfer the data and deploy a DataSync agent on premises. Use the DataSync task to copy files from the on-premises NAS storage to Amazon S3 Glacier.

Answer: A

Explanation: https://www.omnicalculator.com/other/data-transfer

176. - (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 Regions. Associate Regional web ACLs with an API stage.

B. Set up AWS Firewall Manager in both Regions. Centrally configure AWS WAF rules.

C. Set up AWS Shield in bath Regions. Associate Regional web ACLs with an API stage.

D. Set up AWS Shield in one of the Regions. Associate Regional web ACLs with an API stage.

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

177. - (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."

178. - (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 MQ. Create a Multi-AZ Auto Scaling group (or EC2 instances that host the application. Create another Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database.

B. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon MQ. Create a Multi-AZ Auto Scaling group for EC2 instances that host the application. Migrate the database to run on a Multi-AZ deployment of Amazon RDS for PostgreSQL.

C. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queue. Create another Multi-AZ Auto Scaling group for EC2 instances that host the application.

Migrate the database to run on a Multi-AZ deployment of Amazon RDS fqjPostgreSQL.

D. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queue.

Create another Multi-AZ Auto Scaling group for EC2 instances that host the application. Create a third Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database.

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/

179. - (Topic 2)

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

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

A. Replace the EC2 Instances with T3 EC2 instances that run in an Auto Scaling group. Made the changes by using the AWS Management Console.

B. Modify the CloudFormation templates to run the EC2 instances in an Auto Scaling group. Increase the desired capacity and the maximum capacity of the Auto Scaling group manually when an increase is necessary

C. Modify the CloudFormation templates. Replace the EC2 instances with R5 EC2 instances. Use Amazon CloudWatch built-in EC2 memory metrics to track the application performance for future capacity planning.

D. Modify the CloudFormation templates. Replace the EC2 instances with R5 EC2 instances. Deploy the Amazon CloudWatch agent on the EC2 instances to generate custom application latency metrics for future capacity planning.

Answer: D

Explanation:

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

180. - (Topic 2)

A company runs a stateless web application in production on a group of Amazon EC2 On- Demand Instances behind an Application Load Balancer. The application experiences heavy usage during an 8-hour period each business day. Application usage is moderate and steady overnight Application usage is low during weekends.

The company wants to minimize its EC2 costs without affecting the availability of the application.

Which solution will meet these requirements?

A. Use Spot Instances for the entire workload.

B. Use Reserved instances for the baseline level of usage Use Spot Instances for any additional capacity that the application needs.

C. Use On-Demand Instances for the baseline level of usage. Use Spot Instances for any additional capacity that the application needs

D. Use Dedicated Instances for the baseline level of usage. Use On-Demand Instances for any additional capacity that the application needs

Answer: B

Explanation:

Reserved is cheaper than on demand the company has. And it's meet the availabilty (HA) requirement as to spot instance that can be disrupted at any time. PRICING BELOW. On- Demand: 0% There’s no commitment from you. You pay the most with this option. Reserved : 40%-60%1-year or 3-year commitment from you. You save money from that commitment. Spot 50%-90% Ridiculously inexpensive because there’s no commitment from the AWS side.

181. - (Topic 2)

A company needs to retain application logs files for a critical application for 10 years. The application team regularly accesses logs from the past month for troubleshooting, but logs older than 1 month are rarely accessed. The application generates more than 10 TB of logs per month.

Which storage option meets these requirements MOST cost-effectively?

A. Store the logs in Amazon S3 Use AWS Backup lo move logs more than 1 month old to S3 Glacier Deep Archive

B. Store the logs in Amazon S3 Use S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive

C. Store the logs in Amazon CloudWatch Logs Use AWS Backup to move logs more then 1 month old to S3 Glacier Deep Archive

D. Store the logs in Amazon CloudWatch Logs Use Amazon S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive

Answer: B

Explanation:

You need S3 to be able to archive the logs after one month. Cannot do that with CloudWatch Logs.

182. - (Topic 2)

A company wants to migrate its existing on-premises monolithic application to AWS.

The company wants to keep as much of the front- end code and the backend code as possible. However, the company wants to break the application into smaller applications. A different team will manage each application. The company needs a highly scalable solution that minimizes operational overhead.

Which solution will meet these requirements?

A. Host the application on AWS Lambda Integrate the application with Amazon API Gateway.

B. Host the application with AWS Amplify. Connect the application to an Amazon API Gateway API that is integrated with AWS Lambda.

C. Host the application on Amazon EC2 instances. Set up an Application Load Balancer with EC2 instances in an Auto Scaling group as targets.

D. Host the application on Amazon Elastic Container Service (Amazon ECS) Set up an Application Load Balancer with Amazon ECS as the target.

Answer: D

Explanation:

https://aws.amazon.com/blogs/compute/microservice-delivery-with-amazon-ecs-and-application-load-balancers/

183. - (Topic 2)

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

launched using default options.

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

A. Choose a cluster placement group while launching Amazon EC2 instances.

B. Choose dedicated instance tenancy while launching Amazon EC2 instances.

C. Choose an Elastic Inference accelerator while launching Amazon EC2 instances.

D. Choose the required capacity reservation while launching Amazon EC2 instances.

Answer: A

Explanation:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-placementgroup.html

"A cluster placement group is a logical grouping of instances within a single Availability Zone that benefit from low network latency, high network throughput"

184. - (Topic 2)

A solutions architect needs to implement a solution to reduce a company's storage costs. All the company's data is in the Amazon S3 Standard storage class. The company must keep all data for at least 25 years. Data from the most recent 2 years must be highly available and immediately retrievable.

Which solution will meet these requirements?

A. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive immediately.

B. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 2 years.

C. Use S3 Intelligent-Tiering. Activate the archiving option to ensure that data is archived in S3 Glacier Deep Archive.

D. Set up an S3 Lifecycle policy to transition objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately and to S3 Glacier Deep Archive after 2 years.

Answer: B

Explanation:

https://aws.amazon.com/about-aws/whats-new/2018/04/announcing-s3-one-zone-infrequent-access-a-new-amazon-s3-storage-class/?nc1=h_ls

185. - (Topic 2)

A company runs a global web application on Amazon EC2 instances behind an Application Load Balancer The application stores data in Amazon Aurora. The company needs to create a disaster recovery solution and can tolerate up to 30 minutes of downtime and potential data loss. The solution does not need to handle the load when the primary infrastructure is healthy

What should a solutions architect do to meet these requirements?

A. Deploy the application with the required infrastructure elements in place Use Amazon Route 53 to configure active-passive failover Create an Aurora Replica in a second AWS Region

B. Host a scaled-down deployment of the application in a second AWS Region Use Amazon Route 53 to configure active-active failover Create an Aurora Replica in the second Region

C. Replicate the primary infrastructure in a second AWS Region Use Amazon Route 53 to configure active-active failover Create an Aurora database that is restored from the latest snapshot

D. Back up data with AWS Backup Use the backup to create the required infrastructure in a second AWS Region Use Amazon Route 53 to configure active-passive failover Create an Aurora second primary instance in the second Region

Answer: A

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

186. - (Topic 2)

A company has a legacy data processing application that runs on Amazon EC2 instances. Data is processed sequentially, but the order of results does not matter. The application uses a monolithic architecture. The only way that the company can scale the application to meet increased demand is to increase the size of the instances.

The company's developers have decided to rewrite the application to use a microservices architecture on Amazon Elastic Container Service (Amazon ECS).

What should a solutions architect recommend for communication between the microservices?

A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Add code to the data producers, and send data to the queue. Add code to the data consumers to process data from the queue.

B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Add code to the data producers, and publish notifications to the topic. Add code to the data consumers to subscribe to the topic.

C. Create an AWS Lambda function to pass messages. Add code to the data producers to call the Lambda

function with a data object. Add code to the data consumers to receive a data object that is passed from the Lambda function.

D. Create an Amazon DynamoDB table. Enable DynamoDB Streams. Add code to the data producers to insert data into the table. Add code to the data consumers to use the DynamoDB Streams API to detect new table entries and retrieve the data.

Answer: A

Explanation:

Queue has Limited throughput (300 msg/s without batching, 3000 msg/s with batching whereby up-to 10 msg per batch operation; Msg duplicates not allowed in the queue (exactly-once delivery); Msg order is preserved (FIFO); Queue name must end with .fifo

187. - (Topic 2)

A solutions architect is designing a customer-facing application for a company. The application's database will have a clearly defined access pattern throughout the year and will have a variable number of reads and writes that depend on the time of year. The company must retain audit records for the database for 7 days. The recovery point objective (RPO) must be less than 5 hours.

Which solution meets these requirements?

A. Use Amazon DynamoDB with auto scaling Use on-demand backups and Amazon DynamoDB Streams

B. Use Amazon Redshift. Configure concurrency scaling. Activate audit logging. Perform database snapshots every 4 hours.

C. Use Amazon RDS with Provisioned IOPS Activate the database auditing parameter Perform database snapshots every 5 hours

D. Use Amazon Aurora MySQL with auto scaling. Activate the database auditing parameter

Answer: A

Explanation:

This solution meets the requirements of a customer-facing application that has a clearly defined access pattern throughout the year and a variable number of reads and writes that depend on the time of year. Amazon DynamoDB is a fully managed NoSQL database service that can handle any level of request traffic and data size. DynamoDB auto scaling can automatically adjust the provisioned read and write capacity based on the actual workload. DynamoDB on-demand backups can create full backups of the tables for

data protection and archival purposes. DynamoDB Streams can capture a time-ordered sequence of item-level modifications in the tables for audit purposes.

Option B is incorrect because Amazon Redshift is a data warehouse service that is designed for analytical workloads, not for customer-facing applications. Option C is incorrect because Amazon RDS with Provisioned IOPS can provide consistent performance for relational databases, but it may not be able to handle unpredictable spikes in traffic and data size. Option D is incorrect because Amazon Aurora MySQL with auto scaling can provide high performance and availability for relational databases, but it does not support audit logging as a parameter.

References:

- https://aws.amazon.com/dynamodb/
- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScalin g.html
- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/BackupRe store.html
- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.ht ml

188. - (Topic 2)

A company wants to run applications in containers in the AWS Cloud. These applications are stateless and can tolerate disruptions within the underlying infrastructure. The company needs a solution that minimizes cost and operational overhead.

What should a solutions architect do to meet these requirements?

A. Use Spot Instances in an Amazon EC2 Auto Scaling group to run the application containers.

B. Use Spot Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.

C. Use On-Demand Instances in an Amazon EC2 Auto Scaling group to run the application containers.

D. Use On-Demand Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.

Answer: A

Explanation:

https://aws.amazon.com/cn/blogs/compute/cost-optimization-and-resilience-eks-with-spot-instances/

189. - (Topic 2)

A solutions architect needs to securely store a database user name and password that an application uses

to access an Amazon RDS DB instance. The application that accesses the database runs on an Amazon EC2 instance. The solutions architect wants to create a secure parameter in AWS Systems Manager Parameter Store.

What should the solutions architect do to meet this requirement?

A. Create an IAM role that has read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM role to the EC2 instance.

B. Create an IAM policy that allows read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM policy to the EC2 instance.

C. Create an IAM trust relationship between the Parameter Store parameter and the EC2 instance. Specify Amazon RDS as a principal in the trust policy.

D. Create an IAM trust relationship between the DB instance and the EC2 instance. Specify Systems Manager as a principal in the trust policy.

Answer: B

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-services-that-work- with-iam.html

190. - (Topic 2)

A gaming company is designing a highly available architecture. The application runs on a modified Linux kernel and supports only UDP-based traffic. The company needs the front- end tier to provide the best possible user experience. That tier must have low latency, route traffic to the nearest edge location, and provide static IP addresses for entry into the application endpoints.

What should a solutions architect do to meet these requirements?

A. Configure Amazon Route 53 to forward requests to an Application Load Balancer. Use AWS Lambda for the application in AWS Application Auto Scaling.

B. Configure Amazon CloudFront to forward requests to a Network Load Balancer. Use AWS Lambda for the application in an AWS Application Auto Scaling group.

C. Configure AWS Global Accelerator to forward requests to a Network Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.

D. Configure Amazon API Gateway to forward requests to an Application Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.

Answer: C

Explanation:

AWS Global Accelerator and Amazon CloudFront are separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable content (such as images and videos) and dynamic content (such as API acceleration and dynamic site delivery). Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non- HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. Both services integrate with AWS Shield for DDoS protection.

191. - (Topic 2)

A company recently started using Amazon Aurora as the data store for its global ecommerce application When large reports are run developers report that the ecommerce application is performing poorly After reviewing metrics in Amazon CloudWatch, a solutions architect finds that the ReadIOPS and CPUUtilization metrics are spiking when monthly reports run.

What is the MOST cost-effective solution?

A. Migrate the monthly reporting to Amazon Redshift.

B. Migrate the monthly reporting to an Aurora Replica

C. Migrate the Aurora database to a larger instance class

D. Increase the Provisioned IOPS on the Aurora instance

Answer: B

Explanation: https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.htm l #Aurora.Replication.Replicas Aurora Replicas have two main purposes. You can issue queries to them to scale the read operations for your application. You typically do so by connecting to the reader endpoint of the cluster. That way, Aurora can spread the load for read-only connections across as many Aurora Replicas as you have in the cluster. Aurora Replicas also help to increase availability. If the writer instance in a cluster becomes unavailable, Aurora automatically promotes one of the reader instances to take its

place as the new writer.

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

192. - (Topic 2)

A company uses a three-tier web application to provide training to new employees. The application is accessed for only 12 hours every day. The company is using an Amazon RDS for MySQL DB instance to store information and wants to minimize costs.

What should a solutions architect do to meet these requirements?

A. Configure an IAM policy for AWS Systems Manager Session Manager. Create an IAM role for the policy. Update the trust relationship of the role. Set up automatic start and stop for the DB instance.

B. Create an Amazon ElastiCache for Redis cache cluster that gives users the ability to access the data from the cache when the DB instance is stopped. Invalidate the cache after the DB instance is started.

C. Launch an Amazon EC2 instance. Create an IAM role that grants access to Amazon RDS. Attach the role to the EC2 instance. Configure a cron job to start and stop the EC2 instance on the desired schedule.

D. Create AWS Lambda functions to start and stop the DB instance. Create Amazon EventBridge (Amazon CloudWatch Events) scheduled rules to invoke the Lambda functions. Configure the Lambda functions as event targets for the rules

Answer: D

Explanation:

In a typical development environment, dev and test databases are mostly utilized for 8 hours a day and sit idle when not in use. However, the databases are billed for the compute and storage costs during this idle time. To reduce the overall cost, Amazon RDS allows instances to be stopped temporarily. While the instance is stopped, you're charged for storage and backups, but not for the DB instance hours. Please note that a stopped instance will automatically be started after 7 days. This post presents a solution using AWS Lambda and Amazon EventBridge that allows you to schedule a Lambda function to stop and start the idle databases with specific tags to save on compute costs. The second post presents a solution that accomplishes stop and start of the idle Amazon RDS databases using AWS Systems Manager.

193. - (Topic 2)

A company wants to migrate its MySQL database from on premises to AWS. The company recently

experienced a database outage that significantly impacted the business. To ensure this does not happen again, the company wants a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes.

Which solution meets these requirements?

A. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.

B. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.

C. Create an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data.

D. Create an Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance.

Answer: B

Explanation:

Q: What does Amazon RDS manage on my behalf?

Amazon RDS manages the work involved in setting up a relational database: from provisioning the infrastructure capacity you request to installing the database software. Once your database is up and running, Amazon RDS automates common administrative tasks such as performing backups and patching the software that powers your database. With optional Multi-AZ deployments, Amazon RDS also manages synchronous data replication across Availability Zones with automatic failover.

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

194. - (Topic 2)

A company needs to move data from an Amazon EC2 instance to an Amazon S3 bucket. The company must ensure that no API calls and no data are routed through public internet routes. Only the EC2 instance can have access to upload data to the S3 bucket.

Which solution will meet these requirements?

A. Create an interface VPC endpoint for Amazon S3 in the subnet where the EC2 instance is located. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.

B. Create a gateway VPC endpoint for Amazon S3 in the Availability Zone where the EC2 instance is

located. Attach appropriate security groups to the endpoint. Attach a resource policy lo the S3 bucket to only allow the EC2 instance's IAM role for access.

C. Run the nslookup tool from inside the EC2 instance to obtain the private IP address of the S3 bucket's service API endpoint. Create a route in the VPC route table to provide the

EC2 instance with access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.

D. Use the AWS provided, publicly available ip-ranges.json tile to obtain the private IP address of the S3 bucket's service API endpoint. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.

Answer: A

Explanation:

(https://aws.amazon.com/blogs/security/how-to-restrict-amazon-s3-bucket-access-to-a-specific-iam-role/)

195. - (Topic 2)

A company's website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company's website demands globally. The solution should be cost-effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.

Which combination should a solutions architect recommend to meet these requirements?

A. Amazon CloudFront and Amazon S3

B. AWS Lambda and Amazon DynamoDB

C. Application Load Balancer with Amazon EC2 Auto Scaling

D. Amazon Route 53 with internal Application Load Balancers

Answer: A

Explanation:

Cloudfront for rapid response and s3 to minimize infrastructure.

196. - (Topic 2)

A company has implemented a self-managed DNS solution on three Amazon EC2 instances behind a

Network Load Balancer (NLB) in the us-west-2 Region. Most of the company's users are located in the United States and Europe. The company wants to improve the performance and availability of the solution. The company launches and configures three EC2 instances in the eu-west-1 Region and adds the EC2 instances as targets for a new NLB.

Which solution can the company use to route traffic to all the EC2 instances?

A. Create an Amazon Route 53 geolocation routing policy to route requests to one of the two NLBs. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.

B. Create a standard accelerator in AWS Global Accelerator. Create endpoint groups in us- west-2 and eu-west-1. Add the two NLBs as endpoints for the endpoint groups.

C. Attach Elastic IP addresses to the six EC2 instances. Create an Amazon Route 53 geolocation routing policy to route requests to one of the six EC2 instances. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.

D. Replace the two NLBs with two Application Load Balancers (ALBs). Create an Amazon Route 53 latency routing policy to route requests to one of the two ALBs. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.

Answer: B

Explanation:

For standard accelerators, Global Accelerator uses the AWS global network to route traffic to the optimal regional endpoint based on health, client location, and policies that you configure, which increases the availability of your applications. Endpoints for standard accelerators can be Network Load Balancers, Application Load Balancers, Amazon EC2 instances, or Elastic IP addresses that are located in one AWS Region or multiple Regions.

https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html

197. - (Topic 2)

A company is running a multi-tier web application on premises. The web application is containerized and runs on a number of Linux hosts connected to a PostgreSQL database that contains user records. The operational overhead of maintaining the infrastructure and capacity planning is limiting the company's growth. A solutions architect must improve the application's infrastructure.

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

A. Migrate the PostgreSQL database to Amazon Aurora

B. Migrate the web application to be hosted on Amazon EC2 instances.

C. Set up an Amazon CloudFront distribution for the web application content.

D. Set up Amazon ElastiCache between the web application and the PostgreSQL database.

E. Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).

Answer: A,E

Explanation:

Amazon Aurora is a fully managed, scalable, and highly available relational database service that is compatible with PostgreSQL. Migrating the database to Amazon Aurora would reduce the operational overhead of maintaining the database infrastructure and allow the company to focus on building and scaling the application. AWS Fargate is a fully managed container orchestration service that enables users to run containers without the need to manage the underlying EC2 instances. By using AWS Fargate with Amazon Elastic Container Service (Amazon ECS), the solutions architect can improve the scalability and efficiency of the web application and reduce the operational overhead of maintaining the underlying infrastructure.

198. - (Topic 2)

A large media company hosts a web application on AWS. The company wants to start caching confidential media files so that users around the world will have reliable access to the files. The content is stored in Amazon S3 buckets. The company must deliver the content quickly, regardless of where the requests originate geographically.

Which solution will meet these requirements?

A. Use AWS DataSync to connect the S3 buckets to the web application.

B. Deploy AWS Global Accelerator to connect the S3 buckets to the web application.

C. Deploy Amazon CloudFront to connect the S3 buckets to CloudFront edge servers.

D. Use Amazon Simple Queue Service (Amazon SQS) to connect the S3 buckets to the web application.

Answer: C

Explanation: CloudFront uses a local cache to provide the response, AWS Global accelerator proxies requests and connects to the application all the time for the response.

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-acces

s-to-s3.html#private-content-granting-permissions-to-oai

199. - (Topic 2)

A company is running several business applications in three separate VPCs within me us- east-1 Region. The applications must be able to communicate between VPCs. The applications also must be able to consistently send hundreds to gigabytes of data each day to a latency-sensitive application that runs in a single on-premises data center.

A solutions architect needs to design a network connectivity solution that maximizes cost- effectiveness Which solution moots those requirements?

A. Configure three AWS Site-to-Site VPN connections from the data center to AWS Establish connectivity by configuring one VPN connection for each VPC

B. Launch a third-party virtual network appliance in each VPC Establish an iPsec VPN tunnel between the Data center and each virtual appliance

C. Set up three AWS Direct Connect connections from the data center to a Direct Connect gateway in us-east-1 Establish connectivity by configuring each VPC to use one of the Direct Connect connections

D. Set up one AWS Direct Connect connection from the data center to AWS. Create a transit gateway, and attach each VPC to the transit gateway. Establish connectivity between the Direct Connect connection and the transit gateway.

Answer: D

Explanation:

https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway.html

200. - (Topic 2)

A company is migrating an application from on-premises servers to Amazon EC2 instances. As part of the migration design requirements, a solutions architect must implement infrastructure metric alarms. The company does not need to take action if CPU utilization increases to more than 50% for a short burst of time. However, if the CPU

utilization increases to more than 50% and read IOPS on the disk are high at the same time, the company needs to act as soon as possible. The solutions architect also must reduce false alarms.

What should the solutions architect do to meet these requirements?

A. Create Amazon CloudWatch composite alarms where possible.

B. Create Amazon CloudWatch dashboards to visualize the metrics and react to issues quickly.

C. Create Amazon CloudWatch Synthetics canaries to monitor the application and raise an alarm.

D. Create single Amazon CloudWatch metric alarms with multiple metric thresholds where possible.

Answer: A

Explanation: Composite alarms determine their states by monitoring the states of other alarms. You can **use composite alarms to reduce alarm noise**. For example, you can create a composite alarm where the underlying metric alarms go into ALARM when they meet specific conditions. You then can set up your composite alarm to go into ALARM and send you notifications when the underlying metric alarms go into ALARM by configuring the underlying metric alarms never to take actions. Currently, composite alarms can take the following actions:

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

Topic 3, Exam Pool C

201. - (Topic 3)

A company has migrated an application to Amazon EC2 Linux instances. One of these EC2 instances runs several 1-hour tasks on a schedule. These tasks were written by different teams and have no common programming language. The company is concerned about performance and scalability while these tasks run on a single instance. A solutions architect needs to implement a solution to resolve these concerns. Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS Batch to run the tasks as jobs. Schedule the jobs by using Amazon EventBridge (Amazon CloudWatch Events).

B. Convert the EC2 instance to a container. Use AWS App Runner to create the container on demand to run the tasks as jobs.

C. Copy the tasks into AWS Lambda functions. Schedule the Lambda functions by using Amazon EventBridge (Amazon CloudWatch Events).

D. Create an Amazon Machine Image (AMI) of the EC2 instance that runs the tasks. Create an Auto Scaling group with the AMI to run multiple copies of the instance.

Answer: A

Explanation:

AWS Batch is a fully managed service that enables users to run batch jobs on AWS. It can handle different types of tasks written in different languages and run them on EC2 instances. It also integrates with Amazon EventBridge (Amazon CloudWatch Events) to schedule jobs based on time or event triggers. This solution will meet the requirements of performance, scalability and low operational overhead12.

* B. Convert the EC2 instance to a container. Use AWS App Runner to create the container on demand to run the tasks as jobs. This solution will not meet the requirement of low operational overhead, as it involves converting the EC2 instance to a container and using AWS App Runner, which is a service that automatically builds and deploys web applications and load balances traffic2. This is not necessary for running batch jobs.

* C. Copy the tasks into AWS Lambda functions. Schedule the Lambda functions by using Amazon EventBridge (Amazon CloudWatch Events). This solution will not meet the requirement of performance, as AWS Lambda has a limit of 15 minutes for execution time and 10 GB for memory allocation3. These limits may not be sufficient for running 1-hour tasks.

* D. Create an Amazon Machine Image (AMI) of the EC2 instance that runs the tasks. Create an Auto Scaling group with the AMI to run multiple copies of the instance. This solution will not meet the requirement of low operational overhead, as it involves creating and maintaining AMIs and Auto Scaling groups, which are additional resources that need to be configured and managed2.

Reference URL: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/compute- services.html

202. - (Topic 3)

A company is migrating an old application to AWS The application runs a batch job every hour and is CPU intensive The batch job takes 15 minutes on average with an on-premises server The server has 64 virtual CPU (vCPU) and 512 GiB of memory

Which solution will run the batch job within 15 minutes with the LEAST operational overhead?

A. Use AWS Lambda with functional scaling

B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate

C. Use Amazon Lightsail with AWS Auto Scaling

D. Use AWS Batch on Amazon EC2

Answer: D

Explanation:

Use AWS Batch on Amazon EC2. AWS Batch is a fully managed batch processing service that can be used to easily run batch jobs on Amazon EC2 instances. It can scale the number of instances to match the workload, allowing the batch job to be completed in the desired time frame with minimal operational overhead.

Using AWS Lambda with Amazon API Gateway - AWS Lambda

https://docs.aws.amazon.com/lambda/latest/dg/services-apigateway.html

AWS Lambda FAQs https://aws.amazon.com/lambda/faqs/

203. - (Topic 3)

A media company hosts its website on AWS. The website application's architecture includes a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) and a database that is hosted on Amazon Aurora The company's cyber security teem reports that the application is vulnerable to SOL injection.

How should the company resolve this issue?

A. Use AWS WAF in front of the ALB Associate the appropriate web ACLs with AWS WAF.

B. Create an ALB listener rule to reply to SQL injection with a fixed response

C. Subscribe to AWS Shield Advanced to block all SQL injection attempts automatically.

D. Set up Amazon Inspector to block all SOL injection attempts automatically

Answer: A

Explanation:

https://aws.amazon.com/premiumsupport/knowledge-center/waf-block-common-attacks/#:~:text=To%20protect%20your%20applications%20against,%2C%20query%20string%2C%20or%20URI. ---------- ---------- Protect against SQL injection and cross-site scripting To protect your applications against SQL injection and cross-site scripting (XSS) attacks, use the built- in SQL injection and cross-site scripting engines. Remember that attacks can be performed on different parts of the HTTP request, such as the HTTP header, query string, or URI. Configure the AWS WAF rules to inspect different parts of the HTTP request against the built-in mitigation engines.

204. - (Topic 3)

An ecommerce company is experiencing an increase in user traffic. The company's store is deployed on Amazon EC2 instances as a two-tier web application consisting of a web tier and a separate database tier. As traffic increases, the company notices that the architecture is causing significant delays in sending timely marketing and order confirmation email to users. The company wants to reduce the time it spends resolving complex email delivery issues and minimize operational overhead.

What should a solutions architect do to meet these requirements?

A. Create a separate application tier using EC2 instances dedicated to email processing.

B. Configure the web instance to send email through Amazon Simple Email Service (Amazon SES).

C. Configure the web instance to send email through Amazon Simple Notification Service (Amazon SNS)

D. Create a separate application tier using EC2 instances dedicated to email processing. Place the instances in an Auto Scaling group.

Answer: B

Explanation: Amazon SES is a cost-effective and scalable email service that enables businesses to send and receive email using their own email addresses and domains. Configuring the web instance to send email through Amazon SES is a simple and effective solution that can reduce the time spent resolving complex email delivery issues and minimize operational overhead.

205. - (Topic 3)

A company is running a multi-tier recommence web application in the AWS Cloud. The application runs on Amazon EC2 instances with an Amazon RDS for MySQL Multi-AZ OB instance. Amazon ROS is configured with the latest generation DB instance with 2.000 GB of storage In a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBSl volume. The database performance affects the application during periods high demand.

A database administrator analyzes the logs in Amazon CloudWatch Logs and discovers that the application performance always degrades when the number of read and write IOPS is higher than 20.000.

What should a solutions architect do to improve the application performance?

A. Replace the volume with a magnetic volume.

B. Increase the number of IOPS on the gp3 volume.

C. Replace the volume with a Provisioned IOPS SSD (Io2) volume.

D. Replace the 2.000 GB gp3 volume with two 1.000 GB gp3 volumes

Answer: C

Explanation:

https://aws.amazon.com/ebs/features/ Amazon EBS provides a range of options that allow you to optimize storage performance and cost for your workload. These options are divided into two major categories: SSD-backed storage for transactional workloads, such as databases and boot volumes (performance depends primarily on IOPS), and HDD-backed storage for throughput intensive workloads, such as MapReduce and log processing (performance depends primarily on MB/s).

206. - (Topic 3)

A company will deployed a web application on AWS. The company hosts the backend database on Amazon RDS for MySQL with a primary DB instance and five read replicas to support scaling needs. The read replicas must log no more than 1 second bahind the primary DB Instance. The database routinely runs scheduled stored procedures.

As traffic on the website increases, the replicas experinces addtional lag during periods of peak lead. A solutions architect must reduce the replication lag as much as possible. The solutions architect must minimize changes to the applicatin code and must minimize ongoing overhead.

Which solution will meet these requirements?

Migrate the database to Amazon Aurora MySQL. Replace the read replicas with Aurora Replicas, and configure Aurora Auto Scaling. Replace the stored procedures with Aurora

MySQL native functions.

Deploy an Amazon ElasticCache for Redis cluser in front of the database. Modify the application to check the cache before the application queries the database. Repace the stored procedures with AWS Lambda funcions.

A. Migrate the database to a MYSQL database that runs on Amazn EC2 instances. Choose large, compute optimized for all replica nodes. Maintain the stored procedures on the EC2 instances.

B. Deploy an Amazon ElastiCache for Redis cluster in fornt of the database. Modify the application to check the cache before the application queries the database. Replace the stored procedures with AWS Lambda functions.

C. Migrate the database to a MySQL database that runs on Amazon EC2 instances. Choose large,

compute optimized EC2 instances for all replica nodes, Maintain the stored procedures on the EC2 instances.

D. Migrate the database to Amazon DynamoDB, Provision number of read capacity units (RCUs) to support the required throughput, and configure on-demand capacity scaling. Replace the stored procedures with DynamoDB streams.

Answer: A

Explanation:

Option A is the most appropriate solution for reducing replication lag without significant changes to the application code and minimizing ongoing operational overhead. Migrating the database to Amazon Aurora MySQL allows for improved replication performance and higher scalability compared to Amazon RDS for MySQL. Aurora Replicas provide faster replication, reducing the replication lag, and Aurora Auto Scaling ensures that there are enough Aurora Replicas to handle the incoming traffic. Additionally, Aurora MySQL native functions can replace the stored procedures, reducing the load on the database and improving performance.

207. - (Topic 3)

A gaming company is moving its public scoreboard from a data center to the AWS Cloud. The company uses Amazon EC2 Windows Server instances behind an Application Load Balancer to host its dynamic application. The company needs a highly available storage solution for the application. The application consists of static files and dynamic server-side code.

Which combination of steps should a solutions architect take to meet these requirements? (Select TWO.)

A. Store the static files on Amazon S3. Use Amazon CloudFront to cache objects at the edge.

B. Store the static files on Amazon S3. Use Amazon ElastiCache to cache objects at the edge.

C. Store the server-side code on Amazon Elastic File System (Amazon EFS). Mount the EFS volume on each EC2 instance to share the files.

D. Store the server-side code on Amazon FSx for Windows File Server. Mount the FSx for Windows File Server volume on each EC2 instance to share the files.

E. Store the server-side code on a General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on each EC2 instance to share the files.

Answer: A,D

Explanation:

A because Elasticache, despite being ideal for leaderboards per Amazon, doesn't cache at edge locations.

D because FSx has higher performance for low latency needs.

https://www.techtarget.com/searchaws/tip/Amazon-FSx-vs-EFS-Compare-the-AWS-file- services "FSx is built for high performance and submillisecond latency using solid-state drive storage volumes. This design enables users to select storage capacity and latency independently. Thus, even a subterabyte file system can have 256 Mbps or higher throughput and support volumes up to 64 TB."

Amazon S3 is an object storage service that can store static files such as images, videos, documents, etc. Amazon EFS is a file storage service that can store files in a hierarchical structure and supports NFS protocol. Amazon FSx for Windows File Server is a file storage service that can store files in a hierarchical structure and supports SMB protocol. Amazon EBS is a block storage service that can store data in fixed-size blocks and attach to EC2 instances.

Based on these definitions, the combination of steps that should be taken to meet the requirements are:

* A. Store the static files on Amazon S3. Use Amazon CloudFront to cache objects at the edge. D. Store the server-side code on Amazon FSx for Windows File Server. Mount the FSx for Windows File Server volume on each EC2 instance to share the files.

208. - (Topic 3)

A company deploys an appliation on five Amazon EC2 instances. An Applicatin Load Balancer (ALB) distributes traffic to the instances by using a target group. The average CPU usage on each of the insatances is below 10% most of the time. With occasional surges to 65%.

A solution architect needs to implement a solution to automate the scalability of the application. The solution must optimize the cost of the architecture and must ensure that the application has enough CPU resources when surges occur.

Which solution will meet these requirements?

A. Create an Amazon CloudWatch alarm that enters the ALARM state when the CPUUtilization metric is less than 20%. Create an AWS Lambda function that the CloudWatch alarm invokes to terminate one of the EC2 instances in the ALB target group.

B. Create an EC2 Auto Scaling. Select the exisiting ALB as the load balancer and the existing target group as the target group. Set a target tracking scaling policy that is based on the ASGAverageCPUUtilization

metric. Set the minimum instances to 2, the desired capacity to 3, the desired capacity to 3, the maximum instances to 6, and the target value to 50%. And the EC2 instances to the Auto Scaling group.

C. Create an EC2 Auto Scaling. Select the exisiting ALB as the load balancer and the existing target group. Set the minimum instances to 2, the desired capacity to 3, and the maximum instances to 6 Add the EC2 instances to the Scaling group.

D. Create two Amazon CloudWatch alarms. Configure the first CloudWatch alarm to enter the ALARM satet when the average CPUTUilization metric is below 20%. Configure the seconnd CloudWatch alarm to enter the ALARM state when the average CPUUtilization metric is aboove 50%. Configure the alarms to publish to an Amazon Simple Notification Service (Amazon SNS) topic to send an email message. After receiving the message, log in to decrease or increase the number of EC2 instances that are running

Answer: B

Explanation:

• An Auto Scaling group will automatically scale the EC2 instances to match changes in demand. This optimizes cost by only running as many instances as needed.

• A target tracking scaling policy monitors the ASGAverageCPUUtilization metric and scales to keep the average CPU around the 50% target value. This ensures there are enough resources during CPU surges.

• The ALB and target group are reused, so the application architecture does not change. The Auto Scaling group is associated to the existing load balancer setup.

• A minimum of 2 and maximum of 6 instances provides the ability to scale between 3 and 6 instances as needed based on demand.

• Costs are optimized by starting with only 3 instances (the desired capacity) and scaling up as needed. When CPU usage drops, instances are terminated to match the desired capacity.

209. - (Topic 3)

A company wants to use high performance computing (HPC) infrastructure on AWS for financial risk modeling. The company's HPC workloads run on Linux. Each HPC workflow runs on hundreds of Amazon EC2 Spot Instances, is shorl-lived, and generates thousands of output files that are ultimately stored in persistent storage for analytics and long-term future use.

The company seeks a cloud storage solution that permits the copying of on-premises data to long-term persistent storage to make data available for processing by all EC2 instances. The solution should also be

a high performance file system that is integrated with persistent storage to read and write datasets and output files.

Which combination of AWS services meets these requirements?

A. Amazon FSx for Lustre integrated with Amazon S3

B. Amazon FSx for Windows File Server integrated with Amazon S3

C. Amazon S3 Glacier integrated with Amazon Elastic Block Store (Amazon EBS)

D. Amazon S3 bucket with a VPC endpoint integrated with an Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume

Answer: A

Explanation:

https://aws.amazon.com/fsx/lustre/

Amazon FSx for Lustre is a fully managed service that provides cost-effective, high- performance, scalable storage for compute workloads. Many workloads such as machine learning, high performance computing (HPC), video rendering, and financial simulations depend on compute instances accessing the same set of data through high-performance shared storage.

210. - (Topic 3)

A company hosts a marketing website in an on-premises data center. The website consists of static documents and runs on a single server. An administrator updates the website content infrequently and uses an SFTP client to upload new documents.

The company decides to host its website on AWS and to use Amazon CloudFront. The company's solutions architect creates a CloudFront distribution. The solutions architect

must design the most cost-effective and resilient architecture for website hosting to serve as the CloudFront origin.

Which solution will meet these requirements?

A. Create a virtual server by using Amazon Lightsail. Configure the web server in the Lightsail instance. Upload website content by using an SFTP client.

B. Create an AWS Auto Scaling group for Amazon EC2 instances. Use an Application Load Balancer. Upload website content by using an SFTP client.

C. Create a private Amazon S3 bucket. Use an S3 bucket policy to allow access from a CloudFront origin

access identity (OAI). Upload website content by using theAWSCLI.

D. Create a public Amazon S3 bucket. Configure AWS Transfer for SFTP. Configure the S3 bucket for website hosting. Upload website content by using the SFTP client.

Answer: C

Explanation: https://docs.aws.amazon.com/cli/latest/reference/transfer/describe- server.html

211. - (Topic 3)

A company wants to migrate a Windows-based application from on premises to the AWS Cloud. The application has three tiers, a business tier, and a database tier with Microsoft SQL Server. The company wants to use specific features of SQL Server such as native backups and Data Quality Services. The company also needs to share files for process between the tiers.

How should a solution architect design the architecture to meet these requirements?

A. Host all three on Amazon instances. Use Mmazon FSx File Gateway for file sharing between tiers.

B. Host all three on Amazon EC2 instances. Use Amazon FSx for Windows file sharing between the tiers.

C. Host the application tier and the business tier on Amazon EC2 instances. Host the database tier on Amazon RDS. Use Amazon Elastic File system (Amazon EFS) for file sharing between the tiers.

D. Host the application tier and the business tier on Amazon EC2 instances. Host the database tier on Amazon RDS. Use a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume for file sharing between the tiers.

Answer: B

Explanation:

This solution will allow the company to host all three tiers on Amazon EC2 instances while using Amazon FSx for Windows File Server to provide Windows-based file sharing between the tiers. This will allow the company to use specific features of SQL Server, such as native backups and Data Quality Services, while sharing files for processing between the tiers.

212. - (Topic 3)

A company has hundreds of Amazon EC2 Linux-based instances in the AWS Cloud. Systems administrators have used shared SSH keys to manage the instances After a recent audit, the company's security team is mandating the removal of all shared keys. A solutions architect must design a solution that

provides secure access to the EC2 instances.

Which solution will meet this requirement with the LEAST amount of administrative overhead?

A. Use AWS Systems Manager Session Manager to connect to the EC2 instances.

B. Use AWS Security Token Service (AWS STS) to generate one-time SSH keys on demand.

C. Allow shared SSH access to a set of bastion instances. Configure all other instances to allow only SSH access from the bastion instances

D. Use an Amazon Cognito custom authorizer to authenticate users. Invoke an AWS Lambda function to generate a temporary SSH key.

Answer: A

Explanation:

Session Manager is a fully managed AWS Systems Manager capability. With Session Manager, you can manage your Amazon Elastic Compute Cloud (Amazon EC2) instances, edge devices, on-premises servers, and virtual machines (VMs). You can use either an interactive one-click browser-based shell or the AWS Command Line Interface (AWS CLI). Session Manager provides secure and auditable node management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys. Session Manager also allows you to comply with corporate policies that require controlled access to managed nodes, strict security practices, and fully auditable logs with node access details, while providing end users with simple one-click cross-platform access to your managed nodes.

https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html

213. - (Topic 3)

A company is building a new web-based customer relationship management application. The application will use several Amazon EC2 instances that are backed by Amazon Elastic Block Store (Amazon EBS) volumes behind an Application Load Balancer (ALB). The application will also use an Amazon Aurora database. All data for the application must be encrypted at rest and in transit.

Which solution will meet these requirements?

A. Use AWS Key Management Service (AWS KMS) certificates on the ALB to encrypt data in transit. Use AWS Certificate Manager (ACM) to encrypt the EBS volumes and Aurora database storage at rest.

B. Use the AWS root account to log in to the AWS Management Console. Upload the company's encryption certificates. While in the root account, select the option to turn on encryption for all data at rest and in transit

for the account.

C. Use a AWS Key Management Service (AWS KMS) to encrypt the EBS volumes and Aurora database storage at rest. Attach an AWS Certificate Manager (ACM) certificate to the ALB to encrypt data in transit.

D. Use BitLocker to encrypt all data at rest. Import the company's TLS certificate keys to AWS key Management Service (AWS KMS). Attach the KMS keys to the ALB to encrypt data in transit.

Answer: C

Explanation:

This option is the most efficient because it uses AWS Key Management Service (AWS KMS), which is a service that makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and with your applications running on AWS1. It also uses AWS KMS to encrypt the EBS volumes and Aurora database storage at rest, which provides data protection by encrypting your data with encryption keys that you manage23. It also uses AWS Certificate Manager (ACM), which is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources. It also attaches an ACM certificate to the ALB to encrypt data in transit, which provides data protection by enabling SSL/TLS encryption for connections between clients and the load balancer. This solution meets the requirement of encrypting all data for the application at rest and in transit. Option A is less efficient because it uses AWS KMS certificates on the ALB to encrypt data in transit, which is not possible as AWS KMS does not provide certificates but only keys. It also uses AWS Certificate Manager (ACM) to encrypt the EBS volumes and Aurora database storage at rest, which is not possible as ACM does not provide encryption but only certificates. Option B is less efficient because it uses the AWS root account to log in to the AWS Management Console, which is not recommended as it has unrestricted access to all resources in your account. It also uploads the company's encryption certificates, which is not necessary as ACM can provide certificates for free. It also selects the option to turn on encryption for all data at rest and in transit for the account, which is not possible as encryption settings are specific to each service and resource. Option D is less efficient because it uses BitLocker to encrypt all data at rest, which is a Windows feature that provides encryption for volumes on Windows servers. However, this does not provide encryption for Aurora database storage at rest, as Aurora runs on Linux servers. It also imports the company's TLS certificate keys to AWS KMS, which is not necessary as ACM can provide certificates for free. It also attaches the KMS keys to the ALB to encrypt data in transit, which is not possible as ALB

requires certificates and not keys.

214. - (Topic 3)

A telemarketing company is designing its customer call center functionality on AWS. The company needs a solution that provides multiples speaker recognition and generates transcript files The company wants to query the transcript files to analyze the business patterns The transcript files must be stored for 7 years for auditing piloses.

Which solution will meet these requirements?

A. Use Amazon Recognition for multiple speaker recognition. Store the transcript files in Amazon S3 Use machine teaming models for transcript file analysis

B. Use Amazon Transcribe for multiple speaker recognition. Use Amazon Athena for transcript file analysts

C. Use Amazon Translate lor multiple speaker recognition. Store the transcript files in Amazon Redshift Use SQL queues lor transcript file analysis

D. Use Amazon Recognition for multiple speaker recognition. Store the transcript files in Amazon S3 Use Amazon Textract for transcript file analysis

Answer: B

Explanation:

Amazon Transcribe now supports speaker labeling for streaming transcription. Amazon Transcribe is an automatic speech recognition (ASR) service that makes it easy for you to convert speech-to-text. In live audio transcription, each stream of audio may contain multiple speakers. Now you can conveniently turn on the ability to label speakers, thus helping to identify who is saying what in the output transcript.

https://aws.amazon.com/about-aws/whats-new/2020/08/amazon-transcribe-supports-speaker-labeling-streaming-transcription/

215. - (Topic 3)

A company's facility has badge readers at every entrance throughout the building. When badges are scanned, the readers send a message over HTTPS to indicate who attempted to access that particular entrance.

A solutions architect must design a system to process these messages from the sensors. The solution must be highly available, and the results must be made available for the company's security team to analyze.

Which system architecture should the solutions architect recommend?

A. Launch an Amazon EC2 instance to serve as the HTTPS endpoint and to process the messages Configure the EC2 instance to save the results to an Amazon S3 bucket.

B. Create an HTTPS endpoint in Amazon API Gateway. Configure the API Gateway endpoint to invoke an AWS Lambda function to process the messages and save the results to an Amazon DynamoDB table.

C. Use Amazon Route 53 to direct incoming sensor messages to an AWS Lambda function. Configure the Lambda function to process the messages and save the results to an Amazon DynamoDB table.

D. Create a gateway VPC endpoint for Amazon S3. Configure a Site-to-Site VPN connection from the facility network to the VPC so that sensor data can be written directly to an S3 bucket by way of the VPC endpoint.

Answer: B

Explanation:

Deploy Amazon API Gateway as an HTTPS endpoint and AWS Lambda to process and save the messages to an Amazon DynamoDB table. This option provides a highly available and scalable solution that can easily handle large amounts of data. It also integrates with other AWS services, making it easier to analyze and visualize the data for the security team.

216. - (Topic 3)

A solutions architect is designing the architecture for a software demonstration environment The environment will run on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB) The system will experience significant increases in traffic during working hours but Is not required to operate on weekends.

Which combination of actions should the solutions architect take to ensure that the system can scale to meet demand? (Select TWO)

A. Use AWS Auto Scaling to adjust the ALB capacity based on request rate

B. Use AWS Auto Scaling to scale the capacity of the VPC internet gateway

C. Launch the EC2 instances in multiple AWS Regions to distribute the load across Regions

D. Use a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization

E. Use scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends Revert to the default values at the start of the week

Answer: D,E

Explanation: https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html#target-tracking-choose-metrics

A target tracking scaling policy is a type of dynamic scaling policy that adjusts the capacity of an Auto Scaling group based on a specified metric and a target value1. A target tracking scaling policy can automatically scale out or scale in the Auto Scaling group to keep the actual metric value at or near the target value1. A target tracking scaling policy is suitable for scenarios where the load on the application changes frequently and unpredictably, such as during working hours2.

To meet the requirements of the scenario, the solutions architect should use a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization. Instance CPU utilization is a common metric that reflects the demand on the

application1. The solutions architect should specify a target value that represents the ideal average CPU utilization level for the application, such as 50 percent1. Then, the Auto Scaling group will scale out or scale in to maintain that level of CPU utilization.

Scheduled scaling is a type of scaling policy that performs scaling actions based on a date and time3. Scheduled scaling is suitable for scenarios where the load on the application changes periodically and predictably, such as on weekends2.

To meet the requirements of the scenario, the solutions architect should also use scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends. This way, the Auto Scaling group will terminate all instances on weekends when they are not required to operate. The solutions architect should also revert to the default values at the start of the week, so that the Auto Scaling group can resume normal operation.

217. - (Topic 3)

A company provides an online service for posting video content and transcoding it for use by any mobile platform. The application architecture uses Amazon Elastic File System (Amazon EFS) Standard to collect and store the videos so that multiple Amazon EC2 Linux instances can access the video content for processing As the popularity of the service has grown over time, the storage costs have become too expensive.

Which storage solution is MOST cost-effective?

A. Use AWS Storage Gateway for files to store and process the video content

B. Use AWS Storage Gateway for volumes to store and process the video content

C. Use Amazon EFS for storing the video content Once processing is complete transfer the files to Amazon Elastic Block Store (Amazon EBS)

D. Use Amazon S3 for storing the video content Move the files temporarily over to an Amazon Elastic Block Store (Amazon EBS) volume attached to the server for processing

Answer: D

Explanation: • Amazon S3 for large-scale, durable, and inexpensive storage of the video content. S3 storage costs are significantly lower than EFS. • Amazon EBS only temporarily during processing. By mounting an EBS volume only when a video needs to be processed, and unmounting it after, the time the content spends on the higher-cost EBS storage is minimized. • The EBS volume can be sized to match the workload needs for active processing, keeping costs lower. The volume does not need to store the entire video library long-term.

218. - (Topic 3)

A company needs to migrate a legacy application from an on-premises data center to the AWS Cloud because of hardware capacity constraints. The application runs 24 hours a day. & days a week,. The application database storage continues to grow over time.

What should a solution architect do to meet these requirements MOST cost-affectivity?

A. Migrate the application layer to Amazon FC2 Spot Instances Migrate the data storage layer to Amazon S3.

B. Migrate the application layer to Amazon EC2 Reserved Instances Migrate the data storage layer to Amazon RDS On-Demand Instances.

C. Migrate the application layer to Amazon EC2 Reserved instances Migrate the data storage layer to Amazon Aurora Reserved Instances.

D. Migrate the application layer to Amazon EC2 On Demand Amazon Migrate the data storage layer to Amazon RDS Reserved instances.

Answer: C

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

219. - (Topic 3)

A company wants to run an in-memory database for a latency-sensitive application that runs on Amazon EC2 instances. The application processes more than 100,000 transactions each minute and requires high network throughput. A solutions architect needs to provide a cost-effective network design that minimizes data transfer charges.

Which solution meets these requirements?

A. Launch all EC2 instances in the same Availability Zone within the same AWS Region. Specify a placement group with cluster strategy when launching EC2 instances.

B. Launch all EC2 instances in different Availability Zones within the same AWS Region. Specify a placement group with partition strategy when launching EC2 instances.

C. Deploy an Auto Scaling group to launch EC2 instances in different Availability Zones based on a network utilization target.

D. Deploy an Auto Scaling group with a step scaling policy to launch EC2 instances in different Availability Zones.

Answer: A

Explanation:

• Launching instances within a single AZ and using a cluster placement group provides the lowest network latency and highest bandwidth between instances. This maximizes performance for an in-memory database and high-throughput application.

• Communications between instances in the same AZ and placement group are free, minimizing data transfer charges. Inter-AZ and public IP traffic can incur charges.

• A cluster placement group enables the instances to be placed close together within the AZ, allowing the high network throughput required. Partition groups span AZs, reducing bandwidth.

• Auto Scaling across zones could launch instances in AZs that increase data transfer charges. It may reduce network throughput, impacting performance.

220. - (Topic 3)

A company experienced a breach that affected several applications in its on-premises data center The attacker took advantage of vulnerabilities in the custom applications that were running on the servers The

company is now migrating its applications to run on Amazon EC2 instances The company wants to implement a solution that actively scans for vulnerabilities on the EC2 instances and sends a report that details the findings

Which solution will meet these requirements?

A. Deploy AWS Shield to scan the EC2 instances for vulnerabilities Create an AWS Lambda function to log any findings to AWS CloudTrail.

B. Deploy Amazon Macie and AWS Lambda functions to scan the EC2 instances for vulnerabilities Log any findings to AWS CloudTrail

C. Turn on Amazon GuardDuty Deploy the GuardDuty agents to the EC2 instances Configure an AWS Lambda function to automate the generation and distribution of reports that detail the findings

D. Turn on Amazon Inspector Deploy the Amazon Inspector agent to the EC2 instances Configure an AWS Lambda function to automate the generation and distribution of reports that detail the findings

Answer: D

Explanation: Amazon Inspector:

• Performs active vulnerability scans of EC2 instances. It looks for software vulnerabilities, unintended network accessibility, and other security issues.

• Requires installing an agent on EC2 instances to perform scans. The agent must be deployed to each instance.

• Provides scheduled scan reports detailing any findings of security risks or vulnerabilities. These reports can be used to patch or remediate issues.

• Is best suited for proactively detecting security weaknesses and misconfigurations in your AWS environment.

221. - (Topic 3)

A company is using Amazon Route 53 latency-based routing to route requests to its UDP- based application for users around the world. The application is hosted on redundant servers in the company's on-premises data centers in the United States. Asia, and Europe. The company's compliance requirements state that the application must be hosted on premises The company wants to improve the performance and availability of the application

What should a solutions architect do to meet these requirements?

A. A Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints Create an accelerator by using AWS Global Accelerator, and register the NLBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS

B. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator and register the ALBs as its endpoints Provide access to the application by using a CNAME that points to the accelerator DNS

C. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints In Route 53. create a latency-based record that points to the three NLBs. and use it as an origin for an Amazon CloudFront distribution Provide access to the application by using a CNAME that points to the CloudFront DNS

D. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints In Route 53 create a latency-based record that points to the three ALBs and use it as an origin for an Amazon CloudFront distribution- Provide access to the application by using a CNAME that points to the CloudFront DNS

Answer: A

Explanation:

https://aws.amazon.com/step-functions/#:~:text=AWS%20Step%20Functions%20is%20a,machine%20learning%20(ML)%20pipelines.

"A common use case for AWS Step Functions is a task that requires human intervention (for example, an approval process). Step Functions makes it easy to coordinate the components of distributed applications as a series of steps in a visual workflow called a state machine. You can quickly build and run state machines to execute the steps of your application in a reliable and scalable fashion.

(https://aws.amazon.com/pt/blogs/compute/implementing-serverless-manual-approval-steps-in-aws-step-functions-and-amazon-api-gateway/)"

222. - (Topic 3)

A rapidly growing global ecommerce company is hosting its web application on AWS. The web application includes static content and dynamic content. The website stores online transaction processing (OLTP) data in an Amazon RDS database. The website's users are experiencing slow page loads.

Which combination of actions should a solutions architect take to resolve this issue? (Select TWO.)

A. Configure an Amazon Redshift cluster.

B. Set up an Amazon CloudFront distribution

C. Host the dynamic web content in Amazon S3

D. Create a t wd replica tor the RDS DB instance.

E. Configure a Multi-AZ deployment for the RDS DB instance

Answer: B,D

Explanation:

To resolve the issue of slow page loads for a rapidly growing e-commerce website hosted on AWS, a solutions architect can take the following two actions:

* 1. Set up an Amazon CloudFront distribution

* 2. Create a read replica for the RDS DB instance

Configuring an Amazon Redshift cluster is not relevant to this issue since Redshift is a data warehousing service and is typically used for the analytical processing of large amounts of data.

Hosting the dynamic web content in Amazon S3 may not necessarily improve performance since S3 is an object storage service, not a web application server. While S3 can be used to host static web content, it may not be suitable for hosting dynamic web content since S3 doesn't support server-side scripting or processing.

Configuring a Multi-AZ deployment for the RDS DB instance will improve high availability but may not necessarily improve performance.

223. - (Topic 3)

An Amazon EC2 instance is located in a private subnet in a new VPC. This subnet does not have outbound internet access, but the EC2 instance needs the ability to download monthly security updates from an outside vendor.

What should a solutions architect do to meet these requirements?

A. Create an internet gateway, and attach it to the VPC. Configure the private subnet route table to use the internet gateway as the default route.

B. Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.

C. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure

the private subnet route table to use the NAT instance as the default route.

D. Create an internet gateway, and attach it to the VPC. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the internet gateway as the default route.

Answer: B

Explanation: This approach will allow the EC2 instance to access the internet and download the monthly security updates while still being located in a private subnet. By creating a NAT gateway and placing it in a public subnet, it will allow the instances in the private subnet to access the internet through the NAT gateway. And then, configure the private subnet route table to use the NAT gateway as the default route. This will ensure that all outbound traffic is directed through the NAT gateway, allowing the EC2 instance to access the internet while still maintaining the security of the private subnet.

224. - (Topic 3)

A developer has an application that uses an AWS Lambda function to upload files to Amazon S3 and needs the required permissions to perform the task The developer already has an IAM user with valid IAM credentials required for Amazon S3

What should a solutions architect do to grant the permissions?

A. Add required IAM permissions in the resource policy of the Lambda function

B. Create a signed request using the existing IAM credentials n the Lambda function

C. Create a new IAM user and use the existing IAM credentials in the Lambda function.

D. Create an IAM execution role with the required permissions and attach the IAM rote to the Lambda function

Answer: D

Explanation: To grant the necessary permissions to an AWS Lambda function to upload files to Amazon S3, a solutions architect should create an IAM execution role with the required permissions and attach the IAM role to the Lambda function. This approach follows the principle of least privilege and ensures that the Lambda function can only access the resources it needs to perform its specific task.

225. - (Topic 3)

A company has a multi-tier application deployed on several Amazon EC2 instances in an Auto Scaling

group. An Amazon RDS for Oracle instance is the application's data layer that uses Oracle-specific PL/SQL functions. Traffic to the application has been steadily increasing. This is causing the EC2 instances to become overloaded and the RDS instance to run out of storage. The Auto Scaling group does not have any scaling metrics and defines the minimum healthy instance count only. The company predicts that traffic will continue to increase at a steady but unpredictable rate before levelling off.

What should a solutions architect do to ensure the system can automatically scale for the increased traffic? (Select TWO.)

A. Configure storage Auto Scaling on the RDS for Oracle Instance.

B. Migrate the database to Amazon Aurora to use Auto Scaling storage.

C. Configure an alarm on the RDS for Oracle Instance for low free storage space

D. Configure the Auto Scaling group to use the average CPU as the scaling metric

E. Configure the Auto Scaling group to use the average free memory as the seeing metric

Answer: A,D

Explanation:

Auto scaling storage RDS will ease storage issues and migrating Oracle Pl/Sql to Aurora is cumbersome. Also Aurora has auto storage scaling by default.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIOPS.StorageTypes.html#USER_PIOPS.Autoscaling

226. - (Topic 3)

A company has an application thai runs on several Amazon EC2 instances Each EC2 instance has multiple Amazon Elastic Block Store (Amazon EBS) data volumes attached to it The application's EC2 instance configuration and data need to be backed up nightly The application also needs to be recoverable in a different AWS Region

Which solution will meet these requirements in the MOST operationally efficient way?

A. Write an AWS Lambda function that schedules nightly snapshots of the application's EBS volumes and copies the snapshots to a different Region

B. Create a backup plan by using AWS Backup to perform nightly backups. Copy the backups to another Region Add the application's EC2 instances as resources

C. Create a backup plan by using AWS Backup to perform nightly backups Copy the backups to another

Region Add the application's EBS volumes as resources

D. Write an AWS Lambda function that schedules nightly snapshots of the application's EBS volumes and copies the snapshots to a different Availability Zone

Answer: B

Explanation: The most operationally efficient solution to meet these requirements would be to create a backup plan by using AWS Backup to perform nightly backups and copying the backups to another Region. Adding the application's EBS volumes as resources will ensure that the application's EC2 instance configuration and data are backed up, and copying the backups to another Region will ensure that the application is recoverable in a different AWS Region.

227. - (Topic 3)

A company is building a new dynamic ordering website. The company wants to minimize server maintenance and patching. The website must be highly available and must scale read and write capacity as quickly as possible to meet changes in user demand.

Which solution will meet these requirements?

A. Host static content in Amazon S3 Host dynamic content by using Amazon API Gateway and AWS Lambda Use Amazon DynamoDB with on-demand capacity for the database Configure Amazon CloudFront to deliver the website content

B. Host static content in Amazon S3 Host dynamic content by using Amazon API Gateway and AWS Lambda Use Amazon Aurora with Aurora Auto Scaling for the database Configure Amazon CloudFront to deliver the website content

C. Host al the website content on Amazon EC2 instances Create an Auto Scaling group to scale the EC2 Instances Use an Application Load Balancer to distribute traffic Use Amazon DynamoDB with provisioned write capacity for the database

D. Host at the website content on Amazon EC2 instances Create an Auto Scaling group to scale the EC2 instances Use an Application Load Balancer to distribute traffic Use Amazon Aurora with Aurora Auto Scaling for the database

Answer: A

Explanation:

Key phrase in the Question is must scale read and write capacity. Aurora is only for Read. Amazon

DynamoDB has two read/write capacity modes for processing reads and writes on your tables: On-demand Provisioned (default, free-tier eligible)

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html

228. - (Topic 3)

A company is experiencing sudden increases in demand. The company needs to provision large Amazon EC2 instances from an Amazon Machine image (AMI) The instances will run m an Auto Scaling group. The company needs a solution that provides minimum initialization latency to meet the demand.

Which solution meets these requirements?

A. Use the aws ec2 register-image command to create an AMI from a snapshot Use AWS Step Functions to replace the AMI in the Auto Scaling group

B. Enable Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot Provision an AMI by using the snapshot Replace the AMI m the Auto Scaling group with the new AMI

C. Enable AMI creation and define lifecycle rules in Amazon Data Lifecycle Manager (Amazon DLM) Create an AWS Lambda function that modifies the AMI in the Auto Scaling group

D. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke AWS Backup lifecycle policies that provision AMIs Configure Auto Scaling group capacity limits as an event source in EventBridge

Answer: B

Explanation:

Enabling Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot allows you to quickly create a new Amazon Machine Image (AMI) from a snapshot, which can help reduce the initialization latency when provisioning new instances. Once the AMI is provisioned, you can replace the AMI in the Auto Scaling group with the new AMI. This will ensure that new instances are launched from the updated AMI and are able to meet the increased demand quickly.

229. - (Topic 3)

A company is hosting a web application from an Amazon S3 bucket. The application uses Amazon Cognito as an identity provider lo authenticate users and return a JSON Web Token (JWT) that provides access to protected resources that am restored in another S3 bucket.

Upon deployment of the application, users report errors and are unable to access the protected content. A solutions architect must resolve this issue by providing proper permissions so that users can access the protected content.

Which solution meets these requirements?

A. Update the Amazon Cognito identity pool to assume the proper IAM role for access to the protected consent.

B. Update the S3 ACL to allow the application to access the protected content

C. Redeploy the application to Amazon 33 to prevent eventually consistent reads m the S3 bucket from affecting the ability of users to access the protected content.

D. Update the Amazon Cognito pool to use custom attribute mappings within tie Identity pool and grant users the proper permissions to access the protected content

Answer: A

Explanation: Amazon Cognito identity pools assign your authenticated users a set of temporary, limited-privilege credentials to access your AWS resources. The permissions for each user are controlled through IAM roles that you create.

https://docs.aws.amazon.com/cognito/latest/developerguide/role-based-access-control.html

230. - (Topic 3)

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

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

A. Migrate the file share to Amazon RDS

B. Migrate the file share to AWS Storage Gateway

C. Migrate the file share to Amazon FSx for Windows File Server

D. Migrate the file share to Amazon Elastic File System (Amazon EFS)

Answer: C

Explanation: This answer is correct because it provides a resilient and durable replacement for the

on-premises file share that is compatible with Windows IIS web servers. Amazon FSx for Windows File Server is a fully managed service that provides shared file storage built on Windows Server. It supports the SMB protocol and integrates with Microsoft Active Directory, which enables seamless access and authentication for Windows-based applications. Amazon FSx for Windows File Server also offers the following benefits:

- Resilience: Amazon FSx for Windows File Server can be deployed in multiple Availability Zones, which provides high availability and failover protection. It also supports automatic backups and restores, as well as self-healing features that detect and correct issues.
- Durability: Amazon FSx for Windows File Server replicates data within and across Availability Zones, and stores data on highly durable storage devices. It also supports encryption at rest and in transit, as well as file access auditing and data deduplication.
- Performance: Amazon FSx for Windows File Server delivers consistent sub-millisecond latencies and high throughput for file operations. It also supports SSD storage, native Windows features such as Distributed File System (DFS) Namespaces and Replication, and user-driven performance scaling.

References:

- Amazon FSx for Windows File Server
- Using Microsoft Windows file shares

231. - (Topic 3)

A solution architect needs to assign a new microsoft for a company's application. Clients must be able to call an HTTPS endpoint to reach the micoservice. The microservice also must use AWS identity and Access Management (IAM) to authentication calls. The soltions architect will write the logic for this microservice by using a single AWS Lambda function that is written in Go 1.x.

Which solution will deploy the function in the in the MOST operationally efficient way?

A. Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API.

B. Create a Lambda function URL for the function. Specify AWS_IAM as the authentication type.

C. Create an Amazon CloudFront distribution. Deploy the function to Lambda@Edge. Integrate IAM

authentication logic into the Lambda@Edge function.

D. Create an Amazon CloudFront distribuion. Deploy the function to CloudFront Functions. Specify AWS_IAM as the authentication type.

Answer: A

Explanation: A. Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API. This option is the most operationally efficient as it allows you to use API Gateway to handle the HTTPS endpoint and also allows you to use IAM to authenticate the calls to the microservice. API Gateway also provides many additional features such as caching, throttling, and monitoring, which can be useful for a microservice.

232. - (Topic 3)

A company sells datasets to customers who do research in artificial intelligence and machine learning (AI/ML) The datasets are large, formatted files that are stored in an Amazon S3 bucket in the us-east-1 Region The company hosts a web application that the customers use to purchase access to a given dataset The web application is deployed on multiple Amazon EC2 instances behind an Application Load Balancer After a purchase is made customers receive an S3 signed URL that allows access to the files.

The customers are distributed across North America and Europe The company wants to reduce the cost that is associated with data transfers and wants to maintain or improve performance.

What should a solutions architect do to meet these requirements?

A. Configure S3 Transfer Acceleration on the existing S3 bucket Direct customer requests to the S3 Transfer Acceleration endpoint Continue to use S3 signed URLs for access control

B. Deploy an Amazon CloudFront distribution with the existing S3 bucket as the origin Direct customer requests to the CloudFront URL Switch to CloudFront signed URLs for access control

C. Set up a second S3 bucket in the eu-central-1 Region with S3 Cross-Region Replication between the buckets Direct customer requests to the closest Region Continue to use S3 signed URLs for access control

D. Modify the web application to enable streaming of the datasets to end users. Configure the web application to read the data from the existing S3 bucket Implement access control directly in the application

Answer: B

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

233. - (Topic 3)

A transaction processing company has weekly scripted batch jobs that run on Amazon EC2 instances. The EC2 instances are in an Auto Scaling group. The number of transactions can vary but the beseline CPU utilization that is noted on each run is at least 60%. The company needs to provision the capacity 30 minutes before the jobs run.

Currently engineering complete this task by manually modifying the Auto Scaling group parameters. The company does not have the resources to analyze the required capacity trends for the Auto Scaling group counts. The company needs an automated way to modify the Auto Scaling group's capacity.

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

A. Ceate a dynamic scalling policy for the Auto Scaling group. Configure the policy to scale based on the CPU utilization metric to 60%.

B. Create a scheduled scaling polcy for the Auto Scaling group. Set the appropriate desired capacity, minimum capacity, and maximum capacity. Set the recurrence to weekly. Set the start time to 30 minutes. Before the batch jobs run.

C. Create a predictive scaling policy for the Auto Scaling group. Configure the policy to scale based on forecast. Set the scaling metric to CPU utilization. Set the target value for the metric to 60%. In the Policy, set the instances to pre-launch 30 minutes before the jobs run.

D. Create an Amazon EventBridge event to invoke an AWS Lamda function when the CPU utilization metric value for the Auto Scaling group reaches 60%. Configure the Lambda function to increase the Auto Scaling group's desired capacity and maximum capacity by 20%.

Answer: C

Explanation:

This option is the most efficient because it uses a predictive scaling policy for the Auto Scaling group, which is a type of scaling policy that uses machine learning to predict capacity requirements based on historical data from CloudWatch1. It also configures the policy to scale based on forecast, which enables the Auto Scaling group to adjust its capacity in advance of traffic changes. It also sets the scaling metric to CPU utilization and the target value for the metric to 60%, which aligns with the baseline CPU utilization that is noted on each run. It also sets the instances to pre-launch 30 minutes before the jobs run, which ensures that enough capacity is provisioned before the weekly scripted batch jobs start. This solution meets the

requirement of provisioning the capacity 30 minutes before the jobs run with the least operational overhead. Option A is less efficient because it uses a dynamic scaling policy for the Auto Scaling group, which is a type of scaling policy that adjusts your Auto Scaling group's capacity in response to changing demand2. However, this does not provide a way to provision the capacity 30 minutes before the jobs run, as it only reacts to changing traffic. Option B is less efficient because it uses a scheduled scaling policy for the Auto Scaling group, which is a type of scaling policy that lets you scale your Auto Scaling group based on a schedule that you create3. However, this does not provide a way to scale based on forecast or CPU utilization, as it only scales based on predefined metrics and policies. Option D is less efficient because it uses an Amazon EventBridge event to invoke an AWS Lambda function when the CPU utilization metric value for the Auto Scaling group reaches 60%, which is a way to trigger serverless functions based on events. However, this does not provide a way to provision the capacity 30 minutes before the jobs run, as it only reacts to changing traffic.

234. - (Topic 3)

A company runs a public three-Tier web application in a VPC The application runs on Amazon EC2 instances across multiple Availability Zones. The EC2 instances that run in private subnets need to communicate with a license server over the internet The company needs a managed solution that minimizes operational maintenance

Which solution meets these requirements"

A. Provision a NAT instance in a public subnet Modify each private subnets route table with a default route that points to the NAT instance

B. Provision a NAT instance in a private subnet Modify each private subnet's route table with a default route that points to the NAT instance

C. Provision a NAT gateway in a public subnet Modify each private subnet's route table with a default route that points to the NAT gateway

D. Provision a NAT gateway in a private subnet Modify each private subnet's route table with a default route that points to the NAT gateway

Answer: C

Explanation:

A NAT gateway is a type of network address translation (NAT) device that enables instances in a private

subnet to connect to the internet or other AWS services, but prevents the internet from initiating connections with those instances1. A NAT gateway is a managed service that requires minimal operational maintenance and can handle up to 45 Gbps of bursty traffic1. A NAT gateway is suitable for scenarios where EC2 instances in private subnets need to communicate with a license server over the internet, such as the three-tier web application in the scenario1.

To meet the requirements of the scenario, the solutions architect should provision a NAT gateway in a public subnet. The solutions architect should also modify each private subnet's route table with a default route that points to the NAT gateway1. This way, the EC2 instances that run in private subnets can access the license server over the internet through the NAT gateway.

235. - (Topic 3)

A company hosts its application on AWS The company uses Amazon Cognito to manage users When users log in to the application the application fetches required data from Amazon DynamoDB by using a REST API that is hosted in Amazon API Gateway. The company wants an AWS managed solution that will control access to the REST API to reduce development efforts

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

A. Configure an AWS Lambda function to be an authorize! in API Gateway to validate which user made the request

B. For each user, create and assign an API key that must be sent with each request Validate the key by using an AWS Lambda function

C. Send the user's email address in the header with every request Invoke an AWS Lambda function to validate that the user with that email address has proper access

D. Configure an Amazon Cognito user pool authorizer in API Gateway to allow Amazon Cognito to validate each request

Answer: D

Explanation:

https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html

To control access to the REST API and reduce development efforts, the company can use an Amazon Cognito user pool authorizer in API Gateway. This will allow Amazon Cognito to validate each request and ensure that only authenticated users can access the API. This

solution has the LEAST operational overhead, as it does not require the company to develop and maintain any additional infrastructure or code.

236. - (Topic 3)

A company wants to deploy a new public web application on AWS The application includes a web server tier that uses Amazon EC2 instances The application also includes a database tier that uses an Amazon RDS for MySQL DB instance

The application must be secure and accessible for global customers that have dynamic IP addresses

How should a solutions architect configure the security groups to meet these requirements'?

A. Configure the security group tor the web servers lo allow inbound traffic on port 443 from 0.0.0. 0/0) Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers

B. Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers Configure the security group for the DB instance lo allow inbound traffic on port 3306 from the security group of the web servers

C. Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers Configure the security group for the DB instance to allow inbound traffic on port 3306 from the IP addresses of the customers

D. Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0.0 Configure the security group for the DB instance to allow inbound traffic on port 3306 from 0.0.0.0/0)

Answer: A

Explanation:

⇨ Restricting inbound access to the web servers to only port 443, which is used for HTTPS traffic, and allowing access from any IP address (0.0.0.0/0), since the application is public and accessible for global customers.

⇨ Restricting inbound access to the DB instance to only port 3306, which is used for MySQL traffic, and allowing access only from the security group of the web servers, which creates a secure connection between the two tiers and prevents unauthorized access to the database.

⇨ Restricting outbound access to the minimum required for both tiers, which is not specified in the question but can be assumed to be similar to the inbound rules.

References:

- Security groups - Amazon Virtual Private Cloud
- 5 Best Practices for AWS Security Groups - DZone

237. - (Topic 3)

An IAM user made several configuration changes to AWS resources m their company's account during a production deployment last week. A solutions architect learned that a couple of security group rules are not configured as desired. The solutions architect wants to confirm which IAM user was responsible for making changes.

Which service should the solutions architect use to find the desired information?

A. Amazon GuardDuty

B. Amazon Inspector

C. AWS CloudTrail

D. AWS Config

Answer: C

Explanation: The best option is to use AWS CloudTrail to find the desired information. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of AWS account activities. CloudTrail can be used to log all changes made to resources in an AWS account, including changes made by IAM users, EC2 instances, AWS management console, and other AWS services. By using CloudTrail, the solutions architect can identify the IAM user who made the configuration changes to the security group rules.

238. - (Topic 3)

A company selves a dynamic website from a flee! of Amazon EC2 instances behind an Application Load Balancer (ALB) The website needs to support multiple languages to serve customers around the world The website's architecture is running in the us-west-1 Region and is exhibiting high request latency tor users that are located in other parts of the world

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

What should a solutions architect do to meet these requirements?

A. Replace the existing architecture with a website that is served from an Amazon S3 bucket Configure an Amazon CloudFront distribution with the S3 bucket as the origin Set the cache behavior settings to cache based on the Accept-Language request header

B. Configure an Amazon CloudFront distribution with the ALB as the origin Set the cache behavior settings to cache based on the Accept-Language request header

C. Create an Amazon API Gateway API that is integrated with the ALB Configure the API to use the HTTP integration type Set up an API Gateway stage to enable the API cache based on the Accept-Language request header

D. Launch an EC2 instance in each additional Region and configure NGINX to act as a cache server for that Region Put all the EC2 instances and the ALB behind an Amazon Route 53 record set with a geolocation routing policy

Answer: B

Explanation: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/header-caching.html Configuring caching based on the language of the viewer: If you want CloudFront to cache different versions of your objects based on the language specified in the request, configure CloudFront to forward the Accept-Language header to your origin.

239. - (Topic 3)

A company is using AWS to design a web application that will process insurance quotes Users will request quotes from the application Quotes must be separated by quote type, must be responded to within 24 hours, and must not get lost The solution must maximize operational efficiency and must minimize maintenance. Which solution meets these requirements?

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

B. Create an AWS Lambda function and an Amazon Simple Notification Service (Amazon SNS) topic for each quote type Subscribe the Lambda function to its associated SNS topic Configure the application to publish requests tot quotes to the appropriate SNS topic

C. Create a single Amazon Simple Notification Service (Amazon SNS) topic Subscribe Amazon Simple Queue Service (Amazon SQS) queues to the SNS topic Configure SNS message filtering to publish

messages to the proper SQS queue based on the quote type Configure each backend application server to use its own SQS queue

D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon Elasucsearch Service (Amazon ES) cluster Configure the application to send messages to the proper delivery stream Configure each backend group of application servers to search for the messages from Amazon ES and process them accordingly

Answer: C

Explanation: https://aws.amazon.com/getting-started/hands-on/filter-messages-published- to-topics/

240. - (Topic 3)

A company is hosting a three-tier ecommerce application in the AWS Cloud. The company hosts the website on Amazon S3 and integrates the website with an API that handles sales requests. The company hosts the API on three Amazon EC2 instances behind an Application Load Balancer (ALB). The API consists of static and dynamic front-end content along with backend workers that process sales requests asynchronously.

The company is expecting a significant and sudden increase in the number of sales requests during events for the launch of new products

What should a solutions architect recommend to ensure that all the requests are processed successfully?

A. Add an Amazon CloudFront distribution for the dynamic content. Increase the number of EC2 instances to handle the increase in traffic.

B. Add an Amazon CloudFront distribution for the static content. Place the EC2 instances in an Auto Scaling group to launch new instances based on network traffic.

C. Add an Amazon CloudFront distribution for the dynamic content. Add an Amazon ElastiCache instance in front of the ALB to reduce traffic for the API to handle.

D. Add an Amazon CloudFront distribution for the static content. Add an Amazon Simple Queue Service (Amazon SOS) queue to receive requests from the website for later processing by the EC2 instances.

Answer: B

Explanation:

This option is the most efficient because it uses Amazon CloudFront, which is a web service that speeds up distribution of your static and dynamic web content, such as .html,

.css, .js, and image files, to your users1. It also uses a CloudFront distribution for the static content, which reduces the load on the EC2 instances and improves the performance and availability of the website. It also uses an Auto Scaling group to launch new instances based on network traffic, which automatically adjusts the compute capacity of your EC2 instances based on load or a schedule2. This solution meets the requirement of ensuring that all the requests are processed successfully during events for the launch of new products. Option A is less efficient because it uses a CloudFront distribution for the dynamic content, which is not necessary as the dynamic content is already handled by the API on the EC2 instances. It also increases the number of EC2 instances to handle the increase in traffic, which could incur higher costs and complexity than using an Auto Scaling group. Option C is less efficient because it uses an Amazon ElastiCache instance in front of the ALB to reduce traffic for the API to handle, which is a way to provide a fully managed in-memory data store service that provides sub-millisecond latency for caching and data processing3. However, this could introduce additional complexity and latency, and does not scale automatically based on network traffic. Option D is less efficient because it uses an Amazon Simple Queue Service (Amazon SQS) queue to receive requests from the website for later processing by the EC2 instances, which is a way to send, store, and receive messages between software components at any volume. However, this does not provide a faster response time to the users as they have to wait for their requests to be processed by the EC2 instances.

241. - (Topic 3)

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

What should the solutions architect do to meet these requirements?

A. Increase the minimum capacity for the Auto Scaling group.

B. Increase the maximum capacity for the Auto Scaling group.

C. Configure scheduled scaling to scale up to the desired compute level.

D. Change the scaling policy to add more EC2 instances during each scaling operation.

Answer: C

Explanation: By configuring scheduled scaling, the solutions architect can set the Auto Scaling group to automatically scale up to the desired compute level at a specific time (IAM) when the batch job starts and then automatically scale down after the job is complete. This will allow the desired EC2 capacity to be reached quickly and also help in reducing the cost.

242. - (Topic 3)

A company has a custom application with embedded credentials that retrieves information from an Amazon RDS MySQL DB instance. Management says the application must be made more secure with the least amount of programming effort.

What should a solutions architect do to meet these requirements?

A. Use AWS Key Management Service (AWS KMS) customer master keys (CMKs) to create keys. Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation.

B. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Create an AWS Lambda function that rotates the credentials in Secret Manager.

C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.

D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

Answer: C

Explanation:

https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/

243. - (Topic 3)

A company has a three-tier application on AWS that ingests sensor data from its users' devices The traffic

flows through a Network Load Balancer (NLB) then to Amazon EC2 instances for the web tier and finally to EC2 instances for the application tier The application tier makes calls to a database

What should a solutions architect do to improve the security of the data in transit?

A. Configure a TLS listener Deploy the server certrficate on the NLB

B. Configure AWS Shield Advanced Enable AWS WAF on the NLB

C. Change the load balancer to an Application Load Balancer (ALB) Enable AWS WAF on the ALB

D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances by using AWS Key Management Service (AWS KMS)

Answer: A

Explanation:

The best option to improve the security of the data in transit is to configure a TLS listener and deploy the server certificate on the NLB. This will ensure that the data is encrypted and secure as it travels through the network. Additionally, you could also configure AWS Shield Advanced and enable AWS WAF on the NLB to further protect the network from malicious attacks. Alternatively, you could also change the load balancer to an Application Load Balancer (ALB) and enable AWS WAF on the ALB. Finally, you could also encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances by using AWS Key Management Service (AWS KMS).

You must specify an SSL certificate for a TLS listener. The load balancer uses the certificate to terminate the connection and decrypt requests from clients before routing them to targets.

https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create- listener.html

244. - (Topic 3)

A company wants to restrict access to the content of one of its man web applications and to protect the content by using authorization techniques available on AWS. The company wants to implement a serverless architecture end an authentication solution for fewer tian 100 users. The solution needs to integrate with the main web application and serve web content globally. The solution must also scale as to company's user base grows while providing lowest login latency possible.

A. Use Amazon Cognito tor authentication. Use Lambda#Edge tor authorization Use Amazon CloudFront 10 serve the web application globally

B. Use AWS Directory Service for Microsoft Active Directory tor authentication Use AWS Lambda for

authorization Use an Application Load Balancer to serve the web application globally

C. Usa Amazon Cognito for authentication Use AWS Lambda tor authorization Use Amazon S3 Transfer Acceleration 10 serve the web application globally.

D. Use AWS Directory Service for Microsoft Active Directory for authentication Use Lambda@Edge for authorization Use AWS Elastic Beanstalk to serve the web application.

Answer: A

Explanation: https://aws.amazon.com/blogs/networking-and-content-delivery/adding-http-security-headers-using-lambdaedge-and-amazon-cloudfront/

Amazon CloudFront is a global content delivery network (CDN) service that can securely deliver web content, videos, and APIs at scale. It integrates with Cognito for authentication and with Lambda@Edge for authorization, making it an ideal choice for serving web content globally. Lambda@Edge is a service that lets you run AWS Lambda functions globally closer to users, providing lower latency and faster response times. It can also handle authorization logic at the edge to secure content in CloudFront. For this scenario, Lambda@Edge can provide authorization for the web application while leveraging the low- latency benefit of running at the edge.

245. - (Topic 3)

A company is deploying a two-tier web application in a VPC. The web tier is using an Amazon EC2 Auto Scaling group with public subnets that span multiple Availability Zones. The database tier consists of an Amazon RDS for MySQL DB instance in separate private subnets. The web tier requires access to the database to retrieve product information.

The web application is not working as intended. The web application reports that it cannot connect to the database. The database is confirmed to be up and running. All configurations for the network ACLs. security groups, and route tables are still in their default states.

What should a solutions architect recommend to fix the application?

A. Add an explicit rule to the private subnet's network ACL to allow traffic from the web tier's EC2 instances.

B. Add a route in the VPC route table to allow traffic between the web tier's EC2 instances and Ihe database tier.

C. Deploy the web tier's EC2 instances and the database tier's RDS instance into two separate VPCs. and configure VPC peering.

D. Add an inbound rule to the security group of the database tier's RDS instance to allow traffic from the web tier's security group.

Answer: D

Explanation:

This answer is correct because it allows the web tier to access the database tier by using security groups as a source, which is a recommended best practice for VPC connectivity. Security groups are stateful and can reference other security groups in the same VPC, which simplifies the configuration and maintenance of the firewall rules. By adding an inbound rule to the database tier's security group, the web tier's EC2 instances can connect to the RDS instance on port 3306, regardless of their IP addresses or subnets. References:

- Security groups - Amazon Virtual Private Cloud
- Best practices and reference architectures for VPC design

246. - (Topic 3)

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

A. Use AWS Snowball.

B. Use AWS DataSync.

C. Use a secure VPN connection.

D. Use Amazon S3 Transfer Acceleration.

Answer: A

Explanation: AWS Snowball is a secure data transport solution that accelerates moving large amounts of data into and out of the AWS cloud. It can move up to 80 TB of data at a time, and provides a network bandwidth of up to 50 Mbps, so it is well-suited for the task. Additionally, it is secure and easy to use, making it the ideal solution for this migration.

247. - (Topic 3)

A company wants to create an application to store employee data in a hierarchical structured relationship. The company needs a minimum-latency response to high-traffic queries for the employee data and must

protect any sensitive data. The company also need to receive monthly email messages if any financial information is present in the employee data.

Which combination of steps should a solutin architect take to meet these requirement? (Select TWO.)

A. Use Amazon Redshift to store the employee data in hierarchies. Unload the data to Amazon S3 every month.

B. Use Amazon DynamoDB to store the employee data in hierarchies Export the data to Amazon S3 every month.

C. Configure Amazon Macie for the AWS account Integrate Macie with Amazon EventBridge to send monthly events to AWS Lambda.

D. Use Amazon Athena to analyze the employee data in Amazon S3 integrate Athena with Amazon QuickSight to publish analysis dashboards and share the dashboards with users.

E. Configure Amazon Macie for the AWS account. integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon Simple Notification Service (Amazon SNS) subscription.

Answer: B,E

Explanation:

https://docs.aws.amazon.com/prescriptive-guidance/latest/dynamodb-hierarchical-data-model/introduction.html

248. - (Topic 3)

A company has a regional subscription-based streaming service that runs in a single AWS Region. The architecture consists of web servers and application servers on Amazon EC2 instances. The EC2 instances are in Auto Scaling groups behind Elastic Load Balancers. The architecture includes an Amazon Aurora database cluster that extends across multiple Availability Zones.

The company wants to expand globally and to ensure that its application has minimal downtime.

A. Extend the Auto Scaling groups for the web tier and the application tier to deploy instances in Availability Zones in a second Region. Use an Aurora global database to deploy the database in the primary Region and the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region.

B. Deploy the web tier and the application tier to a second Region. Add an Aurora PostgreSQL

cross-Region Aurara Replica in the second Region. Use Amazon Route 53 health checks with a failovers routing policy to the second Region, Promote the secondary to primary as needed.

C. Deploy the web tier and the applicatin tier to a second Region. Create an Aurora PostSQL database in the second Region. Use AWS Database Migration Service (AWS DMS) to replicate the primary database to the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region.

D. Deploy the web tier and the application tier to a second Region. Use an Amazon Aurora global database to deploy the database in the primary Region and the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region. Promote the secondary to primary as needed.

Answer: D

Explanation:

This option is the most efficient because it deploys the web tier and the application tier to a second Region, which provides high availability and redundancy for the application. It also uses an Amazon Aurora global database, which is a feature that allows a single Aurora database to span multiple AWS Regions1. It also deploys the database in the primary Region and the second Region, which provides low latency global reads and fast recovery from a Regional outage. It also uses Amazon Route 53 health checks with a failover routing policy to the second Region, which provides data protection by routing traffic to healthy endpoints in different Regions2. It also promotes the secondary to primary as needed, which provides data consistency by allowing write operations in one of the Regions at a time3. This solution meets the requirement of expanding globally and ensuring that its application has minimal downtime. Option A is less efficient because it extends the Auto Scaling groups for the web tier and the application tier to deploy instances in Availability Zones in a second Region, which could incur higher costs and complexity than deploying them separately. It also uses an Aurora global database to deploy the database in the primary Region and the second Region, which is correct. However, it does not use Amazon Route 53 health checks with a failover routing policy to the second Region, which could result in traffic being routed to unhealthy endpoints. Option B is less efficient because it deploys the web tier and the application tier to a second Region, which is correct. It also adds an Aurora PostgreSQL cross-Region Aurora Replica in the second Region, which provides read scalability across Regions. However, it does not use an Aurora global database, which provides faster replication and recovery than cross-Region replicas. It also uses Amazon Route 53 health checks with a failover routing policy to the second Region, which is correct. However, it

does not promote the secondary to primary as needed, which could result in data inconsistency or loss. Option C is less efficient because it deploys the web tier and the application tier to a second Region, which is correct. It also creates an Aurora PostgreSQL database in the second Region, which provides data redundancy across Regions. However, it does not use an Aurora global database or cross-Region replicas, which provide faster replication and recovery than creating separate databases. It also uses AWS Database Migration Service (AWS DMS) to replicate the primary database to the second Region, which provides data migration between different sources and targets. However, it does not use an Aurora global database or cross-Region replicas, which provide faster replication and recovery than using AWS DMS. It also uses Amazon Route 53 health checks with a failover routing policy to the second Region, which is correct.

249. - (Topic 3)

A rapidly growing ecommerce company is running its workloads in a single AWS Region. A solutions architect must create a disaster recovery (DR) strategy that includes a different AWS Region The company wants its database to be up to date in the DR Region with the least possible latency The remaining infrastructure in the DR Region needs to run at reduced capacity and must be able to scale up it necessary Which solution will meet these requirements with the LOWEST recovery time objective (RTO)?

A. Use an Amazon Aurora global database with a pilot light deployment

B. Use an Amazon Aurora global database with a warm standby deployment

C. Use an Amazon RDS Multi-AZ DB instance with a pilot light deployment

D. Use an Amazon RDS Multi-AZ DB instance with a warm standby deployment

Answer: B

Explanation:

https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html

250. - (Topic 3)

A company is deploying a new application on Amazon EC2 instances. The application writes data to Amazon Elastic Block Store (Amazon EBS) volumes. The company needs to ensure that all data that is written to the EBS volumes is encrypted at rest.

Which solution wil meet this requirement?

A. Create an IAM role that specifies EBS encryption. Attach the role to the EC2 instances.

B. Create the EBS volumes as encrypted volumes Attach the EBS volumes to the EC2 instances.

C. Create an EC2 instance tag that has a key of Encrypt and a value of True. Tag all instances that require encryption at the ESS level.

D. Create an AWS Key Management Service (AWS KMS) key policy that enforces EBS encryption in the account Ensure that the key policy is active.

Answer: B

Explanation:

The solution that will meet the requirement of ensuring that all data that is written to the EBS volumes is encrypted at rest is B. Create the EBS volumes as encrypted volumes and attach the encrypted EBS volumes to the EC2 instances. When you create an EBS volume, you can specify whether to encrypt the volume. If you choose to encrypt the volume, all data written to the volume is automatically encrypted at rest using AWS-managed keys. You can also use customer-managed keys (CMKs) stored in AWS KMS to encrypt and protect your EBS volumes. You can create encrypted EBS volumes and attach them to EC2 instances to ensure that all data written to the volumes is encrypted at rest.

251. - (Topic 3)

A company is running a publicly accessible serverless application that uses Amazon API Gateway and AWS Lambda. The application's traffic recently spiked due to fraudulent requests from botnets.

Which steps should a solutions architect take to block requests from unauthorized users? (Select TWO.)

A. Create a usage plan with an API key that is shared with genuine users only.

B. Integrate logic within the Lambda function to ignore the requests from fraudulent IP addresses.

C. Implement an AWS WAF rule to target malicious requests and trigger actions to filter them out.

D. Convert the existing public API to a private API. Update the DNS records to redirect users to the new API endpoint.

E. Create an IAM role for each user attempting to access the API. A user will assume the role when making the API call.

Answer: A,C

Explanation:

https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html#:~:text=Don%27t%20rely%20on%20API%20keys%20as%20your%20only%20means%20of%20authentication%20and%20authorization%20for%20your%20APIs

https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage- plans.html

252. - (Topic 3)

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

A. Use a VPC endpoint for DynamoDB.

B. Use a NAT gateway in a public subnet.

C. Use a NAT instance in a private subnet.

D. Use the internet gateway attached to the VPC.

Answer: A

Explanation: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html

A VPC endpoint for DynamoDB enables Amazon EC2 instances in your VPC to use their private IP addresses to access DynamoDB with no exposure to the public internet. Your EC2 instances do not require public IP addresses, and you don't need an internet gateway, a NAT device, or a virtual private gateway in your VPC. You use endpoint policies to control access to DynamoDB. Traffic between your VPC and the AWS service does not leave the Amazon network.

253. - (Topic 3)

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

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

A. Create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0.

B. Create a security group with a rule to allow TCP port 443 to destination 0.0.0.0/0.

C. Update the network ACL to allow TCP port 443 from source 0.0.0.0/0.

D. Update the network ACL to allow inbound/outbound TCP port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0.

E. Update the network ACL to allow inbound TCP port 443 from source 0.0.0.0/0 and outbound TCP port 32768-65535 to destination 0.0.0.0/0.

Answer: A,C

Explanation: The combination of steps that will accomplish the task of making the web server accessible from everywhere on port 443 is to create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0 (A) and to update the network ACL to allow inbound TCP port 443 from source 0.0.0.0/0 (C). This will ensure that traffic to port 443 is allowed both at the security group level and at the network ACL level, which will make the web server accessible from everywhere on port 443.

254. - (Topic 3)

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

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

A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0 Create a security group for the MySQL servers and allow port 3306 from the web servers security group

B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0 Create a network ACL (or the MySQL servers and allow port 3306 from the web servers security group

C. Create a security group for the web servers and allow port 443 from the load balancer Create a security group for the MySQL servers and allow port 3306 from the web servers security group

D. Create a network ACL 'or the web servers and allow port 443 from the load balancer Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group

Answer: C

Explanation:

This answer is correct because it provides a resilient and durable replacement for the on- premises file

share that is compatible with Windows IIS web servers. Amazon FSx for Windows File Server is a fully managed service that provides shared file storage built on Windows Server. It supports the SMB protocol and integrates with Microsoft Active Directory, which enables seamless access and authentication for Windows-based applications. Amazon FSx for Windows File Server also offers the following benefits:

- Resilience: Amazon FSx for Windows File Server can be deployed in multiple Availability Zones, which provides high availability and failover protection. It also supports automatic backups and restores, as well as self-healing features that detect and correct issues.
- Durability: Amazon FSx for Windows File Server replicates data within and across Availability Zones, and stores data on highly durable storage devices. It also supports encryption at rest and in transit, as well as file access auditing and data deduplication.
- Performance: Amazon FSx for Windows File Server delivers consistent sub-millisecond latencies and high throughput for file operations. It also supports SSD storage, native Windows features such as Distributed File System (DFS) Namespaces and Replication, and user-driven performance scaling.

By configuring the Amazon FSx file share to use an AWS KMS CMK to encrypt the images in the file share, the company can protect the images from unauthorized access and comply with company policy. By using NTFS permission sets on the images, the company can prevent accidental deletion of the images by restricting who can modify or delete them. References:

- Amazon FSx for Windows File Server
- Using Microsoft Windows file shares

255. - (Topic 3)

A solutions architect needs to design a system to store client case files. The files are core company assets and are important. The number of files will grow over time.

The files must be simultaneously accessible from multiple application servers that run on Amazon EC2 instances. The solution must have built-in redundancy.

Which solution meets these requirements?

A. Amazon Elastic File System (Amazon EFS)

B. Amazon Elastic Block Store (Amazon EBS)

C. Amazon S3 Glacier Deep Archive

D. AWS Backup

Answer: A

Explanation: Amazon EFS provides a simple, scalable, fully managed file system that can be simultaneously accessed from multiple EC2 instances and provides built-in redundancy. It is optimized for multiple EC2 instances to access the same files, and it is designed to be highly available, durable, and secure. It can scale up to petabytes of data and can handle thousands of concurrent connections, and is a cost-effective solution for storing and accessing large amounts of data.

256. - (Topic 3)

A company is running a critical business application on Amazon EC2 instances behind an Application Load Balancer The EC2 instances run in an Auto Scaling group and access an Amazon RDS DB instance The design did not pass an operational review because the EC2 instances and the DB instance are all located in a single Availability Zone A solutions architect must update the design to use a second Availability Zone

Which solution will make the application highly available?

A. Provision a subnet in each Availability Zone Configure the Auto Scaling group to distribute the EC2 instances across both

Availability Zones Configure the DB instance with connections to each network

B. Provision two subnets that extend across both Availability Zones Configure the Auto Scaling group to distribute the EC2 instances

across both Availability Zones Configure the DB instance with connections to each network

C. Provision a subnet in each Availability Zone Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones Configure the DB instance for Multi-AZ deployment

D. Provision a subnet that extends across both Availability Zones Configure the Auto Scaling group to distribute the EC2 instances

across both Availability Zones Configure the DB instance for Multi-AZ deployment

Answer: C

Explanation: https://aws.amazon.com/vpc/faqs/#:~:text=Can%20a%20subnet%20span%20Availability,within%20a%20single%20Availability%20Zone.

257. - (Topic 3)

A research laboratory needs to process approximately 8 TB of data The laboratory requires sub-millisecond latencies and a minimum throughput of 6 GBps for the storage subsystem Hundreds of Amazon EC2 instances that run Amazon Linux will distribute and process the data

Which solution will meet the performance requirements?

A. Create an Amazon FSx for NetApp ONTAP file system Set each volume's tiering policy to ALL Import the raw data into the file system Mount the file system on the EC2 instances

B. Create an Amazon S3 bucket to stofe the raw data Create an Amazon FSx for Lustre file system that uses persistent SSD storage Select the option to import data from and export data to Amazon S3 Mount the file system on the EC2 instances

C. Create an Amazon S3 bucket to store the raw data Create an Amazon FSx for Lustre file system that uses persistent HDD storage Select the option to import data from and export data to Amazon S3 Mount the file system on the EC2 instances

D. Create an Amazon FSx for NetApp ONTAP file system Set each volume's tienng policy to NONE. Import the raw data into the file system Mount the file system on the EC2 instances

Answer: B

Explanation:

Create an Amazon S3 bucket to store the raw data Create an Amazon FSx for Lustre file system that uses persistent SSD storage Select the option to import data from and export data to Amazon S3 Mount the file system on the EC2 instances. Amazon FSx for Lustre uses SSD storage for sub-millisecond latencies and up to 6 GBps throughput, and can import data from and export data to Amazon S3. Additionally, the option to select persistent SSD storage will ensure that the data is stored on the disk and not lost if the file system is stopped.

258. - (Topic 3)

A company wants to configure its Amazon CloudFront distribution to use SSL/TLS certificates. The company does not want to use the default domain name for the distribution. Instead, the company wants to use a different domain name for the distribution.

Which solution will deploy the certificate with icurring any additional costs?

A. Request an Amazon issued private certificate from AWS Certificate Manager (ACM) in the us-east-1 Region

B. Request an Amazon issued private certificate from AWS Certificate Manager (ACM) in the us-west-1 Region.

C. Request an Amazon issued public certificate from AWS Certificate Manager (ACU) in the us-east-1 Region

D. Request an Amazon issued public certificate from AWS Certificate Manager (ACU) in the us-west-1 Regon.

Answer: C

Explanation:

This option is the most efficient because it requests an Amazon issued public certificate from AWS Certificate Manager (ACM), which is a service that lets you easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources1. It also requests the certificate in the us-east-1 Region, which is required for using an ACM certificate with CloudFront2. It also meets the requirement of deploying the certificate without incurring any additional costs, as ACM does not charge for certificates that are used with supported AWS services3. This solution meets the requirement of configuring its CloudFront distribution to use SSL/TLS certificates and using a different domain name for the distribution. Option A is less efficient because it requests an Amazon issued private certificate from ACM, which is a type of certificate that can be used only within your organization or virtual private cloud (VPC). However, this does not meet the requirement of configuring its CloudFront distribution to use SSL/TLS certificates, as CloudFront requires a public certificate. It also requests the certificate in the us-east-1 Region, which is correct. Option B is less efficient because it requests an Amazon issued private certificate from ACM, which is incorrect for the same reason as option A. It also requests the certificate in the us-west-1 Region, which is incorrect as CloudFront requires a certificate in the us-east-1 Region. Option D is less efficient because it requests an Amazon issued public certificate from ACM, which is correct. However, it requests the certificate in the us-west-1 Region, which is incorrect as CloudFront requires a certificate in the us-east-1 Region.

259. - (Topic 3)

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

What should the solutions architect do to accomplish this?

A. Provide an API hosted on an Amazon EC2 instance. The EC2 instance performs the required computations when the API request is made.

B. Design a REST API using Amazon API Gateway that accepts the item names. API Gateway passes item names to AWS Lambda for tax computations.

C. Create an Application Load Balancer that has two Amazon EC2 instances behind it. The EC2 instances will compute the tax on the received item names.

D. Design a REST API using Amazon API Gateway that connects with an API hosted on an Amazon EC2 instance. API Gateway accepts and passes the item names to the EC2 instance for tax computations.

Answer: B

Explanation: Lambda server-less is scalable and elastic than EC2 api gateway solution

260. - (Topic 3)

An online learning company is migrating to the AWS Cloud. The company maintains its student records in a PostgreSQL database. The company needs a solution in which its data is available and online across multiple AWS Regions at all times.

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

A. Migrate the PostgreSQL database to a PostgreSQL cluster on Amazon EC2 instances.

B. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance with the Multi-AZ feature turned on.

C. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Create a read replica in another Region.

D. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Set up DB snapshots to be copied to another Region.

Answer: C

Explanation:

" online across multiple AWS Regions at all times". Currently only Read Replica supports cross-regions , Multi-AZ does not support cross-region (it works only in same region)

https://aws.amazon.com/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/

261. - (Topic 3)

A company uses a payment processing system that requires messages for a particular payment ID to be received in the same order that they were sent Otherwise, the payments might be processed incorrectly. Which actions should a solutions architect take to meet this requirement? (Select TWO.)

A. Write the messages to an Amazon DynamoDB table with the payment ID as the partition key

B. Write the messages to an Amazon Kinesis data stream with the payment ID as the partition key.

C. Write the messages to an Amazon ElastiCache for Memcached cluster with the payment ID as the key

D. Write the messages to an Amazon Simple Queue Service (Amazon SQS) queue Set the message attribute to use the payment ID

E. Write the messages to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the message group to use the payment ID.

Answer: B,E

Explanation:

1) SQS FIFO queues guarantee that messages are received in the exact order they are sent. Using the payment ID as the message group ensures all messages for a payment ID are received sequentially. 2) Kinesis data streams can also enforce ordering on a per partition key basis. Using the payment ID as the partition key will ensure strict ordering of messages for each payment ID.

262. - (Topic 3)

A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store is data and wants to bu4d a new service that sends an alert to the managers of four Internal teams every time a new weather event is recorded. The company does not want true new service to affect the performance of the current application

What should a solutions architect do to meet these requirement with the LEAST amount of operational overhead?

A. Use DynamoDB transactions to write new event data to the table Configure the transactions to notify internal teams.

B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.

C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a mingle Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.

D. Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SOS) queue to which the teams can subscribe.

Answer: C

Explanation:

The best solution to meet these requirements with the least amount of operational overhead is to enable Amazon DynamoDB Streams on the table and use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe. This solution requires minimal configuration and infrastructure setup, and Amazon DynamoDB Streams provide a low-latency way to capture changes to the DynamoDB table. The triggers automatically capture the changes and publish them to the SNS topic, which notifies the internal teams.

263. - (Topic 3)

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

Which service should a solutions architect recommend?

A. Amazon Aurora MySQL

B. Amazon Aurora Serverless tor MySQL

C. Amazon Redshift Spectrum

D. Amazon RDS for MySQL

Answer: B

Explanation: Amazon Aurora Serverless for MySQL is a fully managed, auto-scaling relational database service that scales up or down automatically based on the application demand. This service provides all the capabilities of Amazon Aurora, such as high availability, durability, and security, without requiring the customer to provision any database instances. With Amazon Aurora Serverless for MySQL, the sales team can enjoy minimal downtime since the database is designed to automatically scale to accommodate the

increased traffic. Additionally, the service allows the customer to pay only for the capacity used, making it cost-effective for infrequent access patterns. Amazon RDS for MySQL could also be an option, but it requires the customer to select an instance type, and the database administrator would need to monitor and adjust the instance size manually to accommodate the increasing traffic.

264. - (Topic 3)

A company has an application that collects data from IoT sensors on automobiles. The data is streamed and stored in Amazon S3 through Amazon Kinesis Date Firehose The data produces trillions of S3 objects each year. Each morning, the company uses the data from the previous 30 days to retrain a suite of machine learning (ML) models.

Four times each year, the company uses the data from the previous 12 months to perform analysis and train other ML models The data must be available with minimal delay for up to 1 year. After 1 year, the data must be retained for archival purposes.

Which storage solution meets these requirements MOST cost-effectively?

A. Use the S3 Intelligent-Tiering storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year

B. Use the S3 Intelligent-Tiering storage class. Configure S3 Intelligent-Tiering to automatically move objects to S3 Glacier Deep Archive after 1 year.

C. Use the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.

D. Use the S3 Standard storage class. Create an S3 Lifecycle policy to transition objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days, and then to S3 Glacier Deep Archive after 1 year.

Answer: D

Explanation:

- First 30 days- data access every morning (predictable and frequently) – S3 standard - After 30 days, accessed 4 times a year – S3 infrequently access - Data preserved- S3 Gllacier Deep Archive

265. - (Topic 3)

A company is launching a new application deployed on an Amazon Elastic Container Service (Amazon

ECS) cluster and is using the Fargate launch type tor ECS tasks The company is monitoring CPU and memory usage because it is expecting high traffic to the application upon its launch However the company wants to reduce costs when utilization decreases

What should a solutions architect recommend?

A. Use Amazon EC2 Auto Scaling to scale at certain periods based on previous traffic patterns

B. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm

C. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm

D. Use AWS Application Auto Scaling with target tracking policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm

Answer: D

Explanation:

https://docs.aws.amazon.com/autoscaling/application/userguide/what-is-application-auto- scaling.html

266. - (Topic 3)

A company wants to migrate its 1 PB on-premises image repository to AWS. The images will be used by a serverless web application Images stored in the repository are rarely accessed, but they must be immediately available Additionally, the images must be encrypted at rest and protected from accidental deletion

Which solution meets these requirements?

A. Implement client-side encryption and store the images in an Amazon S3 Glacier vault Set a vault lock to prevent accidental deletion

B. Store the images in an Amazon S3 bucket in the S3 Standard-Infrequent Access (S3 Standard-IA) storage class Enable versioning default encryption and MFA Delete on the S3 bucket.

C. Store the images in an Amazon FSx for Windows File Server file share Configure the Amazon FSx file share to use an AWS Key Management Service (AWS KMS) customer master key (CMK) to encrypt the images in the file share Use NTFS permission sets on the images to prevent accidental deletion

D. Store the images in an Amazon Elastic File System (Amazon EFS) file share in the Infrequent Access

storage class Configure the EFS file share to use an AWS Key Management Service (AWS KMS) customer master key (CMK) to encrypt the images in the file share. Use NFS permission sets on the images to prevent accidental deletion

Answer: B

Explanation:

This answer is correct because it provides a resilient and durable replacement for the on- premises file share that is compatible with a serverless web application. Amazon S3 is a fully managed object storage service that can store any amount of data and serve it over the internet. It supports the following features:

- Resilience: Amazon S3 stores data across multiple Availability Zones within a Region, and offers 99.999999999% (11 9's) of durability. It also supports cross- region replication, which enables automatic and asynchronous copying of objects across buckets in different AWS Regions.
- Durability: Amazon S3 encrypts data at rest using server-side encryption with either Amazon S3-managed keys (SSE-S3), AWS KMS keys (SSE-KMS), or customer-provided keys (SSE-C). It also supports encryption in transit using SSL/TLS. Amazon S3 also provides data protection features such as versioning, which keeps multiple versions of an object in the same bucket, and MFA Delete, which requires additional authentication for deleting an object version or changing the versioning state of a bucket.
- Performance: Amazon S3 delivers high performance and scalability for serving static and dynamic web content. It also supports features such as S3 Transfer Acceleration, which speeds up data transfers by routing requests to AWS edge locations, and S3 Select, which enables retrieving only a subset of data from an object by using simple SQL expressions.

The S3 Standard-Infrequent Access (S3 Standard-IA) storage class is suitable for storing images that are rarely accessed, but must be immediately available when needed. It offers the same high durability, throughput, and low latency as S3 Standard, but with a lower storage cost per GB and a higher per-request cost.

References:

- Amazon Simple Storage Service
- Storage classes - Amazon Simple Storage Service

267. - (Topic 3)

A company hosts rts sialic website by using Amazon S3 The company wants to add a contact form to its

webpage The contact form will have dynamic server-sKle components for users to input their name, email address, phone number and user message The company anticipates that there will be fewer than 100 site visits each month

Which solution will meet these requirements MOST cost-effectively?

A. Host a dynamic contact form page in Amazon Elastic Container Service (Amazon ECS) Set up Amazon Simple Email Service (Amazon SES) to connect to any third-party email provider.

B. Create an Amazon API Gateway endpoinl with an AWS Lambda backend that makes a call to Amazon Simple Email Service (Amazon SES)

C. Convert the static webpage to dynamic by deploying Amazon Ughtsail Use client-side scnpting to build the contact form Integrate the form with Amazon WorkMail

D. Create a Q micro Amazon EC2 instance Deploy a LAMP (Linux Apache MySQL. PHP/Perl/Python) stack to host the webpage Use client-side scripting to buiW the contact form Integrate the form with Amazon WorkMail

Answer: D

Explanation:

Create a t2 micro Amazon EC2 instance. Deploy a LAMP (Linux Apache MySQL, PHP/Perl/Python) stack to host the webpage. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail. This solution will provide the company with the necessary components to host the contact form page and integrate it with Amazon WorkMail at the lowest cost. Option A requires the use of Amazon ECS, which is more expensive than EC2, and Option B requires the use of Amazon API Gateway, which is also more expensive than EC2. Option C requires the use of Amazon Lightsail, which is more expensive than EC2.

Using AWS Lambda with Amazon API Gateway - AWS Lambda

https://docs.aws.amazon.com/lambda/latest/dg/services-apigateway.html

AWS Lambda FAQs https://aws.amazon.com/lambda/faqs/

268. - (Topic 3)

A company plans to use Amazon ElastiCache for its multi-tier web application A solutions architect creates a Cache VPC for the ElastiCache cluster and an App VPC for the application's Amazon EC2 instances Both VPCs are in the us-east-1 Region

The solutions architect must implement a solution to provide tne application's EC2 instances with access to the ElastiCache cluster

Which solution will meet these requirements MOST cost-effectively?

A. Create a peering connection between the VPCs Add a route table entry for the peering connection in both VPCs Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group

B. Create a Transit VPC Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group

C. Create a peering connection between the VPCs Add a route table entry for the peering connection in both VPCs Configure an inbound rule for the peering connection's security group to allow inbound connection from the application's secunty group

D. Create a Transit VPC Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC Configure an inbound rule for the Transit VPCs security group to allow inbound connection from the application's security group

Answer: A

Explanation:

Creating a peering connection between the two VPCs and configuring an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group is the most cost-effective solution. Peering connections are free and you only incur the cost of configuring the security group rules. The Transit VPC solution requires additional VPCs and associated resources, which would incur additional costs.

Before Testing | AWS Certification Information and Policies | AWS

https://aws.amazon.com/certification/policies/before-testing/

269. - (Topic 3)

An image-hosting company stores its objects in Amazon S3 buckets. The company wants to avoid accidental exposure of the objects in the S3 buckets to the public. All S3 objects in the entire AWS account need to remain private

Which solution will meal these requirements?

A. Use Amazon GuardDuty to monitor S3 bucket policies Create an automatic remediation action rule that uses an AWS Lambda function to remediate any change that makes the objects public

B. Use AWS Trusted Advisor to find publicly accessible S3 Dockets Configure email notifications In Trusted Advisor when a change is detected manually change the S3 bucket policy if it allows public access

C. Use AWS Resource Access Manager to find publicly accessible S3 buckets Use Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function when a change it detected. Deploy a Lambda function that programmatically remediates the change.

D. Use the S3 Block Public Access feature on the account level. Use AWS Organizations to create a service control policy (SCP) that prevents IAM users from changing the setting Apply tie SCP to tie account

Answer: D

Explanation:

The S3 Block Public Access feature allows you to restrict public access to S3 buckets and objects within the account. You can enable this feature at the account level to prevent any S3 bucket from being made public, regardless of the bucket policy settings. AWS Organizations can be used to apply a Service Control Policy (SCP) to the account to prevent IAM users from changing this setting, ensuring that all S3 objects remain private. This is a straightforward and effective solution that requires minimal operational overhead.

270. - (Topic 3)

A company has an application that is backed ny an Amazon DynamoDB table. The company's compliance requirements specify that database backups must be taken every month, must be available for 6 months, and must be retained for 7 years.

Which solution will meet these requirements?

A. Create an AWS Backup plan to back up the DynamoDB table on the first day of each month. Specify a lifecycle policy that transitions the backup to cold storage after 6 months. Set the retention period for each backup to 7 years.

B. Create a DynamoDB on-damand backup of the DynamoDB table on the first day of each month Transition the backup to Amazon S3 Glacier Flexible Retrieval after 6 months. Create an S3 Lifecycle policy to delete backups that are older than 7 years.

C. Use the AWS SDK to develop a script that creates an on-demand backup of the DynamoDB table. Set up an Amzon EvenlBridge rule that runs the script on the first day of each month. Create a second script

that will run on the second day of each month to transition DynamoDB backups that are older than 6 months to cold storage and to delete backups that are older than 7 years.

D. Use the AWS CLI to create an on-demand backup of the DynamoDB table Set up an Amazon EventBridge rule that runs the command on the first day of each month with a cron expression Specify in the command to transition the backups to cold storage after 6 months and to delete the backups after 7 years.

Answer: A

Explanation:

This solution satisfies the requirements in the following ways:

• AWS Backup will automatically take full backups of the DynamoDB table on the schedule defined in the backup plan (the first of each month).

• The lifecycle policy can transition backups to cold storage after 6 months, meeting that requirement.

• Setting a 7-year retention period in the backup plan will ensure each backup is retained for 7 years as required.

• AWS Backup manages the backup jobs and lifecycle policies, requiring no custom scripting or management.

271. - (Topic 3)

A company needs to ingested and handle large amounts of streaming data that its application generates. The application runs on Amazon EC2 instances and sends data to Amazon Kinesis Data Streams. which is contained wild default settings. Every other day the application consumes the data and writes the data to an Amazon S3 bucket for business intelligence (BI) processing the company observes that Amazon S3 is not receiving all the data that trio application sends to Kinesis Data Streams.

What should a solutions architect do to resolve this issue?

A. Update the Kinesis Data Streams default settings by modifying the data retention period.

B. Update the application to use the Kinesis Producer Library (KPL) lo send the data to Kinesis Data Streams.

C. Update the number of Kinesis shards lo handle the throughput of me data that is sent to Kinesis Data Streams.

D. Turn on S3 Versioning within the S3 bucket to preserve every version of every object that is ingested in

the S3 bucket.

Answer: A

Explanation:

The data retention period of a Kinesis data stream is the time period from when a record is added to when it is no longer accessible1. The default retention period for a Kinesis data stream is 24 hours, which can be extended up to 8760 hours (365 days)1. The data retention period can be updated by using the AWS Management Console, the AWS CLI, or the Kinesis Data Streams API1.

To meet the requirements of the scenario, the solutions architect should update the Kinesis Data Streams default settings by modifying the data retention period. The solutions architect should increase the retention period to a value that is greater than or equal to the frequency of consuming the data and writing it to S32. This way, the company can ensure that S3 receives all the data that the application sends to Kinesis Data Streams.

272. - (Topic 3)

A development team has launched a new application that is hosted on Amazon EC2 instances inside a development VPC. A solution architect needs to create a new VPC in the same account. The new VPC will be peered with the development VPC. The VPC CIDR block for the development VPC is 192. 168. 00/24. The solutions architect needs to create a CIDR block for the new VPC. The CIDR block must be valid for a VPC peering connection to the development VPC.

What is the SMALLEST CIOR block that meets these requirements?

A. 10.0.1.0/32

B. 192.168.0.0/24

C. 192.168.1.0/32

D. 10.0.1.0/24

Answer: D

Explanation:

The allowed block size is between a /28 netmask and /16 netmask. The CIDR block must not overlap with any existing CIDR block that's associated with the VPC.

https://docs.aws.amazon.com/vpc/latest/userguide/configure-your-vpc.html

273. - (Topic 3)

A company's application runs on AWS. The application stores large documents in an Amazon S3 bucket that uses the S3 Standard-infrequent Access (S3 Standerd-IA) storage class. The company will continue paying to store the data but wants to save on its total S3 costs. The company wants authorized external users to have the ability to access the documents in milliseconds.

Which solution will meet these requirements MOST cost-effectively?

A. Configure the S3 bucket to be a Requester Pays bucket

B. Change the storage tier to S3 Standard for all existing and future objects.

C. Turn on S3 Transfer Acceleration tor the S3 Docket

D. Use Amazon CloudFront to handle all the requests to the S3 bucket

Answer: D

Explanation:

This option is the most efficient because it uses Amazon CloudFront, which is a web service that speeds up distribution of your static and dynamic web content, such as .html,

.css, .js, and image files, to your users1. It also uses CloudFront to handle all the requests to the S3 bucket, which reduces the S3 costs by caching the content at the edge locations and serving it from there. It also allows authorized external users to access the documents in milliseconds, as CloudFront delivers the content with low latency and high data transfer rates. This solution meets the requirement of continuing paying to store the data but saving on its total S3 costs. Option A is less efficient because it configures the S3 bucket to be a Requester Pays bucket, which is a way to shift the cost of data transfer and requests from the bucket owner to the requester2. However, this does not reduce the total S3 costs, as the company still has to pay for storing the data and for any requests made by its own users. Option B is less efficient because it changes the storage tier to S3 Standard for all existing and future objects, which is a way to store frequently accessed data with high durability and availability3. However, this does not reduce the total S3 costs, as S3 Standard has higher storage costs than S3 Standard-IA. Option C is less efficient because it turns on S3 Transfer Acceleration for the S3 bucket, which is a way to speed up transfers into and out of an S3 bucket by routing requests through CloudFront edge locations4. However, this does not reduce the total S3 costs, as S3 Transfer Acceleration has additional charges for data transfer and requests.

274. - (Topic 3)

A company hosts a three-tier web application that includes a PostgreSQL database The database stores the metadata from documents The company searches the metadata for key terms to retrieve documents that the company reviews in a report each month The documents are stored in Amazon S3 The documents are usually written only once, but they are updated frequency The reporting process takes a few hours with the use of relational queries The reporting process must not affect any document modifications or the addition of new documents.

What are the MOST operationally efficient solutions that meet these requirements? (Select TWO)

A. Set up a new Amazon DocumentDB (with MongoDB compatibility) cluster that includes a read replica Scale the read replica to generate the reports.

B. Set up a new Amazon RDS for PostgreSQL Reserved Instance and an On-Demand read replica Scale the read replica to generate the reports

C. Set up a new Amazon Aurora PostgreSQL DB cluster that includes a Reserved Instance and an Aurora Replica issue queries to the Aurora Replica to generate the reports.

D. Set up a new Amazon RDS for PostgreSQL Multi-AZ Reserved Instance Configure the reporting module to query the secondary RDS node so that the reporting module does not affect the primary node

E. Set up a new Amazon DynamoDB table to store the documents Use a fixed write capacity to support new document entries Automatically scale the read capacity to support the reports

Answer: B,C

Explanation:

These options are operationally efficient because they use Amazon RDS read replicas to offload the reporting workload from the primary DB instance and avoid affecting any document modifications or the addition of new documents1. They also use Reserved Instances for the primary DB instance to reduce costs and On-Demand or Aurora Replicas for the read replicas to scale as needed. Option A is less efficient because it uses Amazon S3 Glacier Flexible Retrieval, which is a cold storage class that has higher retrieval costs and longer retrieval times than Amazon S3 Standard. It also uses EventBridge rules to invoke the job nightly, which does not meet the requirement of processing incoming data files as soon as possible. Option D is less efficient because it uses AWS Lambda to process the files, which has a maximum execution time of 15 minutes per invocation, which might not be enough for processing each file that needs 3-8 minutes. It also uses S3 event notifications to invoke the Lambda function when the files arrive, which could cause concurrency issues if there are thousands of small data files arriving periodically.

Option E is less efficient because it uses Amazon DynamoDB, which is a NoSQL database service that does not support relational queries, which are needed for generating the reports. It also uses fixed write capacity, which could cause throttling or underutilization depending on the incoming data files.

275. - (Topic 3)

A company runs an application on a large fleet of Amazon EC2 instances. The application reads and write entries into an Amazon DynamoDB table. The size of the DynamoDB table continuously grows, but the application needs only data from the last 30 days. The company needs a solution that minimizes cost and development effort.

Which solution meets these requirements?

A. Use an AWS CloudFormation template to deploy the complete solution. Redeploy the CloudFormation stack every 30 days, and delete the original stack.

B. Use an EC2 instance that runs a monitoring application from AWS Marketplace. Configure the monitoring application to use Amazon DynamoDB Streams to store the timestamp when a new item is created in the table. Use a script that runs on the EC2 instance to delete items that have a timestamp that is older than 30 days.

C. Configure Amazon DynamoDB Streams to invoke an AWS Lambda function when a new item is created in the table. Configure the Lambda function to delete items in the table that are older than 30 days.

D. Extend the application to add an attribute that has a value of the current timestamp plus 30 days to each new item that is created in the table. Configure DynamoDB to use the attribute as the TTL attribute.

Answer: D

Explanation:

Amazon DynamoDB Time to Live (TTL) allows you to define a per-item timestamp to determine when an item is no longer needed. Shortly after the date and time of the specified timestamp, DynamoDB deletes the item from your table without consuming any write throughput. TTL is provided at no extra cost as a means to reduce stored data volumes by retaining only the items that remain current for your workload's needs.

TTL is useful if you store items that lose relevance after a specific time. The following are example TTL use cases:

Remove user or sensor data after one year of inactivity in an application.

Archive expired items to an Amazon S3 data lake via Amazon DynamoDB Streams and AWS Lambda.

Retain sensitive data for a certain amount of time according to contractual or regulatory obligations.

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html

276. - (Topic 3)

A company collects data from a large number of participants who use wearabledevices.The company stores the data in an Amazon DynamoDB table and uses applications to analyze the data. The data workload is constant and predictable. The company wants to stay at or below its forecasted budget for DynamoDB.

Whihc solution will meet these requirements MOST cost-effectively?

A. Use provisioned mode and DynamoDB Standard-Infrequent Access (DynamoDB Standard-IA). Reserve capacity for the forecasted workload.

B. Use provisioned mode Specify the read capacity units (RCUs) and write capacity units (WCUs).

C. Use on-demand mode. Set the read capacity unite (RCUs) and write capacity units (WCUs) high enough to accommodate changes in the workload.

D. Use on-demand mode. Specify the read capacity units (RCUs) and write capacity units (WCUs) with reserved capacity.

Answer: B

Explanation:

This option is the most efficient because it uses provisioned mode, which is a read/write capacity mode for processing reads and writes on your tables that lets you specify how much read and write throughput you expect your application to perform1. It also specifies the read capacity units (RCUs) and write capacity units (WCUs), which are the amount of data your application needs to read or write per second. It also meets the requirement of staying at or below its forecasted budget for DynamoDB, as provisioned mode has lower costs than on-demand mode for predictable workloads. This solution meets the requirement of collecting data from a large number of participants who use wearable devices with a constant and predictable data workload. Option A is less efficient because it uses provisioned mode and DynamoDB Standard-Infrequent Access (DynamoDB Standard-IA), which is a storage class for infrequently accessed items that require milliseconds latency2. However, this does not meet the requirement of collecting data from a large number of participants who use wearable devices with a constant and predictable data workload, as DynamoDB Standard-IA is more suitable for items that are accessed less frequently than once every 30 days. Option C

is less efficient because it uses on- demand mode, which is a read/write capacity mode that lets you pay only for what you use by automatically adjusting your table's capacity in response to changing demand3. However, this does not meet the requirement of staying at or below its forecasted budget for DynamoDB, as on-demand mode has higher costs than provisioned mode for predictable workloads. Option D is less efficient because it uses on-demand mode and specifies the RCUs and WCUs with reserved capacity, which is a way to reserve read and write capacity for your tables in exchange for discounted hourly rates. However, this does not meet the requirement of staying at or below its forecasted budget for DynamoDB, as on-demand mode has higher costs than provisioned mode for predictable workloads. Also, specifying RCUs and WCUs with reserved capacity is not possible with on-demand mode, as it only applies to provisioned mode.

277. - (Topic 3)

A company stores its data objects in Amazon S3 Standard storage. A solutions architect has found that 75% of the data is rarely accessed after 30 days. The company needs all the data to remain immediately accessible with the same high availability and resiliency, but the company wants to minimize storage costs. Which storage solution will meet these requirements?

A. Move the data objects to S3 Glacier Deep Archive after 30 days.

B. Move the data objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.

C. Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

D. Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately.

Answer: B

Explanation:

Move the data objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days - will meet the requirements of keeping the data immediately accessible with high availability and resiliency, while minimizing storage costs. S3 Standard-IA is designed for infrequently accessed data, and it provides a lower storage cost than S3 Standard, while still offering the same low latency, high throughput, and high durability as S3 Standard.

278. - (Topic 3)

A solutions architect is designing a two-tiered architecture that includes a public subnet and a database

subnet. The web servers in the public subnet must be open to the internet on port 443. The Amazon RDS for MySQL D6 instance in the database subnet must be accessible only to the web servers on port 3306. Which combination of steps should the solutions architect take to meet these requirements? (Select TWO.)

A. Create a network ACL for the public subnet Add a rule to deny outbound traffic to 0 0 0 0/0 on port 3306

B. Create a security group for the DB instance Add a rule to allow traffic from the public subnet CIDR block on port 3306

C. Create a security group for the web servers in the public subnet Add a rule to allow traffic from 0 0 0 O'O on port 443

D. Create a security group for the DB instance Add a rule to allow traffic from the web servers' security group on port 3306

E. Create a security group for the DB instance Add a rule to deny all traffic except traffic from the web servers' security group on port 3306

Answer: B,C

Explanation: Security groups are virtual firewalls that protect AWS instances and can be applied to EC2, ELB and RDS1. Security groups have rules for inbound and outbound traffic and are stateful, meaning that responses to allowed inbound traffic are allowed to flow out of the instance2. Network ACLs are different from security groups in several ways. They cover entire subnets, not individual instances, and are stateless, meaning that they require rules for both inbound and outbound traffic2. Network ACLs also support deny rules, while security groups only support allow rules2.

To meet the requirements of the scenario, the solutions architect should create two security groups: one for the DB instance and one for the web servers in the public subnet. The security group for the DB instance should allow traffic from the public subnet CIDR block on port 3306, which is the default port for MySQL3. This way, only the web servers in the public subnet can access the DB instance on that port. The security group for the web servers should allow traffic from 0 0 0 O'O on port 443, which is the default port for HTTPS 4. This way, the web servers can accept secure connections from the internet on that port.

279. - (Topic 3)

An ecommerce company is building a distributed application that involves several serverless functions and AWS services to complete order-processing tasks. These tasks require manual approvals as part of the workflow A solutions architect needs to design an

architecture for the order-processing application The solution must be able to combine multiple AWS Lambda functions into responsive serverless applications The solution also must orchestrate data and services that run on Amazon EC2 instances, containers, or on- premises servers

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

A. Use AWS Step Functions to build the application.

B. Integrate all the application components in an AWS Glue job

C. Use Amazon Simple Queue Service (Amazon SQS) to build the application

D. Use AWS Lambda functions and Amazon EventBridge (Amazon CloudWatch Events) events to build the application

Answer: A

Explanation:

AWS Step Functions is a fully managed service that makes it easy to build applications by coordinating the components of distributed applications and microservices using visual workflows. With Step Functions, you can combine multiple AWS Lambda functions into responsive serverless applications and orchestrate data and services that run on Amazon EC2 instances, containers, or on-premises servers. Step Functions also allows for manual approvals as part of the workflow. This solution meets all the requirements with the least operational overhead.

https://aws.amazon.com/step-functions/#:~:text=AWS%20Step%20Functions%20is%20a,machine%20learning%20(ML)%20pipelines.

280. - (Topic 3)

A company runs an application that receives data from thousands of geographically dispersed remote devices that use UDP The application processes the data immediately and sends a message back to the device if necessary No data is stored.

The company needs a solution that minimizes latency for the data transmission from the devices. The solution also must provide rapid failover to another AWS Region

Which solution will meet these requirements?

A. Configure an Amazon Route 53 failover routing policy Create a Network Load Balancer (NLB) in each of the two Regions Configure the NLB to invoke an AWS Lambda function to process the data

B. Use AWS Global Accelerator Create a Network Load Balancer (NLB) in each of the two Regions as an

endpoint. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type Create an ECS service on the cluster Set the ECS service as the target for the NLB Process the data in Amazon ECS.

C. Use AWS Global Accelerator Create an Application Load Balancer (ALB) in each of the two Regions as an endpoint Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type Create an ECS service on the cluster. Set the ECS service as the target for the ALB Process the data in Amazon ECS

D. Configure an Amazon Route 53 failover routing policy Create an Application Load Balancer (ALB) in each of the two Regions Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type Create an ECS service on the cluster Set the ECS service as the target for the ALB Process the data in Amazon ECS

Answer: B

Explanation:

To meet the requirements of minimizing latency for data transmission from the devices and providing rapid failover to another AWS Region, the best solution would be to use AWS Global Accelerator in combination with a Network Load Balancer (NLB) and Amazon Elastic Container Service (Amazon ECS). AWS Global Accelerator is a service that improves the availability and performance of applications by using static IP addresses (Anycast) to route traffic to optimal AWS endpoints. With Global Accelerator, you can direct traffic to multiple Regions and endpoints, and provide automatic failover to another AWS Region.

281. - (Topic 3)

A company needs to provide its employee with secure access to confidential and sensitive files. The company wants to ensure that the files can be accessed only by authorized users. The files must be downloaded security to the employees devices.

The files are stored in an on-premises Windows files server. However, due to an increase in remote usage, the file server out of capacity.

Which solution will meet these requirement?

A. Migrate the file server to an Amazon EC2 instance in a public subnet. Configure the security group to limit inbound traffic to the employees ,IP addresses.

B. Migrate the files to an Amazon FSx for Windows File Server file system. Integrate the Amazon FSx file

system with the on-premises Active Directory Configure AWS Client VPN.

C. Migrate the files to Amazon S3, and create a private VPC endpoint. Create a signed URL to allow download.

D. Migrate the files to Amazon S3, and create a public VPC endpoint Allow employees to sign on with AWS IAM identity Center (AWS Sing-On).

Answer: B

Explanation:

Windows file server is on-premise and we need something to replicate the data to the cloud, the only option we have is AWS FSx for Windows File Server. Also, since the information is confidential and sensitive, we also want to make sure that the appropriate users have access to it in a secure manner.

https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html

282. - (Topic 3)

A company is developing a new mobile app. The company must implement proper traffic filtering to protect its Application Load Balancer (ALB) against common application-level attacks, such as cross-site scripting or SQL injection. The company has minimal infrastructure and operational staff. The company needs to reduce its share of the responsibility in managing, updating, and securing servers for its AWS environment. What should a solutions architect recommend to meet these requirements?

A. Configure AWS WAF rules and associate them with the ALB.

B. Deploy the application using Amazon S3 with public hosting enabled.

C. Deploy AWS Shield Advanced and add the ALB as a protected resource.

D. Create a new ALB that directs traffic to an Amazon EC2 instance running a third-party firewall, which then passes the traffic to the current ALB.

Answer: A

Explanation: A solutions architect should recommend option A, which is to configure AWS WAF rules and associate them with the ALB. This will allow the company to apply traffic filtering at the application layer, which is necessary for protecting the ALB against common application-level attacks such as cross-site scripting or SQL injection. AWS WAF is a managed service that makes it easy to protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. The company can easily manage and update the rules to ensure the security of its

application.

283. - (Topic 3)

A solutions architect is designing the architecture of a new application being deployed to the AWS Cloud. The application will run on Amazon EC2 On-Demand Instances and will automatically scale across multiple Availability Zones. The EC2 instances will scale up and down frequently throughout the day. An Application Load Balancer (ALB) will handle the load distribution. The architecture needs to support distributed session data management. The company is willing to make changes to code if needed.

What should the solutions architect do to ensure that the architecture supports distributed session data management?

A. Use Amazon ElastiCache to manage and store session data.

B. Use session affinity (sticky sessions) of the ALB to manage session data.

C. Use Session Manager from AWS Systems Manager to manage the session.

D. Use the GetSessionToken API operation in AWS Security Token Service (AWS STS) to manage the session

Answer: A

Explanation: https://aws.amazon.com/vi/caching/session-management/

In order to address scalability and to provide a shared data storage for sessions that can be accessible from any individual web server, you can abstract the HTTP sessions from the web servers themselves. A common solution to for this is to leverage an In-Memory Key/Value store such as Redis and Memcached.

ElastiCache offerings for In-Memory key/value stores include ElastiCache for Redis, which can support replication, and ElastiCache for Memcached which does not support replication.

284. - (Topic 3)

A company has launched an Amazon RDS for MySQL D6 instance Most of the connections to the database come from serverless applications. Application traffic to the database changes significantly at random intervals At limes of high demand, users report that their applications experience database connection rejection errors.

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

A. Create a proxy in RDS Proxy Configure the users' applications to use the DB instance through RDS

Proxy

B. Deploy Amazon ElastCache for Memcached between the users' application and the DB instance

C. Migrate the DB instance to a different instance class that has higher I/O capacity. Configure the users' applications to use the new DB instance.

D. Configure Multi-AZ for the DB instance Configure the users' application to switch between the DB instances.

Answer: A

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/pt/rds/proxy/)

285. - (Topic 3)

A company stores confidential data in an Amazon Aurora PostgreSQL database in the ap- southeast-3 Region The database is encrypted with an AWS Key Management Service (AWS KMS) customer managed key The company was recently acquired and must securely share a backup of the database with the acquiring company's AWS account in ap- southeast-3.

What should a solutions architect do to meet these requirements?

A. Create a database snapshot Copy the snapshot to a new unencrypted snapshot Share the new snapshot with the acquiring company's AWS account

B. Create a database snapshot Add the acquiring company's AWS account to the KMS key policy Share the snapshot with the acquiring company's AWS account

C. Create a database snapshot that uses a different AWS managed KMS key Add the acquiring company's AWS account to the KMS key alias. Share the snapshot with the acquiring company's AWS account.

D. Create a database snapshot Download the database snapshot Upload the database snapshot to an Amazon S3 bucket Update the S3 bucket policy to allow access from the acquiring company's AWS account

Answer: B

Explanation:

https://docs.aws.amazon.com/kms/latest/developerguide/key-policy-modifying-external-accounts.html

There's no need to create another custom AWS KMS key.

https://aws.amazon.com/premiumsupport/knowledge-center/aurora-share-encrypted- snapshot/ Give target account access to the custom AWS KMS key within the source account 1. Log in to the source account, and go to the AWS KMS console in the same Region as the DB cluster snapshot. 2. Select Customer-managed keys from the navigation pane. 3. Select your custom AWS KMS key (ALREADY CREATED) 4. From the Other AWS accounts section, select Add another AWS account, and then enter the AWS account number of your target account. Then: Copy and share the DB cluster snapshot

286. - (Topic 3)

A company needs to export its database once a day to Amazon S3 for other teams to access. The exported object size vanes between 2 GB and 5 GB. The S3 access pattern for the data is variable and changes rapidly. The data must be immediately available and must remain accessible for up to 3 months. The company needs the most cost-effective solution that will not increase retrieval time

Which S3 storage class should the company use to meet these requirements?

A. S3 Intelligent-Tiering

B. S3 Glacier Instant Retrieval

C. S3 Standard

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

Answer: D

Explanation: S3 Intelligent-Tiering is a cost-optimized storage class that automatically moves data to the most cost-effective access tier based on changing access patterns. Although it offers cost savings, it also introduces additional latency and retrieval time into the data retrieval process, which may not meet the requirement of "immediately available" data. On the other hand, S3 Standard-Infrequent Access (S3 Standard-IA) provides low cost storage with low latency and high throughput performance. It is designed for infrequently accessed data that can be recreated if lost, and can be retrieved in a timely manner if required. It is a cost-effective solution that meets the requirement of immediately available data and remains accessible for up to 3 months.

287. - (Topic 3)

An application that is hosted on Amazon EC2 instances needs to access an Amazon S3 bucket Traffic must not traverse the internet How should a solutions architect configure access to meet these requirements?

A. Create a private hosted zone by using Amazon Route 53

B. Set up a gateway VPC endpoint for Amazon S3 in the VPC

C. Configure the EC2 instances to use a NAT gateway to access the S3 bucket

D. Establish an AWS Site-to-Site VPN connection between the VPC and the S3 bucket

Answer: B

Explanation:

This option is the most efficient because it uses a gateway VPC endpoint for Amazon S3, which provides reliable connectivity to Amazon S3 without requiring an internet gateway or a NAT device for the VPC1. A gateway VPC endpoint routes traffic from the VPC to Amazon S3 using a prefix list for the service and does not leave the AWS network2. This meets the requirement of not traversing the internet. Option A is less efficient because it uses a private hosted zone by using Amazon Route 53, which is a DNS service that allows you to create custom domain names for your resources within your VPC3. However, this does not provide connectivity to Amazon S3 without an internet gateway or a NAT device. Option C is less efficient because it uses a NAT gateway to access the S3 bucket, which is a highly available, managed Network Address Translation (NAT) service that enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating a connection with those instances4. However, this does not meet the requirement of not traversing the internet. Option D is less efficient because it uses an AWS Site-to-Site VPN connection between the VPC and the S3 bucket, which is a secure and encrypted network connection between your on-premises network and your VPC. However, this does not meet the requirement of not traversing the internet.

288. - (Topic 3)

A financial company hosts a web application on AWS. The application uses an Amazon API Gateway Regional API endpoint to give users the ability to retrieve current stock prices. The company's security team has noticed an increase in the number of API requests. The security team is concerned that HTTP flood attacks might take the application offline.

A solutions architect must design a solution to protect the application from this type of attack.

Which solution meats these requirements with the LEAST operational overhead?

A. Create an Amazon CloudFront distribution in front of the API Gateway Regional API endpoint with a maximum TTL of 24 hours

B. Create a Regional AWS WAF web ACL with a rate-based rule. Associate the web ACL with the API Gateway stage.

C. Use Amazon CloudWatch metrics to monitor the Count metric and alert the security team when the predefined rate is reached

D. Create an Amazon CloudFront distribution with Lambda@Edge in front of the API Gateway Regional API endpoint Create an AWS Lambda function to block requests from IP addresses that exceed the predefined rate.

Answer: B

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

A rate-based rule in AWS WAF allows the security team to configure thresholds that trigger rate-based rules, which enable AWS WAF to track the rate of requests for a specified time period and then block them automatically when the threshold is exceeded. This provides the ability to prevent HTTP flood attacks with minimal operational overhead.

289. - (Topic 3)

A company hosts a multi-tier web application that uses an Amazon Aurora MySQL DB cluster for storage. The application tier is hosted on Amazon EC2 instances. The company's IT security guidelines mandate that the database credentials be encrypted and rotated every 14 days

What should a solutions architect do to meet this requirement with the LEAST operational effort?

A. Create a new AWS Key Management Service (AWS KMS) encryption key Use AWS Secrets Manager to create a new

secret that uses the KMS key with the appropriate credentials Associate the secret with the Aurora DB cluster Configure a custom rotation period of 14 days

B. Create two parameters in AWS Systems Manager Parameter Store one for the user

name as a string parameter and one that uses the SecureStnng type for the password Select AWS Key Management Service (AWS KMS) encryption for the password parameter, and load these parameters in the application tier Implement an AWS Lambda function that rotates the password every 14 days.

C. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon Elastic File System (Amazon EFS) file system Mount the EFS file system in all EC2 instances of the application tier. Restrict the access to the file on the file system so that the application can read the file and that only super users can modify the file Implement an AWS Lambda function that rotates the key in Aurora every 14 days and writes new credentials into the file

D. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon S3 bucket that the application uses to load the credentials Download the file to the application regularly to ensure that the correct credentials are used Implement an AWS Lambda function that rotates the Aurora credentials every 14 days and uploads these credentials to the file in the S3 bucket

Answer: A

Explanation:

https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-rotate-credentials-amazon-rds-database-types-oracle/

290. - (Topic 3)

A company has a web application that is based on Java and PHP The company plans to move the application from on premises to AWS The company needs the ability to test new site features frequently. The company also needs a highly available and managed solution that requires minimum operational overhead

Which solution will meet these requirements?

A. Create an Amazon S3 bucket Enable static web hosting on the S3 bucket Upload the static content to the S3 bucket Use AWS Lambda to process all dynamic content

B. Deploy the web application to an AWS Elastic Beanstalk environment Use URL swapping to switch between multiple Elastic Beanstalk environments for feature testing

C. Deploy the web application lo Amazon EC2 instances that are configured with Java and PHP Use Auto Scaling groups and an Application Load Balancer to manage the website's availability

D. Containerize the web application Deploy the web application to Amazon EC2 instances Use the AWS Load Balancer Controller to dynamically route traffic between containers thai contain the new site features for testing

Answer: B

Explanation:

Frequent feature testing -

- Multiple Elastic Beanstalk environments can be created easily for development, testing and production use cases.

- Traffic can be routed between environments for A/B testing and feature iteration using simple URL swapping techniques. No complex routing rules or infrastructure changes required.

291. - (Topic 3)

An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers run on Amazon EC2, and the database runs on Amazon RDS for MYSQL. The backend tier communities with the RDS instance. There are frequent calls to return identical database from the database that are causing performance slowdowns.

Which action should be taken to improve the performance of the backend?

A. Implement Amazon SNS to store the database calls.

B. Implement Amazon ElasticCache to cache the large database.

C. Implement an RDS for MySQL read replica to cache database calls.

D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

Answer: B

Explanation:

the best solution is to implement Amazon ElastiCache to cache the large datasets, which will store the frequently accessed data in memory, allowing for faster retrieval times. This can help to alleviate the frequent calls to the database, reduce latency, and improve the overall performance of the backend tier.

292. - (Topic 3)

A company runs a web application that is backed by Amazon RDS. A new database administrator caused data loss by accidentally editing information in a database table To help recover from this type of incident, the company wants the ability to restore the database to its state from 5 minutes before any change within the last 30 days.

Which feature should the solutions architect include in the design to meet this requirement?

A. Read replicas

B. Manual snapshots

C. Automated backups

D. Multi-AZ deployments

Answer: C

Explanation:

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

Automated backups, will meet the requirement. Amazon RDS allows you to automatically create backups of your DB instance. Automated backups enable point-in-time recovery (PITR) for your DB instance down to a specific second within the retention period, which can be up to 35 days. By setting the retention period to 30 days, the company can restore the database to its state from up to 5 minutes before any change within the last 30 days.

293. - (Topic 3)

A company's web application consists of an Amazon API Gateway API in front of an AWS Lambda function and an Amazon DynamoDB database. The Lambda function handles the business logic, and the DynamoDB table hosts the data. The application uses Amazon Cognito user pools to identify the individual users of the application. A solutions architect needs to update the application so that only users who have a subscription can access premium content.

A. Enable API caching and throttling on the API Gateway API

B. Set up AWS WAF on the API Gateway API Create a rule to filter users who have a subscription

C. Apply fine-grained IAM permissions to the premium content in the DynamoDB table

D. Implement API usage plans and API keys to limit the access of users who do not have a subscription.

Answer: D

Explanation:

This option is the most efficient because it uses API usage plans and API keys, which are features of Amazon API Gateway that allow you to control who can access your API and how much and how fast they can access it1. It also implements API usage plans and API keys to limit the access of users who do not have a subscription, which enables you to create different tiers of access for your API and charge users accordingly. This solution meets the requirement of updating the application so that only users who have a subscription can access premium content. Option A is less efficient because it uses API caching and

throttling on the API Gateway API, which are features of Amazon API Gateway that allow you to improve the performance and availability of your API and protect your backend systems from traffic spikes2. However, this does not provide a way to limit the access of users who do not have a subscription. Option B is less efficient because it uses AWS WAF on the API Gateway API, which is a web application firewall service that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources3. However, this does not provide a way to limit the access of users who do not have a subscription. Option C is less efficient because it uses fine-grained IAM permissions to the premium content in the DynamoDB table, which are permissions that allow you to control access to specific items or attributes within a table4. However, this does not provide a way to limit the access of users who do not have a subscription at the API level.

294. - (Topic 3)

A company has implemented a self-managed DNS service on AWS. The solution consists of the following:

• Amazon EC2 instances in different AWS Regions

• Endpomts of a standard accelerator m AWS Global Accelerator

The company wants to protect the solution against DDoS attacks What should a solutions architect do to meet this requirement?

A. Subscribe to AWS Shield Advanced Add the accelerator as a resource to protect

B. Subscribe to AWS Shield Advanced Add the EC2 instances as resources to protect

C. Create an AWS WAF web ACL that includes a rate-based rule Associate the web ACL with the accelerator

D. Create an AWS WAF web ACL that includes a rate-based rule Associate the web ACL with the EC2 instances

Answer: A

Explanation: AWS Shield is a managed service that provides protection against Distributed Denial of Service (DDoS) attacks for applications running on AWS. AWS Shield Standard is automatically enabled to all AWS customers at no additional cost. AWS Shield Advanced is an optional paid service. AWS Shield Advanced provides additional protections against more sophisticated and larger attacks for your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53.

https://docs.aws.amazon.com/waf/latest/developerguide/ddos-event-mitigation-logic- gax.html

295. - (Topic 3)

A solution architect must create a disaster recovery (DR) plan for a high-volume software as a service (SaaS) platform. All data for the platform is stored in an Amazon Aurora MySQL DB cluster.

The DR plan must replcate data to a secondary AWS Region. Which solution will meet these requirements MOST cost-effectively? Use MySQL binary log replication to an Aurora cluster

A. Use MySQL binary log replication to an Aurora cluster in the secondary Region Provision one DB instance for the Aurora cluster in the secondary Region.

B. Set up an Aurora global database for the DB cluster. When setup is complete, remove the DB instance from the secondary Region.

C. Use AWS Database Migration Service (AWS QMS) to continuously replicate data to an Aurora cluster in the secondary Region Remove theDB instance from the secondary Region.

D. Set up an Aurora global database for the DB cluster Specify a minimum of one DB instance in the secondary Region

Answer: D

Explanation:

"Replication from the primary DB cluster to all secondaries is handled by the Aurora storage layer rather than by the database engine, so lag time for replicating changes is minimal—typically, less than 1 second. Keeping the database engine out of the replication process means that the database engine is dedicated to processing workloads. It also means that you don't need to configure or manage the Aurora MySQL binlog (binary logging) replication."

296. - (Topic 3)

A company is using Amazon CloudFront with this website. The company has enabled logging on the CloudFront distribution, and logs are saved in one of the company's Amazon S3 buckets The company needs to perform advanced analyses on the logs and build visualizations

What should a solutions architect do to meet these requirements'?

A. Use standard SQL queries in Amazon Athena to analyze the CloudFront togs in the S3 bucket Visualize the results with AWS Glue

B. Use standard SQL queries in Amazon Athena to analyze the CloudFront togs in the S3 bucket Visualize the results with Amazon QuickSight

C. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs m the S3 bucket Visualize the results with AWS Glue

D. Use standard SQL queries in Amazon DynamoDB to analyze the CtoudFront logs m the S3 bucket Visualize the results with Amazon QuickSight

Answer: B

Explanation:

https://docs.aws.amazon.com/quicksight/latest/user/welcome.html

Using Athena to query the CloudFront logs in the S3 bucket and QuickSight to visualize the results is the best solution because it is cost-effective, scalable, and requires no infrastructure setup. It also provides a robust solution that enables the company to perform advanced analysis and build interactive visualizations without the need for a dedicated team of developers.

297. - (Topic 3)

A company is migrating its on-premises workload to the AWS Cloud. The company already uses several Amazon EC2 instances and Amazon RDS DB instances. The company wants a solution that automatically starts and stops the EC2 instances and D6 instances outside of business hours. The solution must minimize cost and infrastructure maintenance.

Which solution will meet these requirement?

A. Scale the EC2 instances by using elastic resize Scale the DB instances to zero outside of business hours

B. Explore AWS Marketplace for partner solutions that will automatically start and stop the EC2 Instances and OB instances on a schedule

C. Launch another EC2 instance. Configure a crontab schedule to run shell scripts that will start and stop the existing EC2 instances and DB instances on a schedule.

D. Create an AWS Lambda function that will start and stop the EC2 instances and DB instances Configure Amazon EventBridge to invoke the Lambda function on a schedule

Answer: D

Explanation:

The most efficient solution for automatically starting and stopping EC2 instances and DB instances on a schedule while minimizing cost and infrastructure maintenance is to create an AWS Lambda function and configure Amazon EventBridge to invoke the function on a schedule.

Option A, scaling EC2 instances by using elastic resize and scaling DB instances to zero outside of business hours, is not feasible as DB instances cannot be scaled to zero.

Option B, exploring AWS Marketplace for partner solutions, may be an option, but it may not be the most efficient solution and could potentially add additional costs.

Option C, launching another EC2 instance and configuring a crontab schedule to run shell scripts that will start and stop the existing EC2 instances and DB instances on a schedule, adds unnecessary infrastructure and maintenance.

298. - (Topic 3)

A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods tor IAM user passwords What should the solutions architect do to accomplish this?

A. Set an overall password policy for the entire AWS account

B. Set a password policy for each IAM user in the AWS account

C. Use third-party vendor software to set password requirements

D. Attach an Amazon CloudWatch rule to the Create_newuser event to set the password with the appropriate requirements

Answer: A

Explanation:

This option is the most efficient because it sets an overall password policy for the entire AWS account, which is a way to specify complexity requirements and mandatory rotation periods for IAM user passwords1. It also meets the requirement of setting a password policy for all new users, as the password policy applies to all IAM users in the account. This solution meets the requirement of setting specific complexity requirements and mandatory rotation periods for IAM user passwords. Option B is less efficient because it sets a password policy for each IAM user in the AWS account, which is not possible as password policies can only be set at the account level. Option C is less efficient because it uses third- party vendor software to set password requirements, which is not necessary as IAM provides a built-in way to set password policies. Option D is less efficient because it attaches an Amazon CloudWatch rule to the Create_newuser event to

set the password with the appropriate requirements, which is not possible as CloudWatch rules cannot modify IAM user passwords.

299. - (Topic 3)

A company is building a mobile app on AWS. The company wants to expand its reach to millions of users The company needs to build a platform so that authorized users can watch the company's content on their mobile devices

What should a solutions architect recommend to meet these requirements?

A. Publish content to a public Amazon S3 bucket. Use AWS Key Management Service (AWS KMS) keys to stream content.

B. Set up IPsec VPN between the mobile app and the AWS environment to stream content

C. Use Amazon CloudFront Provide signed URLs to stream content.

D. Set up AWS Client VPN between the mobile app and the AWS environment to stream content.

Answer: C

Explanation:

Amazon CloudFront is a content delivery network (CDN) that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds. CloudFront supports signed URLs that provide authorized access to your content. This feature allows the company to control who can access their content and for how long, providing a secure and scalable solution for millions of users.

300. - (Topic 3)

A company hosts a three-tier ecommerce application on a fleet of Amazon EC2 instances. The instances run in an Auto Scaling group behind an Application Load Balancer (ALB) All ecommerce data is stored in an Amazon RDS for ManaDB Multi-AZ DB instance

The company wants to optimize customer session management during transactions The application must store session data durably

Which solutions will meet these requirements? (Select TWO)

A. Turn on the sticky sessions feature (session affinity) on the ALB

B. Use an Amazon DynamoDB table to store customer session information

C. Deploy an Amazon Cognito user pool to manage user session information

D. Deploy an Amazon ElastiCache for Redis cluster to store customer session information

E. Use AWS Systems Manager Application Manager in the application to manage user session information

Answer: A,D

Explanation:

https://aws.amazon.com/caching/session-management/

301. - (Topic 3)

A company is building a data analysis platform on AWS by using AWS Lake Formation. The platform will ingest data from different sources such as Amazon S3 and Amazon RDS. The company needs a secure solution to prevent access to portions of the data that contain sensitive information.

A. Create an IAM role that includes permissions to access Lake Formation tables.

B. Create data filters to implement row-level security and cell-level security.

C. Create an AWS Lambda function that removes sensitive information before Lake Formation ingests re data.

D. Create an AWS Lambda function that perodically Queries and removes sensitive information from Lake Formation tables.

Answer: B

Explanation:

This option is the most efficient because it uses data filters, which are specifications that restrict access to certain data in query results and engines integrated with Lake Formation1. Data filters can be used to implement row-level security and cell-level security, which are techniques to prevent access to portions of the data that contain sensitive information2. Data filters can be applied when granting Lake Formation permissions on a Data Catalog table, and can use PartiQL expressions to filter data based on conditions3. This solution meets the requirement of providing a secure solution to prevent access to portions of the data that contain sensitive information. Option A is less efficient because it uses an IAM role that includes permissions to access Lake Formation tables, which is a way to grant access to data in Lake Formation using IAM policies4. However, this does not provide a way to prevent access to portions of the data that contain sensitive information. Option C is less efficient because it uses an AWS Lambda function that removes sensitive information before Lake Formation ingests the data, which is a way to perform data cleansing or transformation using serverless functions. However, this could involve significant changes to

the application code and logic, and could also result in data loss or inconsistency. Option D is less efficient because it uses an AWS Lambda function that periodically queries and removes sensitive information from Lake Formation tables, which is a way to perform data cleansing or transformation using serverless functions. However, this could involve significant changes to the application code and logic, and could also result in data loss or inconsistency.

302. - (Topic 3)

A company runs an application on Amazon EC2 Linux instances across multiple Availability Zones. The application needs a storage layer that is highly available and Portable Operating System Interface (POSIX) compliant. The storage layer must provide maximum data durability and must be shareable across the EC2 instances. The data in the storage layer will be accessed frequency for the first 30 days and will be accessed infrequently alter that time.

Which solution will meet these requirements MOST cost-effectively?

A. Use the Amazon S3 Standard storage class Create an S3 Lifecycle policy to move infrequently accessed data to S3 Glacier

B. Use the Amazon S3 Standard storage class. Create an S3 Lifecycle policy to move infrequently accessed data to S3 Standard-Infrequent Access (EF3 Standard-IA).

C. Use the Amazon Elastic File System (Amazon EFS) Standard storage class. Create a Lifecycle management policy to move infrequently accessed data to EFS Standard- Infrequent Access (EFS Standard-IA)

D. Use the Amazon Elastic File System (Amazon EFS) One Zone storage class. Create a Lifecycle management policy to move infrequently accessed data to EFS One Zone- Infrequent Access (EFS One Zone-IA).

Answer: C

Explanation: https://aws.amazon.com/efs/features/infrequent-access/

303. - (Topic 3)

A company is migrating a Linux-based web server group to AWS. The web servers must access files in a shared file store for some content. The company must not make any changes to the application.

What should a solutions architect do to meet these requirements?

A. Create an Amazon S3 Standard bucket with access to the web servers.

B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.

C. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers.

D. Configure a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume to all web servers.

Answer: C

Explanation:

Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers. To meet the requirements of providing a shared file store for Linux-based web servers without making changes to the application, using an Amazon EFS file system is the best solution. Amazon EFS is a managed NFS file system service that provides shared access to files across multiple Linux-based instances, which makes it suitable for this use case. Amazon S3 is not ideal for this scenario since it is an object storage service and not a file system, and it requires additional tools or libraries to mount the S3 bucket as a file system. Amazon CloudFront can be used to improve content delivery performance but is not necessary for this requirement. Additionally, Amazon EBS volumes can only be mounted to one instance at a time, so it is not suitable for sharing files across multiple instances.

304. - (Topic 3)

A solutions architect is designing a multi-tier application for a company. The application's users upload images from a mobile device. The application generates a thumbnail of each image and returns a message to the user to confirm that the image was uploaded successfully.

The thumbnail generation can take up to 60 seconds, but the company wants to provide a faster response time to its users to notify them that the original image was received. The solutions architect must design the application to asynchronously dispatch requests to the different application tiers.

What should the solutions architect do to meet these requirements?

A. Write a custom AWS Lambda function to generate the thumbnail and alert the user. Use the image upload process as an event source to invoke the Lambda function.

B. Create an AWS Step Functions workflow Configure Step Functions to handle the orchestration between the application tiers and alert the user when thumbnail generation is complete

C. Create an Amazon Simple Queue Service (Amazon SQS) message queue. As images are uploaded, place a message on the SQS queue for thumbnail generation. Alert the user through an application message that the image was received

D. Create Amazon Simple Notification Service (Amazon SNS) notification topics and subscriptions Use one subscription with the application to generate the thumbnail after the image upload is complete. Use a second subscription to message the user's mobile app by way of a push notification after thumbnail generation is complete.

Answer: C

Explanation:

This option is the most efficient because it uses Amazon SQS, which is a fully managed message queuing service that lets you send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available1. It also uses an SQS message queue to asynchronously dispatch requests to the different application tiers, which decouples the image upload process from the thumbnail generation process and enables scalability and reliability. It also alerts the user through an application message that the image was received, which provides a faster response time to the user than waiting for the thumbnail generation to complete. Option A is less efficient because it uses a custom AWS Lambda function to generate the thumbnail and alert the user, which is a way to run code without provisioning or managing servers. However, this does not use an asynchronous dispatch mechanism to separate the image upload process from the thumbnail generation process. It also uses the image upload process as an event source to invoke the Lambda function, which could cause concurrency issues if there are many images uploaded at once. Option B is less efficient because it uses AWS Step Functions, which is a fully managed service that provides a graphical console to arrange and visualize the components of your application as a series of steps2. However, this does not use an asynchronous dispatch mechanism to separate the image upload process from the thumbnail generation process. It also uses Step Functions to handle the orchestration between the application tiers and alert the user when thumbnail generation is complete, which could introduce additional complexity and latency. Option D is less efficient because it uses Amazon SNS, which is a fully managed messaging service that enables you to send messages or notifications directly to users with SMS text messages or email3. However, this does not use an asynchronous dispatch mechanism to separate the image upload process from the thumbnail generation process. It also uses SNS notification topics and subscriptions to generate the thumbnail after

the image upload is complete and message the user's mobile app by way of a push notification after thumbnail generation is complete, which could introduce additional complexity and latency.

305. - (Topic 3)

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

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

A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens

B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.

C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period.

D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens

Answer: C

Explanation:

This option will scale up capacity faster in the morning to improve performance, but will still allow capacity to scale down during off hours. It achieves this as follows: • A target tracking action scales based on a CPU utilization target. By triggering at a lower CPU threshold in the morning, the Auto Scaling group will start scaling up sooner as traffic ramps up, launching instances before utilization gets too high and impacts performance. • Decreasing the cooldown period allows Auto Scaling to scale more aggressively, launching more instances faster until the target is reached. This speeds up the ramp-up of capacity. • However, unlike a scheduled action to set a fixed minimum/maximum capacity, with target tracking the group can still scale down during off hours based on demand. This helps minimize costs.

306. - (Topic 3)

A company has a large dataset for its online advertising business stored in an Amazon RDS for MySQL DB instance in a single Availability Zone. The company wants business reporting queries to run without

impacting the write operations to the production DB instance.

Which solution meets these requirements?

A. Deploy RDS read replicas to process the business reporting queries.

B. Scale out the DB instance horizontally by placing it behind an Elastic Load Balancer

C. Scale up the DB instance to a larger instance type to handle write operations and queries

D. Deploy the OB distance in multiple Availability Zones to process the business reporting queries

Answer: A

Explanation:

Read replica use cases - You have a production database that is taking on normal load & You want to run a reporting application to run some analytics • You create a Read Replica to run the new workload there • The production application is unaffected • Read replicas are used for SELECT (=read) only kind of statements (not INSERT, UPDATE, DELETE)

307. - (Topic 3)

A company s order system sends requests from clients to Amazon EC2 instances The EC2 instances process the orders and men store the orders in a database on Amazon RDS Users report that they must reprocess orders when the system fails. The company wants a resilient solution that can process orders automatically it a system outage occurs.

What should a solutions architect do to meet these requirements?

A. Move (he EC2 Instances into an Auto Scaling group Create an Amazon EventBridge (Amazon CloudWatch Events) rule to target an Amazon Elastic Container Service (Amazon ECS) task

B. Move the EC2 instances into an Auto Scaling group behind an Application Load Balancer (ALB) Update the order system to send messages to the ALB endpoint.

C. Move the EC2 instances into an Auto Scaling group Configure the order system to send messages to an Amazon Simple Queue Service (Amazon SQS) queue Configure the EC2 instances to consume messages from the queue

D. Create an Amazon Simple Notification Service (Amazon SNS) topic Create an AWS Lambda function, and subscribe the function to the SNS topic Configure the order system to send messages to the SNS topic Send a command to the EC2 instances to process the messages by using AWS Systems Manager Run Command

Answer: C

Explanation:

To meet the company's requirements of having a resilient solution that can process orders automatically in case of a system outage, the solutions architect needs to implement a fault-tolerant architecture. Based on the given scenario, a potential solution is to move the EC2 instances into an Auto Scaling group and configure the order system to send messages to an Amazon Simple Queue Service (Amazon SQS) queue. The EC2 instances can then consume messages from the queue.

308. - (Topic 3)

A company is moving its data management application to AWS. The company wants to transition to an event-driven architecture. The architecture needs to the more distributed and to use serverless concepts whit performing the different aspects of the workflow. The company also wants to minimize operational overhead.

Which solution will meet these requirements?

A. Build out the workflow in AWS Glue Use AWS Glue to invoke AWS Lambda functions to process the workflow slaps

B. Build out the workflow in AWS Step Functions Deploy the application on Amazon EC2 Instances Use Step Functions to invoke the workflow steps on the EC2 instances

C. Build out the workflow in Amazon EventBridge. Use EventBridge to invoke AWS Lambda functions on a schedule to process the workflow steps.

D. Build out the workflow m AWS Step Functions Use Step Functions to create a stale machine Use the stale machine to invoke AWS Lambda functions to process the workflow steps

Answer: D

Explanation:

This answer is correct because it meets the requirements of transitioning to an event-driven architecture, using serverless concepts, and minimizing operational overhead. AWS Step Functions is a serverless service that lets you coordinate multiple AWS services into workflows using state machines. State machines are composed of tasks and transitions that define the logic and order of execution of the workflow steps. AWS Lambda is a serverless function-as-a-service platform that lets you run code without provisioning or managing servers. Lambda functions can be invoked by Step Functions as tasks in a state

machine, and can perform different aspects of the data management workflow, such as data ingestion, transformation, validation, and analysis. By using Step Functions and Lambda, the company can benefit from the following advantages:

- Event-driven: Step Functions can trigger Lambda functions based on events, such as timers, API calls, or other AWS service events. Lambda functions can also emit events to other services or state machines, creating an event-driven architecture.
- Serverless: Step Functions and Lambda are fully managed by AWS, so the company does not need to provision or manage any servers or infrastructure. The company only pays for the resources consumed by the workflows and functions, and can scale up or down automatically based on demand.
- Operational overhead: Step Functions and Lambda simplify the development and deployment of workflows and functions, as they provide built-in features such as monitoring, logging, tracing, error handling, retry logic, and security. The company can focus on the business logic and data processing rather than the operational details.

References:

- What is AWS Step Functions?
- What is AWS Lambda?

309. - (Topic 3)

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

Which storage solution meets these requirements?

A. S3 Standard

B. S3 Intelligent-Tiering

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

D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: D

Explanation:

S3 One Zone-IA is a storage class that is designed for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3

Standard-IA. This storage class meets the requirements of the company because it provides a low-cost solution for the secondary copy of its on-premises dataset that would rarely need to be accessed. The other storage classes are either more expensive or not suitable for infrequently accessed data.

https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html

310. - (Topic 3)

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

A. Update the bucket policy to deny if the PutObject does not have an s3 x-amz-acl header set

B. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-aci header set to private.

C. Update the bucket policy to deny if the PutObject does not have an aws SecureTransport header set to true

D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-side- encryption header set.

Answer: D

Explanation:

https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/#:~:text=Solution%20overview,console%2C%20CLI%2C%20or%20SDK.&text=To%20encrypt%20an%20object%20at,S3%2C%20or%20SSE%2DKMS.

311. - (Topic 3)

A company recently migrated its entire IT environment to the AWS Cloud. The company discovers that users are provisioning oversized Amazon EC2 instances and modifying security group rules without using the appropriate change control process A solutions architect must devise a strategy to track and audit these inventory and configuration changes.

Which actions should the solutions architect take to meet these requirements? (Select TWO)

A. Enable AWS CloudTrail and use it for auditing

B. Use data lifecycie policies for the Amazon EC2 instances

C. Enable AWS Trusted Advisor and reference the security dashboard

D. Enable AWS Config and create rules for auditing and compliance purposes

E. Restore previous resource configurations with an AWS CloudFormation template

Answer: A,D

Explanation:

A) Enable AWS CloudTrail and use it for auditing. AWS CloudTrail provides a record of API calls and can be used to audit changes made to EC2 instances and security groups. By analyzing CloudTrail logs, the solutions architect can track who provisioned oversized instances or modified security groups without proper approval. D) Enable AWS Config and create rules for auditing and compliance purposes. AWS Config can record the configuration changes made to resources like EC2 instances and security groups. The solutions architect can create AWS Config rules to monitor for non-compliant changes, like launching certain instance types or opening security group ports without permission. AWS Config would alert on any violations of these rules.

312. - (Topic 3)

A company is using a fleet of Amazon EC2 instances to ingest data from on-premises data sources. The data is in JSON format and Ingestion rates can be as high as 1 MB/s. When an EC2 instance is rebooted, the data in-flight is lost. The company's data science team wants to query Ingested data In near-real time. Which solution provides near-real -time data querying that is scalable with minimal data loss?

A. Publish data to Amazon Kinesis Data Streams Use Kinesis data Analytics to query the data.

B. Publish data to Amazon Kinesis Data Firehose with Amazon Redshift as the destination Use Amazon Redshift to query the data

C. Store ingested data m an EC2 Instance store Publish data to Amazon Kinesis Data Firehose with Amazon S3 as the destination. Use Amazon Athena to query the data.

D. Store ingested data m an Amazon Elastic Block Store (Amazon EBS) volume Publish data to Amazon ElastiCache tor Red Subscribe to the Redis channel to query the data

Answer: A

Explanation:

https://docs.aws.amazon.com/kinesisanalytics/latest/dev/what-is.html

313. - (Topic 3)

A company is running a batch application on Amazon EC2 instances. The application consists of a backend

with multiple Amazon RDS databases. The application is causing a high number of leads on the databases.

A solutions architect must reduce the number of database reads while ensuring high availability.

What should the solutions architect do to meet this requirement?

A. Add Amazon RDS read replicas

B. Use Amazon ElastCache for Redis

C. Use Amazon Route 53 DNS caching

D. Use Amazon ElastiCache for Memcached

Answer: A

Explanation:

This solution meets the requirement of reducing the number of database reads while ensuring high availability for a batch application that consists of a backend with multiple Amazon RDS databases. Amazon RDS read replicas are copies of the primary database instance that can serve read-only traffic. You can create one or more read replicas for a primary database instance and connect to them using a special endpoint. Read replicas can improve the performance and availability of your application by offloading read queries from the primary database instance.

Option B is incorrect because using Amazon ElastiCache for Redis can provide a fast, in- memory data store that can cache frequently accessed data, but it does not support replication from Amazon RDS databases. Option C is incorrect because using Amazon Route 53 DNS caching can improve the performance and availability of DNS queries, but it does not reduce the number of database reads. Option D is incorrect because using Amazon ElastiCache for Memcached can provide a fast, in-memory data store that can cache frequently accessed data, but it does not support replication from Amazon RDS databases.

References:

➪ https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.ht ml

314. - (Topic 3)

A company runs a containerized application on a Kubernetes cluster in an on-premises data center. The company is using a MongoDB database for data storage.

The company wants to migrate some of these environments to AWS, but no code changes or deployment method changes are possible at this time. The company needs a solution that minimizes operational overhead.

Which solution meets these requirements?

A. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 worker nodes for compute and MongoDB on EC2 for data storage.

B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute and Amazon DynamoDB for data storage.

C. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 worker nodes for compute and Amazon DynamoDB for data storage.

D. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute and Amazon DocumentDB (with MongoDB compatibility) for data storage.

Answer: D

Explanation:

Amazon DocumentDB (with MongoDB compatibility) is a fast, reliable, and fully managed database service. Amazon DocumentDB makes it easy to set up, operate, and scale MongoDB-compatible databases in the cloud. With Amazon DocumentDB, you can run the same application code and use the same drivers and tools that you use with MongoDB.

https://docs.aws.amazon.com/documentdb/latest/developerguide/what-is.html

315. - (Topic 3)

A company wants to implement a disaster recovery plan for its primary on-premises file storage volume. The file storage volume is mounted from an Internet Small Computer Systems Interface (iSCSI) device on a local storage server. The file storage volume holds hundreds of terabytes (TB) of data.

The company wants to ensure that end users retain immediate access to all file types from the on-premises systems without experiencing latency.

Which solution will meet these requirements with the LEAST amount of change to the company's existing infrastructure?

A. Provision an Amazon S3 File Gateway as a virtual machine (VM) that is hosted on premises. Set the local cache to 10 TB. Modify existing applications to access the files through the NFS protocol. To recover from a disaster, provision an Amazon EC2 instance and mount the S3 bucket that contains the files.

B. Provision an AWS Storage Gateway tape gateway. Use a data backup solution to back up all existing data to a virtual tape library. Configure the data backup solution to run nightly after the initial backup is

complete. To recover from a disaster, provision an Amazon EC2 instance and restore the data to an Amazon Elastic Block Store (Amazon EBS) volume from the volumes in the virtual tape library.

C. Provision an AWS Storage Gateway Volume Gateway cached volume. Set the local cache to 10 TB. Mount the Volume Gateway cached volume to the existing file server by using iSCSI. and copy all files to the storage volume. Configure scheduled snapshots of the storage volume. To recover from a disaster, restore a snapshot to an Amazon Elastic Block Store (Amazon EBS) volume and attach the EBS volume to an Amazon EC2 instance.

D. Provision an AWS Storage Gateway Volume Gateway stored volume with the same amount of disk space as the existing file storage volume. Mount the Volume Gateway stored volume to the existing file server by using iSCSI, and copy all files to the storage volume. Configure scheduled snapshots of the storage volume. To recover from a disaster, restore a snapshot to an Amazon Elastic Block Store (Amazon EBS) volume and attach the EBS volume to an Amazon EC2 instance.

Answer: D

Explanation:

"The company wants to ensure that end users retain immediate access to all file types from the on-premises systems " - Cached volumes: low latency access to most recent data - Stored volumes: entire dataset is on premise, scheduled backups to S3 Hence Volume Gateway stored volume is the apt choice.

316. - (Topic 3)

A company needs a backup strategy for its three-tier stateless web application The web application runs on Amazon EC2 instances in an Auto Scaling group with a dynamic scaling policy that is configured to respond to scaling events The database tier runs on Amazon RDS for PostgreSQL The web application does not require temporary local storage on the EC2 instances The company's recovery point objective (RPO) is 2 hours

The backup strategy must maximize scalability and optimize resource utilization for this environment

Which solution will meet these requirements?

A. Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances and database every 2 hours to meet the RPO

B. Configure a snapshot lifecycle policy to take Amazon Elastic Block Store (Amazon EBS) snapshots Enable automated backups in Amazon RDS to meet the RPO

C. Retain the latest Amazon Machine Images (AMIs) of the web and application tiers Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO

D. Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances every 2 hours Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO

Answer: C

Explanation: Since the application has no local data on instances, AMIs alone can meet the RPO by restoring instances from the most recent AMI backup. When combined with automated RDS backups for the database, this provides a complete backup solution for this environment. The other options involving EBS snapshots would be unnecessary given the stateless nature of the instances. AMIs provide all the backup needed for the app tier. This uses native, automated AWS backup features that require minimal ongoing management: - AMI automated backups provide point-in-time recovery for the stateless app tier. - RDS automated backups provide point-in-time recovery for the database.

317. - (Topic 3)

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

Which solutions meet these requirements? (Select TWO.)

A. Create an Amazon RDS DB instance in Multi-AZ mode.

B. Create an Amazon RDS DB instance and one or more replicas in another Availability Zone.

C. Create an Amazon EC2 in stance-based Docker cluster to handle the dynamic application load.

D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with a Fargate launch type to handle the dynamic application load.

E. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type to handle the dynamic application load.

Answer: A,D

Explanation:

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html

* 1. Relational database: RDS

* 2. Container-based applications: ECS

"Amazon ECS enables you to launch and stop your container-based applications by using simple API calls. You can also retrieve the state of your cluster from a centralized service and have access to many familiar Amazon EC2 features."

* 3. Little manual intervention: Fargate

You can run your tasks and services on a serverless infrastructure that is managed by AWS Fargate. Alternatively, for more control over your infrastructure, you can run your tasks and services on a cluster of Amazon EC2 instances that you manage.

318. - (Topic 3)

A company that primarily runs its application servers on premises has decided to migrate to AWS. The company wants to minimize its need to scale its Internet Small Computer Systems Interface (iSCSI) storage on premises. The company wants only its recently accessed data to remain stored locally.

Which AWS solution should the company use to meet these requirements?

A. Amazon S3 File Gateway

B. AWS Storage Gateway Tape Gateway

C. AWS Storage Gateway Volume Gateway stored volumes

D. AWS Storage Gateway Volume Gateway cachea volumes

Answer: D

Explanation: AWS Storage Gateway Volume Gateway provides two configurations for connecting to iSCSI storage, namely, stored volumes and cached volumes. The stored volume configuration stores the entire data set on-premises and asynchronously backs up the data to AWS. The cached volume configuration stores recently accessed data on- premises, and the remaining data is stored in Amazon S3. Since the company wants only its recently accessed data to remain stored locally, the cached volume configuration would be the most appropriate. It allows the company to keep frequently accessed data on- premises and reduce the need for scaling its iSCSI storage while still providing access to all data through the AWS cloud. This configuration also provides low-latency access to frequently accessed data and cost-effective off-site backups for less frequently accessed data.

https://docs.amazonaws.cn/en_us/storagegateway/latest/vgw/StorageGatewayConcepts.html#storage-gateway-cached-concepts

319. - (Topic 3)

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

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

A. Configure an Amazon CloudFront distribution in from of the ALB.

B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.

C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.

D. Configure Amazon ElasticCache to remove some of the workload from tha EC2 instances.

Answer: C

Explanation:

Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule is the best option because it allows for the proactive scaling of the EC2 instances before the monthly batch run begins. This will ensure that the application is able to handle the increased workload without experiencing downtime. The scheduled scaling policy can be configured to increase the number of instances in the Auto Scaling group a few hours before the batch run and then decrease the number of instances after the batch run is complete. This will ensure that the resources are available when needed and not wasted when not needed. The most appropriate solution to handle the increased workload during the monthly batch run and avoid downtime would be to configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule. https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html

320. - (Topic 3)

A company uses a 100 GB Amazon RDS for Microsoft SQL Server Single-AZ DB instance in the us-east-1 Region to store customer transactions. The company needs high availability and automate recovery for the DB instance.

The company must also run reports on the RDS database several times a year. The report process causes

transactions to take longer than usual to post to the customer‘ accounts.

Which combination of steps will meet these requirements? (Select TWO.)

A. Modify the DB instance from a Single-AZ DB instance to a Multi-AZ deployment.

B. Take a snapshot of the current DB instance. Restore the snapshot to a new RDS deployment in another Availability Zone.

C. Create a read replica of the DB instance in a different Availability Zone. Point All requests for reports to the read replica.

D. Migrate the database to RDS Custom.

E. Use RDS Proxy to limit reporting requests to the maintenance window.

Answer: A,C

Explanation:

https://medium.com/awesome-cloud/aws-difference-between-multi-az-and-read-replicas-in-amazon-rds-60fe848ef53a

321. - (Topic 3)

A company hosts a web application on multiple Amazon EC2 instances The EC2 instances are in an Auto Scaling group that scales in response to user demand The company wants to optimize cost savings without making a long-term commitment

Which EC2 instance purchasing option should a solutions architect recommend to meet these requirements'?

A. Dedicated Instances only

B. On-Demand Instances only

C. A mix of On-Demand instances and Spot Instances

D. A mix of On-Demand instances and Reserved instances

Answer: C

Explanation:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-mixed- instances-groups.html

322. - (Topic 3)

A solutions architect must secure a VPC network that hosts Amazon EC2 instances The EC2 ^stances

contain highly sensitive data and tun n a private subnet According to company policy the EC2 instances mat run m the VPC can access only approved third- party software repositories on the internet for software product updates that use the third party's URL Other internet traffic must be blocked.

Which solution meets these requirements?

A. Update the route table for the private subnet to route the outbound traffic to an AWS Network Firewall. Configure domain list rule groups

B. Set up an AWS WAF web ACL. Create a custom set of rules that filter traffic requests based on source and destination IP address range sets.

C. Implement strict inbound security group roles Configure an outbound rule that allows traffic only to the authorized software repositories on the internet by specifying the URLs

D. Configure an Application Load Balancer (ALB) in front of the EC2 instances. Direct an outbound traffic to the ALB Use a URL-based rule listener in the ALB's target group for outbound access to the internet

Answer: A

Explanation:

Send the outbound connection from EC2 to Network Firewall. In Network Firewall, create stateful outbound rules to allow certain domains for software patch download and deny all other domains.

https://docs.aws.amazon.com/network-firewall/latest/developerguide/suricata-examples.html#suricata-example-domain-filtering

323. - (Topic 3)

A company has an application that places hundreds of .csv files into an Amazon S3 bucket every hour. The files are 1 GB in size. Each time a file is uploaded, the company needs to convert the file to Apache Parquet format and place the output file into an S3 bucket.

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

A. Create an AWS Lambda function to download the .csv files, convert the files to Parquet format, and place the output files in an S3 bucket. Invoke the Lambda function for each S3 PUT event.

B. Create an Apache Spark job to read the .csv files, convert the files to Parquet format, and place the output files in an S3 bucket. Create an AWS Lambda function for each S3 PUT event to invoke the Spark job.

C. Create an AWS Glue table and an AWS Glue crawler for the S3 bucket where the application places

the .csv files. Schedule an AWS Lambda function to periodically use Amazon Athena to query the AWS Glue table, convert the query results into Parquet format, and place the output files into an S3 bucket.

D. Create an AWS Glue extract, transform, and load (ETL) job to convert the .csv files to Parquet format and place the output files into an S3 bucket. Create an AWS Lambda function for each S3 PUT event to invoke the ETL job.

Answer: D

Explanation:

https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html

324. - (Topic 3)

A company needs to transfer 600 TB of data from its on-premises network-attached storage (NAS) system to the AWS Cloud. The data transfer must be complete within 2 weeks. The data is sensitive and must be encrypted in transit. The company's internet connection can support an upload speed of 100 Mbps.

Which solution meets these requirements MOST cost-effectively?

A. Use Amazon S3 multi-part upload functionality to transfer the fees over HTTPS

B. Create a VPN connection between the on-premises NAS system and the nearest AWS Region Transfer the data over the VPN connection

C. Use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices Use the devices to transfer the data to Amazon S3.

D. Set up a 10 Gbps AWS Direct Connect connection between the company location and (he nearest AWS Region Transfer the data over a VPN connection into the Region to store the data in Amazon S3

Answer: C

Explanation:

The best option is to use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices and use the devices to transfer the data to Amazon S3. Snowball Edge is a petabyte-scale data transfer device that can help transfer large amounts of data securely and quickly. Using Snowball Edge can be the most cost-effective solution for transferring large amounts of data over long distances and can help meet the requirement of transferring 600 TB of data within two weeks.

325. - (Topic 3)

A data analytics company wants to migrate its batch processing system to AWS. The company receives thousands of small data files periodically during the day through FTP. A on-premises batch job processes the data files overnight. However, the batch job takes hours to finish running.

The company wants the AWS solution to process incoming data files are possible with minimal changes to the FTP clients that send the files. The solution must delete the incoming data files the files have been processed successfully. Processing for each file needs to take 3-8 minutes.

Which solution will meet these requirements in the MOST operationally efficient way?

A. Use an Amazon EC2 instance that runs an FTP server to store incoming files as objects in Amazon S3 Glacier Flexible Retrieval. Configure a job queue in AWS Batch. Use Amazon EventBridge rules to invoke the job to process the objects nightly from S3 Glacier Flexible Retrieval. Delete the objects after the job has processed the objects.

B. Use an Amazon EC2 instance that runs an FTP server to store incoming files on an Amazon Elastic Block Store (Amazon EBS) volume. Configure a job queue in AWS Batch. Use Amazon EventBridge rules to invoke the process the files nightly from the EBS

volume. Delete the files after the job has processed the files.

C. Use AWS Transfer Family to create an FTP server to store incoming files on an Amazon Elastic Block Store (Amazon EBS) volume. Configure a job queue in AWS Batch. Use an Amazon S3 event notification when each files arrives to invoke the job in AWS Batch. Delete the files after the job has processed the files.

D. Use AWS Transfer Family to create an FTP server to store incoming files in Amazon S3 Standard. Create an AWS Lambda function to process the files and to delete the files after they are proessed.yse an S3 event notification to invoke the lambda function when the fils arrive

Answer: D

Explanation:

This option is the most operationally efficient because it uses AWS Transfer Family to create an FTP server that can store incoming files in Amazon S3 Standard12, which is a low-cost and highly available storage service. It also uses AWS Lambda to process the files and delete them after they are processed, which is a serverless and scalable solution that does not require any batch scheduling or infrastructure management. It also uses S3 event notifications to invoke the Lambda function when the files arrive, which enables near real-time processing of the incoming data files3. Option A is less efficient because it uses Amazon S3

Glacier Flexible Retrieval, which is a cold storage class that has higher retrieval costs and longer retrieval times than Amazon S3 Standard. It also uses EventBridge rules to invoke the job nightly, which does not meet the requirement of processing incoming data files as soon as possible. Option B is less efficient because it uses an EBS volume to store incoming files, which is a block storage service that has higher costs and lower durability than Amazon S3. It also uses EventBridge rules to invoke the job nightly, which does not meet the requirement of processing incoming data files as soon as possible. Option C is less efficient because it uses an EBS volume to store incoming files, which is a block storage service that has higher costs and lower durability than Amazon S3. It also uses AWS Batch to process the files, which requires managing compute resources and job queues.

326. - (Topic 3)

A company needs to create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster to host a digital media streaming application. The EKS cluster will use a managed node group that is backed by Amazon Elastic Block Store (Amazon EBS) volumes for storage. The company must encrypt all data at rest by using a customer managed key that is stored in AWS Key Management Service (AWS KMS)

Which combination of actions will meet this requirement with the LEAST operational overhead? (Select TWO.)

A. Use a Kubernetes plugin that uses the customer managed key to perform data encryption.

B. After creation of the EKS cluster, locate the EBS volumes. Enable encryption by using the customer managed key.

C. Enable EBS encryption by default in the AWS Region where the EKS cluster will be created. Select the customer managed key as the default key.

D. Create the EKS cluster Create an IAM role that has cuwlicy that grants permission to the customer managed key. Associate the role with the EKS cluster.

E. Store the customer managed key as a Kubernetes secret in the EKS cluster. Use the customer managed key to encrypt the EBS volumes.

Answer: C,D

Explanation:

EBS encryption by default is a feature that enables encryption for all new EBS volumes and snapshots created in a Region1. EBS encryption by default uses a service managed key or a customer managed key

that is stored in AWS KMS1. EBS encryption by default is suitable for scenarios where data at rest must be encrypted by using a customer managed key, such as the digital media streaming application in the scenario1.

To meet the requirements of the scenario, the solutions architect should enable EBS encryption by default in the AWS Region where the EKS cluster will be created. The solutions architect should select the customer managed key as the default key for encryption1. This way, all new EBS volumes and snapshots created in that Region will be encrypted by using the customer managed key.

EKS encryption provider support is a feature that enables envelope encryption of Kubernetes secrets in EKS with a customer managed key that is stored in AWS KMS2

. Envelope encryption means that data is encrypted by data encryption keys (DEKs) using AES-GCM; DEKs are encrypted by key encryption keys (KEKs) according to configuration in AWS KMS3. EKS encryption provider support is suitable for scenarios where secrets must be encrypted by using a customer managed key, such as the digital media streaming application in the scenario2.

To meet the requirements of the scenario, the solutions architect should create the EKS cluster and create an IAM role that has a policy that grants permission to the customer managed key. The solutions architect should associate the role with the EKS cluste2r. This way, the EKS cluster can use envelope encryption of Kubernetes secrets with the customer managed key.

327. - (Topic 3)

A company runs a fleet of web servers using an Amazon RDS for PostgreSQL DB instance After a routine compliance check, the company sets a standard that requires a recovery pant objective (RPO) of less than 1 second for all its production databases.

Which solution meets these requirement?

A. Enable a Multi-AZ deployment for the DB Instance

B. Enable auto scaling for the OB instance m one Availability Zone.

C. Configure the 06 instance in one Availability Zone and create multiple read replicas in a separate Availability Zone

D. Configure the 06 instance in one Availability Zone, and configure AWS Database Migration Service (AWS DMS) change data capture (CDC) tasks

Answer: A

Explanation:

This option is the most efficient because it uses a Multi-AZ deployment for the DB instance, which provides enhanced availability and durability for RDS database instances by automatically replicating the data to a standby instance in a different Availability Zone1. It also provides a recovery point objective (RPO) of less than 1 second for all its production databases, as the standby instance is kept in sync with the primary instance using synchronous physical replication2. This solution meets the requirement of requiring a RPO of less than 1 second for all its production databases. Option B is less efficient because it uses auto scaling for the DB instance in one Availability Zone, which is a way to automatically adjust the compute capacity of your DB instance based on load or a schedule 3. However, this does not provide a RPO of less than 1 second for all its production databases, as it does not replicate the data to another Availability Zone. Option C is less efficient because it uses read replicas in a separate Availability Zone, which are read-only copies of your primary database that can serve read traffic and support scaling. However, this does not provide a RPO of less than 1 second for all its production databases, as read replicas use asynchronous replication and can lag behind the primary database. Option D is less efficient because it uses AWS Database Migration Service (AWS DMS) change data capture (CDC) tasks, which are tasks that capture changes made to source data and apply them to target data. However, this does not provide a RPO of less than 1 second for all its production databases, as AWS DMS uses asynchronous replication and can lag behind the source database.

328. - (Topic 3)

A company is planning to store data on Amazon RDS DB instances. The company must encrypt the data at rest.

What should a solutions architect do to meet this requirement?

A. Create an encryption key and store the key in AWS Secrets Manager Use the key to encrypt the DB instances

B. Generate a certificate in AWS Certificate Manager (ACM). Enable SSL/TLS on the DB instances by using the certificate

C. Create a customer master key (CMK) in AWS Key Management Service (AWS KMS) Enable encryption for the DB instances

D. Generate a certificate in AWS Identity and Access Management {IAM) Enable SSUTLS on the DB

instances by using the certificate

Answer: A

Explanation:

To encrypt data at rest in Amazon RDS, you can use the encryption feature of Amazon RDS, which uses AWS Key Management Service (AWS KMS). With this feature, Amazon RDS encrypts each database instance with a unique key. This key is stored securely by AWS KMS. You can manage your own keys or use the default AWS-managed keys. When you enable encryption for a DB instance, Amazon RDS encrypts the underlying storage, including the automated backups, read replicas, and snapshots.

329. - (Topic 3)

A company uses a legacy application to produce data in CSV format The legacy application stores the output data In Amazon S3 The company is deploying a new commercial off-the- shelf (COTS) application that can perform complex SQL queries to analyze data that is stored Amazon Redshift and Amazon S3 only However the COTS application cannot process the csv files that the legacy application produces The company cannot update the legacy application to produce data in another format The company needs to implement a solution so that the COTS application can use the data that the legacy applicator produces. Which solution will meet these requirements with the LEAST operational overhead?

A. Create a AWS Glue extract, transform, and load (ETL) job that runs on a schedule. Configure the ETL job to process the .csv files and store the processed data in Amazon Redshit.

B. Develop a Python script that runs on Amazon EC2 instances to convert the. csv files to sql files invoke the Python script on cron schedule to store the output files in Amazon S3.

C. Create an AWS Lambda function and an Amazon DynamoDB table. Use an S3 event to invoke the Lambda function. Configure the Lambda function to perform an extract transform, and load (ETL) job to process the .csv files and store the processed data in the DynamoDB table.

D. Use Amazon EventBridge (Amazon CloudWatch Events) to launch an Amazon EMR cluster on a weekly schedule. Configure the EMR cluster to perform an extract, tractform, and load (ETL) job to process the .csv files and store the processed data in an Amazon Redshift table.

Answer: A

Explanation:

This solution meets the requirements of implementing a solution so that the COTS application can use the

data that the legacy application produces with the least operational overhead. AWS Glue is a fully managed service that provides a serverless ETL platform to prepare and load data for analytics. AWS Glue can process data in various formats, including .csv files, and store the processed data in Amazon Redshift, which is a fully managed data warehouse service that supports complex SQL queries. AWS Glue can run ETL jobs on a schedule, which can automate the data processing and loading process. Option B is incorrect because developing a Python script that runs on Amazon EC2 instances to convert the .csv files to sql files can increase the operational overhead and complexity, and it may not provide consistent data processing and loading for the COTS application. Option C is incorrect because creating an AWS Lambda function and an Amazon DynamoDB table to process the .csv files and store the processed data in the DynamoDB table does not meet the requirement of using Amazon Redshift as the data source for the COTS application. Option D is incorrect because using Amazon EventBridge (Amazon CloudWatch Events) to launch an Amazon EMR cluster on a weekly schedule to process the .csv files and store the processed data in an Amazon Redshift table can increase the operational overhead and complexity, and it may not provide timely data processing and loading for the COTS application.

References:

- https://aws.amazon.com/glue/
- https://aws.amazon.com/redshift/

330. - (Topic 3)

At part of budget planning. management wants a report of AWS billed dams listed by user. The data will be used to create department budgets. A solution architect needs to determine the most efficient way to obtain this report Information

Which solution meets these requirement?

A. Run a query with Amazon Athena to generate the report.

B. Create a report in Cost Explorer and download the report

C. Access the bill details from the running dashboard and download Via bill.

D. Modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES).

Answer: B

Explanation:

This option is the most efficient because it uses Cost Explorer, which is a tool that allows you to visualize,

understand, and manage your AWS costs and usage over time1. You can create a report in Cost Explorer that lists AWS billed items by user, using the user name tag as a filter2. You can then download the report as a CSV file and use it for budget planning. Option A is less efficient because it uses Amazon Athena, which is a serverless interactive query service that allows you to analyze data in Amazon S3 using standard SQL 3. You would need to set up an Athena table that points to your AWS Cost and Usage Report data in S3, and then run a query to generate the report. This would incur additional costs and complexity. Option C is less efficient because it uses the billing dashboard, which provides a high-level summary of your AWS costs and usage. You can access the bill details from the billing dashboard and download them via bill, but this would not list the billed items by user. You would need to use tags to group your costs by user name, which would require additional steps. Option D is less efficient because it uses AWS Budgets, which is a tool that allows you to plan your service usage, service costs, and instance reservations. You can modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES), but this would not generate a report of AWS billed items by user. This would only notify you when your actual or forecasted costs exceed or are expected to exceed your budgeted amount.

331. - (Topic 3)

A company recently created a disaster recovery site in a Different AWS Region.The company needs to transfer large amounts of data back and forth between NFS file systems in the two Regions on a periods. Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS DataSync.

B. Use AWS Snowball devices

C. Set up an SFTP server on Amazon EC2

D. Use AWS Database Migration Service (AWS DMS)

Answer: A

Explanation:

This option is the most efficient because it uses AWS DataSync, which is a secure, online service that automates and accelerates moving data between on-premises and AWS Storage services1. It also uses DataSync to transfer large amounts of data back and forth between NFS file systems in the two Regions on a periodic basis, which simplifies and speeds up the data transfer process with minimal operational overhead. This solution meets the requirement of transferring large amounts of data back and forth

between NFS file systems in the two Regions on a periodic basis with the least operational overhead.

Option B is less efficient because it uses AWS Snowball devices, which are physical devices that let you transfer large amounts of data into and out of AWS2.

However, this does not provide a periodic data transfer solution, as it requires manual handling and shipping of the devices. Option C is less efficient because it sets up an SFTP server on Amazon EC2, which is a way to provide secure file transfer protocol (SFTP) access to files stored in Amazon S33. However, this does not provide a periodic data transfer solution, as it requires manual initiation and monitoring of the file transfers. Option D is less efficient because it uses AWS Database Migration Service (AWS DMS), which is a service that helps you migrate databases to AWS quickly and securely. However, this does not provide a data transfer solution for NFS file systems, as it only supports relational databases and non-relational data stores.

332. - (Topic 3)

A company hosts a frontend application that uses an Amazon API Gateway API backend that is integrated with AWS Lambda When the API receives requests, the Lambda function loads many libranes Then the Lambda function connects to an Amazon RDS database processes the data and returns the data to the frontend application. The company wants to ensure that response latency is as low as possible for all its users with the fewest number of changes to the company's operations

Which solution will meet these requirements'?

A. Establish a connection between the frontend application and the database to make queries faster by bypassing the API

B. Configure provisioned concurrency for the Lambda function that handles the requests

C. Cache the results of the queries in Amazon S3 for faster retneval of similar datasets.

D. Increase the size of the database to increase the number of connections Lambda can establish at one time

Answer: B

Explanation:

Configure provisioned concurrency for the Lambda function that handles the requests. Provisioned concurrency allows you to set the amount of compute resources that are available to the Lambda function, so that it can handle more requests at once and reduce latency. Caching the results of the queries in

Amazon S3 could also help to reduce latency, but it would not be as effective as setting up provisioned concurrency. Increasing the size of the database would not help to reduce latency, as this would not increase the number of connections the Lambda function could establish, and establishing a direct connection between the frontend application and the database would bypass the API, which would not be the best solution either.

Using AWS Lambda with Amazon API Gateway - AWS Lambda

https://docs.aws.amazon.com/lambda/latest/dg/services-apigateway.html

AWS Lambda FAQs https://aws.amazon.com/lambda/faqs/

333. - (Topic 3)

A payment processing company records all voice communication with its customers and stores the audio files in an Amazon S3 bucket. The company needs to capture the text from the audio files. The company must remove from the text any personally identifiable information (PII) that belongs to customers.

What should a solutions architect do to meet these requirements?

A. Process the audio files by using Amazon Kinesis Video Streams. Use an AWS Lambda function to scan for known PII patterns.

B. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start an Amazon Textract task to analyze the call recordings.

C. Configure an Amazon Transcribe transcription job with PII redaction turned on. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start the transcription job. Store the output in a separate S3 bucket.

D. Create an Amazon Connect contact flow that ingests the audio files with transcription turned on. Embed an AWS Lambda function to scan for known PII patterns. Use Amazon EventBridge (Amazon CloudWatch Events) to start the contact flow when an audio file is uploaded to the S3 bucket.

Answer: C

Explanation:

"Sensitive data redaction replaces personally identifiable information (PII) in the text transcript and the audio file. A redacted transcript replaces the original text with [PII]; a redacted audio file replaces spoken personal information with silence. This parameter is useful for protecting customer information."

https://docs.aws.amazon.com/transcribe/latest/dg/call-analytics-insights.html#call-analytics-

insights-redaction

334. - (Topic 3)

A company is launching an application on AWS. The application uses an Application Load (ALB) to direct traffic to at least two Amazon EC2 instances in a single target group.

The instances are in an Auto Scaling group for each environment. The company requires a development and a production environment. The production environment will have periods of high traffic.

Which solution will configure the development environment MOST cost-effectively?

A. Reconfigure the target group in the development environment to have one EC2 instance as a target.

B. Change the ALB balancing algorithm to least outstanding requests.

C. Reduce the size of the EC2 instances in both environments.

D. Reduce the maximum number of EC2 instances in the development environment's Auto Scaling group

Answer: D

Explanation: This option will configure the development environment in the most cost- effective way as it reduces the number of instances running in the development environment and therefore reduces the cost of running the application. The development environment typically requires less resources than the production environment, and it is unlikely that the development environment will have periods of high traffic that would require a large number of instances. By reducing the maximum number of instances in the development environment's Auto Scaling group, the company can save on costs while still maintaining a functional development environment.

335. - (Topic 3)

A company's security team requests that network traffic be captured in VPC Flow Logs. The logs will be frequently accessed for 90 days and then accessed intermittently.

What should a solutions architect do to meet these requirements when configuring the logs?

A. Use Amazon CloudWatch as the target. Set the CloudWatch log group with an expiration of 90 days

B. Use Amazon Kinesis as the target. Configure the Kinesis stream to always retain the logs for 90 days.

C. Use AWS CloudTrail as the target. Configure CloudTrail to save to an Amazon S3 bucket, and enable S3 Intelligent-Tiering.

D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3

Standard-Infrequent Access (S3 Standard-IA) after 90 days.

Answer: D

Explanation:

There's a table here that specifies that VPC Flow logs can go directly to S3. Does not need to go via CloudTrail and then to S3. Nor via CW.

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AWS-logs-and-resource-policy.html#AWS-logs-infrastructure-S3

336. - (Topic 3)

A company has an AWS Lambda function that needs read access to an Amazon S3 bucket that is located in the same AWS account. Which solution will meet these requirement in the MOST secure manner?

A. Apply an S3 bucket pokey that grants road access to the S3 bucket

B. Apply an IAM role to the Lambda function Apply an IAM policy to the role to grant read access to the S3 bucket

C. Embed an access key and a secret key In the Lambda function's coda to grant the required IAM permissions for read access to the S3 bucket

D. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to all S3 buckets In the account

Answer: B

Explanation:

This option is the most secure because it follows the principle of least privilege and grants only the necessary permissions to the Lambda function without exposing any credentials in the code. The IAM role can be configured as the Lambda function’s execution role and the IAM policy can specify the S3 bucket ARN and the s3:GetObject action12. Option A is less secure because it grants read access to any principal that has access to the S3 bucket, which could be more than the Lambda function. Option C is less secure because it embeds credentials in the code, which could be compromised or exposed. Option D is less secure because it grants read access to all S3 buckets in the account, which could be more than what the Lambda function needs.

337. - (Topic 3)

A solution architect is designing a company's disaster recovery (DR) architecture. The company has a MySQL database that runs on an Amazon EC2 instance in a private subnet with scheduled backup. The DR design to include multiple AWS Regions.

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

A. Migrate the MySQL database to multiple EC2 instances. Configure a standby EC2 instance in the DR Region Turn on replication.

B. Migrate the MySQL database to Amazon RDS. Use a Multi-AZ deployment. Turn on read replication for the primary DB instance in the different Availability Zones.

C. Migrate the MySQL database to an Amazon Aurora global database. Host the primary DB cluster in the primary Region. Host the secondary DB cluster in the DR Region.

D. Store the schedule backup of the MySQL database in an Amazon S3 bucket that is configured for S3 Cross-Region Replication (CRR). Use the data backup to restore the database in the DR Region.

Answer: C

Explanation:

Migrate MySQL database to an Amazon Aurora global database is the best solution

because it requires minimal operational overhead. Aurora is a managed service that provides automatic failover, so standby instances do not need to be manually configured. The primary DB cluster can be hosted in the primary Region, and the secondary DB cluster can be hosted in the DR Region. This approach ensures that the data is always available and up-to-date in multiple Regions, without requiring significant manual intervention.

338. - (Topic 3)

A company is designing a shared storage solution for a gaming application that is hosted in the AWS Cloud The company needs the ability to use SMB clients to access data solution must be fully managed.

Which AWS solution meets these requirements?

A. Create an AWS DataSync task that shares the data as a mountable file system Mount the file system to the application server

B. Create an Amazon EC2 Windows instance Install and configure a Windows file share role on the instance Connect the application server to the file share

C. Create an Amazon FSx for Windows File Server file system Attach the file system to the origin server

Connect the application server to the file system

D. Create an Amazon S3 bucket Assign an IAM role to the application to grant access to the S3 bucket Mount the S3 bucket to the application server

Answer: C

Explanation:

Amazon FSx for Windows File Server (Amazon FSx) is a fully managed, highly available, and scalable file storage solution built on Windows Server that uses the Server Message Block (SMB) protocol. It allows for Microsoft Active Directory integration, data deduplication, and fully managed backups, among other critical enterprise features.

https://aws.amazon.com/blogs/storage/accessing-smb-file-shares-remotely-with-amazon-fsx-for-windows-file-server/

339. - (Topic 3)

A company wants to migrate an Oracle database to AWS. The database consists of a single table that contains millions of geographic information systems (GIS) images that are high resolution and are identified by a geographic code.

When a natural disaster occurs tens of thousands of images get updated every few minutes. Each geographic code has a single image or row that is associated with it. The company wants a solution that is highly available and scalable during such events

Which solution meets these requirements MOST cost-effectively?

A. Store the images and geographic codes in a database table Use Oracle running on an Amazon RDS Multi-AZ DB instance

B. Store the images in Amazon S3 buckets Use Amazon DynamoDB with the geographic code as the key and the image S3 URL as the value

C. Store the images and geographic codes in an Amazon DynamoDB table Configure DynamoDB Accelerator (DAX) during times of high load

D. Store the images in Amazon S3 buckets Store geographic codes and image S3 URLs in a database table Use Oracle running on an Amazon RDS Multi-AZ DB instance.

Answer: B

Explanation:

Amazon S3 is a highly scalable, durable, and cost-effective object storage service that can store millions of images1. Amazon DynamoDB is a fully managed NoSQL database that can handle high throughput and low latency for key-value and document data2. By using S3 to store the images and DynamoDB to store the geographic codes and image S3 URLs, the solution can achieve high availability and scalability during natural disasters. It can also leverage DynamoDB's features such as caching, auto-scaling, and global tables to improve performance and reduce costs2.

* A. Store the images and geographic codes in a database table Use Oracle running on an Amazon RDS Multi-AZ DB instance. This solution will not meet the requirement of scalability and cost-effectiveness, as Oracle is a relational database that may not handle large volumes of unstructured data such as images efficiently3. It also involves higher licensing and operational costs than S3 and DynamoDB12.

* C. Store the images and geographic codes in an Amazon DynamoDB table Configure DynamoDB Accelerator (DAX) during times of high load. This solution will not meet the requirement of cost-effectiveness, as storing images in DynamoDB will consume more storage space and incur higher charges than storing them in S312. It will also require additional configuration and management of DAX clusters to handle high load.

* D. Store the images in Amazon S3 buckets Store geographic codes and image S3 URLs in a database table Use Oracle running on an Amazon RDS Multi-AZ DB instance. This solution will not meet the requirement of scalability and cost-effectiveness, as Oracle is a relational database that may not handle high throughput and low latency for key-value data such as geographic codes efficiently3. It also involves higher licensing and operational costs than DynamoDB2.

Reference URL: https://dynobase.dev/dynamodb-vs-s3/

340. - (Topic 3)

A company has an API that receives real-time data from a fleet of monitoring devices. The API stores this data in an Amazon RDS DB instance for later analysis. The amount of data that the monitoring devices send to the API fluctuates. During periods of heavy traffic, the API often returns timeout errors.

After an inspection of the logs, the company determines that the database is not capable of processing the volume of write traffic that comes from the API. A solutions architect must minimize the number of connections to the database and must ensure that data is not lost during periods of heavy traffic.

Which solution will meet these requirements?

A. Increase the size of the DB instance to an instance type that has more available memory.

B. Modify the DB instance to be a Multi-AZ DB instance. Configure the application to write to all active RDS DB instances.

C. Modify the API to write incoming data to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function that Amazon SQS invokes to write data from the queue to the database.

D. Modify the API to write incoming data to an Amazon Simple Notification Service (Amazon SNS) topic. Use an AWS Lambda function that Amazon SNS invokes to write data from the topic to the database.

Answer: C

Explanation: Using Amazon SQS will help minimize the number of connections to the database, as the API will write data to a queue instead of directly to the database. Additionally, using an AWS Lambda function that Amazon SQS invokes to write data from the queue to the database will help ensure that data is not lost during periods of heavy traffic, as the queue will serve as a buffer between the API and the database.

341. - (Topic 3)

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

Which Amazon EC2 pricing option is the MOST cost-effective?

A. Dedicated Reserved Hosts

B. Dedicated On-Demand Hosts

C. Dedicated Reserved Instances

D. Dedicated On-Oemand Instances

Answer: A

Explanation:

https://aws.amazon.com/ec2/dedicated-hosts/ Amazon EC2 Dedicated Hosts allow you to use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2, so that you get the flexibility and cost effectiveness of using your own licenses, but with the resiliency, simplicity and elasticity of AWS.

342. - (Topic 3)

A hospital is designing a new application that gathers symptoms from patients. The hospital has decided to use Amazon Simple Queue Service (Amazon SOS) and Amazon Simple Notification Service (Amazon SNS) in the architecture.

A solutions architect is reviewing the infrastructure design Data must be encrypted at test and in transit. Only authorized personnel of the hospital should be able to access the data.

Which combination of steps should the solutions architect take to meet these requirements? (Select TWO.)

A. Turn on server-side encryption on the SQS components Update tie default key policy to restrict key usage to a set of authorized principals.

B. Turn on server-side encryption on the SNS components by using an AWS Key Management Service (AWS KMS) customer managed key Apply a key policy to restrict key usage to a set of authorized principals.

C. Turn on encryption on the SNS components Update the default key policy to restrict key usage to a set of authorized principals. Set a condition in the topic pokey to allow only encrypted connections over TLS.

D. Turn on server-side encryption on the SOS components by using an AWS Key Management Service (AWS KMS) customer managed key Apply a key pokey to restrict key usage to a set of authorized principals. Set a condition in the queue pokey to allow only encrypted connections over TLS.

E. Turn on server-side encryption on the SOS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply an IAM pokey to restrict key usage to a set of authorized principals. Set a condition in the queue pokey to allow only encrypted connections over TLS

Answer: B,D

Explanation:

https://docs.aws.amazon.com/sns/latest/dg/sns-server-side-encryption.html

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-server-side-encryption.html

343. - (Topic 3)

A company has a Microsoft NET application that runs on an on-premises Windows Server Trie application stores data by using an Oracle Database Standard Edition server The company is planning a migration to AWS and wants to minimize development changes while moving the application The AWS application environment should be highly available

Which combination of actions should the company take to meet these requirements? (Select TWO)

A. Refactor the application as serverless with AWS Lambda functions running NET Cote

B. Rehost the application in AWS Elastic Beanstalk with the NET platform in a Multi-AZ deployment

C. Replatform the application to run on Amazon EC2 with the Amazon Linux Amazon Machine Image (AMI)

D. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Amazon DynamoDB in a Multi-AZ deployment

E. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment

Answer: B,E

Explanation:

To minimize development changes while moving the application to AWS and to ensure a high level of availability, the company can rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment. This will allow the application to run in a highly available environment without requiring any changes to the application code.

The company can also use AWS Database Migration Service (AWS DMS) to migrate the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment. This will allow the company to maintain the existing database platform while still achieving a high level of availability.

344. - (Topic 3)

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

Which solution meets these requirements?

A. Use AWS Snowball to migrate data out of the on-premises solution to Amazon S3. Configure on-premises systems to mount the Snowball S3 endpoint to provide local access to the data.

B. Use AWS Snowball Edge to migrate data out of the on-premises solution to Amazon S3.Use the Snowball Edge file interface to provide on-premises systems with local access to the data.

C. Use AWS Storage Gateway and configure a cached volume gateway. Run the Storage Gateway software application on premises and configure a percentage of data to cache locally. Mount the gateway

storage volumes to provide local access to the data.

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

Answer: D

Explanation:

This option is the most efficient because it uses AWS Storage Gateway, which is a service that connects an on-premises software appliance with cloud-based storage to provide seamless integration with data security features between your on-premises IT environment and the AWS storage infrastructure1. It also uses a stored volume gateway, which is a type of volume gateway that stores your primary data locally and asynchronously backs up point-in-time snapshots of your data to Amazon S32. It also runs the Storage Gateway software application on premises and maps the gateway storage volumes to on-premises storage, which enables you to use your existing storage hardware and network infrastructure. It also mounts the gateway storage volumes to provide local access to the data, which ensures that your data is available for low latency access on premises while also getting backed up to AWS. This solution meets the requirement of maintaining local access to all the data while it is backed up on AWS and ensuring that the data backed up on AWS is automatically and securely transferred. Option A is less efficient because it uses AWS Snowball, which is a physical device that lets you transfer large amounts of data into and out of AWS3. However, this does not provide a periodic backup solution, as it requires manual handling and shipping of the device. It also configures on-premises systems to mount the Snowball S3 endpoint to provide local access to the data, which could introduce additional complexity and latency. Option B is less efficient because it uses AWS Snowball Edge, which is a physical device that has onboard storage and compute capabilities for select AWS capabilities. However, this does not provide a periodic backup solution, as it requires manual handling and shipping of the device. It also uses the Snowball Edge file interface to provide on-premises systems with local access to the data, which could introduce additional complexity and latency. Option C is less efficient because it uses AWS Storage Gateway and configures a cached volume gateway, which is a type of volume gateway that stores your primary data in Amazon S3 and retains a copy of frequently accessed data subsets locally. However, this does not provide local access to all the data, as only some data subsets are cached locally. It also configures a percentage of data to cache locally, which could incur higher costs and complexity than using a stored volume gateway.

345. - (Topic 3)

A company hosts a multiplayer gaming application on AWS. The company wants the application to read data with sub-millisecond latency and run one-time queries on historical data.

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

A. Use Amazon RDS for data that is frequently accessed. Run a periodic custom script to export the data to an Amazon S3 bucket.

B. Store the data directly in an Amazon S3 bucket. Implement an S3 Lifecycle policy to move older data to S3 Glacier Deep Archive for long-term storage. Run one-time queries on the data in Amazon S3 by using Amazon Athena

C. Use Amazon DynamoDB with DynamoDB Accelerator (DAX) for data that is frequently accessed. Export the data to an Amazon S3 bucket by using DynamoDB table export. Run one-time queries on the data in Amazon S3 by using Amazon Athena.

D. Use Amazon DynamoDB for data that is frequently accessed Turn on streaming to Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to read the data from Kinesis Data Streams. Store the records in an Amazon S3 bucket.

Answer: C

Explanation:

As they would like to retrieve the data with sub-millisecond, DynamoDB with DAX is the answer.

DynamoDB supports some of the world's largest scale applications by providing consistent, single-digit millisecond response times at any scale. You can build applications with virtually unlimited throughput and storage. https://aws.amazon.com/dynamodb/dax/?nc1=h_ls

346. - (Topic 3)

A company is designing a cloud communications platform that is driven by APIs. The application is hosted on Amazon EC2 instances behind a Network Load Balancer (NLB). The company uses Amazon API Gateway to provide external users with access to the application through APIs. The company wants to protect the platform against web exploits like SQL injection and also wants to detect and mitigate large, sophisticated DDoS attacks.

Which combination of solutions provides the MOST protection? (Select TWO.)

A. Use AWS WAF to protect the NLB.

B. Use AWS Shield Advanced with the NLB.

C. Use AWS WAF to protect Amazon API Gateway.

D. Use Amazon GuardDuty with AWS Shield Standard.

E. Use AWS Shield Standard with Amazon API Gateway.

Answer: B,C

Explanation:

AWS Shield Advanced provides expanded DDoS attack protection for your Amazon EC2 instances, Elastic Load Balancing load balancers, CloudFront distributions, Route 53 hosted zones, and AWS Global Accelerator standard accelerators.

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to your protected web application resources. You can protect

the following resource types:

Amazon CloudFront distribution Amazon API Gateway REST API Application Load Balancer

AWS AppSync GraphQL API Amazon Cognito user pool

https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html

347. - (Topic 3)

A company collects data from thousands of remote devices by using a RESTful web services application that runs on an Amazon EC2 instance. The EC2 instance receives the raw data, transforms the raw data, and stores all the data in an Amazon S3 bucket. The number of remote devices will increase into the millions soon. The company needs a highly scalable solution that minimizes operational overhead.

Which combination of steps should a solutions architect take to meet these requirements9 (Select TWO.)

A. Use AWS Glue to process the raw data in Amazon S3.

B. Use Amazon Route 53 to route traffic to different EC2 instances.

C. Add more EC2 instances to accommodate the increasing amount of incoming data.

D. Send the raw data to Amazon Simple Queue Service (Amazon SOS). Use EC2 instances to process the data.

E. Use Amazon API Gateway to send the raw data to an Amazon Kinesis data stream. Configure Amazon Kinesis Data Firehose to use the data stream as a source to deliver the data to Amazon S3.

Answer: A,E

Explanation:

"RESTful web services" => API Gateway.

"EC2 instance receives the raw data, transforms the raw data, and stores all the data in an Amazon S3 bucket" => GLUE with (Extract - Transform - Load)

348. - (Topic 3)

A company runs a web application on Amazon EC2 instances in multiple Availability Zones. The EC2 instances are in private subnets. A solutions architect implements an internet- facing Application Load Balancer (ALB) and specifies the EC2 instances as the target group. However, the internet traffic is not reaching the EC2 instances.

How should the solutions architect reconfigure the architecture to resolve this issue?

A. Replace the ALB with a Network Load Balancer. Configure a NAT gateway in a public subnet to allow internet traffic.

B. Move the EC2 instances to public subnets. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0.

C. Update the route tables for the EC2 instances' subnets to send 0.0.0.0/0 traffic through the internet gateway route. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0.

D. Create public subnets in each Availability Zone. Associate the public subnets with the ALB. Update the route tables for the public subnets with a route to the private subnets.

Answer: D

Explanation: https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/

349. - (Topic 3)

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

Which solution will meet these requirements?

A. Amazon DynamoDB

B. Amazon RDS for MySQL

C. MySQL-compatible Amazon Aurora Serverless

D. MySQL deployed on Amazon EC2 in an Auto Scaling group

Answer: C

Explanation:

Amazon RDS for MySQL is a fully-managed relational database service that makes it easy to set up, operate, and scale MySQL deployments in the cloud. Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora (MySQL-compatible edition), where the database will automatically start up, shut down, and scale capacity up or down based on your application's needs. It is a simple, cost-effective option for infrequent, intermittent, or unpredictable workloads.

350. - (Topic 3)

A company has deployed a server less application that invokes an AWS Lambda function when new documents are uploaded to an Amazon S3 bucket The application uses the Lambda function to process the documents After a recent marketing campaign the company noticed that the application did not process many of The documents

What should a solutions architect do to improve the architecture of this application?

A. Set the Lambda function's runtime timeout value to 15 minutes

B. Configure an S3 bucket replication policy Stage the documents m the S3 bucket for later processing

C. Deploy an additional Lambda function Load balance the processing of the documents across the two Lambda functions

D. Create an Amazon Simple Queue Service (Amazon SOS) queue Send the requests to the queue Configure the queue as an event source for Lambda.

Answer: D

Explanation:

To improve the architecture of this application, the best solution would be to use Amazon Simple Queue Service (Amazon SQS) to buffer the requests and decouple the S3 bucket from the Lambda function. This will ensure that the documents are not lost and can be processed at a later time if the Lambda function is not available. This will ensure that the documents are not lost and can be processed at a later time if the

Lambda function is not available. By using Amazon SQS, the architecture is decoupled and the Lambda function can process the documents in a scalable and fault-tolerant manner

351. - (Topic 3)

A company hostss a three application on Amazon EC2 instances in a single Availability Zone. The web application uses a self-managed MySQL database that is hosted on an EC2 instances to store data in an Amazon Elastic Block Store (Amazon EBS) volumn. The MySQL database currently uses a 1 TB Provisioned IOPS SSD (io2) EBS volume. The company expects traffic of 1,000 IOPS for both reads and writes at peak traffic.

The company wants to minimize any distruptions, stabilize perperformace, and reduce costs while retaining the capacity for double the IOPS. The company wants to more the database tier to a fully managed solution that is highly available and fault tolerant.

Which solution will meet these requirements MOST cost-effectively?

A. Use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with an io2 Block Express EBS volume.

B. Use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with a General Purpose SSD (gp2) EBS volume.

C. Use Amazon S3 Intelligent-Tiering access tiers.

D. Use two large EC2 instances to host the database in active-passive mode.

Answer: B

Explanation:

RDS supported Storage >

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html GP2 max IOPS >

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general- purpose.html#gp2-performance

Amazon RDS provides three storage types: General Purpose SSD (also known as gp2 and gp3), Provisioned IOPS SSD (also known as io1), and magnetic (also known as standard). They differ in performance characteristics and price, which means that you can tailor your storage performance and cost to the needs of your database workload. You can create MySQL, MariaDB, Oracle, and PostgreSQL RDS DB instances with up to 64 tebibytes (TiB) of storage. You can create SQL Server RDS DB instances with up to 16 TiB of storage. For this amount of storage, use the Provisioned IOPS SSD and General Purpose

SSD storage types. https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

352. - (Topic 3)

A company has deployed a web application on AWS. The company hosts the backend database on Amazon RDS for MySQL with a primary DB instance and five read replicas to support scallng needs. The read replicas must lag no more than 1 second behind the primary DB instance. The database routinely runs scheduled stored procedures.

As traffic on the website increases, the replicas experince addtional lag during periods of peak load. A solutions architect must reduce the replication lag as much as possible. The solutin architect must minimize changes to the application code and must minimize ongoing operational overhead.

Which solution will meet these requirements?

A. Migrate the database to Amazon Aurora MySQL. Replace the read replicas with Aurora Replicas, and configure Aurora Auto Scaling. Replace the store procedures with Aurora MySQL native functions.

B. Deploy an Amazon ElasticCache for Redis cluster in front of the database. Modify the application to check the cache before the applicatin queries the database. Replace the stored procedures with AWS Lambda functions.

C. Migrate the database to a MySQL database that runs on Amazon EC2 instances. Choose large, compute optimized EC2 instances for all replica nodes. Maintain the stored procedures on the EC2 instances.

D. Migrate the database to Amazon DynamicDB provision a large number of read capacity units(RCUs) to support the required throught, and configure on-demand capacity scaling. Replace the store procedures with DynamoDB streams

Answer: A

Explanation:

Option A is the most appropriate solution for reducing replication lag without significant changes to the application code and minimizing ongoing operational overhead. Migrating the database to Amazon Aurora MySQL allows for improved replication performance and higher scalability compared to Amazon RDS for MySQL. Aurora Replicas provide faster replication, reducing the replication lag, and Aurora Auto Scaling ensures that there are enough Aurora Replicas to handle the incoming traffic. Additionally, Aurora MySQL native functions can replace the stored procedures, reducing the load on the database and improving

performance.

353. - (Topic 3)

An ecommerce company needs to run a scheduled daily job to aggregate and filler sales records for analytics. The company stores the sales records in an Amazon S3 bucket. Each object can be up to 10 G6 in size Based on the number of sales events, the job can take up to an hour to complete. The CPU and memory usage of the fob are constant and are known in advance.

A solutions architect needs to minimize the amount of operational effort that is needed for the job to run.

Which solution meets these requirements?

A. Create an AWS Lambda function that has an Amazon EventBridge notification Schedule the EventBridge event to run once a day

B. Create an AWS Lambda function Create an Amazon API Gateway HTTP API, and integrate the API with the function Create an Amazon EventBridge scheduled avert that calls the API and invokes the function.

C. Create an Amazon Elastic Container Service (Amazon ECS) duster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.

D. Create an Amazon Elastic Container Service (Amazon ECS) duster with an Amazon EC2 launch type and an Auto Scaling group with at least one EC2 instance. Create an Amazon EventBridge scheduled event that launches an ECS task on the duster to run the job.

Answer: C

Explanation:

The solution that meets the requirements with the least operational overhead is to create a **Regional AWS WAF web ACL with a rate-based rule** and associate the web ACL with the API Gateway stage. This solution will protect the application from HTTP flood attacks by monitoring incoming requests and blocking requests from IP addresses that exceed the predefined rate. Amazon CloudFront distribution with Lambda@Edge in front of the API Gateway Regional API endpoint is also a good solution but it requires more operational overhead than the previous solution. Using Amazon CloudWatch metrics to monitor the Count metric and alerting the security team when the predefined rate is reached is not a solution that can protect against HTTP flood attacks. Creating an Amazon CloudFront distribution in front of the API Gateway Regional API endpoint with a maximum TTL of 24 hours is not a solution that can protect against HTTP flood attacks.

354. - (Topic 3)

A company uses Amazon EC2 instances and AWS Lambda functions to run its application. The company has VPCs with public subnets and private subnets in its AWS account. The EC2 instances run in a private subnet in one of the VPCs. The Lambda functions need direct network access to the EC2 instances for the application to work.

The application will run for at least 1 year. The company expects the number of Lambda functions that the application uses to increase during that time. The company wants to maximize its savings on all application resources and to keep network latency between the services low.

Which solution will meet these requirements?

A. Purchase on an EC2 instance Savings Plan. Optimize the Lambda functions duration and memory usage and the number of invocations. Connect the Lambda functions to the private subnet that contains the EC2 instances.

B. Purchase on an EC2 instance Savings Plan. Optimize the Lambda functions duration and memory usage and the number of invocation, and the amount of data that is transfered. Connect the Lambda functions to a public subnet in the same VPC where the EC2 instances run.

C. Purchase a Compute Savings Plan. Optimize the Lambda functions duration and memory usage, the number of invocations, and the amount of data that is transferred Connect the Lambda function to the Private subnet that contains the EC2 instances.

D. Purchase a Compute Savings Plan. Optimize the Lambda functions‘ duration and memory usage, the number of invocations, and the amount of data that is transferred Keep the Lambda functions in the Lambda service VPC.

Answer: C

Explanation:

By purchasing a Compute Savings Plan, the company can save on the costs of running both EC2 instances and Lambda functions. The Lambda functions can be connected to the private subnet that contains the EC2 instances through a VPC endpoint for AWS services or a VPC peering connection. This provides direct network access to the EC2 instances while keeping the traffic within the private network, which helps to minimize network latency. Optimizing the Lambda functions’ duration, memory usage, number of invocations, and amount of data transferred can help to further minimize costs and improve performance.

Additionally, using a private subnet helps to ensure that the EC2 instances are not directly accessible from the public internet, which is a security best practice.

355. - (Topic 3)

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

Which solution achieves these goals MOST efficiently?

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

B. Use EC2 Auto Scaling lifecycle hooks to run a custom script to send data to the audit system when instances are launched and terminated

C. Use an EC2 Auto Scaling launch configuration to run a custom script through user data to send data to the audit system when instances are launched and terminated

D. Run a custom script on the instance operating system to send data to the audit system Configure the script to be invoked by the EC2 Auto Scaling group when the instance starts and is terminated

Answer: B

Explanation: Amazon EC2 Auto Scaling offers the ability to add lifecycle hooks to your Auto Scaling groups. These hooks let you create solutions that are aware of events in the Auto Scaling instance lifecycle, and then perform a custom action on instances when the corresponding lifecycle event occurs. (https://docs.aws.amazon.com/autoscaling/ec2/userguide/lifecycle-hooks.html)

356. - (Topic 3)

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

Which solution should a solutions architect recommend?

A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage

B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on- demand for data storage

C. Use a Network Load Balancer for traffic distribution and Amazon Aurora Global Database for data storage

D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage

Answer: B

Explanation:

A Network Load Balancer is a type of load balancer that operates at the connection level (Layer 4) and can load balance both TCP and UDP traffic1. A Network Load Balancer is suitable for scenarios where high performance and low latency are required, such as real- time multiplayer games1. A Network Load Balancer can also handle sudden and volatile traffic patterns while using a single static IP address per Availability Zone1.

To meet the requirements of the scenario, the solutions architect should use a Network Load Balancer for traffic distribution between the EC2 instances in the Auto Scaling group. The Network Load Balancer can route UDP traffic from the client to the servers on the appropriate port2. The Network Load Balancer can also support TLS offloading for secure communications between the client and servers1.

Amazon DynamoDB is a fully managed NoSQL database service that can store and retrieve any amount of data with consistent performance and low latency3. Amazon DynamoDB on-demand is a flexible billing option that requires no capacity planning and charges only for the read and write requests that are performed on the tables3. Amazon DynamoDB on-demand is ideal for scenarios where the application traffic is unpredictable or sporadic, such as gaming applications3.

To meet the requirements of the scenario, the solutions architect should use Amazon DynamoDB on-demand for data storage. Amazon DynamoDB on-demand can store gamer scores and other non-relational data without intervention from the developers. Amazon DynamoDB on-demand can also scale automatically to handle any level of request traffic without affecting performance or availability3.

357. - (Topic 3)

A company has an Amazon S3 data lake that is governed by AWS Lake Formation The company wants to

create a visualization in Amazon QuickSight by joining the data in the data lake with operational data that is stored in an Amazon Aurora MySQL database The company wants to enforce column-level authorization so that the company's marketing team can access only a subset of columns in the database

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

A. Use Amazon EMR to ingest the data directly from the database to the QuickSight SPICE engine Include only the required columns

B. Use AWS Glue Studio to ingest the data from the database to the S3 data lake Attach an IAM policy to the QuickSight users to enforce column-level access control. Use Amazon S3 as the data source in QuickSight

C. Use AWS Glue Elastic Views to create a materialized view for the database in Amazon S3 Create an S3 bucket policy to enforce column-level access control for the QuickSight users Use Amazon S3 as the data source in QuickSight.

D. Use a Lake Formation blueprint to ingest the data from the database to the S3 data lake Use Lake Formation to enforce column-level access control for the QuickSight users Use Amazon Athena as the data source in QuickSight

Answer: D

Explanation: Enforce column-level authorization with Amazon QuickSight and AWS Lake Formation

https://aws.amazon.com/blogs/big-data/enforce-column-level-authorization-with-amazon-quicksight-and-aws-lake-formation/

Topic 4, Exam Pool D

358. - (Topic 4)

A company is deploying a new public web application toAWS. The application Will run behind an Application Load Balancer (ALE). 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 SSUTLS certificate. Apply the certificate to the ALB Use the managed renewal feature to automatically rotate the certificate.

B. Use AWS Certificate Manager (ACM) to issue an SSUTLS certificate_ Import the key material from the

certificate. Apply the certificate to the ALB Use the managed

renewal teature to automatically rotate the certificate.

C. Use AWS Private Certificate Authority to issue an SSL/TLS certificate from the root CA. Apply the certificate to the ALB. use the managed renewal feature to automatically rotate the certificate

D. Use AWS Certificate Manager (ACM) to import an SSL/TLS certificate. Apply the certificate to the ALB_ Use Amazon EventBridge to send a notification when the certificate is nearing expiration. Rotate the certificate manually.

Answer: D

Explanation: To use an SSL/TLS certificate that is issued by an external CA, the certificate must be imported to AWS Certificate Manager (ACM). ACM can send a notification when the certificate is nearing expiration, but it cannot automatically rotate the certificate. Therefore, the certificate must be rotated manually by importing a new certificate and applying it to the ALB.

References:

- Importing Certificates into AWS Certificate Manager
- Renewing and Rotating Imported Certificates
- Using an ACM Certificate with an Application Load Balancer

359. - (Topic 4)

A company is using AWS Key Management Service (AWS KMS) keys to encrypt AWS Lambda environment variables. A solutions architect needs to ensure that the required permissions are in place to decrypt and use the environment variables.

Which steps must the solutions architect take to implement the correct permissions? (Choose two.)

A. Add AWS KMS permissions in the Lambda resource policy.

B. Add AWS KMS permissions in the Lambda execution role.

C. Add AWS KMS permissions in the Lambda function policy.

D. Allow the Lambda execution role in the AWS KMS key policy.

E. Allow the Lambda resource policy in the AWS KMS key policy.

Answer: B,D

Explanation: B and D are the correct answers because they ensure that the Lambda execution role has the permissions to decrypt and use the environment variables, and that the AWS KMS key policy allows the

Lambda execution role to use the key. The Lambda execution role is an IAM role that grants the Lambda function permission to access AWS resources, such as AWS KMS. The AWS KMS key policy is a resource-based policy that controls access to the key. By adding AWS KMS permissions in the Lambda execution role and allowing the Lambda execution role in the AWS KMS key policy, the solutions architect can implement the correct permissions for encrypting and decrypting environment variables. References:

- AWS Lambda Execution Role
- Using AWS KMS keys in AWS Lambda

360. - (Topic 4)

The DNS provider that hosts a company's domain name records is experiencing outages that cause service disruption for a website running on AWS. The company needs to

migrate to a more resilient managed DNS service and wants the service to run on AWS. What should a solutions architect do to rapidly migrate the DNS hosting service?

A. Create an Amazon Route 53 public hosted zone for the domain name. Import the zone file containing the domain records hosted by the previous provider

B. Create an Amazon Route 53 private hosted zone for the domain name Import the zone file containing the domain records hosted by the previous provider.

C. Create a Simple AD directory in AWS. Enable zone transfer between the DNS provider and AWS Directory Service for Microsoft Active Directory for the domain records.

D. Create an Amazon Route 53 Resolver inbound endpomt in the VPC. Specify the IP addresses that the provider's DNS will forward DNS queries to. Configure the provider's DNS to forward DNS queries for the domain to the IP addresses that are specified in the inbound endpoint.

Answer: A

Explanation: To migrate the DNS hosting service to a more resilient managed DNS service on AWS, the company should use Amazon Route 53, which is a highly available and scalable cloud DNS web service. Route 53 can host public DNS records for the company’s domain name and provide reliable and secure DNS resolution. To rapidly migrate the DNS hosting service, the company should create a public hosted zone for the domain name in Route 53, which is a container for the domain’s DNS records. Then, the company should import the zone file containing the domain records hosted by the previous provider, which is a text file that defines the DNS records for the domain. This way, the company can quickly transfer the

existing DNS records to Route 53 without manually creating them. After importing the zone file, the company should update the domain registrar to use the name servers that Route 53 assigns to the hosted zone. This will ensure that DNS queries for the domain name are routed to Route 53 and resolved by the imported records.

361. - (Topic 4)

A company uses Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS) volumes to run an application. The company creates one snapshot of each EBS volume every day to meet compliance requirements. The company wants to implement an architecture that prevents the accidental deletion of EBS volume snapshots. The solution must not change the administrative rights of the storage administrator user.

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

A. Create an 1AM role that has permission to delete snapshots. Attach the role to a new EC2 instance. Use the AWS CLI from the new EC2 instance to delete snapshots.

B. Create an 1AM policy that denies snapshot deletion. Attach the policy to the storage administrator user.

C. Add tags to the snapshots. Create retention rules in Recycle Bin for EBS snapshots that have the tags.

D. Lock the EBS snapshots to prevent deletion.

Answer: D

Explanation: EBS snapshots are point-in-time backups of EBS volumes that can be used to restore data or create new volumes. EBS snapshots can be locked to prevent accidental deletion using a feature called EBS Snapshot Lock. When a snapshot is locked, it cannot be deleted by any user, including the root user, until it is unlocked. The lock policy can also specify a retention period, after which the snapshot can be deleted. This solution will meet the requirements with the least administrative effort, as it does not require any code development or policy changes.

References:

- 1 explains how to lock and unlock EBS snapshots using EBS Snapshot Lock.
- 2 describes the concept and benefits of EBS snapshots.

362. - (Topic 4)

A company is running a legacy system on an Amazon EC2 instance. The application code cannot be modified, and the system cannot run on more than one instance. A solutions architect must design a resilient solution that can improve the recovery time for the system.

What should the solutions architect recommend to meet these requirements?

A. Enable termination protection for the EC2 instance.

B. Configure the EC2 instance for Multi-AZ deployment.

C. Create an Amazon CloudWatch alarm to recover the EC2 instance in case of failure.

D. Launch the EC2 instance with two Amazon Elastic Block Store (Amazon EBS) volumes that use RAID configurations for storage redundancy.

Answer: C

Explanation:

To design a resilient solution that can improve the recovery time for the system, a solutions architect should recommend creating an Amazon CloudWatch alarm to recover the EC2 instance in case of failure. This solution has the following benefits:

- It allows the EC2 instance to be automatically recovered when a system status check failure occurs, such as loss of network connectivity, loss of system power, software issues on the physical host, or hardware issues on the physical host that impact network reachability1.
- It preserves the instance ID, private IP addresses, Elastic IP addresses, and all instance metadata of the original instance. A recovered instance is identical to the original instance, except for any data that is in-memory, which is lost during the recovery process1.
- It does not require any modification of the application code or the EC2 instance configuration. The solutions architect can create a CloudWatch alarm using the AWS Management Console, the AWS CLI, or the CloudWatch API2.

References:

- 1: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance- recover.html
- 2: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html#ec2-instance-recover-create-alarm

363. - (Topic 4)

A company needs to retain its AWS CloudTrail logs for 3 years. The company is enforcing CloudTrail

across a set of AWS accounts by using AWS Organizations from the parent account. The CloudTrail target S3 bucket is configured with S3 Versioning enabled. An S3 Lifecycle policy is in place to delete current objects after 3 years.

After the fourth year of use of the S3 bucket, the S3 bucket metrics show that the number of objects has continued to rise. However, the number of new CloudTrail logs that are delivered to the S3 bucket has remained consistent.

Which solution will delete objects that are older than 3 years in the MOST cost-effective manner?

A. Configure the organization's centralized CloudTrail trail to expire objects after 3 years.

B. Configure the S3 Lifecycle policy to delete previous versions as well as current versions.

C. Create an AWS Lambda function to enumerate and delete objects from Amazon S3 that are older than 3 years.

D. Configure the parent account as the owner of all objects that are delivered to the S3 bucket.

Answer: B

Explanation: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html#:~:text=The%20CloudTrail%20trail,time%20has%20passed.

364. - (Topic 4)

A company is designing the network for an online multi-player game. The game uses the UDP networking protocol and will be deployed in eight AWS Regions. The network architecture needs to minimize latency and packet loss to give end users a high-quality gaming experience.

Which solution will meet these requirements?

A. Set up a transit gateway in each Region. Create inter-Region peering attachments between each transit gateway.

B. Set up AWS Global Accelerator with UDP listeners and endpoint groups in each Region.

C. Set up Amazon CloudFront with UDP turned on. Configure an origin in each Region.

D. Set up a VPC peering mesh between each Region. Turn on UDP for each VPC.

Answer: B

Explanation: The best solution for this situation is option B, setting up AWS Global Accelerator with UDP listeners and endpoint groups in each Region. AWS Global Accelerator is a networking service that improves the availability and performance of internet applications by routing user requests to the nearest

AWS Region [1]. It also improves the performance of UDP applications by providing faster, more reliable data transfers with lower latency and fewer packet losses. By setting up UDP listeners and endpoint groups in each Region, Global Accelerator will route traffic to the nearest Region for faster response times and a better user experience.

365. - (Topic 4)

A company wants to implement a backup strategy for Amazon EC2 data and multiple Amazon S3 buckets. Because of regulatory requirements, the company must retain backup files for a specific time period. The company must not alter the files for the duration of the retention period.

Which solution will meet these requirements?

A. Use AWS Backup to create a backup vault that has a vault lock in governance mode. Create the required backup plan.

B. Use Amazon Data Lifecycle Manager to create the required automated snapshot policy.

C. Use Amazon S3 File Gateway to create the backup. Configure the appropriate S3 Lifecycle management.

D. Use AWS Backup to create a backup vault that has a vault lock in compliance mode. Create the required backup plan.

Answer: D

Explanation: AWS Backup is a fully managed service that allows you to centralize and automate data protection of AWS services across compute, storage, and database. AWS Backup Vault Lock is an optional feature of a backup vault that can help you enhance the security and control over your backup vaults. When a lock is active in Compliance mode and the grace time is over, the vault configuration cannot be altered or deleted by a customer, account/data owner, or AWS. This ensures that your backups are available for you until they reach the expiration of their retention periods and meet the regulatory requirements. References: https://docs.aws.amazon.com/aws- backup/latest/devguide/vault-lock.html

366. - (Topic 4)

A company plans to migrate toAWS and use Amazon EC2 On-Demand Instances for its application. During the migration testing phase, a technical team observes that the application takes a long time to launch and load memory to become fully productive.

Which solution will reduce the launch time of the application during the next testing phase?

A. Launch two or more EC2 On-Demand Instances. Turn on auto scaling features and make the EC2 On-Demand Instances available during the next testing phase.

B. Launch EC2 Spot Instances to support the application and to scale the application so it is available during the next testing phase.

C. Launch the EC2 On-Demand Instances with hibernation turned on. Configure EC2 Auto Scaling warm pools during the next testing phase.

D. Launch EC2 On-Demand Instances with Capacity Reservations. Start additional EC2 instances during the next testing phase.

Answer: C

Explanation: The solution that will reduce the launch time of the application during the next testing phase is to launch the EC2 On-Demand Instances with hibernation turned on and configure EC2 Auto Scaling warm pools. This solution allows the application to resume from a hibernated state instead of starting from scratch, which can save time and resources. Hibernation preserves the memory (RAM) state of the EC2 instances to the root EBS volume and then stops the instances. When the instances are resumed, they restore their memory state from the EBS volume and become productive quickly. EC2 Auto Scaling warm pools can be used to maintain a pool of pre-initialized instances that are ready to scale out when needed. Warm pools can also support hibernated instances, which can further reduce the launch time and cost of scaling out. The other solutions are not as effective as the first one because they either do not reduce the launch time, do not guarantee availability, or do not use On-Demand Instances as required. Launching two or more EC2 On-Demand Instances with auto scaling features does not reduce the launch time of the application, as each instance still has to go through the initialization process. Launching EC2 Spot Instances does not guarantee availability, as Spot Instances can be interrupted by AWS at any time when there is a higher demand for capacity. Launching EC2 On-Demand Instances with Capacity Reservations does not reduce the launch time of the application, as it only ensures that there is enough capacity available for the instances, but does not pre-initialize them.

References:

- Hibernating your instance - Amazon Elastic Compute Cloud
- Warm pools for Amazon EC2 Auto Scaling - Amazon EC2 Auto Scaling

367. - (Topic 4)

A company stores data in PDF format in an Amazon S3 bucket The company must follow a legal requirement to retain all new and existing data in Amazon S3 for 7 years.

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

A. Turn on the S3 Versionmg feature for the S3 bucket Configure S3 Lifecycle to delete the data after 7 years. Configure multi-factor authentication (MFA) delete for all S3 objects.

B. Turn on S3 Object Lock with governance retention mode for the S3 bucket Set the retention period to expire after 7 years. Recopy all existing objects to bring the existing data into compliance

C. Turn on S3 Object Lock with compliance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Recopy all existing objects to bring the existing data into compliance

D. Turn on S3 Object Lock with compliance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Use S3 Batch Operations to bring the existing data into compliance

Answer: C

Explanation: S3 Object Lock enables a write-once-read-many (WORM) model for objects stored in Amazon S3. It can help prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely1. S3 Object Lock has two retention modes: governance mode and compliance mode. Compliance mode provides the highest level of protection and prevents any user, including the root user, from deleting or modifying an object version until the retention period expires. To use S3 Object Lock, a new bucket with Object Lock enabled must be created, and a default retention period can be optionally configured for objects placed in the bucket2. To bring existing objects into compliance, they must be recopied into the bucket with a retention period specified.

Option A is incorrect because S3 Versioning and S3 Lifecycle do not provide WORM protection for objects. Moreover, MFA delete only applies to deleting object versions, not modifying them.

Option B is incorrect because governance mode allows users with special permissions to override or remove the retention settings or delete the object if necessary. This does not meet the legal requirement of retaining all data for 7 years.

Option D is incorrect because S3 Batch Operations cannot be used to apply compliance mode retention periods to existing objects. S3 Batch Operations can only apply governance mode retention periods or legal holds. Reference URL: 2: https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-console.html 3:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html#sc-dynamic-data-access 4:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration.html 1:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html :

https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html :

https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-managing.html :

https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/

368. - (Topic 4)

A company hosts a database that runs on an Amazon RDS instance that is deployed to multiple Availability Zones. The company periodically runs a script against the database to report new entries that are added to the database. The script that runs against the database negatively affects the performance of a critical application. The company needs to improve application performance with minimal costs.

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

A. Add functionality to the script to identify the instance that has the fewest active connections. Configure the script to read from that instance to report the total new entries.

B. Create a read replica of the database. Configure the script to query only the read replica to report the total new entries.

C. Instruct the development team to manually export the new entries for the day in the database at the end of each day.

D. Use Amazon ElastiCache to cache the common queries that the script runs against the database.

Answer: B

Explanation: A read replica is a copy of the primary database that supports read-only queries. By creating a read replica, you can offload the read workload from the primary database and improve its performance. The script can query the read replica without affecting the critical application that uses the primary database. This solution also has the least operational overhead, as you do not need to modify the script, export the data manually, or manage a cache cluster. References:

- Working with PostgreSQL, MySQL, and MariaDB Read Replicas
- Amazon RDS Performance Insights

369. - (Topic 4)

A company wants lo build a web application on AWS. Client access requests to the website are not predictable and can be idle for a long time. Only customers who have paid a subscription fee can have the ability to sign in and use the web application.

Which combination of steps will meet these requirements MOST cost-effectively? (Select THREE.)

A. Create an AWS Lambda function to retrieve user information from Amazon DynamoDB. Create an Amazon API Gateway endpoint to accept RESTful APIs. Send the API calls to the Lambda function.

B. Create an Amazon Elastic Container Service (Amazon ECS) service behind an Application Load Balancer to retrieve user information from Amazon RDS. Create an Amazon API Gateway endpoint to accept RESTful APIs. Send the API calls to the Lambda function.

C. Create an Amazon Cogmto user pool to authenticate users

D. Create an Amazon Cognito identity pool to authenticate users.

E. Use AWS Amplify to serve the frontend web content with HTML. CSS, and JS. Use an integrated Amazon CloudFront configuration.

F. Use Amazon S3 static web hosting with PHP. CSS. and JS. Use Amazon CloudFront to serve the frontend web content.

Answer: A,C,E

Explanation:

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

370. - (Topic 4)

A pharmaceutical company is developing a new drug. The volume of data that the company generates has grown exponentially over the past few months. The company's researchers regularly require a subset of the entire dataset to be immediately available with minimal lag. However the entire dataset does not need to be accessed on a daily basis. All the data currently resides in on-premises storage arrays, and the company wants to reduce ongoing capital expenses.

Which storage solution should a solutions architect recommend to meet these requirements?

A. Run AWS DataSync as a scheduled cron job to migrate the data to an Amazon S3 bucket on an ongoing basis.

B. Deploy an AWS Storage Gateway file gateway with an Amazon S3 bucket as the target storage Migrate the data to the Storage Gateway appliance.

C. Deploy an AWS Storage Gateway volume gateway with cached volumes with an Amazon S3 bucket as the target storage. Migrate the data to the Storage Gateway appliance.

D. Configure an AWS Site-to-Site VPN connection from the on-premises environment to AWS. Migrate data to an Amazon Elastic File System (Amazon EFS) file system.

Answer: C

Explanation: AWS Storage Gateway is a hybrid cloud storage service that allows you to seamlessly integrate your on-premises applications with AWS cloud storage. Volume Gateway is a type of Storage Gateway that presents cloud-backed iSCSI block storage volumes to your on-premises applications. Volume Gateway operates in either cache mode or stored mode. In cache mode, your primary data is stored in Amazon S3, while retaining your frequently accessed data locally in the cache for low latency access. In stored mode, your primary data is stored locally and your entire dataset is available for low latency access on premises while also asynchronously getting backed up to Amazon S3.

For the pharmaceutical company's use case, cache mode is the most suitable option, as it meets the following requirements:

- It reduces the need to scale the on-premises storage infrastructure, as most of the data is stored in Amazon S3, which is scalable, durable, and cost-effective.
- It provides low latency access to the subset of the data that the researchers regularly require, as it is cached locally in the Storage Gateway appliance.
- It does not require the entire dataset to be accessed on a daily basis, as it is stored in Amazon S3 and can be retrieved on demand.
- It offers flexible data protection and recovery options, as it allows taking point-in- time copies of the volumes using AWS Backup, which are stored in AWS as Amazon EBS snapshots.

Therefore, the solutions architect should recommend deploying an AWS Storage Gateway volume gateway with cached volumes with an Amazon S3 bucket as the target storage and migrating the data to the Storage Gateway appliance.

References:

- Volume Gateway | Amazon Web Services
- How Volume Gateway works (architecture) - AWS Storage Gateway

⇨ AWS Storage Volume Gateway - Cached volumes - Stack Overflow

371. - (Topic 4)

A company manages its own Amazon EC2 instances that run MySQL databases. The company is manually managing replication and scaling as demand increases or decreases. The company needs a new solution that simplifies the process of adding or removing compute capacity to or from its database tier as needed. The solution also must offer improved performance, scaling, and durability with minimal effort from operations.

Which solution meets these requirements?

A. Migrate the databases to Amazon Aurora Serverless for Aurora MySQL.

B. Migrate the databases to Amazon Aurora Serverless for Aurora PostgreSQL.

C. Combine the databases into one larger MySQL database. Run the larger database on larger EC2 instances.

D. Create an EC2 Auto Scaling group for the database tier. Migrate the existing databases to the new environment.

Answer: A

Explanation: https://aws.amazon.com/rds/aurora/serverless/

372. - (Topic 4)

An online retail company has more than 50 million active customers and receives more than 25,000 orders each day. The company collects purchase data for customers and stores this data in Amazon S3. Additional customer data is stored in Amazon RDS.

The company wants to make all the data available to various teams so that the teams can perform analytics. The solution must provide the ability to manage fine-grained permissions for the data and must minimize operational overhead.

Which solution will meet these requirements?

A. Migrate the purchase data to write directly to Amazon RDS. Use RDS access controls to limit access.

B. Schedule an AWS Lambda function to periodically copy data from Amazon RDS to Amazon S3. Create an AWS Glue crawler. Use Amazon Athena to query the data. Use S3 policies to limit access.

C. Create a data lake by using AWS Lake Formation. Create an AWS Glue JDBC connection to Amazon RDS. Register the S3 bucket in Lake Formation. Use Lake Formation access controls to limit access.

D. Create an Amazon Redshift cluster. Schedule an AWS Lambda function to periodically copy data from Amazon S3 and Amazon RDS to Amazon Redshift. Use Amazon Redshift access controls to limit access.

Answer: C

Explanation:

https://aws.amazon.com/blogs/big-data/manage-fine-grained-access-control-using-aws-lake-formation/

373. - (Topic 4)

A company runs a microservice-based serverless web application. The application must be able to retrieve data from multiple Amazon DynamoDB tables. A solutions architect needs to give the application the ability to retrieve the data with no impact on the baseline performance of the application.

Which solution will meet these requirements in the MOST operationally efficient way?

A. AWSAppSync pipeline resolvers

B. Amazon CloudFront with Lambda@Edge functions

C. Edge-optimized Amazon API Gateway with AWS Lambda functions

D. Amazon Athena Federated Query with a DynamoDB connector

Answer: C

Explanation: An edge-optimized API Gateway is a way to create RESTful APIs that can access multiple DynamoDB tables through AWS Lambda functions. The edge-optimized API Gateway provides low latency and high performance by caching API responses at CloudFront edge locations. The AWS Lambda functions can use the AWS SDK to query or scan the DynamoDB tables and return the data to the API Gateway. This solution meets all the requirements of the question, while the other options do not.

References:

- https://aws.amazon.com/blogs/compute/understanding-database-options-for-your-serverless-web-applications/
- https://aws.amazon.com/getting-started/hands-on/build-serverless-web-app-lambda-apigateway-s3-dynamodb-cognito/module-3/
- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/best- practices.html

374. - (Topic 4)

A company's compliance team needs to move its file shares to AWS. The shares run on a Windows Server SMB file share. A self-managed on-premises Active Directory controls access to the files and folders.

The company wants to use Amazon FSx for Windows File Server as part of the solution. The company must ensure that the on-premises Active Directory groups restrict access to the FSx for Windows File Server SMB compliance shares, folders, and files after the move to AWS. The company has created an FSx for Windows File Server file system.

Which solution will meet these requirements?

A. Create an Active Directory Connector to connect to the Active Directory. Map the Active Directory groups to IAM groups to restrict access.

B. Assign a tag with a Restrict tag key and a Compliance tag value. Map the Active Directory groups to IAM groups to restrict access.

C. Create an IAM service-linked role that is linked directly to FSx for Windows File Server to restrict access.

D. Join the file system to the Active Directory to restrict access.

Answer: D

Explanation:

Joining the FSx for Windows File Server file system to the on-premises Active Directory will allow the company to use the existing Active Directory groups to restrict access to the file shares, folders, and files after the move to AWS. This option allows the company to continue using their existing access controls and management structure, making the transition to AWS more seamless.

375. - (Topic 4)

A company is developing an application that will run on a production Amazon Elastic Kubernetes Service (Amazon EKS) cluster The EKS cluster has managed node groups that are provisioned with On-Demand Instances.

The company needs a dedicated EKS cluster for development work. The company will use the development cluster infrequently to test the resiliency of the application. The EKS cluster must manage all the nodes.

Which solution will meet these requirements MOST cost-effectively?

A. Create a managed node group that contains only Spot Instances.

B. Create two managed node groups. Provision one node group with On-Demand Instances. Provision the second node group with Spot Instances.

C. Create an Auto Scaling group that has a launch configuration that uses Spot Instances. Configure the user data to add the nodes to the EKS cluster.

D. Create a managed node group that contains only On-Demand Instances.

Answer: A

Explanation: Spot Instances are EC2 instances that are available at up to a 90% discount compared to On-Demand prices. Spot Instances are suitable for stateless, fault-tolerant, and flexible workloads that can tolerate interruptions. Spot Instances can be reclaimed by EC2 when the demand for On-Demand capacity increases, but they provide a two-minute warning before termination. EKS managed node groups automate the provisioning and lifecycle management of nodes for EKS clusters. Managed node groups can use Spot Instances to reduce costs and scale the cluster based on demand. Managed node groups also support features such as Capacity Rebalancing and Capacity Optimized allocation strategy to improve the availability and resilience of Spot Instances. This solution will meet the requirements most cost-effectively, as it leverages the lowest-priced EC2 capacity and does not require any manual intervention.

References:

- 1 explains how to create and use managed node groups with EKS.
- 2 describes how to use Spot Instances with managed node groups.
- 3 provides an overview of Spot Instances and their benefits.

376. - (Topic 4)

A company has an application that uses an Amazon DynamoDB table for storage. A solutions architect discovers that many requests to the table are not returning the latest data. The company's users have not reported any other issues with database performance. Latency is in an acceptable range.

Which design change should the solutions architect recommend?

A. Add read replicas to the table.

B. Use a global secondary index (GSI).

C. Request strongly consistent reads for the table.

D. Request eventually consistent reads for the table.

Answer: C

Explanation: The most suitable design change for the company's application is to request strongly consistent reads for the table. This change will ensure that the requests to the table return the latest data, reflecting the updates from all prior write operations.

Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB supports two types of read consistency: eventually consistent reads and strongly consistent reads. By default, DynamoDB uses eventually consistent reads, unless users specify otherwise1. Eventually consistent reads are reads that may not reflect the results of a recently completed write operation. The response might not include the changes because of the latency of propagating the data to all replicas. If users repeat their read request after a short time, the response should return the updated data. Eventually consistent reads are suitable for applications that do not require up-to-date data or can tolerate eventual consistency1.

Strongly consistent reads are reads that return a result that reflects all writes that received a successful response prior to the read. Users can request a strongly consistent read by setting the ConsistentRead parameter to true in their read operations, such as GetItem, Query, or Scan. Strongly consistent reads are suitable for applications that require up-to- date data or cannot tolerate eventual consistency1.

The other options are not correct because they do not address the issue of read consistency or are not relevant for the use case. Adding read replicas to the table is not correct because this option is not supported by DynamoDB. Read replicas are copies of a primary database instance that can serve read-only traffic and improve availability and performance. Read replicas are available for some relational database services, such as Amazon RDS or Amazon Aurora, but not for DynamoDB2. Using a global secondary index (GSI) is not correct because this option is not related to read consistency. A GSI is an index that has a partition key and an optional sort key that are different from those on the base table. A GSI allows users to query the data in different ways, with eventual consistency3. Requesting eventually consistent reads for the table is not correct because this option is already the default behavior of DynamoDB and does not solve the problem of requests not returning the latest data.

References:

- Read consistency - Amazon DynamoDB
- Working with read replicas - Amazon Relational Database Service
- Working with global secondary indexes - Amazon DynamoDB

377. - (Topic 4)

A company has an application that delivers on-demand training videos to students around the world. The application also allows authorized content developers to upload videos. The data is stored in an Amazon S3 bucket in the us-east-2 Region.

The company has created an S3 bucket in the eu-west-2 Region and an S3 bucket in the ap-southeast-1 Region. The company wants to replicate the data to the new S3 buckets. The company needs to minimize latency for developers who upload videos and students who stream videos near eu-west-2 and ap-southeast-1.

Which combination of steps will meet these requirements with the FEWEST changes to the application? (Select TWO.)

A. Configure one-way replication from the us-east-2 S3 bucket to the eu-west-2 S3 bucket. Configure one-way replication from the us-east-2 S3 bucket to the ap-southeast-1 S3 bucket.

B. Configure one-way replication from the us-east-2 S3 bucket to the eu-west-2 S3 bucket. Configure one-way replication from the eu-west-2 S3 bucket to the ap-southeast-1 S3 bucket.

C. Configure two-way (bidirectional) replication among the S3 buckets that are in all three Regions.

D. Create an S3 Multi-Region Access Point. Modify the application to use the Amazon Resource Name (ARN) of the Multi-Region Access Point for video streaming. Do not modify the application for video uploads.

E. Create an S3 Multi-Region Access Point Modify the application to use the Amazon Resource Name (ARN) of the Multi-Region Access Point for video streaming and uploads.

Answer: A,E

Explanation: These two steps will meet the requirements with the fewest changes to the application because they will enable the company to replicate the data to the new S3 buckets and minimize latency for both video streaming and uploads. One-way replication from the us-east-2 S3 bucket to the other two S3 buckets will ensure that the data is synchronized across all three regions. The company can use S3 Cross-Region Replication (CRR) to automatically copy objects across buckets in different AWS Regions. CRR can help the company achieve lower latency and compliance requirements by keeping copies of their data in different regions. Creating an S3 Multi-Region Access Point and modifying the application to use its ARN will allow the company to access the data through a single global endpoint. An S3 Multi-Region Access Point is a globally unique name that can be used to access objects stored in S3 buckets across

multiple regions. It automatically routes requests to the closest S3 bucket with the lowest latency. By using an S3 Multi-Region Access Point, the company can simplify the application architecture and improve the performance and reliability of the application.

References:

- Replicating objects
- Multi-Region Access Points in Amazon S3

378. - (Topic 4)

A company uses AWS Organizations with all features enabled and runs multiple Amazon EC2 workloads in the ap-southeast-2 Region. The company has a service control policy (SCP) that prevents any resources from being created in any other Region. A security policy requires the company to encrypt all data at rest. An audit discovers that employees have created Amazon Elastic Block Store (Amazon EBS) volumes for EC2 instances without encrypting the volumes. The company wants any new EC2 instances that any 1AM user or root user launches in ap-southeast-2 to use encrypted EBS volumes. The company wants a solution that will have minimal effect on employees who create EBS volumes.

Which combination of steps will meet these requirements? (Select TWO.)

A. In the Amazon EC2 console, select the EBS encryption account attribute and define a default encryption key.

B. Create an 1AM permission boundary. Attach the permission boundary to the root organizational unit (OU). Define the boundary to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false.

C. Create an SCR Attach the SCP to the root organizational unit (OU). Define the SCP to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false.

D. Update the 1AM policies for each account to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false.

E. In the Organizations management account, specify the Default EBS volume encryption setting.

Answer: C

Explanation: A service control policy (SCP) is a type of policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control

guidelines. You can use an SCP to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false, which means that any user or role in the accounts under the root OU will not be able to create unencrypted EBS volumes. This solution will have minimal effect on employees who create EBS volumes, as they can still create encrypted volumes as needed. References:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps. html

379. - (Topic 4)

A company runs a website that stores images of historical events. Website users need the ability to search and view images based on the year that the event in the image occurred. On average, users request each image only once or twice a year The company wants a highly available solution to store and deliver the images to users.

Which solution will meet these requirements MOST cost-effectively?

A. Store images in Amazon Elastic Block Store (Amazon EBS). Use a web server that runs on Amazon EC2_

B. Store images in Amazon Elastic File System (Amazon EFS). Use a web server that runs on Amazon EC2.

C. Store images in Amazon S3 Standard. use S3 Standard to directly deliver images by using a static website.

D. Store images in Amazon S3 Standard-InfrequentAccess (S3 Standard-IA). use S3 Standard-IA to directly deliver images by using a static website.

Answer: C

Explanation: it allows the company to store and deliver images to users in a highly available and cost-effective way. By storing images in Amazon S3 Standard, the company can use a durable, scalable, and secure object storage service that offers high availability and performance. By using S3 Standard to directly deliver images by using a static website, the company can avoid running web servers and reduce operational overhead. S3 Standard also offers low storage pricing and free data transfer within AWS Regions. References:

- Amazon S3 Storage Classes
- Hosting a Static Website on Amazon S3

380. - (Topic 4)

A solutions architect has created a new AWS account and must secure AWS account root user access. Which combination of actions will accomplish this? (Choose two.)

A. Ensure the root user uses a strong password.

B. Enable multi-factor authentication to the root user.

C. Store root user access keys in an encrypted Amazon S3 bucket.

D. Add the root user to a group containing administrative permissions.

E. Apply the required permissions to the root user with an inline policy document.

Answer: A,B

Explanation: https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html https://docs.aws.amazon.com/accounts/latest/reference/best-practices-root-user.html * Enable AWS multi-factor authentication (MFA) on your AWS account root user. For more information, see Using multi-factor authentication (MFA) in AWS in the IAM User Guide. * Never share your AWS account root user password or access keys with anyone. * Use a strong password to help protect access to the AWS Management Console. For information about managing your AWS account root user password, see Changing the password for the root user.

381. - (Topic 4)

A company has stored 10 TB of log files in Apache Parquet format in an Amazon S3 bucket The company occasionally needs to use SQL to analyze the log files Which solution will meet these requirements MOST cost-effectively?

A. Create an Amazon Aurora MySQL database Migrate the data from the S3 bucket into Aurora by using AWS Database Migration Service (AWS DMS) Issue SQL statements to the Aurora database.

B. Create an Amazon Redshift cluster Use Redshift Spectrum to run SQL statements directly on the data in the S3 bucket

C. Create an AWS Glue crawler to store and retrieve table metadata from the S3 bucket Use Amazon Athena to run SQL statements directly on the data in the S3 bucket

D. Create an Amazon EMR cluster Use Apache Spark SQL to run SQL statements directly on the data in the S3 bucket

Answer: C

Explanation: AWS Glue is a serverless data integration service that can crawl, catalog, and prepare data for analysis. AWS Glue can automatically discover the schema and partitioning of the data stored in Apache Parquet format in S3, and create a table in the AWS Glue Data Catalog. Amazon Athena is a serverless interactive query service that can run SQL queries directly on data in S3, without requiring any data loading or transformation. Athena can use the table metadata from the AWS Glue Data Catalog to query the data in S3. By using AWS Glue and Athena, you can analyze the log files in S3 most cost-effectively, as you only pay for the resources consumed by the crawler and the queries, and you do not need to provision or manage any servers or clusters.

References:

- AWS Glue
- Amazon Athena
- Analyzing Data in S3 using Amazon Athena

382. - (Topic 4)

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

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

A. Create an Auto Scaling group and a load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.

B. Create an AWS CloudFormation template to create EC2 instances, load balancers, and DynamoDB tables to be launched when needed. Configure DNS failover to point to the new disaster recovery Region's load balancer.

C. Create an AWS CloudFormation template to create EC2 instances and a load balancer to be launched when needed. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.

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

Answer: A

Explanation: This answer is correct because it meets the requirements of securely migrating the existing data to AWS and satisfying the new regulation. AWS DataSync is a service that makes it easy to move large amounts of data online between on-premises storage and Amazon S3. DataSync automatically encrypts data in transit and verifies data integrity during transfer. AWS CloudTrail is a service that records AWS API calls for your account and delivers log files to Amazon S3. CloudTrail can log data events, which show the resource operations performed on or within a resource in your AWS account, such as S3 object-level API activity. By using CloudTrail to log data events, you can audit access at all levels of the stored data.

References:

- https://docs.aws.amazon.com/datasync/latest/userguide/what-is-datasync.html
- https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-data-events- with-cloudtrail.html

383. - (Topic 4)

A company has hired an external vendor to perform work in the company's AWS account. The vendor uses an automated tool that is hosted in an AWS account that the vendor owns. The vendor does not have IAM access to the company's AWS account.

How should a solutions architect grant this access to the vendor?

A. Create an IAM role in the company's account to delegate access to the vendor's IAM role. Attach the appropriate IAM policies to the role for the permissions that the vendor requires.

B. Create an IAM user in the company's account with a password that meets the password complexity requirements. Attach the appropriate IAM policies to the user for the permissions that the vendor requires.

C. Create an IAM group in the company's account. Add the tool's IAM user from the vendor account to the group. Attach the appropriate IAM policies to the group for the permissions that the vendor requires.

D. Create a new identity provider by choosing "AWS account" as the provider type in the IAM console. Supply the vendor's AWS account ID and user name. Attach the appropriate IAM policies to the new provider for the permissions that the vendor requires.

Answer: A

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html

384. - (Topic 4)

A global company runs its applications in multiple AWS accounts in AWS Organizations. The company's applications use multipart uploads to upload data to multiple Amazon S3 buckets across AWS Regions. The company wants to report on incomplete multipart uploads for cost compliance purposes.

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

A. Configure AWS Config with a rule to report the incomplete multipart upload object count.

B. Create a service control policy (SCP) to report the incomplete multipart upload object count.

C. Configure S3 Storage Lens to report the incomplete multipart upload object count.

D. Create an S3 Multi-Region Access Point to report the incomplete multipart upload object count.

Answer: C

Explanation: S3 Storage Lens is a cloud storage analytics feature that provides organization-wide visibility into object storage usage and activity across multiple AWS accounts in AWS Organizations. S3 Storage Lens can report the incomplete multipart upload object count as one of the metrics that it collects and displays on an interactive dashboard in the S3 console. S3 Storage Lens can also export metrics in CSV or Parquet format to an S3 bucket for further analysis. This solution will meet the requirements with the least operational overhead, as it does not require any code development or policy changes. References:

- 1 explains how to use S3 Storage Lens to gain insights into S3 storage usage and activity.
- 2 describes the concept and benefits of multipart uploads.

385. - (Topic 4)

A company has a web application for travel ticketing. The application is based on a database that runs in a single data center in North America. The company wants to expand the application to serve a global user base. The company needs to deploy the application to multiple AWS Regions. Average latency must be less than 1 second on updates to the reservation database.

The company wants to have separate deployments of its web platform across multiple Regions. However the company must maintain a single primary reservation database that is globally consistent.

Which solution should a solutions architect recommend to meet these requirements?

A. Convert the application to use Amazon DynamoDB. Use a global table for the center reservation table.

Use the correct Regional endpoint in each Regional deployment.

B. Migrate the database to an Amazon Aurora MySQL database. Deploy Aurora Read Replicas in each Region. Use the correct Regional endpoint in each Regional deployment for access to the database.

C. Migrate the database to an Amazon RDS for MySQL database Deploy MySQL read replicas in each Region. Use the correct Regional endpoint in each Regional deployment for access to the database.

D. Migrate the application to an Amazon Aurora Serverless database. Deploy instances of the database to each Region. Use the correct Regional endpoint in each Regional deployment to access the database. Use AWS Lambda functions to process event streams in each Region to synchronize the databases.

Answer: B

Explanation: https://aws.amazon.com/rds/aurora/global-database/

https://aws.amazon.com/blogs/architecture/using-amazon-aurora-global-database-for-low-latency-without-application-changes/

386. - (Topic 4)

A company runs an application that uses Amazon RDS for PostgreSQL. The application receives traffic only on weekdays during business hours. The company wants to optimize costs and reduce operational overhead based on this usage.

Which solution will meet these requirements?

A. Use the Instance Scheduler on AWS to configure start and stop schedules.

B. Turn off automatic backups. Create weekly manual snapshots of the database.

C. Create a custom AWS Lambda function to start and stop the database based on minimum CPU utilization.

D. Purchase All Upfront reserved DB instances.

Answer: A

Explanation: https://aws.amazon.com/solutions/implementations/instance-scheduler-on- aws/?nc1=h_ls

The Instance Scheduler on AWS solution automates the starting and stopping of Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Relational Database Service (Amazon RDS) instances. This solution helps reduce operational costs by stopping resources that are not in use and starting them when they are needed1. The solution allows you to define custom schedules and periods using a command line interface (CLI) or an SSM maintenance window1. You can also choose between different payment options for the

reserved DB instances, such as No Upfront, Partial Up front, or All Upfront2.

387. - (Topic 4)

A company wants to analyze and troubleshoot Access Denied errors and Unauthonzed errors that are related to 1AM permissions The company has AWS CloudTrail turned on Which solution will meet these requirements with the LEAST effort?

A. Use AWS Glue and write custom scripts to query CloudTrail logs for the errors

B. Use AWS Batch and write custom scripts to query CloudTrail logs for the errors

C. Search CloudTrail logs with Amazon Athena queries to identify the errors

D. Search CloudTrail logs with Amazon QuickSight. Create a dashboard to identify the errors.

Answer: C

Explanation: This solution meets the following requirements:

⇨ It is the least effort, as it does not require any additional AWS services, custom scripts, or data processing steps. Amazon Athena is a serverless interactive query service that allows you to analyze data in Amazon S3 using standard SQL. You can use Athena to query CloudTrail logs directly from the S3 bucket where they are stored, without any data loading or transformation. You can also use the AWS Management Console, the AWS CLI, or the Athena API to run and manage your queries.

⇨ It is effective, as it allows you to filter, aggregate, and join CloudTrail log data using SQL syntax. You can use various SQL functions and operators to specify the criteria for identifying Access Denied and Unauthorized errors, such as the error code, the user identity, the event source, the event name, the event time, and the resource ARN. You can also use subqueries, views, and common table expressions to simplify and optimize your queries.

⇨ It is flexible, as it allows you to customize and save your queries for future use.

You can also export the query results to other formats, such as CSV or JSON, or integrate them with other AWS services, such as Amazon QuickSight, for further analysis and visualization.

References:

⇨ Querying AWS CloudTrail Logs - Amazon Athena

⇨ Analyzing Data in S3 using Amazon Athena | AWS Big Data Blog

⇨ Troubleshoot IAM permisson access denied or unauthorized errors | AWS re:Post

388. - (Topic 4)

A company's application runs on Amazon EC2 instances that are in multiple Availability Zones. The application needs to ingest real-time data from third-party applications.

The company needs a data ingestion solution that places the ingested raw data in an Amazon S3 bucket.

Which solution will meet these requirements?

A. Create Amazon Kinesis data streams for data ingestion. Create Amazon Kinesis Data Firehose delivery streams to consume the Kinesis data streams. Specify the S3 bucket as the destination of the delivery streams.

B. Create database migration tasks in AWS Database Migration Service (AWS DMS). Specify replication instances of the EC2 instances as the source endpoints. Specify the S3 bucket as the target endpoint. Set the migration type to migrate existing data and replicate ongoing changes.

C. Create and configure AWS DataSync agents on the EC2 instances. Configure DataSync tasks to transfer data from the EC2 instances to the S3 bucket.

D. Create an AWS Direct Connect connection to the application for data ingestion. Create Amazon Kinesis Data Firehose delivery streams to consume direct PUT operations from the application. Specify the S3 bucket as the destination of the delivery streams.

Answer: A

Explanation: The solution that will meet the requirements is to create Amazon Kinesis data streams for data ingestion, create Amazon Kinesis Data Firehose delivery streams to consume the Kinesis data streams, and specify the S3 bucket as the destination of the delivery streams. This solution will allow the company's application to ingest real-time data from third-party applications and place the ingested raw data in an S3 bucket. Amazon Kinesis data streams are scalable and durable streams that can capture and store data from hundreds of thousands of sources. Amazon Kinesis Data Firehose is a fully managed service that can deliver streaming data to destinations such as S3, Amazon Redshift, Amazon OpenSearch Service, and Splunk. Amazon Kinesis Data Firehose can also transform and compress the data before delivering it to S3.

The other solutions are not as effective as the first one because they either do not support real-time data ingestion, do not work with third-party applications, or do not use S3 as the destination. Creating database migration tasks in AWS Database Migration Service (AWS DMS) will not support real-time data ingestion,

as AWS DMS is mainly designed for migrating relational databases, not streaming data. AWS DMS also requires replication instances, source endpoints, and target endpoints to be compatible with specific database engines and versions. Creating and configuring AWS DataSync agents on the EC2 instances will not work with third-party applications, as AWS DataSync is a service that transfers data between on-premises storage systems and AWS storage services, not between applications. AWS DataSync also requires installing agents on the source or destination servers. Creating an AWS Direct Connect connection to the application for data ingestion will not use S3 as the destination, as AWS Direct Connect is a service that establishes a dedicated network connection between on-premises and AWS, not between applications and storage services. AWS Direct Connect also requires a physical connection to an AWS Direct Connect location.

References:

- Amazon Kinesis
- Amazon Kinesis Data Firehose
- AWS Database Migration Service
- AWS DataSync
- AWS Direct Connect

389. - (Topic 4)

A company hosts multiple production applications. One of the applications consists of resources from Amazon EC2, AWS Lambda, Amazon RDS, Amazon Simple Notification Service (Amazon SNS), and Amazon Simple Queue Service (Amazon SQS) across multiple AWS Regions. All company resources are tagged with a tag name of “application” and a value that corresponds to each application. A solutions architect must provide the quickest solution for identifying all of the tagged components.

Which solution meets these requirements?

A. Use AWS CloudTrail to generate a list of resources with the application tag.

B. Use the AWS CLI to query each service across all Regions to report the tagged components.

C. Run a query in Amazon CloudWatch Logs Insights to report on the components with the application tag.

D. Run a query with the AWS Resource Groups Tag Editor to report on the resources globally with the application tag.

Answer: D

Explanation: https://docs.aws.amazon.com/tag-editor/latest/userguide/tagging.html

390. - (Topic 4)

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

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

A. AWS Key Management Service (AWS KMS)

B. VPC endpoint

C. Private subnet

D. Virtual private gateway

Answer: B

Explanation: https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints.html

391. - (Topic 4)

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

Which combination of steps should the solutions architect take to meet this requirement? (Choose two.)

A. Create a route table entry for the endpoint.

B. Create a gateway endpoint for DynamoDB.

C. Create an interface endpoint for Amazon EC2.

D. Create an elastic network interface for the endpoint in each of the subnets of the VPC.

E. Create a security group entry in the endpoint's security group to provide access.

Answer: B,E

Explanation: B and E are the correct answers because they allow the solutions architect to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not travel across the internet. By creating a gateway endpoint for DynamoDB, the solutions architect can enable private connectivity between the VPC and DynamoDB. By creating a security group entry in the endpoint’s security group to provide access, the solutions architect can control which EC2 instances can communicate with DynamoDB through the endpoint. References:

- Gateway Endpoints
- Controlling Access to Services with VPC Endpoints

392. - (Topic 4)

A company is building an ecommerce application and needs to store sensitive customer information. The company needs to give customers the ability to complete purchase transactions on the website. The company also needs to ensure that sensitive customer data is protected, even from database administrators.

Which solution meets these requirements?

A. Store sensitive data in an Amazon Elastic Block Store (Amazon EBS) volume. Use EBS encryption to encrypt the data. Use an IAM instance role to restrict access.

B. Store sensitive data in Amazon RDS for MySQL. Use AWS Key Management Service (AWS KMS) client-side encryption to encrypt the data.

C. Store sensitive data in Amazon S3. Use AWS Key Management Service (AWS KMS) server-side encryption to encrypt the data. Use S3 bucket policies to restrict access.

D. Store sensitive data in Amazon FSx for Windows Server. Mount the file share on application servers. Use Windows file permissions to restrict access.

Answer: B

Explanation: it allows the company to store sensitive customer information in a managed AWS service and give customers the ability to complete purchase transactions on the website. By using AWS Key Management Service (AWS KMS) client-side encryption, the company can encrypt the data before sending it to Amazon RDS for MySQL. This ensures that sensitive customer data is protected, even from database administrators, as only the application has access to the encryption keys. References:

- Using Encryption with Amazon RDS for MySQL
- Encrypting Amazon RDS Resources

393. - (Topic 4)

A company hosts a three-tier web application in the AWS Cloud. A Multi-AZ Amazon RDS for MySQL server forms the database layer. Amazon ElastiCache forms the cache layer. The company wants a caching strategy that adds or updates data in the cache when a customer adds an item to the database.

The data in the cache must always match the data in the database.

Which solution will meet these requirements?

A. Implement the lazy loading caching strategy

B. Implement the write-through caching strategy.

C. Implement the adding TTL caching strategy.

D. Implement the AWS AppConfig caching strategy.

Answer: B

Explanation: A write-through caching strategy adds or updates data in the cache whenever data is written to the database. This ensures that the data in the cache is always consistent with the data in the database. A write-through caching strategy also reduces the cache miss penalty, as data is always available in the cache when it is requested. However, a write-through caching strategy can increase the write latency, as data has to be written to both the cache and the database. A write-through caching strategy is suitable for applications that require high data consistency and low read latency.

A lazy loading caching strategy only loads data into the cache when it is requested, and updates the cache when there is a cache miss. This can result in stale data in the cache, as data is not updated in the cache when it is changed in the database. A lazy loading caching strategy is suitable for applications that can tolerate some data inconsistency and have a low cache miss rate.

An adding TTL caching strategy assigns a time-to-live (TTL) value to each data item in the cache, and removes the data from the cache when the TTL expires. This can help prevent stale data in the cache, as data is periodically refreshed from the database. However, an adding TTL caching strategy can also increase the cache miss rate, as data can be evicted from the cache before it is requested. An adding TTL caching strategy is suitable for applications that have a high cache hit rate and can tolerate some data inconsistency.

An AWS AppConfig caching strategy is not a valid option, as AWS AppConfig is a service that enables customers to quickly deploy validated configurations to applications of any size and scale. AWS AppConfig does not provide a caching layer for web applications.

References: Caching strategies - Amazon ElastiCache, Caching for high-volume workloads with Amazon ElastiCache

394. - (Topic 4)

A company has deployed a database in Amazon RDS for MySQL. Due to increased transactions, the database support team is reporting slow reads against the DB instance and recommends adding a read replica.

Which combination of actions should a solutions architect take before implementing this change? (Choose two.)

A. Enable binlog replication on the RDS primary node.

B. Choose a failover priority for the source DB instance.

C. Allow long-running transactions to complete on the source DB instance.

D. Create a global table and specify the AWS Regions where the table will be available.

E. Enable automatic backups on the source instance by setting the backup retention period to a value other than 0.

Answer: C,E

Explanation: "An active, long-running transaction can slow the process of creating the read replica. We recommend that you wait for long-running transactions to complete before creating a read replica. If you create multiple read replicas in parallel from the same source DB instance, Amazon RDS takes only one snapshot at the start of the first create action. When creating a read replica, there are a few things to consider. First, you must enable automatic backups on the source DB instance by setting the backup retention period to a value other than 0. This requirement also applies to a read replica that is the source DB instance for another read replica"

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

395. - (Topic 4)

A company provides an API interface to customers so the customers can retrieve their financial information. The company expects a larger number of requests during peak usage times of the year.

The company requires the API to respond consistently with low latency to ensure customer satisfaction.

The company needs to provide a compute host for the API.

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

A. Use an Application Load Balancer and Amazon Elastic Container Service (Amazon ECS).

B. Use Amazon API Gateway and AWS Lambda functions with provisioned concurrency.

C. Use an Application Load Balancer and an Amazon Elastic Kubernetes Service (Amazon EKS) cluster.

D. Use Amazon API Gateway and AWS Lambda functions with reserved concurrency.

Answer: B

Explanation: Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers. Lambda scales automatically based on the incoming requests, but it may take some time to initialize new instances of your function if there is a sudden increase in demand. This may result in high latency or cold starts for your API. To avoid this, you can use provisioned concurrency, which ensures that your function is initialized and ready to respond at any time. Provisioned concurrency also helps you achieve consistent low latency for your API by reducing the impact of scaling on performance. References:

https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-develop-integrations-lambda.html https://docs.aws.amazon.com/lambda/latest/dg/configuration- concurrency.html

396. - (Topic 4)

A solutions architect needs to optimize storage costs. The solutions architect must identify any Amazon S3 buckets that are no longer being accessed or are rarely accessed.

Which solution will accomplish this goal with the LEAST operational overhead?

A. Analyze bucket access patterns by using the S3 Storage Lens dashboard for advanced activity metrics.

B. Analyze bucket access patterns by using the S3 dashboard in the AWS Management Console.

C. Turn on the Amazon CloudWatch BucketSizeBytes metric for buckets. Analyze bucket access patterns by using the metrics data with Amazon Athena.

D. Turn on AWS CloudTrail for S3 object monitoring. Analyze bucket access patterns by using CloudTrail logs that are integrated with Amazon CloudWatch Logs.

Answer: A

Explanation: S3 Storage Lens is a fully managed S3 storage analytics solution that provides a comprehensive view of object storage usage, activity trends, and recommendations to optimize costs. Storage Lens allows you to analyze object access patterns across all of your S3 buckets and generate detailed metrics and reports.

397. - (Topic 4)

A solutions architect needs to design a highly available application consisting of web, application, and database tiers. HTTPS content delivery should be as close to the edge as possible, with the least delivery time.

Which solution meets these requirements and is MOST secure?

A. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.

B. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.

C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.

D. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.

Answer: C

Explanation:

This solution meets the requirements for a highly available application with web, application, and database tiers, as well as providing edge-based content delivery.

Additionally, it maximizes security by having the ALB in a private subnet, which limits direct access to the web servers, while still being able to serve traffic over the Internet via the public ALB. This will ensure that the web servers are not exposed to the public Internet, which reduces the attack surface and provides a secure way to access the application.

398. - (Topic 4)

A company has Amazon EC2 instances that run nightly batch jobs to process data. The EC2 instances run in an Auto Scaling group that uses On-Demand billing. If a job fails on one instance: another instance will reprocess the job. The batch jobs run between 12:00 AM and 06 00 AM local time every day.

Which solution will provide EC2 instances to meet these requirements MOST cost- effectively'?

A. Purchase a 1-year Savings Plan for Amazon EC2 that covers the instance family of the Auto Scaling group that the batch job uses.

B. Purchase a 1-year Reserved Instance for the specific instance type and operating system of the

instances in the Auto Scaling group that the batch job uses.

C. Create a new launch template for the Auto Scaling group Set the instances to Spot Instances Set a policy to scale out based on CPU usage.

D. Create a new launch template for the Auto Scaling group Increase the instance size Set a policy to scale out based on CPU usage.

Answer: C

Explanation: This option is the most cost-effective solution because it leverages the Spot Instances, which are unused EC2 instances that are available at up to 90% discount compared to On-Demand prices. Spot Instances can be interrupted by AWS when the demand for On-Demand instances increases, but since the batch jobs are fault-tolerant and can be reprocessed by another instance, this is not a major issue. By using a launch template, the company can specify the configuration of the Spot Instances, such as the instance type, the operating system, and the user data. By using an Auto Scaling group, the company can automatically scale the number of Spot Instances based on the CPU usage, which reflects the load of the batch jobs. This way, the company can optimize the performance and the cost of the EC2 instances for the nightly batch jobs.

A. Purchase a 1-year Savings Plan for Amazon EC2 that covers the instance family of the Auto Scaling group that the batch job uses. This option is not optimal because it requires a commitment to a consistent amount of compute usage per hour for a one-year term, regardless of the instance type, size, region, or operating system. This can limit the flexibility and scalability of the Auto Scaling group and result in overpaying for unused compute capacity. Moreover, Savings Plans do not provide a capacity reservation, which means the company still needs to reserve capacity with On-Demand Capacity Reservations and pay lower prices with Savings Plans.

* B. Purchase a 1-year Reserved Instance for the specific instance type and operating system of the instances in the Auto Scaling group that the batch job uses. This option is not ideal because it requires a commitment to a specific instance configuration for a one-year term, which can reduce the flexibility and scalability of the Auto Scaling group and result in overpaying for unused compute capacity. Moreover, Reserved Instances do not provide a capacity reservation, which means the company still needs to reserve capacity with On- Demand Capacity Reservations and pay lower prices with Reserved Instances.

* D. Create a new launch template for the Auto Scaling group Increase the instance size Set a policy to scale out based on CPU usage. This option is not cost-effective because it does not take advantage of the

lower prices of Spot Instances. Increasing the instance size can improve the performance of the batch jobs, but it can also increase the cost of the On- Demand instances. Moreover, scaling out based on CPU usage can result in launching more instances than needed, which can also increase the cost of the system.

References:

- 1 Spot Instances - Amazon Elastic Compute Cloud
- 2 Launch templates - Amazon Elastic Compute Cloud
- 3 Auto Scaling groups - Amazon EC2 Auto Scaling
- [4] Savings Plans - Amazon EC2 Reserved Instances and Other AWS Reservation Models

399. - (Topic 4)

A hospital needs to store patient records in an Amazon S3 bucket. The hospital's compliance team must ensure that all protected health information (PHI) is encrypted in transit and at rest. The compliance team must administer the encryption key for data at rest.

Which solution will meet these requirements?

A. Create a public SSL/TLS certificate in AWS Certificate Manager (ACM). Associate the certificate with Amazon S3. Configure default encryption for each S3 bucket to use server- side encryption with AWS KMS keys (SSE-KMS). Assign the compliance team to manage the KMS keys.

B. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Configure default encryption for each S3 bucket to use server-side encryption with S3 managed encryption keys (SSE-S3). Assign the compliance team to manage the SSE-S3 keys.

C. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Configure default encryption for each S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Assign the compliance team to manage the KMS keys.

D. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Use Amazon Macie to protect the sensitive data that is stored in Amazon S3. Assign the compliance team to manage Macie.

Answer: C

Explanation: it allows the compliance team to manage the KMS keys used for server-side encryption, thereby providing the necessary control over the encryption keys. Additionally, the use of the "aws:SecureTransport" condition on the bucket policy ensures that all connections to the S3 bucket are

encrypted in transit.

400. - (Topic 4)

A social media company is building a feature for its website. The feature will give users the ability to upload photos. The company expects significant increases in demand during large events and must ensure that the website can handle the upload traffic from users.

Which solution meets these requirements with the MOST scalability?

A. Upload files from the user's browser to the application servers. Transfer the files to an Amazon S3 bucket.

B. Provision an AWS Storage Gateway file gateway. Upload files directly from the user's browser to the file gateway.

C. Generate Amazon S3 presigned URLs in the application. Upload files directly from the user's browser into an S3 bucket.

D. Provision an Amazon Elastic File System (Amazon EFS) file system Upload files directly from the user's browser to the file system

Answer: C

Explanation: This approach allows users to upload files directly to S3 without passing through the application servers, reducing the load on the application and improving scalability. It leverages the client-side capabilities to handle the file uploads and offloads the processing to S3.

401. - (Topic 4)

A company uses an organization in AWS Organizations to manage AWS accounts that contain applications. The company sets up a dedicated monitoring member account in the organization. The company wants to query and visualize observability data across the accounts by using Amazon CloudWatch.

Which solution will meet these requirements?

A. Enable CloudWatch cross-account observability for the monitoring account. Deploy an AWS CloudFormation template provided by the monitoring account in each AWS account to share the data with the monitoring account.

B. Set up service control policies (SCPs) to provide access to CloudWatch in the monitoring account under the Organizations root organizational unit (OU).

C. Configure a new 1AM user in the monitoring account. In each AWS account, configure an 1AM policy to have access to query and visualize the CloudWatch data in the account. Attach the new 1AM policy to the new I AM user.

D. Create a new 1AM user in the monitoring account. Create cross-account 1AM policies in each AWS account. Attach the 1AM policies to the new 1AM user.

Answer: A

Explanation:

CloudWatch cross-account observability is a feature that allows you to monitor and troubleshoot applications that span multiple accounts within a Region. You can seamlessly search, visualize, and analyze your metrics, logs, traces, and Application Insights applications in any of the linked accounts without account boundaries1. To enable CloudWatch cross-account observability, you need to set up one or more AWS accounts as monitoring accounts and link them with multiple source accounts. A monitoring account is a central AWS account that can view and interact with observability data shared by other accounts. A source account is an individual AWS account that shares observability data and resources with one or more monitoring accounts1. To create links between monitoring accounts and source accounts, you can use the CloudWatch console, the AWS CLI, or the AWS API. You can also use AWS Organizations to link accounts in an organization or organizational unit to the monitoring account1. CloudWatch provides a CloudFormation template that you can deploy in each source account to share observability data with the monitoring account. The template creates a sink resource in the monitoring account and an observability link resource in the source account. The template also creates the necessary IAM roles and policies to allow cross-account access to the observability data2. Therefore, the solution that meets the requirements of the question is to enable CloudWatch cross- account observability for the monitoring account and deploy the CloudFormation template provided by the monitoring account in each AWS account to share the data with the monitoring account.

The other options are not valid because:

- Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines3.

SCPs do not provide access to CloudWatch in the monitoring account, but rather restrict the actions that

users and roles can perform in the source accounts. SCPs are not required to enable CloudWatch cross-account observability, as the CloudFormation template creates the necessary IAM roles and policies for cross- account access2.

➪ IAM users are entities that you create in AWS to represent the people or applications that use them to interact with AWS. IAM users can have permissions to access the resources in your AWS account4. Configuring a new IAM user in the monitoring account and an IAM policy in each AWS account to have access to query and visualize the CloudWatch data in the account is not a valid solution, as it does not enable CloudWatch cross-account observability. This solution would require the IAM user to switch between different accounts to view the observability data, which is not seamless and efficient. Moreover, this solution would not allow the IAM user to search, visualize, and analyze metrics, logs, traces, and Application Insights applications across multiple accounts in a single place1.

➪ Cross-account IAM policies are policies that allow you to delegate access to resources that are in different AWS accounts that you own. You attach a cross- account policy to a user or group in one account, and then specify which accounts the user or group can access5. Creating a new IAM user in the monitoring account and cross-account IAM policies in each AWS account is not a valid solution, as it does not enable CloudWatch cross-account observability. This solution would also require the IAM user to switch between different accounts to view the observability data, which is not seamless and efficient. Moreover, this solution would not allow the IAM user to search, visualize, and analyze metrics, logs, traces, and Application Insights applications across multiple accounts in a single place1.

References: CloudWatch cross-account observability, CloudFormation template for CloudWatch cross-account observability, Service control policies, IAM users, Cross- account IAM policies

402. - (Topic 4)

A company moved its on-premises PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. The company successfully launched a new product. The workload on the database has increased.

The company wants to accommodate the larger workload without adding infrastructure. Which solution will meet these requirements MOST cost-effectively?

A. Buy reserved DB instances for the total workload. Make the Amazon RDS for PostgreSQL DB instance larger.

B. Make the Amazon RDS for PostgreSQL DB instance a Multi-AZ DB instance.

C. Buy reserved DB instances for the total workload. Add another Amazon RDS for PostgreSQL DB instance.

D. Make the Amazon RDS for PostgreSQL DB instance an on-demand DB instance.

Answer: A

Explanation: This answer is correct because it meets the requirements of accommodating the larger workload without adding infrastructure and minimizing the cost. Reserved DB instances are a billing discount applied to the use of certain on-demand DB instances in your account. Reserved DB instances provide you with a significant discount compared to on-demand DB instance pricing. You can buy reserved DB instances for the total workload and choose between three payment options: No Upfront, Partial Upfront, or All Upfront. You can make the Amazon RDS for PostgreSQL DB instance larger by modifying its instance type to a higher performance class. This way, you can increase the CPU, memory, and network capacity of your DB instance and handle the increased workload. References:

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWith ReservedDBInstances.html
- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.DBInstanc eClass.html

403. - (Topic 4)

A company is developing a marketing communications service that targets mobile app users. The company needs to send confirmation messages with Short Message Service (SMS) to its users. The users must be able to reply to the SMS messages. The company must store the responses for a year for analysis.

What should a solutions architect do to meet these requirements?

A. Create an Amazon Connect contact flow to send the SMS messages. Use AWS Lambda to process the responses.

B. Build an Amazon Pinpoint journey. Configure Amazon Pinpoint to send events to an Amazon Kinesis data stream for analysis and archiving.

C. Use Amazon Simple Queue Service (Amazon SQS) to distribute the SMS messages. Use AWS Lambda to process the responses.

D. Create an Amazon Simple Notification Service (Amazon SNS) FIFO topic. Subscribe an Amazon Kinesis data stream to the SNS topic for analysis and archiving.

Answer: B

Explanation: https://aws.amazon.com/pinpoint/product-details/sms/ Two-Way Messaging: Receive SMS messages from your customers and reply back to them in a chat-like interactive experience. With Amazon Pinpoint, you can create automatic responses when customers send you messages that contain certain keywords. You can even use Amazon Lex to create conversational bots. A majority of mobile phone users read incoming SMS messages almost immediately after receiving them. If you need to be able to provide your customers with urgent or important information, SMS messaging may be the right solution for you. You can use Amazon Pinpoint to create targeted groups of customers, and then send them campaign-based messages. You can also use Amazon Pinpoint to send direct messages, such as appointment confirmations, order updates, and one-time passwords.

404. - (Topic 4)

A company website hosted on Amazon EC2 instances processes classified data stored in The application writes data to Amazon Elastic Block Store (Amazon EBS) volumes The company needs to ensure that all data that is written to the EBS volumes is encrypted at rest.

Which solution will meet this requirement?

A. Create an 1AM role that specifies EBS encryption Attach the role to the EC2 instances

B. Create the EBS volumes as encrypted volumes Attach the EBS volumes to the EC2 instances

C. Create an EC2 instance tag that has a key of Encrypt and a value of True Tag all instances that require encryption at the EBS level

D. Create an AWS Key Management Service (AWS KMS) key policy that enforces EBS encryption in the account Ensure that the key policy is active

Answer: B

Explanation: The simplest and most effective way to ensure that all data that is written to the EBS volumes is encrypted at rest is to create the EBS volumes as encrypted volumes. You can do this by selecting the encryption option when you create a new EBS volume, or by copying an existing unencrypted volume to a new encrypted volume. You can also specify the AWS KMS key that you want to use for encryption, or use the default AWS- managed key. When you attach the encrypted EBS volumes to the EC2 instances, the data will be automatically encrypted and decrypted by the EC2 host. This solution does not require any additional IAM roles, tags, or policies.

References:

- Amazon EBS encryption
- Creating an encrypted EBS volume
- Encrypting an unencrypted EBS volume

405. - (Topic 4)

A company has an application that processes customer orders. The company hosts the application on an Amazon EC2 instance that saves the orders to an Amazon Aurora database. Occasionally when traffic is high: the workload does not process orders fast enough.

What should a solutions architect do to write the orders reliably to the database as quickly as possible?

A. Increase the instance size of the EC2 instance when traffic is high. Write orders to Amazon Simple Notification Service (Amazon SNS). Subscribe the database endpoint to the SNS topic.

B. Write orders to an Amazon Simple Queue Service (Amazon SQS) queue. Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database.

C. Write orders to Amazon Simple Notification Service (Amazon SNS) Subscribe the database endpoint to the SNS topic Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SNS topic.

D. Write orders to an Amazon Simple Queue Service (Amazon SQS) queue when the EC2 instance reaches CPU threshold limits. Use scheduled scaling of EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database

Answer: B

Explanation:

Amazon SQS is a fully managed message queuing service that can decouple and scale microservices, distributed systems, and serverless applications. By writing orders to an SQS queue, the application can handle spikes in traffic without losing any orders. The EC2 instances in an Auto Scaling group can read from the SQS queue and process orders into the database at a steady pace. The Application Load Balancer can distribute the load across the EC2 instances and provide health checks. This solution meets all the requirements of the question, while the other options do not. References:

- https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/welcome.html
- https://aws.amazon.com/architecture/serverless/

https://aws.amazon.com/sqs/

406. SIMULATION - (Topic 4)

A research company runs experiments that are powered by a simulation application and a visualization application. The simulation application runs on Linux and outputs intermediate data to an NFS share every 5 minutes. The visualization application is a Windows desktop application that displays the simulation output and requires an SMB file system.

The company maintains two synchronized file systems. This strategy is causing data duplication and inefficient resource usage. The company needs to migrate the applications to AWS without making code changes to either application.

Which solution will meet these requirements?

A. Migrate both applications to AWS Lambda. Create an Amazon S3 bucket to exchange data between the applications.

B. Migrate both applications to Amazon Elastic Container Service (Amazon ECS). Configure Amazon FSx File Gateway for storage.

C. Migrate the simulation application to Linux Amazon EC2 instances. Migrate the visualization application to Windows EC2 instances. Configure Amazon Simple Queue Service (Amazon SQS) to exchange data between the applications.

D. Migrate the simulation application to Linux Amazon EC2 instances. Migrate the visualization application to Windows EC2 instances. Configure Amazon FSx for NetApp ONTAP for storage.

Answer: D

Explanation:

This solution will meet the requirements because Amazon FSx for NetApp ONTAP is a fully managed service that provides highly reliable, scalable, and feature-rich file storage built on NetApp's popular ONTAP file system. FSx for ONTAP supports both NFS and SMB protocols, which means it can be accessed by both Linux and Windows applications without code changes. FSx for ONTAP also eliminates data duplication and inefficient resource usage by automatically tiering infrequently accessed data to a lower-cost storage tier and providing storage efficiency features such as deduplication and compression. FSx for ONTAP also integrates with other AWS services such as Amazon S3, AWS Backup, and AWS CloudFormation. By migrating the applications to Amazon EC2 instances, the company can leverage the

scalability, security, and performance of AWS compute resources.

407. - (Topic 4)

A solutions architect is designing an AWS Identity and Access Management (1AM) authorization model for a company's AWS account. The company has designated five specific employees to have full access to AWS services and resources in the AWS account.

The solutions architect has created an 1AM user for each of the five designated employees and has created an 1AM user group.

Which solution will meet these requirements?

A. Attach the AdministratorAccess resource-based policy to the 1AM user group. Place each of the five designated employee IAM users in the 1AM user group.

B. Attach the SystemAdministrator identity-based policy to the IAM user group. Place each of the five designated employee IAM users in the IAM user group.

C. Attach the AdministratorAccess identity-based policy to the IAM user group. Place each of the five designated employee IAM users in the IAM user group.

D. Attach the SystemAdministrator resource-based policy to the IAM user group. Place each of the five designated employee IAM users in the IAM user group.

Answer: C

Explanation: This solution meets the requirements because it uses the following components and features:

- AdministratorAccess identity-based policy: This is an AWS managed policy that provides full access to AWS services and resources1. By attaching this policy to the IAM user group, the solutions architect can grant the permissions needed for the designated employees to perform any task in the AWS account.
- IAM user group: This is a collection of IAM users that share common permissions2. By creating a user group and adding the five designated employees as members, the solutions architect can simplify the management of permissions and reduce the risk of human errors or inconsistencies.
- IAM users: These are identities that represent the designated employees in AWS2.

By creating an IAM user for each employee and requiring them to sign in with their own credentials, the solutions architect can enhance the security and accountability of the AWS account.

408. - (Topic 4)

A company has one million users that use its mobile app. The company must analyze the data usage in near-real time. The company also must encrypt the data in near-real time and must store the data in a centralized location in Apache Parquet format for further processing.

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

A. Create an Amazon Kinesis data stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data. Invoke an AWS Lambda function to send the data to the Kinesis Data Analytics application.

B. Create an Amazon Kinesis data stream to store the data in Amazon S3. Create an Amazon EMR cluster to analyze the data. Invoke an AWS Lambda function to send the data to the EMR cluster.

C. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon EMR cluster to analyze the data.

D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data

Answer: D

Explanation: This solution will meet the requirements with the least operational overhead as it uses Amazon Kinesis Data Firehose, which is a fully managed service that can automatically handle the data collection, data transformation, encryption, and data storage in near-real time. Kinesis Data Firehose can automatically store the data in Amazon S3 in Apache Parquet format for further processing. Additionally, it allows you to create an Amazon Kinesis Data Analytics application to analyze the data in near real-time, with no need to manage any infrastructure or invoke any Lambda function. This way you can process a large amount of data with the least operational overhead.

409. - (Topic 4)

A company has an AWS Direct Connect connection from its corporate data center to its VPC in the us-east-1 Region. The company recently acquired a corporation that has several VPCs and a Direct Connect connection between its on-premises data center and the eu-west-2 Region. The CIDR blocks for the VPCs of the company and the corporation do not overlap. The company requires connectivity between two Regions and the data centers. The company needs a solution that is scalable while reducing

operational overhead.

What should a solutions architect do to meet these requirements?

A. Set up inter-Region VPC peering between the VPC in us-east-1 and the VPCs in eu- west-2.

B. Create private virtual interfaces from the Direct Connect connection in us-east-1 to the VPCs in eu-west-2.

C. Establish VPN appliances in a fully meshed VPN network hosted by Amazon EC2. Use AWS VPN CloudHub to send and receive data between the data centers and each VPC.

D. Connect the existing Direct Connect connection to a Direct Connect gateway. Route traffic from the virtual private gateways of the VPCs in each Region to the Direct Connect gateway.

Answer: D

Explanation: This solution meets the requirements because it allows the company to use a single Direct Connect connection to connect to multiple VPCs in different Regions using a Direct Connect gateway. A Direct Connect gateway is a globally available resource that enables you to connect your on-premises network to VPCs in any AWS Region, except the AWS China Regions. You can associate a Direct Connect gateway with a transit gateway or a virtual private gateway in each Region. By routing traffic from the virtual private gateways of the VPCs to the Direct Connect gateway, you can enable inter-Region and on-premises connectivity for your VPCs. This solution is scalable because you can add more VPCs in different Regions to the Direct Connect gateway without creating additional connections. This solution also reduces operational overhead because you do not need to manage multiple VPN appliances, VPN connections, or VPC peering connections. References:

- Direct Connect gateways
- Inter-Region VPC peering

410. - (Topic 4)

A research company uses on-premises devices to generate data for analysis. The company wants to use the AWS Cloud to analyze the data. The devices generate .csv files and support writing the data to SMB file share. Company analysts must be able to use SQL commands to query the data. The analysts will run queries periodically throughout the day.

Which combination of steps will meet these requirements MOST cost-effectively? (Select THREE.)

A. Deploy an AWS Storage Gateway on premises in Amazon S3 File Gateway mode.

B. Deploy an AWS Storage Gateway on premises in Amazon FSx File Gateway mode.

C. Set up an AWS Glue crawler to create a table based on the data that is in Amazon S3.

D. Set up an Amazon EMR cluster with EMR Fife System (EMRFS) to query the data that is in Amazon S3. Provide access to analysts.

E. Set up an Amazon Redshift cluster to query the data that is in Amazon S3. Provide access to analysts.

F. Set up Amazon Athena to query the data that is in Amazon S3. Provide access to analysts.

Answer: A,C,F

Explanation: To meet the requirements of the use case in a cost-effective way, the following steps are recommended:

➪ Deploy an AWS Storage Gateway on premises in Amazon S3 File Gateway mode.

This will allow the company to write the .csv files generated by the devices to an SMB file share, which will be stored as objects in Amazon S3 buckets. AWS Storage Gateway is a hybrid cloud storage service that integrates on-premises environments with AWS storage. Amazon S3 File Gateway mode provides a seamless way to connect to Amazon S3 and access a virtually unlimited amount of cloud storage1.

➪ Set up an AWS Glue crawler to create a table based on the data that is in Amazon

S3. This will enable the company to use standard SQL to query the data stored in Amazon S3 buckets. AWS Glue is a serverless data integration service that simplifies data preparation and analysis. AWS Glue crawlers can automatically discover and classify data from various sources, and create metadata tables in the AWS Glue Data Catalog2. The Data Catalog is a central repository that stores information about data sources and how to access them3.

➪ Set up Amazon Athena to query the data that is in Amazon S3. This will provide

the company analysts with a serverless and interactive query service that can analyze data directly in Amazon S3 using standard SQL. Amazon Athena is integrated with the AWS Glue Data Catalog, so users can easily point Athena at the data source tables defined by the crawlers. Amazon Athena charges only for the queries that are run, and offers a pay-per-query pricing model, which makes it a cost-effective option for periodic queries4.

The other options are not correct because they are either not cost-effective or not suitable for the use case. Deploying an AWS Storage Gateway on premises in Amazon FSx File Gateway mode is not correct because this mode provides low-latency access to fully managed Windows file shares in AWS, which is not required for the use case. Setting up an Amazon EMR cluster with EMR File System (EMRFS) to query the

data that is in Amazon S3 is not correct because this option involves setting up and managing a cluster of EC2 instances, which adds complexity and cost to the solution. Setting up an Amazon Redshift cluster to query the data that is in Amazon S3 is not correct because this option also involves provisioning and managing a cluster of nodes, which adds overhead and cost to the solution.

References:

- What is AWS Storage Gateway?
- What is AWS Glue?
- AWS Glue Data Catalog
- What is Amazon Athena?

411. - (Topic 4)

A company has multiple AWS accounts that use consolidated billing. The company runs several active high performance Amazon RDS for Oracle On-Demand DB instances for 90 days. The company's finance team has access to AWS Trusted Advisor in the consolidated billing account and all other AWS accounts.

The finance team needs to use the appropriate AWS account to access the Trusted Advisor check recommendations for RDS. The finance team must review the appropriate Trusted Advisor check to reduce RDS costs.

Which combination of steps should the finance team take to meet these requirements? (Select TWO.)

A. Use the Trusted Advisor recommendations from the account where the RDS instances are running.

B. Use the Trusted Advisor recommendations from the consolidated billing account to see all RDS instance checks at the same time.

C. Review the Trusted Advisor check for Amazon RDS Reserved Instance Optimization.

D. Review the Trusted Advisor check for Amazon RDS Idle DB Instances.

E. Review the Trusted Advisor check for Amazon Redshift Reserved Node Optimization.

Answer: B,C

Explanation: B. Use the Trusted Advisor recommendations from the consolidated billing account to see all RDS instance checks at the same time.

The consolidated billing account has access to all the other AWS accounts that use consolidated billing. Using the Trusted Advisor recommendations from the consolidated billing account will allow the finance

team to see all RDS instance checks for all accounts at the same time.

* C. Review the Trusted Advisor check for Amazon RDS Reserved Instance Optimization. The Trusted Advisor check for Amazon RDS Reserved Instance Optimization provides recommendations for purchasing reserved instances to reduce RDS costs. By reviewing this check, the finance team can identify which RDS instances can be converted to reserved instances to save costs.

412. - (Topic 4)

A company hosts an application on Amazon EC2 instances that run in a single Availability Zone. The application is accessible by using the transport layer of the Open Systems Interconnection (OSI) model. The company needs the application architecture to have high availability

Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO_)

A. Configure new EC2 instances in a different Availability Zone. Use Amazon Route 53 to route traffic to all instances.

B. Configure a Network Load Balancer in front of the EC2 instances.

C. Configure a Network Load Balancer tor TCP traffic to the instances. Configure an Application Load Balancer tor HTTP and HTTPS traffic to the instances.

D. Create an Auto Scaling group for the EC2 instances. Configure the Auto Scaling group to use multiple Availability Zones. Configure the Auto Scaling group to run application health checks on the instances_

E. Create an Amazon CloudWatch alarm. Configure the alarm to restart EC2 instances that transition to a stopped state

Answer: A,D

Explanation: To achieve high availability for an application that runs on EC2 instances, the application should be deployed across multiple Availability Zones and use a load balancer to distribute traffic. An Auto Scaling group can be used to launch and manage EC2 instances in multiple Availability Zones and perform health checks on them. A Network Load Balancer can be used to handle transport layer traffic to the EC2 instances. References:

- Auto Scaling Groups
- What Is a Network Load Balancer?

413. - (Topic 4)

A company needs to connect several VPCs in the us-east-1 Region that span hundreds of AWS accounts. The company's networking team has its own AWS account to manage the cloud network.

What is the MOST operationally efficient solution to connect the VPCs?

A. Set up VPC peering connections between each VPC. Update each associated subnet's route table.

B. Configure a NAT gateway and an internet gateway in each VPC to connect each VPC through the internet.

C. Create an AWS Transit Gateway in the networking team's AWS account. Configure static routes from each VPC.

D. Deploy VPN gateways in each VPC. Create a transit VPC in the networking team's AWS account to connect to each VPC.

Answer: C

Explanation: AWS Transit Gateway is a highly scalable and centralized hub for connecting multiple VPCs, on-premises networks, and remote networks. It simplifies network connectivity by providing a single entry point and reducing the number of connections required. In this scenario, deploying an AWS Transit Gateway in the networking team's AWS account allows for efficient management and control over the network connectivity across multiple VPCs.

414. - (Topic 4)

A company uses Amazon API Gateway to run a private gateway with two REST APIs in the same VPC. The BuyStock RESTful web service calls the CheckFunds RESTful

web service to ensure that enough funds are available before a stock can be purchased.

The company has noticed in the VPC flow logs that the BuyStock RESTful web

service calls the CheckFunds RESTful web service over the internet instead of through the VPC. A solutions architect must implement a solution so that the APIs

communicate through the VPC.

Which solution will meet these requirements with the FEWEST changes to the code? (Select Correct Option/s and give detailed explanation from AWS Certified Solutions

Architect - Associate (SAA-C03) Study Manual or documents)

A. Add an X-API-Key header in the HTTP header for authorization.

B. Use an interface endpoint.

C. Use a gateway endpoint.

D. Add an Amazon Simple Queue Service (Amazon SQS) queue between the two REST APIs.

Answer: B

Explanation: Using an interface endpoint will allow the BuyStock RESTful web service and the CheckFunds RESTful web service to communicate through the VPC without any changes to the code. An interface endpoint creates an elastic network interface (ENI) in the customer's VPC, and then configures the route tables to route traffic from the APIs to the ENI. This will ensure that the two APIs will communicate through the VPC without any changes to the code.

415. - (Topic 4)

A company has deployed a Java Spring Boot application as a pod that runs on Amazon Elastic Kubernetes Service (Amazon EKS) in private subnets. The application needs to write data to an Amazon DynamoDB table. A solutions architect must ensure that the application can interact with the DynamoDB table without exposing traffic to the internet.

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

A. Attach an IAM role that has sufficient privileges to the EKS pod.

B. Attach an IAM user that has sufficient privileges to the EKS pod.

C. Allow outbound connectivity to the DynamoDB table through the private subnets' network ACLs.

D. Create a VPC endpoint for DynamoDB.

E. Embed the access keys in the Java Spring Boot code.

Answer: A,D

Explanation: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html

https://aws.amazon.com/about-aws/whats-new/2019/09/amazon-eks-adds-support-to-assign-iam-permissions-to-kubernetes-service-accounts/

416. - (Topic 4)

A company runs an application using Amazon ECS. The application creates resized versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3.

How can a solutions architect ensure that the application has permission to access Amazon $3?

A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.

B. Create an IAM role with S3 permissions, and then specify that role as the taskRoleArn in the task definition.

C. Create a security group that allows access from Amazon ECS to Amazon $3, and update the launch configuration used by the ECS cluster.

D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

Answer: B

Explanation: This answer is correct because it allows the application to access Amazon S3 by using an IAM role that is associated with the ECS task. The task role grants permissions to the containers running in the task, and can be used to make AWS API calls from the application code. The taskRoleArn is a parameter in the task definition that specifies the IAM role to use for the task.

References:

- https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task-iam- roles.html
- https://docs.aws.amazon.com/AmazonECS/latest/APIReference/API_TaskDefinitio n.html

417. - (Topic 4)

A company has a serverless application on AWS that uses Amazon RDS as a backend database. The application sometimes experiences a sudden unpredictable increase in traffic. During traffic increases, the application frequently opens and closes connections to the database, which causes the application to receive errors from the database or run out of connections. The company needs to ensure that the application is always scalable and highly available.

Which solution will meet these requirements WITHOUT any code changes to the application?

A. Increase the maximum number of connections in the option group of the RDS database of the serverless application.

B. Increase the instance size of the RDS DB instance to meet the peak load traffic.

C. Deploy Amazon RDS Proxy between the serverless application and Amazon RDS.

D. Purchase Reserved Instances for Amazon RDS to ensure that the database is highly available during peak load traffic.

Answer: C

Explanation: Amazon RDS Proxy is a fully managed database proxy that makes applications more scalable, more resilient to database failures, and more secure. RDS Proxy sits between your application and your relational database to pool and share established database connections, improving database efficiency and application scalability. RDS Proxy also reduces the load on the database by handling connection management and query retries for transient errors. By deploying RDS Proxy between your serverless application and Amazon RDS, you can avoid opening and closing connections to the database frequently, which can cause errors or run out of connections. This solution will also reduce operational costs and improve availability of your application. References: https://aws.amazon.com/rds/proxy/

418. - (Topic 4)

A company is building an application that consists of several microservices. The company has decided to use container technologies to deploy its software on AWS. The company needs a solution that minimizes the amount of ongoing effort for maintenance and scaling. The company cannot manage additional infrastructure.

Which combination of actions should a solutions architect take to meet these requirements? (Choose two.)

A. Deploy an Amazon Elastic Container Service (Amazon ECS) cluster.

B. Deploy the Kubernetes control plane on Amazon EC2 instances that span multiple Availability Zones.

C. Deploy an Amazon Elastic Container Service (Amazon ECS) service with an Amazon EC2 launch type. Specify a desired task number level of greater than or equal to 2.

D. Deploy an Amazon Elastic Container Service (Amazon ECS) service with a Fargate launch type. Specify a desired task number level of greater than or equal to 2.

E. Deploy Kubernetes worker nodes on Amazon EC2 instances that span multiple Availability Zones. Create a deployment that specifies two or more replicas for each microservice.

Answer: A,D

Explanation:

AWS Fargate is a technology that you can use with Amazon ECS to run containers without having to manage servers or clusters of Amazon EC2 instances. With Fargate, you no longer have to provision, configure, or scale clusters of virtual machines to run containers.

https://docs.aws.amazon.com/AmazonECS/latest/userguide/what-is-fargate.html

419. - (Topic 4)

A company's marketing data is uploaded from multiple sources to an Amazon S3 bucket A series ot data preparation jobs aggregate the data for reporting The data preparation jobs need to run at regular intervals in parallel A few jobs need to run in a specific order later

The company wants to remove the operational overhead of job error handling retry logic, and state management

Which solution will meet these requirements?

A. Use an AWS Lambda function to process the data as soon as the data is uploaded to the S3 bucket Invoke Other Lambda functions at regularly scheduled intervals

B. Use Amazon Athena to process the data Use Amazon EventBndge Scheduler to invoke Athena on a regular internal

C. Use AWS Glue DataBrew to process the data Use an AWS Step Functions state machine to run the DataBrew data preparation jobs

D. Use AWS Data Pipeline to process the data. Schedule Data Pipeline to process the data once at midnight.

Answer: C

Explanation: AWS Glue DataBrew is a visual data preparation tool that allows you to easily clean, normalize, and transform your data without writing any code. You can create and run data preparation jobs on your data stored in Amazon S3, Amazon Redshift, or other data sources. AWS Step Functions is a service that lets you coordinate multiple AWS services into serverless workflows. You can use Step Functions to orchestrate your DataBrew jobs, define the order and parallelism of execution, handle errors and retries, and monitor the state of your workflow. By using AWS Glue DataBrew and AWS Step Functions, you can meet the requirements of the company with minimal operational overhead, as you do not need to write any code, manage any servers, or deal with complex dependencies.

References:

- AWS Glue DataBrew
- AWS Step Functions
- Orchestrate AWS Glue DataBrew jobs using AWS Step Functions

420. - (Topic 4)

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

What should the solutions architect recommend?

A. Export the data to Amazon DynamoDB and have the business analysts run their queries.

B. Load the data into Amazon ElastiCache and have the business analysts run their queries.

C. Create a read replica of the primary database and have the business analysts run their queries.

D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries

Answer: C

Explanation: Creating a read replica of the primary RDS database will offload the read- only SQL queries from the primary database, which will help to improve the performance of the web application. Read replicas are exact copies of the primary database that can be used to handle read-only traffic, which will reduce the load on the primary database and improve the performance of the web application. This solution can be implemented with minimal changes to the existing web application, as the business analysts can continue to run their queries on the read replica without modifying the code.

421. - (Topic 4)

A company's infrastructure consists of Amazon EC2 instances and an Amazon RDS DB instance in a single AWS Region. The company wants to back up its data in a separate Region.

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

A. Use AWS Backup to copy EC2 backups and RDS backups to the separate Region.

B. Use Amazon Data Lifecycle Manager (Amazon DLM) to copy EC2 backups and RDS backups to the separate Region.

C. Create Amazon Machine Images (AMIs) of the EC2 instances. Copy the AMIs to the separate Region. Create a read replica for the RDS DB instance in the separate Region.

D. Create Amazon Elastic Block Store (Amazon EBS) snapshots. Copy the EBS snapshots to the separate Region. Create RDS snapshots. Export the RDS snapshots to Amazon S3. Configure S3 Cross-Region Replication (CRR) to the separate Region.

Answer: A

Explanation: To back up EC2 instances and RDS DB instances in a separate Region with the least operational overhead, AWS Backup is a simple and cost-effective solution. AWS Backup can copy EC2 backups and RDS backups to another Region automatically and

securely. AWS Backup also supports backup policies, retention rules, and monitoring features.

References:

- What Is AWS Backup?
- Cross-Region Backup

422. - (Topic 4)

An ecommerce application uses a PostgreSQL database that runs on an Amazon EC2 instance. During a monthly sales event, database usage increases and causes database connection issues for the application. The traffic is unpredictable for subsequent monthly sales events, which impacts the sales forecast. The company needs to maintain performance when there is an unpredictable increase in traffic.

Which solution resolves this issue in the MOST cost-effective way?

A. Migrate the PostgreSQL database to Amazon Aurora Serverless v2.

B. Enable auto scaling for the PostgreSQL database on the EC2 instance to accommodate increased usage.

C. Migrate the PostgreSQL database to Amazon RDS for PostgreSQL with a larger instance type

D. Migrate the PostgreSQL database to Amazon Redshift to accommodate increased usage

Answer: A

Explanation: Amazon Aurora Serverless v2 is a cost-effective solution that can automatically scale the database capacity up and down based on the application's needs. It can handle unpredictable traffic spikes without requiring any provisioning or management of database instances. It is compatible with PostgreSQL and offers high performance, availability, and durability1. References: 1: AWS Ramp-Up Guide: Architect2, page 312: AWS Certified Solutions Architect - Associate exam guide3, page 9.

423. - (Topic 4)

A solutions architect is designing a workload that will store hourly energy consumption by business tenants in a building. The sensors will feed a database through HTTP requests that will add up usage for each

tenant. The solutions architect must use managed services when possible. The workload will receive more features in the future as the solutions

architect adds independent components.

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

A. Use Amazon API Gateway with AWS Lambda functions to receive the data from the sensors, process the data, and store the data in an Amazon DynamoDB table.

B. Use an Elastic Load Balancer that is supported by an Auto Scaling group of Amazon EC2 instances to receive and process the data from the sensors. Use an Amazon S3 bucket to store the processed data.

C. Use Amazon API Gateway with AWS Lambda functions to receive the data from the sensors, process the data, and store the data in a Microsoft SQL Server Express database on an Amazon EC2 instance.

D. Use an Elastic Load Balancer that is supported by an Auto Scaling group of Amazon EC2 instances to receive and process the data from the sensors. Use an Amazon Elastic File System (Amazon EFS) shared file system to store the processed data.

Answer: A

Explanation: To use an event-driven programming model with AWS Lambda and reduce operational overhead, Amazon API Gateway and Amazon DynamoDB are suitable solutions. Amazon API Gateway can receive the data from the sensors and invoke AWS Lambda functions to process the data. AWS Lambda can run code without provisioning or managing servers, and scale automatically with the incoming requests. Amazon DynamoDB can store the data in a fast and flexible NoSQL database that can handle any amount of data with consistent performance.

References:

- What Is Amazon API Gateway?
- What Is AWS Lambda?
- What Is Amazon DynamoDB?

424. - (Topic 4)

A company has deployed its application on Amazon EC2 instances with an Amazon RDS database. The company used the principle of least privilege to configure the database access credentials. The company's security team wants to protect the application and the database from SQL injection and other web-based attacks.

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

A. Use security groups and network ACLs to secure the database and application servers.

B. Use AWS WAF to protect the application. Use RDS parameter groups to configure the security settings.

C. Use AWS Network Firewall to protect the application and the database.

D. Use different database accounts in the application code for different functions. Avoid granting excessive privileges to the database users.

Answer: B

Explanation: AWS WAF is a web application firewall that helps protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF allows users to create rules that block, allow, or count web requests based on customizable web security rules. One of the types of rules that can be created is an SQL injection rule, which allows users to specify a list of IP addresses or IP address ranges that they want to allow or block. By using AWS WAF to protect the application, the company can prevent SQL injection and other web-based attacks from reaching the application and the database.

RDS parameter groups are collections of parameters that define how a database instance operates. Users can modify the parameters in a parameter group to change the behavior and performance of the database. By using RDS parameter groups to configure the security settings, the company can enforce best practices such as disabling remote root login, requiring SSL connections, and limiting the maximum number of connections.

The other options are not correct because they do not effectively protect the application and the database from SQL injection and other web-based attacks. Using security groups and network ACLs to secure the database and application servers is not sufficient because they only filter traffic at the network layer, not at the application layer. Using AWS Network Firewall to protect the application and the database is not necessary because it is a stateful firewall service that provides network protection for VPCs, not for individual applications or databases. Using different database accounts in the application code for different functions is a good practice, but it does not prevent SQL injection attacks from exploiting vulnerabilities in the application code.

References:

- AWS WAF

- How AWS WAF works
- Working with IP match conditions
- Working with DB parameter groups
- Amazon RDS security best practices

425. - (Topic 4)

A company wants to migrate 100 GB of historical data from an on-premises location to an Amazon S3 bucket. The company has a 100 megabits per second (Mbps) internet connection on premises. The company needs to encrypt the data in transit to the S3
bucket. The company will store new data directly in Amazon S3.

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

A. Use the s3 sync command in the AWS CLI to move the data directly to an S3 bucket.

B. Use AWS DataSync to migrate the data from the on-premises location to an S3 bucket.

C. Use AWS Snowball to move the data to an S3 bucket.

D. Set up an IPsec VPN from the on-premises location to AWS. Use the s3 cp command in the AWS CLI to move the data directly to an S3 bucket.

Answer: B

Explanation: AWS DataSync is a data transfer service that makes it easy for you to move large amounts of data online between on-premises storage and AWS storage services over the internet or AWS Direct Connect. DataSync automatically encrypts your data in transit using TLS encryption, and verifies data integrity during transfer using checksums. DataSync can transfer data up to 10 times faster than open-source tools, and reduces operational overhead by simplifying and automating tasks such as scheduling, monitoring, and resuming transfers. References: https://aws.amazon.com/datasync/

426. - (Topic 4)

A company wants to share accounting data with an external auditor. The data is stored in an Amazon RDS DB instance that resides in a private subnet. The auditor has its own AWS account and requires its own copy of the database.

What is the MOST secure way for the company to share the database with the auditor?

A. Create a read replica of the database. Configure IAM standard database authentication to grant the

auditor access.

B. Export the database contents to text files. Store the files in an Amazon S3 bucket. Create a new IAM user for the auditor. Grant the user access to the S3 bucket.

C. Copy a snapshot of the database to an Amazon S3 bucket. Create an IAM user. Share the user's keys with the auditor to grant access to the object in the $3 bucket.

D. Create an encrypted snapshot of the database. Share the snapshot with the auditor. Allow access to the AWS Key Management Service (AWS KMS) encryption key.

Answer: D

Explanation: This answer is correct because it meets the requirements of sharing the database with the auditor in a secure way. You can create an encrypted snapshot of the database by using AWS Key Management Service (AWS KMS) to encrypt the snapshot

with a customer managed key. You can share the snapshot with the auditor by modifying the permissions of the snapshot and specifying the AWS account ID of the auditor. You can also allow access to the AWS KMS encryption key by adding a key policy statement that grants permissions to the auditor's account. This way, you can ensure that only the auditor can access and restore the snapshot in their own AWS account.

References:

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ShareSnapsh ot.html
- https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html#key-policy-default-allow-root-enable-iam

427. - (Topic 4)

A company needs to store contract documents. A contract lasts for 5 years. During the 5- year period, the company must ensure that the documents cannot be overwritten or deleted. The company needs to encrypt the documents at rest and rotate the encryption keys automatically every year.

Which combination of steps should a solutions architect take to meet these requirements with the LEAST operational overhead? (Select TWO.)

A. Store the documents in Amazon S3. Use S3 Object Lock in governance mode.

B. Store the documents in Amazon S3. Use S3 Object Lock in compliance mode.

C. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Configure key rotation.

D. Use server-side encryption with AWS Key Management Service (AWS KMS) customer managed keys.

Configure key rotation.

E. Use server-side encryption with AWS Key Management Service (AWS KMS) customer provided (imported) keys. Configure key rotation.

Answer: B,D

Explanation: Consider using the default aws/s3 KMS key if: You're uploading or accessing S3 objects using AWS Identity and Access Management (IAM) principals that are in the same AWS account as the AWS KMS key. You don't want to manage policies for the KMS key. Consider using a customer managed key if: You want to create, rotate, disable, or define access controls for the key. You want to grant cross-account access to your S3 objects. You can configure the policy of a customer managed key to allow access from another account. https://repost.aws/knowledge-center/s3-object-encryption-keys

428. - (Topic 4)

A company that uses AWS needs a solution to predict the resources needed for manufacturing processes each month. The solution must use historical values that are currently stored in an Amazon S3 bucket The company has no machine learning (ML) experience and wants to use a managed service for the training and predictions.

Which combination of steps will meet these requirements? (Select TWO.)

A. Deploy an Amazon SageMaker model. Create a SageMaker endpoint for inference.

B. Use Amazon SageMaker to train a model by using the historical data in the S3 bucket.

C. Configure an AWS Lambda function with a function URL that uses Amazon SageMaker endpoints to create predictions based on the inputs.

D. Configure an AWS Lambda function with a function URL that uses an Amazon Forecast predictor to create a prediction based on the inputs.

E. Train an Amazon Forecast predictor by using the historical data in the S3 bucket.

Answer: B,E

Explanation: To predict the resources needed for manufacturing processes each month using historical values that are currently stored in an Amazon S3 bucket, a solutions architect should use Amazon SageMaker to train a model by using the historical data in the S3 bucket, and deploy an Amazon SageMaker model and create a SageMaker endpoint for inference. Amazon SageMaker is a fully managed service that provides an easy way to build, train, and deploy machine learning (ML) models. The solutions

architect can use the built-in algorithms or frameworks provided by SageMaker, or bring their own custom code, to train a model using the historical data in the S3 bucket as input. The trained model can then be deployed to a SageMaker endpoint, which is a scalable and secure web service that can handle requests for predictions from the application. The solutions architect does not need to have any ML experience or manage any infrastructure to use SageMaker.

429. - (Topic 4)

A company's data platform uses an Amazon Aurora MySQL database. The database has multiple read replicas and multiple DB instances across different Availability Zones. Users have recently reported errors from the database that indicate that there are too many connections. The company wants to reduce the failover time by 20% when a read replica is promoted to primary writer.

Which solution will meet this requirement?

A. Switch from Aurora to Amazon RDS with Multi-AZ cluster deployment.

B. Use Amazon RDS Proxy in front of the Aurora database.

C. Switch to Amazon DynamoDB with DynamoDB Accelerator (DAX) for read connections.

D. Switch to Amazon Redshift with relocation capability.

Answer: B

Explanation: Amazon RDS Proxy is a service that provides a fully managed, highly available database proxy for Amazon RDS and Aurora databases. It allows you to pool and share database connections, reduce database load, and improve application scalability and availability.

By using Amazon RDS Proxy in front of your Aurora database, you can achieve the following benefits:

- You can reduce the number of connections to your database and avoid errors that indicate that there are too many connections. Amazon RDS Proxy handles the connection management and multiplexing for you, so you can use fewer database connections and resources.
- You can reduce the failover time by 20% when a read replica is promoted to primary writer. Amazon RDS Proxy automatically detects failures and routes traffic to the new primary instance without requiring changes to your application code or configuration. According to a benchmark test, using Amazon RDS Proxy reduced the failover time from 66 seconds to 53 seconds, which is a 20% improvement.
- You can improve the security and compliance of your database access. Amazon

RDS Proxy integrates with AWS Secrets Manager and AWS Identity and Access Management (IAM) to enable secure and granular authentication and authorization for your database connections.

430. - (Topic 4)

A company copies 200 TB of data from a recent ocean survey onto AWS Snowball Edge Storage Optimized devices. The company has a high performance computing (HPC) cluster that is hosted on AWS to look for oil and gas deposits. A solutions architect must provide the cluster with consistent sub-millisecond latency and high-throughput access to the data on the Snowball Edge Storage Optimized devices. The company is sending the devices back to AWS.

Which solution will meet these requirements?

A. Create an Amazon S3 bucket. Import the data into the S3 bucket. Configure an AWS Storage Gateway file gateway to use the S3 bucket. Access the file gateway from the HPC cluster instances.

B. Create an Amazon S3 bucket. Import the data into the S3 bucket. Configure an Amazon FSx for Lustre file system, and integrate it with the S3 bucket. Access the FSx for Lustre file system from the HPC cluster instances.

C. Create an Amazon S3 bucket and an Amazon Elastic File System (Amazon EFS) file system. Import the data into the S3 bucket. Copy the data from the S3 bucket to the EFS file system. Access the EFS file system from the HPC cluster instances.

D. Create an Amazon FSx for Lustre file system. Import the data directly into the FSx for Lustre file system. Access the FSx for Lustre file system from the HPC cluster instances.

Answer: B

Explanation: To provide the HPC cluster with consistent sub-millisecond latency and high- throughput access to the data on the Snowball Edge Storage Optimized devices, a solutions architect should configure an Amazon FSx for Lustre file system, and integrate it with an Amazon S3 bucket. This solution has the following benefits:

- It allows the HPC cluster to access the data on the Snowball Edge devices using a POSIX-compliant file system that is optimized for fast processing of large datasets1.
- It enables the data to be imported from the Snowball Edge devices into the S3 bucket using the AWS Snow Family Console or the AWS CLI2. The data can then be accessed from the FSx for Lustre file system using the S3 integration feature3.

- It supports high availability and durability of the data, as the FSx for Lustre file system can automatically copy the data to and from the S3 bucket3. The data can also be accessed from other AWS services or applications using the S3 API4.

References:

- 1: https://aws.amazon.com/fsx/lustre/
- 2: https://docs.aws.amazon.com/snowball/latest/developer-guide/using- adapter.html
- 3: https://docs.aws.amazon.com/fsx/latest/LustreGuide/create-fs-linked-data- repo.html
- 4: https://docs.aws.amazon.com/fsx/latest/LustreGuide/export-data-repo.html

431. - (Topic 4)

A company is subscribed to the AWS Business Support plan. Compliance rules require the company to check on AWS infrastructure health before deployments can proceed. The company needs a programmatic and automated way to check on infrastructure health at the beginning of new deployments.

Which solution will meet these requirements?

A. Use the AWS Trusted Advisor API at the start of each deployment. Pause all new deployments if the API returns any issues.

B. Use the AWS Health API at the start of each deployment. Pause all new deployments if the API returns any issues.

C. Query the AWS Support API at the start of each deployment. Pause all new deployments if the API returns any open issues.

D. Send an API call to each workload ahead of deployment. Pause the deployments if the API call fails.

Answer: B

Explanation: The AWS Health API provides programmatic access to the AWS Health information that is presented in the AWS Personal Health Dashboard. You can use the API operations to get information about AWS Health events that affect your AWS services and resources. You can also use the API to enable or disable health-based insights for your organization. You can use the AWS Health API at the start of each deployment to check on AWS infrastructure health and pause all new deployments if the API returns any issues. References: https://docs.aws.amazon.com/health/latest/APIReference/Welcome.html

432. - (Topic 4)

A company is designing a tightly coupled high performance computing (HPC) environment in the AWS Cloud The company needs to include features that will optimize the HPC environment for networking and storage.

Which combination of solutions will meet these requirements? (Select TWO)

A. Create an accelerator in AWS Global Accelerator. Configure custom routing for the accelerator.

B. Create an Amazon FSx for Lustre file system. Configure the file system with scratch storage.

C. Create an Amazon CloudFront distribution. Configure the viewer protocol policy to be HTTP and HTTPS.

D. Launch Amazon EC2 instances. Attach an Elastic Fabric Adapter (EFA) to the instances.

E. Create an AWS Elastic Beanstalk deployment to manage the environment.

Answer: B,D

Explanation: These two solutions will optimize the HPC environment for networking and storage. Amazon FSx for Lustre is a fully managed service that provides cost-effective, high-performance, scalable storage for compute workloads. It is built on the world's most popular high-performance file system, Lustre, which is designed for applications that require fast storage, such as HPC and machine learning. By configuring the file system with scratch storage, you can achieve sub-millisecond latencies, up to hundreds of GBs/s of throughput, and millions of IOPS. Scratch file systems are ideal for temporary storage and shorter-term processing of data. Data is not replicated and does not persist if a file server fails. For more information, see Amazon FSx for Lustre.

Elastic Fabric Adapter (EFA) is a network interface for Amazon EC2 instances that enables customers to run applications requiring high levels of inter-node communications at scale on AWS. Its custom-built operating system (OS) bypass hardware interface enhances the performance of inter-instance communications, which is critical to scaling HPC and machine learning applications. EFA provides a low-latency, low-jitter channel for inter- instance communications, enabling your tightly-coupled HPC or distributed machine learning applications to scale to thousands of cores. EFA uses libfabric interface and libfabric APIs for communications, which are supported by most HPC programming models. For more information, see Elastic Fabric Adapter.

The other solutions are not suitable for optimizing the HPC environment for networking and storage. AWS Global Accelerator is a networking service that helps you improve the availability, performance, and security of your public applications by using the AWS global network. It provides two global static public IPs, deterministic routing, fast failover, and TCP termination at the edge for your application endpoints. However,

it does not support OS- bypass capabilities or high-performance file systems that are required for HPC and machine learning applications. For more information, see AWS Global Accelerator. Amazon CloudFront is a content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront is integrated with AWS services such as Amazon S3, Amazon EC2, AWS Elemental Media Services, AWS Shield, AWS WAF, and AWS Lambda@Edge. However, CloudFront is not designed for HPC and machine learning applications that require high levels of inter-node communications and fast storage. For more information, see [Amazon CloudFront].

AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS. You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. However, Elastic Beanstalk is not optimized for HPC and machine learning applications that require OS-bypass capabilities and high-performance file systems. For more information, see [AWS Elastic Beanstalk].

References: Amazon FSx for Lustre, Elastic Fabric Adapter, AWS Global Accelerator, [Amazon CloudFront], [AWS Elastic Beanstalk].

433. - (Topic 4)

A company runs container applications by using Amazon Elastic Kubernetes Service (Amazon EKS) and the Kubernetes Horizontal Pod Autoscaler. The workload is not

consistent throughout the day. A solutions architect notices that the number of nodes does not automatically scale out when the existing nodes have reached maximum capacity in the cluster, which causes performance issues

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

A. Scale out the nodes by tracking the memory usage

B. Use the Kubernetes Cluster Autoscaler to manage the number of nodes in the cluster.

C. Use an AWS Lambda function to resize the EKS cluster automatically.

D. Use an Amazon EC2 Auto Scaling group to distribute the workload.

Answer: B

Explanation: The Kubernetes Cluster Autoscaler is a component that automatically adjusts the number of nodes in your cluster when pods fail or are rescheduled onto other nodes. It uses Auto Scaling groups to scale up or down the nodes according to the demand and capacity of your cluster1.

By using the Kubernetes Cluster Autoscaler in your Amazon EKS cluster, you can achieve the following benefits:

- You can improve the performance and availability of your container applications by ensuring that there are enough nodes to run your pods and that there are no idle nodes wasting resources.
- You can reduce the administrative overhead of managing your cluster size manually or using custom scripts. The Cluster Autoscaler handles the scaling decisions and actions for you based on the metrics and events from your cluster.
- You can leverage the integration of Amazon EKS and AWS Auto Scaling to optimize the cost and efficiency of your cluster. You can use features such as launch templates, mixed instances policies, and spot instances to customize your node configuration and save up to 90% on compute costs2

434. - (Topic 4)

A company seeks a storage solution for its application The solution must be highly available and scalable. The solution also must function as a file system, be mountable by multiple Linux instances in AWS and on premises through native protocols, and have no minimum size requirements. The company has set up a Site-to-Site VPN for access from its on-premises network to its VPC.

Which storage solution meets these requirements?

A. Amazon FSx Multi-AZ deployments

B. Amazon Elastic Block Store (Amazon EBS) Multi-Attach volumes

C. Amazon Elastic File System (Amazon EFS) with multiple mount targets

D. Amazon Elastic File System (Amazon EFS) with a single mount target and multiple access points

Answer: C

Explanation: Amazon EFS is a fully managed file system that can be mounted by multiple Linux instances in AWS and on premises through native protocols such as NFS and SMB. Amazon EFS has no minimum size requirements and can scale up and down automatically as files are added and removed. Amazon EFS also supports high availability and durability by allowing multiple mount targets in different Availability

Zones within a region. Amazon EFS meets all the requirements of the question, while the other options do not. References:

- https://aws.amazon.com/efs/
- https://docs.aws.amazon.com/wellarchitected/latest/performance-efficiency-pillar/storage-architecture-selection.html
- https://aws.amazon.com/blogs/storage/from-on-premises-to-aws-hybrid-cloud-architecture-for-network-file-shares/

435. - (Topic 4)

A company uses an on-premises network-attached storage (NAS) system to provide file shares to its high performance computing (HPC) workloads. The company wants to migrate its latency-sensitive HPC workloads and its storage to the AWS Cloud. The company must be able to provide NFS and SMB multi-protocol access from the file system.

Which solution will meet these requirements with the LEAST latency? (Select TWO.)

A. Deploy compute optimized EC2 instances into a cluster placement group.

B. Deploy compute optimized EC2 instances into a partition placement group.

C. Attach the EC2 instances to an Amazon FSx for Lustre file system.

D. Attach the EC2 instances to an Amazon FSx for OpenZFS file system.

E. Attach the EC2 instances to an Amazon FSx for NetApp ONTAP file system.

Answer: A,E

Explanation: A cluster placement group is a logical grouping of EC2 instances within a single Availability Zone that are placed close together to minimize network latency. This is suitable for latency-sensitive HPC workloads that require high network performance. A compute optimized EC2 instance is an instance type that has a high ratio of vCPUs to memory, which is ideal for compute-intensive applications. Amazon FSx for NetApp ONTAP is a fully managed service that provides NFS and SMB multi-protocol access from the file system, as well as features such as data deduplication, compression, thin provisioning, and snapshots. This solution will meet the requirements with the least latency,

as it leverages the low-latency network and storage performance of AWS.

References:

- 1 explains how cluster placement groups work and their benefits.

- 2 describes the characteristics and use cases of compute optimized EC2 instances.
- 3 provides an overview of Amazon FSx for NetApp ONTAP and its features.

436. - (Topic 4)

A company is building a RESTful serverless web application on AWS by using Amazon API Gateway and AWS Lambda. The users of this web application will be geographically distributed, and the company wants to reduce the latency of API requests to these users Which type of endpoint should a solutions architect use to meet these requirements?

A. Private endpoint

B. Regional endpoint

C. Interface VPC endpoint

D. Edge-optimzed endpoint

Answer: D

Explanation: An edge-optimized API endpoint is best for geographically distributed clients, as it routes the API requests to the nearest CloudFront Point of Presence (POP). This reduces the latency and improves the performance of the API. Edge-optimized endpoints are the default type for API Gateway REST APIs1. A regional API endpoint is intended for clients in the same region as the API, and it does not use CloudFront to route the requests. A private API endpoint is an API endpoint that can only be accessed from a VPC using an interface VPC endpoint. A regional or private endpoint would not meet the requirement of reducing the latency for geographically distributed users1.

437. - (Topic 4)

A solutions architect needs to review a company's Amazon S3 buckets to discover personally identifiable information (Pll). The company stores the Pll data in the us-east-I Region and us-west-2 Region.

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

A. Configure Amazon Macie in each Region. Create a job to analyze the data that is in Amazon S3_

B. Configure AWS Security Hub for all Regions. Create an AWS Config rule to analyze the data that is in Amazon S3_

C. Configure Amazon Inspector to analyze the data that IS in Amazon S3.

D. Configure Amazon GuardDuty to analyze the data that is in Amazon S3.

Answer: A

Explanation: it allows the solutions architect to review the S3 buckets to discover personally identifiable information (PII) with the least operational overhead. Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect sensitive data in AWS. Amazon Macie can analyze data in S3 buckets across multiple regions and provide insights into the type, location, and level of sensitivity of the data. References:

- Amazon Macie
- Analyzing data with Amazon Macie

438. - (Topic 4)

A company runs its applications on Amazon EC2 instances that are backed by Amazon Elastic Block Store (Amazon EBS). The EC2 instances run the most recent Amazon Linux release. The applications are experiencing availability issues when the company's employees store and retrieve files that are 25 GB or larger. The company needs a solution that does not require the company to transfer files between EC2 instances. The files must be available across many EC2 instances and across multiple Availability Zones. Which solution will meet these requirements?

A. Migrate all the files to an Amazon S3 bucket. Instruct the employees to access the files from the S3 bucket.

B. Take a snapshot of the existing EBS volume. Mount the snapshot as an EBS volume across the EC2 instances. Instruct the employees to access the files from the EC2 instances.

C. Mount an Amazon Elastic File System (Amazon EFS) file system across all the EC2 instances. Instruct the employees to access the files from the EC2 instances.

D. Create an Amazon Machine Image (AMI) from the EC2 instances. Configure new EC2 instances from the AMI that use an instance store volume. Instruct the employees to access the files from the EC2 instances

Answer: C

Explanation: To store and access files that are 25 GB or larger across many EC2 instances and across multiple Availability Zones, Amazon Elastic File System (Amazon EFS) is a suitable solution. Amazon EFS provides a simple, scalable, elastic file system that can be mounted on multiple EC2 instances concurrently.

Amazon EFS supports high availability and durability by storing data across multiple Availability Zones within a Region. References:

- What Is Amazon Elastic File System?
- Using EFS with EC2

439. - (Topic 4)

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

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

A. Use AWS Snowmobile to ship the data to AWS.

B. Order multiple AWS Snowball devices to ship the data to AWS.

C. Enable Amazon S3 Transfer Acceleration and securely upload the data.

D. Create an Amazon S3 VPC endpoint and establish a VPN to upload the data.

Answer: B

Explanation: AWS Snowball is a petabyte-scale data transport service that uses secure devices to transfer large amounts of data into and out of the AWS Cloud. Snowball addresses common challenges with large-scale data transfers including high network costs, long transfer times, and security concerns. AWS Snowball can transfer up to 80 TB of data per device, and multiple devices can be used in parallel to meet the migration deadline. AWS Snowball is more cost-effective than AWS Snowmobile, which is designed for exabyte-scale data transfers, or Amazon S3 Transfer Acceleration, which is optimized for fast transfers over long distances. Amazon S3 VPC endpoint does not increase the upload speed, but only provides a secure and private connection between the VPC and

S3. References: AWS Snowball, AWS Snowmobile, Amazon S3 Transfer Acceleration, Amazon S3 VPC endpoint

440. - (Topic 4)

A company has a new mobile app. Anywhere in the world, users can see local news on topics they choose. Users also can post photos and videos from inside the app.

Users access content often in the first minutes after the content is posted. New content quickly replaces

older content, and then the older content disappears. The local nature of the news means that users consume 90% of the content within the AWS Region where it is uploaded.

Which solution will optimize the user experience by providing the LOWEST latency for content uploads?

A. Upload and store content in Amazon S3. Use Amazon CloudFront for the uploads.

B. Upload and store content in Amazon S3. Use S3 Transfer Acceleration for the uploads.

C. Upload content to Amazon EC2 instances in the Region that is closest to the user. Copy the data to Amazon S3.

D. Upload and store content in Amazon S3 in the Region that is closest to the user. Use multiple distributions of Amazon CloudFront.

Answer: B

Explanation: The most suitable solution for optimizing the user experience by providing the lowest latency for content uploads is to upload and store content in Amazon S3 and use S3 Transfer Acceleration for the uploads. This solution will enable the company to leverage the AWS global network and edge locations to speed up the data transfer between the users and the S3 buckets.

Amazon S3 is a storage service that provides scalable, durable, and highly available object storage for any type of data. Amazon S3 allows users to store and retrieve data from anywhere on the web, and offers various features such as encryption, versioning, lifecycle management, and replication1.

S3 Transfer Acceleration is a feature of Amazon S3 that helps users transfer data to and from S3 buckets more quickly. S3 Transfer Acceleration works by using optimized network paths and Amazon's backbone network to accelerate data transfer speeds. Users can enable S3 Transfer Acceleration for their buckets and use a distinct URL to access them, such as <bucket>.s3-accelerate.amazonaws.com2.

The other options are not correct because they either do not provide the lowest latency or are not suitable for the use case. Uploading and storing content in Amazon S3 and using

Amazon CloudFront for the uploads is not correct because this solution is not designed for optimizing uploads, but rather for optimizing downloads. Amazon CloudFront is a content delivery network (CDN) that helps users distribute their content globally with low latency and high transfer speeds. CloudFront works by caching the content at edge locations around the world, so that users can access it quickly and easily from anywhere3. Uploading content to Amazon EC2 instances in the Region that is closest to the user and copying the data to Amazon S3 is not correct because this solution adds unnecessary complexity and cost to the process. Amazon EC2 is a computing service that provides scalable and secure virtual servers in the

cloud. Users can launch, stop, or terminate EC2 instances as needed, and choose from various instance types, operating systems, and configurations4. Uploading and storing content in Amazon S3 in the Region that is closest to the user and using multiple distributions of Amazon CloudFront is not correct because this solution is not cost-effective or efficient for the use case. As mentioned above, Amazon CloudFront is a CDN that helps users distribute their content globally with low latency and high transfer speeds. However, creating multiple CloudFront distributions for each Region would incur additional charges and management overhead, and would not be necessary since 90% of the content is consumed within the same Region where it is uploaded3.

References:

- What Is Amazon Simple Storage Service? - Amazon Simple Storage Service
- Amazon S3 Transfer Acceleration - Amazon Simple Storage Service
- What Is Amazon CloudFront? - Amazon CloudFront
- What Is Amazon EC2? - Amazon Elastic Compute Cloud

441. - (Topic 4)

A group requires permissions to list an Amazon S3 bucket and delete objects from that bucket An administrator has created the following 1AM policy to provide access to the bucket and applied that policy to the group. The group is not able to delete objects in the bucket. The company follows least-privilege access rules.

A)

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

B)

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

C)

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

D)

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

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

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

"Statement": [

{

"Action": ["s3:ListBucket", "s3:DeleteObject"

],

"Resource": ["arn:aws:s3:::<bucket-name>"

],

"Effect": "Allow",

},

{

"Action": "s3:*DeleteObject", "Resource": [

"arn:aws:s3:::<bucket-name>/*" # <- The policy clause kludge "added" to match the solution (Q248.1) example

],

"Effect": "Allow"

}

]

}

442. - (Topic 4)

A company wants to use Amazon Elastic Container Service (Amazon ECS) clusters and Amazon RDS DB instances to build and run a payment processing application. The company will run the application in its on-premises data center for compliance purposes.

A solutions architect wants to use AWS Outposts as part of the solution. The solutions architect is working with the company's operational team to build the application.

Which activities are the responsibility of the company's operational team? (Select THREE.)

A. Providing resilient power and network connectivity to the Outposts racks

B. Managing the virtualization hypervisor, storage systems, and the AWS services that run on Outposts

C. Physical security and access controls of the data center environment

D. Availability of the Outposts infrastructure including the power supplies, servers, and network-ing equipment within the Outposts racks

E. Physical maintenance of Outposts components

F. Providing extra capacity for Amazon ECS clusters to mitigate server failures and maintenance events

Answer: A,C,F

Explanation: These answers are correct because they reflect the customer’s responsibilities for using AWS Outposts as part of the solution. According to the AWS shared responsibility model, the customer is responsible for providing resilient power and network connectivity to the Outposts racks, ensuring physical security and access controls of the data center environment, and providing extra capacity for Amazon ECS clusters to mitigate server failures and maintenance events. AWS is responsible for managing the virtualization hypervisor, storage systems, and the AWS services that run on Outposts, as well as the availability of the Outposts infrastructure including the power supplies, servers, and networking equipment

within the Outposts racks, and the physical maintenance of Outposts components.

References:

- https://docs.aws.amazon.com/outposts/latest/userguide/what-is-outposts.html
- https://www.contino.io/insights/the-sandwich-responsibility-model-aws-outposts/

443. - (Topic 4)

A company wants to deploy its containerized application workloads to a VPC across three Availability Zones. The company needs a solution that is highly available across Availability Zones. The solution must require minimal changes to the application.

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

A. Use Amazon Elastic Container Service (Amazon ECS). Configure Amazon ECS Service Auto Scaling to use target tracking scaling. Set the minimum capacity to 3. Set the task placement strategy type to spread with an Availability Zone attribute.

B. Use Amazon Elastic Kubernetes Service (Amazon EKS) self-managed nodes. Configure Application Auto Scaling to use target tracking scaling. Set the minimum capacity to 3.

C. Use Amazon EC2 Reserved Instances. Launch three EC2 instances in a spread placement group. Configure an Auto Scaling group to use target tracking scaling. Set the minimum capacity to 3.

D. Use an AWS Lambda function. Configure the Lambda function to connect to a VPC. Configure Application Auto Scaling to use Lambda as a scalable target. Set the minimum capacity to 3.

Answer: A

Explanation: The company wants to deploy its containerized application workloads to a VPC across three Availability Zones, with high availability and minimal changes to the application. The solution that will meet these requirements with the least operational overhead is:

- Use Amazon Elastic Container Service (Amazon ECS). Amazon ECS is a fully managed container orchestration service that allows you to run and scale containerized applications on AWS. Amazon ECS eliminates the need for you to install, operate, and scale your own cluster management infrastructure. Amazon ECS also integrates with other AWS services, such as VPC, ELB, CloudFormation, CloudWatch, IAM, and more.
- Configure Amazon ECS Service Auto Scaling to use target tracking scaling.

Amazon ECS Service Auto Scaling allows you to automatically adjust the number of tasks in your service

based on the demand or custom metrics. Target tracking scaling is a policy type that adjusts the number of tasks in your service to keep a specified metric at a target value. For example, you can use target tracking scaling to maintain a target CPU utilization or request count per task for your service.

- Set the minimum capacity to 3. This ensures that your service always has at least three tasks running across three Availability Zones, providing high availability and fault tolerance for your application.
- Set the task placement strategy type to spread with an Availability Zone attribute. This ensures that your tasks are evenly distributed across the Availability Zones in your cluster, maximizing the availability of your service.

This solution will provide high availability across Availability Zones, require minimal changes to the application, and reduce the operational overhead of managing your own cluster infrastructure.

References:

- Amazon Elastic Container Service
- Amazon ECS Service Auto Scaling
- Target Tracking Scaling Policies for Amazon ECS Services
- Amazon ECS Task Placement Strategies

444. - (Topic 4)

A company needs to extract the names of ingredients from recipe records that are stored as text files in an Amazon S3 bucket A web application will use the ingredient names to query an Amazon DynamoDB table and determine a nutrition score.

The application can handle non-food records and errors The company does not have any employees who have machine learning knowledge to develop this solution

Which solution will meet these requirements MOST cost-effectively?

A. Use S3 Event Notifications to invoke an AWS Lambda function when PutObject requests occur Program the Lambda function to analyze the object and extract the ingredient names by using Amazon Comprehend Store the Amazon Comprehend output in the DynamoDB table.

B. Use an Amazon EventBridge rule to invoke an AWS Lambda function when PutObject requests occur. Program the Lambda function to analyze the object by using Amazon Forecast to extract the ingredient names Store the Forecast output in the DynamoDB table.

C. Use S3 Event Notifications to invoke an AWS Lambda function when PutObject requests occur Use Amazon Polly to create audio recordings of the recipe records. Save the audio files in the S3 bucket Use Amazon Simple Notification Service (Amazon SNS) to send a URL as a message to employees Instruct the employees to listen to the audio files and calculate the nutrition score Store the ingredient names in the DynamoDB table.

D. Use an Amazon EventBridge rule to invoke an AWS Lambda function when a PutObject request occurs Program the Lambda function to analyze the object and extract the ingredient names by using Amazon SageMaker Store the inference output from the SageMaker endpoint in the DynamoDB table.

Answer: A

Explanation: This solution meets the following requirements:

- It is cost-effective, as it only uses serverless components that are charged based on usage and do not require any upfront provisioning or maintenance.
- It is scalable, as it can handle any number of recipe records that are uploaded to the S3 bucket without any performance degradation or manual intervention.
- It is easy to implement, as it does not require any machine learning knowledge or complex data processing logic. Amazon Comprehend is a natural language processing service that can automatically extract entities such as ingredients from text files. The Lambda function can simply invoke the Comprehend API and store the results in the DynamoDB table.
- It is reliable, as it can handle non-food records and errors gracefully. Amazon Comprehend can detect the language and domain of the text files and return an appropriate response. The Lambda function can also implement error handling and logging mechanisms to ensure the data quality and integrity.

References:

- Using AWS Lambda with Amazon S3 - AWS Lambda
- What Is Amazon Comprehend? - Amazon Comprehend
- Working with Tables - Amazon DynamoDB

445. - (Topic 4)

A company is building a three-tier application on AWS. The presentation tier will serve a static website. The logic tier is a containerized application. This application will store data in a relational database. The company wants to simplify deployment and to reduce operational costs.

Which solution will meet these requirements?

A. Use Amazon S3 to host static content. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute power. Use a managed Amazon RDS cluster for the database.

B. Use Amazon CloudFront to host static content. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 for compute power. Use a managed Amazon RDS cluster for the database.

C. Use Amazon S3 to host static content. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute power. Use a managed Amazon RDS cluster for the database.

D. Use Amazon EC2 Reserved Instances to host static content. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 for compute power. Use a managed Amazon RDS cluster for the database.

Answer: A

Explanation: Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance. You can use Amazon S3 to host static content for your website, such as HTML files, images, videos, etc. Amazon Elastic Container Service (Amazon ECS) is a fully managed container orchestration service that allows you to run and scale containerized applications on AWS. AWS Fargate is a serverless compute engine for containers that works with both Amazon ECS and Amazon EKS. Fargate makes it easy for you to focus on building your applications by removing the need to provision and manage servers. You can use Amazon ECS with AWS Fargate for compute power for your containerized application logic tier. Amazon RDS is a managed relational database service that makes it easy to set up, operate, and scale a relational database in the cloud. You can use a managed Amazon RDS cluster for the database tier of your application. This solution will simplify deployment and reduce operational costs for your three-tier application. References: https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

446. - (Topic 4)

A company is using a centralized AWS account to store log data in various Amazon S3 buckets. A solutions architect needs to ensure that the data is encrypted at rest before the data is uploaded to the S3 buckets. The data also must be encrypted in transit.

Which solution meets these requirements?

A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.

B. Use server-side encryption to encrypt the data that is being uploaded to the S3 buckets.

C. Create bucket policies that require the use of server-side encryption with S3 managed encryption keys (SSE-S3) for S3 uploads.

D. Enable the security option to encrypt the S3 buckets through the use of a default AWS Key Management Service (AWS KMS) key.

Answer: A

Explanation: Client-side encryption is a method of encrypting data before uploading it to Amazon S3. It allows users to manage the encryption process, encryption keys, and related tools1. By using client-side encryption, the solution can ensure that the data is encrypted at rest and in transit, as Amazon S3 will not have access to the encryption keys or the unencrypted data2.

447. - (Topic 4)

A solutions architect is designing a shared storage solution for a web application that is deployed across multiple Availability Zones The web application runs on Amazon EC2 instances that are in an Auto Scaling group The company plans to make frequent changes to the content The solution must have strong consistency in returning the new content as soon as the changes occur.

Which solutions meet these requirements? (Select TWO)

A. Use AWS Storage Gateway Volume Gateway Internet Small Computer Systems Interface (iSCSI) block storage that is mounted to the individual EC2 instances

B. Create an Amazon Elastic File System (Amazon EFS) file system Mount the EFS file system on the individual EC2 instances

C. Create a shared Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on the individual EC2 instances.

D. Use AWS DataSync to perform continuous synchronization of data between EC2 hosts in the Auto Scaling group

E. Create an Amazon S3 bucket to store the web content Set the metadata for the Cache- Control header to no-cache Use Amazon CloudFront to deliver the content

Answer: B,E

Explanation: These options are the most suitable ways to design a shared storage solution for a web

application that is deployed across multiple Availability Zones and requires strong consistency. Option B uses Amazon Elastic File System (Amazon EFS) as a shared file system that can be mounted on multiple EC2 instances in different Availability Zones. Amazon EFS provides high availability, durability, scalability, and performance for file-based workloads. It also supports strong consistency, which means that any changes made to the file system are immediately visible to all clients. Option E uses Amazon S3 as a shared object store that can store the web content and serve it through Amazon CloudFront, a content delivery network (CDN). Amazon S3 provides high availability, durability, scalability, and performance for object-based workloads. It also supports strong consistency for read-after-write and list operations, which means that any changes made to the objects are immediately visible to all clients. By setting the metadata for the Cache- Control header to no-cache, the web content can be prevented from being cached by the browsers or the CDN edge locations, ensuring that the latest content is always delivered to the users.

Option A is not suitable because using AWS Storage Gateway Volume Gateway as a shared storage solution for a web application is not efficient or scalable. AWS Storage Gateway Volume Gateway is a hybrid cloud storage service that provides block storage volumes that can be mounted on-premises or on EC2 instances as iSCSI devices. It is useful for migrating or backing up data to AWS, but it is not designed for serving web content or providing strong consistency. Moreover, using Volume Gateway would incur additional costs and complexity, and it would not leverage the native AWS storage services.

Option C is not suitable because creating a shared Amazon EBS volume and mounting it on multiple EC2 instances is not possible or reliable. Amazon EBS is a block storage service that provides persistent and high-performance volumes for EC2 instances. However, EBS volumes can only be attached to one EC2 instance at a time, and they are constrained to a single Availability Zone. Therefore, creating a shared EBS volume for a web application that is deployed across multiple Availability Zones is not feasible. Moreover, EBS volumes do not support strong consistency, which means that any changes made to the volume may not be immediately visible to other clients.

Option D is not suitable because using AWS DataSync to perform continuous synchronization of data between EC2 hosts in the Auto Scaling group is not efficient or scalable. AWS DataSync is a data transfer service that helps you move large amounts of data to and from AWS storage services. It is useful for migrating or archiving data, but it is not designed for serving web content or providing strong consistency. Moreover, using DataSync would incur additional costs and complexity, and it would not leverage the native AWS storage services. References:

- What Is Amazon Elastic File System?
- What Is Amazon Simple Storage Service?
- What Is Amazon CloudFront?
- What Is AWS Storage Gateway?
- What Is Amazon Elastic Block Store?
- What Is AWS DataSync?

448. - (Topic 4)

An application runs on an Amazon EC2 instance that has an Elastic IP address in VPC A. The application requires access to a database in VPC B. Both VPCs are in the same AWS account.

Which solution will provide the required access MOST securely?

A. Create a DB instance security group that allows all traffic from the public IP address of the application server in VPC A.

B. Configure a VPC peering connection between VPC A and VPC B.

C. Make the DB instance publicly accessible. Assign a public IP address to the DB instance.

D. Launch an EC2 instance with an Elastic IP address into VPC B. Proxy all requests through the new EC2 instance.

Answer: B

Explanation: A VPC peering connection is a networking connection between two VPCs that enables users to route traffic between them using private IP addresses. Instances in either VPC can communicate with each other as if they are within the same network. A VPC peering connection can be created between VPCs in the same or different AWS accounts and Regions1. By configuring a VPC peering connection between VPC A and VPC B, the solution can provide the required access most securely.

* A. Create a DB instance security group that allows all traffic from the public IP address of the application server in VPC A. This solution will not provide the required access most securely, as it involves exposing the DB instance to the public internet and relying on a single IP address for access control2.

* C. Make the DB instance publicly accessible. Assign a public IP address to the DB instance. This solution will not provide the required access most securely, as it involves exposing the DB instance to the public internet and allowing any source to connect to it2.

* D. Launch an EC2 instance with an Elastic IP address into VPC B. Proxy all requests through the new

EC2 instance. This solution will not provide the required access most securely, as it involves creating an additional resource and configuring a proxy server that may introduce latency and complexity3.

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

449. - (Topic 4)

A company has multiple AWS accounts for development work. Some staff consistently use oversized Amazon EC2 instances, which causes the company to exceed the yearly budget for the development accounts The company wants to centrally restrict the creation of AWS resources in these accounts

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

A. Develop AWS Systems Manager templates that use an approved EC2 creation process. Use the approved Systems Manager templates to provision EC2 instances.

B. Use AWS Organizations to organize the accounts into organizational units (OUs). Define and attach a service control policy (SCP) to control the usage of EC2 instance types.

C. Configure an Amazon EventBridge rule that invokes an AWS Lambda function when an EC2 instance is created. Stop disallowed EC2 instance types.

D. Set up AWS Service Catalog products for the staff to create the allowed EC2 instance types Ensure that staff can deploy EC2 instances only by using the Service Catalog products.

Answer: B

Explanation: AWS Organizations is a service that helps users centrally manage and govern multiple AWS accounts. It allows users to create organizational units (OUs) to group accounts based on business needs or other criteria. It also allows users to define and attach service control policies (SCPs) to OUs or accounts to restrict the actions that can be performed by the accounts1. By using AWS Organizations, the solution can centrally restrict the creation of AWS resources in the development accounts.

* A. Develop AWS Systems Manager templates that use an approved EC2 creation process. Use the approved Systems Manager templates to provision EC2 instances. This solution will not meet the requirement of the least development effort, as it involves developing and maintaining custom templates for EC2 creation, and relying on the staff to use the approved templates instead of enforcing a restriction2.

* C. Configure an Amazon EventBridge rule that invokes an AWS Lambda function when an EC2 instance is created. Stop disallowed EC2 instance types. This solution will not meet the requirement of the least development effort, as it involves writing custom code for Lambda functions, and handling events and

errors for EC2 creation3.

* D. Set up AWS Service Catalog products for the staff to create the allowed EC2 instance types En-sure that staff can deploy EC2 instances only by using the Service Catalog products. This solution will not meet the requirement of the least development effort, as it involves setting up and managing Service Catalog products for EC2 creation, and ensuring that staff can only use Service Catalog products instead of enforcing a restriction. Reference URL: https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps. html

450. - (Topic 4)

A company has an AWS Direct Connect connection from its on-premises location to an AWS account The AWS account has 30 different VPCs in the same AWS Region The VPCs use private virtual interfaces (VIFs) Each VPC has a CIDR block that does not overlap with other networks under the company's control The company wants to centrally manage the networking architecture while still allowing each VPC to communicate with all other VPCs and on-premises networks

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

A. Create a transit gateway and associate the Direct Connect connection with a new transit VIF Turn on the transit gateway's route propagation feature

B. Create a Direct Connect gateway Recreate the private VIFs to use the new gateway Associate each VPC by creating new virtual private gateways

C. Create a transit VPC Connect the Direct Connect connection to the transit VPC Create a peenng connection between all other VPCs in the Region Update the route tables

D. Create AWS Site-to-Site VPN connections from on premises to each VPC Ensure that both VPN tunnels are UP for each connection Turn on the route propagation feature

Answer: A

Explanation: This solution meets the following requirements:

⇨ It is operationally efficient, as it only requires one transit gateway and one transit VIF to connect the Direct Connect connection to all the VPCs in the same AWS Region. The transit gateway acts as a regional network hub that simplifies the network management and reduces the number of VIFs and gateways needed.

⇨ It is scalable, as it can support up to 5000 attachments per transit gateway, which can include VPCs,

VPNs, Direct Connect gateways, and peering connections. The transit gateway can also be connected to other transit gateways in different Regions or accounts using peering connections, enabling cross-Region and cross-account connectivity.

- It is flexible, as it allows each VPC to communicate with all other VPCs and on- premises networks using dynamic routing protocols such as Border Gateway Protocol (BGP). The transit gateway's route propagation feature automatically propagates the routes from the attached VPCs and VPNs to the transit gateway route table, eliminating the need to manually update the route tables.

References:

- Transit Gateways - Amazon Virtual Private Cloud
- Working with transit gateways - AWS Direct Connect
- Amazon VPC-to-Amazon VPC connectivity options - Amazon Virtual Private Cloud Connectivity Options

451. - (Topic 4)

A company has an organization in AWS Organizations. The company runs Amazon EC2 instances across four AWS accounts in the root organizational unit (OU). There are three nonproduction accounts and one production account. The company wants to prohibit users from launching EC2 instances of a certain size in the nonproduction accounts. The company has created a service control policy (SCP) to deny access to launch instances that use the prohibited types.

Which solutions to deploy the SCP will meet these requirements? (Select TWO.)

A. Attach the SCP to the root OU for the organization.

B. Attach the SCP to the three nonproduction Organizations member accounts.

C. Attach the SCP to the Organizations management account.

D. Create an OU for the production account. Attach the SCP to the OU. Move the production member account into the new OU.

E. Create an OU for the required accounts. Attach the SCP to the OU. Move the nonproduction member accounts into the new OU.

Answer: B,E

Explanation: SCPs are a type of organization policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization. SCPs help you to ensure your accounts stay within your organization's access control

guidelines1.

To apply an SCP to a specific set of accounts, you need to create an OU for those accounts and attach the SCP to the OU. This way, the SCP affects only the member accounts in that OU and not the other accounts in the organization. If you attach the SCP to the root OU, it will apply to all accounts in the organization, including the production account, which is not the desired outcome. If you attach the SCP to the management account, it will have no effect, as SCPs do not affect users or roles in the management account1.

Therefore, the best solutions to deploy the SCP are B and E. Option B attaches the SCP directly to the three nonproduction accounts, while option E creates a separate OU for the nonproduction accounts and attaches the SCP to the OU. Both options will achieve the same result of restricting the EC2 instance types in the nonproduction accounts, but option E might be more scalable and manageable if there are more accounts or policies to be applied in the future2.

References:

- 1: Service control policies (SCPs) - AWS Organizations
- 2: Best Practices for AWS Organizations Service Control Policies in a Multi- Account Environment

452. - (Topic 4)

A company is preparing a new data platform that will ingest real-time streaming data from multiple sources. The company needs to transform the data before writing the data to Amazon S3. The company needs the ability to use SQL to query the transformed data.

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

A. Use Amazon Kinesis Data Streams to stream the data. Use Amazon Kinesis Data Analytics to transform the data. Use Amazon Kinesis Data Firehose to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.

B. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to stream the data. Use AWS Glue to transform the data and to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.

C. Use AWS Database Migration Service (AWS DMS) to ingest the data. Use Amazon EMR to transform the data and to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.

D. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to stream the data. Use Amazon Kinesis Data Analytics to transform the data and to write the data to Amazon S3. Use the Amazon RDS query editor to query the transformed data from Amazon S3.

E. Use Amazon Kinesis Data Streams to stream the data. Use AWS Glue to transform the data. Use Amazon Kinesis Data Firehose to write the data to Amazon S3. Use the Amazon RDS query editor to query the transformed data from Amazon S3.

Answer: A,B

Explanation: To ingest, transform, and query real-time streaming data from multiple sources, Amazon Kinesis and Amazon MSK are suitable solutions. Amazon Kinesis Data Streams can stream the data from various sources and integrate with other AWS services. Amazon Kinesis Data Analytics can transform the data using SQL or Apache Flink.

Amazon Kinesis Data Firehose can write the data to Amazon S3 or other destinations. Amazon Athena can query the transformed data from Amazon S3 using standard SQL. Amazon MSK can stream the data using Apache Kafka, which is a popular open-source platform for streaming data. AWS Glue can transform the data using Apache Spark or Python scripts and write the data to Amazon S3 or other destinations. Amazon Athena can also query the transformed data from Amazon S3 using standard SQL.

References:

- What Is Amazon Kinesis Data Streams?
- What Is Amazon Kinesis Data Analytics?
- What Is Amazon Kinesis Data Firehose?
- What Is Amazon Athena?
- What Is Amazon MSK?
- What Is AWS Glue?

453. - (Topic 4)

A company stores text files in Amazon S3. The text files include customer chat messages, date and time information, and customer personally identifiable information (PII).

The company needs a solution to provide samples of the conversations to an external service provider for quality control. The external service provider needs to randomly pick sample conversations up to the most recent conversation. The company must not share the customer PII with the external service provider. The

solution must scale when the number of customer conversations increases.

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

A. Create an Object Lambda Access Point. Create an AWS Lambda function that redacts the PII when the function reads the file. Instruct the external service provider to access the Object Lambda Access Point.

B. Create a batch process on an Amazon EC2 instance that regularly reads all new files, redacts the PII from the files, and writes the redacted files to a different S3 bucket. Instruct the external service provider to access the bucket that does not contain the PII.

C. Create a web application on an Amazon EC2 instance that presents a list of the files, redacts the PII from the files, and allows the external service provider to download new versions of the files that have the PII redacted.

D. Create an Amazon DynamoDB table. Create an AWS Lambda function that reads only the data in the files that does not contain PII. Configure the Lambda function to store the non-PII data in the DynamoDB table when a new file is written to Amazon S3. Grant the external service provider access to the DynamoDB table.

Answer: A

Explanation: The correct solution is to create an Object Lambda Access Point and an AWS Lambda function that redacts the PII when the function reads the file. This way, the company can use the S3 Object Lambda feature to modify the S3 object content on the fly, without creating a copy or changing the original object. The external service provider can access the Object Lambda Access Point and get the redacted version of the file. This solution has the least operational overhead because it does not require any additional storage, processing, or synchronization. The solution also scales automatically with the number of customer conversations and the demand from the external service provider. The other options are incorrect because:

- Option B is using a batch process on an EC2 instance to read, redact, and write the files to a different S3 bucket. This solution has more operational overhead because it requires managing the EC2 instance, the batch process, and the additional S3 bucket. It also introduces latency and inconsistency between the original and the redacted files.
- Option C is using a web application on an EC2 instance to present, redact, and download the files. This solution has more operational overhead because it requires managing the EC2 instance, the web application, and the download process. It also exposes the original files to the web application, which

increases the risk of leaking the PII.

➪ Option D is using a DynamoDB table and a Lambda function to store the non-PII data from the files. This solution has more operational overhead because it requires managing the DynamoDB table, the Lambda function, and the data transformation. It also changes the format and the structure of the original files, which may affect the quality control process.

References:

➪ S3 Object Lambda

➪ Object Lambda Access Point

➪ Lambda function

454. - (Topic 4)

An analytics company uses Amazon VPC to run its multi-tier services. The company wants to use RESTful APIs to offer a web analytics service to millions of users. Users must be verified by using an authentication service to access the APIs.

Which solution will meet these requirements with the MOST operational efficiency?

A. Configure an Amazon Cognito user pool for user authentication. Implement Amazon API Gateway REST APIs with a Cognito authorizer.

B. Configure an Amazon Cognito identity pool for user authentication. Implement Amazon API Gateway HTTP APIs with a Cognito authorizer.

C. Configure an AWS Lambda function to handle user authentication. Implement Amazon API Gateway REST APIs with a Lambda authorizer.

D. Configure an 1AM user to handle user authentication. Implement Amazon API Gateway HTTP APIs with an 1AM authorizer.

Answer: A

Explanation: This solution will meet the requirements with the most operational efficiency because:

➪ Amazon Cognito user pools provide a secure and scalable user directory that can store and manage user profiles, and handle user sign-up, sign-in, and access control. User pools can also integrate with social identity providers and enterprise identity providers via SAML or OIDC. User pools can issue JSON Web Tokens (JWTs) that can be used to authenticate users and authorize API requests.

➪ Amazon API Gateway REST APIs enable you to create and deploy APIs that

expose your backend services to your clients. REST APIs support multiple authorization mechanisms, including Cognito user pools, IAM, Lambda, and custom authorizers. A Cognito authorizer is a type of Lambda authorizer that uses a Cognito user pool as the identity source. When a client makes a request to a REST API method that is configured with a Cognito authorizer, API Gateway verifies the JWTs that are issued by the user pool and grants access based on the token's claims and the authorizer's configuration.

- By using Cognito user pools and API Gateway REST APIs with a Cognito authorizer, you can achieve a high level of security, scalability, and performance for your web analytics service. You can also leverage the built-in features of Cognito and API Gateway, such as user management, token validation, caching, throttling, and monitoring, without having to implement them yourself. This reduces the operational overhead and complexity of your solution.

References:

- Amazon Cognito User Pools
- Amazon API Gateway REST APIs
- Use API Gateway Lambda authorizers

455. - (Topic 4)

A company is deploying a new application on Amazon EC2 instances. The application writes data to Amazon Elastic Block Store (Amazon EBS) volumes. The company needs to ensure that all data that is written to the EBS volumes is encrypted at rest.

Which solution will meet this requirement?

A. Create an 1AM role that specifies EBS encryption. Attach the role to the EC2 instances.

B. Create the EBS volumes as encrypted volumes. Attach the EBS volumes to the EC2 instances

C. Create an EC2 instance tag that has a key of Encrypt and a value of True. Tag all instances that require encryption at the EBS level.

D. Create an AWS Key Management Service (AWS KMS) key policy that enforces EBS encryption in the account. Ensure that the key policy is active

Answer: B

Explanation: The solution that will meet the requirement of ensuring that all data that is written to the EBS volumes is encrypted at rest is B. Create the EBS volumes as encrypted volumes and attach the encrypted EBS volumes to the EC2 instances. When you create an EBS volume, you can specify whether to encrypt

the volume. If you choose to encrypt the volume, all data written to the volume is automatically encrypted at rest using AWS- managed keys. You can also use customer-managed keys (CMKs) stored in AWS KMS to encrypt and protect your EBS volumes. You can create encrypted EBS volumes and attach them to EC2 instances to ensure that all data written to the volumes is encrypted at rest.

456. - (Topic 4)

A company runs an application on a group of Amazon Linux EC2 instances. For compliance reasons, the company must retain all application log files for 7 years. The log files will be analyzed by a reporting tool that must be able to access all the files concurrently.

Which storage solution meets these requirements MOST cost-effectively?

A. Amazon Elastic Block Store (Amazon EBS)

B. Amazon Elastic File System (Amazon EFS)

C. Amazon EC2 instance store

D. Amazon S3

Answer: D

Explanation: https://docs.aws.amazon.com/efs/latest/ug/transfer-data-to-efs.html

457. - (Topic 4)

A company hosts an internal serverless application on AWS by using Amazon API Gateway and AWS Lambda. The company's employees report issues with high latency when they begin using the application each day. The company wants to reduce latency.

Which solution will meet these requirements?

A. Increase the API Gateway throttling limit.

B. Set up a scheduled scaling to increase Lambda provisioned concurrency before employees begin to use the application each day.

C. Create an Amazon CloudWatch alarm to initiate a Lambda function as a target for the alarm at the beginning of each day.

D. Increase the Lambda function memory.

Answer: B

Explanation: AWS Lambda is a serverless compute service that lets you run code without provisioning or

managing servers. Lambda scales automatically based on the incoming requests, but it may take some time to initialize new instances of your function if there is a sudden increase in demand. This may result in high latency or cold starts for your application. To avoid this, you can use provisioned concurrency, which ensures that your function is initialized and ready to respond at any time. You can also set up a scheduled scaling policy that increases the provisioned concurrency before employees begin to use the application each day, and decreases it when the demand is low. References:

https://docs.aws.amazon.com/lambda/latest/dg/configuration-concurrency.html

458. - (Topic 4)

A company has a financial application that produces reports. The reports average 50 KB in size and are stored in Amazon S3. The reports are frequently accessed during the first week after production and must be stored for several years. The reports must be retrievable within 6 hours.

Which solution meets these requirements MOST cost-effectively?

A. Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Glacier after 7 days.

B. Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Standard- Infrequent Access (S3 Standard-IA) after 7 days.

C. Use S3 Intelligent-Tiering. Configure S3 Intelligent-Tiering to transition the reports to S3 Standard-Infrequent Access (S3 Standard-IA) and S3 Glacier.

D. Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Glacier Deep Archive after 7 days.

Answer: A

Explanation: To store and retrieve reports that are frequently accessed during the first week and must be stored for several years, S3 Standard and S3 Glacier are suitable

solutions. S3 Standard offers high durability, availability, and performance for frequently accessed data. S3 Glacier offers secure and durable storage for long-term data archiving at a low cost. S3 Lifecycle rules can be used to transition the reports from S3 Standard to S3 Glacier after 7 days, which can reduce storage costs. S3 Glacier also supports retrieval within 6 hours.

References:

- Storage Classes
- Object Lifecycle Management

- Retrieving Archived Objects from Amazon S3 Glacier

459. - (Topic 4)

A company wants to migrate its on-premises Microsoft SQL Server Enterprise edition database to AWS. The company's online application uses the database to process transactions. The data analysis team uses the same production database to run reports for analytical processing. The company wants to reduce operational overhead by moving to managed services wherever possible.

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

A. Migrate to Amazon RDS for Microsoft SQL Server. Use read replicas for reporting purposes.

B. Migrate to Microsoft SQL Server on Amazon EC2. Use Always On read replicas for reporting purposes.

C. Migrate to Amazon DynamoDB. Use DynamoDB on-demand replicas for reporting purposes.

D. Migrate to Amazon Aurora MySQL. Use Aurora read replicas for reporting purposes.

Answer: A

Explanation: Amazon RDS for Microsoft SQL Server is a fully managed service that offers SQL Server 2014, 2016, 2017, and 2019 editions while offloading database administration tasks such as backups, patching, and scaling. Amazon RDS supports read replicas, which are read-only copies of the primary database that can be used for reporting purposes without affecting the performance of the online application. This solution will meet the requirements with the least operational overhead, as it does not require any code changes or manual intervention.

References:

- 1 provides an overview of Amazon RDS for Microsoft SQL Server and its benefits.
- 2 explains how to create and use read replicas with Amazon RDS.

460. - (Topic 4)

A company's applications run on Amazon EC2 instances in Auto Scaling groups. The company notices that its applications experience sudden traffic increases on random days of the week The company wants to maintain application performance during sudden traffic increases.

Which solution will meet these requirements MOST cost-effectively?

A. Use manual scaling to change the size of the Auto Scaling group.

B. Use predictive scaling to change the size of the Auto Scaling group.

C. Use dynamic scaling to change the size of the Auto Scaling group.

D. Use schedule scaling to change the size of the Auto Scaling group

Answer: C

Explanation: Dynamic scaling is a type of autoscaling that automatically adjusts the number of EC2 instances in an Auto Scaling group based on demand or load. It uses CloudWatch alarms to trigger scaling actions when a specified metric crosses a threshold. It can scale out (add instances) or scale in (remove instances) as neede1d. By using dynamic scaling, the solution can maintain application performance during sudden traffic increases most cost-effectively.

* A. Use manual scaling to change the size of the Auto Scaling group. This solution will not meet the requirement of maintaining application performance during sudden traffic increases, as manual scaling requires users to manually increase or decrease the number of instances through a CLI or console. It does not respond automatically to changes in demand or load2.

* B. Use predictive scaling to change the size of the Auto Scaling group. This solution will not meet the requirement of most cost-effectiveness, as predictive scaling uses machine learning and artificial intelligence tools to evaluate traffic loads and anticipate when more or fewer resources are needed. It performs scheduled scaling actions based on the prediction, which may not match the actual demand or load at any given time. Predictive scaling is more suitable for scenarios where there are predictable traffic patterns or known changes in traffic loads3.

* D. Use schedule scaling to change the size of the Auto Scaling group. This solution will not meet the requirement of maintaining application performance during sudden traffic increases, as schedule scaling performs scaling actions at specific times that users schedule. It does not respond automatically to changes in demand or load. Schedule scaling is more suitable for scenarios where there are predictable traffic drops or spikes at specific times of the day.

Reference URL: https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-on-demand.html

461. - (Topic 4)

A development team is collaborating with another company to create an integrated product. The other company needs to access an Amazon Simple Queue Service (Amazon SQS) queue that is contained in the development team's account. The other company wants to poll the queue without giving up its own account permissions to do so.

How should a solutions architect provide access to the SQS queue?

A. Create an instance profile that provides the other company access to the SQS queue.

B. Create an 1AM policy that provides the other company access to the SQS queue.

C. Create an SQS access policy that provides the other company access to the SQS queue.

D. Create an Amazon Simple Notification Service (Amazon SNS) access policy that provides the other company access to the SQS queue.

Answer: C

Explanation: To provide access to the SQS queue to the other company without giving up its own account permissions, a solutions architect should create an SQS access policy that provides the other company access to the SQS queue. An SQS access policy is a resource-based policy that defines who can access the queue and what actions they can perform. The policy can specify the AWS account ID of the other company as a principal, and grant permissions for actions such as sqs:ReceiveMessage, sqs:DeleteMessage, and sqs:GetQueueAttributes. This way, the other company can poll the queue using its own credentials, without needing to assume a role or use cross-account access keys. References:

- Using identity-based policies (IAM policies) for Amazon SQS
- Using custom policies with the Amazon SQS access policy language

462. - (Topic 4)

A company hosts multiple applications on AWS for different product lines. The applications use different compute resources, including Amazon EC2 instances and Application Load Balancers. The applications run in different AWS accounts under the same organization in AWS Organizations across multiple AWS Regions. Teams for each product line have tagged each compute resource in the individual accounts.

The company wants more details about the cost for each product line from the consolidated billing feature in Organizations.

Which combination of steps will meet these requirements? (Select TWO.)

A. Select a specific AWS generated tag in the AWS Billing console.

B. Select a specific user-defined tag in the AWS Billing console.

C. Select a specific user-defined tag in the AWS Resource Groups console.

D. Activate the selected tag from each AWS account.

E. Activate the selected tag from the Organizations management account.

Answer: B,E

Explanation: User-defined tags are key-value pairs that can be applied to AWS resources to categorize and track them. User-defined tags can also be used to allocate costs and create detailed billing reports in the AWS Billing console. To use user-defined tags for cost allocation, the tags must be activated from the Organizations management account, which is the root account that has full control over all the member accounts in the organization. Once activated, the user-defined tags will appear as columns in the cost allocation report, and can be used to filter and group costs by product line. This solution will meet the requirements with the least operational overhead, as it leverages the existing tagging strategy and does not require any code development or manual intervention.

References:

- 1 explains how to use user-defined tags for cost allocation.
- 2 describes how to access and manage member accounts from the Organizations management account.
- 3 discusses how to create and view cost allocation reports in the AWS Billing console.

463. - (Topic 4)

A company wants to experiment with individual AWS accounts for its engineer team. The company wants to be notified as soon as the Amazon EC2 instance usage for a given month exceeds a specific threshold for each account.

What should a solutions architect do to meet this requirement MOST cost-effectively?

A. Use Cost Explorer to create a daily report of costs by service. Filter the report by EC2 instances. Configure Cost Explorer to send an Amazon Simple Email Service (Amazon SES) notification when a threshold is exceeded.

B. Use Cost Explorer to create a monthly report of costs by service. Filter the report by EC2 instances. Configure Cost Explorer to send an Amazon Simple Email Service (Amazon SES) notification when a threshold is exceeded.

C. Use AWS Budgets to create a cost budget for each account. Set the period to monthly. Set the scope to EC2 instances. Set an alert threshold for the budget. Configure an Amazon Simple Notification Service

(Amazon SNS) topic to receive a notification when a threshold is exceeded.

D. Use AWS Cost and Usage Reports to create a report with hourly granularity. Integrate the report data with Amazon Athena. Use Amazon EventBridge to schedule an Athena query. Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded.

Answer: C

Explanation: AWS Budgets allows you to create budgets for your AWS accounts and set alerts when usage exceeds a certain threshold. By creating a budget for each account, specifying the period as monthly and the scope as EC2 instances, you can effectively track the EC2 usage for each account and be notified when a threshold is exceeded. This solution is the most cost-effective option as it does not require additional resources such as Amazon Athena or Amazon EventBridge.

464. - (Topic 4)

A solutions architect is creating a new Amazon CloudFront distribution for an application. Some of the information submitted by users is sensitive. The application uses HTTPS but needs another layer of security. The sensitive information should.be protected throughout the entire application stack, and access to the information should be restricted to certain applications.

Which action should the solutions architect take?

A. Configure a CloudFront signed URL.

B. Configure a CloudFront signed cookie.

C. Configure a CloudFront field-level encryption profile.

D. Configure CloudFront and set the Origin Protocol Policy setting to HTTPS Only for the Viewer Protocol Policy.

Answer: C

Explanation: it allows the company to protect sensitive information submitted by users throughout the entire application stack and restrict access to certain applications. By configuring a CloudFront field-level encryption profile, the company can encrypt specific fields of user data at the edge locations before sending it to the origin servers. By using public-private key pairs, the company can ensure that only authorized applications can decrypt and access the sensitive information. References:

- Field-Level Encryption
- Encrypting and Decrypting Data

465. - (Topic 4)

A medical research lab produces data that is related to a new study. The lab wants to make the data available with minimum latency to clinics across the country for their on-premises, file-based applications. The data files are stored in an Amazon S3 bucket that has read- only permissions for each clinic.

What should a solutions architect recommend to meet these requirements?

A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic

B. Migrate the files to each clinic's on-premises applications by using AWS DataSync for processing.

C. Deploy an AWS Storage Gateway volume gateway as a virtual machine (VM) on premises at each clinic.

D. Attach an Amazon Elastic File System (Amazon EFS) file system to each clinic's on- premises servers.

Answer: A

Explanation: AWS Storage Gateway is a service that connects an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization's on-premises IT environment and AWS's storage infrastructure. By deploying a file gateway as a virtual machine on each clinic's premises, the medical research lab can provide low-latency access to the data stored in the S3 bucket while maintaining read-only permissions for each clinic. This solution allows the clinics to access the data files directly from their on-premises file-based applications without the need for data transfer or migration.

466. - (Topic 4)

A company runs a highly available web application on Amazon EC2 instances behind an Application Load Balancer The company uses Amazon CloudWatch metrics

As the traffic to the web application Increases, some EC2 instances become overloaded with many outstanding requests The CloudWatch metrics show that the number of requests processed and the time to receive the responses from some EC2 instances are both higher compared to other EC2 instances The company does not want new requests to be forwarded to the EC2 instances that are already overloaded.

Which solution will meet these requirements?

A. Use the round robin routing algorithm based on the RequestCountPerTarget and Active Connection Count CloudWatch metrics.

B. Use the least outstanding requests algorithm based on the RequestCountPerTarget and

ActiveConnectionCount CloudWatch metrics.

C. Use the round robin routing algorithm based on the RequestCount and TargetResponseTime CloudWatch metrics.

D. Use the least outstanding requests algorithm based on the RequestCount and TargetResponseTime CloudWatch metrics.

Answer: D

Explanation: The least outstanding requests (LOR) algorithm is a load balancing algorithm that distributes incoming requests to the target with the fewest outstanding requests. This helps to avoid overloading any single target and improves the overall performance and availability of the web application. The LOR algorithm can use the RequestCount and TargetResponseTime CloudWatch metrics to determine the number of outstanding requests and the response time of each target. These metrics measure the number of requests processed by each target and the time elapsed after the request leaves the load balancer until a response from the target is received by the load balancer, respectively. By using these metrics, the LOR algorithm can route new requests to the targets that are less busy and more responsive, and avoid sending requests to the targets that are already overloaded or slow. This solution meets the requirements of the company.

References:

- Application Load Balancer now supports Least Outstanding Requests algorithm for load balancing requests
- Target groups for your Application Load Balancers
- Elastic Load Balancing - Application Load Balancers

467. - (Topic 4)

A security audit reveals that Amazon EC2 instances are not being patched regularly. A solutions architect needs to provide a solution that will run regular security scans across a large fleet of EC2 instances. The solution should also patch the EC2 instances on a regular schedule and provide a report of each instance's patch status.

Which solution will meet these requirements?

A. Set up Amazon Macie to scan the EC2 instances for software vulnerabilities. Set up a cron job on each EC2 instance to patch the instance on a regular schedule.

B. Turn on Amazon GuardDuty in the account. Configure GuardDuty to scan the EC2 instances for software vulnerabilities. Set up AWS Systems Manager Session Manager to patch the EC2 instances on a regular schedule.

C. Set up Amazon Detective to scan the EC2 instances for software vulnerabilities. Set up an Amazon EventBridge scheduled rule to patch the EC2 instances on a regular schedule.

D. Turn on Amazon Inspector in the account. Configure Amazon Inspector to scan the EC2 instances for software vulnerabilities. Set up AWS Systems Manager Patch Manager to patch the EC2 instances on a regular schedule.

Answer: D

Explanation: Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity1. Amazon Inspector can scan the EC2 instances for software vulnerabilities and provide a report of each instance's patch status. AWS Systems Manager Patch Manager is a capability of AWS Systems Manager that automates the process of patching managed nodes with both security-related updates and other types of updates. Patch Manager uses patch baselines, which include rules for auto- approving patches within days of their release, in addition to optional lists of approved and rejected patches. Patch Manager can patch fleets of Amazon EC2 instances, edge devices, on-premises servers, and virtual machines (VMs) by operating system type2. Patch Manager can patch the EC2 instances on a regular schedule and provide a report of each instance's patch status. Therefore, the combination of Amazon Inspector and AWS Systems Manager Patch Manager will meet the requirements of the question.

The other options are not valid because:

- Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie does not scan the EC2 instances for software vulnerabilities, but rather for data classification and protection3. A cron job is a Linux command for scheduling a task to be executed sometime in the future. A cron job is not a reliable way to patch the EC2 instances on a regular schedule, as it may fail or be interrupted by other processes4.
- Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. Amazon

GuardDuty does not scan the EC2 instances for software vulnerabilities, but rather for network and API activity anomalies5. AWS Systems Manager Session Manager is a fully managed AWS Systems Manager capability

that lets you manage your Amazon EC2 instances, edge devices, on-premises servers, and virtual machines (VMs) through an interactive one-click browser- based shell or the AWS Command Line Interface (AWS CLI). Session Manager does not patch the EC2 instances on a regular schedule, but rather provides secure and auditable node management2.

➪ Amazon Detective is a security service that makes it easy to analyze, investigate,

and quickly identify the root cause of potential security issues or suspicious activities. Amazon Detective does not scan the EC2 instances for software vulnerabilities, but rather collects and analyzes data from AWS sources such as Amazon GuardDuty, Amazon VPC Flow Logs, and AWS CloudTrail. Amazon EventBridge is a serverless event bus that makes it easy to connect applications using data from your own applications, integrated Software-as-a-Service (SaaS) applications, and AWS services. EventBridge delivers a stream of real-time data from event sources, such as Zendesk, Datadog, or Pagerduty, and routes that data to targets like AWS Lambda. EventBridge does not patch the EC2 instances on a regular schedule, but rather triggers actions based on events.

References: Amazon Inspector, AWS Systems Manager Patch Manager, Amazon Macie, Cron job, Amazon GuardDuty, [Amazon Detective], [Amazon EventBridge]

468. - (Topic 4)

The following IAM policy is attached to an IAM group. This is the only policy applied to the group.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-1"
                }
            }
        },
        {
            "Sid": "2",
            "Effect": "Deny",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {"aws:MultiFactorAuthPresent": false}
            }
        }
    ]
}
```

A. Group members are permitted any Amazon EC2 action within the us-east-1 Region. Statements after the Allow permission are not applied.

B. Group members are denied any Amazon EC2 permissions in the us-east-1 Region unless they are logged in with multi-factor authentication (MFA).

C. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for all Regions when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action.

D. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action within the us-east-1 Region.

Answer: D

Explanation: This answer is correct because it reflects the effect of the IAM policy on the group members. The policy has two statements: one with an Allow effect and one with a Deny effect. The Allow statement grants permission to perform any EC2 action on any resource within the us-east-1 Region. The Deny statement overrides the Allow statement and denies permission to perform the ec2:StopInstances and ec2:TerminateInstances actions on any resource within the us-east-1 Region, unless the group member is

logged in with MFA. Therefore, the group members can perform any EC2 action except stopping or terminating instances in the us-east-1 Region, unless they use MFA.

469. - (Topic 4)

A gaming company uses Amazon DynamoDB to store user information such as geographic location, player data, and leaderboards. The company needs to configure continuous backups to an Amazon S3 bucket with a minimal amount of coding. The backups must not affect availability of the application and must not affect the read capacity units (RCUs) that are defined for the table

Which solution meets these requirements?

A. Use an Amazon EMR cluster. Create an Apache Hive job to back up the data to Amazon S3.

B. Export the data directly from DynamoDB to Amazon S3 with continuous backups. Turn on point-in-time recovery for the table.

C. Configure Amazon DynamoDB Streams. Create an AWS Lambda function to consume the stream and export the data to an Amazon S3 bucket.

D. Create an AWS Lambda function to export the data from the database tables to Amazon S3 on a regular basis. Turn on point-in-time recovery for the table.

Answer: B

Explanation: https://aws.amazon.com/blogs/database/dynamodb-streams-use-cases-and- design-patterns/ https://aws.amazon.com/premiumsupport/knowledge-center/back-up-dynamodb-s3/

470. - (Topic 4)

A company's web application that is hosted in the AWS Cloud recently increased in popularity. The web application currently exists on a single Amazon EC2 instance in a single public subnet. The web application has not been able to meet the demand of the increased web traffic.

The company needs a solution that will provide high availability and scalability to meet the increased user demand without rewriting the web application.

Which combination of steps will meet these requirements? (Select TWO.)

A. Replace the EC2 instance with a larger compute optimized instance.

B. Configure Amazon EC2 Auto Scaling with multiple Availability Zones in private subnets.

C. Configure a NAT gateway in a public subnet to handle web requests.

D. Replace the EC2 instance with a larger memory optimized instance.

E. Configure an Application Load Balancer in a public subnet to distribute web traffic

Answer: B,E

Explanation:

These two steps will meet the requirements because they will provide high availability and scalability for the web application without rewriting it. Amazon EC2 Auto Scaling allows you to automatically adjust the number of EC2 instances in response to changes in demand. By configuring Auto Scaling with multiple Availability Zones in private subnets, you can ensure that your web application is distributed across isolated and fault-tolerant locations, and that your instances are not directly exposed to the internet. An Application Load Balancer operates at the application layer and distributes incoming web traffic across multiple targets, such as EC2 instances, containers, or Lambda functions. By configuring an Application Load Balancer in a public subnet, you can enable your web application to handle requests from the internet and route them to the appropriate targets in the private subnets.

References:

- What is Amazon EC2 Auto Scaling?
- What is an Application Load Balancer?

471. - (Topic 4)

A company runs a three-tier web application in a VPC across multiple Availability Zones. Amazon EC2 instances run in an Auto Scaling group for the application tier.

The company needs to make an automated scaling plan that will analyze each resource's daily and weekly historical workload trends. The configuration must scale resources appropriately according to both the forecast and live changes in utilization.

Which scaling strategy should a solutions architect recommend to meet these requirements?

A. Implement dynamic scaling with step scaling based on average CPU utilization from the EC2 instances.

B. Enable predictive scaling to forecast and scale. Configure dynamic scaling with target tracking.

C. Create an automated scheduled scaling action based on the traffic patterns of the web application.

D. Set up a simple scaling policy. Increase the cooldown period based on the EC2 instance startup time

Answer: B

Explanation:

This solution meets the requirements because it allows the company to use both predictive scaling and dynamic scaling to optimize the capacity of its Auto Scaling group. Predictive scaling uses machine learning to analyze historical data and forecast future traffic patterns. It then adjusts the desired capacity of the group in advance of the predicted changes. Dynamic scaling uses target tracking to maintain a specified metric (such as CPU utilization) at a target value. It scales the group in or out as needed to keep the metric close to the target. By using both scaling methods, the company can benefit from faster, simpler, and more accurate scaling that responds to both forecasted and live changes in utilization. References:

- Predictive scaling for Amazon EC2 Auto Scaling
- [Target tracking scaling policies for Amazon EC2 Auto Scaling]

472. - (Topic 4)

A company uses Amazon Elastic Kubernetes Service (Amazon EKS) to run a container application. The EKS cluster stores sensitive information in the Kubernetes secrets object. The company wants to ensure that the information is encrypted

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

A. Use the container application to encrypt the information by using AWS Key Management Service (AWS KMS).

B. Enable secrets encryption in the EKS cluster by using AWS Key Management Service (AWS KMS)_

C. Implement an AWS Lambda tuncüon to encrypt the information by using AWS Key Management Service (AWS KMS).

D. use AWS Systems Manager Parameter Store to encrypt the information by using AWS Key Management Service (AWS KMS).

Answer: B

Explanation: it allows the company to encrypt the Kubernetes secrets object in the EKS cluster with the least operational overhead. By enabling secrets encryption in the EKS

cluster, the company can use AWS Key Management Service (AWS KMS) to generate and manage encryption keys for encrypting and decrypting secrets at rest. This is a simple and secure way to protect sensitive information in EKS clusters. References:

- Encrypting Kubernetes secrets with AWS KMS
- Kubernetes Secrets

473. - (Topic 4)

A company wants to use artificial intelligence (AI) to determine the quality of its customer service calls. The company currently manages calls in four different languages, including English. The company will offer new languages in the future. The company does not have the resources to regularly maintain machine learning (ML) models.

The company needs to create written sentiment analysis reports from the customer service call recordings. The customer service call recording text must be translated into English.

Which combination of steps will meet these requirements? (Select THREE.)

A. Use Amazon Comprehend to translate the audio recordings into English.

B. Use Amazon Lex to create the written sentiment analysis reports.

C. Use Amazon Polly to convert the audio recordings into text.

D. Use Amazon Transcribe to convert the audio recordings in any language into text.

E. Use Amazon Translate to translate text in any language to English.

F. Use Amazon Comprehend to create the sentiment analysis reports.

Answer: D,E,F

Explanation: These answers are correct because they meet the requirements of creating written sentiment analysis reports from the customer service call recordings in any language and translating them into English. Amazon Transcribe is a service that uses advanced machine learning technologies to recognize speech in audio files and transcribe them into text. You can use Amazon Transcribe to convert the audio recordings in any language into text, and specify the language code of the source audio. Amazon Translate is a neural machine translation service that delivers fast, high-quality, and affordable language translation. You can use Amazon Translate to translate text in any language to English, and specify the source and target language codes. Amazon Comprehend is a natural language processing (NLP) service that uses machine learning to find insights and relationships in text. You can use Amazon Comprehend to create the sentiment analysis reports, which determine if the text is positive, negative, neutral, or mixed.

References:

- https://docs.aws.amazon.com/transcribe/latest/dg/what-is-transcribe.html
- https://docs.aws.amazon.com/translate/latest/dg/what-is.html
- https://docs.aws.amazon.com/comprehend/latest/dg/how-sentiment.html

474. - (Topic 4)

A company runs a three-tier web application in the AWS Cloud that operates across three Availability Zones. The application architecture has an Application Load Balancer, an Amazon EC2 web server that hosts user session states, and a MySQL database that runs on an EC2 instance. The company expects sudden increases in application traffic. The company wants to be able to scale to meet future application capacity demands and to ensure high availability across all three Availability Zones.

Which solution will meet these requirements?

A. Migrate the MySQL database to Amazon RDS for MySQL with a Multi-AZ DB cluster deployment. Use Amazon ElastiCache for Redis with high availability to store session data and to cache reads. Migrate the web server to an Auto Scaling group that is in three Availability Zones.

B. Migrate the MySQL database to Amazon RDS for MySQL with a Multi-AZ DB cluster deployment. Use Amazon ElastiCache for Memcached with high availability to store session data and to cache reads. Migrate the web server to an Auto Scaling group that is in three Availability Zones.

C. Migrate the MySQL database to Amazon DynamoDB. Use DynamoDB Accelerator (DAX) to cache reads. Store the session data in DynamoDB. Migrate the web server to an Auto Scaling group that is in three Availability Zones.

D. Migrate the MySQL database to Amazon RDS for MySQL in a single Availability Zone. Use Amazon ElastiCache for Redis with high availability to store session data and to cache reads. Migrate the web server to an Auto Scaling group that is in three Availability Zones.

Answer: A

Explanation: This answer is correct because it meets the requirements of scaling to meet future application capacity demands and ensuring high availability across all three Availability Zones. By migrating the MySQL database to Amazon RDS for MySQL with a Multi-AZ DB cluster deployment, the company can benefit from automatic failover, backup, and patching of the database across multiple Availability Zones. By using Amazon ElastiCache for Redis with high availability, the company can store session data and cache reads in a fast, in-memory data store that can also fail over across Availability Zones. By migrating the web server to an Auto Scaling group that is in three Availability Zones, the company can automatically scale the web server capacity based on the demand and traffic

patterns. References:

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html
- https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/AutoFailover.html
- https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2- auto-scaling.html

475. - (Topic 4)

A company is building a solution that will report Amazon EC2 Auto Scaling events across all the applications in an AWS account. The company needs to use a serverless solution to store the EC2 Auto Scaling status data in Amazon S3. The company then will use the data in Amazon S3 to provide near-real-time updates in a dashboard. The solution must not affect the speed of EC2 instance launches. How should the company move the data to Amazon S3 to meet these requirements?

A. Use an Amazon CloudWatch metric stream to send the EC2 Auto Scaling status data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.

B. Launch an Amazon EMR cluster to collect the EC2 Auto Scaling status data and send the data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.

C. Create an Amazon EventBridge rule to invoke an AWS Lambda function on a schedule. Configure the Lambda function to send the EC2 Auto Scaling status data directly to Amazon S3.

D. Use a bootstrap script during the launch of an EC2 instance to install Amazon Kinesis Agent. Configure Kinesis Agent to collect the EC2 Auto Scaling status data and send the data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.

Answer: A

Explanation:

You can use metric streams to continually stream CloudWatch metrics to a destination of your choice, with near-real-time delivery and low latency. One of the use cases is Data Lake: create a metric stream and direct it to an Amazon Kinesis Data Firehose delivery stream that delivers your CloudWatch metrics to a data lake such as Amazon S3.

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Metric- Streams.html

476. - (Topic 4)

A company wants to run its experimental workloads in the AWS Cloud. The company has a budget for

cloud spending. The company's CFO is concerned about cloud spending accountability for each department. The CFO wants to receive notification when the spending threshold reaches 60% of the budget.

Which solution will meet these requirements?

A. Use cost allocation tags on AWS resources to label owners. Create usage budgets in AWS Budgets. Add an alert threshold to receive notification when spending exceeds 60% of the budget.

B. Use AWS Cost Explorer forecasts to determine resource owners. Use AWS Cost Anomaly Detection to create alert threshold notifications when spending exceeds 60% of the budget.

C. Use cost allocation tags on AWS resources to label owners. Use AWS Support API on AWS Trusted Advisor to create alert threshold notifications when spending exceeds 60% of the budget

D. Use AWS Cost Explorer forecasts to determine resource owners. Create usage budgets in AWS Budgets. Add an alert threshold to receive notification when spending exceeds 60% of the budget.

Answer: A

Explanation: This solution meets the requirements because it allows the company to track and manage its cloud spending by using cost allocation tags to assign costs to different departments, creating usage budgets to set spending limits, and adding alert thresholds to receive notifications when the spending reaches a certain percentage of the budget. This way, the company can monitor its experimental workloads and avoid overspending on the cloud.

References:

- Using Cost Allocation Tags
- Creating an AWS Budget
- Creating an Alert for an AWS Budget

477. - (Topic 4)

A company has multiple AWS accounts with applications deployed in the us-west-2 Region Application logs are stored within Amazon S3 buckets in each account The company wants

to build a centralized log analysis solution that uses a single S3 bucket Logs must not leave us-west-2, and the company wants to incur minimal operational overhead

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

A. Create an S3 Lifecycle policy that copies the objects from one of the application S3 buckets to the

centralized S3 bucket

B. Use S3 Same-Region Replication to replicate logs from the S3 buckets to another S3 bucket in us-west-2 Use this S3 bucket for log analysis.

C. Write a script that uses the PutObject API operation every day to copy the entire contents of the buckets to another S3 bucket in us-west-2 Use this S3 bucket for log analysis.

D. Write AWS Lambda functions in these accounts that are triggered every time logs are delivered to the S3 buckets (s3 ObjectCreated a event) Copy the logs to another S3 bucket in us-west-2. Use this S3 bucket for log analysis.

Answer: B

Explanation: This solution meets the following requirements:

⇨ It is cost-effective, as it only charges for the storage and data transfer of the replicated objects, and does not require any additional AWS services or custom scripts. S3 Same-Region Replication (SRR) is a feature that automatically replicates objects across S3 buckets within the same AWS Region. SRR can help you aggregate logs from multiple sources to a single destination for analysis and auditing. SRR also preserves the metadata, encryption, and access control of the source objects.

⇨ It is operationally efficient, as it does not require any manual intervention or scheduling. SRR replicates objects as soon as they are uploaded to the source bucket, ensuring that the destination bucket always has the latest log data. SRR also handles any updates or deletions of the source objects, keeping the destination bucket in sync. SRR can be enabled with a few clicks in the S3 console or with a simple API call.

⇨ It is secure, as it does not allow the logs to leave the us-west-2 Region. SRR only replicates objects within the same AWS Region, ensuring that the data sovereignty and compliance requirements are met. SRR also supports encryption of the source and destination objects, using either server-side encryption with AWS KMS or S3- managed keys, or client-side encryption.

References:

⇨ Same-Region Replication - Amazon Simple Storage Service

⇨ How do I replicate objects across S3 buckets in the same AWS Region?

⇨ Centralized Logging on AWS | AWS Solutions | AWS Solutions Library

478. - (Topic 4)

A company uses multiple vendors to distribute digital assets that are stored in Amazon S3 buckets The company wants to ensure that its vendor AWS accounts have the minimum access that is needed to download objects in these S3 buckets

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

A. Design a bucket policy that has anonymous read permissions and permissions to list ail buckets.

B. Design a bucket policy that gives read-only access to users. Specify 1AM entities as principals

C. Create a cross-account 1AM role that has a read-only access policy specified for the 1AM role.

D. Create a user policy and vendor user groups that give read-only access to vendor users

Answer: C

Explanation:

A cross-account IAM role is a way to grant users from one AWS account access to resources in another AWS account. The cross-account IAM role can have a read-only access policy attached to it, which allows the users to download objects from the S3 buckets without modifying or deleting them. The cross-account IAM role also reduces the operational overhead of managing multiple IAM users and policies in each account. The cross-account IAM role meets all the requirements of the question, while the other options do not. References:

- https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-walkthroughs-managing-access-example2.html
- https://aws.amazon.com/blogs/storage/setting-up-cross-account-amazon-s3-access-with-s3-access-points/
- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for- user_externalid.html

479. - (Topic 4)

A company wants to run its payment application on AWS The application receives payment notifications from mobile devices Payment notifications require a basic validation before they are sent for further processing

The backend processing application is long running and requires compute and memory to be adjusted The company does not want to manage the infrastructure

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

A. Create an Amazon Simple Queue Service (Amazon SQS) queue Integrate the queue with an Amazon

EventBndge rule to receive payment notifications from mobile devices Configure the rule to validate payment notifications and send the notifications to the backend application Deploy the backend application on Amazon Elastic Kubernetes Service (Amazon EKS) Anywhere Create a standalone cluster

B. Create an Amazon API Gateway API Integrate the API with anAWS Step Functions state machine to receive payment notifications from mobile devices Invoke the state machine to validate payment notifications and send the notifications to the backend application Deploy the backend application on Amazon Elastic Kubernetes Sen/ice (Amazon EKS). Configure an EKS cluster with self-managed nodes.

C. Create an Amazon Simple Queue Sen/ice (Amazon SQS) queue Integrate the queue with an Amazon EventBridge rule to receive payment notifications from mobile devices Configure the rule to validate payment notifications and send the notifications to the backend application Deploy the backend application on Amazon EC2 Spot Instances Configure a Spot Fleet with a default allocation strategy.

D. Create an Amazon API Gateway API Integrate the API with AWS Lambda to receive payment notifications from mobile devices Invoke a Lambda function to validate payment notifications and send the notifications to the backend application Deploy the backend application on Amazon Elastic Container Service (Amazon ECS). Configure Amazon ECS with an AWS Fargate launch type.

Answer: D

Explanation:

This option is the best solution because it allows the company to run its payment application on AWS with minimal operational overhead and infrastructure management. By using Amazon API Gateway, the company can create a secure and scalable API to receive payment notifications from mobile devices. By using AWS Lambda, the company can run a serverless function to validate the payment notifications and send them to the backend application. Lambda handles the provisioning, scaling, and security of the function, reducing the operational complexity and cost. By using Amazon ECS with AWS Fargate, the company can run the backend application on a fully managed container service that scales the compute resources automatically and does not require any EC2 instances to manage. Fargate allocates the right amount of CPU and memory for each container and adjusts them as needed.

* A. Create an Amazon Simple Queue Service (Amazon SQS) queue Integrate the queue with an Amazon EventBndge rule to receive payment notifications from mobile devices Configure the rule to validate payment notifications and send the notifications to the backend application Deploy the backend application on Amazon Elastic Kubernetes Service (Amazon EKS) Anywhere Create a standalone cluster. This option

is not optimal because it requires the company to manage the Kubernetes cluster that runs the backend application. Amazon EKS Anywhere is a deployment option that allows the company to create and operate Kubernetes clusters on-premises or in other environments outside AWS. The company would need to provision, configure, scale, patch, and monitor the cluster nodes, which can increase the operational overhead and complexity. Moreover, the company would need to ensure the connectivity and security between the AWS services and the EKS Anywhere cluster, which can also add challenges and risks.

* B. Create an Amazon API Gateway API Integrate the API with anAWS Step Functions state ma-chine to receive payment notifications from mobile devices Invoke the state machine to validate payment notifications and send the notifications to the backend application Deploy the backend application on Amazon Elastic Kubernetes Sen/ice (Amazon EKS). Configure an EKS cluster with self-managed nodes. This option is not ideal because it requires the company to manage the EC2 instances that host the Kubernetes cluster that runs the backend application. Amazon EKS is a fully managed service that runs Kubernetes on AWS, but it still requires the company to manage the worker nodes that run the containers. The company would need to provision, configure, scale, patch, and monitor the EC2 instances, which can increase the operational overhead and infrastructure costs. Moreover, using AWS Step Functions to validate the payment notifications may be unnecessary and complex, as the validation logic can be implemented in a simpler way with Lambda or other services.

* C. Create an Amazon Simple Queue Sen/ice (Amazon SQS) queue Integrate the queue with an Amazon EventBridge rule to receive payment notifications from mobile devices Configure the rule to validate payment notifications and send the notifications to the backend application Deploy the backend application on Amazon EC2 Spot Instances Configure a Spot Fleet with a default al-location strategy. This option is not cost-effective because it requires the company to manage the EC2 instances that run the backend application. The company would need to provision, configure, scale, patch, and monitor the EC2 instances, which can increase the operational overhead and infrastructure costs. Moreover, using Spot Instances can introduce the risk of interruptions, as Spot Instances are reclaimed by AWS when the demand for On-Demand Instances increases. The company would need to handle the interruptions gracefully and ensure the availability and reliability of the backend application.

References:

- 1 Amazon API Gateway - Amazon Web Services
- 2 AWS Lambda - Amazon Web Services

- 3 Amazon Elastic Container Service - Amazon Web Services
- 4 AWS Fargate - Amazon Web Services

480. - (Topic 4)

A company is building a shopping application on AWS. The application offers a catalog that changes once each month and needs to scale with traffic volume. The company wants the lowest possible latency from the application. Data from each user's shopping carl needs to be highly available. User session data must be available even if the user is disconnected and reconnects.

What should a solutions architect do to ensure that the shopping cart data is preserved at all times?

A. Configure an Application Load Balancer to enable the sticky sessions feature (session affinity) for access to the catalog in Amazon Aurora.

B. Configure Amazon ElastiCacJie for Redis to cache catalog data from Amazon DynamoDB and shopping carl data from the user's session.

C. Configure Amazon OpenSearch Service to cache catalog data from Amazon DynamoDB and shopping cart data from the user's session.

D. Configure an Amazon EC2 instance with Amazon Elastic Block Store (Amazon EBS) storage for the catalog and shopping cart. Configure automated snapshots.

Answer: B

Explanation:

To ensure that the shopping cart data is preserved at all times, a solutions architect should configure Amazon ElastiCache for Redis to cache catalog data from Amazon DynamoDB and shopping cart data from the user’s session. This solution has the following benefits:

- It offers the lowest possible latency from the application, as ElastiCache for Redis is a blazing fast in-memory data store that provides sub-millisecond latency to power internet-scale real-time applications1.
- It scales with traffic volume, as ElastiCache for Redis supports horizontal scaling by adding more nodes or shards to the cluster, and vertical scaling by changing the node type2.
- It is highly available, as ElastiCache for Redis supports replication across multiple Availability Zones and automatic failover in case of a primary node failure3.
- It preserves user session data even if the user is disconnected and reconnects, as ElastiCache for

Redis can store session data, such as user login information and shopping cart contents, in a persistent and durable manner using snapshots or AOF (append-only file) persistence4.

References:

- 1: https://aws.amazon.com/elasticache/redis/
- 2: https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/Scaling.html
- 3: https://docs.aws.amazon.com/AmazonElastiCache/latest/red- ug/Replication.html
- 4: https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/backups.html

481. - (Topic 4)

A serverless application uses Amazon API Gateway. AWS Lambda, and Amazon DynamoDB. The Lambda function needs permissions to read and write to the DynamoDB table.

Which solution will give the Lambda function access to the DynamoDB table MOST securely?

A. Create an 1AM user with programmatic access to the Lambda function. Attach a policy to the user that allows read and write access to the DynamoDB table. Store the access_key_id and secret_access_key parameters as part of the Lambda environment variables. Ensure that other AWS users do not have read and write access to the Lambda function configuration

B. Create an 1AM role that includes Lambda as a trusted service. Attach a policy to the role that allows read and write access to the DynamoDB table. Update the configuration of the Lambda function to use the new role as the execution role.

C. Create an 1AM user with programmatic access to the Lambda function. Attach a policy to the user that allows read and write access to the DynamoDB table. Store the access_key_id and secret_access_key parameters in AWS Systems Manager Parameter Store as secure string parameters. Update the Lambda function code to retrieve the secure string parameters before connecting to the DynamoDB table.

D. Create an 1AM role that includes DynamoDB as a trusted service. Attach a policy to the role that allows read and write access from the Lambda function. Update the code of the Lambda function to attach to the new role as an execution role.

Answer: B

Explanation: Option B suggests creating an IAM role that includes Lambda as a trusted service, meaning the role is specifically designed for Lambda functions. The role should have a policy attached to it that grants the required read and write access to the DynamoDB table.

482. - (Topic 4)

A company has a serverless website with millions of objects in an Amazon S3 bucket. The company uses the S3 bucket as the origin for an Amazon CloudFront distribution. The company did not set encryption on the S3 bucket before the objects were loaded. A solutions architect needs to enable encryption for all existing objects and for all objects that are added to the S3 bucket in the future.

Which solution will meet these requirements with the LEAST amount of effort?

A. Create a new S3 bucket. Turn on the default encryption settings for the new S3 bucket. Download all existing objects to temporary local storage. Upload the objects to the new S3 bucket.

B. Turn on the default encryption settings for the S3 bucket. Use the S3 Inventory feature to create a .csv file that lists the unencrypted objects. Run an S3 Batch Operations job that uses the copy command to encrypt those objects.

C. Create a new encryption key by using AWS Key Management Service (AWS KMS). Change the settings on the S3 bucket to use server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Turn on versioning for the S3 bucket.

D. Navigate to Amazon S3 in the AWS Management Console. Browse the S3 bucket's objects. Sort by the encryption field. Select each unencrypted object. Use the Modify button to apply default encryption settings to every unencrypted object in the S3 bucket.

Answer: B

Explanation: https://spin.atomicobject.com/2020/09/15/aws-s3-encrypt-existing-objects/

483. - (Topic 4)

A company runs applications on AWS that connect to the company's Amazon RDS database. The applications scale on weekends and at peak times of the year. The company wants to scale the database more effectively for its applications that connect to the database.

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

A. Use Amazon DynamoDB with connection pooling with a target group configuration for the database. Change the applications to use the DynamoDB endpoint.

B. Use Amazon RDS Proxy with a target group for the database. Change the applications to use the RDS Proxy endpoint.

C. Use a custom proxy that runs on Amazon EC2 as an intermediary to the database. Change the applications to use the custom proxy endpoint.

D. Use an AWS Lambda function to provide connection pooling with a target group configuration for the database. Change the applications to use the Lambda function.

Answer: B

Explanation:

Amazon RDS Proxy is a fully managed, highly available database proxy for Amazon Relational Database Service (RDS) that makes applications more scalable, more resilient to database failures, and more secure1. RDS Proxy allows applications to pool and share connections established with the database, improving database efficiency and application scalability2. RDS Proxy also reduces failover times for Aurora and RDS databases by up to 66% and enables IAM authentication and Secrets Manager integration for database access1. RDS Proxy can be enabled for most applications with no code changes2.

484. - (Topic 4)

A company uses high concurrency AWS Lambda functions to process a constantly increasing number of messages in a message queue during marketing events. The Lambda functions use CPU intensive code to process the messages. The company wants to reduce the compute costs and to maintain service latency for its customers.

Which solution will meet these requirements?

A. Configure reserved concurrency for the Lambda functions. Decrease the memory allocated to the Lambda functions.

B. Configure reserved concurrency for the Lambda functions. Increase the memory according to AWS Compute Optimizer recommendations.

C. Configure provisioned concurrency for the Lambda functions. Decrease the memory allocated to the Lambda functions.

D. Configure provisioned concurrency for the Lambda functions. Increase the memory according to AWS Compute Optimizer recommendations.

Answer: D

Explanation: The company wants to reduce the compute costs and maintain service latency for its Lambda functions that process a constantly increasing number of messages in a message queue. The Lambda

functions use CPU intensive code to process the messages. To meet these requirements, a solutions architect should recommend the following solution:

- Configure provisioned concurrency for the Lambda functions. Provisioned concurrency is the number of pre-initialized execution environments that are allocated to the Lambda functions. These execution environments are prepared to respond immediately to incoming function requests, reducing the cold start latency. Configuring provisioned concurrency also helps to avoid throttling errors due to reaching the concurrency limit of the Lambda service.
- Increase the memory according to AWS Compute Optimizer recommendations.

AWS Compute Optimizer is a service that provides recommendations for optimal AWS resource configurations based on your utilization data. By increasing the memory allocated to the Lambda functions, you can also increase the CPU power and improve the performance of your CPU intensive code. AWS Compute Optimizer can help you find the optimal memory size for your Lambda functions based on your workload characteristics and performance goals.

This solution will reduce the compute costs by avoiding unnecessary over-provisioning of memory and CPU resources, and maintain service latency by using provisioned concurrency and optimal memory size for the Lambda functions.

References:

- Provisioned Concurrency
- AWS Compute Optimizer

485. - (Topic 4)

A company has a nightly batch processing routine that analyzes report files that an on- premises file system receives daily through SFTP. The company wants to move the solution to the AWS Cloud. The solution must be highly available and resilient. The solution also must minimize operational effort.

Which solution meets these requirements?

A. Deploy AWS Transfer for SFTP and an Amazon Elastic File System (Amazon EFS) file system for storage. Use an Amazon EC2 instance in an Auto Scaling group with a scheduled scaling policy to run the batch operation.

B. Deploy an Amazon EC2 instance that runs Linux and an SFTP service. Use an Amazon Elastic Block Store {Amazon EBS) volume for storage. Use an Auto Scaling group with the minimum number of

instances and desired number of instances set to 1.

C. Deploy an Amazon EC2 instance that runs Linux and an SFTP service. Use an Amazon Elastic File System (Amazon EFS) file system for storage. Use an Auto Scaling group with the minimum number of instances and desired number of instances set to 1.

D. Deploy AWS Transfer for SFTP and an Amazon S3 bucket for storage. Modify the application to pull the batch files from Amazon S3 to an Amazon EC2 instance for processing. Use an EC2 instance in an Auto Scaling group with a scheduled scaling policy to run the batch operation.

Answer: D

Explanation: The solution that meets the requirements of high availability, performance, security, and static IP addresses is to use Amazon CloudFront, Application Load Balancers (ALBs), Amazon Route 53, and AWS WAF. This solution allows the company to distribute its HTTP-based application globally using CloudFront, which is a content delivery network (CDN) service that caches content at edge locations and provides static IP addresses for each edge location. The company can also use Route 53 latency-based routing to route requests to the closest ALB in each Region, which balances the load across the EC2 instances. The company can also deploy AWS WAF on the CloudFront distribution to protect the application against common web exploits by creating rules that allow, block, or count web requests based on conditions that are defined. The other solutions do not meet all the requirements because they either use Network Load Balancers (NLBs), which do not support HTTP-based applications, or they do not use CloudFront, which provides better performance and security than AWS Global Accelerator. References :=

- Amazon CloudFront
- Application Load Balancer
- Amazon Route 53
- AWS WAF

486. - (Topic 4)

A company runs container applications by using Amazon Elastic Kubernetes Service (Amazon EKS). The company's workload is not consistent throughout the day The company wants Amazon EKS to scale in and out according to the workload.

Which combination of steps will meet these requirements with the LEAST operational overhead? {Select TWO.)

A. Use an AWS Lambda function to resize the EKS cluster

B. Use the Kubernetes Metrics Server to activate horizontal pod autoscaling.

C. Use the Kubernetes Cluster Autoscaler to manage the number of nodes in the cluster.

D. Use Amazon API Gateway and connect it to Amazon EKS

E. Use AWS App Mesh to observe network activity.

Answer: B,C

Explanation: https://docs.aws.amazon.com/eks/latest/userguide/horizontal-pod- autoscaler.html

https://docs.aws.amazon.com/eks/latest/userguide/autoscaling.html

Horizontal pod autoscaling is a feature of Kubernetes that automatically scales the number of pods in a deployment, replication controller, or replica set based on that resource's CPU utilization. It requires a metrics source such as the Kubernetes Metrics Server to provide CPU usage data1. Cluster autoscaling is a feature of Kubernetes that automatically adjusts the number of nodes in a cluster when pods fail or are rescheduled onto other nodes. It requires an integration with AWS Auto Scaling groups to manage the EC2 instances that join the cluster2. By using both horizontal pod autoscaling and cluster autoscaling, the solution can ensure that Amazon EKS scales in and out according to the workload.

487. - (Topic 4)

A social media company runs its application on Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is the origin for an Amazon CloudFront distribution. The application has more than a billion images stored in an Amazon S3 bucket and processes thousands of images each second. The company wants to resize the images dynamically and serve appropriate formats to clients.

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

A. Install an external image management library on an EC2 instance. Use the image management library to process the images.

B. Create a CloudFront origin request policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.

C. Use a Lambda@Edge function with an external image management library. Associate the Lambda@Edge function with the CloudFront behaviors that serve the images.

D. Create a CloudFront response headers policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.

Answer: C

Explanation:

To resize images dynamically and serve appropriate formats to clients, a Lambda@Edge function with an external image management library can be used. Lambda@Edge allows running custom code at the edge locations of CloudFront, which can process the images on the fly and optimize them for different devices and browsers. An external image management library can provide various image manipulation and optimization features. References:

- Lambda@Edge
- Resizing Images with Amazon CloudFront & Lambda@Edge

488. - (Topic 4)

A company manages AWS accounts in AWS Organizations. AWS 1AM Identity Center (AWS Single Sign-On) and AWS Control Tower are configured for the accounts. The company wants to manage multiple user permissions across all the accounts.

The permissions will be used by multiple 1AM users and must be split between the developer and administrator teams. Each team requires different permissions. The company wants a solution that includes new users that are hired on both teams.

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

A. Create individual users in 1AM Identity Center (or each account. Create separate developer and administrator groups in 1AM Identity Center. Assign the users to the appropriate groups Create a custom 1AM policy for each group to set fine-grained permissions.

B. Create individual users in 1AM Identity Center for each account. Create separate developer and administrator groups in 1AM Identity Center. Assign the users to the appropriate groups. Attach AWS managed 1AM policies to each user as needed for fine- grained permissions.

C. Create individual users in 1AM Identity Center Create new developer and administrator groups in 1AM Identity Center. Create new permission sets that include the appropriate 1AM policies for each group. Assign the new groups to the appropriate accounts Assign the new permission sets to the new groups When new users are hired, add them to the appropriate group.

D. Create individual users in 1AM Identity Center. Create new permission sets that include the appropriate 1AM policies for each user. Assign the users to the appropriate accounts. Grant additional 1AM

permissions to the users from within specific accounts. When new users are hired, add them to 1AM Identity Center and assign them to the accounts.

Answer: C

Explanation: This solution meets the requirements with the least operational overhead because it leverages the features of IAM Identity Center and AWS Control Tower to centrally manage multiple user permissions across all the accounts. By creating new groups and permission sets, the company can assign fine-grained permissions to the developer and administrator teams based on their roles and responsibilities. The permission sets are applied to the groups at the organization level, so they are automatically inherited by all the accounts in the organization. When new users are hired, the company only needs to add them to the appropriate group in IAM Identity Center, and they will automatically get the permissions assigned to that group. This simplifies the user management and reduces the manual effort of assigning permissions to each user individually.

References:

- Managing access to AWS accounts and applications
- Managing permissions sets
- Managing groups

489. - (Topic 4)

A company needs a solution to prevent photos with unwanted content from being uploaded to the company's web application. The solution must not involve training a machine learning (ML) model. Which solution will meet these requirements?

A. Create and deploy a model by using Amazon SageMaker Autopilot. Create a real-time endpoint that the web application invokes when new photos are uploaded.

B. Create an AWS Lambda function that uses Amazon Rekognition to detect unwanted content. Create a Lambda function URL that the web application invokes when new photos are uploaded.

C. Create an Amazon CloudFront function that uses Amazon Comprehend to detect unwanted content. Associate the function with the web application.

D. Create an AWS Lambda function that uses Amazon Rekognition Video to detect unwanted content. Create a Lambda function URL that the web application invokes when new photos are uploaded.

Answer: B

Explanation:

The solution that will meet the requirements is to create an AWS Lambda function that uses Amazon Rekognition to detect unwanted content, and create a Lambda function URL that the web application invokes when new photos are uploaded. This solution does not involve training a machine learning model, as Amazon Rekognition is a fully managed service that provides pre-trained computer vision models for image and video analysis. Amazon Rekognition can detect unwanted content such as explicit or suggestive adult content, violence, weapons, drugs, and more. By using AWS Lambda, the company can create a serverless function that can be triggered by an HTTP request from the web application. The Lambda function can use the Amazon Rekognition API to analyze the uploaded photos and return a response indicating whether they contain unwanted content or not.

The other solutions are not as effective as the first one because they either involve training a machine learning model, do not support image analysis, or do not work with photos. Creating and deploying a model by using Amazon SageMaker Autopilot involves training a machine learning model, which is not required for the scenario. Amazon SageMaker Autopilot is a service that automatically creates, trains, and tunes the best machine learning models for classification or regression based on the data provided by the user. Creating an Amazon CloudFront function that uses Amazon Comprehend to detect unwanted content does not support image analysis, as Amazon Comprehend is a natural language processing service that analyzes text, not images. Amazon Comprehend can extract insights and relationships from text such as language, sentiment, entities, topics, and more. Creating an AWS Lambda function that uses Amazon Rekognition Video to detect unwanted content does not work with photos, as Amazon Rekognition Video is designed for analyzing video streams, not static images. Amazon Rekognition Video can detect activities, objects, faces, celebrities, text, and more in video streams.

References:

- Amazon Rekognition
- AWS Lambda
- Detecting unsafe content - Amazon Rekognition
- Amazon SageMaker Autopilot
- Amazon Comprehend

490. - (Topic 4)

A company needs to provide customers with secure access to its data. The company processes customer data and stores the results in an Amazon S3 bucket.

All the data is subject to strong regulations and security requirements. The data must be encrypted at rest. Each customer must be able to access only their data from their AWS account. Company employees must not be able to access the data.

Which solution will meet these requirements?

A. Provision an AWS Certificate Manager (ACM) certificate for each customer. Encrypt the data client-side. In the private certificate policy, deny access to the certificate for all principals except an 1AM role that the customer provides.

B. Provision a separate AWS Key Management Service (AWS KMS) key for each customer. Encrypt the data server-side. In the S3 bucket policy, deny decryption of data for all principals except an 1AM role that the customer provides.

C. Provision a separate AWS Key Management Service (AWS KMS) key for each customer. Encrypt the data server-side. In each KMS key policy, deny decryption of data for all principals except an 1AM role that the customer provides.

D. Provision an AWS Certificate Manager (ACM) certificate for each customer. Encrypt the data client-side. In the public certificate policy, deny access to the certificate for all principals except an 1AM role that the customer provides.

Answer: C

Explanation: The correct solution is to provision a separate AWS KMS key for each customer and encrypt the data server-side. This way, the company can use the S3 encryption feature to protect the data at rest and delegate the control of the encryption keys to the customers. The customers can then use their own IAM roles to access and decrypt their data. The company employees will not be able to access the data because they are not authorized by the KMS key policies. The other options are incorrect because:

- Option A and D are using ACM certificates to encrypt the data client-side. This is not a recommended practice for S3 encryption because it adds complexity and overhead to the encryption process. Moreover, the company will have to manage the certificates and their policies for each customer, which is not scalable and secure.
- Option B is using a separate KMS key for each customer, but it is using the S3

bucket policy to control the decryption access. This is not a secure solution because the bucket policy applies to the entire bucket, not to individual objects. Therefore, the customers will be able to access and decrypt each other's data if they have the permission to list the bucket contents. The bucket policy also overrides the KMS key policy, which means the company employees can access the data if they have the permission to use the KMS key.

References:

- S3 encryption
- KMS key policies
- ACM certificates

491. - (Topic 4)

A company is storing 700 terabytes of data on a large network-attached storage (NAS) system in fts corporate data center. The company has a hybrid environment with a 10 Gbps AWS Direct Connect connection.

After an audit from a regulator, the company has 90 days to move the data to the cloud. The company needs to move the data efficiently and without disruption. The company still needs to be able to access and update the data during the transfer window.

Which solution will meet these requirements?

A. Create an AWS DataSync agent in the corporate data center. Create a data transfer task. Start the transfer to an Amazon S3 bucket.

B. Back up the data to AWS Snowball Edge Storage Optimized devices. Ship the devices to an AWS data center. Mount a target Amazon S3 bucket on the on-premises file system.

C. Use rsync to copy the data directly from local storage to a designated Amazon S3 bucket over the Direct Connect connection.

D. Back up the data on tapes. Ship the tapes to an AWS data center. Mount a target Amazon S3 bucket on the on-premises file system.

Answer: A

Explanation: This answer is correct because it meets the requirements of moving the data efficiently and without disruption, and still being able to access and update the data during the transfer window. AWS DataSync is an online data movement and discovery service that simplifies and accelerates data migrations

to AWS and helps you move data quickly and securely between on-premises storage, edge locations, other clouds, and AWS Storage. You can create an AWS DataSync agent in the corporate data center to connect your NAS system to AWS over the Direct Connect connection. You can create a data transfer task to specify the source location, destination location, and options for transferring the data. You can start the transfer to an Amazon S3 bucket and monitor the progress of the task. DataSync automatically encrypts data in transit and verifies data integrity during transfer. DataSync also supports incremental transfers, which means that only files that have changed since the last transfer are copied. This way, you can ensure that your data is synchronized between your NAS system and S3 bucket, and you can access and update the data during the transfer window.

References:

- https://docs.aws.amazon.com/datasync/latest/userguide/what-is-datasync.html
- https://docs.aws.amazon.com/datasync/latest/userguide/how-datasync-works.html

492. - (Topic 4)

An ecommerce company runs applications in AWS accounts that are part of an organization in AWS Organizations The applications run on Amazon Aurora PostgreSQL databases across all the accounts The company needs to prevent malicious activity and must identify abnormal failed and incomplete login attempts to the databases

Which solution will meet these requirements in the MOST operationally efficient way?

A. Attach service control policies (SCPs) to the root of the organization to identify the failed login attempts

B. Enable the Amazon RDS Protection feature in Amazon GuardDuty for the member accounts of the organization

C. Publish the Aurora general logs to a log group in Amazon CloudWatch Logs Export the log data to a central Amazon S3 bucket

D. Publish all the Aurora PostgreSQL database events in AWS CloudTrail to a central Amazon S3 bucket

Answer: C

Explanation: This option is the most operationally efficient way to meet the requirements because it allows the company to monitor and analyze the database login activity across all the accounts in the organization. By publishing the Aurora general logs to a log group in Amazon CloudWatch Logs, the company can enable the logging of the database connections, disconnections, and failed authentication attempts. By exporting

the log data to a central Amazon S3 bucket, the company can store the log data in a durable and cost-effective way and use other AWS services or tools to perform further analysis or alerting on the log data. For example, the company can use Amazon Athena to query the log data in Amazon S3, or use Amazon SNS to send notifications based on the log data.

* A. Attach service control policies (SCPs) to the root of the organization to identify the failed login attempts. This option is not effective because SCPs are not designed to identify the failed login attempts, but to restrict the actions that the users and roles can perform in the member accounts of the organization. SCPs are applied to the AWS API calls, not to the database login attempts. Moreover, SCPs do not provide any logging or analysis capabilities for the database activity.

* B. Enable the Amazon RDS Protection feature in Amazon GuardDuty for the member accounts of the organization. This option is not optimal because the Amazon RDS Protection feature in Amazon GuardDuty is not available for Aurora PostgreSQL databases, but only for Amazon RDS for MySQL and Amazon RDS for MariaDB databases. Moreover, the Amazon RDS Protection feature does not monitor the database login attempts, but the network and API activity related to the RDS instances.

* D. Publish all the Aurora PostgreSQL database events in AWS CloudTrail to a central Amazon S3 bucket. This option is not sufficient because AWS CloudTrail does not capture the database login attempts, but only the AWS API calls made by or on behalf of the Aurora PostgreSQL database. For example, AWS CloudTrail can record the events such as creating, modifying, or deleting the database instances, clusters, or snapshots, but not the events such as connecting, disconnecting, or failing to authenticate to the database. References:

- 1 Working with Amazon Aurora PostgreSQL - Amazon Aurora
- 2 Working with log groups and log streams - Amazon CloudWatch Logs
- 3 Exporting Log Data to Amazon S3 - Amazon CloudWatch Logs
- [4] Amazon GuardDuty FAQs
- [5] Logging Amazon RDS API Calls with AWS CloudTrail - Amazon Relational Database Service

493. - (Topic 4)

A company runs a Java-based job on an Amazon EC2 instance. The job runs every hour and takes 10 seconds to run. The job runs on a scheduled interval and consumes 1 GB of memory. The CPU utilization of the instance is low except for short surges during which the job uses the maximum CPU available. The

company wants to optimize the costs to run the job.

Which solution will meet these requirements?

A. Use AWS App2Container (A2C) to containerize the job. Run the job as an Amazon Elastic Container Service (Amazon ECS) task on AWS Fargate with 0.5 virtual CPU (vCPU) and 1 GB of memory.

B. Copy the code into an AWS Lambda function that has 1 GB of memory. Create an Amazon EventBridge scheduled rule to run the code each hour.

C. Use AWS App2Container (A2C) to containerize the job. Install the container in the existing Amazon Machine Image (AMI). Ensure that the schedule stops the container when the task finishes.

D. Configure the existing schedule to stop the EC2 instance at the completion of the job and restart the EC2 instance when the next job starts.

Answer: B

Explanation: AWS Lambda is a serverless compute service that allows you to run code without provisioning or managing servers. You can create Lambda functions using various languages, including Java, and specify the amount of memory and CPU allocated to your function. Lambda charges you only for the compute time you consume, which is calculated based on the number of requests and the duration of your code execution. You can use Amazon EventBridge to trigger your Lambda function on a schedule, such as every hour, using cron or rate expressions. This solution will optimize the costs to run the job, as you will not pay for any idle time or unused resources, unlike running the job on an EC2 instance. References: 1: AWS Lambda - FAQs2, General Information section2: Tutorial: Schedule AWS Lambda functions using EventBridge3, Introduction section3: Schedule expressions using rate or cron - AWS Lambda4, Introduction section.

494. - (Topic 4)

A company has applications hosted on Amazon EC2 instances with IPv6 addresses. The applications must initiate communications with other external applications using the internet.

However, the company's security policy states that any external service cannot initiate a connection to the EC2 instances.

What should a solutions architect recommend to resolve this issue?

A. Create a NAT gateway and make it the destination of the subnet's route table.

B. Create an internet gateway and make it the destination of the subnet's route table

C. Create a virtual private gateway and make it the destination of the subnet's route table.

D. Create an egress-only internet gateway and make it the destination of the subnet's route table.

Answer: D

Explanation: An egress-only internet gateway is a VPC component that allows outbound communication over IPv6 from instances in your VPC to the internet, and prevents the internet from initiating an IPv6 connection with your instances. This meets the company's security policy and requirements. To use an egress-only internet gateway, you need to add a route in the subnet's route table that routes IPv6 internet traffic (::/0) to the egress-only internet gateway.

Reference URLs:

1 https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html

2 https://dev.to/aws-builders/what-is-an-egress-only-internet-gateways-in-aws-7gp

3 https://docs.aws.amazon.com/vpc/latest/userguide/route-table-options.html

495. - (Topic 4)

A company is running its production and nonproduction environment workloads in multiple AWS accounts. The accounts are in an organization in AWS Organizations. The company needs to design a solution that will prevent the modification of cost usage tags.

Which solution will meet these requirements?

A. Create a custom AWS Config rule to prevent tag modification except by authorized principals.

B. Create a custom trail in AWS CloudTrail to prevent tag modification

C. Create a service control policy (SCP) to prevent tag modification except by authonzed principals.

D. Create custom Amazon CloudWatch logs to prevent tag modification.

Answer: C

Explanation: This solution meets the requirements because it uses SCPs to restrict the actions that can be performed on cost usage tags in the organization. SCPs are a type of organization policy that you can use to manage permissions in your organization. SCPs specify the maximum permissions for an organization, organizational unit (OU), or account. You can use SCPs to enforce consistent tag policies across your organization and prevent unauthorized or accidental changes to your tags. You can also create exceptions for authorized principals, such as administrators or auditors, who need to modify tags for legitimate purposes.

References:

- Service control policies (SCPs) - AWS Organizations
- Tag policies - AWS Organizations

496. - (Topic 4)

A company has hired a solutions architect to design a reliable architecture for its application. The application consists of one Amazon RDS DB instance and two manually provisioned Amazon EC2 instances that run web servers. The EC2 instances are located in a single Availability Zone.

An employee recently deleted the DB instance, and the application was unavailable for 24 hours as a result. The company is concerned with the overall reliability of its environment.

What should the solutions architect do to maximize reliability of the application's infrastructure?

A. Delete one EC2 instance and enable termination protection on the other EC2 instance. Update the DB instance to be Multi-AZ, and enable deletion protection.

B. Update the DB instance to be Multi-AZ, and enable deletion protection. Place the EC2 instances behind an Application Load Balancer, and run them in an EC2 Auto Scaling group across multiple Availability Zones.

C. Create an additional DB instance along with an Amazon API Gateway and an AWS Lambda function. Configure the application to invoke the Lambda function through API Gateway. Have the Lambda function write the data to the two DB instances.

D. Place the EC2 instances in an EC2 Auto Scaling group that has multiple subnets located in multiple Availability Zones. Use Spot Instances instead of On-Demand Instances. Set up Amazon CloudWatch alarms to monitor the health of the instances. Update the DB instance to be Multi-AZ, and enable deletion protection.

Answer: B

Explanation: This answer is correct because it meets the requirements of maximizing the reliability of the application’s infrastructure. You can update the DB instance to be Multi-AZ, which means that Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance. It can also help protect your

databases against DB instance failure and Availability Zone disruption. You can also enable deletion protection on the DB instance, which prevents the DB instance from being deleted by any user. You can place the EC2 instances behind an Application Load Balancer, which distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. This increases the availability and fault tolerance of your applications. You can run the EC2 instances in an EC2 Auto Scaling group across multiple Availability Zones, which ensures that you have the correct number of EC2 instances available to handle the load for your application. You can use scaling policies to adjust the number of instances in your Auto Scaling group in response to changing demand.

References:

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZSin gleStandby.html
- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_DeleteInstan ce.html#USER_DeleteInstance.DeletionProtection
- https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.h tml
- https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html

497. - (Topic 4)

A company runs a real-time data ingestion solution on AWS. The solution consists of the most recent version of Amazon Managed Streaming for Apache Kafka (Amazon MSK). The solution is deployed in a VPC in private subnets across three Availability Zones.

A solutions architect needs to redesign the data ingestion solution to be publicly available over the internet. The data in transit must also be encrypted.

Which solution will meet these requirements with the MOST operational efficiency?

A. Configure public subnets in the existing VPC. Deploy an MSK cluster in the public subnets. Update the MSK cluster security settings to enable mutual TLS authentication.

B. Create a new VPC that has public subnets. Deploy an MSK cluster in the public subnets. Update the MSK cluster security settings to enable mutual TLS authentication.

C. Deploy an Application Load Balancer (ALB) that uses private subnets. Configure an ALB security group inbound rule to allow inbound traffic from the VPC CIDR block for HTTPS protocol.

D. Deploy a Network Load Balancer (NLB) that uses private subnets. Configure an NLB listener for HTTPS communication over the internet.

Answer: A

Explanation: The solution that meets the requirements with the most operational efficiency is to configure public subnets in the existing VPC and deploy an MSK cluster in the public subnets. This solution allows the data ingestion solution to be publicly available over the internet without creating a new VPC or deploying a load balancer. The solution also ensures that the data in transit is encrypted by enabling mutual TLS authentication, which requires both the client and the server to present certificates for verification. This solution leverages the public access feature of Amazon MSK, which is available for clusters running Apache Kafka 2.6.0 or later versions1.

The other solutions are not as efficient as the first one because they either create unnecessary resources or do not encrypt the data in transit. Creating a new VPC with public subnets would incur additional costs and complexity for managing network resources and routing. Deploying an ALB or an NLB would also add more costs and latency for the data ingestion solution. Moreover, an ALB or an NLB would not encrypt the data in transit by itself, unless they are configured with HTTPS listeners and certificates, which would require additional steps and maintenance. Therefore, these solutions are not optimal for the given requirements.

References:

- Public access - Amazon Managed Streaming for Apache Kafka

498. - (Topic 4)

A company wants to rearchitect a large-scale web application to a serverless microservices architecture. The application uses Amazon EC2 instances and is written in Python.

The company selected one component of the web application to test as a microservice. The component supports hundreds of requests each second. The company wants to create and test the microservice on an AWS solution that supports Python. The solution must also scale automatically and require minimal infrastructure and minimal operational support.

Which solution will meet these requirements?

A. Use a Spot Fleet with auto scaling of EC2 instances that run the most recent Amazon Linux operating system.

B. Use an AWS Elastic Beanstalk web server environment that has high availability configured.

C. Use Amazon Elastic Kubernetes Service (Amazon EKS). Launch Auto Scaling groups of self-managed EC2 instances.

D. Use an AWS Lambda function that runs custom developed code.

Answer: D

Explanation: AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers. You can use Lambda to create and test microservices that are written in Python or other supported languages. Lambda scales automatically to handle the number of requests per second. You only pay for the compute time you consume. Lambda also integrates with other AWS services, such as Amazon API Gateway, Amazon S3, Amazon DynamoDB, and Amazon SQS, to enable event-driven architectures. Lambda has minimal infrastructure and operational overhead, as you do not need to manage servers, operating systems, patches, or scaling policies.

The other options are not serverless solutions and require more infrastructure and operational support. They also do not scale automatically to handle the number of requests per second. A Spot Fleet is a collection of EC2 instances that run on spare capacity at low prices. However, Spot Instances can be interrupted by AWS at any time, which can affect the availability and performance of your microservice. AWS Elastic Beanstalk is a service that automates the deployment and management of web applications on EC2 instances. However, you still need to provision, configure, and monitor the underlying EC2 instances and load balancers. Amazon EKS is a service that runs Kubernetes on AWS. However, you still need to create, configure, and manage the EC2 instances that form the Kubernetes cluster and nodes. You also need to install and update the Kubernetes software and tools. References:

- What is AWS Lambda?
- Building Lambda functions with Python
- Create a layer for a Lambda Python function
- AWS Lambda – Function in Python
- How do I call my AWS Lambda function from a local python script?

499. - (Topic 4)

A solutions architect must provide an automated solution for a company's compliance policy that states security groups cannot include a rule that allows SSH from 0.0.0.0/0. The company needs to be notified if there is any breach in the policy. A solution is needed as soon as possible.

What should the solutions architect do to meet these requirements with the LEAST operational overhead?

A. Write an AWS Lambda script that monitors security groups for SSH being open to 0.0.0.0/0 addresses

and creates a notification every time it finds one.

B. Enable the restricted-ssh AWS Config managed rule and generate an Amazon Simple Notification Service (Amazon SNS) notification when a noncompliant rule is created.

C. Create an 1AM role with permissions to globally open security groups and network ACLs. Create an Amazon Simple Notification Service (Amazon SNS) topic to generate a notification every time the role is assumed by a user.

D. Configure a service control policy (SCP) that prevents non-administrative users from creating or editing security groups. Create a notification in the ticketing system when a user requests a rule that needs administrator permissions.

Answer: B

Explanation: The most suitable solution for the company's compliance policy is to enable the restricted-ssh AWS Config managed rule and generate an Amazon Simple Notification Service (Amazon SNS) notification when a noncompliant rule is created. This solution has the least operational overhead because it uses a predefined rule that is already available in AWS Config, which is a service that enables users to assess, audit, and evaluate the configurations of their AWS resources. The restricted-ssh rule checks whether security groups that are in use have inbound rules that allow SSH from 0.0.0.0/0 addresses, and reports them as noncompliant1. Users can configure the rule to send notifications to an Amazon SNS topic when a noncompliant change occurs, and subscribe to the topic to receive alerts via email, SMS, or other methods2.

The other options are not correct because they either have more operational overhead or do not meet the requirements. Writing an AWS Lambda script that monitors security groups for SSH being open to 0.0.0.0/0 addresses and creates a notification every time it finds one is not correct because it requires custom code development and maintenance, which adds complexity and cost to the solution. Creating an IAM role with permissions to globally open security groups and network ACLs, and creating an Amazon SNS topic to generate a notification every time the role is assumed by a user is not correct because it does not prevent or detect the creation of noncompliant rules by other users or roles, and it does not address the existing rules that may violate the policy. Configuring a service control policy (SCP) that prevents non-administrative users from creating or editing security groups, and creating a notification in the ticketing system when a user requests a rule that needs administrator permissions is not correct because it does not provide an automated solution for the policy enforcement and notification, and it may limit the flexibility and

productivity of the users.

References:

- restricted-ssh - AWS Config
- Getting Notifications When Your Resources Change - AWS Config

500. - (Topic 4)

A manufacturing company has machine sensors that upload .csv files to an Amazon S3 bucket. These .csv files must be converted into images and must be made available as soon as possible for the automatic generation of graphical reports.

The images become irrelevant after 1 month, but the .csv files must be kept to train machine learning (ML) models twice a year. The ML trainings and audits are planned weeks in advance.

Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO.)

A. Launch an Amazon EC2 Spot Instance that downloads the .csv files every hour, generates the image files, and uploads the images to the S3 bucket.

B. Design an AWS Lambda function that converts the .csv files into images and stores the images in the S3 bucket. Invoke the Lambda function when a .csv file is uploaded.

C. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 Glacier 1 day after they are uploaded. Expire the image files after 30 days.

D. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) 1 day after they are uploaded. Expire the image files after 30 days.

E. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 1 day after they are uploaded. Keep the image files in Reduced Redundancy Storage (RRS).

Answer: B,C

Explanation: These answers are correct because they meet the requirements of converting the .csv files into images, making them available as soon as possible, and minimizing the storage costs. AWS Lambda is a service that lets you run code without provisioning or managing servers. You can use AWS Lambda to design a function that converts the .csv files into images and stores the

images in the S3 bucket. You can invoke the Lambda function when a .csv file is uploaded to the S3 bucket by using an S3 event notification. This way, you can ensure that the images are generated and made available as soon as possible for the graphical reports. S3 Lifecycle is a feature that enables you to manage your objects so that they are stored cost effectively throughout their lifecycle. You can create S3 Lifecycle rules for .csv files and image files in the S3 bucket to transition them to different storage classes or expire them based on your business needs. You can transition the .csv files from S3 Standard to S3 Glacier 1 day after they are uploaded, since they are only needed twice a year for ML trainings and audits that are planned weeks in advance. S3 Glacier is a storage class for data archiving that offers secure, durable, and extremely low-cost storage with retrieval times ranging from minutes to hours. You can expire the image files after 30 days, since they become irrelevant after 1 month. References:

- https://docs.aws.amazon.com/lambda/latest/dg/welcome.html
- https://docs.aws.amazon.com/AmazonS3/latest/userguide/NotificationHowTo.html
- https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle- mgmt.html
- https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class- intro.html#sc-glacier

501. - (Topic 4)

A company has two VPCs that are located in the us-west-2 Region within the same AWS account. The company needs to allow network traffic between these VPCs. Approximately 500 GB of data transfer will occur between the VPCs each month.

What is the MOST cost-effective solution to connect these VPCs?

A. Implement AWS Transit Gateway to connect the VPCs. Update the route tables of each VPC to use the transit gateway for inter-VPC communication.

B. Implement an AWS Site-to-Site VPN tunnel between the VPCs. Update the route tables of each VPC to use the VPN tunnel for inter-VPC communication.

C. Set up a VPC peering connection between the VPCs. Update the route tables of each VPC to use the VPC peering connection for inter-VPC communication.

D. Set up a 1 GB AWS Direct Connect connection between the VPCs. Update the route tables of each VPC to use the Direct Connect connection for inter-VPC communication.

Answer: C

Explanation: To connect two VPCs in the same Region within the same AWS account, VPC peering is the

most cost-effective solution. VPC peering allows direct network traffic between the VPCs without requiring a gateway, VPN connection, or AWS Transit Gateway. VPC peering also does not incur any additional charges for data transfer between the VPCs.

References:

- What Is VPC Peering?
- VPC Peering Pricing

502. - (Topic 4)

A company has a popular gaming platform running on AWS. The application is sensitive to latency because latency can impact the user experience and introduce unfair advantages to some players. The application is deployed in every AWS Region. It runs on Amazon EC2 instances that are part of Auto Scaling groups configured behind Application Load Balancers (ALBs). A solutions architect needs to implement a mechanism to monitor the health of the application and redirect traffic to healthy endpoints.

Which solution meets these requirements?

A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on, and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.

B. Create an Amazon CloudFront distribution and specify the ALB as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.

C. Create an Amazon CloudFront distribution and specify Amazon S3 as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.

D. Configure an Amazon DynamoDB database to serve as the data store for the application. Create a DynamoDB Accelerator (DAX) cluster to act as the in-memory cache for DynamoDB hosting the application data.

Answer: A

Explanation:

AWS Global Accelerator directs traffic to the optimal healthy endpoint based on health checks, it can also route traffic to the closest healthy endpoint based on geographic location of the client. By configuring an accelerator and attaching it to a Regional endpoint

in each Region, and adding the ALB as the endpoint, the solution will redirect traffic to healthy endpoints, improving the user experience by reducing latency and ensuring that the application is running optimally.

This solution will ensure that traffic is directed to the closest healthy endpoint and will help to improve the overall user experience.

503. - (Topic 4)

A company is deploying an application in three AWS Regions using an Application Load Balancer Amazon Route 53 will be used to distribute traffic between these Regions. Which Route 53 configuration should a solutions architect use to provide the MOST high- performing experience?

A. Create an A record with a latency policy.

B. Create an A record with a geolocation policy.

C. Create a CNAME record with a failover policy.

D. Create a CNAME record with a geoproximity policy.

Answer: A

Explanation:

To provide the most high-performing experience for the users of the application, a solutions architect should use a latency routing policy for the Route 53 A record. This policy allows Route 53 to route traffic to the AWS Region that provides the lowest possible latency for the users1. A latency routing policy can also improve the availability of the application, as Route 53 can automatically route traffic to another Region if the primary Region becomes unavailable2.

References:

- 1: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-latency
- 2: https://aws.amazon.com/route53/faqs/#Latency_Based_Routing

504. - (Topic 4)

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

What should a solutions architect do to meet these requirements?

A. Create an Amazon S3 bucket. Allow access from all the EC2 instances in the VPC.

B. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system from each

EC2 instance.

C. Create a file system on a Provisioned IOPS SSD (102) Amazon Elastic Block Store (Amazon EBS) volume. Attach the EBS volume to all the EC2 instances.

D. Create file systems on Amazon Elastic Block Store (Amazon EBS) volumes that are attached to each EC2 instance. Synchromze the EBS volumes across the different EC2 instances.

Answer: B

Explanation: it allows the EC2 instances to read and write rapidly and concurrently to shared storage across two Availability Zones. Amazon EFS provides a scalable, elastic, and highly available file system that can be mounted from multiple EC2 instances. Amazon EFS supports high levels of throughput and IOPS, and consistent low latencies. Amazon EFS also supports NFSv4 lock upgrading and downgrading, which enables high levels of concurrency. References:

- Amazon EFS Features
- Using Amazon EFS with Amazon EC2

505. - (Topic 4)

A company hosts a website on Amazon EC2 instances behind an Application Load Balancer (ALB) The website serves static content Website traffic is increasing and the company is concerned about a potential increase in cost.

What should a solutions architect do to reduce the cost of the website?

A. Create an Amazon CloudFront distribution to cache static files at edge locations.

B. Create an Amazon ElastiCache cluster Connect the ALB to the ElastiCache cluster to serve cached files.

C. Create an AWS WAF web ACL and associate it with the ALB. Add a rule to the web ACL to cache static files.

D. Create a second ALB in an alternative AWS Region Route user traffic to the closest Region to minimize data transfer costs

Answer: A

Explanation: Amazon CloudFront is a content delivery network (CDN) that can improve the performance and reduce the cost of serving static content from a website. CloudFront

can cache static files at edge locations closer to the users, reducing the latency and data transfer costs. CloudFront can also integrate with Amazon S3 as the origin for the static content, eliminating the need for

EC2 instances to host the website. CloudFront meets all the requirements of the question, while the other options do not. References:

➪ https://aws.amazon.com/blogs/architecture/architecting-a-low-cost-web-content-publishing-system/

➪ https://nodeployfriday.com/posts/static-website-hosting/

➪ https://aws.amazon.com/cloudfront/

506. - (Topic 4)

A company uses AWS Organizations. The company wants to operate some of its AWS accounts with different budgets. The company wants to receive alerts and automatically prevent provisioning of additional resources on AWS accounts when the allocated budget threshold is met during a specific period.

Which combination of solutions will meet these requirements? (Select THREE.)

A. Use AWS Budgets to create a budget. Set the budget amount under the Cost and Usage Reports section of the required AWS accounts.

B. Use AWS Budgets to create a budget. Set the budget amount under the Billing dashboards of the required AWS accounts.

C. Create an 1AM user for AWS Budgets to run budget actions with the required permissions.

D. Create an 1AM role for AWS Budgets to run budget actions with the required permissions.

E. Add an alert to notify the company when each account meets its budget threshold. Add a budget action that selects the 1AM identity created with the appropriate config rule to prevent provisioning of additional resources.

F. Add an alert to notify the company when each account meets its budget threshold. Add a budget action that selects the 1AM identity created with the appropriate service control policy (SCP) to prevent provisioning of additional resources.

Answer: B,D,F

Explanation: To use AWS Budgets to create and manage budgets for different AWS accounts, the company needs to do the following steps:

➪ Use AWS Budgets to create a budget for each AWS account that needs a different budget amount. The budget can be based on cost or usage metrics, and can have different time periods, filters, and thresholds. The company can set the budget amount under the Billing dashboards of the

required AWS accounts1.

➪ Create an IAM role for AWS Budgets to run budget actions with the required permissions. A budget action is a response that AWS Budgets initiates when a budget exceeds a specified threshold. The IAM role allows AWS Budgets to perform actions on behalf of the company, such as applying an IAM policy or a service control policy (SCP) to restrict the provisioning of additional resources2.

➪ Add an alert to notify the company when each account meets its budget threshold.

The alert can be sent via email or Amazon SNS. The company can also add a budget action that selects the IAM role created and the appropriate SCP to prevent provisioning of additional resources. An SCP is a type of policy that can be applied to an AWS account or an organizational unit (OU) within AWS Organizations. An SCP can limit the actions that users and roles can perform in the account or OU3.

References:

➪ 4: https://aws.amazon.com/budgets/

➪ 1: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets- create.html

➪ 2: https://docs.aws.amazon.com/cost-management/latest/userguide/budgets- controls.html

➪ 3:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policie s_scps.html

507. - (Topic 4)

A company has NFS servers in an on-premises data center that need to periodically back up small amounts of data to Amazon S3. Which solution meets these requirements and is MOST cost-effective?

A. Set up AWS Glue to copy the data from the on-premises servers to Amazon S3.

B. Set up an AWS DataSync agent on the on-premises servers, and sync the data to Amazon S3.

C. Set up an SFTP sync using AWS Transfer for SFTP to sync data from on premises to Amazon S3.

D. Set up an AWS Direct Connect connection between the on-premises data center and a VPC, and copy the data to Amazon S3.

Answer: B

Explanation: AWS DataSync is a service that makes it easy to move large amounts of data online between on-premises storage and AWS storage services. AWS DataSync can transfer data at speeds up to 10 times faster than open-source tools by using a purpose- built network protocol and parallelizing data transfers.

AWS DataSync also handles encryption, data integrity verification, and bandwidth optimization. To use AWS DataSync, users need to deploy a DataSync agent on their on-premises servers, which connects to the NFS servers and syncs the data to Amazon S3. Users can schedule periodic or one- time sync tasks and monitor the progress and status of the transfers.

The other options are not correct because they are either not cost-effective or not suitable for the use case. Setting up AWS Glue to copy the data from the on-premises servers to Amazon S3 is not cost-effective because AWS Glue is a serverless data integration service that is mainly used for extract, transform, and load (ETL) operations, not for simple data backup. Setting up an SFTP sync using AWS Transfer for SFTP to sync data from on premises to Amazon S3 is not cost-effective because AWS Transfer for SFTP is a fully managed service that provides secure file transfer using the SFTP protocol, which is more suitable for exchanging data with third parties than for backing up data. Setting up an AWS Direct Connect connection between the on-premises data center and a VPC, and copying the data to Amazon S3 is not cost-effective because AWS Direct Connect is a dedicated network connection between AWS and the on-premises location, which has high upfront costs and requires additional configuration.

References:

- AWS DataSync
- How AWS DataSync works
- AWS DataSync FAQs

508. - (Topic 4)

A company is moving its on-premises Oracle database to Amazon Aurora PostgreSQL. The database has several applications that write to the same tables. The applications need to be migrated one by one with a month in between each migration. Management has expressed concerns that the database has a high number of reads and writes. The data must be kept in sync across both databases throughout the migration.

What should a solutions architect recommend?

A. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a change data capture (CDC) replication task and a table mapping to select all tables.

B. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.

C. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a memory optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.

D. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a compute optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select the largest tables.

Answer: C

Explanation: https://aws.amazon.com/ko/premiumsupport/knowledge-center/dms- memory-optimization/

509. - (Topic 4)

The customers of a finance company request appointments with financial advisors by sending text messages. A web application that runs on Amazon EC2 instances accepts the appointment requests. The text messages are published to an Amazon Simple Queue Service (Amazon SQS) queue through the web application. Another application that runs on EC2 instances then sends meeting invitations and meeting confirmation email messages to the customers. After successful scheduling, this application stores the meeting information in an Amazon DynamoDB database.

As the company expands, customers report that their meeting invitations are taking longer to arrive.

What should a solutions architect recommend to resolve this issue?

A. Add a DynamoDB Accelerator (DAX) cluster in front of the DynamoDB database.

B. Add an Amazon API Gateway API in front of the web application that accepts the appointment requests.

C. Add an Amazon CloudFront distribution. Set the origin as the web application that accepts the appointment requests.

D. Add an Auto Scaling group for the application that sends meeting invitations. Configure the Auto Scaling group to scale based on the depth of the SQS queue.

Answer: D

Explanation: To resolve the issue of longer delivery times for meeting invitations, the solutions architect can recommend adding an Auto Scaling group for the application that sends meeting invitations and configuring the Auto Scaling group to scale based on the depth of the SQS queue. This will allow the application to scale up as the number of appointment requests increases, improving the performance and delivery times of the meeting invitations.

510. - (Topic 4)

An IoT company is releasing a mattress that has sensors to collect data about a user's sleep. The sensors will send data to an Amazon S3 bucket. The sensors collect approximately 2 MB of data every night for each mattress. The company must process and summarize the data for each mattress. The results need to be available as soon as possible Data processing will require 1 GB of memory and will finish within 30 seconds.

Which solution will meet these requirements MOST cost-effectively?

A. Use AWS Glue with a Scalajob.

B. Use Amazon EMR with an Apache Spark script.

C. Use AWS Lambda with a Python script.

D. Use AWS Glue with a PySpark job.

Answer: C

Explanation: AWS Lambda charges you based on the number of invocations and the execution time of your function. Since the data processing job is relatively small (2 MB of data), Lambda is a cost-effective choice. You only pay for the actual usage without the need to provision and maintain infrastructure.

511. - (Topic 4)

A company has an online gaming application that has TCP and UDP multiplayer gaming capabilities. The company uses Amazon Route 53 to point the application traffic to multiple Network Load Balancers (NLBs) in different AWS Regions. The company needs to improve application performance and decrease latency for the online game in preparation for user growth.

Which solution will meet these requirements?

A. Add an Amazon CloudFront distribution in front of the NLBs. Increase the Cache- Control: max-age parameter.

B. Replace the NLBs with Application Load Balancers (ALBs). Configure Route 53 to use latency-based routing.

C. Add AWS Global Accelerator in front of the NLBs. Configure a Global Accelerator endpoint to use the correct listener ports.

D. 'Add an Amazon API Gateway endpoint behind the NLBs. Enable API caching. Override method caching

for the different stages.

Answer: C

Explanation: This answer is correct because it improves the application performance and decreases latency for the online game by using AWS Global Accelerator. AWS Global Accelerator is a networking service that helps you improve the availability, performance, and security of your public applications. Global Accelerator provides two global static public IPs that act as a fixed entry point to your application endpoints, such as NLBs, in different AWS Regions. Global Accelerator uses the AWS global network to route traffic to the optimal regional endpoint based on health, client location, and policies that you configure. Global Accelerator also terminates TCP and UDP traffic at the edge locations, which reduces the number of hops and improves the network performance. By adding AWS Global Accelerator in front of the NLBs, you can achieve up to 60% improvement in latency for your online game.

References:

- https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global- accelerator.html
- https://aws.amazon.com/global-accelerator/

512. - (Topic 4)

A company is designing a new web application that will run on Amazon EC2 Instances. The application will use Amazon DynamoDB for backend data storage. The application traffic will be unpredictable. T company expects that the application read and write throughput to the database will be moderate to high. The company needs to scale in response to application traffic.

Which DynamoDB table configuration will meet these requirements MOST cost-effectively?

A. Configure DynamoDB with provisioned read and write by using the DynamoDB Standard table class. Set DynamoDB auto scaling to a maximum defined capacity.

B. Configure DynamoDB in on-demand mode by using the DynamoDB Standard table class.

C. Configure DynamoDB with provisioned read and write by using the DynamoDB Standard Infrequent Access (DynamoDB Standard-IA) table class. Set DynamoDB auto scaling to a maximum defined capacity.

D. Configure DynamoDB in on-demand mode by using the DynamoDB Standard Infrequent Access (DynamoDB Standard-IA) table class.

Answer: B

Explanation: The most cost-effective DynamoDB table configuration for the web application is to configure

DynamoDB in on-demand mode by using the DynamoDB Standard table class. This configuration will allow the company to scale in response to application traffic and pay only for the read and write requests that the application performs on the table.

On-demand mode is a flexible billing option that can handle thousands of requests per second without capacity planning. On-demand mode automatically adjusts the table's capacity based on the incoming traffic, and charges only for the read and write requests that are actually performed. On-demand mode is suitable for applications with unpredictable or variable workloads, or applications that prefer the ease of paying for only what they use1.

The DynamoDB Standard table class is the default and recommended table class for most workloads. The DynamoDB Standard table class offers lower throughput costs than the DynamoDB Standard-Infrequent Access (DynamoDB Standard-IA) table class, and is more cost-effective for tables where throughput is the dominant cost. The DynamoDB Standard table class also offers the same performance, durability, and availability as the DynamoDB Standard-IA table class2.

The other options are not correct because they are either not cost-effective or not suitable for the use case. Configuring DynamoDB with provisioned read and write by using the DynamoDB Standard table class, and setting DynamoDB auto scaling to a maximum defined capacity is not correct because this configuration requires manual estimation and management of the table's capacity, which adds complexity and cost to the solution. Provisioned mode is a billing option that requires users to specify the amount of read and write capacity units for their tables, and charges for the reserved capacity regardless of usage. Provisioned mode is suitable for applications with predictable or stable workloads, or applications that require finer-grained control over their capacity settings1. Configuring DynamoDB with provisioned read and write by using the DynamoDB Standard-Infrequent Access (DynamoDB Standard-IA) table class, and setting DynamoDB auto scaling to a maximum defined capacity is not correct because this configuration is not cost-effective for tables with moderate to high throughput. The DynamoDB Standard-IA table class offers lower storage costs than the DynamoDB Standard table class, but higher throughput costs. The DynamoDB Standard-IA table class is optimized for tables where storage is the dominant cost, such as tables that store infrequently accessed data2. Configuring DynamoDB in on-demand mode by using the DynamoDB Standard-Infrequent Access (DynamoDB Standard-IA) table class is not correct because this configuration is not cost- effective for tables with moderate to high throughput. As mentioned above, the DynamoDB Standard-IA table class has higher throughput costs than the DynamoDB Standard table class, which can offset the savings from

lower storage costs.

References:

- Table classes - Amazon DynamoDB
- Read/write capacity mode - Amazon DynamoDB

513. - (Topic 4)

A company has multiple Windows file servers on premises. The company wants to migrate and consolidate its files into an Amazon FSx for Windows File Server file system. File permissions must be preserved to ensure that access rights do not change.

Which solutions will meet these requirements? (Select TWO.)

A. Deploy AWS DataSync agents on premises. Schedule DataSync tasks to transfer the data to the FSx for Windows File Server file system.

B. Copy the shares on each file server into Amazon S3 buckets by using the AWS CLI Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system.

C. Remove the drives from each file server Ship the drives to AWS for import into Amazon S3. Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system

D. Order an AWS Snowcone device. Connect the device to the on-premises network. Launch AWS DataSync agents on the device. Schedule DataSync tasks to transfer the data to the FSx for Windows File Server file system,

E. Order an AWS Snowball Edge Storage Optimized device. Connect the device to the on- premises network. Copy data to the device by using the AWS CLI. Ship the device back to AWS for import into Amazon S3. Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system.

Answer: A,D

Explanation: A This option involves deploying DataSync agents on your on-premises file servers and using DataSync to transfer the data directly to the FSx for Windows File Server. DataSync ensures that file permissions are preserved during the migration process. D This option involves using an AWS Snowcone device, a portable data transfer device. You would connect the Snowcone device to your on-premises network, launch DataSync agents on the device, and schedule DataSync tasks to transfer the data to FSx for Windows File Server. DataSync handles the migration process while preserving file permissions.

514. - (Topic 4)

A company has a large workload that runs every Friday evening. The workload runs on Amazon EC2 instances that are in two Availability Zones in the us-east-1 Region. Normally, the company must run no more than two instances at all times. However, the company wants to scale up to six instances each Friday to handle a regularly repeating increased workload.

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

A. Create a reminder in Amazon EventBridge to scale the instances.

B. Create an Auto Scaling group that has a scheduled action.

C. Create an Auto Scaling group that uses manual scaling.

D. Create an Auto Scaling group that uses automatic scaling.

Answer: B

Explanation: An Auto Scaling group is a collection of EC2 instances that share similar characteristics and can be scaled in or out automatically based on demand. An Auto Scaling group can have a scheduled action, which is a configuration that tells the group to scale to a specific size at a specific time. This way, the company can scale up to six instances each Friday evening to handle the increased workload, and scale down to two instances at other times to save costs. This solution meets the requirements with the least operational overhead, as it does not require manual intervention or custom scripts. References:

- 1 explains how to create a scheduled action for an Auto Scaling group.
- 2 describes the concept and benefits of an Auto Scaling group.

515. - (Topic 4)

A social media company wants to allow its users to upload images in an application that is hosted in the AWS Cloud. The company needs a solution that automatically resizes the images so that the images can be displayed on multiple device types. The application experiences unpredictable traffic patterns throughout the day. The company is seeking a highly available solution that maximizes scalability.

What should a solutions architect do to meet these requirements?

A. Create a static website hosted in Amazon S3 that invokes AWS Lambda functions to resize the images and store the images in an Amazon S3 bucket.

B. Create a static website hosted in Amazon CloudFront that invokes AWS Step Functions to resize the

images and store the images in an Amazon RDS database.

C. Create a dynamic website hosted on a web server that runs on an Amazon EC2 instance Configure a process that runs on the EC2 instance to resize the images and store the images in an Amazon S3 bucket.

D. Create a dynamic website hosted on an automatically scaling Amazon Elastic Container Service (Amazon ECS) cluster that creates a resize job in Amazon Simple Queue Service (Amazon SQS). Set up an image-resizing program that runs on an Amazon EC2 instance to process the resize jobs

Answer: A

Explanation: By using Amazon S3 and AWS Lambda together, you can create a serverless architecture that provides highly scalable and available image resizing capabilities. Here's how the solution would work: Set up an Amazon S3 bucket to store the original images uploaded by users. Configure an event trigger on the S3 bucket to invoke an AWS Lambda function whenever a new image is uploaded. The Lambda function can be designed to retrieve the uploaded image, perform the necessary resizing operations based on device requirements, and store the resized images back in the S3 bucket or a different bucket designated for resized images. Configure the Amazon S3 bucket to make the resized images publicly accessible for serving to users.

516. - (Topic 4)

A company is running a microservices application on Amazon EC2 instances. The company wants to migrate the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for scalability. The company must configure the Amazon EKS control plane with endpoint private access set to true and endpoint public access set to false to maintain security compliance The company must also put the data plane in private subnets. However, the company has received error notifications because the node cannot join the cluster.

Which solution will allow the node to join the cluster?

A. Grant the required permission in AWS Identity and Access Management (1AM) to the AmazonEKSNodeRole 1AM role.

B. Create interface VPC endpoints to allow nodes to access the control plane.

C. Recreate nodes in the public subnet Restrict security groups for EC2 nodes

D. Allow outbound traffic in the security group of the nodes.

Answer: B

Explanation: Kubernetes API requests within your cluster's VPC (such as node to control plane communication) use the private VPC endpoint.

https://docs.aws.amazon.com/eks/latest/userguide/cluster-endpoint.html

517. - (Topic 4)

A company needs to store data from its healthcare application. The application's data frequently changes. A new regulation requires audit z access at all levels of the stored data.

The company hosts the application on an on-premises infrastructure that is running out of storage capacity. A solutions architect must securely migrate the existing data to AWS while satisfying the new regulation.

Which solution will meet these requirements?

A. Use AWS DataSync to move the existing data to Amazon S3. Use AWS CloudTrail to log data events.

B. Use AWS Snowcone to move the existing data to Amazon $3. Use AWS CloudTrail to log management events.

C. Use Amazon S3 Transfer Acceleration to move the existing data to Amazon S3. Use AWS CloudTrail to log data events.

D. Use AWS Storage Gateway to move the existing data to Amazon S3. Use AWS CloudTrail to log management events.

Answer: A

Explanation: This answer is correct because it meets the requirements of securely migrating the existing data to AWS and satisfying the new regulation. AWS DataSync is a service that makes it easy to move large amounts of data online between on-premises storage and Amazon S3. DataSync automatically encrypts data in transit and verifies data integrity during transfer. AWS CloudTrail is a service that records AWS API calls for your account and delivers log files to Amazon S3. CloudTrail can log data events, which show the resource operations performed on or within a resource in your AWS account, such as S3 object-level API activity. By using CloudTrail to log data events, you can audit access at all levels of the stored data.

References:

- https://docs.aws.amazon.com/datasync/latest/userguide/what-is-datasync.html
- https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-data-events- with-cloudtrail.html

518. - (Topic 4)

A company stores critical data in Amazon DynamoDB tables in the company's AWS account. An IT administrator accidentally deleted a DynamoDB table. The deletion caused a significant loss of data and disrupted the company's operations. The company wants to prevent this type of disruption in the future.

Which solution will meet this requirement with the LEAST operational overhead?

A. Configure a trail in AWS CloudTrail. Create an Amazon EventBridge rule for delete actions. Create an AWS Lambda function to automatically restore deleted DynamoDB tables.

B. Create a backup and restore plan for the DynamoDB tables. Recover the DynamoDB tables manually.

C. Configure deletion protection on the DynamoDB tables.

D. Enable point-in-time recovery on the DynamoDB tables.

Answer: C

Explanation: Deletion protection is a feature of DynamoDB that prevents accidental deletion of tables. When deletion protection is enabled, you cannot delete a table unless you explicitly disable it first. This adds an extra layer of security and reduces the risk of data loss and operational disruption. Deletion protection is easy to enable and disable using the AWS Management Console, the AWS CLI, or the DynamoDB API. This solution has the least operational overhead, as you do not need to create, manage, or invoke any additional resources or services. References:

- Using deletion protection to protect your table
- Preventing Accidental Table Deletion in DynamoDB
- Amazon DynamoDB now supports table deletion protection

519. - (Topic 4)

A company is running a photo hosting service in the us-east-1 Region. The service enables users across multiple countries to upload and view photos. Some photos are heavily viewed for months, and others are viewed for less than a week. The application allows uploads of up to 20 MB for each photo. The service uses the photo metadata to determine which photos to display to each user.

Which solution provides the appropriate user access MOST cost-effectively?

A. Store the photos in Amazon DynamoDB. Turn on DynamoDB Accelerator (DAX) to cache frequently viewed items.

B. Store the photos in the Amazon S3 Intelligent-Tiering storage class. Store the photo metadata and its S3 location in DynamoDB.

C. Store the photos in the Amazon S3 Standard storage class. Set up an S3 Lifecycle policy to move photos older than 30 days to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Use the object tags to keep track of metadata.

D. Store the photos in the Amazon S3 Glacier storage class. Set up an S3 Lifecycle policy to move photos older than 30 days to the S3 Glacier Deep Archive storage class. Store the photo metadata and its S3 location in Amazon OpenSearch Service.

Answer: B

Explanation: This solution provides the appropriate user access most cost-effectively because it uses the Amazon S3 Intelligent-Tiering storage class, which automatically optimizes storage costs by moving data to the most cost-effective access tier when access patterns change, without performance impact or operational overhead1. This storage class is ideal for data with unknown, changing, or unpredictable access patterns, such as photos that are heavily viewed for months or less than a week. By storing the photo metadata and its S3 location in DynamoDB, the application can quickly query and retrieve the relevant photos for each user. DynamoDB is a fast, scalable, and fully managed NoSQL database service that supports key-value and document data models2.

References: 1: Amazon S3 Intelligent-Tiering Storage Class | AWS3, Overview section2: Amazon DynamoDB - NoSQL Cloud Database Service4, Overview section.

520. - (Topic 4)

A global marketing company has applications that run in the ap-southeast-2 Region and the eu-west-1 Region. Applications that run in a VPC in eu-west-1 need to communicate securely with databases that run in a VPC in ap-southeast-2.

Which network design will meet these requirements?

A. Create a VPC peering connection between the eu-west-1 VPC and the ap-southeast-2 VPC. Create an inbound rule in the eu-west-1 application security group that allows traffic from the database server IP addresses in the ap-southeast-2 security group.

B. Configure a VPC peering connection between the ap-southeast-2 VPC and the eu-west- 1 VPC. Update the subnet route tables. Create an inbound rule in the ap-southeast-2 database security group that

references the security group ID of the application servers in eu-west-1.

C. Configure a VPC peering connection between the ap-southeast-2 VPC and the eu-west- 1 VPC. Update the subnet route tables Create an inbound rule in the ap-southeast-2 database security group that allows traffic from the eu-west-1 application server IP addresses.

D. Create a transit gateway with a peering attachment between the eu-west-1 VPC and the ap-southeast-2 VPC. After the transit gateways are properly peered and routing is configured, create an inbound rule in the database security group that references the security group ID of the application servers in eu-west-1.

Answer: C

Explanation: "You cannot reference the security group of a peer VPC that's in a different Region. Instead, use the CIDR block of the peer VPC."

https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-security-groups.html

521. - (Topic 4)

A company has data collection sensors at different locations. The data collection sensors stream a high volume of data to the company. The company wants to design a platform on AWS to ingest and process high-volume streaming data. The solution must be scalable and support data collection in near real time. The company must store the data in Amazon S3 for future reporting.

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

A. Use Amazon Kinesis Data Firehose to deliver streaming data to Amazon S3.

B. Use AWS Glue to deliver streaming data to Amazon S3.

C. Use AWS Lambda to deliver streaming data and store the data to Amazon S3.

D. Use AWS Database Migration Service (AWS DMS) to deliver streaming data to Amazon S3.

Answer: A

Explanation: To ingest and process high-volume streaming data with the least operational overhead, Amazon Kinesis Data Firehose is a suitable solution. Amazon Kinesis Data Firehose can capture, transform, and deliver streaming data to Amazon S3 or other destinations. Amazon Kinesis Data Firehose can scale automatically to match the throughput of the data and handle any amount of data. Amazon Kinesis Data Firehose is also a fully managed service that does not require any servers to provision or manage. References:

- What Is Amazon Kinesis Data Firehose?

⇨ Amazon Kinesis Data Firehose Pricing

522. - (Topic 4)

A company runs a website that uses a content management system (CMS) on Amazon EC2. The CMS runs on a single EC2 instance and uses an Amazon Aurora MySQL Multi- AZ DB instance for the data tier. Website images are stored on an Amazon Elastic Block Store (Amazon EBS) volume that is mounted inside the EC2 instance.

Which combination of actions should a solutions architect take to improve the performance and resilience of the website? (Select TWO.)

A. Move the website images into an Amazon S3 bucket that is mounted on every EC2 instance.

B. Share the website images by using an NFS share from the primary EC2 instance. Mount this share on the other EC2 instances.

C. Move the website images onto an Amazon Elastic File System (Amazon EFS) file system that is mounted on every EC2 instance.

D. Create an Amazon Machine Image (AMI) from the existing EC2 instance Use the AMI to provision new instances behind an Application Load Balancer as part of an Auto Scaling group. Configure the Auto Scaling group to maintain a minimum of two instances. Configure an accelerator in AWS Global Accelerator for the website.

E. Create an Amazon Machine Image (AMI) from the existing EC2 instance. Use the AMI to provision new instances behind an Application Load Balancer as part of an Auto Scaling group. Configure the Auto Scaling group to maintain a minimum of two instances. Configure an Amazon CloudFront distribution for the website.

Answer: C,E

Explanation: Option C provides moving the website images onto an Amazon EFS file system that is mounted on every EC2 instance. Amazon EFS provides a scalable and fully managed file storage solution that can be accessed concurrently from multiple EC2 instances. This ensures that the website images can be accessed efficiently and consistently by all instances, improving performance In Option E The Auto Scaling group maintains a minimum of two instances, ensuring resilience by automatically replacing any unhealthy instances. Additionally, configuring an Amazon CloudFront distribution for the website further improves performance by caching content at edge locations closer to the end-users, reducing latency and

improving content delivery. Hence combining these actions, the website's performance is improved through efficient image storage and content delivery

523. - (Topic 4)

An ecommerce company stores terabytes of customer data in the AWS Cloud. The data contains personally identifiable information (PII). The company wants to use the data in three applications. Only one of the applications needs to process the PII. The PII must be removed before the other two applications process the data.

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

A. Store the data in an Amazon DynamoDB table. Create a proxy application layer to intercept and process the data that each application requests.

B. Store the data in an Amazon S3 bucket. Process and transform the data by using S3 Object Lambda before returning the data to the requesting application.

C. Process the data and store the transformed data in three separate Amazon S3 buckets so that each application has its own custom dataset. Point each application to its respective S3 bucket.

D. Process the data and store the transformed data in three separate Amazon DynamoDB tables so that each application has its own custom dataset. Point each application to its respective DynamoDB table.

Answer: B

Explanation: https://aws.amazon.com/blogs/aws/introducing-amazon-s3-object-lambda-use-your-code-to-process-data-as-it-is-being-retrieved-from-s3/

S3 Object Lambda is a new feature of Amazon S3 that enables customers to add their own code to process data retrieved from S3 before returning it to the application. By using S3 Object Lambda, the data can be processed and transformed in real-time, without the need to store multiple copies of the data in separate S3 buckets or DynamoDB tables.

In this case, the PII can be removed from the data by the code added to S3 Object Lambda before returning the data to the two applications that do not need to process PII. The one application that requires PII can be pointed to the original S3 bucket where the PII is still stored.

Using S3 Object Lambda is the simplest and most cost-effective solution, as it eliminates the need to maintain multiple copies of the same data in different buckets or tables, which can result in additional

storage costs and operational overhead.

524. - (Topic 4)

A company wants to create an application to store employee data in a hierarchical structured relationship. The company needs a minimum-latency response to high-traffic queries for the employee data and must protect any sensitive data. The company also needs to receive monthly email messages if any financial information is present in the employee data.

Which combination of steps should a solutions architect take to meet these requirements? (Select TWO.)

A. Use Amazon Redshift to store the employee data in hierarchies. Unload the data to Amazon S3 every month.

B. Use Amazon DynamoDB to store the employee data in hierarchies. Export the data to Amazon S3 every month.

C. Configure Amazon fvlacie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly events to AWS Lambda.

D. Use Amazon Athena to analyze the employee data in Amazon S3. Integrate Athena with Amazon QuickSight to publish analysis dashboards and share the dashboards with users.

E. Configure Amazon Macie for the AWS account Integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon Simple Notification Service (Amazon SNS) subscription.

Answer: B,E

Explanation: Generally, for building a hierarchical relationship model, a graph database such as Amazon Neptune is a better choice. In some cases, however, DynamoDB is a better choice for hierarchical data modeling because of its flexibility, security, performance, and scale.

https://docs.aws.amazon.com/prescriptive-guidance/latest/dynamodb-hierarchical-data-model/introduction.html

525. - (Topic 4)

A company runs a web application on Amazon EC2 instances in an Auto Scaling group that has a target group. The company desgned the application to work with session affinity (sticky sessions) for a better user experience.

The application must be available publicly over the internet as an endpoint_ A WAF must be applied to the endpoint for additional security. Session affinity (sticky sessions) must be configured on the endpoint

Which combination of steps will meet these requirements? (Select TWO)

A. Create a public Network Load Balancer Specify the application target group.

B. Create a Gateway Load Balancer Specify the application target group.

C. Create a public Application Load Balancer Specify the application target group.

D. Create a second target group. Add Elastic IP addresses to the EC2 instances

E. Create a web ACL in AWS WAF Associate the web ACL with the endpoint

Answer: C,E

Explanation: C and E are the correct answers because they allow the company to create a public endpoint for its web application that supports session affinity (sticky sessions) and has a WAF applied for additional security. By creating a public Application Load Balancer, the company can distribute incoming traffic across multiple EC2 instances in an Auto Scaling group and specify the application target group. By creating a web ACL in AWS WAF and associating it with the Application Load Balancer, the company can protect its web application from common web exploits. By enabling session stickiness on the

Application Load Balancer, the company can ensure that subsequent requests from a user during a session are routed to the same target. References:

- Application Load Balancers
- AWS WAF
- Target Groups for Your Application Load Balancers
- How Application Load Balancer Works with Sticky Sessions

526. - (Topic 4)

A company previously migrated its data warehouse solution to AWS. The company also has an AWS Direct Connect connection. Corporate office users query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 50 MB and each webpage sent by the visualization tool is approximately 500 KB. Result sets returned by the data warehouse are not cached.

Which solution provides the LOWEST data transfer egress cost for the company?

A. Host the visualization tool on premises and query the data warehouse directly over the internet.

B. Host the visualization tool in the same AWS Region as the data warehouse. Access it over the internet.

C. Host the visualization tool on premises and query the data warehouse directly over a Direct Connect connection at a location in the same AWS Region.

D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection at a location in the same Region.

Answer: D

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

https://aws.amazon.com/blogs/aws/aws-data-transfer-prices-reduced/

527. - (Topic 4)

A company runs a container application on a Kubernetes cluster in the company's data center The application uses Advanced Message Queuing Protocol (AMQP) to communicate with a message queue The data center cannot scale fast enough to meet the company's expanding business needs The company wants to migrate the workloads to AWS

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

A. Migrate the container application to Amazon Elastic Container Service (Amazon ECS) Use Amazon Simple Queue Service (Amazon SQS) to retrieve the messages.

B. Migrate the container application to Amazon Elastic Kubernetes Service (Amazon EKS) Use Amazon MQ to retrieve the messages.

C. Use highly available Amazon EC2 instances to run the application Use Amazon MQ to retrieve the messages.

D. Use AWS Lambda functions to run the application Use Amazon Simple Queue Service (Amazon SQS) to retrieve the messages.

Answer: B

Explanation: This option is the best solution because it allows the company to migrate the container application to AWS with minimal changes and leverage a managed service to run the Kubernetes cluster and the message queue. By using Amazon EKS, the company can run the container application on a fully managed Kubernetes control plane that is compatible with the existing Kubernetes tools and plugins. Amazon EKS handles the provisioning, scaling, patching, and security of the Kubernetes cluster, reducing the operational overhead and complexity. By using Amazon MQ, the company can use a fully managed message broker service that supports AMQP and other popular messaging protocols. Amazon MQ handles

the administration, maintenance, and scaling of the message broker, ensuring high availability, durability, and security of the messages.

* A. Migrate the container application to Amazon Elastic Container Service (Amazon ECS) Use Amazon Simple Queue Service (Amazon SQS) to retrieve the messages. This option is not optimal because it requires the company to change the container orchestration platform from Kubernetes to ECS, which can introduce additional complexity and risk. Moreover, it requires the company to change the messaging protocol from AMQP to SQS, which can also affect the application logic and performance. Amazon ECS and Amazon SQS are both fully managed services that simplify the deployment and management of containers and messages, but they may not be compatible with the existing application architecture and requirements.

* C. Use highly available Amazon EC2 instances to run the application Use Amazon MQ to retrieve the messages. This option is not ideal because it requires the company to manage the EC2 instances that host the container application. The company would need to provision, configure, scale, patch, and monitor the EC2 instances, which can increase the operational overhead and infrastructure costs. Moreover, the company would need to install and maintain the Kubernetes software on the EC2 instances, which can also add complexity and risk. Amazon MQ is a fully managed message broker service that supports AMQP and other popular messaging protocols, but it cannot compensate for the lack of a managed Kubernetes service.

* D. Use AWS Lambda functions to run the application Use Amazon Simple Queue Service (Amazon SQS) to retrieve the messages. This option is not feasible because AWS Lambda does not support running container applications directly. Lambda functions are executed in a sandboxed environment that is isolated from other functions and resources. To run container applications on Lambda, the company would need to use a custom runtime or a wrapper library that emulates the container API, which can introduce additional complexity and overhead. Moreover, Lambda functions have limitations in terms of available CPU, memory, and runtime, which may not suit the application needs. Amazon SQS is a fully managed message queue service that supports asynchronous communication, but it does not support AMQP or other messaging protocols.

References:

- 1 Amazon Elastic Kubernetes Service - Amazon Web Services
- 2 Amazon MQ - Amazon Web Services

- 3 Amazon Elastic Container Service - Amazon Web Services
- 4 AWS Lambda FAQs - Amazon Web Services

528. - (Topic 4)

A company wants to manage Amazon Machine Images (AMIs). The company currently copies AMIs to the same AWS Region where the AMIs were created. The company needs to design an application that captures AWS API calls and sends alerts whenever the Amazon EC2 CreateImage API operation is called within the company's account.

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

A. Create an AWS Lambda function to query AWS CloudTrail logs and to send an alert when a CreateImage API call is detected.

B. Configure AWS CloudTrail with an Amazon Simple Notification Service (Amazon SNS) notification that occurs when updated logs are sent to Amazon S3. Use Amazon Athena to create a new table and to query on CreateImage when an API call is detected.

C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for the CreateImage API call. Configure the target as an Amazon Simple Notification Service (Amazon SNS) topic to send an alert when a CreateImage API call is detected.

D. Configure an Amazon Simple Queue Service (Amazon SQS) FIFO queue as a target for AWS CloudTrail logs. Create an AWS Lambda function to send an alert to an Amazon Simple Notification Service (Amazon SNS) topic when a CreateImage API call is detected.

Answer: C

Explanation: https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/monitor-ami-events.html#:~:text=For%20example%2C%20you%20can%20create%20an%20EventBridge%20rule%20that%20detects%20when%20the%20AMI%20creation%20process%20has%20completed%20and%20then%20invokes%20an%20Amazon%20SNS%20topic%20to%20send%20an%20email%20notification%20to%20you.

529. - (Topic 4)

A company is deploying an application that processes streaming data in near-real time The company plans to use Amazon EC2 instances for the workload The network architecture must be configurable to provide

the lowest possible latency between nodes

Which combination of network solutions will meet these requirements? (Select TWO)

A. Enable and configure enhanced networking on each EC2 instance

B. Group the EC2 instances in separate accounts

C. Run the EC2 instances in a cluster placement group

D. Attach multiple elastic network interfaces to each EC2 instance

E. Use Amazon Elastic Block Store (Amazon EBS) optimized instance types.

Answer: A,C

Explanation: These options are the most suitable ways to configure the network architecture to provide the lowest possible latency between nodes. Option A enables and configures enhanced networking on each EC2 instance, which is a feature that improves the network performance of the instance by providing higher bandwidth, lower latency, and lower jitter. Enhanced networking uses single root I/O virtualization (SR-IOV) or Elastic Fabric Adapter (EFA) to provide direct access to the network hardware. You can enable and configure enhanced networking by choosing a supported instance type and a compatible operating system, and installing the required drivers. Option C runs the EC2 instances in a cluster placement group, which is a logical grouping of instances within a single Availability Zone that are placed close together on the same underlying hardware. Cluster placement groups provide the lowest network latency and the highest network throughput among the placement group options. You can run the EC2 instances in a cluster placement group by creating a placement group and launching the instances into it. Option B is not suitable because grouping the EC2 instances in separate accounts does not provide the lowest possible latency between nodes. Separate accounts are used to isolate and organize resources for different purposes, such as security, billing, or compliance. However, they do not affect the network performance or proximity of the instances. Moreover, grouping the EC2 instances in separate accounts would incur additional costs and complexity, and it would require setting up cross-account networking and permissions.

Option D is not suitable because attaching multiple elastic network interfaces to each EC2 instance does not provide the lowest possible latency between nodes. Elastic network interfaces are virtual network interfaces that can be attached to EC2 instances to provide additional network capabilities, such as multiple IP addresses, multiple subnets, or enhanced security. However, they do not affect the network performance or proximity of the instances. Moreover, attaching multiple elastic network interfaces to each EC2 instance would consume additional resources and limit the instance type choices.

Option E is not suitable because using Amazon EBS optimized instance types does not provide the lowest possible latency between nodes. Amazon EBS optimized instance types are instances that provide dedicated bandwidth for Amazon EBS volumes, which are block storage volumes that can be attached to EC2 instances. EBS optimized instance types improve the performance and consistency of the EBS volumes, but they do not affect the network performance or proximity of the instances. Moreover, using EBS optimized instance types would incur additional costs and may not be necessary for the streaming data workload. References:

- Enhanced networking on Linux
- Placement groups
- Elastic network interfaces
- Amazon EBS-optimized instances

530. - (Topic 4)

A company has a production workload that is spread across different AWS accounts in various AWS Regions. The company uses AWS Cost Explorer to continuously monitor costs and usage. The company wants to receive notifications when the cost and usage spending of the workload is unusual.

Which combination of steps will meet these requirements? (Select TWO.)

A. In the AWS accounts where the production workload is running, create a linked account budget by using Cost Explorer in the AWS Cost Management console

B. In ys AWS accounts where the production workload is running, create a linked account monitor by using AWS Cost Anomaly Detection in the AWS Cost Management console

C. In the AWS accounts where the production workload is running, create a Cost and Usage Report by using Cost Anomaly Detection in the AWS Cost Management console.

D. Create a report and send email messages to notify the company on a weekly basis.

E. Create a subscription with the required threshold and notify the company by using weekly summaries.

Answer: B,E

Explanation: AWS Cost Anomaly Detection allows you to create monitors that track the cost and usage of your AWS resources and alert you when there is an unusual spending pattern. You can create monitors based on different dimensions, such as AWS services, accounts, tags, or cost categories. You can also create alert subscriptions that notify you by email or Amazon SNS when an anomaly is detected. You can

specify the threshold and frequency of the alerts, and choose to receive weekly summaries of your anomalies. Reference URLs:

1 https://aws.amazon.com/aws-cost-management/aws-cost-anomaly-detection/

2 https://docs.aws.amazon.com/cost-management/latest/userguide/getting-started-ad.html

3 https://docs.aws.amazon.com/cost-management/latest/userguide/manage-ad.html

531. - (Topic 4)

A company's reporting system delivers hundreds of .csv files to an Amazon S3 bucket each day. The company must convert these files to Apache Parquet format and must store the files in a transformed data bucket.

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

A. Create an Amazon EMR cluster with Apache Spark installed. Write a Spark application to transform the data. Use EMR File System (EMRFS) to write files to the transformed data bucket.

B. Create an AWS Glue crawler to discover the data. Create an AWS Glue extract, transform, and load (ETL) job to transform the data. Specify the transformed data bucket in the output step.

C. Use AWS Batch to create a job definition with Bash syntax to transform the data and output the data to the transformed data bucket. Use the job definition to submit a job. Specify an array job as the job type.

D. Create an AWS Lambda function to transform the data and output the data to the transformed data bucket. Configure an event notification for the S3 bucket. Specify the Lambda function as the destination for the event notification.

Answer: B

Explanation: https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html

532. - (Topic 4)

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

solutions architect do to meet these requirements?

A. Deploy a NAT instance in the VPC. Route all the internet-based traffic through the NAT instance.

B. Deploy a NAT gateway in the public subnets. Modify the private subnet route table to direct all internet-bound traffic to the NAT gateway.

C. Configure an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the internet gateway.

D. Configure a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the virtual private gateway.

Answer: B

Explanation: To allow the MySQL database in the private subnets to access the internet without exposing it to the public, a NAT gateway is a suitable solution. A NAT gateway enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating a connection with those instances. A NAT gateway resides in the public subnets and can handle high throughput of traffic with low latency. A NAT gateway is also a managed service that does not require any operational overhead.

References:

- NAT Gateways
- NAT Gateway Pricing

533. - (Topic 4)

A company runs analytics software on Amazon EC2 instances The software accepts job requests from users to process data that has been uploaded to Amazon S3 Users report that some submitted data is not being processed Amazon CloudWatch reveals that the EC2 instances have a consistent CPU utilization at or near 100% The company wants to improve system performance and scale the system based on user load.

What should a solutions architect do to meet these requirements?

A. Create a copy of the instance Place all instances behind an Application Load Balancer

B. Create an S3 VPC endpoint for Amazon S3 Update the software to reference the endpoint

C. Stop the EC2 instances. Modify the instance type to one with a more powerful CPU and more memory. Restart the instances.

D. Route incoming requests to Amazon Simple Queue Service (Amazon SQS) Configure an EC2 Auto

Scaling group based on queue size Update the software to read from the queue.

Answer: D

Explanation: This option is the best solution because it allows the company to decouple the analytics software from the user requests and scale the EC2 instances dynamically based on the demand. By using Amazon SQS, the company can create a queue that stores the user requests and acts as a buffer between the users and the analytics software. This way, the software can process the requests at its own pace without losing any data or overloading the EC2 instances. By using EC2 Auto Scaling, the company can create an Auto Scaling group that launches or terminates EC2 instances automatically based on the size of the queue. This way, the company can ensure that there are enough instances to handle the load and optimize the cost and performance of the system. By updating the software to read from the queue, the company can enable the analytics software to consume the requests from the queue and process the data from Amazon S3.

* A. Create a copy of the instance Place all instances behind an Application Load Balancer. This option is not optimal because it does not address the root cause of the problem, which is the high CPU utilization of the EC2 instances. An Application Load Balancer can distribute the incoming traffic across multiple instances, but it cannot scale the instances based on the load or reduce the processing time of the analytics software. Moreover, this option can incur additional costs for the load balancer and the extra instances.

* B. Create an S3 VPC endpoint for Amazon S3 Update the software to reference the endpoint. This option is not effective because it does not solve the issue of the high CPU utilization of the EC2 instances. An S3 VPC endpoint can enable the EC2 instances to access Amazon S3 without going through the internet, which can improve the network performance and security. However, it cannot reduce the processing time of the analytics software or scale the instances based on the load.

* C. Stop the EC2 instances. Modify the instance type to one with a more powerful CPU and more memory. Restart the instances. This option is not scalable because it does not account for the variability of the user load. Changing the instance type to a more powerful one can improve the performance of the analytics software, but it cannot adjust the number of instances based on the demand. Moreover, this option can increase the cost of the system and cause downtime during the instance modification.

References:

- 1 Using Amazon SQS queues with Amazon EC2 Auto Scaling - Amazon EC2 Auto Scaling

- 2 Tutorial: Set up a scaled and load-balanced application - Amazon EC2 Auto Scaling
- 3 Amazon EC2 Auto Scaling FAQs

534. - (Topic 4)

A company sends AWS CloudTrail logs from multiple AWS accounts to an Amazon S3 bucket in a centralized account. The company must keep the CloudTrail logs. The company must also be able to query the CloudTrail logs at any time

Which solution will meet these requirements?

A. Use the CloudTrail event history in the centralized account to create an Amazon Athena table. Query the CloudTrail logs from Athena.

B. Configure an Amazon Neptune instance to manage the CloudTrail logs. Query the CloudTrail logs from Neptune.

C. Configure CloudTrail to send the logs to an Amazon DynamoDB table. Create a dashboard in Amazon QulCkSight to query the logs in the table.

D. use Amazon Athena to create an Athena notebook. Configure CloudTrail to send the logs to the notebook. Run queries from Athena.

Answer: A

Explanation: it allows the company to keep the CloudTrail logs and query them at any time. By using the CloudTrail event history in the centralized account, the company can view, filter, and download recent API activity across multiple AWS accounts. By creating an Amazon Athena table from the CloudTrail event history, the company can use a serverless interactive query service that makes it easy to analyze data in S3 using standard SQL. By querying the CloudTrail logs from Athena, the company can gain insights into user activity and resource changes. References:

- Viewing Events with CloudTrail Event History
- Querying AWS CloudTrail Logs
- Amazon Athena

535. - (Topic 4)

A company has resources across multiple AWS Regions and accounts. A newly hired solutions architect discovers a previous employee did not provide details about the resources invent^. The solutions architect

needs to build and map the relationship details of the various workloads across all accounts.

Which solution will meet these requirements in the MOST operationally efficient way?

A. Use AWS Systems Manager Inventory to generate a map view from the detailed view report.

B. Use AWS Step Functions to collect workload details Build architecture diagrams of the workloads manually.

C. Use Workload Discovery on AWS to generate architecture diagrams of the workloads.

D. Use AWS X-Ray to view the workload details Build architecture diagrams with relationships

Answer: C

Explanation:

Workload Discovery on AWS (formerly called AWS Perspective) is a tool that visualizes AWS Cloud workloads. It maintains an inventory of the AWS resources across your accounts and Regions, mapping relationships between them, and displaying them in a web UI. It also allows you to query AWS Cost and Usage Reports, search for resources, save and export architecture diagrams, and more1. By using Workload Discovery on AWS, the solution can build and map the relationship details of the various workloads across all accounts with the least operational effort.

* A. Use AWS Systems Manager Inventory to generate a map view from the detailed view report. This solution will not meet the requirement of building and mapping the relationship details of the various workloads across all accounts, as AWS Systems Manager Inventory is a feature that collects metadata from your managed instances and stores it in a central Amazon S3 bucket. It does not provide a map view or architecture diagrams of the workloads2.

* B. Use AWS Step Functions to collect workload details Build architecture diagrams of the work-loads manually. This solution will not meet the requirement of the least operational effort, as it involves creating and managing state machines to orchestrate the workload details collection, and building architecture diagrams manually.

* D. Use AWS X-Ray to view the workload details Build architecture diagrams with relationships. This solution will not meet the requirement of the least operational effort, as it involves instrumenting your applications with X-Ray SDKs to collect workload details, and building architecture diagrams manually.

Reference URL: https://aws.amazon.com/solutions/implementations/workload-discovery- on-aws/

536. - (Topic 4)

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

What should the solutions architect recommend?

A. Configure AWS CloudTrail trails to tog S3 API calls Use AWS AppSync to process the files.

B. Configure an object-created event notification within the S3 bucket to invoke an AWS Lambda function to process the files.

C. Configure Amazon Kinesis Data Streams to process and send data to Amazon S3. Invoke an AWS Lambda function to process the files.

D. Configure an Amazon Simple Notification Service (Amazon SNS) topic to process the files uploaded to Amazon S3 Invoke an AWS Lambda function to process the files.

Answer: B

Explanation: This option is the most cost-effective and scalable way to process the files uploaded to S3. AWS CloudTrail is used to log API calls, not to trigger actions based on them. AWS AppSync is a service for building GraphQL APIs, not for processing files. Amazon Kinesis Data Streams is used to ingest and process streaming data, not to send data to S3. Amazon SNS is a pub/sub service that can be used to notify subscribers of events, not to process files. References:

- Using AWS Lambda with Amazon S3
- AWS CloudTrail FAQs
- What Is AWS AppSync?
- [What Is Amazon Kinesis Data Streams?]
- [What Is Amazon Simple Notification Service?]

537. - (Topic 4)

A company uses Amazon S3 as its data lake. The company has a new partner that must use SFTP to upload data files A solutions architect needs to implement a highly available SFTP solution that minimizes operational overhead.

Which solution will meet these requirements?

A. Use AWS Transfer Family to configure an SFTP-enabled server with a publicly accessible endpoint

Choose the S3 data lake as the destination

B. Use Amazon S3 File Gateway as an SFTP server Expose the S3 File Gateway endpoint URL to the new partner Share the S3 File Gateway endpoint with the new

partner

C. Launch an Amazon EC2 instance in a private subnet in a VPC. Instruct the new partner to upload files to the EC2 instance by using a VPN. Run a cron job script on the EC2 instance to upload files to the S3 data lake

D. Launch Amazon EC2 instances in a private subnet in a VPC. Place a Network Load Balancer (NLB) in front of the EC2 instances. Create an SFTP listener port for the NLB

Share the NLB hostname with the new partner Run a cron job script on the EC2 instances to upload files to the S3 data lake.

Answer: A

Explanation: This option is the most cost-effective and simple way to enable SFTP access to the S3 data lake. AWS Transfer Family is a fully managed service that supports secure file transfers over SFTP, FTPS, and FTP protocols. You can create an SFTP-enabled server with a public endpoint and associate it with your S3 bucket. You can also use AWS Identity and Access Management (IAM) roles and policies to control access to your S3 data lake. The service scales automatically to handle any volume of file transfers and provides high availability and durability. You do not need to provision, manage, or patch any servers or load balancers.

Option B is not correct because Amazon S3 File Gateway is not an SFTP server. It is a hybrid cloud storage service that provides a local file system interface to S3. You can use it to store and retrieve files as objects in S3 using standard file protocols such as NFS and SMB. However, it does not support SFTP protocol, and it requires deploying a file gateway appliance on-premises or on EC2.

Option C is not cost-effective or scalable because it requires launching and managing an EC2 instance in a private subnet and setting up a VPN connection for the new partner. This would incur additional costs for the EC2 instance, the VPN connection, and the data transfer. It would also introduce complexity and security risks to the solution. Moreover, it would require running a cron job script on the EC2 instance to upload files to the S3 data lake, which is not efficient or reliable.

Option D is not cost-effective or scalable because it requires launching and managing multiple EC2 instances in a private subnet and placing a NLB in front of them. This would incur additional costs for the

EC2 instances, the NLB, and the data transfer. It would also introduce complexity and security risks to the solution. Moreover, it would require running a cron job script on the EC2 instances to upload files to the S3 data lake, which is not efficient or reliable. References:

- What Is AWS Transfer Family?
- What Is Amazon S3 File Gateway?
- What Is Amazon EC2?
- [What Is Amazon Virtual Private Cloud?]
- [What Is a Network Load Balancer?]

538. - (Topic 4)

A media company collects and analyzes user activity data on premises. The company wants to migrate this capability to AWS. The user activity data store will continue to grow

and will be petabytes in size. The company needs to build a highly available data ingestion solution that facilitates on-demand analytics of existing data and new data with SQL.

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

A. Send activity data to an Amazon Kinesis data stream. Configure the stream to deliver the data to an Amazon S3 bucket.

B. Send activity data to an Amazon Kinesis Data Firehose delivery stream. Configure the stream to deliver the data to an Amazon Redshift cluster.

C. Place activity data in an Amazon S3 bucket. Configure Amazon S3 to run an AWS Lambda function on the data as the data arrives in the S3 bucket.

D. Create an ingestion service on Amazon EC2 instances that are spread across multiple Availability Zones. Configure the service to forward data to an Amazon RDS Multi-AZ database.

Answer: B

Explanation: Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. You can start with just a few hundred gigabytes of data and scale to a petabyte or more. This allows you to use your data to gain new insights for your business and customers. The first step to create a data warehouse is to launch a set of nodes, called an Amazon Redshift cluster. After you provision your cluster, you can upload your data set and then perform data analysis queries. Regardless of the size of the data set, Amazon Redshift offers fast query performance using the same SQL-based tools and business intelligence

applications that you use today.

539. - (Topic 4)

A company runs multiple workloads in its on-premises data center. The company's data center cannot scale fast enough to meet the company's expanding business needs. The company wants to collect usage and configuration data about the on-premises servers and workloads to plan a migration to AWS.

Which solution will meet these requirements?

A. Set the home AWS Region in AWS Migration Hub. Use AWS Systems Manager to collect data about the on-premises servers.

B. Set the home AWS Region in AWS Migration Hub. Use AWS Application Discovery Service to collect data about the on-premises servers.

C. Use the AWS Schema Conversion Tool (AWS SCT) to create the relevant templates. Use AWS Trusted Advisor to collect data about the on-premises servers.

D. Use the AWS Schema Conversion Tool (AWS SCT) to create the relevant templates.

Use AWS Database Migration Service (AWS DMS) to collect data about the on-premises servers.

Answer: B

Explanation: The most suitable solution for the company’s requirements is to set the home AWS Region in AWS Migration Hub and use AWS Application Discovery Service to collect data about the on-premises servers. This solution will enable the company to gather usage and configuration data of its on-premises servers and workloads, and plan a migration to AWS.

AWS Migration Hub is a service that simplifies and accelerates migration tracking by aggregating migration status information into a single console. Users can view the discovered servers, group them into applications, and track the migration status of each application from the Migration Hub console in their home Region. The home Region is the AWS Region where users store their migration data, regardless of which Regions they migrate into1.

AWS Application Discovery Service is a service that helps users plan their migration to AWS by collecting usage and configuration data about their on-premises servers and databases. Application Discovery Service is integrated with AWS Migration Hub and supports two methods of performing discovery: agentless discovery and agent-based discovery. Agentless discovery can be performed by deploying the Application Discovery Service Agentless Collector through VMware vCenter, which collects static

configuration data and utilization data for virtual machines (VMs) and databases. Agent-based discovery can be performed by deploying the AWS Application Discovery Agent on each of the VMs and physical servers, which collects static configuration data, detailed time-series system- performance information, inbound and outbound network connections, and processes that are running2.

The other options are not correct because they do not meet the requirements or are not relevant for the use case. Using the AWS Schema Conversion Tool (AWS SCT) to create the relevant templates and using AWS Trusted Advisor to collect data about the on- premises servers is not correct because this solution is not suitable for collecting usage and configuration data of on-premises servers and workloads. AWS SCT is a tool that helps users convert database schemas and code objects from one database engine to another, such as from Oracle to PostgreSQL3. AWS Trusted Advisor is a service that provides best practice recommendations for cost optimization, performance, security, fault tolerance, and service limits4. Using the AWS Schema Conversion Tool (AWS SCT) to create the relevant templates and using AWS Database Migration Service (AWS DMS) to collect data about the on-premises servers is not correct because this solution is not suitable for collecting usage and configuration data of on-premises servers and workloads. As mentioned above, AWS SCT is a tool that helps users convert database schemas and code objects from one database engine to another. AWS DMS is a service that helps users migrate relational databases, non-relational databases, and other types of data stores to

AWS with minimal downtime5. References:

- Home Region - AWS Migration Hub
- What is AWS Application Discovery Service? - AWS Application Discovery Service
- AWS Schema Conversion Tool - Amazon Web Services
- What Is Trusted Advisor? - Trusted Advisor
- What Is AWS Database Migration Service? - AWS Database Migration Service

540. - (Topic 4)

A company has a three-tier application for image sharing. The application uses an Amazon EC2 instance for the front-end layer, another EC2 instance for the application layer, and a third EC2 instance for a MySQL database. A solutions architect must design a scalable and highly available solution that requires the least amount of change to the application.

Which solution meets these requirements?

A. Use Amazon S3 to host the front-end layer. Use AWS Lambda functions for the application layer. Move the database to an Amazon DynamoDB table. Use Amazon S3 to store and serve users' images.

B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS DB instance with multiple read replicas to serve users' images.

C. Use Amazon S3 to host the front-end layer. Use a fleet of EC2 instances in an Auto Scaling group for the application layer. Move the database to a memory optimized instance type to store and serve users' images.

D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS Multi-AZ DB instance. Use Amazon S3 to store and serve users' images.

Answer: D

Explanation: for "Highly available": Multi-AZ & for "least amount of changes to the application": Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring

541. - (Topic 4)

A gaming company wants to launch a new internet-facing application in multiple AWS Regions The application will use the TCP and UDP protocols for communication. The company needs to provide high availability and minimum latency for global users.

Which combination of actions should a solutions architect take to meet these requirements? (Select TWO.)

A. Create internal Network Load Balancers in front of the application in each Region.

B. Create external Application Load Balancers in front of the application in each Region.

C. Create an AWS Global Accelerator accelerator to route traffic to the load balancers in each Region.

D. Configure Amazon Route 53 to use a geolocation routing policy to distribute the traffic.

E. Configure Amazon CloudFront to handle the traffic and route requests to the application in each Region.

Answer: B,C

Explanation: This combination of actions will provide high availability and minimum latency for global users by using AWS Global Accelerator and Application Load Balancers. AWS Global Accelerator is a networking service that helps you improve the availability, performance, and security of your internet-facing

applications by using the AWS global network. It provides two global static public IPs that act as a fixed entry point to your application endpoints, such as Application Load Balancers, in multiple Regions1. Global Accelerator uses the AWS backbone network to route traffic to the optimal regional endpoint based on health, client location, and policies that you configure. It also offers TCP and UDP support, traffic encryption, and DDoS protection2. Application Load Balancers are external load balancers that distribute incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. They support both HTTP and HTTPS (SSL/TLS) protocols, and offer advanced features such as content-based routing, health checks, and integration with other AWS services3. By creating external Application Load Balancers in front of the application in each Region, you can ensure that the application can handle varying load patterns and scale on demand. By creating an AWS Global Accelerator accelerator to route traffic to the load balancers in each Region, you can leverage the performance, security, and availability of the AWS global network to deliver the best possible user experience.

References: 1: What is AWS Global Accelerator? - AWS Global Accelerator4, Overview section2: Network Acceleration Service - AWS Global Accelerator - AWS5, Why AWS Global Accelerator? section. 3: What is an Application Load Balancer? - Elastic Load Balancing6, Overview section.

542. - (Topic 4)

A company wants to use an event-driven programming model with AWS Lambda. The company wants to reduce startup latency for Lambda functions that run on Java 11. The company does not have strict latency requirements for the applications. The company wants to reduce cold starts and outlier latencies when a function scales up.

Which solution will meet these requirements MOST cost-effectively?

A. Configure Lambda provisioned concurrency.

B. Increase the timeout of the Lambda functions.

C. Increase the memory of the Lambda functions.

D. Configure Lambda SnapStart.

Answer: D

Explanation: To reduce startup latency for Lambda functions that run on Java 11, Lambda SnapStart is a suitable solution. Lambda SnapStart is a feature that enables faster cold starts and lower outlier latencies for Java 11 functions. Lambda SnapStart uses a pre- initialized Java Virtual Machine (JVM) to run the

functions, which reduces the initialization time and memory footprint. Lambda SnapStart does not incur any additional charges. References:

- Lambda SnapStart for Java 11 Functions
- Lambda SnapStart FAQs

543. - (Topic 4)

A company designed a stateless two-tier application that uses Amazon EC2 in a single Availability Zone and an Amazon RDS Multi-AZ DB instance New company management wants to ensure the application is highly available.

What should a solutions architect do to meet this requirement?

A. Configure the application to use Multi-AZ EC2 Auto Scaling and create an Application Load Balancer

B. Configure the application to take snapshots of the EC2 instances and send them to a different AWS Region.

C. Configure the application to use Amazon Route 53 latency-based routing to feed requests to the application.

D. Configure Amazon Route 53 rules to handle incoming requests and create a Multi-AZ Application Load Balancer

Answer: A

Explanation: https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-availability- zone.html

544. - (Topic 4)

A company needs to minimize the cost of its 1 Gbps AWS Direct Connect connection. The company's average connection utilization is less than 10%. A solutions architect must recommend a solution that will reduce the cost without compromising security.

Which solution will meet these requirements?

A. Set up a new 1 Gbps Direct Connect connection. Share the connection with another AWS account.

B. Set up a new 200 Mbps Direct Connect connection in the AWS Management Console.

C. Contact an AWS Direct Connect Partner to order a 1 Gbps connection. Share the connection with another AWS account.

D. Contact an AWS Direct Connect Partner to order a 200 Mbps hosted connection for an existing AWS

account.

Answer: D

Explanation: company need to setup a cheaper connection (200 M) but B is incorrect because you can only order port speeds of 1, 10, or 100 Gbps for more flexibility you can go with hosted connection, You can order port speeds between 50 Mbps and 10 Gbps.

https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct- connect.html

545. - (Topic 4)

A company runs a container application by using Amazon Elastic Kubernetes Service (Amazon EKS). The application includes microservices that manage customers and place orders. The company needs to route incoming requests to the appropriate microservices.

Which solution will meet this requirement MOST cost-effectively?

A. Use the AWS Load Balancer Controller to provision a Network Load Balancer.

B. Use the AWS Load Balancer Controller to provision an Application Load Balancer.

C. Use an AWS Lambda function to connect the requests to Amazon EKS.

D. Use Amazon API Gateway to connect the requests to Amazon EKS.

Answer: B

Explanation: An Application Load Balancer is a type of Elastic Load Balancer that operates at the application layer (layer 7) of the OSI model. It can distribute incoming traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can also route requests based on the content of the request, such as the host name, path, or query parameters1.

The AWS Load Balancer Controller is a controller that helps you manage Elastic Load Balancers for your Kubernetes cluster. It can provision Application Load Balancers or Network Load Balancers when you create Kubernetes Ingress or Service resources2.

By using the AWS Load Balancer Controller to provision an Application Load Balancer for your Amazon EKS cluster, you can achieve the following benefits:

- You can route incoming requests to the appropriate microservices based on the rules you define in your Ingress resource. For example, you can route requests with different host names or paths to different microservices that handle customers and orders2.
- You can improve the performance and availability of your container applications by

distributing the load across multiple targets and enabling health checks and automatic scaling1.

➪ You can reduce the cost and complexity of managing your load balancers by using a single controller that integrates with Amazon EKS and Kubernetes. You do not need to manually create or configure load balancers or update them when your cluster changes2.

546. - (Topic 4)

A company needs to integrate with a third-party data feed. The data feed sends a webhook to notify an external service when new data is ready for consumption A developer wrote an AWS Lambfe function to retrieve data when the company receives a webhook callback The developer must make the Lambda function available for the third party to call.

Which solution will meet these requirements with the MOST operational efficiency?

A. Create a function URL for the Lambda function. Provide the Lambda function URL to the third party for the webhook.

B. Deploy an Application Load Balancer (ALB) in front of the Lambda function. Provide the ALB URL to the third party for the webhook

C. Create an Amazon Simple Notification Service (Amazon SNS) topic. Attach the topic to the Lambda function. Provide the public hostname of the SNS topic to the third party for the webhook.

D. Create an Amazon Simple Queue Service (Amazon SQS) queue. Attach the queue to the Lambda function. Provide the public hostname of the SQS queue to the third party for the webhook.

Answer: A

Explanation:

A function URL is a unique identifier for a Lambda function that can be used to invoke the function over HTTPS. It is composed of the API endpoint of the AWS Region where the function is deployed, and the name or ARN of the function1. By creating a function URL for the Lambda function, the solution can make the Lambda function available for the third party to call with the most operational efficiency.

* B. Deploy an Application Load Balancer (ALB) in front of the Lambda function. Provide the ALB URL to the third party for the webhook. This solution will not meet the requirement of the most operational efficiency, as it involves creating and managing an additional resource (ALB) that is not necessary for invoking a Lambda function over HTTPS2.

* C. Create an Amazon Simple Notification Service (Amazon SNS) topic. Attach the topic to the Lambda function. Provide the public hostname of the SNS topic to the third party for the webhook. This solution will not work, as Amazon SNS topics do not have public hostnames that can be used as webhooks. SNS topics are used to publish messages to subscribers, not to receive messages from external sources3.

* D. Create an Amazon Simple Queue Service (Amazon SQS) queue. Attach the queue to the Lamb-da function. Provide the public hostname of the SQS queue to the third party for the webhook. This solution will not work, as Amazon SQS queues do not have public hostnames that can be used as webhooks. SQS queues are used to send, store, and receive messages between AWS services, not to receive messages from external sources. Reference URL:

https://docs.aws.amazon.com/lambda/latest/dg/lambda-api-permissions- ref.html

547. - (Topic 4)

A company hosts a data lake on Amazon S3. The data lake ingests data in Apache Parquet format from various data sources. The company uses multiple transformation steps to prepare the ingested data. The steps include filtering of anomalies, normalizing of data to standard date and time values, and generation of aggregates for analyses.

The company must store the transformed data in S3 buckets that data analysts access. The company needs a prebuilt solution for data transformation that does not require code. The solution must provide data lineage and data profiling. The company needs to share the data transformation steps with employees throughout the company.

Which solution will meet these requirements?

A. Configure an AWS Glue Studio visual canvas to transform the data. Share the transformation steps with employees by using AWS Glue jobs.

B. Configure Amazon EMR Serverless to transform the data. Share the transformation steps with employees by using EMR Serveriess jobs.

C. Configure AWS Glue DataBrew to transform the data. Share the transformation steps with employees by using DataBrew recipes.

D. Create Amazon Athena tables for the data. Write Athena SQL queries to transform the data. Share the Athena SQL queries with employees.

Answer: C

Explanation: The most suitable solution for the company's requirements is to configure AWS Glue DataBrew to transform the data and share the transformation steps with employees by using DataBrew recipes. This solution will provide a prebuilt solution for data transformation that does not require code, and will also provide data lineage and data profiling. The company can easily share the data transformation steps with employees throughout the company by using DataBrew recipes.

AWS Glue DataBrew is a visual data preparation tool that makes it easy for data analysts and data scientists to clean and normalize data for analytics or machine learning by up to 80% faster. Users can upload their data from various sources, such as Amazon S3, Amazon RDS, Amazon Redshift, Amazon Aurora, or Glue Data Catalog, and use a point- and-click interface to apply over 250 built-in transformations. Users can also preview the results of each transformation step and see how it affects the quality and distribution of the data1.

A DataBrew recipe is a reusable set of transformation steps that can be applied to one or more datasets. Users can create recipes from scratch or use existing ones from the DataBrew recipe library. Users can also export, import, or share recipes with other users or groups within their AWS account or organization2. DataBrew also provides data lineage and data profiling features that help users understand and improve their data quality. Data lineage shows the source and destination of each dataset and how it is transformed by each recipe step. Data profiling shows various statistics and metrics about each dataset, such as column

548. - (Topic 4)

A company runs its applications on Amazon EC2 instances. The company performs periodic financial assessments of itsAWS costs. The company recently identified unusual spending.

The company needs a solution to prevent unusual spending. The solution must monitor costs and notify responsible stakeholders in the event of unusual spending. Which solution will meet these requirements?

A. Use an AWS Budgets template to create a zero spend budget

B. Create an AWS Cost Anomaly Detection monitor in the AWS Billing and Cost Management console.

C. CreateAWS Pricing Calculator estimates for the current running workload pricing details_

D. Use Amazon CloudWatch to monitor costs and to identify unusual spending

Answer: B

Explanation: it allows the company to monitor costs and notify responsible stakeholders in the event of unusual spending. By creating an AWS Cost Anomaly Detection monitor in the AWS Billing and Cost

Management console, the company can use a machine learning service that automatically detects and alerts on anomalous spend. By configuring alert thresholds, notification preferences, and root cause analysis, the company can prevent unusual spending and identify its source. References:

- AWS Cost Anomaly Detection
- Creating a Cost Anomaly Monitor

549. - (Topic 4)

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

What should a solutions architect recommend?

A. Deploy Amazon Inspector and associate it with the ALB.

B. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.

C. Deploy rules to the network ACLs associated with the ALB to block the incoming traffic.

D. Deploy Amazon GuardDuty and enable rate-limiting protection when configuring GuardDuty.

Answer: B

Explanation: This answer is correct because it meets the requirements of blocking the illegitimate incoming requests in a way that has a minimal impact on legitimate users. AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic patterns you define. You can associate AWS WAF with an ALB to protect the web application from malicious requests. You can configure a rate-limiting rule in AWS WAF to track the rate of requests for each originating IP address and block requests from an IP address that exceeds a certain limit within a five-minute period. This way, you can mitigate potential DDoS attacks and improve the performance of your website.

References:

- https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html

➪ https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type- rate-based.html

550. - (Topic 4)

A company wants to use high-performance computing and artificial intelligence to improve its fraud prevention and detection technology. The company requires distributed processing to complete a single workload as quickly as possible.

Which solution will meet these requirements?

A. Use Amazon Elastic Kubernetes Service (Amazon EKS) and multiple containers.

B. Use AWS ParallelCluster and the Message Passing Interface (MPI) libraries.

C. Use an Application Load Balancer and Amazon EC2 instances.

D. Use AWS Lambda functions.

Answer: B

Explanation: AWS ParallelCluster is a service that allows you to create and manage high- performance computing (HPC) clusters on AWS. It supports multiple schedulers, including AWS Batch, which can run distributed workloads across multiple EC2 instances1.

MPI is a standard for message passing between processes in parallel computing. It provides functions for sending and receiving data, synchronizing processes, and managing communication groups2.

By using AWS ParallelCluster and MPI libraries, you can take advantage of the following benefits:

➪ You can easily create and configure HPC clusters that meet your specific requirements, such as instance type, number of nodes, network configuration, and storage options1.

➪ You can leverage the scalability and elasticity of AWS to run large-scale parallel workloads without worrying about provisioning or managing servers1.

➪ You can use MPI libraries to optimize the performance and efficiency of your parallel applications by enabling inter-process communication and data exchange2.

➪ You can choose from a variety of MPI implementations that are compatible with AWS ParallelCluster, such as Open MPI, Intel MPI, and MPICH3.

551. - (Topic 4)

A company runs a three-tier application in two AWS Regions. The web tier, the application tier, and the database tier run on Amazon EC2 instances. The company uses Amazon RDS for Microsoft SQL Server

Enterprise for the database tier The database tier is experiencing high load when weekly and monthly reports are run. The company wants to reduce the load on the database tier.

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

A. Create read replicas. Configure the reports to use the new read replicas.

B. Convert the RDS database to Amazon DynamoDB_ Configure the reports to use DynamoDB

C. Modify the existing RDS DB instances by selecting a larger instance size.

D. Modify the existing ROS DB instances and put the instances into an Auto Scaling group.

Answer: A

Explanation: it allows the company to create read replicas of its RDS database and reduce the load on the database tier. By creating read replicas, the company can offload read traffic from the primary database instance to one or more replicas. By configuring the reports to use the new read replicas, the company can improve performance and availability of its database tier. References:

- Working with Read Replicas
- Read Replicas for Amazon RDS for SQL Server

552. - (Topic 4)

A solutions architect needs to copy files from an Amazon S3 bucket to an Amazon Elastic File System (Amazon EFS) file system and another S3 bucket. The files must be copied continuously. New files are added to the original S3 bucket consistently. The copied files should be overwritten only if the source file changes.

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

A. Create an AWS DataSync location for both the destination S3 bucket and the EFS file system. Create a task for the destination S3 bucket and the EFS file system. Set the transfer mode to transfer only data that has changed.

B. Create an AWS Lambda function. Mount the file system to the function. Set up an S3 event notification to invoke the function when files are created and changed in Amazon S3. Configure the function to copy files to the file system and the destination S3 bucket.

C. Create an AWS DataSync location for both the destination S3 bucket and the EFS file system. Create a task for the destination S3 bucket and the EFS file system. Set the transfer mode to transfer all data.

D. Launch an Amazon EC2 instance in the same VPC as the file system. Mount the file system. Create a

script to routinely synchronize all objects that changed in the origin S3 bucket to the destination S3 bucket and the mounted file system.

Answer: A

Explanation: AWS DataSync is a service that makes it easy to move large amounts of data between AWS storage services and on-premises storage systems. AWS DataSync can copy files from an S3 bucket to an EFS file system and another S3 bucket continuously, as well as overwrite only the files that have changed in the source. This solution will meet the requirements with the least operational overhead, as it does not require any code development or manual intervention.

References:

- 4 explains how to create AWS DataSync locations for different storage services.
- 5 describes how to create and configure AWS DataSync tasks for data transfer.
- 6 discusses the different transfer modes that AWS DataSync supports.

553. - (Topic 4)

A company is making a prototype of the infrastructure for its new website by manually provisioning the necessary infrastructure. This infrastructure includes an Auto Scaling group, an Application Load Balancer, and an Amazon RDS database. After the configuration has been thoroughly validated, the company wants the capability to immediately deploy the infrastructure for development and production use in two Availability Zones in an automated fashion.

What should a solutions architect recommend to meet these requirements?

A. Use AWS Systems Manager to replicate and provision the prototype infrastructure in two Availability Zones.

B. Define the infrastructure as a template by using the prototype infrastructure as a guide. Deploy the infrastructure with AWS CloudFormation

C. Use AWS Config to record the inventory of resources that are used in the prototype infrastructure. Use AWS Config to deploy the prototype infrastructure into two Availability Zones.

D. Use AWS Elastic Beanstalk and configure it to use an automated reference to the prototype infrastructure to automatically deploy new environments in two Availability Zones

Answer: B

Explanation:

AWS CloudFormation is a service that helps you model and set up your AWS resources by using templates that describe all the resources that you want, such as Auto Scaling groups, load balancers, and databases. You can use AWS CloudFormation to deploy your infrastructure in an automated and consistent way across multiple environments and regions. You can also use AWS CloudFormation to update or delete your infrastructure as a single unit.

Reference URLs:

1 https://aws.amazon.com/cloudformation/

2 https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html

3 https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-whatis- concepts.html

554. - (Topic 4)

A company built an application with Docker containers and needs to run the application in the AWS Cloud The company wants to use a managed sen/ice to host the application

The solution must scale in and out appropriately according to demand on the individual container services The solution also must not result in additional operational overhead or infrastructure to manage

Which solutions will meet these requirements? (Select TWO)

A. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate.

B. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate.

C. Provision an Amazon API Gateway API Connect the API to AWS Lambda to run the containers.

D. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 worker nodes.

E. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 worker nodes.

Answer: A,B

Explanation: These options are the best solutions because they allow the company to run the application with Docker containers in the AWS Cloud using a managed service that scales automatically and does not require any infrastructure to manage. By using AWS Fargate, the company can launch and run containers without having to provision, configure, or scale clusters of EC2 instances. Fargate allocates the right amount of compute resources for each container and scales them up or down as needed. By using Amazon ECS or Amazon EKS, the company can choose the container orchestration platform that suits its needs. Amazon ECS is a fully managed service that integrates with other AWS services and simplifies the

deployment and management of containers. Amazon EKS is a managed service that runs Kubernetes on AWS and provides compatibility with existing Kubernetes tools and plugins.

* C. Provision an Amazon API Gateway API Connect the API to AWS Lambda to run the containers. This option is not feasible because AWS Lambda does not support running Docker containers directly. Lambda functions are executed in a sandboxed environment that is isolated from other functions and resources. To run Docker containers on Lambda, the company would need to use a custom runtime or a wrapper library that emulates the Docker API, which can introduce additional complexity and overhead.

* D. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 worker nodes. This option is not optimal because it requires the company to manage the EC2 instances that host the containers. The company would need to provision, configure, scale, patch, and monitor the EC2 instances, which can increase the operational overhead and infrastructure costs.

* E. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 worker nodes. This option is not ideal because it requires the company to manage the EC2 instances that host the containers. The company would need to provision, configure, scale, patch, and monitor the EC2 instances, which can increase the operational overhead and infrastructure costs.

References:

- 1 AWS Fargate - Amazon Web Services
- 2 Amazon Elastic Container Service - Amazon Web Services
- 3 Amazon Elastic Kubernetes Service - Amazon Web Services
- 4 AWS Lambda FAQs - Amazon Web Services

555. - (Topic 4)

A retail company has several businesses. The IT team for each business manages its own AWS account. Each team account is part of an organization in AWS Organizations. Each team monitors its product inventory levels in an Amazon DynamoDB table in the team's own AWS account.

The company is deploying a central inventory reporting application into a shared AWS account. The application must be able to read items from all the teams' DynamoDB tables.

Which authentication option will meet these requirements MOST securely?

A. Integrate DynamoDB with AWS Secrets Manager in the inventory application account. Configure the application to use the correct secret from Secrets Manager to authenticate and read the DynamoDB table.

Schedule secret rotation for every 30 days.

B. In every business account, create an 1AM user that has programmatic access. Configure the application to use the correct 1AM user access key ID and secret access key to authenticate and read the DynamoDB table. Manually rotate 1AM access keys every 30 days.

C. In every business account, create an 1AM role named BU_ROLE with a policy that gives the role access to the DynamoDB table and a trust policy to trust a specific role in the inventory application account. In the inventory account, create a role named APP_ROLE that allows access to the STS AssumeRole API operation. Configure the application to use APP_ROLE and assume the cross-account role BU_ROLE to read the DynamoDB table.

D. Integrate DynamoDB with AWS Certificate Manager (ACM). Generate identity certificates to authenticate DynamoDB. Configure the application to use the correct certificate to authenticate and read the DynamoDB table.

Answer: C

Explanation: This solution meets the requirements most securely because it uses IAM roles and the STS AssumeRole API operation to authenticate and authorize the inventory application to access the DynamoDB tables in different accounts. IAM roles are more secure than IAM users or certificates because they do not require long-term credentials or passwords. Instead, IAM roles provide temporary security credentials that are automatically rotated and can be configured with a limited duration. The STS AssumeRole API operation enables you to request temporary credentials for a role that you are allowed to assume. By using this operation, you can delegate access to resources that are in different AWS accounts that you own or that are owned by third parties. The trust policy of the role defines which entities can assume the role, and the permissions policy of the role defines which actions can be performed on the resources. By using this solution, you can avoid hard- coding credentials or certificates in the inventory application, and you can also avoid storing them in Secrets Manager or ACM. You can also leverage the built-in security features of IAM and STS, such as MFA, access logging, and policy conditions.

References:

- IAM Roles
- STS AssumeRole
- Tutorial: Delegate Access Across AWS Accounts Using IAM Roles

556. - (Topic 4)

A company has a web application hosted over 10 Amazon EC2 instances with traffic directed by Amazon Route 53. The company occasionally experiences a timeout error when attempting to browse the application. The networking team finds that some DNS queries return IP addresses of unhealthy instances, resulting in the timeout error.

What should a solutions architect implement to overcome these timeout errors?

A. Create a Route 53 simple routing policy record for each EC2 instance. Associate a health check with each record.

B. Create a Route 53 failover routing policy record for each EC2 instance. Associate a health check with each record.

C. Create an Amazon CloudFront distribution with EC2 instances as its origin. Associate a health check with the EC2 instances.

D. Create an Application Load Balancer (ALB) with a health check in front of the EC2 instances. Route to the ALB from Route 53.

Answer: D

Explanation:

An Application Load Balancer (ALB) allows you to distribute incoming traffic across multiple backend instances, and can automatically route traffic to healthy instances while removing traffic from unhealthy instances. By using an ALB in front of the EC2 instances and routing traffic to it from Route 53, the load balancer can perform health checks on the instances and only route traffic to healthy instances, which should help to reduce or eliminate timeout errors caused by unhealthy instances.

557. - (Topic 4)

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

Policy 1

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

Policy 2

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

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

A. Deleting IAM users

B. Deleting directories

C. Deleting Amazon EC2 instances

D. Deleting logs from Amazon CloudWatch Logs

Answer: C

Explanation:

https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ds/index.html

558. - (Topic 4)

A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world. Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.

What should a solutions architect do to accomplish this?

A. Use Amazon S3 with Transfer Acceleration to host the application.

B. Use Amazon S3 with CacheControl headers to host the application.

C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.

D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

Answer: C

Explanation:

This answer is correct because it meets the requirements of hosting a scalable web application that can handle large data transfers from different geographic regions. Amazon EC2 provides scalable compute capacity for hosting web applications. Auto Scaling can automatically adjust the number of EC2 instances based on the demand and traffic patterns. Amazon CloudFront is a content delivery network (CDN) that can cache static and dynamic content at edge locations closer to the users, reducing latency and improving performance. CloudFront can also use S3 Transfer Acceleration to speed up the transfers between S3 buckets and CloudFront edge locations.

References:

- https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2- auto-scaling.html
- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introducti on.html
- https://aws.amazon.com/s3/transfer-acceleration/

559. - (Topic 4)

A solutions architect is designing a REST API in Amazon API Gateway for a cash payback service The application requires 1 GB of memory and 2 GB of storage for its computation resources. The application will require that the data is in a relational format.

Which additional combination of AWS services will meet these requirements with the LEAST administrative effort? {Select TWO.)

A. Amazon EC2

B. AWS Lambda

C. Amazon RDS

D. Amazon DynamoDB

E. Amazon Elastic Kubernetes Services (Amazon EKS)

Answer: B,C

Explanation: AWS Lambda is a service that lets users run code without provisioning or managing servers. It automatically scales and manages the underlying compute resources for the code. It supports multiple languages, such as Java, Python, Node.js, and G1o. By using AWS Lambda for the REST API, the solution can meet the requirements of 1 GB of memory and minimal administrative effort.

Amazon RDS is a service that makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. It supports multiple database engines, such as MySQL, PostgreSQL, Oracle, and SQL Server2. By using Amazon RDS for the data store, the solution can meet the requirements of 2 GB of storage and a relational format.

* A. Amazon EC2. This solution will not meet the requirement of minimal administrative effort, as Amazon EC2 is a service that provides virtual servers in the cloud that users have to configure and manage themselves. It requires users to choose an instance type, an operating system, a security group, and other options3.

* D. Amazon DynamoDB. This solution will not meet the requirement of a relational format, as Amazon DynamoDB is a service that provides a key-value and document database that delivers single-digit millisecond performance at any scale. It is a non-relational or NoSQL database that does not support joins or transactions.

* E. Amazon Elastic Kubernetes Services (Amazon EKS). This solution will not meet the requirement of minimal administrative effort, as Amazon EKS is a service that provides a fully managed Kubernetes service that users have to configure and manage themselves. It requires users to create clusters, nodes groups, pods, services, and other Kubernetes resources.

Reference URL: https://aws.amazon.com/lambda/

560. - (Topic 4)

A company is conducting an internal audit. The company wants to ensure that the data in an Amazon S3

bucket that is associated with the company's AWS Lake Formation data lake does not contain sensitive customer or employee data. The company wants to discover personally identifiable information (PII) or financial information, including passport numbers and credit card numbers.

Which solution will meet these requirements?

A. Configure AWS Audit Manager on the account. Select the Payment Card Industry Data Security Standards (PCI DSS) for auditing.

B. Configure Amazon S3 Inventory on the S3 bucket. Configure Amazon Athena to query the inventory.

C. Configure Amazon Macie to run a data discovery job that uses managed identifiers for the required data types.

D. Use Amazon S3 Select to run a report across the S3 bucket.

Answer: C

Explanation: Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS. Macie can run data discovery jobs that use managed identifiers for various types of PII or financial information, such as passport numbers and credit card numbers. Macie can also generate findings that alert you to potential issues or risks with your data. References:

https://docs.aws.amazon.com/macie/latest/userguide/macie-identifiers.html

561. - (Topic 4)

A retail company uses a regional Amazon API Gateway API for its public REST APIs. The API Gateway endpoint is a custom domain name that points to an Amazon Route 53 alias record. A solutions architect needs to create a solution that has minimal effects on customers and minimal data loss to release the new version of APIs.

Which solution will meet these requirements?

A. Create a canary release deployment stage for API Gateway. Deploy the latest API version. Point an appropriate percentage of traffic to the canary stage. After API verification, promote the canary stage to the production stage.

B. Create a new API Gateway endpoint with a new version of the API in OpenAPI YAML file format. Use the import-to-update operation in merge mode into the API in API Gateway. Deploy the new version of the API to the production stage.

C. Create a new API Gateway endpoint with a new version of the API in OpenAPI JSON file format. Use the import-to-update operation in overwrite mode into the API in API Gateway. Deploy the new version of the API to the production stage.

D. Create a new API Gateway endpoint with new versions of the API definitions. Create a custom domain name for the new API Gateway API. Point the Route 53 alias record to the new API Gateway API custom domain name.

Answer: A

Explanation: This answer is correct because it meets the requirements of releasing the new version of APIs with minimal effects on customers and minimal data loss. A canary release deployment is a software development strategy in which a new version of an API is deployed for testing purposes, and the base version remains deployed as a production release for normal operations on the same stage. In a canary release deployment, total API traffic is separated at random into a production release and a canary release with a pre- configured ratio. Typically, the canary release receives a small percentage of API traffic and the production release takes up the rest. The updated API features are only visible to API traffic through the canary. You can adjust the canary traffic percentage to optimize test coverage or performance. By keeping canary traffic small and the selection random, most users are not adversely affected at any time by potential bugs in the new version, and no single user is adversely affected all the time. After the test metrics pass your requirements, you can promote the canary release to the production release and disable the canary from the deployment. This makes the new features available in the production stage. References:

☞ https://docs.aws.amazon.com/apigateway/latest/developerguide/canary-release.html

562. - (Topic 4)

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

What should the solutions architect recommend?

A. Remove the two NAT instances and replace them with two NAT gateways in the same Availability Zone.

B. Use Auto Scaling groups with Network Load Balancers for the NAT instances in different Availability Zones.

C. Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones.

D. Replace the two NAT instances with Spot Instances in different Availability Zones and deploy a Network Load Balancer.

Answer: C

Explanation: If you have resources in multiple Availability Zones and they share one NAT gateway, and if the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose internet access. To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone. https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html#nat-gateway- basics

563. - (Topic 4)

A company runs demonstration environments for its customers on Amazon EC2 instances. Each environment is isolated in its own VPC. The company's operations team needs to be notified when RDP or SSH access to an environment has been established.

A. Configure Amazon CloudWatch Application Insights to create AWS Systems Manager OpsItems when RDP or SSH access is detected.

B. Configure the EC2 instances with an IAM instance profile that has an IAM role with the AmazonSSMManagedInstanceCore policy attached.

C. Publish VPC flow logs to Amazon CloudWatch Logs. Create required metric filters. Create an Amazon CloudWatch metric alarm with a notification action for when the alarm is in the ALARM state.

D. Configure an Amazon EventBridge rule to listen for events of type EC2 Instance State- change Notification. Configure an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the operations team to the topic.

Answer: C

Explanation: https://aws.amazon.com/blogs/security/how-to-monitor-and-visualize-failed-ssh-access-attempts-to-amazon-ec2-linux-instances/

564. - (Topic 4)

A company has deployed a multiplayer game for mobile devices. The game requires live location tracking of players based on latitude and longitude. The data store for the game must support rapid updates and retrieval of locations.

The game uses an Amazon RDS for PostgreSQL DB instance with read replicas to store the location data. During peak usage periods, the database is unable to maintain the performance that is needed for reading and writing updates. The game's user base is increasing rapidly.

What should a solutions architect do to improve the performance of the data tier?

A. Take a snapshot of the existing DB instance. Restore the snapshot with Multi-AZ enabled.

B. Migrate from Amazon RDS to Amazon OpenSearch Service with OpenSearch Dashboards.

C. Deploy Amazon DynamoDB Accelerator (DAX) in front of the existing DB instance. Modify the game to use DAX.

D. Deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instance. Modify the game to use Redis.

Answer: D

Explanation: The solution that will improve the performance of the data tier is to deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instance and modify the game to use Redis. This solution will enable the game to store and retrieve the location data of the players in a fast and scalable way, as Redis is an in-memory data store that supports geospatial data types and commands. By using ElastiCache for Redis, the game can reduce the load on the RDS for PostgreSQL DB instance, which is not optimized for high-frequency updates and queries of location data. ElastiCache for Redis also supports replication, sharding, and auto scaling to handle the increasing user base of the game. The other solutions are not as effective as the first one because they either do not improve the performance, do not support geospatial data, or do not leverage caching. Taking a snapshot of the existing DB instance and restoring it with Multi-AZ enabled will not improve the performance of the data tier, as it only provides high availability and durability, but not scalability or low latency. Migrating from Amazon RDS to Amazon OpenSearch Service with OpenSearch Dashboards will not improve the performance of the data tier, as OpenSearch Service is mainly designed for full-text search and analytics, not for real-time location tracking. OpenSearch Service also does not support geospatial data types and commands natively, unlike Redis. Deploying Amazon DynamoDB Accelerator (DAX) in front of the existing DB instance and modifying the game to use DAX will not improve the performance of the data tier, as DAX is only compatible with DynamoDB, not with RDS for PostgreSQL. DAX also does not support geospatial data types and commands. References:

- Amazon ElastiCache for Redis
- Geospatial Data Support - Amazon ElastiCache for Redis

- Amazon RDS for PostgreSQL
- Amazon OpenSearch Service
- Amazon DynamoDB Accelerator (DAX)

565. - (Topic 4)

A company runs an infrastructure monitoring service. The company is building a new feature that will enable the service to monitor data in customer AWS accounts. The new feature will call AWS APIs in customer accounts to describe Amazon EC2 instances and read Amazon CloudWatch metrics.

What should the company do to obtain access to customer accounts in the MOST secure way?

A. Ensure that the customers create an 1AM role in their account with read-only EC2 and CloudWatch permissions and a trust policy to the company's account.

B. Create a serverless API that implements a token vending machine to provide temporary AWS credentials for a role with read-only EC2 and CloudWatch permissions.

C. Ensure that the customers create an 1AM user in their account with read-only EC2 and CloudWatch permissions. Encrypt and store customer access and secret keys in a secrets management system.

D. Ensure that the customers create an Amazon Cognito user in their account to use an 1AM role with read-only EC2 and CloudWatch permissions. Encrypt and store the Amazon Cognito user and password in a secrets management system.

Answer: A

Explanation: By having customers create an IAM role with the necessary permissions in their own accounts, the company can use AWS Identity and Access Management (IAM) to establish cross-account access. The trust policy allows the company's AWS account to assume the customer's IAM role temporarily, granting access to the specified resources (EC2 instances and CloudWatch metrics) within the customer's account. This approach follows the principle of least privilege, as the company only requests the necessary permissions and does not require long-term access keys or user credentials from the customers.

566. - (Topic 4)

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

seconds after a request is made.

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

A. An AWS Glue job

B. An AWS Lambda function

C. A containerized service hosted in Amazon Elastic Kubernetes Service (Amazon EKS)

D. A containerized service hosted in Amazon ECS with Amazon EC2

Answer: B

Explanation: API Gateway + Lambda is the perfect solution for modern applications with serverless architecture.

567. - (Topic 4)

A company runs a web application that is deployed on Amazon EC2 instances in the private subnet of a VPC. An Application Load Balancer (ALB) that extends across the public subnets directs web traffic to the EC2 instances. The company wants to implement new security measures to restrict inbound traffic from the ALB to the EC2 instances while preventing access from any other source inside or outside the private subnet of the EC2 instances.

Which solution will meet these requirements?

A. Configure a route in a route table to direct traffic from the internet to the private IP addresses of the EC2 instances.

B. Configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB.

C. Move the EC2 instances into the public subnet. Give the EC2 instances a set of Elastic IP addresses.

D. Configure the security group for the ALB to allow any TCP traffic on any port.

Answer: B

Explanation: To restrict inbound traffic from the ALB to the EC2 instances, the security group for the EC2 instances should only allow traffic that comes from the security group for the ALB. This way, the EC2 instances can only receive requests from the ALB and not from any other source inside or outside the private subnet.

References:

- Security Groups for Your Application Load Balancers
- Security Groups for Your VPC

568. - (Topic 4)

A company is developing a new machine learning (ML) model solution on AWS. The models are developed as independent microservices that fetch approximately 1 GB of model data from Amazon $3 at startup and load the data into memory. Users access the models through an asynchronous API. Users can send a request or a batch of requests and specify where the results should be sent.

The company provides models to hundreds of users. The usage patterns for the models are irregular. Some models could be unused for days or weeks. Other models could receive batches of thousands of requests at a time.

Which design should a solutions architect recommend to meet these requirements?

A. Direct the requests from the API to a Network Load Balancer (NLB). Deploy the models as AWS Lambda functions that are invoked by the NLB.

B. Direct the requests from the API to an Application Load Balancer (ALB). Deploy the models as Amazon Elastic Container Service (Amazon ECS) services that read from an Amazon Simple Queue Service (Amazon SQS) queue. Use AWS App Mesh to scale the instances of the ECS cluster based on the SQS queue size.

C. Direct the requests from the API into an Amazon Simple Queue Service (Amazon SQS) queue. Deploy the models as AWS Lambda functions that are invoked by SQS events. Use AWS Auto Scaling to increase the number of vCPUs for the Lambda functions based on the SQS queue size.

D. Direct the requests from the API into an Amazon Simple Queue Service (Amazon SQS) queue. Deploy the models as Amazon Elastic Container Service (Amazon ECS) services that read from the queue. Enable AWS Auto Scaling on Amazon ECS for both the cluster and copies of the service based on the queue size.

Answer: D

Explanation: This answer is correct because it meets the requirements of running the ML models as independent microservices that can handle irregular and unpredictable usage patterns. By directing the requests from the API into an Amazon SQS queue, the company can decouple the request processing from the model execution, and ensure that no requests are lost due to spikes in demand. By deploying the models as Amazon ECS services that read from the queue, the company can leverage containers to isolate

and package each model as a microservice, and fetch the model data from S3 at startup. By enabling AWS Auto Scaling on Amazon ECS for both the cluster and copies of the service based on the queue size, the company can automatically scale up or down the number of EC2 instances in the cluster and the number of tasks in each service to match the demand and optimize performance.

References:

- https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGui de/welcome.html
- https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html
- https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-ecs.html

569. - (Topic 4)

A city has deployed a web application running on Amazon EC2 instances behind an Application Load Balancer (ALB). The application's users have reported sporadic performance, which appears to be related to DDoS attacks originating from random IP addresses. The city needs a solution that requires minimal configuration changes and provides an audit trail for the DDoS sources.

Which solution meets these requirements?

A. Enable an AWS WAF web ACL on the ALB, and configure rules to block traffic from unknown sources.

B. Subscribe to Amazon Inspector. Engage the AWS DDoS Response Team (DRT) to integrate mitigating controls into the service.

C. Subscribe to AWS Shield Advanced. Engage the AWS DDoS Response Team (DRT) to integrate mitigating controls into the service.

D. Create an Amazon CloudFront distribution for the application, and set the ALB as the origin. Enable an AWS WAF web ACL on the distribution, and configure rules to block traffic from unknown sources.

Answer: C

Explanation: To protect the web application from DDoS attacks originating from random IP addresses, a solutions architect should subscribe to AWS Shield Advanced and engage the AWS DDoS Response Team (DRT) to integrate mitigating controls into the service. AWS Shield Advanced is a managed service that provides protection against large and sophisticated DDoS attacks, with access to 24/7 support and response from the DRT. The DRT can help the city configure proactive and reactive safeguards, such as AWS WAF rules, rate-based rules, and network ACLs, to block malicious traffic and improve the application’s resilience. The service also provides an audit trail for the DDoS sources through detailed

attack reports and Amazon CloudWatch metrics.

570. - (Topic 4)

A company operates a two-tier application for image processing. The application uses two Availability Zones, each with one public subnet and one private subnet. An Application Load Balancer (ALB) for the web tier uses the public subnets. Amazon EC2 instances for the application tier use the private subnets. Users report that the application is running more slowly than expected. A security audit of the web server log files shows that the application is receiving millions of illegitimate requests from a small number of IP addresses. A solutions architect needs to resolve the immediate performance problem while the company investigates a more permanent solution.

What should the solutions architect recommend to meet this requirement?

A. Modify the inbound security group for the web tier. Add a deny rule for the IP addresses that are consuming resources.

B. Modify the network ACL for the web tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources

C. Modify the inbound security group for the application tier. Add a deny rule for the IP addresses that are consuming resources.

D. Modify the network ACL for the application tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources

Answer: B

Explanation: Deny the request from the first entry at the public subnet, dont allow it to cross and get to the private subnet.

In this scenario, the security audit reveals that the application is receiving millions of illegitimate requests from a small number of IP addresses. To address this issue, it is recommended to modify the network ACL (Access Control List) for the web tier subnets. By adding an inbound deny rule specifically targeting the IP addresses that are consuming resources, the network ACL can block the illegitimate traffic at the subnet level before it reaches the web servers. This will help alleviate the excessive load on the web tier and improve the application's performance.

571. - (Topic 4)

A company needs to create an AWS Lambda function that will run in a VPC in the company's primary AWS account. The Lambda function needs to access files that the company stores in an Amazon Elastic File System (Amazon EFS) file system. The EFS file system is located in a secondary AWS account. As the company adds files to the file system the solution must scale to meet the demand. Which solution will meet these requirements MOST cost-effectively?

A. Create a new EPS file system in the primary account Use AWS DataSync to copy the contents of the original EPS file system to the new EPS file system

B. Create a VPC peering connection between the VPCs that are in the primary account and the secondary account

C. Create a second Lambda function In the secondary account that has a mount that is configured for the file system. Use the primary account's Lambda function to invoke the secondary account's Lambda function

D. Move the contents of the file system to a Lambda Layer's Configure the Lambda layer's permissions to allow the company's secondary account to use the Lambda layer.

Answer: B

Explanation: This option is the most cost-effective and scalable way to allow the Lambda function in the primary account to access the EFS file system in the secondary account. VPC peering enables private connectivity between two VPCs without requiring gateways, VPN connections, or dedicated network connections. The Lambda function can use the VPC peering connection to mount the EFS file system as a local file system and access the files as needed. The solution does not incur additional data transfer or storage costs, and it leverages the existing EFS file system without duplicating or moving the data.

Option A is not cost-effective because it requires creating a new EFS file system and using AWS DataSync to copy the data from the original EFS file system. This would incur additional storage and data transfer costs, and it would not provide real-time access to the files.

Option C is not scalable because it requires creating a second Lambda function in the secondary account and configuring cross-account permissions to invoke it from the primary account. This would add complexity and latency to the solution, and it would increase the Lambda invocation costs.

Option D is not feasible because Lambda layers are not designed to store large amounts of data or provide file system access. Lambda layers are used to share common code or libraries across multiple Lambda functions. Moving the contents of the EFS file system to a Lambda layer would exceed the size limit of 250 MB for a layer, and it would not allow the Lambda function to read or write files to the layer. References:

- What Is VPC Peering?
- Using Amazon EFS file systems with AWS Lambda
- What Are Lambda Layers?

572. - (Topic 4)

A company stores multiple Amazon Machine Images (AMIs) in an AWS account to launch its Amazon EC2 instances. The AMIs contain critical data and configurations that are necessary for the company's operations. The company wants to implement a solution that will recover accidentally deleted AMIs quickly and efficiently.

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

A. Create Amazon Elastic Block Store (Amazon EBS) snapshots of the AMIs. Store the snapshots in a separate AWS account.

B. Copy all AMIs to another AWS account periodically.

C. Create a retention rule in Recycle Bin.

D. Upload the AMIs to an Amazon S3 bucket that has Cross-Region Replication.

Answer: C

Explanation: Recycle Bin is a data recovery feature that enables you to restore accidentally deleted Amazon EBS snapshots and EBS-backed AMIs. When using Recycle Bin, if your resources are deleted, they are retained in the Recycle Bin for a time period that you specify before being permanently deleted. You can restore a resource from the Recycle Bin at any time before its retention period expires. This solution has the least operational overhead, as you do not need to create, copy, or upload any additional resources. You can also manage tags and permissions for AMIs in the Recycle Bin. AMIs in the Recycle Bin do not incur any additional charges. References:

- Recover AMIs from the Recycle Bin
- Recover an accidentally deleted Linux AMI

573. - (Topic 4)

A company used an Amazon RDS for MySQL DB instance during application testing. Before terminating the DB instance at the end of the test cycle, a solutions architect created two backups. The solutions architect created the first backup by using the mysqldump utility to create a database dump. The solutions

architect created the second backup by enabling the final DB snapshot option on RDS termination.

The company is now planning for a new test cycle and wants to create a new DB instance from the most recent backup. The company has chosen a MySQL-compatible edition of Amazon Aurora to host the DB instance.

Which solutions will create the new DB instance? (Select TWO.)

A. Import the RDS snapshot directly into Aurora.

B. Upload the RDS snapshot to Amazon S3. Then import the RDS snapshot into Aurora.

C. Upload the database dump to Amazon S3. Then import the database dump into Aurora.

D. Use AWS Database Migration Service (AWS DMS) to import the RDS snapshot into Aurora.

E. Upload the database dump to Amazon S3. Then use AWS Database Migration Service (AWS DMS) to import the database dump into Aurora.

Answer: A,C

Explanation: These answers are correct because they meet the requirements of creating a new DB instance from the most recent backup and using a MySQL-compatible edition of Amazon Aurora to host the DB instance. You can import the RDS snapshot directly into Aurora if the MySQL DB instance and the Aurora DB cluster are running the same version of MySQL. For example, you can restore a MySQL version 5.6 snapshot directly to Aurora MySQL version 5.6, but you can't restore a MySQL version 5.6 snapshot directly to Aurora MySQL version 5.7. This method is simple and requires the fewest number of steps. You can upload the database dump to Amazon S3 and then import the database dump into Aurora if the MySQL DB instance and the Aurora DB cluster are running different versions of MySQL. For example, you can import a MySQL version 5.6 database dump into Aurora MySQL version 5.7, but you can't restore a MySQL version 5.6 snapshot directly to Aurora MySQL version 5.7. This method is more flexible and allows you to migrate across different versions of MySQL.

References:

- https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Migrating.RDSMySQL.Import.html
- https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Migrating.RDSMySQL.Dump.html

574. - (Topic 4)

A company is building an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for its workloads. All secrets that are stored in Amazon EKS must be encrypted in the Kubernetes etcd key-value store.

Which solution will meet these requirements?

A. Create a new AWS Key Management Service (AWS KMS) key Use AWS Secrets Manager to manage rotate, and store all secrets in Amazon EKS.

B. Create a new AWS Key Management Service (AWS KMS) key Enable Amazon EKS KMS secrets encryption on the Amazon EKS cluster.

C. Create the Amazon EKS cluster with default options Use the Amazon Elastic Block Store (Amazon EBS) Container Storage Interface (CSI) driver as an add-on.

D. Create a new AWS Key Management Service (AWS KMS) key with the ahas/aws/ebs alias Enable default Amazon Elastic Block Store (Amazon EBS) volume encryption for the account.

Answer: B

Explanation: This option is the most secure and simple way to encrypt the secrets that are stored in Amazon EKS. AWS Key Management Service (AWS KMS) is a service that allows you to create and manage encryption keys that can be used to encrypt your data. Amazon EKS KMS secrets encryption is a feature that enables you to use a KMS key to encrypt the secrets that are stored in the Kubernetes etcd key-value store. This provides an additional layer of protection for your sensitive data, such as passwords, tokens, and keys. You can create a new KMS key or use an existing one, and then enable the Amazon EKS KMS secrets encryption on the Amazon EKS cluster. You can also use IAM policies to control who can access or use the KMS key.

Option A is not correct because using AWS Secrets Manager to manage, rotate, and store all secrets in Amazon EKS is not necessary or efficient. AWS Secrets Manager is a service that helps you securely store, retrieve, and rotate your secrets, such as database credentials, API keys, and passwords. You can use it to manage secrets that are used by your applications or services outside of Amazon EKS, but it is not designed to encrypt the secrets that are stored in the Kubernetes etcd key-value store. Moreover, using AWS Secrets Manager would incur additional costs and complexity, and it would not leverage the native Kubernetes secrets management capabilities.

Option C is not correct because using the Amazon EBS Container Storage Interface (CSI) driver as an add-on does not encrypt the secrets that are stored in Amazon EKS. The Amazon EBS CSI driver is a plugin that allows you to use Amazon EBS volumes as persistent storage for your Kubernetes pods. It is

useful for providing durable and scalable storage for your applications, but it does not affect the encryption of the secrets that are stored in the Kubernetes etcd key-value store. Moreover, using the Amazon EBS CSI driver would require additional configuration and resources, and it would not provide the same level of security as using a KMS key.

Option D is not correct because creating a new AWS KMS key with the alias aws/ebs and enabling default Amazon EBS volume encryption for the account does not encrypt the secrets that are stored in Amazon EKS. The alias aws/ebs is a reserved alias that is used by AWS to create a default KMS key for your account. This key is used to encrypt the Amazon EBS volumes that are created in your account, unless you specify a different KMS key. Enabling default Amazon EBS volume encryption for the account is a setting that ensures that all new Amazon EBS volumes are encrypted by default. However, these features do not affect the encryption of the secrets that are stored in the Kubernetes etcd key-value store. Moreover, using the default KMS key or the default encryption setting would not provide the same level of control and security as using a custom KMS key and enabling the Amazon EKS KMS secrets encryption feature.

References:

- Encrypting secrets used in Amazon EKS
- What Is AWS Key Management Service?
- What Is AWS Secrets Manager?
- Amazon EBS CSI driver
- Encryption at rest

575. - (Topic 4)

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

Which method should the solutions architect select?

A. Configure Amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use the DAXendpoint.

B. Add DynamoDB read repticas to handle the increased read load. Update the application to point to the read endpoint for the read replicas.

C. Double the number of read capacity units for the new messages table in DynamoDB. Continue to use

the existing DynamoDB endpoint.

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

Answer: A

Explanation: https://aws.amazon.com/premiumsupport/knowledge-center/dynamodb-high- latency/

Amazon DynamoDB Accelerator (DAX) is a fully managed in-memory cache for DynamoDB that improves the performance of DynamoDB tables by up to 10 times and

provides microsecond level of response time at any scale. It is compatible with DynamoDB API operations and requires minimal code changes to use1. By configuring DAX for the

new messages table, the solution can reduce the latency for reading new messages with minimal application changes.

* B. Add DynamoDB read repticas to handle the increased read load. Update the application to point to the read endpoint for the read replicas. This solution will not work, as DynamoDB does not support read replicas as a feature. Read replicas are available for Amazon RDS, not for DynamoDB2.

* C. Double the number of read capacity units for the new messages table in DynamoDB. Continue to use the existing DynamoDB endpoint. This solution will not meet the requirement of reading new messages with as little latency as possible, as increasing the

read capacity units will only increase the throughput of DynamoDB, not the performance or latency3.

* D. Add an Amazon ElastiCache for Redis cache to the application stack. Update the application to point to the Redis cache endpoint instead of DynamoDB. This solution will not meet the requirement of minimal application changes, as adding ElastiCache for Redis will require significant code changes to implement caching logic, such as querying cache first, updating cache after writing to DynamoDB, and invalidating cache when needed. Reference URL: https://aws.amazon.com/dynamodb/dax/

576. - (Topic 4)

To meet security requirements, a company needs to encrypt all of its application data in transit while communicating with an Amazon RDS MySQL DB instance. A recent security audit revealed that encryption at rest is enabled using AWS Key Management Service (AWS KMS), but data in transit is not enabled.

What should a solutions architect do to satisfy the security requirements?

A. Enable 1AM database authentication on the database.

B. Provide self-signed certificates. Use the certificates in all connections to the RDS instance.

C. Take a snapshot of the RDS instance. Restore the snapshot to a new instance with encryption enabled.

D. Download AWS-provided root certificates. Provide the certificates in all connections to the RDS instance.

Answer: D

Explanation: To satisfy the security requirements, the solutions architect should download AWS-provided root certificates and provide the certificates in all connections to the RDS instance. This will enable SSL/TLS encryption for data in transit between the application and the RDS instance. SSL/TLS encryption provides a layer of security by encrypting data that moves between the client and the server. Amazon RDS creates an SSL certificate and installs the certificate on the DB instance when the instance is provisioned. The application can use the AWS-provided root certificates to verify the identity of the DB instance and establish a secure connection1.

The other options are not correct because they do not enable encryption for data in transit or are not relevant for the use case. Enabling IAM database authentication on the database is not correct because this option only provides a method of authentication, not encryption. IAM database authentication allows users to use AWS Identity and Access Management (IAM) users and roles to access a database, instead of using a database user name and password2. Providing self-signed certificates is not correct because this option is not secure or reliable. Self-signed certificates are certificates that are signed by the same entity that issued them, instead of by a trusted certificate authority (CA). Self-signed certificates can be easily forged or compromised, and are not recognized by most browsers and applications3. Taking a snapshot of the RDS instance and restoring it to a new instance with encryption enabled is not correct because this option only enables encryption at rest, not encryption in transit. Encryption at rest protects data that is stored on disk, but does not protect data that is moving between the client and the server4.

References:

- Using SSL/TLS to encrypt a connection to a DB instance - Amazon Relational Database Service
- IAM database authentication for MySQL and PostgreSQL - Amazon Relational Database Service
- What are self-signed certificates?
- Encrypting Amazon RDS resources - Amazon Relational Database Service

577. - (Topic 4)

A company runs an SMB file server in its data center. The file server stores large files that the company frequently accesses for up to 7 days after the file creation date. After 7 days, the company needs to be able to access the files with a maximum retrieval time of 24 hours.

Which solution will meet these requirements?

A. Use AWS DataSync to copy data that is older than 7 days from the SMB file server to AWS.

B. Create an Amazon S3 File Gateway to increase the company's storage space. Create an S3 Lifecycle policy to transition the data to S3 Glacier Deep Archive after 7 days.

C. Create an Amazon FSx File Gateway to increase the company's storage space. Create an Amazon S3 Lifecycle policy to transition the data after 7 days.

D. Configure access to Amazon S3 for each user. Create an S3 Lifecycle policy to transition the data to S3 Glacier Flexible Retrieval after 7 days.

Answer: B

Explanation:

Amazon S3 File Gateway is a service that provides a file-based interface to Amazon S3, which appears as a network file share. It enables you to store and retrieve Amazon S3 objects through standard file storage protocols such as SMB. S3 File Gateway can also cache frequently accessed data locally for low-latency access. S3 Lifecycle policy is a feature that allows you to define rules that automate the management of your objects throughout their lifecycle. You can use S3 Lifecycle policy to transition objects to different storage classes based on their age and access patterns. S3 Glacier Deep Archive is a storage class that offers the lowest cost for long-term data archiving, with a retrieval time of 12 hours or 48 hours. This solution will meet the requirements, as it allows the company to store large files in S3 with SMB file access, and to move the files to S3 Glacier Deep Archive after 7 days for cost savings and compliance.

References:

- 1 provides an overview of Amazon S3 File Gateway and its benefits.
- 2 explains how to use S3 Lifecycle policy to manage object storage lifecycle.
- 3 describes the features and use cases of S3 Glacier Deep Archive storage class.

578. - (Topic 4)

A company is deploying an application that processes large quantities of data in parallel. The company plans to use Amazon EC2 instances for the workload. The network architecture must be configurable to

prevent groups of nodes from sharing the same underlying hardware.

Which networking solution meets these requirements?

A. Run the EC2 instances in a spread placement group.

B. Group the EC2 instances in separate accounts.

C. Configure the EC2 instances with dedicated tenancy.

D. Configure the EC2 instances with shared tenancy.

Answer: A

Explanation: it allows the company to deploy an application that processes large quantities of data in parallel and prevent groups of nodes from sharing the same underlying hardware. By running the EC2 instances in a spread placement group, the company can launch a small number of instances across distinct underlying hardware to reduce correlated failures. A spread placement group ensures that each instance is isolated from each other at the rack level. References:

- Placement Groups
- Spread Placement Groups

579. - (Topic 4)

A company wants to migrate an on-premises legacy application to AWS. The application ingests customer order files from an on-premises enterprise resource planning (ERP) system. The application then uploads the files to an SFTP server. The application uses a scheduled job that checks for order files every hour. The company already has an AWS account that has connectivity to the on-premises network. The new application on AWS must support integration with the existing ERP system. The new application must be secure and resilient and must use the SFTP protocol to process orders from the ERP system immediately.

Which solution will meet these requirements?

A. Create an AWS Transfer Family SFTP internet-facing server in two Availability Zones. Use Amazon S3 storage. Create an AWS Lambda function to process order files. Use S3 Event Notifications to send s3: ObjectCreated: * events to the Lambda function.

B. Create an AWS Transfer Family SFTP internet-facing server in one Availability Zone. Use Amazon Elastic File System (Amazon EFS) storage. Create an AWS Lambda function to process order files. Use a Transfer Family managed workflow to invoke the Lambda function.

C. Create an AWS Transfer Family SFTP internal server in two Availability Zones. Use Amazon Elastic File

System (Amazon EFS) storage. Create an AWS Step Functions state machine to process order files. Use Amazon EventBridge Scheduler to invoke the state machine to periodically check Amazon EFS for order files.

D. Create an AWS Transfer Family SFTP internal server in two Availability Zones. Use Amazon S3 storage. Create an AWS Lambda function to process order files. Use a Transfer Family managed workflow to invoke the Lambda function.

Answer: D

Explanation: This solution meets the requirements because it uses the following components and features:

- AWS Transfer Family SFTP internal server: This allows the application to securely transfer order files from the on-premises ERP system to AWS using the SFTP protocol over a private connection. The internal server is deployed in two Availability Zones for high availability and fault tolerance.
- Amazon S3 storage: This provides scalable, durable, and cost-effective object storage for the order files. Amazon S3 also supports encryption at rest and in transit, as well as lifecycle policies and versioning for data protection and compliance.
- AWS Lambda function: This enables the application to process the order files in a serverless manner, without provisioning or managing servers. The Lambda function can perform any custom logic or transformation on the order files, such as validating, parsing, or enriching the data.
- Transfer Family managed workflow: This simplifies the orchestration of the file processing tasks by triggering the Lambda function as soon as a file is uploaded to the SFTP server. The managed workflow also provides error handling, retry policies, and logging capabilities.

580. - (Topic 4)

A company is reviewing a recent migration of a three-tier application to a VPC. The security team discovers that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.

What should a solutions architect do to correct this issue?

A. Create security group rules using the instance ID as the source or destination.

B. Create security group rules using the security group ID as the source or destination.

C. Create security group rules using the VPC CIDR blocks as the source or destination.

D. Create security group rules using the subnet CIDR blocks as the source or destination.

Answer: B

Explanation: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group- rules.html

581. - (Topic 4)

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

What should a solutions architect recommend?

A. Set up AWS Storage Gateway to connect with the backup applications using the NFS interface.

B. Set up an Amazon EFS file system that connects with the backup applications using the NFS interface.

C. Set up an Amazon EFS file system that connects with the backup applications using the iSCSI interface.

D. Set up AWS Storage Gateway to connect with the backup applications using the iSCSI- virtual tape library (VTL) interface.

Answer: D

Explanation: it allows the company to simplify the on-premises backup infrastructure and reduce costs by eliminating the use of physical backup tapes. By setting up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface, the company can store backup data on virtual tapes in S3 or Glacier. This preserves the existing investment in the on-premises backup applications and workflows while leveraging AWS storage services. References:

- AWS Storage Gateway
- Tape Gateway

582. - (Topic 4)

A company maintains about 300 TB in Amazon S3 Standard storage month after month The S3 objects are each typically around 50 GB in size and are frequently replaced with multipart uploads by their global application The number and size of S3 objects remain constant but the company's S3 storage costs are increasing each month.

How should a solutions architect reduce costs in this situation?

A. Switch from multipart uploads to Amazon S3 Transfer Acceleration.

B. Enable an S3 Lifecycle policy that deletes incomplete multipart uploads.

C. Configure S3 inventory to prevent objects from being archived too quickly.

D. Configure Amazon CloudFront to reduce the number of objects stored in Amazon S3.

Answer: B

Explanation: This option is the most cost-effective way to reduce the S3 storage costs in this situation. Incomplete multipart uploads are parts of objects that are not completed or aborted by the application. They consume storage space and incur charges until they are deleted. By enabling an S3 Lifecycle policy that deletes incomplete multipart uploads, you can automatically remove them after a specified period of time (such as one day) and free up the storage space. This will reduce the S3 storage costs and also improve the performance of the application by avoiding unnecessary retries or errors.

Option A is not correct because switching from multipart uploads to Amazon S3 Transfer Acceleration will not reduce the S3 storage costs. Amazon S3 Transfer Acceleration is a feature that enables faster data transfers to and from S3 by using the AWS edge network. It is useful for improving the upload speed of large objects over long distances, but it does not affect the storage space or charges. In fact, it may increase the costs by adding a data transfer fee for using the feature.

Option C is not correct because configuring S3 inventory to prevent objects from being archived too quickly will not reduce the S3 storage costs. Amazon S3 Inventory is a feature that provides a report of the objects and their metadata in an S3 bucket. It is useful for managing and auditing the S3 objects, but it does not affect the storage space or charges. In fact, it may increase the costs by generating additional S3 objects for the inventory reports.

Option D is not correct because configuring Amazon CloudFront to reduce the number of objects stored in Amazon S3 will not reduce the S3 storage costs. Amazon CloudFront is a content delivery network (CDN) that distributes the S3 objects to edge locations for faster and lower latency access. It is useful for improving the download speed and availability of the S3 objects, but it does not affect the storage space or charges. In fact, it may increase the costs by adding a data transfer fee for using the service. References:

- Managing your storage lifecycle
- Using multipart upload
- Amazon S3 Transfer Acceleration
- Amazon S3 Inventory
- What Is Amazon CloudFront?

583. - (Topic 4)

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

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

A. Enable a read-only bucket ACL.

B. Enable versioning on the bucket.

C. Attach an IAM policy to the bucket.

D. Enable MFA Delete on the bucket.

E. Encrypt the bucket using AWS KMS.

Answer: B,D

Explanation: Versioning is a feature of Amazon S3 that allows users to keep multiple versions of the same object in a bucket. It can help prevent accidental deletion of the documents and ensure that all versions of the documents are available1. MFA Delete is a feature of Amazon S3 that adds an extra layer of security by requiring two forms of authentication to delete a version or change the versioning state of a bucket. It can help prevent unauthorized or accidental deletion of the documents2. By enabling both versioning and MFA Delete on the bucket, the solution can meet the requirements.

* A. Enable a read-only bucket ACL. This solution will not meet the requirement of allowing users to download, modify, and upload documents, as a read-only bucket ACL will prevent write access to the bucket3.

* C. Attach an IAM policy to the bucket. This solution will not meet the requirement of preventing accidental deletion of the documents and ensuring that all versions of the documents are available, as an IAM policy is used to grant or deny permissions to users or roles, not to enable versioning or MFA Delete4.

* E. Encrypt the bucket using AWS KMS. This solution will not meet the requirement of preventing accidental deletion of the documents and ensuring that all versions of the documents are available, as encrypting the bucket using AWS KMS is a method of protecting data at rest, not enabling versioning or MFA Delete.

Reference URL: https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html

584. - (Topic 4)

A company wants to migrate its three-tier application from on premises to AWS. The web tier and the application tier are running on third-party virtual machines (VMs). The database tier is running on MySQL. The company needs to migrate the application by making the fewest possible changes to the architecture. The company also needs a database solution that can restore data to a specific point in time.

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

A. Migrate the web tier and the application tier to Amazon EC2 instances in private subnets. Migrate the database tier to Amazon RDS for MySQL in private subnets.

B. Migrate the web tier to Amazon EC2 instances in public subnets. Migrate the application tier to EC2 instances in private subnets. Migrate the database tier to Amazon Aurora MySQL in private subnets.

C. Migrate the web tier to Amazon EC2 instances in public subnets. Migrate the application tier to EC2 instances in private subnets. Migrate the database tier to Amazon RDS for MySQL in private subnets.

D. Migrate the web tier and the application tier to Amazon EC2 instances in public subnets. Migrate the database tier to Amazon Aurora MySQL in public subnets.

Answer: C

Explanation: The solution that meets the requirements with the least operational overhead is to migrate the web tier to Amazon EC2 instances in public subnets, migrate the application tier to EC2 instances in private subnets, and migrate the database tier to Amazon RDS for MySQL in private subnets. This solution allows the company to migrate its three-tier application to AWS by making minimal changes to the architecture, as it preserves the same web, application, and database tiers and uses the same MySQL database engine. The solution also provides a database solution that can restore data to a specific point in time, as Amazon RDS for MySQL supports automated backups and point- in-time recovery. This solution also reduces the operational overhead by using managed services such as Amazon EC2 and Amazon RDS, which handle tasks such as provisioning, patching, scaling, and monitoring.

The other solutions do not meet the requirements as well as the first one because they either involve more changes to the architecture, do not provide point-in-time recovery, or do not follow best practices for security and availability. Migrating the database tier to Amazon Aurora MySQL would require changing the database engine and potentially modifying the application code to ensure compatibility. Migrating the web tier and the application tier to public subnets would expose them to more security risks and reduce their availability in case of a subnet failure. Migrating the database tier to public subnets would also compromise

its security and performance. References:

- Migrate Your Application Database to Amazon RDS
- Amazon RDS for MySQL
- Amazon Aurora MySQL
- Amazon VPC

585. - (Topic 4)

A company uses Amazon EC2 instances to host its internal systems. As part of a deployment operation, an administrator tries to use the AWS CLI to terminate an EC2 instance. However, the administrator receives a 403 (Access Denied) error message.

The administrator is using an IAM role that has the following IAM policy attached:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["ec2:TerminateInstances"],
            "Resource": ["*"]
        },
        {
            "Effect": "Deny",
            "Action": ["ec2:TerminateInstances"],
            "Condition": {
                "NotIpAddress": {
                    "aws:SourceIp": [
                        "192.0.2.0/24",
                        "203.0.113.0/24"
                    ]
                }
            },
            "Resource": ["*"]
        }
    ]
}
```

What is the cause of the unsuccessful request?

A. The EC2 instance has a resource-based policy with a Deny statement.

B. The principal has not been specified in the policy statement

C. The "Action" field does not grant the actions that are required to terminate the EC2 instance.

D. The request to terminate the EC2 instance does not originate from the CIDR blocks 192.0.2.0/24 or

203.0 113.0/24

Answer: D

586. - (Topic 4)

A company is implementing new data retention policies for all databases that run on Amazon RDS DB instances. The company must retain daily backups for a minimum period of 2 years. The backups must be consistent and restorable.

Which solution should a solutions architect recommend to meet these requirements?

A. Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan.

B. Configure a backup window for the RDS DB instances for daily snapshots. Assign a snapshot retention policy of 2 years to each RDS DB instance. Use Amazon Data Lifecycle Manager (Amazon DLM) to schedule snapshot deletions.

C. Configure database transaction logs to be automatically backed up to Amazon CloudWatch Logs with an expiration period of 2 years.

D. Configure an AWS Database Migration Service (AWS DMS) replication task. Deploy a replication instance, and configure a change data capture (CDC) task to stream database changes to Amazon S3 as the target. Configure S3 Lifecycle policies to delete the snapshots after 2 years.

Answer: A

Explanation:

AWS Backup is a fully managed service that enables users to centralize and automate the backup of data across AWS services. It can create and manage backup plans that specify the frequency and retention period of backups. It can also assign backup resources to backup vaults, which are containers that store backup data1. By using AWS Backup, the solution can ensure that the RDS backups are consistent, restorable, and retained for a minimum period of 2 years.

* B. Configure a backup window for the RDS DB instances for daily snapshots. Assign a snapshot retention policy of 2 years to each RDS DB instance. Use Amazon Data Lifecycle Manager (Amazon DLM) to schedule snapshot deletions. This solution will not meet the requirement of ensuring that the backups are consistent and restorable, as Amazon DLM is not compatible with RDS snapshots and cannot be used to

schedule snapshot deletions2.

* C. Configure database transaction logs to be automatically backed up to Amazon CloudWatch Logs with an expiration period of 2 years. This solution will not meet the requirement of ensuring that the backups are consistent and restorable, as database transaction logs are not sufficient to restore a database to a point in time. They only capture the changes made to the database, not the full state of the database3.

* D. Configure an AWS Database Migration Service (AWS DMS) replication task. Deploy a replication instance, and configure a change data capture (CDC) task to stream database changes to Amazon S3 as the target. Configure S3 Lifecycle policies to delete the snapshots after 2 years. This solution will not meet the requirement of ensuring that the backups are consistent and restorable, as AWS DMS is a service that helps users migrate databases to AWS, not back up databases. It also requires additional resources and configuration, such as replication instances and CDC tasks.

Reference URL: https://docs.aws.amazon.com/aws- backup/latest/devguide/whatisbackup.html

587. - (Topic 4)

A company is using an Application Load Balancer (ALB) to present its application to the internet. The company finds abnormal traffic access patterns across the application. A solutions architect needs to improve visibility into the infrastructure to help the company understand these abnormalities better.

What is the MOST operationally efficient solution that meets these requirements?

A. Create a table in Amazon Athena for AWS CloudTrail logs. Create a query for the relevant information.

B. Enable ALB access logging to Amazon S3. Create a table in Amazon Athena, and query the logs.

C. Enable ALB access logging to Amazon S3 Open each file in a text editor, and search each line for the relevant information

D. Use Amazon EMR on a dedicated Amazon EC2 instance to directly query the ALB to acquire traffic access log information.

Answer: B

Explanation: This solution meets the requirements because it allows the company to improve visibility into the infrastructure by using ALB access logging and Amazon Athena. ALB access logging is a feature that captures detailed information about requests sent to the load balancer, such as the client's IP address, request path, response code, and latency. By enabling ALB access logging to Amazon S3, the company can store the access logs in an S3 bucket as compressed files. Amazon Athena is an interactive query

service that makes it easy to analyze data in Amazon S3 using standard SQL. By creating a table in Amazon Athena for the access logs, the company can query the logs and get results in seconds. This way, the company can better understand the abnormal traffic access patterns across the application.

References:

- Access logs for your Application Load Balancer
- Querying Application Load Balancer Logs

588. - (Topic 4)

A company runs a highly available SFTP service. The SFTP service uses two Amazon EC2 Linux instances that run with elastic IP addresses to accept traffic from trusted IP sources on the internet. The SFTP service is backed by shared storage that is attached to the instances. User accounts are created and managed as Linux users in the SFTP servers.

The company wants a serverless option that provides high IOPS performance and highly configurable security. The company also wants to maintain control over user permissions.

Which solution will meet these requirements?

A. Create an encrypted Amazon Elastic Block Store (Amazon EBS) volume. Create an AWS Transfer Family SFTP service with a public endpoint that allows only trusted IP addresses. Attach the EBS volume to the SFTP service endpoint. Grant users access to the SFTP service.

B. Create an encrypted Amazon Elastic File System (Amazon EFS) volume. Create an AWS Transfer Family SFTP service with elastic IP addresses and a VPC endpoint that has internet-facing access. Attach a security group to the endpoint that allows only trusted IP addresses. Attach the EFS volume to the SFTP service endpoint. Grant users access to the SFTP service.

C. Create an Amazon S3 bucket with default encryption enabled. Create an AWS Transfer Family SFTP service with a public endpoint that allows only trusted IP addresses. Attach the S3 bucket to the SFTP service endpoint. Grant users access to the SFTP service.

D. Create an Amazon S3 bucket with default encryption enabled. Create an AWS Transfer Family SFTP service with a VPC endpoint that has internal access in a private subnet. Attach a security group that allows only trusted IP addresses. Attach the S3 bucket to the SFTP service endpoint. Grant users access to the SFTP service.

Answer: C

Explanation:

AWS Transfer Family is a secure transfer service that enables you to transfer files into and out of AWS storage services using SFTP, FTPS, FTP, and AS2 protocols. You can use AWS Transfer Family to create an SFTP-enabled server with a public endpoint that allows only trusted IP addresses. You can also attach an Amazon S3 bucket with default encryption enabled to the SFTP service endpoint, which will provide high IOPS performance and highly configurable security for your data at rest. You can also maintain control over user permissions by granting users access to the SFTP service using IAM roles or service-managed identities. References:

https://docs.aws.amazon.com/transfer/latest/userguide/what-is-aws-transfer-family.html

https://docs.aws.amazon.com/transfer/latest/userguide/create-server-s3.html

589. - (Topic 4)

An online video game company must maintain ultra-low latency for its game servers. The game servers run on Amazon EC2 instances. The company needs a solution that can

handle millions of UDP internet traffic requests each second.

Which solution will meet these requirements MOST cost-effectively?

A. Configure an Application Load Balancer with the required protocol and ports for the internet traffic. Specify the EC2 instances as the targets.

B. Configure a Gateway Load Balancer for the internet traffic. Specify the EC2 instances as the targets.

C. Configure a Network Load Balancer with the required protocol and ports for the internet traffic. Specify the EC2 instances as the targets.

D. Launch an identical set of game servers on EC2 instances in separate AWS Regions. Route internet traffic to both sets of EC2 instances.

Answer: C

Explanation: The most cost-effective solution for the online video game company is to configure a Network Load Balancer with the required protocol and ports for the internet traffic and specify the EC2 instances as the targets. This solution will enable the company to handle millions of UDP requests per second with ultra-low latency and high performance. A Network Load Balancer is a type of Elastic Load Balancing that operates at the connection level (Layer 4) and routes traffic to targets (EC2 instances, microservices, or containers) within Amazon VPC based on IP protocol data. A Network Load Balancer is ideal for load

balancing of both TCP and UDP traffic, as it is capable of handling millions of requests per second while maintaining high throughput at ultra-low latency. A Network Load Balancer also preserves the source IP address of the clients to the back-end applications, which can be useful for logging or security purposes1.

590. - (Topic 4)

A company wants to move from many standalone AWS accounts to a consolidated, multi- account architecture The company plans to create many new AWS accounts for different business units. The company needs to authenticate access to these AWS accounts by using a centralized corporate directory service.

Which combination of actions should a solutions architect recommend to meet these requirements? (Select TWO.)

A. Create a new organization in AWS Organizations with all features turned on. Create the new AWS accounts in the organization.

B. Set up an Amazon Cognito identity pool. Configure AWS 1AM Identity Center (AWS Single Sign-On) to accept Amazon Cognito authentication.

C. Configure a service control policy (SCP) to manage the AWS accounts. Add AWS 1AM Identity Center (AWS Single Sign-On) to AWS Directory Service.

D. Create a new organization in AWS Organizations. Configure the organization's authentication mechanism to use AWS Directory Service directly.

E. Set up AWS 1AM Identity Center (AWS Single Sign-On) in the organization. Configure 1AM Identity Center, and integrate it with the company's corporate directory service.

Answer: A,E

Explanation: AWS Organizations is a service that helps users centrally manage and govern multiple AWS accounts. It allows users to create organizational units (OUs) to group accounts based on business needs or other criteria. It also allows users to define and attach service control policies (SCPs) to OUs or accounts to restrict the actions that can be performed by the accounts1. By creating a new organization in AWS Organizations with all features turned on, the solution can consolidate and manage the new AWS accounts for different business units.

AWS IAM Identity Center (formerly known as AWS Single Sign-On) is a service that provides single sign-on access for all of your AWS accounts and cloud applications. It connects with Microsoft Active Directory

through AWS Directory Service to allow users in that directory to sign in to a personalized AWS access portal using their existing Active Directory user names and passwords. From the AWS access portal, users have access to all the AWS accounts and cloud applications that they have permissions for2. By setting up IAM Identity Center in the organization and integrating it with the company's corporate directory service, the solution can authenticate access to these AWS accounts using a centralized corporate directory service.

* B. Set up an Amazon Cognito identity pool. Configure AWS 1AM Identity Center (AWS Single Sign-On) to accept Amazon Cognito authentication. This solution will not meet the requirement of authenticating access to these AWS accounts by using a centralized corporate directory service, as Amazon Cognito is a service that provides user sign-up, sign-in, and access control for web and mobile applications, not for corporate directory services3.

* C. Configure a service control policy (SCP) to manage the AWS accounts. Add AWS 1AM Identi-ty Center (AWS Single Sign-On) to AWS Directory Service. This solution will not work, as SCPs are used to restrict the actions that can be performed by the accounts in an organization, not to manage the accounts themselves1. Also, IAM Identity Center cannot be added to AWS Directory Service, as it is a separate service that connects with Microsoft Active Directory through AWS Directory Service2.

* D. Create a new organization in AWS Organizations. Configure the organization's authentication mechanism to use AWS Directory Service directly. This solution will not work, as AWS Organizations does not have an authentication mechanism that can use AWS Directory Service directly. AWS Organizations relies on IAM Identity Center to provide single sign-on access for the accounts in an organization.

Reference URL:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_integrate_services.html

591. - (Topic 4)

A manufacturing company runs its report generation application on AWS. The application generates each report in about 20 minutes. The application is built as a monolith that runs on a single Amazon EC2 instance. The application requires frequent updates to its tightly coupled modules. The application becomes complex to maintain as the company adds new features.

Each time the company patches a software module, the application experiences downtime. Report generation must restart from the beginning after any interruptions. The company wants to redesign the application so that the application can be flexible, scalable, and gradually improved. The company wants to

minimize application downtime.

Which solution will meet these requirements?

A. Run the application on AWS Lambda as a single function with maximum provisioned concurrency.

B. Run the application on Amazon EC2 Spot Instances as microservices with a Spot Fleet default allocation strategy.

C. Run the application on Amazon Elastic Container Service (Amazon ECS) as microservices with service auto scaling.

D. Run the application on AWS Elastic Beanstalk as a single application environment with an all-at-once deployment strategy.

Answer: C

Explanation: The solution that will meet the requirements is to run the application on Amazon Elastic Container Service (Amazon ECS) as microservices with service auto scaling. This solution will allow the application to be flexible, scalable, and gradually improved, as well as minimize application downtime. By breaking down the monolithic application into microservices, the company can decouple the modules and update them independently, without affecting the whole application. By running the microservices on Amazon ECS, the company can leverage the benefits of containerization, such as portability, efficiency, and isolation. By enabling service auto scaling, the company can adjust the number of containers running for each microservice based on demand, ensuring optimal performance and cost. Amazon ECS also supports various deployment strategies, such as rolling update or blue/green deployment, that can reduce or eliminate downtime during updates.

The other solutions are not as effective as the first one because they either do not meet the requirements or introduce new challenges. Running the application on AWS Lambda as a single function with maximum provisioned concurrency will not meet the requirements, as it will not break down the monolith into microservices, nor will it reduce the complexity of maintenance. Lambda functions are also limited by execution time (15 minutes), memory size (10 GB), and concurrency quotas, which may not be sufficient for the report generation application. Running the application on Amazon EC2 Spot Instances as microservices with a Spot Fleet default allocation strategy will not meet the requirements, as it will introduce the risk of interruptions due to spot price fluctuations. Spot Instances are not guaranteed to be available or stable, and may be reclaimed by AWS at any time with a two-minute warning. This may cause report generation to fail or restart from scratch. Running the application on AWS Elastic Beanstalk as a single application

environment with an all-at- once deployment strategy will not meet the requirements, as it will not break down the monolith into microservices, nor will it minimize application downtime. The all-at-once deployment strategy will deploy updates to all instances simultaneously, causing a brief outage for the application.

References:

- Amazon Elastic Container Service
- Microservices on AWS
- Service Auto Scaling - Amazon Elastic Container Service
- AWS Lambda
- Amazon EC2 Spot Instances
- [AWS Elastic Beanstalk]

592. - (Topic 4)

A company has an on-premises server that uses an Oracle database to process and store customer information The company wants to use an AWS database service to achieve higher availability and to improve application performance. The company also wants to offload reporting from its primary database system.

Which solution will meet these requirements in the MOST operationally efficient way?

A. Use AWS Database Migration Service (AWS DMS) to create an Amazon RDS DB instance in multiple AWS Regions Point the reporting functions toward a separate DB instance from the primary DB instance.

B. Use Amazon RDS in a Single-AZ deployment to create an Oracle database Create a read replica in the same zone as the primary DB instance. Direct the reporting functions to the read replica.

C. Use Amazon RDS deployed in a Multi-AZ cluster deployment to create an Oracle database Direct the reporting functions to use the reader instance in the cluster deployment

D. Use Amazon RDS deployed in a Multi-AZ instance deployment to create an Amazon Aurora database. Direct the reporting functions to the reader instances.

Answer: D

Explanation: Amazon Aurora is a fully managed relational database that is compatible with MySQL and PostgreSQL. It provides up to five times better performance than MySQL and

up to three times better performance than PostgreSQL. It also provides high availability and durability by replicating data across multiple Availability Zones and continuously backing up data to Amazon S31. By

using Amazon RDS deployed in a Multi-AZ instance deployment

to create an Amazon Aurora database, the solution can achieve higher availability and improve application performance.

Amazon Aurora supports read replicas, which are separate instances that share the same underlying storage as the primary instance. Read replicas can be used to offload read-only queries from the primary instance and improve performance. Read replicas can also be used for reporting functions2. By directing the reporting functions to the reader instances, the solution can offload reporting from its primary database system.

* A. Use AWS Database Migration Service (AWS DMS) to create an Amazon RDS DB instance in multiple AWS Regions Point the reporting functions toward a separate DB instance from the pri-mary DB instance. This solution will not meet the requirement of using an AWS database service, as AWS DMS is a service that helps users migrate databases to AWS, not a database service itself. It also involves creating multiple DB instances in different Regions, which may increase complexity and cost.

* B. Use Amazon RDS in a Single-AZ deployment to create an Oracle database Create a read replica in the same zone as the primary DB instance. Direct the reporting functions to the read replica. This solution will not meet the requirement of achieving higher availability, as a Single-AZ deployment does not provide failover protection in case of an Availability Zone outage. It also involves using Oracle as the database engine, which may not provide better performance than Aurora.

* C. Use Amazon RDS deployed in a Multi-AZ cluster deployment to create an Oracle database Di-rect the reporting functions to use the reader instance in the cluster deployment. This solution will not meet the requirement of improving application performance, as Oracle may not provide better performance than Aurora. It also involves using a cluster deployment, which is only supported for Aurora, not for Oracle.

Reference URL: https://aws.amazon.com/rds/aurora/

593. - (Topic 4)

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

What should be done to secure the root user?

A. Create 1AM users for daily administrative tasks. Disable the root user.

B. Create 1AM users for daily administrative tasks. Enable multi-factor authentication on the root user.

C. Generate an access key for the root user Use the access key for daily administration tasks instead of the AWS Management Console.

D. Provide the root user credentials to the most senior solutions architect. Have the solutions architect use the root user for daily administration tasks.

Answer: B

Explanation: This answer is the most secure and recommended option for securing the root user of a new AWS account. The root user is the identity that has complete access to all AWS services and resources in the account. It is accessed by signing in with the email address and password that were used to create the account. To protect the root user credentials from unauthorized use, AWS advises the following best practices:

- Create IAM users for daily administrative tasks. IAM users are identities that you create in your account that have specific permissions to access AWS resources. You can create individual IAM users for yourself and for others who need access to your account. You can also assign IAM users to IAM groups that have a set of policies that grant permissions to perform common tasks. By using IAM users instead of the root user, you can follow the principle of least privilege and reduce the risk of compromising your account.
- Enable multi-factor authentication (MFA) on the root user. MFA is a security feature that requires users to prove their identity by providing two pieces of information: their password and a code from a device that only they have access to. By enabling MFA on the root user, you can add an extra layer of protection to your account and prevent unauthorized access even if your password is compromised.
- Limit the tasks you perform with the root user account. You should use the root user only for tasks that require root user credentials, such as changing your account settings, closing your account, or managing consolidated billing. For a complete list of tasks that require root user credentials, see Tasks that require root user credentials. For all other tasks, you should use IAM users or roles that have the appropriate permissions.

References:

- AWS account root user
- Root user best practices for your AWS account

⇨ Tasks that require root user credentials

594. - (Topic 4)

A company is designing a new web service that will run on Amazon EC2 instances behind an Elastic Load Balancing (ELB) load balancer. However, many of the web service clients can only reach IP addresses authorized on their firewalls.

What should a solutions architect recommend to meet the clients' needs?

A. A Network Load Balancer with an associated Elastic IP address.

B. An Application Load Balancer with an associated Elastic IP address.

C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address.

D. An EC2 instance with a public IP address running as a proxy in front of the load balancer.

Answer: A

Explanation: A Network Load Balancer can be assigned one Elastic IP address for each Availability Zone it uses1. This allows the clients to reach the load balancer using a static IP address that can be authorized on their firewalls. An Application Load Balancer cannot be assigned an Elastic IP address2. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address would not work because the load balancer would still use its own IP address as the source of the forwarded requests to the web service. An EC2 instance with a public IP address running as a proxy in front of the load balancer would add unnecessary complexity and cost, and would not provide the same scalability and availability as a Network Load Balancer. References: 1: Network Load Balancers - Elastic Load Balancing3, IP address type section2: How to assign Elastic IP to Application Load Balancer in AWS?4, answer section.

595. - (Topic 4)

A company offers a food delivery service that is growing rapidly. Because of the growth, the company's order processing system is experiencing scaling problems during peak traffic hours. The current architecture includes the following:

• A group of Amazon EC2 instances that run in an Amazon EC2 Auto Scaling group to collect orders from the application

• Another group of EC2 instances that run in an Amazon EC2 Auto Scaling group to fulfill orders

The order collection process occurs quickly, but the order fulfillment process can take longer. Data must not

be lost because of a scaling event.

A solutions architect must ensure that the order collection process and the order fulfillment process can both scale properly during peak traffic hours. The solution must optimize utilization of the company's AWS resources. Which solution meets these requirements?

A. Use Amazon CloudWatch metrics to monitor the CPU of each instance in the Auto Scaling groups. Configure each Auto Scaling group's minimum capacity according to peak workload values.

B. Use Amazon CloudWatch metrics to monitor the CPU of each instance in the Auto Scaling groups. Configure a CloudWatch alarm to invoke an Amazon Simple Notification Service (Amazon SNS) topic that creates additional Auto Scaling groups on demand.

C. Provision two Amazon Simple Queue Service (Amazon SQS) queues: one for order collection and another for order fulfillment. Configure the EC2 instances to poll their respective queue. Scale the Auto Scaling groups based on notifications that the queues send.

D. Provision two Amazon Simple Queue Service (Amazon SQS) queues: one for order collection and another for order fulfillment. Configure the EC2 instances to poll their respective queue. Create a metric based on a backlog per instance calculation. Scale the Auto Scaling groups based on this metric.

Answer: D

Explanation: The number of instances in your Auto Scaling group can be driven by how long it takes to process a message and the acceptable amount of latency (queue delay). The solution is to use a backlog per instance metric with the target value being the acceptable backlog per instance to maintain.

596. - (Topic 4)

A company runs an application on AWS. The application receives inconsistent amounts of usage. The application uses AWS Direct Connect to connect to an on-premises MySQL- compatible database. The on-premises database consistently uses a minimum of 2 GiB of memory.

The company wants to migrate the on-premises database to a managed AWS service. The company wants to use auto scaling capabilities to manage unexpected workload increases.

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

A. Provision an Amazon DynamoDB database with default read and write capacity settings.

B. Provision an Amazon Aurora database with a minimum capacity of 1 Aurora capacity unit (ACU).

C. Provision an Amazon Aurora Serverless v2 database with a minimum capacity of 1 Aurora capacity unit (ACU).

D. Provision an Amazon RDS for MySQL database with 2 GiB of memory.

Answer: C

Explanation: it allows the company to migrate the on-premises database to a managed AWS service that supports auto scaling capabilities and has the least administrative overhead. Amazon Aurora Serverless v2 is a configuration of Amazon Aurora that automatically scales compute capacity based on workload demand. It can scale from hundreds to hundreds of thousands of transactions in a fraction of a second. Amazon Aurora Serverless v2 also supports MySQL-compatible databases and AWS Direct Connect connectivity. References:

- Amazon Aurora Serverless v2
- Connecting to an Amazon Aurora DB Cluster

597. - (Topic 4)

A company is deploying a new application to Amazon Elastic Kubernetes Service (Amazon EKS) with an AWS Fargate cluster. The application needs a storage solution for data persistence. The solution must be highly available and fault tolerant. The solution also must be shared between multiple application containers.

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

A. Create Amazon Elastic Block Store (Amazon EBS) volumes in the same Availability Zones where EKS worker nodes are placed. Register the volumes in a StorageClass object on an EKS cluster. Use EBS Multi-Attach to share the data between containers.

B. Create an Amazon Elastic File System (Amazon EFS) file system. Register the file system in a StorageClass object on an EKS cluster. Use the same file system for all containers.

C. Create an Amazon Elastic Block Store (Amazon EBS) volume. Register the volume in a StorageClass object on an EKS cluster. Use the same volume for all containers.

D. Create Amazon Elastic File System (Amazon EFS) file systems in the same Availability Zones where EKS worker nodes are placed. Register the file systems in a StorageClass object on an EKS cluster. Create an AWS Lambda function to synchronize the data between file systems.

Answer: B

Explanation: Amazon EFS is a fully managed, elastic, and scalable file system that can be shared between multiple containers. It provides high availability and fault tolerance by replicating data across multiple Availability Zones. Amazon EFS is compatible with Amazon EKS and AWS Fargate, and can be registered in a StorageClass object on an EKS cluster. Amazon EBS volumes are not supported by AWS Fargate, and cannot be shared between multiple containers without using EBS Multi-Attach, which has limitations and performance implications. EBS Multi-Attach also requires the volumes to be in the same Availability Zone as the worker nodes, which reduces availability and fault tolerance. Synchronizing data between multiple EFS file systems using AWS Lambda is unnecessary, complex, and prone to errors. References:

- Amazon EFS Storage Classes
- Amazon EKS Storage Classes
- Amazon EBS Multi-Attach

598. - (Topic 4)

A company has an organization in AWS Organizations that has all features enabled The company requires that all API calls and logins in any existing or new AWS account must be audited The company needs a managed solution to prevent additional work and to minimize costs The company also needs to know when any AWS account is not compliant with the AWS Foundational Security Best Practices (FSBP) standard. Which solution will meet these requirements with the LEAST operational overhead?

A. Deploy an AWS Control Tower environment in the Organizations management account Enable AWS Security Hub and AWS Control Tower Account Factory in the environment.

B. Deploy an AWS Control Tower environment in a dedicated Organizations member account Enable AWS Security Hub and AWS Control Tower Account Factory in the environment.

C. Use AWS Managed Services (AMS) Accelerate to build a multi-account landing zone (MALZ) Submit an RFC to self-service provision Amazon GuardDuty in the MALZ.

D. Use AWS Managed Services (AMS) Accelerate to build a multi-account landing zone (MALZ) Submit an RFC to self-service provision AWS Security Hub in the MALZ.

Answer: A

Explanation: AWS Control Tower is a fully managed service that simplifies the setup and governance of a secure, compliant, multi-account AWS environment. It establishes a landing zone that is based on

best-practices blueprints, and it enables governance using controls you can choose from a pre-packaged list. The landing zone is a well-architected, multi-account baseline that follows AWS best practices. Controls implement governance rules for security, compliance, and operations. AWS Security Hub is a service that provides a comprehensive view of your security posture across your AWS accounts. It aggregates, organizes, and prioritizes security alerts and findings from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS Firewall Manager, and AWS IAM Access Analyzer, as well as from AWS Partner solutions. AWS Security Hub continuously monitors your environment using automated compliance checks based on the AWS best practices and industry standards, such as the AWS Foundational Security Best Practices (FSBP) standard. AWS Control Tower Account Factory is a feature that automates the provisioning of new AWS accounts that are preconfigured to meet your business, security, and compliance requirements. By deploying an AWS Control Tower environment in the Organizations management account, you can leverage the existing organization structure and policies, and enable AWS Security Hub and AWS Control Tower Account Factory in the environment. This way, you can audit all API calls and logins in any existing or new AWS account, monitor the compliance status of each account with the FSBP standard, and provision new accounts with ease and consistency. This solution meets the requirements with the least operational overhead, as you do not need to manage any infrastructure, perform any data migration, or submit any requests for changes. References:

- AWS Control Tower
- [AWS Security Hub]
- [AWS Control Tower Account Factory]

599. - (Topic 4)

A company needs to use its on-premises LDAP directory service to authenticate its users to the AWS Management Console. The directory service is not compatible with Security Assertion Markup Language (SAML).

Which solution meets these requirements?

A. Enable AWS 1AM Identity Center (AWS Single Sign-On) between AWS and the on- premises LDAP.

B. Create an 1AM policy that uses AWS credentials, and integrate the policy into LDAP.

C. Set up a process that rotates the I AM credentials whenever LDAP credentials are updated.

D. Develop an on-premises custom identity broker application or process that uses AWS Security Token

Service (AWS STS) to get short-lived credentials.

Answer: D

Explanation: The solution that meets the requirements is to develop an on-premises custom identity broker application or process that uses AWS Security Token Service (AWS STS) to get short-lived credentials. This solution allows the company to use its existing LDAP directory service to authenticate its users to the AWS Management Console, without requiring SAML compatibility. The custom identity broker application or process can act as a proxy between the LDAP directory service and AWS STS, and can request temporary security credentials for the users based on their LDAP attributes and roles. The users can then use these credentials to access the AWS Management Console via a sign-in URL generated by the identity broker. This solution also enhances security by using short-lived credentials that expire after a specified duration.

The other solutions do not meet the requirements because they either require SAML compatibility or do not provide access to the AWS Management Console. Enabling AWS IAM Identity Center (AWS Single Sign-On) between AWS and the on-premises LDAP would require the LDAP directory service to support SAML 2.0, which is not the case for this scenario. Creating an IAM policy that uses AWS credentials and integrating the policy into LDAP would not provide access to the AWS Management Console, but only to the AWS APIs. Setting up a process that rotates the IAM credentials whenever LDAP credentials are updated would also not provide access to the AWS Management Console, but only to the AWS CLI. Therefore, these solutions are not suitable for the given requirements.

600. - (Topic 4)

A company maintains an Amazon RDS database that maps users to cost centers. The company has accounts in an organization in AWS Organizations. The company needs a solution that will tag all resources that are created in a specific AWS account in the organization. The solution must tag each resource with the cost center ID of the user who created the resource.

Which solution will meet these requirements?

A. Move the specific AWS account to a new organizational unit (OU) in Organizations from the management account. Create a service control policy (SCP) that requires all existing resources to have the correct cost center tag before the resources are created. Apply the SCP to the new OU.

B. Create an AWS Lambda function to tag the resources after the Lambda function looks up the appropriate

cost center from the RDS database. Configure an Amazon EventBridge rule that reacts to AWS CloudTrail events to invoke the Lambda function.

C. Create an AWS CloudFormation stack to deploy an AWS Lambda function. Configure the Lambda function to look up the appropriate cost center from the RDS database and to tag resources. Create an Amazon EventBridge scheduled rule to invoke the CloudFormation stack.

D. Create an AWS Lambda function to tag the resources with a default value. Configure an Amazon EventBridge rule that reacts to AWS CloudTrail events to invoke the Lambda function when a resource is missing the cost center tag.

Answer: B

Explanation: AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers. Lambda can be used to tag resources with the cost center ID of the user who created the resource, by querying the RDS database that maps users to cost centers. Amazon EventBridge is a serverless event bus service that enables event-driven architectures. EventBridge can be configured to react to AWS CloudTrail events, which are recorded API calls made by or on behalf of the AWS account. EventBridge can invoke the Lambda function when a resource is created in the specific AWS account, passing the user identity and resource information as parameters. This solution will meet the requirements, as it enables automatic tagging of resources based on the user and cost center mapping.

References:

- 1 provides an overview of AWS Lambda and its benefits.
- 2 provides an overview of Amazon EventBridge and its benefits.
- 3 explains the concept and benefits of AWS CloudTrail events.

601. - (Topic 4)

A company wants to securely exchange data between its software as a service (SaaS) application Salesforce account and Amazon S3. The company must encrypt the data at rest by using AWS Key Management Service (AWS KMS) customer managed keys (CMKs). The company must also encrypt the data in transit. The company has enabled API access for the Salesforce account.

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

A. Create AWS Lambda functions to transfer the data securely from Salesforce to Amazon S3.

B. Create an AWS Step Functions workflow Define the task to transfer the data securely from Salesforce to

Amazon S3.

C. Create Amazon AppFlow flows to transfer the data securely from Salesforce to Amazon S3.

D. Create a custom connector for Salesforce to transfer the data securely from Salesforce to Amazon S3.

Answer: C

Explanation: Amazon AppFlow is a fully managed integration service that enables users to transfer data securely between SaaS applications and AWS services. It supports Salesforce as a source and Amazon S3 as a destination. It also supports encryption of data at rest using AWS KMS CMKs and encryption of data in transit using SSL/TLS1. By using Amazon AppFlow, the solution can meet the requirements with the least development effort.

* A. Create AWS Lambda functions to transfer the data securely from Salesforce to Amazon S3. This solution will not meet the requirement of the least development effort, as it involves writing custom code to interact with Salesforce and Amazon S3 APIs, handle authentication, encryption, error handling, and monitoring2.

* B. Create an AWS Step Functions workflow Define the task to transfer the data securely from Salesforce to Amazon S3. This solution will not meet the requirement of the least development effort, as it involves creating a state machine definition to orchestrate the data transfer task, and invoking Lambda functions or other services to perform the actual data transfer3.

* D. Create a custom connector for Salesforce to transfer the data securely from Salesforce to Ama-zon S3. This solution will not meet the requirement of the least development effort, as it involves using the Amazon AppFlow Custom Connector SDK to build and deploy a custom connector for Salesforce, which requires additional configuration and management. Reference URL: https://aws.amazon.com/appflow/

602. - (Topic 4)

A company hosts a multi-tier web application on Amazon Linux Amazon EC2 instances behind an Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The company observes that the Auto Scaling group launches more On-Demand Instances when the application's end users access high volumes of static web content. The company wants to optimize cost. What should a solutions architect do to redesign the application MOST cost-effectively?

A. Update the Auto Scaling group to use Reserved Instances instead of On-Demand Instances.

B. Update the Auto Scaling group to scale by launching Spot Instances instead of On- Demand Instances.

C. Create an Amazon CloudFront distribution to host the static web contents from an Amazon S3 bucket.

D. Create an AWS Lambda function behind an Amazon API Gateway API to host the static website contents.

Answer: C

Explanation:

This answer is correct because it meets the requirements of optimizing cost and reducing the workload on the database. Amazon CloudFront is a content delivery network (CDN) service that speeds up distribution of your static and dynamic web content, such as .html,.css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the request is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance. You can create an Amazon CloudFront distribution to host the static web contents from an Amazon S3 bucket, which is an origin that you define for CloudFront. This way, you can offload the requests for static web content from your EC2 instances to CloudFront, which can improve the performance and availability of your website, and reduce the cost of running your EC2 instances.

References:

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introducti on.html
- https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html

603. - (Topic 4)

A company is creating an application The company stores data from tests of the application in multiple on-premises locations

The company needs to connect the on-premises locations to VPCs in an AWS Region in the AWS Cloud The number of accounts and VPCs will increase during the next year The network architecture must simplify the administration of new connections and must provide the ability to scale.

Which solution will meet these requirements with the LEAST administrative overhead'?

A. Create a peering connection between the VPCs Create a VPN connection between the VPCs and the on-premises locations.

B. Launch an Amazon EC2 instance On the instance, include VPN software that uses a VPN connection to connect all VPCs and on-premises locations.

C. Create a transit gateway Create VPC attachments for the VPC connections Create VPN attachments for the on-premises connections.

D. Create an AWS Direct Connect connection between the on-premises locations and a central VPC. Connect the central VPC to other VPCs by using peering connections.

Answer: C

Explanation: A transit gateway is a network transit hub that enables you to connect your VPCs and on-premises networks in a centralized and scalable way. You can create VPC attachments to connect your VPCs to the transit gateway, and VPN attachments to connect your on-premises networks to the transit gateway over the internet. The transit gateway acts as a router between the attached networks, and simplifies the administration of new connections by reducing the number of peering or VPN connections required. You can also use transit gateway route tables to control the routing of traffic between the attached networks. By creating a transit gateway and using VPC and VPN attachments, you can meet the requirements of the company with the least administrative overhead.

References:

- AWS Transit Gateway
- Transit gateway attachments
- Transit gateway route tables

604. - (Topic 4)

A company has users all around the world accessing its HTTP-based application deployed on Amazon EC2 instances in multiple AWS Regions. The company wants to improve the availability and performance of the application. The company also wants to protect the application against common web exploits that may affect availability, compromise security, or consume excessive resources. Static IP addresses are required. What should a solutions architect recommend to accomplish this?

A. Put the EC2 instances behind Network Load Balancers (NLBs) in each Region. Deploy AWS WAF on the NLBs. Create an accelerator using AWS Global Accelerator and register the NLBs as endpoints.

B. Put the EC2 instances behind Application Load Balancers (ALBs) in each Region. Deploy AWS WAF on the ALBs. Create an accelerator using AWS Global Accelerator and register the ALBs as endpoints.

C. Put the EC2 instances behind Network Load Balancers (NLBs) in each Region. Deploy AWS WAF on the NLBs. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53

latency-based routing to route requests to the NLBs.

D. Put the EC2 instances behind Application Load Balancers (ALBs) in each Region. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the ALBs. Deploy AWS WAF on the CloudFront distribution.

Answer: A

Explanation: The company wants to improve the availability and performance of the application, as well as protect it against common web exploits. The company also needs static IP addresses for the application. To meet these requirements, a solutions architect should recommend the following solution:

- Put the EC2 instances behind Network Load Balancers (NLBs) in each Region.

NLBs are designed to handle millions of requests per second while maintaining high throughput at ultra-low latency. NLBs also support static IP addresses for each Availability Zone, which can be useful for whitelisting or firewalling purposes.

- Deploy AWS WAF on the NLBs. AWS WAF is a web application firewall that helps protect web applications from common web exploits that could affect availability, security, or performance. AWS WAF lets you define customizable web security rules that control which traffic to allow or block to your web applications.
- Create an accelerator using AWS Global Accelerator and register the NLBs as endpoints. AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in any AWS Region. It uses the AWS global network to optimize the path from your users to your applications, improving the performance of your TCP and UDP traffic.

This solution will provide high availability across Availability Zones and Regions, improve performance by routing traffic over the AWS global network, protect the application from common web attacks, and provide static IP addresses for the application.

References:

- Network Load Balancer
- AWS WAF
- AWS Global Accelerator

605. - (Topic 4)

A media company stores movies in Amazon S3. Each movie is stored in a single video file that ranges from 1 GB to 10 GB in size.

The company must be able to provide the streaming content of a movie within 5 minutes of a user purchase. There is higher demand for movies that are less than 20 years old than for movies that are more than 20 years old. The company wants to minimize hosting service costs based on demand.

Which solution will meet these requirements?

A. Store all media content in Amazon S3. Use S3 Lifecycle policies to move media data into the Infrequent Access tier when the demand for a movie decreases.

B. Store newer movie video files in S3 Standard Store older movie video files in S3 Standard-Infrequent Access (S3 Standard-IA). When a user orders an older movie, retrieve the video file by using standard retrieval.

C. Store newer movie video files in S3 Intelligent-Tiering. Store older movie video files in S3 Glacier Flexible Retrieval. When a user orders an older movie, retrieve the video file by using expedited retrieval.

D. Store newer movie video files in S3 Standard. Store older movie video files in S3 Glacier Flexible Retrieval. When a user orders an older movie, retrieve the video file by using bulk retrieval.

Answer: C

Explanation: This solution will meet the requirements of minimizing hosting service costs based on demand and providing the streaming content of a movie within 5 minutes of a user purchase. S3 Intelligent-Tiering is a storage class that automatically optimizes storage costs by moving data to the most cost-effective access tier when access patterns change. It is suitable for data with unknown, changing, or unpredictable access patterns, such as newer movies that may have higher demand1. S3 Glacier Flexible Retrieval is a storage class that provides low-cost storage for archive data that is retrieved asynchronously. It offers flexible data retrieval options from minutes to hours, and free bulk retrievals in 5-12 hours. It is ideal for backup, disaster recovery, and offsite data storage needs2. By using expedited retrieval, the user can access the older movie video file in 1-5 minutes, which meets the requirement of 5 minutes3.

References: 1: Amazon S3 Intelligent-Tiering Storage Class | AWS4, Overview section2: Amazon S3 Glacier Flexible Retrieval and Glacier Deep Archive Retrieval …1, Amazon S3 Glacier Flexible Retrieval section3: Amazon S3 Glacier Flexible Retrieval and Glacier Deep Archive Retrieval …1, Retrieval Rates section.

606. - (Topic 4)

An image hosting company uploads its large assets to Amazon S3 Standard buckets The company uses multipart upload in parallel by using S3 APIs and overwrites if the same object is uploaded again. For the first 30 days after upload, the objects will be accessed frequently. The objects will be used less frequently after 30 days, but the access patterns for each object will be inconsistent The company must optimize its S3 storage costs while maintaining high availability and resiliency of stored assets.

Which combination of actions should a solutions architect recommend to meet these requirements? (Select TWO.)

A. Move assets to S3 Intelligent-Tiering after 30 days.

B. Configure an S3 Lifecycle policy to clean up incomplete multipart uploads.

C. Configure an S3 Lifecycle policy to clean up expired object delete markers.

D. Move assets to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days

E. Move assets to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

Answer: A,B

Explanation: S3 Intelligent-Tiering is a storage class that automatically moves data to the most cost-effective access tier based on access frequency, without performance impact, retrieval fees, or operational overhead1. It is ideal for data with unknown or changing access patterns, such as the company's assets. By moving assets to S3 Intelligent-Tiering after 30 days, the company can optimize its storage costs while maintaining high availability and resilience of stored assets.

S3 Lifecycle is a feature that enables you to manage your objects so that they are stored cost effectively throughout their lifecycle2. You can create lifecycle rules to define actions that Amazon S3 applies to a group of objects. One of the actions is to abort incomplete multipart uploads that can occur when an upload is interrupted. By configuring an S3 Lifecycle policy to clean up incomplete multipart uploads, the company can reduce its storage costs and avoid paying for parts that are not used.

Option C is incorrect because expired object delete markers are automatically deleted by Amazon S3 and do not incur any storage costs3. Therefore, configuring an S3 Lifecycle policy to clean up expired object delete markers will not have any effect on the company's storage costs.

Option D is incorrect because S3 Standard-IA is a storage class for data that is accessed less frequently, but requires rapid access when needed1. It has a lower storage cost than S3 Standard, but it has a higher

retrieval cost and a minimum storage duration charge of 30 days. Therefore, moving assets to S3 Standard-IA after 30 days may not optimize the company's storage costs if the assets are still accessed occasionally.

Option E is incorrect because S3 One Zone-IA is a storage class for data that is accessed less frequently, but requires rapid access when needed1. It has a lower storage cost than S3 Standard-IA, but it stores data in only one Availability Zone and has less resilience than other storage classes. It also has a higher retrieval cost and a minimum storage duration charge of 30 days. Therefore, moving assets to S3 One Zone-IA after 30 days may not optimize the company's storage costs if the assets are still accessed occasionally or require high availability. Reference URL: 1: https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html 2: https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html 3: https://docs.aws.amazon.com/AmazonS3/latest/userguide/delete-or-empty-bucket.html#delete-bucket-considerations : https://docs.aws.amazon.com/AmazonS3/latest/userguide/mpuoverview.html : https://aws.amazon.com/certification/certified-solutions-architect-associate/

607. - (Topic 4)

A solutions architect is designing a highly available Amazon ElastiCache for Redis based solution. The solutions architect needs to ensure that failures do not result in performance degradation or loss of data locally and within an AWS Region. The solution needs to provide high availability at the node level and at the Region level.

Which solution will meet these requirements?

A. Use Multi-AZ Redis replication groups with shards that contain multiple nodes.

B. Use Redis shards that contain multiple nodes with Redis append only files (AOF) tured on.

C. Use a Multi-AZ Redis cluster with more than one read replica in the replication group.

D. Use Redis shards that contain multiple nodes with Auto Scaling turned on.

Answer: A

Explanation: This answer is correct because it provides high availability at the node level and at the Region level for the ElastiCache for Redis solution. A Multi-AZ Redis replication group consists of a primary cluster and up to five read replica clusters, each in a different Availability Zone. If the primary cluster fails, one of

the read replicas is automatically promoted to be the new primary cluster. A Redis replication group with shards enables partitioning of the data across multiple nodes, which increases the scalability and performance of the solution. Each shard can have one or more replicas to provide redundancy and read scaling.

References:

- https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/AutoFailover.html
- https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/Shards.html

608. - (Topic 4)

A financial company needs to handle highly sensitive data The company will store the data in an Amazon S3 bucket The company needs to ensure that the data is encrypted in transit and at rest The company must manage the encryption keys outside the AWS Cloud

Which solution will meet these requirements?

A. Encrypt the data in the S3 bucket with server-side encryption (SSE) that uses an AWS Key Management Service (AWS KMS) customer managed key

B. Encrypt the data in the S3 bucket with server-side encryption (SSE) that uses an AWS Key Management Service (AWS KMS) AWS managed key

C. Encrypt the data in the S3 bucket with the default server-side encryption (SSE)

D. Encrypt the data at the company's data center before storing the data in the S3 bucket

Answer: D

Explanation: This option is the only solution that meets the requirements because it allows the company to encrypt the data with its own encryption keys and tools outside the AWS Cloud. By encrypting the data at the company's data center before storing the data in the S3 bucket, the company can ensure that the data is encrypted in transit and at rest, and that the company has full control over the encryption keys and processes. This option also avoids the need to use any AWS encryption services or features, which may not be compatible with the company's security policies or compliance standards.

* A. Encrypt the data in the S3 bucket with server-side encryption (SSE) that uses an AWS Key Management Service (AWS KMS) customer managed key. This option does not meet the requirements because it does not allow the company to manage the encryption keys outside the AWS Cloud. Although the company can create and use its own customer managed key in AWS KMS, the key is still stored and

managed by AWS KMS, which is a service within the AWS Cloud. Moreover, the company still needs to use the AWS encryption features and APIs to encrypt and decrypt the data in the S3 bucket, which may not be compatible with the company's security policies or compliance standards.

* B. Encrypt the data in the S3 bucket with server-side encryption (SSE) that uses an AWS Key Management Service (AWS KMS) AWS managed key. This option does not meet the requirements because it does not allow the company to manage the encryption keys outside the AWS Cloud. In this option, the company uses the default AWS managed key in AWS KMS, which is created and managed by AWS on behalf of the company. The company has no control over the key rotation, deletion, or recovery policies. Moreover, the company still needs to use the AWS encryption features and APIs to encrypt and decrypt the data in the S3 bucket, which may not be compatible with the company's security policies or compliance standards.

* C. Encrypt the data in the S3 bucket with the default server-side encryption (SSE). This option does not meet the requirements because it does not allow the company to manage the encryption keys outside the AWS Cloud. In this option, the company uses the default server-side encryption with Amazon S3 managed keys (SSE-S3), which is applied to every bucket in Amazon S3. The company has no visibility or control over the encryption keys, which are managed by Amazon S3. Moreover, the company still needs to use the AWS encryption features and APIs to encrypt and decrypt the data in the S3 bucket, which may not be compatible with the company's security policies or compliance standards. References:

- 1 Protecting data with encryption - Amazon Simple Storage Service
- 2 Protecting data with server-side encryption - Amazon Simple Storage Service
- 3 Protecting data by using client-side encryption - Amazon Simple Storage Service
- 4 AWS Key Management Service Concepts - AWS Key Management Service

609. - (Topic 4)

A social media company runs its application on Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is the origin for an Amazon CloudFront distribution. The application has more than a billion images stored in an Amazon S3 bucket and processes thousands of images each second. The company wants to resize the images dynamically and serve appropriate formats to clients.

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

A. Install an external image management library on an EC2 instance. Use the image management library to

process the images.

B. Create a CloudFront origin request policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.

C. Use a Lambda@Edge function with an external image management library. Associate the Lambda@Edge function with the CloudFront behaviors that serve the images.

D. Create a CloudFront response headers policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.

Answer: C

Explanation: Lambda@Edge is a service that allows you to run Lambda functions at CloudFront edge locations. It can be used to modify requests and responses that flow through CloudFront. CloudFront origin request policy is a policy that controls the values (URL query strings, HTTP headers, and cookies) that are included in requests that CloudFront sends to the origin. It can be used to collect additional information at the origin or to customize the origin response. CloudFront response headers policy is a policy that specifies the HTTP headers that CloudFront removes or adds in responses that it sends to viewers. It can be used to add security or custom headers to responses.

Based on these definitions, the solution that will meet the requirements with the least operational overhead is:

* C. Use a Lambda@Edge function with an external image management library. Associate the Lambda@Edge function with the CloudFront behaviors that serve the images.

This solution would allow the application to use a Lambda@Edge function to resize the images dynamically and serve appropriate formats to clients based on the User-Agent HTTP header in the request. The Lambda@Edge function would run at the edge locations,

reducing latency and load on the origin. The application code would only need to include an external image management library that can perform image manipulation tasks1.

610. - (Topic 4)

A company's ecommerce website has unpredictable traffic and uses AWS Lambda functions to directly access a private Amazon RDS for PostgreSQL DB instance. The company wants to maintain predictable database performance and ensure that the Lambda invocations do not overload the database with too many connections.

What should a solutions architect do to meet these requirements?

A. Point the client driver at an RDS custom endpoint. Deploy the Lambda functions inside a VPC.

B. Point the client driver at an RDS proxy endpoint. Deploy the Lambda functions inside a VPC.

C. Point the client driver at an RDS custom endpoint. Deploy the Lambda functions outside a VPC.

D. Point the client driver at an RDS proxy endpoint. Deploy the Lambda functions outside a VPC.

Answer: B

Explanation: To maintain predictable database performance and ensure that the Lambda invocations do not overload the database with too many connections, a solutions architect should point the client driver at an RDS proxy endpoint and deploy the Lambda functions inside a VPC. An RDS proxy is a fully managed database proxy that allows applications to share connections to a database, improving database availability and scalability. By using an RDS proxy, the Lambda functions can reuse existing connections, rather than creating new ones for every invocation, reducing the connection overhead and latency. Deploying the Lambda functions inside a VPC allows them to access the private RDS DB instance securely and efficiently, without exposing it to the public internet. References:

- Using Amazon RDS Proxy with AWS Lambda
- Configuring a Lambda function to access resources in a VPC

611. - (Topic 4)

A company needs to migrate a MySQL database from its on-premises data center to AWS within 2 weeks. The database is 20 TB in size. The company wants to complete the migration with minimal downtime. Which solution will migrate the database MOST cost-effectively?

A. Order an AWS Snowball Edge Storage Optimized device. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with replication of ongoing changes. Send the Snowball Edge device to AWS to finish the migration and continue the ongoing replication.

B. Order an AWS Snowmobile vehicle. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database wjgh ongoing changes. Send the Snowmobile vehicle back to AWS to finish the migration and continue the ongoing replication.

C. Order an AWS Snowball Edge Compute Optimized with GPU device. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with ongoing

changes. Send the Snowball device to AWS to finish the migration and continue the ongoing replication.

D. Order a 1 GB dedicated AWS Direct Connect connection to establish a connection with the data center. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool(AWS SCT) to migrate the database with replication of ongoing changes.

Answer: A

Explanation: This answer is correct because it meets the requirements of migrating a 20 TB MySQL database within 2 weeks with minimal downtime and cost-effectively. The AWS Snowball Edge Storage Optimized device has up to 80 TB of usable storage space, which is enough to fit the database. The AWS Database Migration Service (AWS DMS) can migrate data from MySQL to Amazon Aurora, Amazon RDS for MySQL, or MySQL on Amazon EC2 with minimal downtime by continuously replicating changes from the source to the target. The AWS Schema Conversion Tool (AWS SCT) can convert the source schema and code to a format compatible with the target database. By using these services together, the company can migrate the database to AWS with minimal downtime and cost. The Snowball Edge device can be shipped back to AWS to finish the migration and continue the ongoing replication until the database is fully migrated.

References:

- https://docs.aws.amazon.com/snowball/latest/developer-guide/device- differences.html
- https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Source.MySQL.html
- https://docs.aws.amazon.com/SchemaConversionTool/latest/userguide/CHAP_So urce.MySQL.htm

612. - (Topic 4)

A company uses on-premises servers to host its applications The company is running out of storage capacity. The applications use both block storage and NFS storage. The company needs a high-performing solution that supports local caching without re-

architecting its existing applications.

Which combination of actions should a solutions architect take to meet these requirements? (Select TWO.)

A. Mount Amazon S3 as a file system to the on-premises servers.

B. Deploy an AWS Storage Gateway file gateway to replace NFS storage.

C. Deploy AWS Snowball Edge to provision NFS mounts to on-premises servers.

D. Deploy an AWS Storage Gateway volume gateway to replace the block storage

E. Deploy Amazon Elastic File System (Amazon EFS) volumes and mount them to on- premises servers.

Answer: B,D

Explanation: https://aws.amazon.com/storagegateway/file/

File Gateway provides a seamless way to connect to the cloud in order to store application data files and backup images as durable objects in Amazon S3 cloud storage. File Gateway offers SMB or NFS-based access to data in Amazon S3 with local caching. It can be used for on-premises applications, and for Amazon EC2-based applications that need file protocol access to S3 object storage.

https://aws.amazon.com/storagegateway/volume/

Volume Gateway presents cloud-backed iSCSI block storage volumes to your on-premises applications. Volume Gateway stores and manages on-premises data in Amazon S3 on your behalf and operates in either cache mode or stored mode. In the cached Volume Gateway mode, your primary data is stored in Amazon S3, while retaining your frequently accessed data locally in the cache for low latency access.

613. - (Topic 4)

A company stores raw collected data in an Amazon S3 bucket. The data is used for several types of analytics on behalf of the company's customers. The type of analytics requested to determines the access pattern on the S3 objects.

The company cannot predict or control the access pattern. The company wants to reduce its S3 costs. which solution will meet these requirements?

A. Use S3 replication to transition infrequently accessed objects to S3 Standard-Infrequent Access (S3 Standard-1A)

B. Use S3 Lifecycle rules to transition objects from S3 Standard to Standard-Infrequent Access (S3 Standard-1A).

C. Use S3 Lifecycle rules for transition objects from S3 Standard to S3 Intelligent-Tiering.

D. Use S3 Inventory to identify and transition objects that have not been accessed from S3 Standard to S3 Intelligent-Tiering.

Answer: C

Explanation: S3 Intelligent-Tiering is a storage class that automatically reduces storage costs by moving data to the most cost-effective access tier based on access frequency. It has two access tiers: frequent access and infrequent access. Data is stored in the frequent access tier by default, and moved to the

infrequent access tier after 30 consecutive days of no access. If the data is accessed again, it is moved back to the frequent access tie1r. By using S3 Lifecycle rules to transition objects from S3 Standard to S3 Intelligent-Tiering, the solution can reduce S3 costs for data with unknown or changing access patterns.

* A. Use S3 replication to transition infrequently accessed objects to S3 Standard-Infrequent Access (S3 Standard-IA). This solution will not meet the requirement of reducing S3 costs for data with unknown or changing access patterns, as S3 replication is a feature that copies objects across buckets or Regions for redundancy or compliance purposes. It does not automatically move objects to a different storage class based on access frequency2.

* B. Use S3 Lifecycle rules to transition objects from S3 Standard to Standard-Infrequent Access (S3 Standard-IA). This solution will not meet the requirement of reducing S3 costs for data with unknown or changing access patterns, as S3 Standard-IA is a storage class that offers lower storage costs than S3 Standard, but charges a retrieval fee for accessing the data. It is suitable for long-lived and infrequently accessed data, not for data with changing access patterns1.

* D. Use S3 Inventory to identify and transition objects that have not been accessed from S3 Stand-ard to S3 Intelligent-Tiering. This solution will not meet the requirement of reducing S3 costs for data with unknown or changing access patterns, as S3 Inventory is a feature that provides a report of the objects in a bucket and their metadata on a daily or weekly basis. It does not automatically move objects to a different storage class based on access frequency3.

Reference URL: https://aws.amazon.com/s3/storage-classes/intelligent-tiering/

S3 Intelligent-Tiering is the best solution for reducing S3 costs when the access pattern is unpredictable or changing. S3 Intelligent-Tiering automatically moves objects between two access tiers (frequent and infrequent) based on the access frequency, without any performance impact or retrieval fees. S3 Intelligent-Tiering also has an optional archive tier for objects that are rarely accessed. S3 Lifecycle rules can be used to transition objects from S3 Standard to S3 Intelligent-Tiering.

Reference URLs:

1 https://aws.amazon.com/s3/storage-classes/intelligent-tiering/

2 https://docs.aws.amazon.com/AmazonS3/latest/userguide/using-intelligent-tiering.html

3 https://docs.aws.amazon.com/AmazonS3/latest/userguide/intelligent-tiering- overview.html

614. - (Topic 4)

A company has a multi-tier payment processing application that is based on virtual machines (VMs). The communication between the tiers occurs asynchronously through a third-party middleware solution that guarantees exactly-once delivery.

The company needs a solution that requires the least amount of infrastructure management. The solution must guarantee exactly-once delivery for application messaging

Which combination of actions will meet these requirements? (Select TWO.)

A. Use AWS Lambda for the compute layers in the architecture.

B. Use Amazon EC2 instances for the compute layers in the architecture.

C. Use Amazon Simple Notification Service (Amazon SNS) as the messaging component between the compute layers.

D. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues as the messaging component between the compute layers.

E. Use containers that are based on Amazon Elastic Kubemetes Service (Amazon EKS) for the compute layers in the architecture.

Answer: A,D

Explanation: This solution meets the requirements because it requires the least amount of infrastructure management and guarantees exactly-once delivery for application messaging. AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers. You only pay for the compute time you consume. Lambda scales automatically with the size of your workload. Amazon SQS FIFO queues are designed to ensure that messages are processed exactly once, in the exact order that they are sent. FIFO queues have high availability and deliver messages in a strict first-in, first-out order. You can use Amazon SQS to decouple and scale microservices, distributed systems, and serverless applications. References: AWS Lambda, Amazon SQS FIFO queues

615. - (Topic 4)

A company containerized a Windows job that runs on .NET 6 Framework under a Windows container. The company wants to run this job in the AWS Cloud. The job runs every 10 minutes. The job's runtime varies between 1 minute and 3 minutes.

Which solution will meet these requirements MOST cost-effectively?

A. Create an AWS Lambda function based on the container image of the job. Configure Amazon

EventBridge to invoke the function every 10 minutes.

B. Use AWS Batch to create a job that uses AWS Fargate resources. Configure the job scheduling to run every 10 minutes.

C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate to run the job. Create a scheduled task based on the container image of the job to run every 10 minutes.

D. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate to run the job. Create a standalone task based on the container image of the job. Use Windows task scheduler to run the job every 10 minutes.

Answer: A

Explanation: AWS Lambda supports container images as a packaging format for functions. You can use existing container development workflows to package and deploy Lambda functions as container images of up to 10 GB in size. You can also use familiar tools such as Docker CLI to build, test, and push your container images to Amazon Elastic Container Registry (Amazon ECR). You can then create an AWS Lambda function based on the container image of your job and configure Amazon EventBridge to invoke the function every 10 minutes using a cron expression. This solution will be cost-effective as you only pay for the compute time you consume when your function runs. References:

https://docs.aws.amazon.com/lambda/latest/dg/images-create.html

https://docs.aws.amazon.com/eventbridge/latest/userguide/run-lambda-schedule.html

616. - (Topic 4)

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

A. Deploy an Amazon EC2 instance to host an API that sends data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.

B. Deploy an Amazon EC2 instance to host an API that sends data to AWS Glue. Stop source/destination checking on the EC2 instance. Use AWS Glue to transform the data and to send the data to Amazon S3.

C. Configure an Amazon API Gateway API to send data to an Amazon Kinesis data

stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.

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

Answer: C

Explanation: It uses Amazon Kinesis Data Firehose which is a fully managed service for delivering real-time streaming data to destinations such as Amazon S3. This service requires less operational overhead as compared to option A, B, and D. Additionally, it also uses Amazon API Gateway which is a fully managed service for creating, deploying, and managing APIs. These services help in reducing the operational overhead and automating the data ingestion process.

617. - (Topic 4)

A solutions architect wants to use the following JSON text as an identity-based policy to grant specific permissions:

```
{    "Statement": [
        {
            "Action": [
                "ssm:ListDocuments",
                "ssm:GetDocument"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Sid": ""
        }
    ],
    "Version": "2012-10-17"
}
```

Which IAM principals can the solutions architect attach this policy to? (Select TWO.)

A. Role

B. Group

C. Organization

D. Amazon Elastic Container Service (Amazon ECS) resource

E. Amazon EC2 resource

Answer: A,B

Explanation:

This JSON text is an identity-based policy that grants specific permissions. The IAM principals that the solutions architect can attach this policy to are Role and Group. This is because the policy is written in JSON and is an identity-based policy, which can be attached to IAM principals such as users, groups, and roles. Identity-based policies are permissions policies that you attach to IAM identities (users, groups, or roles) and explicitly state what that identity is allowed (or denied) to do1. Identity-based policies are different from resource-based policies, which define the permissions around the specific resource1. Resource-based policies are attached to a resource, such as an Amazon S3 bucket or an Amazon EC2 instance1. Resource-based policies can also specify a principal, which is the entity that is allowed or denied access to the resource1. Organization is not an IAM principal, but a feature of AWS Organizations that allows you to manage multiple AWS accounts centrally2. Amazon ECS resource and Amazon EC2 resource are not IAM principals, but AWS resources that can have resource-based policies attached to them34. References:

- Identity-based policies and resource-based policies
- AWS Organizations
- Amazon ECS task role
- Amazon EC2 instance profile

618. - (Topic 4)

A company wants to analyze and generate reports to track the usage of its mobile app. The app is popular and has a global user base The company uses a custom report building program to analyze application usage.

The program generates multiple reports during the last week of each month. The program takes less than 10 minutes to produce each report. The company rarely uses the program to generate reports outside of the last week of each month. The company wants to generate reports in the least amount of time when the reports are requested.

Which solution will meet these requirements MOST cost-effectively?

A. Run the program by using Amazon EC2 On-Demand Instances. Create an Amazon EventBridge rule to start the EC2 instances when reports are requested. Run the EC2 instances continuously during the last week of each month.

B. Run the program in AWS Lambda. Create an Amazon EventBridge rule to run a Lambda function when reports are requested.

C. Run the program in Amazon Elastic Container Service (Amazon ECS). Schedule Amazon ECS to run the program when reports are requested.

D. Run the program by using Amazon EC2 Spot Instances. Create an Amazon EventBridge rule to start the EC2 instances when reports are requested. Run the EC2 instances continuously during the last week of each month.

Answer: B

Explanation: This solution meets the requirements most cost-effectively because it leverages the serverless and event-driven capabilities of AWS Lambda and Amazon EventBridge. AWS Lambda allows you to run code without provisioning or managing servers, and you pay only for the compute time you consume. Amazon EventBridge is a serverless event bus service that lets you connect your applications with data from various sources and routes that data to targets such as AWS Lambda. By using Amazon EventBridge, you can create a rule that triggers a Lambda function to run the program when reports are requested, and you can also schedule the rule to run during the last week of each month. This way, you can generate reports in the least amount of time and pay only for the resources you use.

References:

- AWS Lambda
- Amazon EventBridge

619. - (Topic 4)

A company has an application that uses Docker containers in its local data center The application runs on a container host that stores persistent data in a volume on the host. The container instances use the stored persistent data.

The company wants to move the application to a fully managed service because the company does not want to manage any servers or storage infrastructure.

Which solution will meet these requirements?

A. Use Amazon Elastic Kubernetes Service (Amazon EKS) with self-managed nodes. Create an Amazon Elastic Block Store (Amazon EBS) volume attached to an Amazon EC2 instance. Use the EBS volume as a persistent volume mounted in the containers.

B. Use Amazon Elastic Container Service (Amazon ECS) with an AWS Fargate launch type. Create an Amazon Elastic File System (Amazon EFS) volume. Add the EFS volume as a persistent storage volume mounted in the containers.

C. Use Amazon Elastic Container Service (Amazon ECS) with an AWS Fargate launch type. Create an Amazon S3 bucket. Map the S3 bucket as a persistent storage volume mounted in the containers.

D. Use Amazon Elastic Container Service (Amazon ECS) with an Amazon EC2 launch type. Create an Amazon Elastic File System (Amazon EFS) volume. Add the EFS volume as a persistent storage volume mounted in the containers.

Answer: B

Explanation: This solution meets the requirements because it allows the company to move the application to a fully managed service without managing any servers or storage infrastructure. AWS Fargate is a serverless compute engine for containers that runs the Amazon ECS tasks. With Fargate, the company does not need to provision, configure, or scale clusters of virtual machines to run containers. Amazon EFS is a fully managed file system that can be accessed by multiple containers concurrently. With EFS, the company does not need to provision and manage storage capacity. EFS provides a simple interface to create and configure file systems quickly and easily. The company can use the EFS volume as a persistent storage volume mounted in the containers to store the persistent data. The company can also use the EFS mount helper to simplify the mounting process. References: Amazon ECS on AWS Fargate, Using Amazon EFS file systems with Amazon ECS, Amazon EFS mount helper.

620. - (Topic 4)

An ecommerce company is running a seasonal online sale. The company hosts its website on Amazon EC2 instances spanning multiple Availability Zones. The company wants its website to manage sudden traffic increases during the sale.

Which solution will meet these requirements MOST cost-effectively?

A. Create an Auto Scaling group that is large enough to handle peak traffic load. Stop half of the Amazon EC2 instances. Configure the Auto Scaling group to use the stopped instances to scale out when traffic

increases.

B. Create an Auto Scaling group for the website. Set the minimum size of the Auto Scaling group so that it can handle high traffic volumes without the need to scale out.

C. Use Amazon CloudFront and Amazon ElastiCache to cache dynamic content with an Auto Scaling group set as the origin. Configure the Auto Scaling group with the instances necessary to populate CloudFront and ElastiCache. Scale in after the cache is fully populated.

D. Configure an Auto Scaling group to scale out as traffic increases. Create a launch template to start new instances from a preconfigured Amazon Machine Image (AMI).

Answer: D

Explanation:

The solution that meets the requirements of high availability, resiliency, and minimal operational effort is to use AWS Transfer for SFTP and an Amazon S3 bucket for storage. This solution allows the company to securely transfer files over SFTP to Amazon S3, which is a durable and scalable object storage service. The company can then modify the application to pull the batch files from Amazon S3 to an Amazon EC2 instance for processing. The EC2 instance can be part of an Auto Scaling group with a scheduled scaling policy to run the batch operation only at night. This way, the company can save costs by scaling down the EC2 instances when they are not needed. The other solutions do not meet all the requirements because they either use Amazon EFS or Amazon EBS for storage, which are more expensive and less scalable than Amazon S3, or they do not use a scheduled scaling policy to optimize the EC2 instances usage.

References :=

- AWS Transfer for SFTP
- Amazon S3
- Amazon EC2 Auto Scaling

621. - (Topic 4)

A company is moving its data and applications to AWS during a multiyear migration project. The company wants to securely access data on Amazon S3 from the company's AWS Region and from the company's on-premises location. The data must not traverse the internet. The company has established an AWS Direct Connect connection between its Region and its on-premises location

Which solution will meet these requirements?

A. Create gateway endpoints for Amazon S3. Use the gateway endpoints to securely access the data from the Region and the on-premises location.

B. Create a gateway in AWS Transit Gateway to access Amazon S3 securely from the Region and the on-premises location.

C. Create interface endpoints for Amazon S3_ Use the interface endpoints to securely access the data from the Region and the on-premises location.

D. Use an AWS Key Management Service (AWS KMS) key to access the data securely from the Region and the on-premises location.

Answer: B

Explanation: A gateway endpoint is a gateway that is a target for a specified route in your route table, used for traffic destined to a supported AWS service1. Amazon S3 does not support gateway endpoints, only interface endpoints2. Therefore, option A is incorrect.

An interface endpoint is an elastic network interface with a private IP address that serves as an entry point for traffic destined to a supported service1. An interface endpoint can provide secure access to Amazon S3 from within the Region, but not from the on-premises location. Therefore, option C is incorrect.

AWS Key Management Service (AWS KMS) is a service that allows you to create and manage encryption keys to protect your data3. AWS KMS does not provide a way to access data on Amazon S3 without traversing the internet. Therefore, option D is incorrect. AWS Transit Gateway is a service that enables you to connect your Amazon Virtual Private Clouds (VPCs) and your on-premises networks to a single gateway. You can create a gateway in AWS Transit Gateway to access Amazon S3 securely from both the Region and the on-premises location using AWS Direct Connect. Therefore, option B is correct.

622. - (Topic 4)

A company wants to use an AWS CloudFormatlon stack for its application in a test environment. The company stores the CloudFormation template in an Amazon S3 bucket that blocks public access. The company wants to grant CloudFormation access to the template in the S3 bucket based on specific user requests to create the test environment The solution must follow security best practices.

Which solution will meet these requirements?

A. Create a gateway VPC endpoint for Amazon S3. Configure the CloudFormation stack to use the S3 object URL

B. Create an Amazon API Gateway REST API that has the S3 bucket as the target. Configure the CloudFormat10n stack to use the API Gateway URL _

C. Create a presigned URL for the template object_ Configure the CloudFormation stack to use the presigned URL.

D. Allow public access to the template object in the S3 bucket. Block the public access after the test environment is created

Answer: C

Explanation: it allows CloudFormation to access the template in the S3 bucket without granting public access or creating additional resources. A presigned URL is a URL that is

signed with the access key of an IAM user or role that has permission to access the object. The presigned URL can be used by anyone who receives it, but it expires after a specified time. By creating a presigned URL for the template object and configuring the CloudFormation stack to use it, the company can grant CloudFormation access to the template based on specific user requests and follow security best practices.

References:

- Using Amazon S3 Presigned URLs
- Using Amazon S3 Buckets

623. - (Topic 4)

A company has two VPCs named Management and Production. The Management VPC uses VPNs through a customer gateway to connect to a single device in the data center. The Production VPC uses a virtual private gateway AWS Direct Connect connections. The Management and Production VPCs both use a single VPC peering connection to allow communication between the

What should a solutions architect do to mitigate any single point of failure in this architecture?

A. Add a set of VPNs between the Management and Production VPCs.

B. Add a second virtual private gateway and attach it to the Management VPC.

C. Add a second set of VPNs to the Management VPC from a second customer gateway device.

D. Add a second VPC peering connection between the Management VPC and the Production VPC.

Answer: C

Explanation: This answer is correct because it provides redundancy for the VPN connection between the Management VPC and the data center. If one customer gateway device or one VPN tunnel becomes

unavailable, the traffic can still flow over the second customer gateway device and the second VPN tunnel. This way, the single point of failure in the VPN connection is mitigated.

References:

- https://docs.aws.amazon.com/vpn/latest/s2svpn/vpn-redundant-connection.html
- https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/VPC/vpn-tunnel-redundancy.html

624. - (Topic 4)

A company is creating an application that runs on containers in a VPC. The application stores and accesses data in an Amazon S3 bucket During the development phase, the application will store and access 1 TB of data in Amazon S3 each day. The company wants to minimize costs and wants to prevent traffic from traversing the internet whenever possible.

Which solution will meet these requirements?

A. Enable S3 Intelligent-Tiering for the S3 bucket.

B. Enable S3 Transfer Acceleration for the S3 bucket.

C. Create a gateway VPC endpoint for Amazon S3. Associate this endpoint with all route tables in the VPC.

D. Create an interface endpoint for Amazon S3 in the VPC. Associate this endpoint with all route tables in the VPC.

Answer: C

Explanation:

A gateway VPC endpoint for Amazon S3 enables private connections between the VPC and Amazon S3 that do not require an internet gateway or NAT device. This minimizes costs and prevents traffic from traversing the internet. A gateway VPC endpoint uses a prefix list as the route target in a VPC route table to route traffic privately to Amazon S31. Associating the endpoint with all route tables in the VPC ensures that all subnets can access Amazon S3 through the endpoint.

Option A is incorrect because S3 Intelligent-Tiering is a storage class that optimizes storage costs by automatically moving objects between two access tiers based on changing access patterns. It does not affect the network traffic between the VPC and Amazon S32.

Option B is incorrect because S3 Transfer Acceleration is a feature that enables fast, easy, and secure transfers of files over long distances between clients and an S3 bucket. It does not prevent traffic from

traversing the internet3.

Option D is incorrect because an interface VPC endpoint for Amazon S3 is powered by AWS PrivateLink, which requires an elastic network interface (ENI) with a private IP address in each subnet. This adds complexity and cost to the solution. Moreover, an interface VPC endpoint does not support cross-Region access to Amazon S3. Reference URL: 1: https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html 2: https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html#sc-dynamic-data-access 3: https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration.html : https://aws.amazon.com/blogs/architecture/choosing-your-vpc-endpoint-strategy-for- amazon-s3/

625. - (Topic 4)

A company migrated a MySQL database from the company's on-premises data center to an Amazon RDS for MySQL DB instance. The company sized the RDS DB instance to meet the company's average daily workload. Once a month, the database performs slowly when the company runs queries for a report. The company wants to have the ability to run reports and maintain the performance of the daily workloads. Which solution will meet these requirements?

A. Create a read replica of the database. Direct the queries to the read replica.

B. Create a backup of the database. Restore the backup to another DB instance. Direct the queries to the new database.

C. Export the data to Amazon S3. Use Amazon Athena to query the S3 bucket.

D. Resize the DB instance to accommodate the additional workload.

Answer: C

Explanation: Amazon Athena is a service that allows you to run SQL queries on data stored in Amazon S3. It is serverless, meaning you do not need to provision or manage any infrastructure. You only pay for the queries you run and the amount of data scanned1.

By using Amazon Athena to query your data in Amazon S3, you can achieve the following benefits:

- You can run queries for your report without affecting the performance of your Amazon RDS for MySQL DB instance. You can export your data from your DB instance to an S3 bucket and use Athena to query the data in the bucket. This way, you can avoid the overhead and contention of

running queries on your DB instance.

➪ You can reduce the cost and complexity of running queries for your report. You do not need to create a read replica or a backup of your DB instance, which would incur additional charges and require maintenance. You also do not need to resize your DB instance to accommodate the additional workload, which would increase your operational overhead.

➪ You can leverage the scalability and flexibility of Amazon S3 and Athena. You can store large amounts of data in S3 and query them with Athena without worrying about capacity or performance limitations. You can also use different formats, compression methods, and partitioning schemes to optimize your data storage and query performance1.

626. - (Topic 4)

A company has a business-critical application that runs on Amazon EC2 instances. The application stores data in an Amazon DynamoDB table. The company must be able to revert the table to any point within the last 24 hours.

Which solution meets these requirements with the LEAST operational overhead?

A. Configure point-in-time recovery for the table.

B. Use AWS Backup for the table.

C. Use an AWS Lambda function to make an on-demand backup of the table every hour.

D. Turn on streams on the table to capture a log of all changes to the table in the last 24 hours Store a copy of the stream in an Amazon S3 bucket.

Answer: A

Explanation: Point-in-time recovery (PITR) for DynamoDB is a feature that enables you to restore your table data to any point in time during the last 35 days. PITR helps protect your table from accidental write or delete operations, such as a test script writing to a production table or a user issuing a wrong command. PITR is easy to use, fully managed, fast, and scalable. You can enable PITR with a single click in the DynamoDB console or with a simple API call. You can restore a table to a new table using the console, the AWS CLI, or the DynamoDB API. PITR does not consume any provisioned table capacity and has no impact on the performance or availability of your production applications. PITR meets the requirements of the company with the least operational overhead, as it does not require any manual backup creation, scheduling, or maintenance. It also provides per-second granularity for restoring the table to any point

within the last 24 hours.

References:

- Point-in-time recovery for DynamoDB - Amazon DynamoDB
- Amazon DynamoDB point-in-time recovery (PITR)
- Enable Point-in-Time Recovery (PITR) for Dynamodb global tables
- Restoring a DynamoDB table to a point in time - Amazon DynamoDB
- Point-in-time recovery: How it works - Amazon DynamoDB

627. - (Topic 4)

A company has an on-premises MySQL database that handles transactional data. The company is migrating the database to the AWS Cloud. The migrated database must maintain compatibility with the company's applications that use the database. The migrated database also must scale automatically during periods of increased demand.

Which migration solution will meet these requirements?

A. Use native MySQL tools to migrate the database to Amazon RDS for MySQL. Configure elastic storage scaling.

B. Migrate the database to Amazon Redshift by using the mysqldump utility. Turn on Auto Scaling for the Amazon Redshift cluster.

C. Use AWS Database Migration Service (AWS DMS) to migrate the database to Amazon Aurora. Turn on Aurora Auto Scaling.

D. Use AWS Database Migration Service (AWS DMS) to migrate the database to Amazon DynamoDB. Configure an Auto Scaling policy.

Answer: C

Explanation: To migrate a MySQL database to AWS with compatibility and scalability, Amazon Aurora is a suitable option. Aurora is compatible with MySQL and can scale automatically with Aurora Auto Scaling. AWS Database Migration Service (AWS DMS) can be used to migrate the database from on-premises to Aurora with minimal downtime. References:

- What Is Amazon Aurora?
- Using Amazon Aurora Auto Scaling with Aurora Replicas
- What Is AWS Database Migration Service?

628. - (Topic 4)

A solutions architect needs to design the architecture for an application that a vendor provides as a Docker container image The container needs 50 GB of storage available for temporary files The infrastructure must be serverless.

Which solution meets these requirements with the LEAST operational overhead?

A. Create an AWS Lambda function that uses the Docker container image with an Amazon S3 mounted volume that has more than 50 GB of space

B. Create an AWS Lambda function that uses the Docker container image with an Amazon Elastic Block Store (Amazon EBS) volume that has more than 50 GB of space

C. Create an Amazon Elastic Container Service (Amazon ECS) cluster that uses the AWS Fargate launch type Create a task definition for the container image with an Amazon Elastic File System (Amazon EFS) volume. Create a service with that task definition.

D. Create an Amazon Elastic Container Service (Amazon ECS) cluster that uses the Amazon EC2 launch type with an Amazon Elastic Block Store (Amazon EBS) volume that has more than 50 GB of space Create a task definition for the container image. Create a service with that task definition.

Answer: C

Explanation:

The AWS Fargate launch type is a serverless way to run containers on Amazon ECS,

without having to manage any underlying infrastructure. You only pay for the resources required to run your containers, and AWS handles the provisioning, scaling, and security of the cluster. Amazon EFS is a fully managed, elastic, and scalable file system that can be mounted to multiple containers, and provides high availability and durability. By using AWS Fargate and Amazon EFS, you can run your Docker container image with 50 GB of storage available for temporary files, with the least operational overhead. This solution meets the requirements of the question.

References:

- AWS Fargate
- Amazon Elastic File System
- Using Amazon EFS file systems with Amazon ECS

629. - (Topic 4)

A law firm needs to share information with the public The information includes hundreds of files that must be publicly readable Modifications or deletions of the files by anyone before a designated future date are prohibited.

Which solution will meet these requirements in the MOST secure way?

A. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Grant read-only 1AM permissions to any AWS principals that access the S3 bucket until the designated date.

B. Create a new Amazon S3 bucket with S3 Versioning enabled Use S3 Object Lock with a retention period in accordance with the designated date Configure the S3 bucket for static website hosting. Set an S3 bucket policy to allow read-only access to the objrcts.

C. Create a new Amazon S3 bucket with S3 Versioning enabled Configure an event trigger to run an AWS Lambda function in case of object modification or deletion. Configure the Lambda function to replace the objects with the original versions from a private S3 bucket.

D. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Select the folder that contains the files. Use S3 Object Lock with a retention period in accordance with the designated date. Grant read-only 1AM permissions to any AWS principals that access the S3 bucket.

Answer: B

Explanation: Amazon S3 is a service that provides object storage in the cloud. It can be used to store and serve static web content, such as HTML, CSS, JavaScript, images, and videos1. By creating a new Amazon S3 bucket and configuring it for static website hosting, the solution can share information with the public.

Amazon S3 Versioning is a feature that keeps multiple versions of an object in the same bucket. It helps protect objects from accidental deletion or overwriting by preserving, retrieving, and restoring every version of every object stored in an S3 bucket2. By enabling S3 Versioning on the new bucket, the solution can prevent modifications or deletions of the files by anyone.

Amazon S3 Object Lock is a feature that allows users to store objects using a write-once- read-many (WORM) model. It can help prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. It requires S3 Versioning to be enabled on the bucket3. By using S3 Object Lock with a retention period in accordance with the designated date, the solution can prohibit modifications or deletions of the files by anyone before that date.

Amazon S3 bucket policies are JSON documents that define access permissions for a bucket and its objects. They can be used to grant or deny access to specific users or groups based on conditions such as IP address, time of day, or source bucket. By setting an S3 bucket policy to allow read-only access to the objects, the solution can ensure that the files are publicly readable.

* A. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Grant read-only 1AM permissions to any AWS principals that access the S3 bucket until the designated date. This solution will not meet the requirement of prohibiting modifications or deletions of the files by anyone before a designated future date, as IAM permissions only apply to AWS principals, not to public users. It also does not use any feature to prevent accidental or intentional deletion or overwriting of the files.

* C. Create a new Amazon S3 bucket with S3 Versioning enabled Configure an event trigger to run an AWS Lambda function in case of object modification or deletion. Configure the Lambda func-tion to replace the objects with the original versions from a private S3 bucket. This solution will not meet the requirement of prohibiting modifications or deletions of the files by anyone before a designated future date, as it only reacts to object modification or deletion events after they occur. It also involves creating and managing an additional resource (Lambda function) and a private S3 bucket.

* D. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Select the folder that contains the files. Use S3 Object Lock with a retention period in accordance with the designated date. Grant read-only 1AM permissions to any AWS principals that access the S3 bucket. This solution will not meet the requirement of prohibiting modifications or deletions of the files by anyone before a designated future date, as it does not enable S3 Versioning on the bucket, which is required for using S3 Object Lock. It also does not allow read-only access to public users.

Reference URL: https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html

630. - (Topic 4)

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

Which solution meets these requirements?

A. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance

and specifying the Multi-AZ option.

B. Create a new RDS Multi-AZ deployment. Take a snapshot of the current RDS instance and restore the new Multi-AZ deployment with the snapshot.

C. Create a read-only replica of the PostgreSQL database in another Availability Zone. Use Amazon Route 53 weighted record sets to distribute requests across the databases.

D. Place the RDS for PostgreSQL database in an Amazon EC2 Auto Scaling group with a minimum group size of two. Use Amazon Route 53 weighted record sets to distribute requests across instances.

Answer: A

Explanation: https://aws.amazon.com/rds/features/multi-az/ To convert an existing Single- AZ DB Instance to a Multi-AZ deployment, use the "Modify" option corresponding to your DB Instance in the AWS Management Console.

631. - (Topic 4)

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

What should a solutions architect do to meet these requirements?

A. Set up an Amazon ElastiCache for Memcached cluster to cache the scores for the web application to display.

B. Set up an Amazon ElastiCache for Redis cluster to compute and cache the scores for the web application to display.

C. Place an Amazon CloudFront distribution in front of the web application to cache the scoreboard in a section of the application.

D. Create a read replica on Amazon RDS for MySQL to run queries to compute the scoreboard and serve the read traffic to the web application.

Answer: B

Explanation: This answer is correct because it meets the requirements of displaying a top- 10 scoreboard in near-real time and offering the ability to stop and restore the game while preserving the current scores. Amazon ElastiCache for Redis is a blazing fast in-memory data store that provides sub-millisecond latency

to power internet-scale real-time applications. You can use Amazon ElastiCache for Redis to set up an ElastiCache for Redis cluster to compute and cache the scores for the web application to display. You can use Redis data structures such as sorted sets and hashes to store and rank the scores of the players, and use Redis commands such as ZRANGE and ZADD to retrieve and update the scores efficiently. You can also use Redis persistence features such as snapshots and append-only files (AOF) to enable point-in-time recovery of your data, which can help you stop and restore the game while preserving the current scores.

References:

- https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/WhatIs.html
- https://redis.io/topics/data-types
- https://redis.io/topics/persistence

632. - (Topic 4)

A solutions architect is implementing a complex Java application with a MySQL database. The Java application must be deployed on Apache Tomcat and must be highly available.

What should the solutions architect do to meet these requirements?

A. Deploy the application in AWS Lambda. Configure an Amazon API Gateway API to connect with the Lambda functions.

B. Deploy the application by using AWS Elastic Beanstalk. Configure a load-balanced environment and a rolling deployment policy.

C. Migrate the database to Amazon ElastiCache. Configure the ElastiCache security group to allow access from the application.

D. Launch an Amazon EC2 instance. Install a MySQL server on the EC2 instance. Configure the application on the server. Create an AMI. Use the AMI to create a launch template with an Auto scaling group.

Answer: B

Explanation: AWS Elastic Beanstalk provides an easy and quick way to deploy, manage, and scale applications. It supports a variety of platforms, including Java and Apache Tomcat. By using Elastic Beanstalk, the solutions architect can upload the Java application and configure the environment to run Apache Tomcat.

633. - (Topic 4)

A financial services company wants to shut down two data centers and migrate more than 100 TB of data to AWS. The data has an intricate directory structure with millions of small files stored in deep hierarchies of subfolders. Most of the data is unstructured, and the company's file storage consists of SMB-based storage types from multiple vendors. The company does not want to change its applications to access the data after migration.

What should a solutions architect do to meet these requirements with the LEAST operational overhead?

A. Use AWS Direct Connect to migrate the data to Amazon S3.

B. Use AWS DataSync to migrate the data to Amazon FSx for Lustre.

C. Use AWS DataSync to migrate the data to Amazon FSx for Windows File Server.

D. Use AWS Direct Connect to migrate the data on-premises file storage to an AWS Storage Gateway volume gateway.

Answer: C

Explanation: AWS DataSync is a data transfer service that simplifies, automates, and accelerates moving data between on-premises storage systems and AWS storage services over the internet or AWS Direct Connect1. AWS DataSync can transfer data to Amazon FSx for Windows File Server, which is a fully managed file system that is accessible over the industry-standard Server Message Block (SMB) protocol. Amazon FSx for Windows File Server is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration2. This solution meets the requirements of the question because:

- It can migrate more than 100 TB of data to AWS within a reasonable time frame, as AWS DataSync is optimized for high-speed and efficient data transfer1.
- It can preserve the intricate directory structure and the millions of small files stored in deep hierarchies of subfolders, as AWS DataSync can handle complex file structures and metadata, such as file names, permissions, and timestamps1.
- It can avoid changing the applications to access the data after migration, as Amazon FSx for Windows File Server supports the same SMB protocol and Windows Server features that the company's on-premises file storage uses2.
- It can reduce the operational overhead, as AWS DataSync and Amazon FSx for Windows File Server are fully managed services that handle the tasks of setting up, configuring, and maintaining the data

transfer and the file system12.

634. - (Topic 4)

A company has applications that run on Amazon EC2 instances. The EC2 instances connect to Amazon RDS databases by using an 1AM role that has associated policies. The company wants to use AWS Systems Manager to patch the EC2 instances without disrupting the running applications.

Which solution will meet these requirements?

A. Create a new 1AM role. Attach the AmazonSSMManagedInstanceCore policy to the new 1AM role. Attach the new 1AM role to the EC2 instances and the existing 1AM role.

B. Create an 1AM user. Attach the AmazonSSMManagedInstanceCore policy to the 1AM user. Configure Systems Manager to use the 1AM user to manage the EC2 instances.

C. Enable Default Host Configuration Management in Systems Manager to manage the EC2 instances.

D. Remove the existing policies from the existing 1AM role. Add the AmazonSSMManagedInstanceCore policy to the existing 1AM role.

Answer: C

Explanation: The most suitable solution for the company's requirements is to enable Default Host Configuration Management in Systems Manager to manage the EC2 instances. This solution will allow the company to patch the EC2 instances without disrupting the running applications and without manually creating or modifying IAM roles or users.

Default Host Configuration Management is a feature of AWS Systems Manager that enables Systems Manager to manage EC2 instances automatically as managed instances. A managed instance is an EC2 instance that is configured for use with Systems Manager. The benefits of managing instances with Systems Manager include the following:

- Connect to EC2 instances securely using Session Manager.
- Perform automated patch scans using Patch Manager.
- View detailed information about instances using Systems Manager Inventory.
- Track and manage instances using Fleet Manager.
- Keep SSM Agent up to date automatically.

Default Host Configuration Management makes it possible to manage EC2 instances without having to manually create an IAM instance profile. Instead, Default Host Configuration Management creates and

applies a default IAM role to ensure that Systems Manager has permissions to manage all instances in the Region and account where it is activated. If the permissions provided are not sufficient for the use case, the default IAM role can be modified or replaced with a custom role1.

The other options are not correct because they either have more operational overhead or do not meet the requirements. Creating a new IAM role, attaching the AmazonSSMManagedInstanceCore policy to the new IAM role, and attaching the new IAM

role and the existing IAM role to the EC2 instances is not correct because this solution requires manual creation and management of IAM roles, which adds complexity and cost to the solution. The AmazonSSMManagedInstanceCore policy is a managed policy that grants permissions for Systems Manager core functionality2. Creating an IAM user, attaching the AmazonSSMManagedInstanceCore policy to the IAM user, and configuring Systems Manager to use the IAM user to manage the EC2 instances is not correct because this solution requires manual creation and management of IAM users, which adds complexity and cost to the solution. An IAM user is an identity within an AWS account that has specific permissions for a single person or application3. Removing the existing policies from the existing IAM role and adding the AmazonSSMManagedInstanceCore policy to the existing IAM role is not correct because this solution may disrupt the running applications that rely on the existing policies for accessing RDS databases. An IAM role is an identity within an AWS account that has specific permissions for a service or entity4.

References:

- AWS managed policy: AmazonSSMManagedInstanceCore
- IAM users
- IAM roles
- Default Host Management Configuration - AWS Systems Manager

635. - (Topic 4)

A company stores its data on premises. The amount of data is growing beyond the company's available capacity.

The company wants to migrate its data from the on-premises location to an Amazon S3 bucket The company needs a solution that will automatically validate the integrity of the data after the transfer

Which solution will meet these requirements?

A. Order an AWS Snowball Edge device Configure the Snowball Edge device to perform the online data transfer to an S3 bucket.

B. Deploy an AWS DataSync agent on premises. Configure the DataSync agent to perform the online data transfer to an S3 bucket.

C. Create an Amazon S3 File Gateway on premises. Configure the S3 File Gateway to perform the online data transfer to an S3 bucket

D. Configure an accelerator in Amazon S3 Transfer Acceleration on premises. Configure the accelerator to perform the online data transfer to an S3 bucket.

Answer: B

Explanation: it allows the company to migrate its data from the on-premises location to an Amazon S3 bucket and automatically validate the integrity of the data after the transfer. By deploying an AWS DataSync agent on premises, the company can use a fully managed data transfer service that makes it easy to move large amounts of data to and from AWS. By configuring the DataSync agent to perform the online data transfer to an S3 bucket, the company can take advantage of DataSync's features, such as encryption, compression, bandwidth throttling, and data validation. DataSync automatically verifies data integrity at both source and destination after each transfer task. References:

- AWS DataSync
- Deploying an Agent for AWS DataSync
- How AWS DataSync Works

636. - (Topic 4)

A company is developing a mobile gaming app in a single AWS Region. The app runs on multiple Amazon EC2 instances in an Auto Scaling group. The company stores the app data in Amazon DynamoDB. The app communicates by using TCP traffic and UDP traffic between the users and the servers. The application will be used globally. The company wants to ensure the lowest possible latency for all users.

Which solution will meet these requirements?

A. Use AWS Global Accelerator to create an accelerator. Create an Application Load Balancer (ALB) behind an accelerator endpoint that uses Global Accelerator integration and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the ALB.

B. Use AWS Global Accelerator to create an accelerator. Create a Network Load Balancer (NLB) behind an

accelerator endpoint that uses Global Accelerator integration and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the NLB

C. Create an Amazon CloudFront content delivery network (CDN) endpoint. Create a Network Load Balancer (NLB) behind the endpoint and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the NLB. Update CloudFront to use the NLB as the origin.

D. Create an Amazon Cloudfront content delivery network (CDN) endpoint. Create an Application Load Balancer (ALB) behind the endpoint and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the ALB. Update CloudFront to use the ALB as the origin

Answer: B

Explanation:

AWS Global Accelerator is a networking service that improves the performance and availability of applications for global users. It uses the AWS global network to route user traffic to the optimal endpoint based on performance and health. It also provides static IP addresses that act as a fixed entry point to the applications and support both TCP and UDP protocols1. By using AWS Global Accelerator, the solution can ensure the lowest possible latency for all users.

* A. Use AWS Global Accelerator to create an accelerator. Create an Application Load Balancer (ALB) behind an accelerator endpoint that uses Global Accelerator integration and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the ALB. This solution will not work, as ALB does not support UDP protoco2l.

* C. Create an Amazon CloudFront content delivery network (CDN) endpoint. Create a Network Load Balancer (NLB) behind the endpoint and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the NLB. Update CloudFront to use the NLB as the origin. This solution will not work, as CloudFront does not support UDP protocol3.

* D. Create an Amazon Cloudfront content delivery network (CDN) endpoint. Create an Application Load Balancer (ALB) behind the endpoint and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the ALB. Update CloudFront to use the ALB as the origin. This solution will not work, as CloudFront and ALB do not support UDP protocol23.

Reference URL: https://aws.amazon.com/global-accelerator/

637. - (Topic 4)

A company has migrated multiple Microsoft Windows Server workloads to Amazon EC2 instances that run in the us-west-1 Region. The company manually backs up the workloads to create an image as needed.

In the event of a natural disaster in the us-west-1 Region, the company wants to recover workloads quickly in the us-west-2 Region. The company wants no more than 24 hours of data loss on the EC2 instances. The company also wants to automate any backups of the EC2 instances.

Which solutions will meet these requirements with the LEAST administrative effort? (Select TWO.)

A. Create an Amazon EC2-backed Amazon Machine Image (AMI) lifecycle policy to create a backup based on tags. Schedule the backup to run twice daily. Copy the image on demand.

B. Create an Amazon EC2-backed Amazon Machine Image (AMI) lifecycle policy to create a backup based on tags. Schedule the backup to run twice daily. Configure the copy to the us-west-2 Region.

C. Create backup vaults in us-west-1 and in us-west-2 by using AWS Backup. Create a backup plan for the EC2 instances based on tag values. Create an AWS Lambda function to run as a scheduled job to copy the backup data to us-west-2.

D. Create a backup vault by using AWS Backup. Use AWS Backup to create a backup plan for the EC2 instances based on tag values. Define the destination for the copy as us-west-2. Specify the backup schedule to run twice daily.

E. Create a backup vault by using AWS Backup. Use AWS Backup to create a backup plan for the EC2 instances based on tag values. Specify the backup schedule to run twice daily. Copy on demand to us-west-2.

Answer: B,D

Explanation: Option B suggests using an EC2-backed Amazon Machine Image (AMI) lifecycle policy to automate the backup process. By configuring the policy to run twice daily and specifying the copy to the us-west-2 Region, the company can ensure regular backups are created and copied to the alternate region.

Option D proposes using AWS Backup, which provides a centralized backup management solution. By creating a backup vault and backup plan based on tag values, the company can automate the backup process for the EC2 instances. The backup schedule can be set to run twice daily, and the destination for the copy can be defined as the us-west-2 Region.

Both options automate the backup process and include copying the backups to the us- west-2 Region, ensuring data resilience in the event of a disaster. These solutions minimize administrative effort by leveraging automated backup and copy mechanisms provided by AWS services.

638. - (Topic 4)

A company has a web application that includes an embedded NoSQL database. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group in a single Availability Zone.

A recent increase in traffic requires the application to be highly available and for the database to be eventually consistent

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

A. Replace the ALB with a Network Load Balancer Maintain the embedded NoSQL database with its replication service on the EC2 instances.

B. Replace the ALB with a Network Load Balancer Migrate the embedded NoSQL database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS).

C. Modify the Auto Scaling group to use EC2 instances across three Availability Zones. Maintain the embedded NoSQL database with its replication service on the EC2 instances.

D. Modify the Auto Scaling group to use EC2 instances across three Availability Zones. Migrate the embedded NoSQL database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS).

Answer: D

Explanation: This solution will meet the requirements of high availability and eventual consistency with the least operational overhead. By modifying the Auto Scaling group to use EC2 instances across three Availability Zones, the web application can handle the increase in traffic and tolerate the failure of one or two Availability Zones. By migrating the embedded NoSQL database to Amazon DynamoDB, the company can benefit from a fully managed, scalable, and reliable NoSQL database service that supports eventual consistency. AWS Database Migration Service (AWS DMS) is a cloud service that makes it easy to migrate relational databases, data warehouses, NoSQL databases, and other types of data stores. AWS DMS can migrate the embedded NoSQL database to Amazon DynamoDB with minimal downtime and zero data loss.

References: AWS Database Migration Service (AWS DMS), Amazon DynamoDB Features, Amazon EC2 Auto Scaling

639. - (Topic 4)

A company has a small Python application that processes JSON documents and outputs the results to an on-premises SQL database. The application runs thousands of times each day. The company wants to move the application to the AWS Cloud. The company needs a highly available solution that maximizes scalability and minimizes operational overhead.

Which solution will meet these requirements?

A. Place the JSON documents in an Amazon S3 bucket. Run the Python code on multiple Amazon EC2 instances to process the documents. Store the results in an Amazon Aurora DB cluster

B. Place the JSON documents in an Amazon S3 bucket. Create an AWS Lambda function that runs the Python code to process the documents as they arrive in the S3 bucket. Store the results in an Amazon Aurora DB cluster.

C. Place the JSON documents in an Amazon Elastic Block Store (Amazon EBS) volume. Use the EBS Multi-Attach feature to attach the volume to multiple Amazon EC2 instances.

Run the Python code on the EC2 instances to process the documents. Store the results on an Amazon RDS DB instance.

D. Place the JSON documents in an Amazon Simple Queue Service (Amazon SQS) queue as messages Deploy the Python code as a container on an Amazon Elastic Container Service (Amazon ECS) cluster that is configured with the Amazon EC2 launch type. Use the container to process the SQS messages. Store the results on an Amazon RDS DB instance.

Answer: B

Explanation: By placing the JSON documents in an S3 bucket, the documents will be stored in a highly durable and scalable object storage service. The use of AWS Lambda allows the company to run their Python code to process the documents as they arrive in the S3 bucket without having to worry about the underlying infrastructure. This also allows for horizontal scalability, as AWS Lambda will automatically scale the number of instances of the function based on the incoming rate of requests. The results can be stored in an Amazon Aurora DB cluster, which is a fully-managed, high-performance database service that is compatible with MySQL and PostgreSQL. This will provide the necessary durability and scalability for the results of the processing.

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

640. - (Topic 4)

A company is planning to use an Amazon DynamoDB table for data storage. The company is concerned about cost optimization. The table will not be used on most mornings. In the evenings, the read and write traffic will often be unpredictable. When traffic spikes occur, they will happen very quickly.

What should a solutions architect recommend?

A. Create a DynamoDB table in on-demand capacity mode.

B. Create a DynamoDB table with a global secondary index

C. Create a DynamoDB table with provisioned capacity and auto scaling.

D. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table

Answer: A

Explanation: Provisioned capacity is best if you have relatively predictable application traffic, run applications whose traffic is consistent, and ramps up or down gradually. On- demand capacity mode is best when you have unknown workloads, unpredictable application traffic and also if you only want to pay exactly for what you use. The on-demand pricing model is ideal for bursty, new, or unpredictable workloads whose traffic can spike in seconds or minutes, and when under-provisioned capacity would impact the user experience. https://docs.aws.amazon.com/wellarchitected/latest/serverless-applications- lens/capacity.html

641. - (Topic 4)

A company is expecting rapid growth in the near future. A solutions architect needs to configure existing users and grant permissions to new users on AWS. The solutions architect has decided to create 1AM groups. The solutions architect will add the new users to 1AM groups based on department.

Which additional action is the MOST secure way to grant permissions to the new users?

A. Apply service control policies (SCPs) to manage access permissions.

B. Create IAM roles that have least privilege permission. Attach the roles to the 1AM groups.

C. Create an IAM policy that grants least privilege permission. Attach the policy to the 1AM groups.

D. Create 1AM roles. Associate the roles with a permissions boundary that defines the maximum permissions.

Answer: C

Explanation: An IAM policy is a document that defines the permissions for an IAM identity (such as a user, group, or role). You can use IAM policies to grant permissions to existing users and groups based on department. You can create an IAM policy that grants least privilege permission, which means that you only

grant the minimum permissions required for the users to perform their tasks. You can then attach the policy to the IAM groups, which will apply the policy to all the users in those groups. This solution will reduce operational costs and simplify configuration and management of permissions. References: https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

642. - (Topic 4)

A company stores data in Amazon S3. According to regulations, the data must not contain personally identifiable information (PII). The company recently discovered that S3 buckets have some objects that contain PII. The company needs to automatically detect PII in S3 buckets and to notify the company's security team.

Which solution will meet these requirements?

A. Use Amazon Macie. Create an Amazon EventBridge rule to filter the SensitiveData event type from Macie findings and to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.

B. Use Amazon GuardDuty. Create an Amazon EventBridge rule to filter the CRITICAL event type from GuardDuty findings and to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.

C. Use Amazon Macie. Create an Amazon EventBridge rule to filter the SensitiveData:S30bject/Personal event type from Macie findings and to send an Amazon Simple Queue Service (Amazon SQS) notification to the security team.

D. Use Amazon GuardDuty. Create an Amazon EventBridge rule to filter the CRITICAL event type from GuardDuty findings and to send an Amazon Simple Queue Service (Amazon SQS) notification to the security team.

Answer: A

Explanation: Amazon Macie can also send its findings to Amazon EventBridge, which is a serverless event bus that makes it easy to connect applications using data from a variety of sources. You can create an EventBridge rule that filters the SensitiveData event type from Macie findings and sends an Amazon SNS notification to the security team. Amazon SNS is a fully managed messaging service that enables you to send messages to subscribers or other applications. References: https://docs.aws.amazon.com/macie/latest/userguide/macie-findings.html#macie-findings- eventbridge

643. - (Topic 4)

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

What should a solutions architect do to protect the application?

A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address.

B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address.

C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.

D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.

Answer: B

Explanation: AWS WAF is a web application firewall that helps protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF allows users to create rules that block, allow, or count web requests based on customizable web security rules. One of the types of rules that can be created is an IP match rule, which allows users to specify a list of IP addresses or IP address ranges that they want to allow or block. By modifying the configuration of AWS WAF to add an IP match condition to block the malicious IP address, the solution architect can prevent the attacker from accessing the website through the CloudFront distribution and the ALB.

The other options are not correct because they do not effectively block the malicious IP address from accessing the website. Modifying the network ACL on the CloudFront distribution or the EC2 instances in the target groups behind the ALB will not work because network ACLs are stateless and do not evaluate traffic at the application layer. Modifying the security groups for the EC2 instances in the target groups behind the ALB will not work because security groups are stateful and only evaluate traffic at the instance level, not at the load balancer level.

References:

- AWS WAF
- How AWS WAF works
- Working with IP match conditions

644. - (Topic 4)

A company runs an application on Amazon EC2 instances. The company needs to implement a disaster recovery (DR) solution for the application. The DR solution needs to have a recovery time objective (RTO) of less than 4 hours. The DR solution also needs to use the fewest possible AWS resources during normal operations.

Which solution will meet these requirements in the MOST operationally efficient way?

A. Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS Lambda and custom scripts.

B. Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS CloudFormation.

C. Launch EC2 instances in a secondary AWS Region. Keep the EC2 instances in the secondary Region active at all times.

D. Launch EC2 instances in a secondary Availability Zone. Keep the EC2 instances in the secondary Availability Zone active at all times.

Answer: B

Explanation: it allows the company to implement a disaster recovery (DR) solution for the application that has a recovery time objective (RTO) of less than 4 hours and uses the fewest possible AWS resources during normal operations. By creating Amazon Machine Images (AMIs) to back up the EC2 instances and copying the AMIs to a secondary AWS Region, the company can create point-in-time snapshots of the application and store them in a different geographical location. By automating infrastructure deployment in the secondary Region by using AWS CloudFormation, the company can quickly launch a stack of resources from a template in case of a disaster. This is a cost-effective and operationally efficient way to implement a DR solution for EC2 instances. References:

- Amazon Machine Images (AMI)
- Copying an AMI

- AWS CloudFormation
- Working with Stacks

645. - (Topic 4)

A company has deployed its newest product on AWS. The product runs in an Auto Scaling group behind a Network Load Balancer. The company stores the product's objects in an Amazon S3 bucket.

The company recently experienced malicious attacks against its systems. The company needs a solution that continuously monitors for malicious activity in the AWS account, workloads, and access patterns to the S3 bucket. The solution must also report suspicious activity and display the information on a dashboard.

Which solution will meet these requirements?

A. Configure Amazon Made to monitor and report findings to AWS Config.

B. Configure Amazon Inspector to monitor and report findings to AWS CloudTrail.

C. Configure Amazon GuardDuty to monitor and report findings to AWS Security Hub.

D. Configure AWS Config to monitor and report findings to Amazon EventBridge.

Answer: C

Explanation: Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior across the AWS account and workloads. GuardDuty analyzes data sources such as AWS CloudTrail event logs, Amazon VPC Flow

Logs, and DNS logs to identify potential threats such as compromised instances, reconnaissance, port scanning, and data exfiltration. GuardDuty can report its findings to AWS Security Hub, which is a service that provides a comprehensive view of the security posture of the AWS account and workloads. Security Hub aggregates, organizes, and prioritizes security alerts from multiple AWS services and partner solutions, and displays them on a dashboard. This solution will meet the requirements, as it enables continuous monitoring, reporting, and visualization of malicious activity in the AWS account, workloads, and access patterns to the S3 bucket.

References:

- 1 provides an overview of Amazon GuardDuty and its benefits.
- 2 explains how GuardDuty generates and reports findings based on threat detection.
- 3 provides an overview of AWS Security Hub and its benefits.
- 4 describes how Security Hub collects and displays findings from multiple sources on a dashboard

646. - (Topic 4)

A company's website handles millions of requests each day, and the number of requests continues to increase. A solutions architect needs to improve the response time of the web application. The solutions architect determines that the application needs to decrease latency when retrieving product details from the Amazon DynamoDB table.

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

A. Set up a DynamoDB Accelerator (DAX) cluster. Route all read requests through DAX.

B. Set up Amazon ElastiCache for Redis between the DynamoDB table and the web application. Route all read requests through Redis.

C. Set up Amazon ElastiCache for Memcached between the DynamoDB table and the web application. Route all read requests through Memcached.

D. Set up Amazon DynamoDB Streams on the table, and have AWS Lambda read from the table and populate Amazon ElastiCache. Route all read requests through ElastiCache.

Answer: A

Explanation: it allows the company to improve the response time of the web application and decrease latency when retrieving product details from the Amazon DynamoDB table.

By setting up a DynamoDB Accelerator (DAX) cluster, the company can use a fully managed, highly available, in-memory cache for DynamoDB that delivers up to a 10x performance improvement. By routing all read requests through DAX, the company can reduce the number of read operations on the DynamoDB table and improve the user experience. References:

- Amazon DynamoDB Accelerator (DAX)
- Using DAX with DynamoDB

647. - (Topic 4)

A company has a stateless web application that runs on AWS Lambda functions that are invoked by Amazon API Gateway. The company v wants to deploy the application across multiple AWS Regions to provide Regional failover capabilities.

What should a solutions architect do to route traffic to multiple Regions?

A. Create Amazon Route 53 health checks for each Region. Use an active-active failover configuration.

B. Create an Amazon CloudFront distribution with an origin for each Region. Use CloudFront health checks to route traffic.

C. Create a transit gateway. Attach the transit gateway to the API Gateway endpoint in each Region. Configure the transit gateway to route requests.

D. Create an Application Load Balancer in the primary Region. Set the target group to point to the API Gateway endpoint hostnames in each Region.

Answer: C

Explanation: This answer is correct because it provides Regional failover capabilities for the online gaming application by using AWS Global Accelerator. AWS Global Accelerator is a networking service that helps you improve the availability, performance, and security of your public applications. Global Accelerator provides two global static public IPs that act as a fixed entry point to your application endpoints, such as NLBs, in different AWS Regions. Global Accelerator uses the AWS global network to route traffic to the optimal regional endpoint based on health, client location, and policies that you configure. Global Accelerator also terminates TCP and UDP traffic at the edge locations, which reduces the number of hops and improves the network performance. By adding AWS Global Accelerator in front of the NLBs, you can achieve Regional failover for your online gaming application.

References:

- https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global- accelerator.html
- https://aws.amazon.com/global-accelerator/

648. - (Topic 4)

A company is using a content management system that runs on a single Amazon EC2 instance. The EC2 instance contains both the web server and the database software. The company must make its website platform highly available and must enable the website to scale to meet user demand.

What should a solutions architect recommend to meet these requirements?

A. Move the database to Amazon RDS, and enable automatic backups. Manually launch another EC2 instance in the same Availability Zone. Configure an Application Load Balancer in the Availability Zone, and set the two instances as targets.

B. Migrate the database to an Amazon Aurora instance with a read replica in the same Availability Zone as the existing EC2 instance. Manually launch another EC2 instance in the same Availability Zone. Configure

an Application Load Balancer, and set the two EC2 instances as targets.

C. Move the database to Amazon Aurora with a read replica in another Availability Zone. Create an Amazon Machine Image (AMI) from the EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

D. Move the database to a separate EC2 instance, and schedule backups to Amazon S3. Create an Amazon Machine Image (AMI) from the original EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

Answer: C

Explanation: This approach will provide both high availability and scalability for the website platform. By moving the database to Amazon Aurora with a read replica in another availability zone, it will provide a failover option for the database. The use of an Application Load Balancer and an Auto Scaling group across two availability zones allows for automatic scaling of the website to meet increased user demand. Additionally, creating an AMI from the original EC2 instance allows for easy replication of the instance in case of failure.

649. - (Topic 4)

A company uses Amazon S3 to store high-resolution pictures in an S3 bucket. To minimize application changes, the company stores the pictures as the latest version of an S3 object

The company needs to retain only the two most recent versions ot the pictures.

The company wants to reduce costs. The company has identified the S3 bucket as a large expense.

Which solution will reduce the S3 costs with the LEAST operational overhead?

A. Use S3 Lifecycle to delete expired object versions and retain the two most recent versions.

B. Use an AWS Lambda function to check for older versions and delete all but the two most recent versions

C. Use S3 Batch Operations to delete noncurrent object versions and retain only the two most recent versions

D. Deactivate versioning on the S3 bucket and retain the two most recent versions.

Answer: A

Explanation: S3 Lifecycle is a feature that allows you to automate the management of your S3 objects based on predefined rules. You can use S3 Lifecycle to delete expired object versions and retain the two most recent versions by creating a lifecycle configuration rule that applies to all objects in the bucket and

specifies the expiration action for noncurrent versions. This way, you can reduce the storage costs of your S3 bucket without requiring any application changes or manual intervention. S3 Lifecycle runs once a day and marks the eligible object versions for deletion. You are no longer charged for the objects that are marked for deletion. S3 Lifecycle is the most cost-effective and simple solution among the options.

* B. Use an AWS Lambda function to check for older versions and delete all but the two most recent versions. This option is not optimal because it requires you to write, test, and maintain a custom Lambda function that scans the S3 bucket for older versions and deletes them. This can incur additional costs for Lambda invocations and increase the operational complexity and overhead. Moreover, you need to ensure that your Lambda function has the appropriate permissions and error handling mechanisms to perform the deletion operation.

* C. Use S3 Batch Operations to delete noncurrent object versions and retain only the two most recent versions. This option is not ideal because S3 Batch Operations is designed for performing large-scale operations on S3 objects, such as copying, tagging, restoring, or invoking a Lambda function. To use S3 Batch Operations to delete noncurrent object versions, you need to provide a manifest file that lists the object versions that you want to delete. This can be challenging and time-consuming to generate and update. Moreover, S3 Batch Operations charges you for each operation that you perform, which can increase your costs.

* D. Deactivate versioning on the S3 bucket and retain the two most recent versions. This option is not feasible because deactivating versioning on an S3 bucket does not delete the existing object versions. Instead, it prevents new versions from being created. Therefore, you still need to delete the older versions manually or use another method to do so. Additionally, deactivating versioning can compromise the data protection and recovery capabilities of your S3 bucket.

References:

- 1 Considering four different replication options for data in Amazon S3 | AWS Storage Blog
- 2 Using AWS Lambda with Amazon S3 batch operations - AWS Lambda
- 3 Empty an Amazon S3 bucket with a lifecycle configuration rule
- 4 Amazon S3 - Lifecycle Management - GeeksforGeeks

650. - (Topic 4)

A company is developing a mobile game that streams score updates to a backend processor and then

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

What should the solutions architect do to meet these requirements?

A. Push score updates to Amazon Kinesis Data Streams Process the updates in Kinesis Data Streams with AWS Lambda Store the processed updates in Amazon DynamoDB.

B. Push score updates to Amazon Kinesis Data Streams. Process the updates with a fleet of Amazon EC2 instances set up for Auto Scaling Store the processed updates in Amazon Redshift.

C. Push score updates to an Amazon Simple Notification Service (Amazon SNS) topic Subscribe an AWS Lambda function to the SNS topic to process the updates. Store the processed updates in a SQL database running on Amazon EC2.

D. Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue. Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SQS queue. Store the processed updates in an Amazon RDS Multi-AZ DB instance.

Answer: A

Explanation: Amazon Kinesis Data Streams is a scalable and reliable service that can ingest, buffer, and process streaming data in real-time. It can handle large traffic spikes and preserve the order of the incoming data records. AWS Lambda is a serverless compute service that can process the data streams from Kinesis Data Streams without requiring any infrastructure management. It can also scale automatically to match the throughput of the data stream. Amazon DynamoDB is a fully managed, highly available, and fast NoSQL database that can store the processed updates from Lambda. It can also handle high write throughput and provide consistent performance. By using these services, the solutions architect can design a solution that meets the requirements of the company with the least operational overhead.

651. - (Topic 4)

A solutions architect is using an AWS CloudFormation template to deploy a three-tier web application. The web application consists of a web tier and an application tier that stores and retrieves user data in Amazon DynamoDB tables. The web and application tiers are hosted on Amazon EC2 instances, and the database tier is not publicly accessible. The application EC2 instances need to access the DynamoDB tables without

exposing API credentials in the template.

What should the solutions architect do to meet these requirements?

A. Create an IAM role to read the DynamoDB tables. Associate the role with the application instances by referencing an instance profile.

B. Create an IAM role that has the required permissions to read and write from the DynamoDB tables. Add the role to the EC2 instance profile, and associate the instance profile with the application instances.

C. Use the parameter section in the AWS CloudFormation template to have the user input access and secret keys from an already-created IAM user that has the required permissions to read and write from the DynamoDB tables.

D. Create an IAM user in the AWS CloudFormation template that has the required permissions to read and write from the DynamoDB tables. Use the GetAtt function to retrieve the access and secret keys, and pass them to the application instances through the user data.

Answer: B

Explanation: it allows the application EC2 instances to access the DynamoDB tables without exposing API credentials in the template. By creating an IAM role that has the required permissions to read and write from the DynamoDB tables and adding it to the EC2 instance profile, the application instances can use temporary security credentials that are automatically rotated by AWS. This is a secure and best practice way to grant access to AWS resources from EC2 instances. References:

- IAM Roles for Amazon EC2
- Using Instance Profiles

652. - (Topic 4)

A company has a workload in an AWS Region. Customers connect to and access the workload by using an Amazon API Gateway REST API. The company uses Amazon Route 53 as its DNS provider. The company wants to provide individual and secure URLs for all customers.

Which combination of steps will meet these requirements with the MOST operational efficiency? (Select THREE.)

A. Register the required domain in a registrar. Create a wildcard custom domain name in a Route 53 hosted zone and record in the zone that points to the API Gateway endpoint.

B. Request a wildcard certificate that matches the domains in AWS Certificate Manager (ACM) in a different

Region.

C. Create hosted zones for each customer as required in Route 53. Create zone records that point to the API Gateway endpoint.

D. Request a wildcard certificate that matches the custom domain name in AWS Certificate Manager (ACM) in the same Region.

E. Create multiple API endpoints for each customer in API Gateway.

F. Create a custom domain name in API Gateway for the REST API. Import the certificate from AWS Certificate Manager (ACM).

Answer: A,D,F

Explanation: To provide individual and secure URLs for all customers using an API Gateway REST API, you need to do the following steps:

➪ A. Register the required domain in a registrar. Create a wildcard custom domain name in a Route 53 hosted zone and record in the zone that points to the API Gateway endpoint. This step will allow you to use a custom domain name for your API instead of the default one generated by API Gateway. A wildcard custom domain name means that you can use any subdomain under your domain name (such as customer1.example.com or customer2.example.com) to access your API. You need to register your domain name with a registrar (such as Route 53 or a third-party registrar) and create a hosted zone in Route 53 for your domain name. You also need to create a record in the hosted zone that points to the API Gateway endpoint using an alias record.

➪ D. Request a wildcard certificate that matches the custom domain name in AWS Certificate Manager (ACM) in the same Region. This step will allow you to secure your API with HTTPS using a certificate issued by ACM. A wildcard certificate means that it can match any subdomain under your domain name (such as

*.example.com). You need to request or import a certificate in ACM that matches your custom domain name and verify that you own the domain name. You also need to request the certificate in the same Region as your API.

➪ F. Create a custom domain name in API Gateway for the REST API. Import the certificate from AWS Certificate Manager (ACM). This step will allow you to associate your custom domain name with your API and use the certificate from ACM to enable HTTPS. You need to create a custom domain name in API Gateway for the REST API and specify the certificate ARN from ACM. You also need

to create a base path mapping that maps a path from your custom domain name to your API stage.

References: https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-custom-domains.html https://docs.aws.amazon.com/acm/latest/userguide/gs-acm- request.html

653. - (Topic 4)

A company is designing a web application on AWS The application will use a VPN connection between the company's existing data centers and the company's VPCs. The company uses Amazon Route 53 as its DNS service. The application must use private DNS records to communicate with the on-premises services from a VPC. Which solution will meet these requirements in the MOST secure manner?

A. Create a Route 53 Resolver outbound endpoint. Create a resolver rule. Associate the resolver rule with the VPC

B. Create a Route 53 Resolver inbound endpoint. Create a resolver rule. Associate the resolver rule with the VPC.

C. Create a Route 53 private hosted zone. Associate the private hosted zone with the VPC.

D. Create a Route 53 public hosted zone. Create a record for each service to allow service communication.

Answer: A

Explanation: To meet the requirements of the web application in the most secure manner, the company should create a Route 53 Resolver outbound endpoint, create a resolver rule, and associate the resolver rule with the VPC. This solution will allow the application to use private DNS records to communicate with the on-premises services from a VPC. Route 53 Resolver is a service that enables DNS resolution between on-premises networks and AWS VPCs. An outbound endpoint is a set of IP addresses that Resolver uses to forward DNS queries from a VPC to resolvers on an on-premises network. A resolver rule is a rule that specifies the domain names for which Resolver forwards DNS queries to the IP addresses that you specify in the rule. By creating an outbound endpoint and a resolver rule, and associating them with the VPC, the company can securely resolve DNS queries for the on-premises services using private DNS records12.

The other options are not correct because they do not meet the requirements or are not secure. Creating a Route 53 Resolver inbound endpoint, creating a resolver rule, and associating the resolver rule with the VPC is not correct because this solution will allow DNS queries from on-premises networks to access resources in a VPC, not vice versa. An inbound endpoint is a set of IP addresses that Resolver uses to receive DNS queries from resolvers on an on-premises network1. Creating a Route 53 private hosted zone

and associating it with the VPC is not correct because this solution will only allow DNS resolution for resources within the VPC or other VPCs that are associated with the same hosted zone. A private hosted zone is a container for DNS records that are only accessible from one or more VPCs3. Creating a Route 53 public hosted zone and creating a record for each service to allow service communication is not correct because this solution will expose the on-premises services to the public internet, which is not secure. A public hosted zone is a container for DNS records that are accessible from anywhere on the internet3.

References:

- Resolving DNS queries between VPCs and your network - Amazon Route 53
- Working with rules - Amazon Route 53
- Working with private hosted zones - Amazon Route 53

654. - (Topic 4)

A company recently announced the deployment of its retail website to a global audience. The website runs on multiple Amazon EC2 instances behind an Elastic Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones.

The company wants to provide its customers with different versions of content based on the devices that the customers use to access the website.

Which combination of actions should a solutions architect take to meet these requirements? (Choose two.)

A. Configure Amazon CloudFront to cache multiple versions of the content.

B. Configure a host header in a Network Load Balancer to forward traffic to different instances.

C. Configure a Lambda@Edge function to send specific objects to users based on the User-Agent header.

D. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up host-based routing to different EC2 instances.

E. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up path-based routing to different EC2 instances.

Answer: A,C

Explanation:

For C: IMPROVED USER EXPERIENCE Lambda@Edge can help improve your users' experience with your websites and web applications across the world, by letting you personalize content for them without sacrificing performance. Real-time Image Transformation You can customize your users' experience by

transforming images on the fly based on the user characteristics. For example, you can resize images based on the viewer's device type—mobile, desktop, or tablet. You can also cache the transformed images at CloudFront Edge locations to further improve performance when delivering images.

https://aws.amazon.com/lambda/edge/

655. - (Topic 4)

A company uses an organization in AWS Organizations to manage AWS accounts that contain applications. The company sets up a dedicated monitoring member account in the organization. The company wants to query and visualize observability data across the accounts by using Amazon CloudWatch.

Which solution will meet these requirements?

A. Enable CloudWatch cross-account observability for the monitoring account. Deploy an AWS CloudFormation template provided by the monitoring account in each AWS account to share the data with the monitoring account.

B. Set up service control policies (SCPs) to provide access to CloudWatch in the monitoring account under the Organizations root organizational unit (OU).

C. Configure a new IAM user in the monitoring account. In each AWS account, configure an 1AM policy to have access to query and visualize the CloudWatch data in the account. Attach the new 1AM policy to the new 1AM user.

D. Create a new IAM user in the monitoring account. Create cross-account 1AM policies in each AWS account. Attach the 1AM policies to the new IAM user.

Answer: A

Explanation: This solution meets the requirements because it allows the monitoring account to query and visualize observability data across the accounts by using CloudWatch. CloudWatch cross-account observability is a feature that enables a central monitoring account to view and interact with observability data shared by other accounts. To enable cross-account observability, the monitoring account needs to configure the types of data to be shared (metrics, logs, and traces) and the source accounts to be linked. The source accounts can be specified by account IDs, organization IDs, or organization paths. To share the data with the monitoring account, the source accounts need to deploy an AWS CloudFormation template provided by the monitoring account. This template creates an observability link resource that represents the link between the source account and the monitoring account. The template also creates a sink resource

that represents an attachment point in the monitoring account. The source accounts can share their observability data with the sink in the monitoring account. The monitoring account can then use the CloudWatch console, API, or CLI to search, analyze, and correlate the observability data across the accounts. References: CloudWatch cross-account observability, Setting up CloudWatch cross-account observability, [Observability Access Manager API Reference]

656. - (Topic 4)

A company has five organizational units (OUs) as part of its organization in AWS Organizations. Each OU correlates to the five businesses that the company owns. The company's research and development (R&D) business is separating from the company and will need its own organization. A solutions architect creates a separate new management account for this purpose.

What should the solutions architect do next in the new management account?

A. Have the R&D AWS account be part of both organizations during the transition.

B. Invite the R&D AWS account to be part of the new organization after the R&D AWS account has left the prior organization.

C. Create a new R&D AWS account in the new organization. Migrate resources from the prior R&D AWS account to the new R&D AWS account.

D. Have the R&D AWS account join the new organization. Make the new management account a member of the prior organization.

Answer: B

Explanation: it allows the solutions architect to create a separate organization for the research and development (R&D) business and move its AWS account to the new organization. By inviting the R&D AWS account to be part of the new organization after it has left the prior organization, the solutions architect can ensure that there is no overlap or conflict between the two organizations. The R&D AWS account can accept or decline the invitation to join the new organization. Once accepted, it will be subject to any policies and controls applied by the new organization. References:

- Inviting an AWS Account to Join Your Organization
- Leaving an Organization as a Member Account

657. - (Topic 4)

A company has a mobile game that reads most of its metadata from an Amazon RDS DB instance. As the game increased in popularity, developers noticed slowdowns related to the game's metadata load times Performance metrics indicate that simply scaling the database will not help A solutions architect must explore all options that include capabilities for snapshots, replication, and sub-millisecond response times What should the solutions architect recommend to solve these issues'?

A. Migrate the database to Amazon Aurora with Aurora Replicas

B. Migrate the database to Amazon DynamoDB with global tables

C. Add an Amazon ElastiCache for Redis layer in front of the database.

D. Add an Amazon ElastiCache for Memcached layer in front of the database

Answer: C

Explanation: This option is the most suitable way to improve the game’s metadata load times without migrating the database. Amazon ElastiCache for Redis is a fully managed, in- memory data store that provides sub-millisecond latency and high throughput for read- intensive workloads. You can use it as a caching layer in front of your RDS DB instance to store frequently accessed metadata and reduce the load on the database. You can also take advantage of Redis features such as snapshots, replication, and data persistence to ensure data durability and availability. ElastiCache for Redis scales automatically to meet your demand and integrates with other AWS services such as CloudFormation, CloudWatch, and IAM.

Option A is not optimal because migrating the database to Amazon Aurora with Aurora Replicas would incur additional costs and complexity. Amazon Aurora is a relational database service that provides high performance, availability, and compatibility with MySQL and PostgreSQL. Aurora Replicas are read-only copies of the primary database that can be used for scaling read capacity and enhancing availability. However, migrating the database to Aurora would require modifying the application code, testing the compatibility, and performing the data migration. Moreover, Aurora Replicas may not provide sub-millisecond response times as ElastiCache for Redis does.

Option B is not optimal because migrating the database to Amazon DynamoDB with global tables would incur additional costs and complexity. Amazon DynamoDB is a NoSQL database service that provides fast and flexible data access for any scale. Global tables are a feature of DynamoDB that enables you to replicate your data across multiple AWS Regions for high availability and performance. However, migrating the database to DynamoDB would require changing the data model, modifying the application code, and performing the data migration. Moreover, global tables may not be necessary for the game’s metadata, as

they are mainly used for cross-region data access and disaster recovery.

Option D is not optimal because adding an Amazon ElastiCache for Memcached layer in front of the database would not provide the same capabilities as ElastiCache for Redis. Amazon ElastiCache for Memcached is another fully managed, in-memory data store that provides high performance and scalability for caching workloads. However, Memcached

does not support snapshots, replication, or data persistence, which means that the cached data may be lost in case of a node failure or a cache eviction. Moreover, Memcached does not integrate with other AWS services as well as Redis does. Therefore, ElastiCache for Redis is a better choice for this scenario.

References:

- What Is Amazon ElastiCache for Redis?
- What Is Amazon Aurora?
- What Is Amazon DynamoDB?
- What Is Amazon ElastiCache for Memcached?

658. - (Topic 4)

A company uses AWS Organizations to run workloads within multiple AWS accounts A tagging policy adds department tags to AWS resources when the company creates tags.

An accounting team needs to determine spending on Amazon EC2 consumption The accounting team must determine which departments are responsible for the costs regardless of AWS account The accounting team has access to AWS Cost Explorer for all AWS accounts within the organization and needs to access all reports from Cost Explorer.

Which solution meets these requirements in the MOST operationally efficient way'?

A. From the Organizations management account billing console, activate a user-defined cost allocation tag named department Create one cost report in Cost Explorer grouping by tag name, and filter by EC2.

B. From the Organizations management account billing console, activate an AWS-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name, and filter by EC2.

C. From the Organizations member account billing console, activate a user-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by the tag name, and filter by EC2.

D. From the Organizations member account billing console, activate an AWS-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name and filter by EC2.

Answer: B

Explanation: This solution meets the following requirements:

➪ It is operationally efficient, as it only requires one activation of the cost allocation tag and one creation of the cost report from the management account, which has access to all the member accounts' data and billing preferences.

➪ It is consistent, as it uses the AWS-defined cost allocation tag named department, which is automatically applied to resources when the company creates tags using the tagging policy enforced by AWS Organizations. This ensures that the tag name and value are the same across all the resources and accounts, and avoids any

discrepancies or errors that might arise from user-defined tags.

➪ It is informative, as it creates one cost report in Cost Explorer grouping by the tag name, and filters by EC2. This allows the accounting team to see the breakdown of EC2 consumption and costs by department, regardless of the AWS account. The team can also use other features of Cost Explorer, such as charts, filters, and forecasts, to analyze and optimize the spending.

References:

➪ Using AWS cost allocation tags - AWS Billing

➪ User-defined cost allocation tags - AWS Billing

➪ Cost Tagging and Reporting with AWS Organizations

659. - (Topic 4)

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

How can these requirements be met?

A. Deploy Amazon S3 Glacier Vault and enable expedited retrieval. Enable provisioned retrieval capacity for the workload.

B. Deploy AWS Storage Gateway using cached volumes. Use Storage Gateway to store data in Amazon S3 while retaining copies of frequently accessed data subsets locally.

C. Deploy AWS Storage Gateway using stored volumes to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.

D. Deploy AWS Direct Connect to connect with the on-premises data center. Configure AWS Storage Gateway to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.

Answer: B

Explanation:

The solution that will meet the requirements is to deploy AWS Storage Gateway using cached volumes and use Storage Gateway to store data in Amazon S3 while retaining copies of frequently accessed data subsets locally. This solution will allow the company to migrate its storage infrastructure to AWS while minimizing bandwidth costs, as it will only transfer data that is not cached locally. The solution will also allow for immediate retrieval of data at no additional cost, as the cached volumes will provide low-latency access to the most recently used data. The data stored in Amazon S3 will be durable, scalable, and secure. The other solutions are not as effective as the first one because they either do not meet the requirements or introduce additional costs or complexity. Deploying Amazon S3 Glacier Vault and enabling expedited retrieval will not meet the requirements, as it will incur additional costs for both storage and retrieval. Amazon S3 Glacier is a low-cost storage service for data archiving and backup, but it has longer retrieval times than Amazon S3. Expedited retrieval is a feature that allows faster access to data, but it charges a higher fee per GB retrieved. Provisioned retrieval capacity is a feature that reserves dedicated capacity for expedited retrievals, but it also charges a monthly fee per provisioned capacity unit. Deploying AWS Storage Gateway using stored volumes to store data locally and use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3 will not meet the requirements, as it will not migrate the storage infrastructure to AWS, but only create backups. Stored volumes are volumes that store the primary data locally and back up snapshots to Amazon S3. This solution will not reduce the storage capacity needed on-premises, nor will it leverage the benefits of cloud storage. Deploying AWS Direct Connect to connect with the on-premises data center and configuring AWS Storage Gateway to store data locally and use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3 will not meet the requirements, as it will also not migrate the storage infrastructure to AWS, but only create backups. AWS Direct Connect is a service that establishes a dedicated network connection between the on-premises data center and AWS, which can reduce network costs and increase bandwidth. However, this solution will also not reduce the storage capacity needed on- premises, nor will it leverage the benefits of cloud storage.

References:

- AWS Storage Gateway
- Cached volumes - AWS Storage Gateway
- Amazon S3 Glacier
- Retrieving archives from Amazon S3 Glacier vaults - Amazon Simple Storage Service
- Stored volumes - AWS Storage Gateway
- AWS Direct Connect

660. - (Topic 4)

A company is designing a containerized application that will use Amazon Elastic Container Service (Amazon ECS). The application needs to access a shared file system that is highly durable and can recover data to another AWS Region with a recovery point objective (RPO) of 8 hours. The file system needs to provide a mount target in each Availability Zone within a Region.

A solutions architect wants to use AWS Backup to manage the replication to another Region.

Which solution will meet these requirements?

A. 'Amazon FSx for Windows File Server with a Multi-AZ deployment

B. Amazon FSx for NetApp ONTAP with a Multi-AZ deployment

C. 'Amazon Elastic File System (Amazon EFS) with the Standard storage class

D. Amazon FSx for OpenZFS

Answer: B

Explanation: This answer is correct because it meets the requirements of accessing a shared file system that is highly durable, can recover data to another AWS Region, and can provide a mount target in each Availability Zone within a Region. Amazon FSx for NetApp ONTAP is a fully managed service that provides enterprise-grade data management and storage for your Windows and Linux applications. You can use Amazon FSx for NetApp ONTAP to create file systems that span multiple Availability Zones within an AWS Region, providing high availability and durability. You can also use AWS Backup to manage the replication of your file systems to another AWS Region, with a recovery point objective (RPO) of 8 hours or less. AWS Backup is a fully managed backup service that automates and centralizes backup of data over AWS services. You can use AWS Backup to create backup policies and monitor activity for your AWS resources in one place.

References:

- https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/what-is.html
- https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html

661. - (Topic 4)

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

Which solution meets these requirements?

A. Set up S3 bucket policies to allow access from a VPC endpomt.

B. Set up an 1AM policy to grant read-write access to the S3 bucket.

C. Set up a NAT gateway to access resources outside the private subnet.

D. Set up an access key ID and a secret access key to access the S3 bucket.

Answer: A

Explanation: This solution meets the following requirements:

- It is private and secure, as it allows the EC2 instances to access the S3 bucket without using the public internet. A VPC endpoint is a gateway that enables you to create a private connection between your VPC and another AWS service, such as S3, within the same Region. A VPC endpoint for S3 provides secure and direct access to S3 buckets and objects using private IP addresses from your VPC. You can also use VPC endpoint policies and S3 bucket policies to control the access to the S3 resources based on the endpoint, the IAM user, the IAM role, or the source IP address.
- It is simple and scalable, as it does not require any additional AWS services, gateways, or NAT devices. A VPC endpoint for S3 is a fully managed service that scales automatically with the network traffic. You can create a VPC endpoint for S3 with a few clicks in the VPC console or with a simple API call. You can also use the same VPC endpoint to access multiple S3 buckets in the same Region.

References:

- VPC Endpoints - Amazon Virtual Private Cloud
- Gateway VPC endpoints - Amazon Virtual Private Cloud
- Using Amazon S3 with interface VPC endpoints - Amazon Simple Storage Service

⇨ Using Amazon S3 with gateway VPC endpoints - Amazon Simple Storage Service

662. - (Topic 4)

A company recently migrated its web application to AWS by rehosting the application on Amazon EC2 instances in a single AWS Region. The company wants to redesign its application architecture to be highly available and fault tolerant. Traffic must reach all running EC2 instances randomly.

Which combination of steps should the company take to meet these requirements? (Choose two.)

A. Create an Amazon Route 53 failover routing policy.

B. Create an Amazon Route 53 weighted routing policy.

C. Create an Amazon Route 53 multivalue answer routing policy.

D. Launch three EC2 instances: two instances in one Availability Zone and one instance in another Availability Zone.

E. Launch four EC2 instances: two instances in one Availability Zone and two instances in another Availability Zone.

Answer: C,E

Explanation: https://aws.amazon.com/premiumsupport/knowledge-center/multivalue-versus-simple-policies/

663. - (Topic 4)

A company has a service that reads and writes large amounts of data from an Amazon S3 bucket in the same AWS Region. The service is deployed on Amazon EC2 instances within the private subnet of a VPC. The service communicates with Amazon S3 over a NAT gateway in the public subnet. However, the company wants a solution that will reduce the data output costs.

Which solution will meet these requirements MOST cost-effectively?

A. Provision a dedicated EC2 NAT instance in the public subnet. Configure the route table for the private subnet to use the elastic network interface of this instance as the destination for all S3 traffic.

B. Provision a dedicated EC2 NAT instance in the private subnet. Configure the route table for the public subnet to use the elastic network interface of this instance as the destination for all S3 traffic.

C. Provision a VPC gateway endpoint. Configure the route table for the private subnet to use the gateway endpoint as the route for all S3 traffic.

D. Provision a second NAT gateway. Configure the route table for the private subnet to use this NAT gateway as the destination for all S3 traffic.

Answer: C

Explanation: it allows the company to reduce the data output costs for accessing Amazon S3 from Amazon EC2 instances in a VPC. By provisioning a VPC gateway endpoint, the company can enable private connectivity between the VPC and S3. By configuring the route table for the private subnet to use the gateway endpoint as the route for all S3 traffic, the company can avoid using a NAT gateway, which charges for data processing and data transfer. References:

- VPC Endpoints for Amazon S3
- VPC Endpoints Pricing

664. - (Topic 4)

A company is building a microservices-based application that will be deployed on Amazon Elastic Kubernetes Service (Amazon EKS). The microservices will interact with each other. The company wants to ensure that the application is observable to identify performance issues in the future.

Which solution will meet these requirements?

A. Configure the application to use Amazon ElastiCache to reduce the number of requests that are sent to the microservices.

B. Configure Amazon CloudWatch Container Insights to collect metrics from the EKS clusters Configure AWS X-Ray to trace the requests between the microservices.

C. Configure AWS CloudTrail to review the API calls. Build an Amazon QuickSight dashboard to observe the microservice interactions.

D. Use AWS Trusted Advisor to understand the performance of the application.

Answer: B

Explanation: This solution meets the requirements because it enables the company to observe the performance and behavior of its microservices-based application on Amazon EKS. Amazon CloudWatch Container Insights is a feature that collects, aggregates, and summarizes metrics and logs from containerized applications and microservices. Container Insights integrates with Amazon EKS and Kubernetes to provide metrics at the cluster, node, pod, task, and service level. You can use Container Insights to monitor the CPU, memory, disk, and network utilization of your EKS clusters and identify

bottlenecks, latency spikes, and other issues. AWS X-Ray is a service that collects data about requests that your application serves, and provides tools that you can use to view, filter, and gain insights into that data. X-Ray integrates with Amazon EKS and Kubernetes to trace the requests that your microservices make to downstream AWS resources, microservices, databases, and web APIs. You can use X-Ray to analyze the root cause of errors, faults, and performance issues, and visualize the service map of your application.

References:

- Using Container Insights
- AWS X-Ray

665. - (Topic 4)

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

What is the MOST cost-effective solution?

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

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

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

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

Answer: A

Explanation:

Amazon S3 Glacier is a storage class that provides secure, durable, and extremely low-cost storage for data archiving and long-term backup. It is designed for data that is rarely accessed and for which retrieval times of several hours are suitable1. By storing the video archives in Amazon S3 Glacier, the solution can minimize costs.

Amazon S3 Glacier offers three options for data retrieval: Expedited, Standard, and Bulk. Expedited retrievals typically return data in 1–5 minutes and are suitable for Active Archive use cases. Standard retrievals typically complete within 3–5 hours and are suitable for less urgent needs. Bulk retrievals typically complete within 5–12 hours and are the lowest-cost retrieval option2. By using Expedited retrievals, the solution can meet the requirement of restoring the files in a maximum of five minutes.

* B. Store the video archives in Amazon S3 Glacier and use Standard retrievals. This solution will not meet

the requirement of restoring the files in a maximum of five minutes, as Standard retrievals typically complete within 3–5 hours.

* C. Store the video archives in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). This solution will not meet the requirement of minimizing costs, as S3 Standard-IA is a storage class that provides low-cost storage for data that is accessed less frequently but requires rapid access when needed. It has a higher storage cost than S3 Glacier.

* D. Store the video archives in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA). This solution will not meet the requirement of minimizing costs, as S3 One Zone-IA is a storage class that provides low-cost storage for data that is accessed less frequently but requires rapid access when needed. It has a higher storage cost than S3 Glacier. Reference URL: https://aws.amazon.com/s3/glacier/

666. - (Topic 4)

A company hosts its web application on AWS using seven Amazon EC2 instances. The company requires that the IP addresses of all healthy EC2 instances be returned in response to DNS queries.

Which policy should be used to meet this requirement?

A. Simple routing policy

B. Latency routing policy

C. Multivalue routing policy

D. Geolocation routing policy

Answer: C

Explanation: Use a multivalue answer routing policy to help distribute DNS responses across multiple resources. For example, use multivalue answer routing when you want to

associate your routing records with a Route 53 health check. For example, use multivalue answer routing when you need to return multiple values for a DNS query and route traffic to multiple IP addresses.

https://aws.amazon.com/premiumsupport/knowledge- center/multivalue-versus-simple-policies/

667. - (Topic 4)

A company plans to use Amazon ElastiCache for its multi-tier web application. A solutions architect creates a Cache VPC for the ElastiCache cluster and an App VPC for the application's Amazon EC2 instances. Both VPCs are in the us-east-1 Region.

The solutions architect must implement a solution to provide the application's EC2 instances with access to the ElastiCache cluster.

Which solution will meet these requirements MOST cost-effectively?

A. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.

B. Create a Transit VPC. Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.

C. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the peering connection's security group to allow inbound connection from the application's security group.

D. Create a Transit VPC. Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC. Configure an inbound rule for the Transit VPC's security group to allow inbound connection from the application's security group.

Answer: A

Explanation:

Creating a peering connection between the VPCs allows the application's EC2 instances to communicate with the ElastiCache cluster directly and efficiently. This is the most cost- effective solution as it does not involve creating additional resources such as a Transit VPC, and it does not incur additional costs for traffic passing through the Transit VPC. Additionally, it is also more secure as it allows you to configure a more restrictive security group rule to allow inbound connection from only the application's security group.

668. - (Topic 4)

A 4-year-old media company is using the AWS Organizations all features feature set fo organize its AWS accounts. According to he company's finance team, the billing information on the member accounts must not be accessible to anyone, including the root user of the member accounts. Which solution will meet these requirements?

A. Add all finance team users to an IAM group. Attach an AWS managed policy named Billing to the group.

B. Attach an identity-based policy to deny access to the billing information to all users, including the root

user.

C. Create a service control policy (SCP) to deny access to the billing information. Attach the SCP to the root organizational unit (OU).

D. Convert from the Organizations all features feature set to the Organizations consolidated billing feature set.

Answer: C

Explanation: Service Control Policies (SCP): SCPs are an integral part of AWS Organizations and allow you to set fine-grained permissions on the organizational units (OUs) within your AWS Organization. SCPs provide central control over the maximum permissions that can be granted to member accounts, including the root user. Denying Access to Billing Information: By creating an SCP and attaching it to the root OU, you can explicitly deny access to billing information for all accounts within the organization. SCPs can be used to restrict access to various AWS services and actions, including billing- related services. Granular Control: SCPs enable you to define specific permissions and restrictions at the organizational unit level. By denying access to billing information at the root OU, you can ensure that no member accounts, including root users, have access to the billing information.

669. - (Topic 4)

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

Which solution will meet these requirements?

A. Set up a VPC peering connection between VPC-A and VPC-B.

B. Set up VPC gateway endpoints for the EC2 instance running in VPC-B.

C. Attach a virtual private gateway to VPC-B and set up routing from VPC-A.

D. Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-A.

Answer: A

Explanation:

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway

nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

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

670. - (Topic 4)

A company is migrating its multi-tier on-premises application to AWS. The application consists of a single-node MySQL database and a multi-node web tier. The company must minimize changes to the application during the migration. The company wants to improve application resiliency after the migration. Which combination of steps will meet these requirements? (Select TWO.)

A. Migrate the web tier to Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer.

B. Migrate the database to Amazon EC2 instances in an Auto Scaling group behind a Network Load Balancer.

C. Migrate the database to an Amazon RDS Multi-AZ deployment.

D. Migrate the web tier to an AWS Lambda function.

E. Migrate the database to an Amazon DynamoDB table.

Answer: A,C

Explanation: An Auto Scaling group is a collection of EC2 instances that share similar characteristics and can be scaled in or out automatically based on demand. An Auto

Scaling group can be placed behind an Application Load Balancer, which is a type of Elastic Load Balancing load balancer that distributes incoming traffic across multiple targets in multiple Availability Zones. This solution will improve the resiliency of the web tier by providing high availability, scalability, and fault tolerance. An Amazon RDS Multi-AZ deployment is a configuration that automatically creates a primary database instance and synchronously replicates the data to a standby instance in a different Availability Zone. When a failure occurs, Amazon RDS automatically fails over to the standby instance without manual intervention. This solution will improve the resiliency of the database tier by providing data redundancy, backup support, and availability. This combination of steps will meet the requirements with minimal changes to the application during the migration. References:

- 1 describes the concept and benefits of an Auto Scaling group.
- 2 provides an overview of Application Load Balancers and their benefits.

- 3 explains how Amazon RDS Multi-AZ deployments work and their benefits.

671. - (Topic 4)

A solutions architect creates a VPC that includes two public subnets and two private subnets. A corporate security mandate requires the solutions architect to launch all Amazon EC2 instances in a private subnet. However, when the solutions architect launches an EC2 instance that runs a web server on ports 80 and 443 in a private subnet, no external internet traffic can connect to the server.

What should the solutions architect do to resolve this issue?

A. Attach the EC2 instance to an Auto Scaling group in a private subnet. Ensure that the DNS record for the website resolves to the Auto Scaling group identifier.

B. Provision an internet-facing Application Load Balancer (ALB) in a public subnet. Add the EC2 instance to the target group that is associated with the ALB. Ensure that the DNS record for the website resolves to the ALB.

C. Launch a NAT gateway in a private subnet. Update the route table for the private subnets to add a default route to the NAT gateway. Attach a public Elastic IP address to the NAT gateway.

D. Ensure that the security group that is attached to the EC2 instance allows HTTP traffic on port 80 and HTTPS traffic on port 443. Ensure that the DNS record for the website resolves to the public IP address of the EC2 instance.

Answer: B

Explanation: An Application Load Balancer (ALB) is a type of Elastic Load Balancer (ELB) that distributes incoming application traffic across multiple targets, such as EC2 instances,
containers, Lambda functions, and IP addresses, in multiple Availability Zones1. An ALB can be internet-facing or internal. An internet-facing ALB has a public DNS name that clients can use to send requests over the internet1. An internal ALB has a private DNS name that clients can use to send requests within a VPC1. This solution meets the requirements of the question because:

- It allows external internet traffic to connect to the web server on ports 80 and 443, as the ALB listens for requests on these ports and forwards them to the EC2 instance in the private subnet1.
- It does not violate the corporate security mandate, as the EC2 instance is launched in a private subnet and does not have a public IP address or a route to an internet gateway2.
- It reduces the operational overhead, as the ALB is a fully managed service that handles the tasks of

load balancing, health checking, scaling, and security1.

672. - (Topic 4)

A company hosts a serverless application on AWS. The application uses Amazon API Gateway, AWS Lambda, and an Amazon RDS for PostgreSQL database. The company notices an increase in application errors that result from database connection timeouts during times Of peak traffic or unpredictable traffic. The company needs a solution that reduces the application failures with the least amount of change to the code.

What should a solutions architect do to meet these requirements?

A. Reduce the Lambda concurrency rate.

B. Enable RDS Proxy on the RDS DB instance.

C. Resize the RDS DB instance class to accept more connections.

D. Migrate the database to Amazon DynamoDB with on-demand scaling.

Answer: B

Explanation: Using RDS Proxy, you can handle unpredictable surges in database traffic. Otherwise, these surges might cause issues due to oversubscribing connections or creating new connections at a fast rate. RDS Proxy establishes a database connection pool and reuses connections in this pool. This approach avoids the memory and CPU overhead of opening a new database connection each time. To protect the database against oversubscription, you can control the number of database connections that are created.

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html

673. - (Topic 4)

A company deployed a serverless application that uses Amazon DynamoDB as a database layer The application has experienced a large increase in users. The company wants to improve database response time from milliseconds to microseconds and to cache requests to the database.

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

A. Use DynamoDB Accelerator (DAX).

B. Migrate the database to Amazon Redshift.

C. Migrate the database to Amazon RDS.

D. Use Amazon ElastiCache for Redis.

Answer: A

Explanation: DynamoDB Accelerator (DAX) is a fully managed, highly available caching service built for Amazon DynamoDB. DAX delivers up to a 10 times performance improvement—from milliseconds to microseconds—even at millions of requests per second. DAX does all the heavy lifting required to add in-memory acceleration to your DynamoDB tables, without requiring developers to manage cache invalidation, data population, or cluster management. Now you can focus on building great applications for your customers without worrying about performance at scale. You do not need to modify application logic because DAX is compatible with existing DynamoDB API calls. This solution will meet the requirements with the least operational overhead, as it does not require any code development or manual intervention.

References:

- 1 provides an overview of Amazon DynamoDB Accelerator (DAX) and its benefits.
- 2 explains how to use DAX with DynamoDB for in-memory acceleration.

674. - (Topic 4)

A company's developers want a secure way to gain SSH access on the company's Amazon EC2 instances that run the latest version of Amazon Linux. The developers work remotely and in the corporate office. The company wants to use AWS services as a part of the solution. The EC2 instances are hosted in a VPC private subnet and access the internet through a NAT gateway that is deployed in a public subnet.

What should a solutions architect do to meet these requirements MOST cost-effectively?

A. Create a bastion host in the same subnet as the EC2 instances. Grant the ec2: CreateVpnConnection 1AM permission to the developers. Install EC2 Instance Connect so that the developers can connect to the EC2 instances.

B. Create an AWS Site-to-Site VPN connection between the corporate network and the VPC. Instruct the developers to use the Site-to-Site VPN connection to access the EC2 instances when the developers are on the corporate network. Instruct the developers to set up another VPN connection for access when they work remotely.

C. Create a bastion host in the public subnet of the VPC. Configure the security groups and SSH keys of the bastion host to only allow connections and SSH authentication from the developers' corporate and remote networks. Instruct the developers to connect through the bastion host by using SSH to reach the EC2 instances.

D. Attach the AmazonSSMManagedInstanceCore 1AM policy to an 1AM role that is associated with the EC2 instances. Instruct the developers to use AWS Systems Manager Session Manager to access the EC2 instances.

Answer: D

Explanation: AWS Systems Manager Session Manager is a service that enables you to securely connect to your EC2 instances without using SSH keys or bastion hosts. You can use Session Manager to access your instances through the AWS Management Console, the AWS CLI, or the AWS SDKs. Session Manager uses IAM policies and roles to control who can access which instances. By attaching the AmazonSSMManagedInstanceCore IAM policy to an IAM role that is associated with the EC2 instances, you grant the Session Manager service the necessary permissions to perform actions on your instances. You also need to attach another IAM policy to the developers' IAM users or roles that allows them to start sessions to the instances. Session Manager uses the AWS Systems Manager Agent (SSM Agent) that is installed by default on Amazon Linux 2 and other supported Linux distributions. Session Manager also encrypts all session data between your client and your instances, and streams session logs to Amazon S3, Amazon CloudWatch Logs, or both for auditing purposes. This solution is the most cost-effective, as it does not require any additional resources or services, such as bastion hosts, VPN connections, or NAT gateways. It also simplifies the security and management of SSH access, as it eliminates the need for SSH keys, port opening, or firewall rules. References:

- What is AWS Systems Manager?
- Setting up Session Manager
- Getting started with Session Manager
- Controlling access to Session Manager
- Logging Session Manager activity

675. - (Topic 4)

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

A. Amazon S3 with Amazon CloudFront

B. Amazon S3 Glacier with Amazon ElastiCache

C. Amazon Elastic Block Store (Amazon EBS) volumes with Amazon CloudFront

D. AWS Storage Gateway with Amazon ElastiCache

Answer: A

Explanation: To store and view engineering drawings with caching support, Amazon S3 and Amazon CloudFront are suitable solutions. Amazon S3 can store any amount of data with high durability, availability, and performance. Amazon CloudFront can distribute the engineering drawings to edge locations closer to the users, which can reduce the latency and improve the user experience. Amazon CloudFront can also cache the engineering drawings at the edge locations, which can minimize the amount of time that users wait for the drawings to load.

References:

- What Is Amazon S3?
- What Is Amazon CloudFront?

676. - (Topic 4)

An application uses an Amazon RDS MySQL DB instance. The RDS database is becoming low on disk space. A solutions architect wants to increase the disk space without downtime.

Which solution meets these requirements with the LEAST amount of effort?

A. Enable storage autoscaling in RDS.

B. Increase the RDS database instance size.

C. Change the RDS database instance storage type to Provisioned IOPS.

D. Back up the RDS database, increase the storage capacity, restore the database, and stop the previous instance

Answer: A

Explanation: https://aws.amazon.com/about-aws/whats-new/2019/06/rds-storage-auto- scaling/

677. - (Topic 4)

A company has a three-tier environment on AWS that ingests sensor data from its users' devices The traffic flows through a Network Load Balancer (NIB) then to Amazon EC2 instances for the web tier and finally to

EC2 instances for the application tier that makes database calls

What should a solutions architect do to improve the security of data in transit to the web tier?

A. Configure a TLS listener and add the server certificate on the NLB

B. Configure AWS Shield Advanced and enable AWS WAF on the NLB

C. Change the load balancer to an Application Load Balancer and attach AWS WAF to it

D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances using AWS Key Management Service (AWS KMS)

Answer: A

Explanation: A: How do you protect your data in transit?

Best Practices:

Implement secure key and certificate management: Store encryption keys and certificates securely and rotate them at appropriate time intervals while applying strict access control; for example, by using a certificate management service, such as AWS Certificate Manager (ACM).

Enforce encryption in transit: Enforce your defined encryption requirements based on appropriate standards and recommendations to help you meet your organizational, legal, and compliance requirements.

Automate detection of unintended data access: Use tools such as GuardDuty to automatically detect attempts to move data outside of defined boundaries based on data classification level, for example, to detect a trojan that is copying data to an unknown or untrusted network using the DNS protocol.

Authenticate network communications: Verify the identity of communications by using protocols that support authentication, such as Transport Layer Security (TLS) or IPsec.

https://wa.aws.amazon.com/wat.question.SEC_9.en.html