

Get Success in Passing Your
Certification Exam at first attempt!

Copyright © CertBus.com, All Rights Reserved.

All our exam practice questions and answers are only for our product buyers to get prepared for their coming certification examinations. Any unauthorized sharing is forbidden. It may cause the suspending of ones account, membership and product update if there is a violation of this rule.



Vendor: Amazon

Exam Code: SAA-C03

Exam Name: AWS Certified Solutions Architect - Associate (SAA-C03)

Q&As: 692 (There are 6 parts in the dump, 692 questions in total.)

Exam A

QUESTION 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.

Correct Answer: D

Explanation

Explanation/Reference:

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

QUESTION 2

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.

Correct Answer: C

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>

Immediately after a message is received, it remains in the queue. To prevent other consumers from processing the message again, Amazon SQS sets a visibility timeout, a period of time during which Amazon SQS prevents other consumers from receiving and processing the message. The default visibility timeout for a message is 30 seconds. The minimum is 0 seconds. The maximum is 12 hours.

QUESTION 3

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.

Correct Answer: A

Explanation

Explanation/Reference:

<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

QUESTION 4

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

What should a solutions architect do to accomplish this?

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

Correct Answer: A

Explanation

QUESTION 5

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

Correct Answer: D

Explanation

Explanation/Reference:

The solution that will meet these requirements with the least operational overhead is 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, and use Amazon API Gateway and AWS Lambda functions for the backend APIs. Store the data in Amazon DynamoDB.

Using Amazon S3 to host static content and Amazon CloudFront to distribute the content can provide high performance and scale for websites with millions of requests each hour. Amazon API Gateway and AWS Lambda can be used to build scalable and highly available backend APIs to support the website, and Amazon DynamoDB can be used to store the data. This solution requires minimal operational overhead as it leverages fully managed services that automatically scale to meet demand.

QUESTION 6

A company is migrating a distributed application to AWS. The application serves variable workloads. The legacy platform consists of a primary server that 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 jobs. 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.

Correct Answer: B

Explanation

Explanation/Reference:

1. Running all tiers on EC2 allows using SQL Server on EC2 with its native features like backups and Data Quality Services. SQL Server cannot be run directly on RDS.
2. Amazon FSx for Windows File Server provides fully managed Windows file storage with SMB access. This allows sharing files between the Windows EC2 instances for all three tiers.
3. FSx for Windows File Server has high performance, so it can handle file sharing needs between the tiers.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>

QUESTION 7

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 endpoint 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.

Correct Answer: D

Explanation

Explanation/Reference:

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.

QUESTION 8

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

Which solution offers the MOST reliable data transfer?

- A. AWS DataSync over public internet
- B. AWS DataSync over AWS Direct Connect
- C. AWS Database Migration Service (AWS DMS) over public internet
- D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

Correct Answer: B

Explanation

Explanation/Reference:

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/>

QUESTION 9

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.

Correct Answer: C

Explanation

QUESTION 10

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.

Correct Answer: AB

Explanation

Explanation/Reference:

<https://aws.amazon.com/it/premiumsupport/knowledge-center/s3-audit-deleted-missing-objects/>

It states the following:

To prevent or mitigate future accidental deletions, consider the following features:

Enable versioning to keep historical versions of an object.

Enable Cross-Region Replication of objects.

Enable MFA delete to require multi-factor authentication (MFA) when deleting an object version.

QUESTION 11

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

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

Which solution will satisfy these requirements?

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

Correct Answer: D

Explanation

Explanation/Reference:

Amazon FSx for Windows File Server is a fully managed file storage service that is designed to be used with Microsoft Windows workloads. It is integrated with Active Directory for access control and is highly available, as it stores data across multiple availability zones. Additionally, FSx can be used to migrate data from on-premises Microsoft Windows file servers to the AWS Cloud. This makes it a good fit for the requirements described in the question.

QUESTION 12

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.

Correct Answer: C

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-regional-api-custom-domain-create.html>

QUESTION 13

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 the objects in the bucket. If objects contain PII, trigger an S3 Lifecycle policy to remove the objects that contain PII.
- B. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Macie to scan the objects in the bucket. If objects contain PII, use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain PII.
- C. Implement custom scanning algorithms in an AWS Lambda function. Trigger the function when objects are loaded into the bucket. If objects contain PII, use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain PII.
- D. Implement custom scanning algorithms in an AWS Lambda function. Trigger the function when objects are loaded into the bucket. If objects contain PII, use Amazon Simple Email Service (Amazon SES) to trigger a notification to the administrators and trigger an S3 Lifecycle policy to remove the objects that contain PII.

Correct Answer: B

Explanation

QUESTION 14

A company hosts its web applications in the AWS Cloud. The company configures Elastic Load Balancers to use certificates 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 in 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 30 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 Notification 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).

Correct Answer: B

Explanation

Explanation/Reference:

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

QUESTION 15

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

What should the solutions architect recommend?

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

Correct Answer: C

Explanation

Explanation/Reference:

<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

QUESTION 16

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.

Correct Answer: C

Explanation

Explanation/Reference:

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>

QUESTION 17

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

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

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

- A. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days
- B. Launch Amazon EC2 instances across two Availability Zones and place them behind an Elastic Load Balancer to ingest the alerts Create a script on the EC2 instances that will store the alerts in an Amazon S3 bucket Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days
- C. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon Elasticsearch Service (Amazon ES) cluster Set up the Amazon ES cluster to take manual snapshots every day and delete data from the cluster that is older than 14 days
- D. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to ingest the alerts and set the message retention period to 14 days Configure consumers to poll the SQS queue check the age of the message and analyze the message data as needed If the message is 14 days old the consumer should copy the message to an Amazon S3 bucket and delete the message from the SQS queue

Correct Answer: A

Explanation

Explanation/Reference:

<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>

QUESTION 18

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).

Correct Answer: A

Explanation

Explanation/Reference:

The solution that will accomplish this goal is A: Turn on AWS Config with the appropriate rules.

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. You can use AWS Config to monitor and record changes to the configuration of your Amazon S3 buckets. By turning on AWS Config and enabling the appropriate rules, you can ensure that your S3 buckets do not have unauthorized configuration changes.

QUESTION 19

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.

Correct Answer: D

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-fast-snapshot-restore.html>

Amazon EBS fast snapshot restore (FSR) enables you to create a volume from a snapshot that is fully initialized at creation. This eliminates the latency of I/O operations on a block when it is accessed for the first time. Volumes that are created using fast snapshot restore instantly deliver all of their provisioned performance.

QUESTION 20

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.

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 21

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

Which solution meets these requirements?

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

Correct Answer: C

Explanation

Explanation/Reference:

Security groups are stateful. All inbound traffic is blocked by default. If you create an inbound rule allowing traffic in, that traffic is automatically allowed back out again. You cannot block specific IP address using Security groups (instead use Network Access Control Lists).

"You can specify allow rules, but not deny rules." "When you first create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group." Source:

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

QUESTION 22

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.

Correct Answer: D

Explanation

Explanation/Reference:

A - refactoring can be a solution, BUT requires a LOT of effort - not the answer

B - DynamoDB is NoSQL and Aurora is SQL, so it requires a DB migration... again a LOT of effort, so no the answer

C and D are similar in structure, but...

C uses SNS, which would notify the 2nd Lambda function... provoking the same bottleneck... not the solution

D uses SQS, so the 2nd lambda function can go to the queue when responsive to keep with the DB load process.

Usually the app decoupling helps with the performance improvement by distributing load. In this case, the bottleneck is solved by uses queues... so D is the answer.

QUESTION 23

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

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

Which solution will meet these requirements?

- A. Use Amazon Redshift with a single node for leader and compute functionality.
- B. Use Amazon RDS with a Single-AZ deployment. Configure Amazon RDS to add reader instances in a different Availability Zone.
- C. Use Amazon Aurora with a Multi-AZ deployment. Configure Aurora Auto Scaling with Aurora Replicas.
- D. Use Amazon ElastiCache for Memcached with EC2 Spot Instances.

Correct Answer: C

Explanation**Explanation/Reference:**

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

QUESTION 24

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

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

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

Correct Answer: A

Explanation**Explanation/Reference:**

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

You have customers that upload to a centralized bucket from all over the world.

You transfer gigabytes to terabytes of data on a regular basis across continents.

You are unable to utilize all of your available bandwidth over the Internet when uploading to Amazon S3.
<https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html>

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

"Amazon S3 Transfer Acceleration can speed up content transfers to and from Amazon S3 by as much as 50-500% for long-distance transfer of larger objects. Customers who have either web or mobile applications with widespread users or applications hosted far away from their S3 bucket can experience long and variable upload and download speeds over the Internet"

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

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

QUESTION 25

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

What should a solutions architect do to meet this requirement?

- A. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled
- B. Store the uploaded documents in an Amazon S3 bucket. Configure an S3 Lifecycle policy to archive the documents periodically.
- C. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning enabled. Configure an ACL to restrict all access to read-only.
- D. Store the uploaded documents on an Amazon Elastic File System (Amazon EFS) volume. Access the data by mounting the volume in read-only mode.

Correct Answer: A

Explanation

Explanation/Reference:

You can use S3 Object Lock to store objects using a write-once-read-many (WORM) model. Object Lock can help prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. You can use S3 Object Lock to meet regulatory requirements that require WORM storage, or add an extra layer of protection against object changes and deletion.

Versioning is required and automatically activated as Object Lock is enabled.

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

QUESTION 26

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

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

- A. Add the `aws:PrincipalOrgID` global condition key with a reference to the organization ID to the S3 bucket policy.
- B. Create an organizational unit (OU) for each department. Add the `aws:PrincipalOrgPaths` global condition key to the S3 bucket policy.
- C. Use AWS CloudTrail to monitor the `CreateAccount`, `InviteAccountToOrganization`, `LeaveOrganization`, and `RemoveAccountFromOrganization` events. Update the S3 bucket policy accordingly.
- D. Tag each user that needs access to the S3 bucket. Add the `aws:PrincipalTag` global condition key to the S3 bucket policy.

Correct Answer: A
Explanation

QUESTION 27

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.

Correct Answer: BD
Explanation

QUESTION 28

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

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

Which solution meets these requirements?

- 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.

Correct Answer: C
Explanation

QUESTION 29

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.

Correct Answer: AC

Explanation

Explanation/Reference:

"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#SecurityGroupRules

QUESTION 30

A company wants to migrate an on-premises data center to AWS. The data center 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 Availability Zone as the EFS file system
- B. install an AWS DataSync agent in the on-premises data center
- C. Create a secondary Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instance for 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 on-premises SFTP server

Correct Answer: AB

Explanation

QUESTION 31

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

Which architecture offers the HIGHEST availability?

- A. Add a second ActiveMQ server to another Availability Zone Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.
- B. Use Amazon MQ with active/standby brokers configured across two Availability Zones Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.
- C. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for MySQL with Multi-AZ enabled.
- D. Use Amazon MQ with active/standby brokers configured across two Availability Zones Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use Amazon RDS for MySQL with Multi-AZ enabled.

Correct Answer: D
Explanation

QUESTION 32

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.

Correct Answer: A
Explanation

Explanation/Reference:

Global Accelerator has automatic failover and is perfect for this scenario with VoIP
<https://aws.amazon.com/global-accelerator/faqs/>

QUESTION 33

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

What should the solutions architect do to meet these requirements?

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

Correct Answer: A
Explanation

Explanation/Reference:

Direct Connect goes through 1 Gbps, 10 Gbps or 100 Gbps and the VPN goes up to 1.25 Gbps.

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-vpn.html>

QUESTION 34

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.

Correct Answer: C

Explanation

Explanation/Reference:

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

QUESTION 35

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

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

Correct Answer: D

Explanation

Explanation/Reference:

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

QUESTION 36

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.

Correct Answer: B

Explanation

Explanation/Reference:

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/>

QUESTION 37

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

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

Which solution meets these requirements?

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

Correct Answer: D

Explanation

Explanation/Reference:

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

QUESTION 38

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.

Correct Answer: D

Explanation

QUESTION 39

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).

Correct Answer: C

Explanation

Explanation/Reference:

<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/>

QUESTION 40

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

What should the company do to guarantee the EC2 capacity?

- A. Purchase Reserved instances that specify the Region needed
- B. Create an On Demand Capacity Reservation that specifies the Region needed
- C. Purchase Reserved instances that specify the Region and three Availability Zones needed
- D. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed

Correct Answer: D

Explanation

Explanation/Reference:

<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

QUESTION 41

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.

Correct Answer: A
Explanation

Explanation/Reference:

AWS Global Accelerator vs CloudFront

1. They both use the AWS global network and its edge locations around the world
2. Both services integrate with AWS Shield for DDoS protection.
3. CloudFront
4. Improves performance for both cacheable content (such as images and videos)
5. Dynamic content (such as API acceleration and dynamic site delivery)
6. Content is served at the edge
7. Global Accelerator
8. Improves performance for a wide range of applications over TCP or UDP
9. Proxying packets at the edge to applications running in one or more AWS Regions.
10. Good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP
11. Good for HTTP use cases that require static IP addresses
12. Good for HTTP use cases that required deterministic, fast regional failover

QUESTION 42

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

Correct Answer: D
Explanation

QUESTION 43

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.

Correct Answer: A

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-dashboard-sharing.html>

Share a single dashboard and designate specific email addresses of the people who can view the dashboard. Each of these users creates their own password that they must enter to view the dashboard.

QUESTION 44

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 interface (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.

Correct Answer: B

Explanation

QUESTION 45

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

Correct Answer: C

Explanation

Explanation/Reference:

Deploying a gateway VPC endpoint for Amazon S3 is the most cost-effective way for the company to avoid Regional data transfer charges. A gateway VPC endpoint is a network gateway that allows communication between instances in a VPC and a service, such as Amazon S3, without requiring an Internet gateway or a NAT device. Data transfer between the VPC and the service through a gateway VPC endpoint is free of charge, while data transfer between the VPC and the Internet through an Internet gateway or NAT device is subject to data transfer charges. By using a gateway VPC endpoint, the company can reduce its data transfer costs by eliminating the need to transfer data through the NAT gateway to access Amazon S3. This option would provide the required connectivity to Amazon S3 and minimize data transfer charges.

QUESTION 46

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.

Correct Answer: D

Explanation

Explanation/Reference:

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

QUESTION 47

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.

Correct Answer: C

Explanation

Explanation/Reference:

In compliance mode, a protected object version can't be overwritten or deleted by any user, including the root user in your AWS account.

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

QUESTION 48

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.

Correct Answer: A

Explanation

Explanation/Reference:

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

QUESTION 49

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.

Correct Answer: B

Explanation

Explanation/Reference:

AWS Direct Connect is a network service that allows you to establish a dedicated network connection from your on-premises data center to AWS. This connection bypasses the public Internet and can provide more reliable, lower-latency communication between your on-premises application and Amazon S3. By directing backup traffic through the AWS Direct Connect connection, you can minimize the impact on your internet bandwidth and ensure timely backups to S3.

QUESTION 50

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

Correct Answer: B

Explanation

QUESTION 51

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.

Correct Answer: C

Explanation

QUESTION 52

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.

Correct Answer: B

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/filegateway/latest/files3/CreatingAnSMBFileShare.html>

QUESTION 53

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.

Correct Answer: C
Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/athena/latest/ug/what-is.html>

Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon Simple Storage Service (Amazon S3) using standard SQL. With a few actions in the AWS Management Console, you can point Athena at your data stored in Amazon S3 and begin using standard SQL to run ad-hoc queries and get results in seconds.

QUESTION 54

A survey company has gathered data for several years from areas in the United States. The company hosts the data in an Amazon S3 bucket that is 3 TB in 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.

Correct Answer: A
Explanation

Explanation/Reference:

"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>

QUESTION 55

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 QuickSight. 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 PostgreSQL. Generate reports by using Amazon Athena. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.

Correct Answer: B
Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/quicksight/latest/user/sharing-a-dashboard.html>

QUESTION 56

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

Correct Answer: CD

Explanation

Explanation/Reference:

C because from on-prem network to bastion through internet (using on-prem resource's public IP),
D because bastion and ec2 is in same VPC, meaning bastion can communicate to EC2 via its private IP address

QUESTION 57

A company is storing sensitive user information in an Amazon S3 bucket. The company wants to provide secure access to this bucket from the application tier running on Amazon EC2 instances inside a VPC.

Which combination of steps should a solutions architect take to accomplish this? (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

Correct Answer: AC

Explanation

Explanation/Reference:

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

QUESTION 58

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

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

- A. Copy the data so both EBS volumes contain all the documents.
- B. Configure the Application Load Balancer to direct a user to the server with the documents

- C. Copy the data from both EBS volumes to Amazon EFS Modify the application to save new documents to Amazon EFS
- D. Configure the Application Load Balancer to send the request to both servers Return each document from the correct server.

Correct Answer: C

Explanation

Explanation/Reference:

C is right answer, user will never get all the documents at one place in other solutions

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

QUESTION 59

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

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

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

Correct Answer: B

Explanation

Explanation/Reference:

KMS Multi-region keys are required <https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-overview.html>

QUESTION 60

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.

Correct Answer: A

Explanation

Explanation/Reference:

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

QUESTION 61

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.

Correct Answer: B

Explanation

Explanation/Reference:

Tricky question!!! forget one-way or two-way. In this scenario, AWS applications (Amazon Chime, Amazon Connect, Amazon QuickSight, AWS Single Sign-On, Amazon WorkDocs, Amazon WorkMail, Amazon WorkSpaces, AWS Client VPN, AWS Management Console, and AWS Transfer Family) need to be able to look up objects from the on-premises domain in order for them to function. This tells you that authentication needs to flow both ways. This scenario requires a two-way trust between the on-premises and AWS Managed Microsoft AD domains.

It is a requirement of the application

Scenario 2: <https://aws.amazon.com/es/blogs/security/everything-you-wanted-to-know-about-trusts-with-aws-managed-microsoft-ad/>

QUESTION 62

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

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

Correct Answer: B

Explanation

Explanation/Reference:

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.

QUESTION 63

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.

Correct Answer: B

Explanation

Explanation/Reference:

<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>

QUESTION 64

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.

Correct Answer: C

Explanation

Explanation/Reference:

EFS is not supported on Windows instances

<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>

QUESTION 65

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

What should the solutions architect recommend?

- A. Change the existing database to a Multi-AZ deployment. Serve the read requests from the primary Availability Zone.
- B. Change the existing database to a Multi-AZ deployment. Serve the read requests from the secondary Availability Zone.
- C. Create read replicas for the database. Configure the read replicas with half of the compute and storage resources as the source database.
- D. Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.

Correct Answer: D

Explanation

Explanation/Reference:

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

QUESTION 66

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.

Correct Answer: A

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html>

QUESTION 67

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

Which solution meets these requirements and is MOST operationally efficient?

- A. Server-side encryption with customer-provided keys (SSE-C)
- B. Server-side encryption with Amazon S3 managed keys (SSE-S3)
- C. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with manual rotation
- D. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with automatic rotation

Correct Answer: D

Explanation

Explanation/Reference:

<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.

QUESTION 68

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. The solutions architect must minimize the costs of storing and retrieving the media files.

Which storage option meets these requirements?

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

Correct Answer: B

Explanation

Explanation/Reference:

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

QUESTION 69

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.

Correct Answer: AB

Explanation

Explanation/Reference:

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.

QUESTION 70

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.

Correct Answer: C

Explanation

QUESTION 71

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

Which storage solution is MOST cost-effective?

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

Correct Answer: C

Explanation

QUESTION 72

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

Which AWS solution meets these requirements?

- A. Create an AWS 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 to 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 file system. Attach the file system to the origin server. Connect the application server to the file system.

Correct Answer: D

Explanation

Explanation/Reference:

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>

QUESTION 73

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 to store objects that are encrypted with an AWS Key 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 (on 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.

Correct Answer: A

Explanation

Explanation/Reference:

<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/>

QUESTION 74

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

```

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

```

What is the effect of this policy?

- A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
- B. Users can terminate an EC2 instance with the IP address 10 100 100 1 in the us-east-1 Region
- C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.
- D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100 100 254

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 75

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

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

- A. Use the CreateQueue API call to create a new queue

- B. Use the Add Permission API call to add appropriate permissions
- C. Use the ReceiveMessage API call to set an appropriate wait time
- D. Use the ChangeMessageVisibility API call to increase the visibility timeout

Correct Answer: D

Explanation

Explanation/Reference:

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

QUESTION 76

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

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

Which solution will meet these requirements?

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

Correct Answer: D

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

QUESTION 77

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.

Correct Answer: C

Explanation

Explanation/Reference:

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

QUESTION 78

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.

Correct Answer: B

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html>

QUESTION 79

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

Correct Answer: BD

Explanation

Explanation/Reference:

You can use SES to format the report in HTML.

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

QUESTION 80

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.

Correct Answer: D

Explanation

Explanation/Reference:

It's a third-party certificate, hence AWS cannot manage renewal automatically. The closest thing you can do is to send a notification to renew the 3rd party certificate.

QUESTION 81

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.

Correct Answer: C

Explanation

Explanation/Reference:

AWS Network Firewall supports both inspection and filtering as required

QUESTION 82

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.

Correct Answer: C

Explanation

QUESTION 83

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.

Correct Answer: B

Explanation

Explanation/Reference:

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>

QUESTION 84

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.

Correct Answer: D

Explanation

QUESTION 85

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 reaches the web server. Which solution will meet these requirements with the

LEAST operational overhead?

- A. Create a Network Load Balancer in the public subnet of the application's VPC to route the traffic to 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 in the inspection VPC. Configure route tables to route the incoming packets 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.

Correct Answer: D

Explanation

Explanation/Reference:

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

QUESTION 86

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.

Correct Answer: B

Explanation

Explanation/Reference:

"Amazon DynamoDB offers two types of backups: point-in-time recovery (PITR) and on-demand backups. (==> D is not the answer) PITR is used to recover your table to any point in time in a rolling 35 day window, which is used to help customers mitigate accidental deletes or writes to their tables from bad code, malicious access, or user error. (==> A isn't the answer) On demand backups are designed for long-term archiving and retention, which is typically used to help customers meet compliance and regulatory requirements. This is the second of a series of two blog posts about using AWS Backup to set up scheduled on-demand backups for Amazon DynamoDB. Part 1 presents the steps to set up a scheduled backup for DynamoDB tables from the AWS Management Console." (==> Not the DynamoDB console and C isn't the answer either)

<https://aws.amazon.com/blogs/database/part-2-set-up-scheduled-backups-for-amazon-dynamodb-using-aws-backup/>

QUESTION 87

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

What should a solutions architect recommend?

- A. Create a DynamoDB table in on-demand capacity mode.
- B. Create a DynamoDB table with a global secondary index.
- C. Create a DynamoDB table with provisioned capacity and auto scaling.
- D. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table.

Correct Answer: A
Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html#HowItWorks.OnDemand>

QUESTION 88

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

Which design should a solutions architect recommend?

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

Correct Answer: A
Explanation

Explanation/Reference:

Interesting point that Amazon RDS event notification doesn't support any notification when data inside DB is updated.

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

So subscription to RDS events doesn't give any value for Fanout = SNS => SQS

QUESTION 89

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.

Correct Answer: B
Explanation

Explanation/Reference:

RDS Proxy for Aurora <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

QUESTION 90

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.

Correct Answer: C
Explanation

QUESTION 91

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.

Correct Answer: B
Explanation

Explanation/Reference:

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>

QUESTION 92

A company runs its Infrastructure on AWS and has a registered base of 700,000 users for its document management application. The company intends to create a product that converts large PDF files to JPG image 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 time.

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 back 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.

Correct Answer: A

Explanation

Explanation/Reference:

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

QUESTION 93

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

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

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

Correct Answer: A

Explanation

Explanation/Reference:

<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>

QUESTION 94

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 Multi-AZ deployment and read replicas for production. Use the standby instance for 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.

Correct Answer: B

Explanation

Explanation/Reference:

The recommended solution is Option B: Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Use database cloning to create the staging database on-demand.

To alleviate the application latency issue, the recommended solution is to use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production, and use database cloning to create the staging database on-demand. This allows the development team to continue using the staging environment without delay, while also providing elasticity and availability for the production application.

QUESTION 95

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 ParallelCluster to establish an HPC cluster that can process the incoming requests at the appropriate scale.

Correct Answer: A

Explanation

Explanation/Reference:

AWS Fargate is a technology that you can use with Amazon ECS to run containers without having to manage servers on clusters of Amazon EC2 instances. With Fargate, you no longer have to provision, configure, or scale of virtual machines to run containers.

<https://docs.aws.amazon.com/AmazonECS/latest/userguide/what-is-fargate.html>

QUESTION 96

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.

Correct Answer: D

Explanation

Explanation/Reference:

The primary focus of Patch Manager, a capability of AWS Systems Manager, is on installing operating systems security-related updates on managed nodes. By default, Patch Manager doesn't install all available patches, but rather a smaller set of patches focused on security. (Ref <https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-how-it-works-selection.html>)

Run Command allows you to automate common administrative tasks and perform one-time configuration changes at scale. (Ref <https://docs.aws.amazon.com/systems-manager/latest/userguide/execute-remote-commands.html>)

Seems like patch manager is meant for OS level patches and not 3rd party applications. And this falls under run command wheelhouse to carry out one-time configuration changes (update of 3rd party application) at scale.

QUESTION 97

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

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

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

Correct Answer: D

Explanation**Explanation/Reference:**

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

QUESTION 98

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 track 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.

Correct Answer: D

Explanation**Explanation/Reference:**

"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>

QUESTION 99

A company wants to run its critical applications in containers to meet requirements for scalability and availability. The company prefers to focus on maintenance of the critical applications. The company does

not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload

What should a solutions architect do to meet those requirements?

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

Correct Answer: C

Explanation

Explanation/Reference:

AWS Fargate is a serverless, pay-as-you-go compute engine that lets you focus on building applications without having to manage servers. AWS Fargate is compatible with Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS).

<https://aws.amazon.com/fr/fargate/>

QUESTION 100

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

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

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

Correct Answer: A

Explanation

Explanation/Reference:

<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

QUESTION 101

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

Correct Answer: AC

Explanation

Explanation/Reference:

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

QUESTION 102

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

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

- A. Store the credentials as secrets in AWS Secrets Manager. 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.

Correct Answer: A

Explanation

Explanation/Reference:

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

QUESTION 103

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

Correct Answer: A

Explanation

Explanation/Reference:

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.

QUESTION 104

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

Correct Answer: BE

Explanation

QUESTION 105

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

What should a solutions architect recommend to meet these requirements?

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

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 106

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

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

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

Correct Answer: A

Explanation

QUESTION 107

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.

Correct Answer: B

Explanation

Explanation/Reference:

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

QUESTION 108

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.

Correct Answer: B

Explanation**Explanation/Reference:**

Using an API Gateway integration to send a message to an Amazon SQS FIFO queue is the recommended solution. FIFO queues in Amazon SQS guarantee the order of message delivery, ensuring that orders are processed in the order they are received. By configuring the SQS FIFO queue to invoke an AWS Lambda function for processing, the application can process the orders sequentially while maintaining the order in which they were received.

QUESTION 109

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.

Correct Answer: B

Explanation**QUESTION 110**

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.

Correct Answer: A

Explanation

Explanation/Reference:

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>

QUESTION 111

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.

Correct Answer: B

Explanation

QUESTION 112

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

Which design should the solutions architect use?

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

Correct Answer: C
Explanation

Explanation/Reference:

"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

QUESTION 113

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.

Correct Answer: B
Explanation

Explanation/Reference:

"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/>

QUESTION 114

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.

Correct Answer: B

Explanation

Explanation/Reference:

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.

QUESTION 115

A company is developing a new machine learning (ML) model solution on AWS. The models are developed as independent microservices that fetch approximately 1GB of model data from Amazon S3 at startup and load the data into memory. Users access the models through an asynchronous API. Users can send a request or a batch of requests and specify where the results should be sent.

The company provides models to hundreds of users. The usage patterns for the models are irregular. Some models could be unused for days or weeks. Other models could receive batches of thousands of requests at a time.

Which 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.

Correct Answer: D

Explanation

Explanation/Reference:

Batch requests/async = Amazon SQS

Microservices = Amazon ECS

Workload variations = AWS Auto Scaling on Amazon ECS

QUESTION 116

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.

Correct Answer: C

Explanation

Exam B

QUESTION 1

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.

Correct Answer: D

Explanation

Explanation/Reference:

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.

It's worth noting that FIFO queues guarantee that messages are processed in the order they are received, and prevent duplicates.

QUESTION 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.

Correct Answer: B

Explanation

Explanation/Reference:

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

This option is incorrect because AWS Storage Gateway is not a file storage service. It is a hybrid storage service that allows you to store data in the cloud while maintaining low-latency access to frequently accessed data. It is designed to integrate with on-premises storage systems, not to provide file storage for Amazon EC2 instances.

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

This is the correct answer. Amazon FSx for Windows File Server is a fully managed file storage service that provides a native Windows file system that can be accessed over the SMB protocol. It is specifically designed for use with Windows-based applications, and it can be easily integrated with existing applications by mounting the file system to each EC2 instance.

QUESTION 3

A business's backup data totals 700 terabytes (TB) and is kept in network attached storage (NAS) at its data center. This backup data must be available in the event of occasional regulatory inquiries and preserved for a period of seven years. The organization has chosen to relocate its backup data from its on-premises data center to Amazon Web Services (AWS). Within one month, the migration must be completed. The company's public internet connection provides 500 Mbps of dedicated capacity for data transport.

What should a solutions architect do to ensure that data is migrated and stored at the LOWEST possible cost?

- A. Order AWS Snowball devices to transfer the data. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
- B. Deploy a VPN connection between the data center and Amazon VPC. Use the AWS CLI to copy the data from on premises to Amazon S3 Glacier.
- C. Provision a 500 Mbps AWS Direct Connect connection and transfer the data to Amazon S3. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
- D. Use AWS DataSync to transfer the data and deploy a DataSync agent on premises. Use the DataSync task to copy files from the on-premises NAS storage to Amazon S3 Glacier.

Correct Answer: A

Explanation

QUESTION 4

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.

Correct Answer: BE

Explanation

Explanation/Reference:

Usually documents it can be few pages with text, so storing large text in Mysql is not very sufficient + deploy it on EC2 required operation overhead, so A is out.

Only Textract is used for converting documents to text and Comprehend Medical to parse medical phrases. So E is correct.

QUESTION 5

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

Which configuration will meet this requirement?

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

Correct Answer: C

Explanation

Explanation/Reference:

To meet the requirement of allowing the web application to be accessed from one specific country only, the company should configure AWS WAF (Web Application Firewall) on the Application Load Balancer in a VPC (Option C).

AWS WAF is a web application firewall service that helps protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF allows you to create rules that block or allow traffic based on the values of specific request parameters, such as IP address, HTTP header, or query string value. By configuring AWS WAF on the Application Load Balancer and creating rules that allow traffic from a specific country, the company can ensure that the web application is only accessible from that country.

QUESTION 6

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.

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 7

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 keys (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.

Correct Answer: A

Explanation

Explanation/Reference:

SSE-KMS vs SSE-S3 - The last seems to have less overhead (as the keys are automatically generated by S3 and applied on data at upload, and don't require further actions. KMS provides more flexibility, but in turn involves a different service, which finally is more "complex" than just managing one (S3). So A and B are excluded. If you are in doubt, you are having 2 buckets in A and B, while just keeping one in C and D. <https://s3browser.com/server-side-encryption-types.aspx>

Decide between C and D is deciding on Athena or RDS. RDS is a relational db, and we have documents on S3, which is the use case for Athena. Athena is also serverless, which eliminates the need of controlling the underlying infrastructure and capacity. So C is the answer.

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

QUESTION 8

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

Which solution will meet these requirements?

- A. Use a duster 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
- B. Use a cluster placement group. Create shared file 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

Correct Answer: A

Explanation

QUESTION 9

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

Which action should the solutions architect take to accomplish this?

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

Correct Answer: D

Explanation

Explanation/Reference:

The most effective and efficient solution would be Option D (Use Amazon CloudFront with the S3 bucket as its origin.)

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.

QUESTION 10

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

Correct Answer: B

Explanation

Explanation/Reference:

<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.>

QUESTION 11

A company is running a multi-tier web application on premises. The web application is containerized and runs on a number of Linux hosts connected to a PostgreSQL database that contains user records. The operational overhead of maintaining the infrastructure and capacity planning is limiting the company's growth. A solutions architect must improve the application's infrastructure.

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

- A. Migrate the PostgreSQL database to Amazon Aurora
- B. Migrate the web application to be hosted on Amazon EC2 instances.
- C. Set up an Amazon CloudFront distribution for the web application content.
- D. Set up Amazon ElastiCache between the web application and the PostgreSQL database.
- E. Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).

Correct Answer: AE

Explanation

QUESTION 12

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

content available. The solution must provide high scalability and enhanced security.

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

- A. Configure Amazon CloudFront in front of the website to use 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.

Correct Answer: AC

Explanation

Explanation/Reference:

LEAST operational overhead = Serverless

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

QUESTION 13

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.

Correct Answer: B

Explanation

QUESTION 14

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

What should a solutions architect do to meet these requirements?

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

Correct Answer: D

Explanation

Explanation/Reference:

I want to restrict access to my Amazon Simple Storage Service (Amazon S3) bucket so that objects can be accessed only through my Amazon CloudFront distribution. How can I do that? Create a CloudFront origin access identity (OAI)

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

QUESTION 15

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

Correct Answer: B

Explanation

Explanation/Reference:

The short name or full Amazon Resource Name (ARN) of the AWS Identity and Access Management role that grants containers in the task permission to call AWS APIs on your behalf.

QUESTION 16

A new employee has joined a company as a deployment engineer. The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources. A solutions architect wants the deployment engineer to perform job activities while following the principle of least privilege.

Which steps should the solutions architect do in conjunction to reach this goal? (Select two.)

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

Correct Answer: DE

Explanation

Explanation/Reference:

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

QUESTION 17

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

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

- A. Replace the EC2 instances with T3 EC2 instances that run in an Auto Scaling group. Make 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.

Correct Answer: D

Explanation

Explanation/Reference:

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

QUESTION 18

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

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

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

Correct Answer: B

Explanation

Explanation/Reference:

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

QUESTION 19

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

Correct Answer: D

Explanation

Explanation/Reference:

Amazon S3 is cheapest and can be accessed from anywhere.

QUESTION 20

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.

Correct Answer: D

Explanation

Explanation/Reference:

<https://aws.amazon.com/blogs/compute/microservice-delivery-with-amazon-ecs-and-application-load-balancers/>

QUESTION 21

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)

Correct Answer: A

Explanation

Explanation/Reference:

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

> You can configure a CloudWatch Logs log group to stream data it receives to your Amazon OpenSearch Service cluster in NEAR REAL-TIME through a CloudWatch Logs subscription

least overhead compared to kinesis

QUESTION 22

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

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

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

- A. Create a new SSL certificate using AWS Certificate Manager (ACM) install the ACM certificate on each instance
- B. Create an Amazon S3 bucket Migrate the SSL certificate to the S3 bucket Configure the EC2 instances to reference the bucket for SSL termination
- C. Create another EC2 instance as a proxy server Migrate the SSL certificate to the new instance and configure it to direct connections to the existing EC2 instances

- D. Import the SSL certificate into AWS Certificate Manager (ACM) Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM

Correct Answer: D

Explanation

Explanation/Reference:

<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."

QUESTION 23

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.

Correct Answer: A

Explanation

Explanation/Reference:

Depending on the Regions involved and the amount of data to be copied, a cross-Region snapshot copy can take hours to complete and will be a factor to consider for the RPO requirements. You need to take this into account when you estimate the RPO of this DR strategy.

If you have strict RTO and RPO requirements, you should consider a different DR strategy, such as Amazon Aurora Global Database.

<https://aws.amazon.com/blogs/database/cost-effective-disaster-recovery-for-amazon-aurora-databases-using-aws-backup/>

QUESTION 24

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 meet 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.

Correct Answer: D
Explanation

Explanation/Reference:

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/>

QUESTION 25

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

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

Which solution meets these requirements MOST cost-effectively?

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

Correct Answer: B
Explanation

Explanation/Reference:

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

QUESTION 26

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.

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 27

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 for Redis 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 to the writer endpoint.
- D. Use Amazon ROS Proxy to create a proxy. Set the DB cluster as the target database. Configure the Lambda functions to connect to the proxy rather than to the DB cluster.

Correct Answer: D

Explanation

QUESTION 28

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

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

- A. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted snapshot
- B. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it. Enable encryption on the DB instance
- C. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS). Restore encrypted snapshot to an existing DB instance
- D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS)

Correct Answer: A

Explanation

Explanation/Reference:

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>

QUESTION 29

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

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

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

Correct Answer: B

Explanation

Explanation/Reference:

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.

QUESTION 30

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 it 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.

Correct Answer: A

Explanation

QUESTION 31

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

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

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

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

Correct Answer: D

Explanation

Explanation/Reference:

To address the issue of lost user requests and improve the availability of the API, the solutions architect should use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB. Option D (correct answer)

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.

QUESTION 32

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.

Correct Answer: A

Explanation

Explanation/Reference:

To configure a VPC for an existing function:

1. Open the Functions page of the Lambda console.
2. Choose a function.
3. Choose Configuration and then choose VPC.
4. Under VPC, choose Edit.
5. Choose a VPC, subnets, and security groups

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

QUESTION 33

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

What should a solutions architect do to accomplish this?

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

Correct Answer: D

Explanation

Explanation/Reference:

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.html.

QUESTION 34

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.

Correct Answer: C

Explanation

Explanation/Reference:

<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>

QUESTION 35

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

Correct Answer: B

Explanation

QUESTION 36

A company recently started using Amazon Aurora as the data store for its global ecommerce application. When large reports are run, developers report that the ecommerce application is performing poorly. After reviewing metrics in Amazon CloudWatch, a solutions architect finds that the ReadIOPS and CPU Utilization metrics are spiking when monthly reports run.

What is the MOST cost-effective solution?

- A. Migrate the monthly reporting to Amazon Redshift.
- B. Migrate the monthly reporting to an Aurora Replica
- C. Migrate the Aurora database to a larger instance class
- D. Increase the Provisioned IOPS on the Aurora instance

Correct Answer: B

Explanation

Explanation/Reference:

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

#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>

QUESTION 37

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

- A. Amazon CloudFront
- B. AWS Global Accelerator
- C. Amazon Route 53
- D. Amazon S3 Transfer Acceleration

Correct Answer: A

Explanation

Explanation/Reference:

Serve video on demand or live streaming video

CloudFront offers several options for streaming your media to global viewers--both pre-recorded files and live events.

For video on demand (VOD) streaming, you can use CloudFront to stream in common formats such as MPEG DASH, Apple HLS, Microsoft Smooth Streaming, and CMAF, to any device.

For broadcasting a live stream, you can cache media fragments at the edge, so that multiple requests for the manifest file that delivers the fragments in the right order can be combined, to reduce the load on your origin server.

QUESTION 38

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

How should the solutions architect comply with these requirements?

- A. Configure an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.

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

Correct Answer: D

Explanation

Explanation/Reference:

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

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-aws-waf.html>

QUESTION 39

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

Which solution meets these requirements MOST cost-effectively?

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

Correct Answer: D

Explanation

Explanation/Reference:

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>

QUESTION 40

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.

Correct Answer: C

Explanation

Explanation/Reference:

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-access-to-s3.html#private-content-granting-permissions-to-oai>

QUESTION 41

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

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

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

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

Correct Answer: D

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/sns/latest/dg/sns-message-delivery-retries.html>

QUESTION 42

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.

Correct Answer: B

Explanation

Explanation/Reference:

<https://aws.amazon.com/about-aws/whats-new/2020/12/amazon-eks-support-ec2-spot-instances-managed-node-groups/>

QUESTION 43

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 to 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 than 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.

Correct Answer: B
Explanation

Explanation/Reference:

You need S3 to be able to archive the logs after one month. Cannot do that with CloudWatch Logs.

QUESTION 44

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.

Correct Answer: A
Explanation

QUESTION 45

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.

Correct Answer: D
Explanation

Explanation/Reference:

1. Intelligent-tiering requires no configuration for class transitions - your option is just whether to opt into Archive/Deep Archive Access tier, which does not make sense for the requirement. Those two classes are cheapest in terms of storage but charges high for retrieval.
2. Nowhere has it mentioned that the access pattern is unpredictable. If we really have to assume, I would rather assume that new songs have higher access frequency. In this case, you don't really benefit from the auto-transition feature that Intel-tier provides. You will be paying the same rate as S3 Standard class + additional fee for using Intel-tiering. Since the req is to have the most cost-efficient solution, D is the answer.

QUESTION 46

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.

Correct Answer: B

Explanation

Explanation/Reference:

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 its 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.

QUESTION 47

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 for 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 the databases to an Amazon Redshift cluster
- D. Use an AWS Glue extract transform, and load (ETL) job to convert the data into JSON format Load the data into multiple Amazon OpenSearch Service (Amazon Elasticsearch Service) clusters
- 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

Correct Answer: AE

Explanation

Explanation/Reference:

AWS Lake Formation uses as a central place to have all your data for analytics purposes (E). Athena integrates perfectly with S3 and can make queries (A).

QUESTION 48

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

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

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

- A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.
- B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.
- C. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones. Deploy an RDS Multi-AZ DB instance in private subnets.
- D. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnet.
- E. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnets.

Correct Answer: AD

Explanation

Explanation/Reference:

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.

QUESTION 49

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.

Correct Answer: B

Explanation

Explanation/Reference:

RDS Proxy is a fully managed database proxy that allows applications to pool and share connections to an RDS database instance, reducing the number of connections made to the database and improving the performance of read-heavy workloads. RDS Proxy also provides features like connection pooling, query logging, and automatic failover, which can help to improve the availability and performance of the database.

By using RDS Proxy between the application and the database, the gaming company can improve the performance of the application without making significant changes to the application's architecture. RDS Proxy can help to reduce the number of connections made to the database, optimize query execution, and provide automatic failover in case of a database failure.

QUESTION 50

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

Correct Answer: AC

Explanation

Explanation/Reference:

AWS Database Migration Service (AWS DMS) helps you migrate databases to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. With AWS Database Migration Service, you can also continuously replicate data with low latency from any supported source to any supported target.

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

QUESTION 51

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.

Correct Answer: B

Explanation

QUESTION 52

A company uses a three-tier web application to provide training to new employees. The application is accessed for only 12 hours every day. The company is using an Amazon RDS for MySQL DB instance to store information and wants to minimize costs.

What should a solutions architect do to meet these requirements?

- A. Configure an IAM policy for AWS Systems Manager Session Manager. Create an IAM role for the policy. Update the trust relationship of the role. Set up automatic start and stop for the DB instance.
- B. Create an Amazon ElastiCache for Redis cache cluster that gives users the ability to access the data from the cache when the DB instance is stopped. Invalidate the cache after the DB instance is started.
- C. Launch an Amazon EC2 instance. Create an IAM role that grants access to Amazon RDS. Attach the role to the EC2 instance. Configure a cron job to start and stop the EC2 instance on the desired schedule.
- D. Create AWS Lambda functions to start and stop the DB instance. Create Amazon EventBridge (Amazon CloudWatch Events) scheduled rules to invoke the Lambda functions. Configure the Lambda functions as event targets for the rules

Correct Answer: D

Explanation

Explanation/Reference:

By using AWS Lambda functions triggered by Amazon EventBridge scheduled rules, the company can automate the start and stop actions for the Amazon RDS for MySQL DB instance based on the 12-hour access period. This allows them to minimize costs by only running the DB instance when it is needed.

Option A is not the most suitable solution because it refers to IAM policies for AWS Systems Manager Session Manager, which is primarily used for interactive shell access to EC2 instances and does not directly address the requirement of starting and stopping the DB instance.

Option B is not the most suitable solution because it suggests using Amazon ElastiCache for Redis as a cache cluster, which may not provide the desired cost optimization for the DB instance.

Option C is not the most suitable solution because launching an EC2 instance and configuring cron jobs to start and stop it does not directly address the requirement of minimizing costs for the Amazon RDS DB instance.

QUESTION 53

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 to 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 file 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.

Correct Answer: B

Explanation

Explanation/Reference:

What is VPC gateway endpoint

Consider a scenario where you have to access S3 from your EC2 instance in a public subnet. As the subnet has an internet gateway attached, the traffic to S3 will go through the public internet. However, the problem arises if your instance is in a private subnet and does not have any NAT gateway/instance attached or you cannot afford charges of NAT gateway. Currently, AWS S3 and DynamoDB are the only services supported by gateway endpoints. Using Gateway endpoints does not incur any data processing or hourly charges.

<https://digitalcloud.training/vpc-interface-endpoint-vs-gateway-endpoint-in-aws/>

QUESTION 54

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.

Correct Answer: AC

Explanation

QUESTION 55

A company has a service that produces event data. The company wants to use AWS to process the event data as it is received. The data is written in a specific order that must be maintained throughout processing. The company wants to implement a solution that minimizes operational overhead.

How should a solutions architect accomplish this?

- A. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue.
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an AWS Lambda function as a subscriber.
- C. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to hold messages. Set up an AWS Lambda function to process messages from the queue independently.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a subscriber.

Correct Answer: A

Explanation

Explanation/Reference:

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.

QUESTION 56

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

Which solution meets these requirements?

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

to synchronously replicate the data to an Amazon RDS MySQL DB instance.

Correct Answer: B

Explanation

Explanation/Reference:

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/>

QUESTION 57

A company is migrating an application from on-premises servers to Amazon EC2 instances. As part of the migration design requirements, a solutions architect must implement infrastructure metric alarms. The company does not need to take action if CPU utilization increases to more than 50% for a short burst of time. However, if the CPU utilization increases to more than 50% and read IOPS on the disk are high at the same time, the company needs to act as soon as possible. The solutions architect also must reduce false alarms.

What should the solutions architect do to meet these requirements?

- A. Create Amazon CloudWatch composite alarms where possible.
- B. Create Amazon CloudWatch dashboards to visualize the metrics and react to issues quickly.
- C. Create Amazon CloudWatch Synthetics canaries to monitor the application and raise an alarm.
- D. Create single Amazon CloudWatch metric alarms with multiple metric thresholds where possible.

Correct Answer: A

Explanation

Explanation/Reference:

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_Alarm.html

QUESTION 58

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.

Correct Answer: C
Explanation

Explanation/Reference:

The correct solution is Option C. 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.

This solution does not require the company to create a Lambda function or query CloudTrail logs, which makes it the most cost-effective and efficient option.

QUESTION 59

A company's website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company's website demands globally. The solution should be cost-effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.

Which combination should a solutions architect recommend to meet these requirements?

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

Correct Answer: A
Explanation

QUESTION 60

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

What should the solutions architect recommend?

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

Correct Answer: A
Explanation

QUESTION 61

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

Which solution will meet these requirements?

- A. Use S3 Object Lock In governance mode with a legal hold of 1 year

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

Correct Answer: B

Explanation

Explanation/Reference:

S3 Object Lock provides the necessary features to enforce immutability and retention of objects in an S3. Compliance mode ensures that the locked objects cannot be deleted or modified by any user, including those with write access. By setting a retention period of 365 days, the company can ensure that every file in the repository is kept for a minimum of 1 year after its creation date.

A does not provide the same level of protection as compliance mode. In governance mode, there is a possibility for authorized users to remove the legal hold, potentially allowing objects to be modified or deleted.

C can restrict users from deleting or changing objects, but it does not enforce the retention period requirement. It also does not provide the same level of immutability and protection against accidental or malicious modifications.

D does not address the requirement of preventing users from modifying or deleting files. It provides a mechanism for tracking changes but does not enforce the desired access restrictions or retention period.

QUESTION 62

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

Correct Answer: B

Explanation

QUESTION 63

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

Correct Answer: C

Explanation

Explanation/Reference:

S3 Standard is a highly durable and scalable storage option suitable for backup and disaster recovery purposes. It offers millisecond access to data when needed and provides durability guarantees. It is also cost-effective compared to other storage options like OpenSearch Service, S3 Glacier, and RDS for PostgreSQL, which may have higher costs or longer access times for retrieving the data.

A-OpenSearch Service (Elasticsearch Service): While it offers fast data retrieval, it may incur higher costs compared to storing data directly in S3, especially considering the amount of data being generated.

B-S3 Glacier: While it provides long-term archival storage at a lower cost, it does not meet the requirement of immediate access in milliseconds. Retrieving data from Glacier typically takes several hours.

D-RDS for PostgreSQL: While it can be used for data storage, it may be overkill and more expensive for a backup and disaster recovery solution compared to S3 Standard, which is more suitable and cost-effective for storing and retrieving data.

QUESTION 64

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.

Correct Answer: D

Explanation

QUESTION 65

A company is running several business applications in three separate VPCs within the us-east-1 Region. The applications must be able to communicate between VPCs. The applications also must be able to consistently send hundreds of 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 meets 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.

Correct Answer: D

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway.html>

QUESTION 66

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.

Correct Answer: C

Explanation

Explanation/Reference:

<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>

QUESTION 67

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. Text, letter
- B. Text
- C. Text, application
- D. Text, application

Correct Answer: A

Explanation

Explanation/Reference:

https://docs.amazonaws.cn/en_us/IAM/latest/UserGuide/reference_policies_examples_s3_rw-bucket.html

QUESTION 68

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

What should a solutions architect recommend to meet this requirement?

- A. Use Amazon ElastiCache for Redis.

- B. Use Amazon DynamoDB Accelerator (DAX).
- C. Replicate data by using DynamoDB global tables.
- D. Use Amazon ElastiCache for Memcached with Auto Discovery enabled.

Correct Answer: B

Explanation

Explanation/Reference:

Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB that helps improve the read performance of DynamoDB tables. DAX provides a caching layer between the application and DynamoDB, reducing the number of read requests made directly to DynamoDB. This can significantly reduce read latencies and improve overall application performance.

QUESTION 69

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 s3objectCreated: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 s3objectCreated: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.

Correct Answer: D

Explanation

QUESTION 70

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.

Correct Answer: B

Explanation

Explanation/Reference:

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

QUESTION 71

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.

Correct Answer: A

Explanation

Explanation/Reference:

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content

QUESTION 72

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.

Correct Answer: A

Explanation

Explanation/Reference:

To securely store a database user name and password in AWS Systems Manager Parameter Store and allow an application running on an EC2 instance to access it, the solutions architect should create an IAM role that has read access to the Parameter Store parameter and allow Decrypt access to an AWS KMS

key that is used to encrypt the parameter. The solutions architect should then assign this IAM role to the EC2 instance.

This approach allows the EC2 instance to access the parameter in the Parameter Store and decrypt it using the specified KMS key while enforcing the necessary security controls to ensure that the parameter is only accessible to authorized parties.

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html

QUESTION 73

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.

Correct Answer: AC

Explanation

Explanation/Reference:

A-By using Control Tower, the company can enforce data residency guardrails and restrict internet access for VPCs and denies access to all Regions except the required ap-northeast-3 Region.

C-With Organizations, the company can configure SCPs to prevent VPCs from gaining internet access. By denying access to all Regions except ap-northeast-3, the company ensures that VPCs can only be deployed in the specified Region.

Option B is incorrect because using rules in AWS WAF alone does not address the requirement of denying access to all AWS Regions except ap-northeast-3.

Option D is incorrect because configuring outbound rules in network ACLs and IAM policies for users can help restrict traffic and access, but it does not enforce the company's requirement of denying access to all Regions except ap-northeast-3.

Option E is incorrect because using AWS Config and managed rules can help detect and alert for specific resources and configurations, but it does not directly enforce the restriction of internet access or deny access to specific Regions.

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

QUESTION 74

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

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

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

- B. Amazon EBS for maximum performance, Amazon EFS for durable data storage and Amazon S3 Glacier for archival storage
- C. Amazon EC2 instance store for maximum performance. Amazon EFS for durable data storage and Amazon S3 for archival storage
- D. Amazon EC2 Instance store for maximum performance. Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

Correct Answer: D

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html#instance-store-volumes>

QUESTION 75

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

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

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

Correct Answer: A

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-placementgroup.html>

"A cluster placement group is a logical grouping of instances within a single Availability Zone that benefit from low network latency, high network throughput"

QUESTION 76

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.

Correct Answer: B

Explanation

Explanation/Reference:

For self-managed DNS solution:

<https://aws.amazon.com/blogs/security/how-to-protect-a-self-managed-dns-service-against-ddos-attacks->

QUESTION 77

An ecommerce company has an order-processing application that uses Amazon API Gateway and an AWS Lambda function. The application stores data in an Amazon Aurora PostgreSQL database. During a recent sales event, a sudden surge in customer orders occurred. Some customers experienced timeouts and the application did not process the orders of those customers

A solutions architect determined that the CPU utilization and memory utilization were high on the database because of a large number of open connections. The solutions architect needs to prevent the timeout errors while making the least possible changes to the application.

Which solution will meet these requirements?

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

Correct Answer: B

Explanation

Explanation/Reference:

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/>

QUESTION 78

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 both 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.

Correct Answer: B

Explanation

Explanation/Reference:

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>

QUESTION 79

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 for PostgreSQL.
- 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.

Correct Answer: B

Explanation

Explanation/Reference:

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 Postgres (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/>

QUESTION 80

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.

Correct Answer: D

Explanation

QUESTION 81

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

Which actions should a solutions architect take to improve the query performance and reliability? (Select TWO.)

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

Correct Answer: CE

Explanation

QUESTION 82

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.

Correct Answer: C

Explanation

Explanation/Reference:

Application must be moved in Private subnet. This is a prerequisite in using VPC endpoints with S3 <https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

QUESTION 83

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.

Correct Answer: A

Explanation

Explanation/Reference:

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

QUESTION 84

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.

Correct Answer: A

Explanation

Explanation/Reference:

Deploying the application servers in an Auto Scaling group across multiple Availability Zones (AZs) ensures high availability and fault tolerance. An Auto Scaling group allows the application to scale horizontally to meet user demand. Using Amazon RDS DB instance in a Multi-AZ configuration ensures that the database is automatically replicated to a standby instance in a different AZ. This provides database redundancy and avoids any single point of failure.

QUESTION 85

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.

Correct Answer: C

Explanation

Explanation/Reference:

<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."

QUESTION 86

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.

Correct Answer: C

Explanation

Explanation/Reference:

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that helps protect web applications running on AWS from DDoS attacks. AWS Shield Advanced is an additional layer of protection that provides enhanced DDoS protection capabilities, including proactive monitoring and automatic inline mitigations, to help protect against even the largest and most sophisticated DDoS attacks. By enabling AWS Shield Advanced, the solutions architect can help protect the application from DDoS attacks and reduce the risk of disruption to the application.

QUESTION 87

A company wants to create a mobile app that allows users to stream slow-motion video clips on their mobile devices. Currently, the app captures video clips and uploads the video clips in raw format into an Amazon S3 bucket. The app retrieves these video clips directly from the S3 bucket. However, the videos are large in their raw format.

Users are experiencing issues with buffering and playback on mobile devices. The company wants to implement solutions to maximize the performance and scalability of the app while minimizing operational overhead.

Which combination of solutions will meet these requirements? (Select TWO.)

- A. Deploy Amazon CloudFront for content delivery and caching
- B. Use AWS DataSync to replicate the video files across AWS Regions in other S3 buckets
- C. Use Amazon Elastic Transcoder to convert the video files to more appropriate formats
- D. Deploy an Auto Scaling group of Amazon EC2 instances in Local Zones for content delivery and caching
- E. Deploy an Auto Scaling group of Amazon EC2 instances to convert the video files to more appropriate formats

Correct Answer: AC

Explanation

Explanation/Reference:

Amazon CloudFront is a content delivery network (CDN) that can help improve the performance and scalability of the app by caching content at edge locations, reducing latency, and improving the delivery of video clips to users. CloudFront can also provide features such as DDoS protection, SSL/TLS encryption, and content compression to optimize the delivery of video clips.

Amazon Elastic Transcoder is a service that can help optimize the video format for mobile devices, reducing the size of the video files, and improving the playback performance. Elastic Transcoder can also convert videos into multiple formats to support different devices and platforms.

QUESTION 88

A solution 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 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 Dynamo tables without exposing API credentials in the template.

What should the solution architect do to meet the 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 secret keys, and pass them to the application instances through the user data.

Correct Answer: B

Explanation

QUESTION 89

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

Correct Answer: B

Explanation

Explanation/Reference:

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. With RDS Proxy, failover times for Aurora and RDS databases are reduced by up to 66%.

<https://aws.amazon.com/rds/proxy/>

QUESTION 90

A company hosts an application on AWS. The application uses AWS Lambda functions and stores data in Amazon DynamoDB tables. The Lambda functions are connected to a VPC that does not have internet access.

The traffic to access DynamoDB must not travel across the internet. The application must have write access to only specific DynamoDB tables.

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

- A. Attach a VPC endpoint policy for DynamoDB to allow write access to only the specific DynamoDB tables.
- B. Attach a security group to the interface VPC endpoint to allow write access to only the specific DynamoDB tables.
- C. Create a resource-based IAM policy to grant write access to only the specific DynamoDB tables. Attach the policy to the DynamoDB tables.
- D. Create a gateway VPC endpoint for DynamoDB that is associated with the Lambda VPC. Ensure that the Lambda execution role can access the gateway VPC endpoint.
- E. Create an interface VPC endpoint for DynamoDB that is associated with the Lambda VPC. Ensure that the Lambda execution role can access the interface VPC endpoint.

Correct Answer: AE

Explanation

QUESTION 91

A company stores data in an Amazon Aurora PostgreSQL DB cluster. The company must store all the data for 5 years and must delete all the data after 5 years. The company also must indefinitely keep audit logs of actions that are performed within the database. Currently, the company has automated backups configured for Aurora.

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

- A. Take a manual snapshot of the DB cluster.
- B. Create a lifecycle policy for the automated backups.
- C. Configure automated backup retention for 5 years.
- D. Configure an Amazon CloudWatch Logs export for the DB cluster.
- E. Use AWS Backup to take the backups and to keep the backups for 5 years.

Correct Answer: DE

Explanation

Explanation/Reference:

AWS Backup provides a centralized console, automated backup scheduling, backup retention management, and backup monitoring and alerting. AWS Backup offers advanced features such as lifecycle policies to transition backups to a low-cost storage tier. It also includes backup storage and encryption independent from its source data, audit and compliance reporting capabilities with AWS Backup Audit Manager, and delete protection with AWS Backup Vault Lock.

QUESTION 92

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

Correct Answer: B

Explanation

QUESTION 93

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.

Correct Answer: B

Explanation

Explanation/Reference:

S3 provides a single control to automatically encrypt all new objects in a bucket with SSE-S3 or SSE-KMS. Unfortunately, these controls only affect new objects. If your bucket already contains millions of unencrypted objects, then turning on automatic encryption does not make your bucket secure as the unencrypted objects remain.

For S3 buckets with a large number of objects (millions to billions), use Amazon S3 Inventory to get a list of the unencrypted objects, and Amazon S3 Batch Operations to encrypt the large number of old, unencrypted files.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html>

QUESTION 94

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

Correct Answer: AC

Explanation

QUESTION 95

A company runs a latency-sensitive gaming service in the AWS Cloud. The gaming service runs on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). An Amazon DynamoDB table stores the gaming data. All the infrastructure is in a single AWS Region. The main user base is in that same Region.

A solutions architect needs to update the architecture to support a global expansion of the gaming service must operate with the least possible latency.

Which solution will meet these requirements?

- A. Create an Amazon CloudFront distribution in front of the ALB.
- B. Deploy an Amazon API Gateway regional API endpoint. Integrate the API endpoint with the ALB.
- C. Create an accelerator in AWS Global Accelerator. Add a listener. Configure the endpoint to point to the ALB.
- D. Deploy the ALB and the fleet of EC2 instances to another Region. Use Amazon Route 53 geolocation routing.

Correct Answer: C

Explanation

QUESTION 96

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.

Correct Answer: A

Explanation

Explanation/Reference:

AWS Transfer Family is a fully managed AWS service that you can use to transfer files into and out of Amazon Simple Storage Service (Amazon S3) storage or Amazon Elastic File System (Amazon EFS) file systems over the following protocols:

Secure Shell (SSH) File Transfer Protocol (SFTP): version 3
File Transfer Protocol Secure (FTPS)
File Transfer Protocol (FTP)
Application Statement 2 (AS2)

QUESTION 97

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.

Correct Answer: C

Explanation

QUESTION 98

An online retail company needs to run near-real-time analytics on website traffic to analyze top-selling products across different locations. The product purchase data and the user location details are sent to a third-party application that runs on premises The application processes the data and moves the data into the company's analytics engine.

The company needs to implement a cloud-based solution to make the data available for near-real-time analytics.

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

- A. Use Amazon Kinesis Data Streams to ingest the data Use AWS Lambda to transform the data Configure Lambda to write the data to Amazon Amazon OpenSearch Service (Amazon Elasticsearch Service)
- B. Configure Amazon Kinesis Data Streams to write the data to an Amazon S3 bucket Schedule an AWS Glue crawler job to enrich the data and update the AWS Glue Data Catalog Use Amazon Athena for analytics
- C. Configure Amazon Kinesis Data Streams to write the data to an Amazon S3 bucket Add an Apache Spark job on Amazon EMR to enrich the data in the S3 bucket and write the data to Amazon OpenSearch Service (Amazon Elasticsearch Service)
- D. Use Amazon Kinesis Data Firehose to ingest the data Enable Kinesis Data Firehose data transformation with AWS Lambda Configure Kinesis Data Firehose to write the data to Amazon OpenSearch Service (Amazon Elasticsearch Service).

Correct Answer: C

Explanation

QUESTION 99

A company stores millions of objects in Amazon S3. The data is in JSON format and Apache Parquet format. The data is partitioned and new objects are added daily. A solutions architect needs to create a solution so that employees can use SQL to perform one-time queries against all the data. The solution must avoid code changes and must minimize operational overhead.

Which solution will meet these requirements?

- A. Use S3 Select to perform queries against all the S3 objects
- B. Create an AWS Glue table and an AWS Glue crawler Schedule the crawler to run daily Perform queries with Amazon Athena
- C. Create an Amazon EMR cluster Set up C. EMR File System (EMRFS) to access the S3 bucket Perform queries with Apache Spark
- D. Create an Amazon Redshift cluster Schedule an AWS Lambda function to perform the COPY command on the Redshift cluster to load the S3 data Perform queries on the Redshift cluster.

Correct Answer: D

Explanation

QUESTION 100

A company deploys Amazon EC2 instances that run in a VPC The EC2 instances load source data into Amazon S3 buckets so that the data can be processed in the future According to compliance laws, the

data must not be transmitted over the public internet Servers in the company's on-premises data center will consume the output from an application that runs on the EC2 instances

Which solution will meet these requirements?

- A. Deploy an interface VPC endpoint for Amazon EC2 Create an AWS Site-to-Site VPN connection between the company and the VPC
- B. Deploy a gateway VPC endpoint for Amazon S3 Set up an AWS Direct Connect connection between the on-premises network and the VPC
- C. Set up an AWS Transit Gateway connection from the VPC to the S3 buckets Create an AWS Site-to-Site VPN connection between the company and the VPC
- D. Set up proxy EC2 instances that have routes to NAT gateways Configure the proxy EC2 instances to fetch S3 data and feed the application instances

Correct Answer: A

Explanation

QUESTION 101

A company has a business system that generates hundreds of reports each day. The business system saves the reports to a network share in CSV format The company needs to store this data in the AWS Cloud in near-real time for analysis.

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

- A. Use AWS DataSync to transfer the files to Amazon S3 Create a scheduled task that runs at the end of each day.
- B. Create an Amazon S3 File Gateway Update the business system to use a new network share from the S3 File Gateway.
- C. Use AWS DataSync to transfer the files to Amazon S3 Create an application that uses the DataSync API in the automation workflow.
- D. Deploy an AWS Transfer for SFTP endpoint Create a script that checks for new files on the network share and uploads the new files by using SFTP.

Correct Answer: B

Explanation

QUESTION 102

A company needs to develop a repeatable solution to process time-ordered information from websites around the world. The company collects the data from the websites by using Amazon Kinesis Data Streams and stores the data in Amazon S3.

The processing logic needs to collect events and handle data from the last 5 years.

The processing logic also must generate results in an S3 bucket so that a business intelligence application can analyze and compare the results. The processing must be repeated multiple times.

What should a solutions architect do to meet these requirements?

- A. Use Amazon S3 to collect events. Create an AWS Lambda function to process the events. Create different Lambda functions to handle repeated processing.
- B. Use Amazon EventBridge (Amazon CloudWatch Events) to collect events Set AWS Lambda as an event target. Use EventBridge (CloudWatch Events) to create an archive for the events and to replay the events.
- C. Use an Amazon Simple Queue Service (Amazon SQS) FIFO queue to collect events. Process the events by using Amazon EC2. Use AWS Step Function to create an archive for the events and to replay the events.
- D. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to collect events. Process the events by using Amazon Elastic Kubernetes Service (Amazon EKS) Use Amazon MSK to create an archive for the events and to replay the events.

Correct Answer: B
Explanation

QUESTION 103

A company has an ordering application that stores customer information in Amazon RDS for MySQL. During regular business hours, employees run one-time queries for reporting purposes. Timeouts are occurring during order processing because the reporting queries are taking a long time to run. The company needs to eliminate the timeouts without preventing employees from performing queries.

What should a solutions architect do to meet those requirements?

- A. Create a read replica Move reporting queries to the read replica.
- B. Create a read replica. Distribute the ordering application to the primary DB instance and the read replica.
- C. Migrate the ordering application to Amazon DynamoDB with on-demand capacity.
- D. Schedule the reporting queries for non-peak hours.

Correct Answer: A
Explanation

Explanation/Reference:

Creating a read replica allows the company to offload the reporting queries to a separate database instance, reducing the load on the primary database used for order processing. By moving the reporting queries to the read replica, the ordering application running on the primary DB instance can continue to process orders without timeouts due to the long-running reporting queries.

Option B is not a good solution because distributing the ordering application to the primary DB instance and the read replica does not address the issue of long-running reporting queries causing timeouts during order processing.

QUESTION 104

A company must save all the email messages that its employees send to customers for a period of 12 months. The messages are stored in a binary format and vary in size from 1 KB to 20 KB. The company has selected Amazon S3 as the storage service for the messages

Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO.)

- A. Create an S3 bucket policy that denies the s3 Delete Object action.
- B. Create an S3 lifecycle configuration that deletes the messages after 12 months.
- C. Upload the messages to Amazon S3 Use S3 Object Lock in governance mode
- D. Upload the messages to Amazon S3. Use S3 Object Lock in compliance mode.
- E. Use S3 Inventory Create an AWS Batch job that periodically scans the inventory and deletes the messages after 12 months

Correct Answer: BD
Explanation

QUESTION 105

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.

Correct Answer: D

Explanation

QUESTION 106

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

Which solution should the solution architect recommend?

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

Correct Answer: C

Explanation

QUESTION 107

A company wants to build a data lake on AWS from data that is stored in an on-premises Oracle relational database. The data lake must receive ongoing updates from the on-premises database.

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

- A. Use AWS DataSync to transfer the data to Amazon S3. Use AWS Glue to transform the data and integrate the data into a data lake.
- B. Use AWS Snowball to transfer the data to Amazon S3. Use AWS Batch to transform the data and integrate the data into a data lake.
- C. Use AWS Database Migration Service (AWS DMS) to transfer the data to Amazon S3 Use AWS Glue to transform the data and integrate the data into a data lake.
- D. Use an Amazon EC2 instance to transfer the data to Amazon S3. Configure the EC2 instance to transform the data and integrate the data into a data lake.

Correct Answer: C

Explanation

QUESTION 108

A company is planning on deploying a newly built application on AWS in a default VPC. The application will consist of a web layer and database layer. The web server was created in public subnets, and the MySQL database was created in private subnet. All subnets are created with the default network ACL settings, and the default security group in the VPC will be replaced with new custom security groups.

- A. Create a database server security group with inbound and outbound rules for MySQL port 3306 traffic to and from anywhere (0.0.0.0/0).
- B. Create a database server security group with an inbound rule for MySQL port 3300 and specify the

source as a web server security group.

- C. Create a web server security group within an inbound allow rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0) and an inbound deny rule for IP range 182. 20.0.0/16.
- D. Create a web server security group with an inbound rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0). Create network ACL inbound and outbound deny rules for IP range 182. 20.0.0/16.
- E. Create a web server security group with an inbound and outbound rules for HTTPS port 443 traffic to and from anywhere (0.0.0.0/0). Create a network ACL inbound deny rule for IP range 182. 20.0.0/16.

Correct Answer: BD

Explanation

QUESTION 109

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 (Amazon CloudWatch Events) 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.

Correct Answer: B

Explanation

Exam C

QUESTION 1

A company is reviewing a recent migration of a three-tier application to a VPC. The security team discovers that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.

What should a solutions architect do to correct this issue?

- A. Create security group rules using the instance ID as the source or destination.
- B. Create security group rules using the security group ID as the source or destination.
- C. Create security group rules using the VPC CIDR blocks as the source or destination.
- D. Create security group rules using the subnet CIDR blocks as the source or destination.

Correct Answer: B

Explanation

Explanation/Reference:

This way, the security team can ensure that the least privileged access is given to the application tiers by allowing only the necessary communication between the security groups. For example, the web tier security group should only allow incoming traffic from the load balancer security group and outgoing traffic to the application tier security group. This approach provides a more granular and secure way to control traffic between the different tiers of the application and also allows for easy modification of access if needed.

It's also worth noting that it's good practice to minimize the number of open ports and protocols, and use security groups as a first line of defense, in addition to network access control lists (ACLs) to control traffic between subnets.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules.html>

QUESTION 2

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 replicate 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 DMS) to continuously replicate data to an Aurora cluster in the secondary Region Remove the DB 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

Correct Answer: D

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html>

QUESTION 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

Correct Answer: B

Explanation

Explanation/Reference:

S3 and DynamoDB are the only services with Gateway endpoint options

QUESTION 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.

Correct Answer: AB

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/SetUp/latest/UserGuide/best-practices-root-user.html>

QUESTION 5

A solutions architect is designing the architecture of a new application being deployed to the AWS Cloud. The application will run on Amazon EC2 On-Demand Instances and will automatically scale across multiple Availability Zones. The EC2 instances will scale up and down frequently throughout the day. An Application Load Balancer (ALB) will handle the load distribution. The architecture needs to support distributed session data management. The company is willing to make changes to code if needed.

What should the solutions architect do to ensure that the architecture supports distributed session data management?

- A. Use Amazon ElastiCache to manage and store session data.
- B. Use session affinity (sticky sessions) of the ALB to manage session data.
- C. Use Session Manager from AWS Systems Manager to manage the session.
- D. Use the GetSessionToken API operation in AWS Security Token Service (AWS STS) to manage the session

Correct Answer: A

Explanation

Explanation/Reference:

<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.

QUESTION 6

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.

Correct Answer: BE

Explanation

Explanation/Reference:

- 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.

QUESTION 7

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

What should the solutions architect do to meet these requirements?

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

Correct Answer: C

Explanation

Explanation/Reference:

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 (1 AM) 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.

QUESTION 8

A company has a Microsoft .NET application that runs on an on-premises Windows Server. The application stores data by using an Oracle Database Standard Edition server. The company is planning a migration to AWS and wants to minimize development changes while moving the application. The AWS application environment should be highly available.

Which combination of actions should the company take to meet these requirements? (Select TWO)

- A. Refactor the application as serverless with AWS Lambda functions running .NET Core
- B. Rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment
- C. Replatform the application to run on Amazon EC2 with the Amazon Linux Amazon Machine Image (AMI)
- D. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Amazon DynamoDB in a Multi-AZ deployment
- E. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment

Correct Answer: BE

Explanation

Explanation/Reference:

B. Rehost the application in AWS Elastic Beanstalk with the .NET platform 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.

Rehosting the application in Elastic Beanstalk with the .NET platform can minimize development changes. Multi-AZ deployment of Elastic Beanstalk will increase the availability of application, so it meets the requirement of high availability.

Using AWS Database Migration Service (DMS) to migrate the database to Amazon RDS Oracle will ensure compatibility, so the application can continue to use the same database technology, and the development team can use their existing skills. It also migrates to a managed service, which will handle the availability, so the team do not have to worry about it. Multi-AZ deployment will increase the availability of the database.

QUESTION 9

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

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

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

Correct Answer: B

Explanation**Explanation/Reference:**

API Gateway + Lambda is the perfect solution for modern applications with serverless architecture.

QUESTION 10

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.

Correct Answer: A

Explanation**Explanation/Reference:**

Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets

QUESTION 11

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 Amazon 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.

Correct Answer: B

Explanation

QUESTION 12

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 the data.
- D. Create an AWS Lambda function that periodically queries and removes sensitive information from Lake Formation tables.

Correct Answer: B

Explanation

Explanation/Reference:

The best solution to meet the requirements with the least operational overhead is to create data filters to implement row-level security and cell-level security.

Data filters are a feature of Lake Formation that allow you to restrict access to data based on row and column values. This can be used to implement row-level security and cell-level security.

To implement row-level security, you would create a data filter that only allows users to access rows where the values in certain columns meet certain criteria. For example, you could create a data filter that only allows users to access rows where the value in the `customer_id` column matches the user's own customer ID.

QUESTION 13

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.

Correct Answer: C

Explanation

Explanation/Reference:

Creating an Amazon Simple Queue Service (SQS) message queue and placing messages on the queue for thumbnail generation can help separate the image upload and thumbnail generation processes.

QUESTION 14

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.

Correct Answer: B

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/kms/latest/developerguide/key-policy-modifying-external-accounts.html>

QUESTION 15

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.

Correct Answer: A

Explanation

Explanation/Reference:

A# By reducing the number of EC2 instances in the target group of the development environment to just one, you can lower the cost associated with running multiple instances. Since the development environment typically has lower traffic and does not require the same level of availability and scalability as the production environment, having a single instance is sufficient for testing and development purposes.

QUESTION 16

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 MySQL 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

Correct Answer: AB

Explanation

QUESTION 17

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.

Correct Answer: B

Explanation

Explanation/Reference:

Step 1: S3 inventory to get object list

Step 2 (If needed): Use S3 Select to filter

Step 3: S3 object operations to encrypt the unencrypted objects.

On the go object use default encryption.

<https://spin.atomicobject.com/2020/09/15/aws-s3-encrypt-existing-objects/>

QUESTION 18

A company has a popular gaming platform running on AWS. The application is sensitive to latency because latency can impact the user experience and introduce unfair advantages to some players. The application is deployed in every AWS Region. It runs on Amazon EC2 instances that are part of Auto Scaling groups configured behind Application Load Balancers (ALBs). A solutions architect needs to implement a mechanism to monitor the health of the application and redirect traffic to healthy endpoints.

Which solution meets these requirements?

- A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on, and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.

- B. Create an Amazon CloudFront distribution and specify the ALB as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
- C. Create an Amazon CloudFront distribution and specify Amazon S3 as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
- D. Configure an Amazon DynamoDB database to serve as the data store for the application. Create a DynamoDB Accelerator (DAX) cluster to act as the in-memory cache for DynamoDB hosting the application data.

Correct Answer: A

Explanation

Explanation/Reference:

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.

QUESTION 19

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 cached volumes

Correct Answer: D

Explanation

Explanation/Reference:

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.

QUESTION 20

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 files 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 the nearest

AWS Region Transfer the data over a VPN connection into the Region to store the data in Amazon S3

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 21

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.

Correct Answer: D

Explanation

Explanation/Reference:

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.

QUESTION 22

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

Correct Answer: D

Explanation

Explanation/Reference:

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.

This option provides the lowest-cost storage by using:

1. Amazon S3 for large-scale, durable, and inexpensive storage of the video content. S3 storage costs are significantly lower than EFS.
2. 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.
3. 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.

QUESTION 23

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.

Correct Answer: A

Explanation

QUESTION 24

A company is designing a shared storage solution for a gaming application that is hosted in the AWS Cloud. The company needs the ability to use SMB clients to access data. The solution must be fully managed.

Which AWS solution meets these requirements?

- A. Create an AWS DataSync task that shares the data as a mountable file system. Mount the file system to the application server.
- B. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
- C. Create an Amazon FSx for Windows File Server file system. Attach the file system to the origin server. Connect the application server to the file system.
- D. Create an Amazon S3 bucket. Assign an IAM role to the application to grant access to the S3 bucket. Mount the S3 bucket to the application server.

Correct Answer: C

Explanation

Explanation/Reference:

1. Amazon FSx for Windows File Server provides a fully managed native Windows file system that can be accessed using the industry-standard SMB protocol. This allows Windows clients like the gaming application to directly access file data.
2. FSx for Windows File Server handles time-consuming file system administration tasks like provisioning, setup, maintenance, file share management, backups, security, and software patching - reducing operational overhead.
3. FSx for Windows File Server supports high file system throughput, IOPS, and consistent low latencies.

required for performance-sensitive workloads. This makes it suitable for a gaming application.

4. The file system can be directly attached to EC2 instances, providing a performant shared storage solution for the gaming servers.

QUESTION 25

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 policy that grants read access to the S3 bucket
- B. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to the S3 bucket.
- C. Embed an access key and a secret key in the Lambda function's code to grant the required IAM permissions for read access to the S3 bucket
- D. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to all S3 buckets in the account

Correct Answer: B

Explanation

Explanation/Reference:

This solution satisfies the needs in the most secure manner:

- 1. An IAM role provides temporary credentials to the Lambda function to access AWS resources. The function does not have persistent credentials.
- 2. The IAM policy grants least privilege access by specifying read access only to the specific S3 bucket needed. Access is not granted to all S3 buckets.
- 3. If the Lambda function is compromised, the attacker would only gain access to the one specified S3 bucket. They would not receive broad access to resources.

QUESTION 26

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.

Correct Answer: D

Explanation

Explanation/Reference:

The solution that will meet the requirement with the least operational overhead is to implement API Gateway usage plans and API keys to limit access to premium content for users who do not have a subscription. Option A is incorrect because API caching and throttling are not designed for authentication or authorization purposes, and it does not provide access control. Option B is incorrect because although AWS WAF is a useful tool to protect web applications from common web exploits, it is not designed for authorization purposes, and it might require additional configuration, which increases the operational overhead.

Option C is incorrect because although IAM permissions can restrict access to data stored in a DynamoDB table, it does not provide a mechanism for limiting access to specific content based on the user subscription. Moreover, it might require a significant amount of additional IAM permissions configuration, which increases the operational overhead.

QUESTION 27

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.

Correct Answer: B

Explanation

Explanation/Reference:

The most secure solution to provide access to the database in VPC B from the application running on an EC2 instance in VPC A is to configure a VPC peering connection between the two VPCs. This will allow the application to access the database using the private IP addresses, and will not require any public IP addresses or Internet access. The traffic will be confined to the VPCs, and can be further secured with security group rules.

QUESTION 28

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 team reports that the application is vulnerable to SQL 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 SQL injection attempts automatically.

Correct Answer: A

Explanation

Explanation/Reference:

AWS WAF is a managed service that protects web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF enables customers to create custom rules that block common attack patterns, such as SQL injection attacks.

By using AWS WAF in front of the ALB and associating the appropriate web ACLs with AWS WAF, the company can protect its website application from SQL injection attacks. AWS WAF will inspect incoming traffic to the website application and block requests that match the defined SQL injection patterns in the web ACLs. This will help to prevent SQL injection attacks from reaching the application, thereby improving the overall security posture of the application.

QUESTION 29

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

Correct Answer: B

Explanation

Explanation/Reference:

Key words: geographically dispersed, UDP.

Geographically dispersed (related to UDP) - Global Accelerator - multiple entrances worldwide to the AWS network to provide better transfer rates.

UDP - NLB (Network Load Balancer).

QUESTION 30

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 .

Correct Answer: C

Explanation

Explanation/Reference:

minimizes operational maintenance = NGW

QUESTION 31

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.

Correct Answer: A

Explanation

Explanation/Reference:

AWS Systems Manager Session Manager provides secure shell access to EC2 instances without the need for SSH keys. It meets the security requirement to remove shared SSH keys while minimizing administrative overhead.

QUESTION 32

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.

Correct Answer: A

Explanation

Explanation/Reference:

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.

QUESTION 33

A company has a custom application with embedded credentials that retrieves information from an Amazon RDS MySQL DB instance. Management says the application must be made more secure with the least amount of programming effort.

What should a solutions architect do to meet these requirements?

- A. Use AWS Key Management Service (AWS KMS) customer master keys (CMKs) to create keys. Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation.
- B. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Create an AWS Lambda function that rotates the credentials in Secret Manager.
- C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.
- D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

Correct Answer: C

Explanation

Explanation/Reference:

C is a valid solution for securing the custom application with the least amount of programming effort. It involves creating credentials on the RDS for MySQL database for the application user and storing them in AWS Secrets Manager. The application can then be configured to load the database credentials from Secrets Manager. Additionally, the solution includes setting up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager, which will automatically rotate the credentials at a specified interval without requiring any programming effort.

QUESTION 34

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 a policy 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.

Correct Answer: BD

Explanation

Explanation/Reference:

Option B is the simplest and most direct way to enable encryption for the EBS volumes associated with the EKS cluster. After the EKS cluster is created, you can manually locate the EBS volumes and enable encryption using the customer managed key through the AWS Management Console, AWS CLI, or SDKs.

Option D involves creating an IAM role with a policy that grants permission to the customer managed key, and then associating that role with the EKS cluster. This allows the EKS cluster to have the necessary permissions to access the customer managed key for encrypting and decrypting data on the EBS volumes. This approach is more automated and can be easily managed through IAM, which provides centralized control and reduces operational overhead.

QUESTION 35

A company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight, the application becomes much slower when the month-end financial calculation batch runs. This causes the CPU utilization of the EC2 instances 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 front of the ALB.
- B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.
- C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.
- D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances.

Correct Answer: C

Explanation

Explanation/Reference:

By configuring a scheduled scaling policy, the EC2 Auto Scaling group can proactively launch additional EC2 instances before the CPU utilization peaks to 100%. This will ensure that the application can handle the workload during the month-end financial calculation batch, and avoid any disruption or downtime.

Configuring a simple scaling policy based on CPU utilization or adding Amazon CloudFront distribution or Amazon ElastiCache will not directly address the issue of handling the monthly peak workload.

QUESTION 36

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.

Correct Answer: D

Explanation

Explanation/Reference:

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.

QUESTION 37

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

Which storage solution meets these requirements?

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

Correct Answer: C

Explanation

QUESTION 38

A company has implemented a self-managed DNS service on AWS. The solution consists of the following:

1. Amazon EC2 instances in different AWS Regions
2. Endpoints of a standard accelerator in 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.

Correct Answer: A

Explanation

Explanation/Reference:

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.

QUESTION 39

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.

Correct Answer: AD

Explanation

Explanation/Reference:

"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."

<https://www.techtarget.com/searchaws/tip/Amazon-FSx-vs-EFS-Compare-the-AWS-file-services>

QUESTION 40

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.

Correct Answer: B

Explanation

Explanation/Reference:

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.

QUESTION 41

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.

Correct Answer: C

Explanation

Explanation/Reference:

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:

1. AMI automated backups provide point-in-time recovery for the stateless app tier.
2. RDS automated backups provide point-in-time recovery for the database.

QUESTION 42

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

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

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

Correct Answer: A

Explanation

Explanation/Reference:

Publishing data to Amazon Kinesis Data Streams can support ingestion rates as high as 1 MB/s and provide real-time data processing. Kinesis Data Analytics can query the ingested data in real-time with low latency, and the solution can scale as needed to accommodate increases in ingestion rates or querying.

needs. This solution also ensures minimal data loss in the event of an EC2 instance reboot since Kinesis Data Streams has a persistent data store for up to 7 days by default.

QUESTION 43

A company manages its own Amazon EC2 instances that run MySQL databases. The company is manually managing replication and scaling as demand increases or decreases. The company needs a new solution that simplifies the process of adding or removing compute capacity to or from its database tier as needed. The solution also must offer improved performance, scaling, and durability with minimal effort from operations.

Which solution meets these requirements?

- A. Migrate the databases to Amazon Aurora Serverless for Aurora MySQL.
- B. Migrate the databases to Amazon Aurora Serverless for Aurora PostgreSQL.
- C. Combine the databases into one larger MySQL database. Run the larger database on larger EC2 instances.
- D. Create an EC2 Auto Scaling group for the database tier. Migrate the existing databases to the new environment.

Correct Answer: A

Explanation

Explanation/Reference:

<https://aws.amazon.com/rds/aurora/serverless/>

QUESTION 44

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.

Correct Answer: A

Explanation

Explanation/Reference:

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>

QUESTION 45

A company has an application that is backed by 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-demand 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 Amazon EventBridge 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.

Correct Answer: A

Explanation

Explanation/Reference:

This solution satisfies the requirements in the following ways:

- 1. AWS Backup will automatically take full backups of the DynamoDB table on the schedule defined in the backup plan (the first of each month).
- 2. The lifecycle policy can transition backups to cold storage after 6 months, meeting that requirement.
- 3. Setting a 7-year retention period in the backup plan will ensure each backup is retained for 7 years as required.
- 4. AWS Backup manages the backup jobs and lifecycle policies, requiring no custom scripting or management.

QUESTION 46

An online learning company is migrating to the AWS Cloud. The company maintains its student records in a PostgreSQL database. The company needs a solution in which its data is available and online across multiple AWS Regions at all times.

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

- A. Migrate the PostgreSQL database to a PostgreSQL cluster on Amazon EC2 instances.
- B. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance with the Multi-AZ feature turned on.
- C. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Create a read replica in another Region.
- D. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Set up DB snapshots to be copied to another Region.

Correct Answer: C

Explanation

Explanation/Reference:

"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/>

QUESTION 47

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 frequently. 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

Correct Answer: BC

Explanation

QUESTION 48

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

What should the solutions architect do to accomplish this?

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

Correct Answer: B

Explanation

Explanation/Reference:

Lambda server-less is scalable and elastic than EC2 api gateway solution

QUESTION 49

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

Correct Answer: B

Explanation

Explanation/Reference:

Amazon Athena can be used to analyze data in S3 buckets using standard SQL queries without requiring any data transformation. By using Athena, a solutions architect can easily and efficiently query the

CloudFront logs stored in the S3 bucket. The results of the queries can be visualized using Amazon QuickSight, which provides powerful data visualization capabilities and easy-to-use dashboards. Together, Athena and QuickSight provide a cost-effective and scalable solution to analyze CloudFront logs and build visualizations.

QUESTION 50

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.

Correct Answer: AD

Explanation

Explanation/Reference:

<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/>

QUESTION 51

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.

Correct Answer: A

Explanation

Explanation/Reference:

AWS Step Functions is a serverless workflow service that makes it easy to coordinate distributed applications and microservices using visual workflows. It is an ideal solution for designing architectures for distributed applications that involve multiple AWS services and serverless functions, as it allows us to orchestrate the flow of our application components using visual workflows. AWS Step Functions also integrates with other AWS services like AWS Lambda, Amazon EC2, and Amazon ECS, and it has built-in error handling and retry mechanisms. This option provides a serverless solution with the least operational overhead for building the application.

QUESTION 52

A company wants to use high performance computing (HPC) infrastructure on AWS for financial risk modeling. The company's HPC workloads run on Linux. Each HPC workflow runs on hundreds of Amazon EC2 Spot Instances, is short-lived, and generates thousands of output files that are ultimately stored in persistent storage for analytics and long-term future use.

The company seeks a cloud storage solution that permits the copying of on-premises data to long-term persistent storage to make data available for processing by all EC2 instances. The solution should also be a high performance file system that is integrated with persistent storage to read and write datasets and output files. Which combination of AWS services meets these requirements?

- A. Amazon FSx for Lustre integrated with Amazon S3
- B. Amazon FSx for Windows File Server integrated with Amazon S3
- C. Amazon S3 Glacier integrated with Amazon Elastic Block Store (Amazon EBS)
- D. Amazon S3 bucket with a VPC endpoint integrated with an Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume

Correct Answer: A

Explanation

Explanation/Reference:

<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.

QUESTION 53

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

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

Correct Answer: A

Explanation

Explanation/Reference:

<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.

QUESTION 54

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 baseline 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 requirements with the LEAST operational overhead?

- A. Create a dynamic scaling policy for the Auto Scaling group. Configure the policy to scale based on the CPU utilization metric to 60%.
- B. Create a scheduled scaling policy 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 Lambda 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%.

Correct Answer: C

Explanation

QUESTION 55

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

Correct Answer: B

Explanation

Explanation/Reference:

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>)

QUESTION 56

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.

Correct Answer: D

Explanation

Explanation/Reference:

<https://aws.amazon.com/directconnect/pricing/> <https://aws.amazon.com/blogs/aws/aws-data-transfer-prices-reduced/>

QUESTION 57

A company hosts 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 distrupctions, 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.

Correct Answer: B
Explanation

Explanation/Reference:

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

QUESTION 58

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

What should the solutions architect recommend?

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

Correct Answer: C
Explanation

Explanation/Reference:

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>

QUESTION 59

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 scaling 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 experience additional lag during periods of peak load. A solutions architect must reduce the replication lag as much as possible. The solutions 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 stored procedures with Aurora MySQL native functions.
- B. Deploy an Amazon ElastiCache for Redis cluster in front 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 a large number of read capacity units (RCUs) to support the required throughput, and configure on-demand capacity scaling. Replace the stored procedures with DynamoDB streams. optimized EC2 instances for all replica nodes. Maintain the stored procedures on the EC2 instances.

Correct Answer: A

Explanation

Explanation/Reference:

Using Cache required huge changes in the application. Several things need to change to use cache in front of the DB in the application.

QUESTION 60

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.

Correct Answer: CE

Explanation

Explanation/Reference:

"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

QUESTION 61

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 transferred. 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.

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 62

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

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

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

Correct Answer: C

Explanation

Explanation/Reference:

Load balancer is public-facing, accepting all traffic coming towards the VPC (0.0.0.0/0). The web server needs to trust traffic originating from the ALB. The DB will only trust traffic originating from the Web server on port 3306 for MySQL.

QUESTION 63

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.

Correct Answer: CE

Explanation

Explanation/Reference:

Option C, creating an Amazon Route 53 multivalue answer routing policy, is the correct choice. With this routing policy, Route 53 returns multiple IP addresses for the same domain name, allowing the traffic to be distributed randomly among the available EC2 instances. This ensures that the traffic is evenly distributed across the instances launched in different Availability Zones, achieving the desired randomness and load balancing.

Option E is the correct choice. By launching instances in different Availability Zones, the company ensures that there are redundant copies of the application running in separate physical locations, providing fault tolerance. With two instances in one Availability Zone and two instances in another, traffic can be distributed randomly among them, improving availability and load balancing.

<https://aws.amazon.com/premiumsupport/knowledge-center/multivalue-versus-simple-policies/>

QUESTION 64

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:

1. A group of Amazon EC2 instances that run in an Amazon EC2 Auto Scaling group to collect orders from the application
2. 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.

Correct Answer: D

Explanation

Explanation/Reference:

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.

QUESTION 65

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.

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 66

A company needs to ingest and handle large amounts of streaming data that its application generates. The application runs on Amazon EC2 instances and sends data to Amazon Kinesis Data Streams, which is configured with default settings. Every other day the application consumes the data and writes the data to an Amazon S3 bucket for business intelligence (BI) processing. The company observes that Amazon S3 is not receiving all the data that the application sends to Kinesis Data Streams.

What should a solutions architect do to resolve this issue?

- A. Update the Kinesis Data Streams default settings by modifying the data retention period.
- B. Update the application to use the Kinesis Producer Library (KPL) to send the data to Kinesis Data Streams.
- C. Update the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams.
- D. Turn on S3 Versioning within the S3 bucket to preserve every version of every object that is ingested in the S3 bucket.

Correct Answer: A

Explanation

Explanation/Reference:

Need to increase default retention period

QUESTION 67

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.

Correct Answer: D

Explanation**Explanation/Reference:**

1. The company wants to maintain local access to all the data. Only stored volumes keep the complete dataset on-premises, providing low-latency access. Cached volumes only cache a subset locally.
2. The company wants the data backed up on AWS. With stored volumes, periodic backups (snapshots) of the on-premises data are sent to S3, providing durable and scalable backup storage.
3. The company wants the data transfer to AWS to be automatic and secure. Storage Gateway provides an encrypted connection between the on-premises gateway and AWS storage. Backups to S3 are sent asynchronously and automatically based on the backup schedule configured.

QUESTION 68

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.

Correct Answer: C

Explanation**Explanation/Reference:**

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.

QUESTION 69

A company serves a dynamic website from a fleet 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 for 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.

Correct Answer: B

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/header-caching.html>

QUESTION 70

A company is moving its data management application to AWS. The company wants to transition to an event-driven architecture. The architecture needs to be more distributed and to use serverless concepts while 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 steps.
- 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 in AWS Step Functions. Use Step Functions to create a state machine. Use the state machine to invoke AWS Lambda functions to process the workflow steps.

Correct Answer: D

Explanation

Explanation/Reference:

Step Functions is based on state machines and tasks. A state machine is a workflow. A task is a state in a workflow that represents a single unit of work that another AWS service performs. Each step in a workflow is a state.

Depending on your use case, you can have Step Functions call AWS services, such as Lambda, to perform tasks.

<https://docs.aws.amazon.com/step-functions/latest/dg/welcome.html>

QUESTION 71

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

Correct Answer: D

Explanation

Explanation/Reference:

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.

QUESTION 72

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 incurring 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 Region.

Correct Answer: B

Explanation

QUESTION 73

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 communicates 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 ElastiCache 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.

Correct Answer: B

Explanation

Explanation/Reference:

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.

QUESTION 74

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

Correct Answer: D

Explanation

QUESTION 75

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

Correct Answer: A

Explanation

Explanation/Reference:

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.

QUESTION 76

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 lifecycle 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

Correct Answer: AD

Explanation

Explanation/Reference:

CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS Command Line Interface (CLI), and AWS SDKs and APIs. By enabling CloudTrail, the company can track user activity and changes to AWS resources, and monitor compliance with internal policies and external regulations.

AWS Config provides a detailed inventory of the AWS resources in your account, and continuously records changes to the configurations of those resources. By creating rules in AWS Config, the company can automate the evaluation of resource configurations against desired state, and receive alerts when configurations drift from compliance.

QUESTION 77

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

Correct Answer: DE

Explanation

QUESTION 78

An IAM user made several configuration changes to AWS resources in 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

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 79

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.

Correct Answer: A

Explanation

Explanation/Reference:

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/>

QUESTION 80

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.

Correct Answer: C

Explanation

Explanation/Reference:

A subnet must reside within a single Availability Zone.

<https://aws.amazon.com/vpc/faqs/#:~:text=Can%20a%20subnet%20span%20Availability,within%20a%20single%20Availability%20Zone.>

QUESTION 81

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.

Correct Answer: B

Explanation

QUESTION 82

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

Correct Answer: D

Explanation

Explanation/Reference:

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.

QUESTION 83

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 192.168.0.0/24. The solution 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 CIDR 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

Correct Answer: D

Explanation

Explanation/Reference:

Option A (10.0.1.0/32) is invalid - a /32 CIDR prefix is a host route, not a VPC range.

Option B (192.168.0.0/24) overlaps the development VPC and so cannot be used.

Option C (192.168.1.0/32) is invalid - a /32 CIDR prefix is a host route, not a VPC range.

Option D (10.0.1.0/24) satisfies the non-overlapping CIDR requirement but is a larger block than needed.

Since only two VPCs need to be peered, a /24 block provides more addresses than necessary.

QUESTION 84

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 as 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 job to 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 file 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 processed. Use an S3 event notification to invoke the Lambda function when the files arrive.

Correct Answer: D

Explanation

QUESTION 85

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 in 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 role to the Lambda function

Correct Answer: D

Explanation

Explanation/Reference:

Create Lambda execution role and attach existing S3 IAM role to the lambda function

QUESTION 86

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.

Correct Answer: A

Explanation

Explanation/Reference:

1. 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.
2. 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.
3. 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.
4. Auto Scaling across zones could launch instances in AZs that increase data transfer charges. It may reduce network throughput, impacting performance.

QUESTION 87

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

Correct Answer: B

Explanation

QUESTION 88

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.

Correct Answer: D

Explanation

Explanation/Reference:

This solution will resolve the issue by allowing the internet traffic to reach the EC2 instances. By creating public subnets in each availability zone and associating them with the ALB, the internet traffic will be directed to the ALB. Updating the route tables for the public subnets with a route to the private subnets will allow the traffic to be routed to the private subnets where the EC2 instances reside. This ensures that the traffic reaches the correct target group, and the security group of the instances allows inbound traffic from the internet.

<https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/>

QUESTION 89

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 in 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 application produces.

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

- A. Create an 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 Redshift.
- B. Develop a Python script that runs on Amazon EC2 instances to convert the .CSV files to SQL files. Invoke the Python script on a 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, transform, and load (ETL) job to process the .CSV files and store the processed data in an Amazon Redshift table.

Correct Answer: A

Explanation

Explanation/Reference:

A would be the best solution as it involves the least operational overhead. With this solution, an AWS Glue ETL job is created to process the .csv files and store the processed data directly in Amazon Redshift. This is a serverless approach that does not require any infrastructure to be provisioned, configured, or maintained. AWS Glue provides a fully managed, pay-as-you-go ETL service that can be easily configured to process data from S3 and load it into Amazon Redshift. This approach allows the legacy application to continue to produce data in the CSV format that it currently uses, while providing the new COTS application with the ability to analyze the data using complex SQL queries.

QUESTION 90

An ecommerce company needs to run a scheduled daily job to aggregate and filter sales records for analytics. The company stores the sales records in an Amazon S3 bucket. Each object can be up to 10 GB 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 job 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 event that calls the API and invokes the function.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type and an Auto Scaling group with at least one EC2 instance. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.

Correct Answer: C

Explanation**Explanation/Reference:**

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.

QUESTION 91

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.

Correct Answer: C

Explanation

Explanation/Reference:

<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.>

QUESTION 92

A company has an application that collects data from IoT sensors on automobiles. The data is streamed and stored in Amazon S3 through Amazon Kinesis Data Firehose. The data produces trillions of S3 objects each year. Each morning, the company uses the data from the previous 30 days to retrain a suite of machine learning (ML) models.

Four times each year, the company uses the data from the previous 12 months to perform analysis and train other ML models. The data must be available with minimal delay for up to 1 year. After 1 year, the data must be retained for archival purposes.

Which storage solution meets these requirements MOST cost-effectively?

- A. Use the S3 Intelligent-Tiering storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
- B. Use the S3 Intelligent-Tiering storage class. Configure S3 Intelligent-Tiering to automatically move objects to S3 Glacier Deep Archive after 1 year.
- C. Use the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
- D. Use the S3 Standard storage class. Create an S3 Lifecycle policy to transition objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days, and then to S3 Glacier Deep Archive after 1 year.

Correct Answer: D

Explanation

QUESTION 93

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.

Correct Answer: D
Explanation

Explanation/Reference:

This solution leverages AWS Lake Formation to ingest data from the Aurora MySQL database into the S3 data lake, while enforcing column-level access control for QuickSight users. Lake Formation can be used to create and manage the data lake's metadata and enforce security and governance policies, including column-level access control. This solution then uses Amazon Athena as the data source in QuickSight to query the data in the S3 data lake. This solution minimizes operational overhead by leveraging AWS services to manage and secure the data, and by using a standard query service (Amazon Athena) to provide a SQL interface to the data.

QUESTION 94

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 to provide signed URLs to stream content.
- D. Set up AWS Client VPN between the mobile app and the AWS environment to stream content.

Correct Answer: C
Explanation

Explanation/Reference:

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.

QUESTION 95

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.

Correct Answer: C
Explanation

Explanation/Reference:

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to the following locations: Amazon CloudWatch Logs, Amazon S3, or Amazon Kinesis Data Firehose. After you create a flow log, you can retrieve and view the flow log records in the log group, bucket, or delivery stream that you configured.

Flow logs can help you with a number of tasks, such as:

1. Diagnosing overly restrictive security group rules
2. Monitoring the traffic that is reaching your instance
3. Determining the direction of the traffic to and from the network interfaces

Ref link: <https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>

QUESTION 96

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.

Correct Answer: A

Explanation

Explanation/Reference:

The maximum AWS Lambda function run time is 15 minutes. If a Lambda function runs for longer than 15 minutes, it will be terminated by AWS Lambda. This limit is in place to prevent the Lambda environment from becoming stale and to ensure that resources are available for other functions.

QUESTION 97

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 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.

Correct Answer: B

Explanation

Explanation/Reference:

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.

Answer A is incorrect because attaching an IAM role to the EC2 instances does not automatically encrypt

the EBS volumes.

Answer C is incorrect because adding an EC2 instance tag does not ensure that the EBS volumes are encrypted.

QUESTION 98

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.

Correct Answer: B

Explanation

Explanation/Reference:

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.

QUESTION 99

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.

Correct Answer: A

Explanation

Explanation/Reference:

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.

QUESTION 100

A company is hosting a web application from an Amazon S3 bucket. The application uses Amazon Cognito as an identity provider to authenticate users and return a JSON Web Token (JWT) that provides access to protected resources that are stored 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 content.
- B. Update the S3 ACL to allow the application to access the protected content
- C. Redeploy the application to Amazon S3 to prevent eventually consistent reads in 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 the Identity pool and grant users the proper permissions to access the protected content

Correct Answer: A

Explanation

Explanation/Reference:

Services access other services via IAM Roles. Hence why updating AWS Cognito identity pool to assume proper IAM Role is the right solution.

QUESTION 101

A company wants to restrict access to the content of one of its many web applications and to protect the content by using authorization techniques available on AWS. The company wants to implement a serverless architecture and an authentication solution for fewer than 100 users. The solution needs to integrate with the main web application and serve web content globally. The solution must also scale as the company's user base grows while providing lowest login latency possible.

- A. Use Amazon Cognito for authentication. Use Lambda@Edge for authorization. Use Amazon CloudFront to serve the web application globally.
- B. Use AWS Directory Service for Microsoft Active Directory for authentication. Use AWS Lambda for authorization. Use an Application Load Balancer to serve the web application globally.
- C. Use Amazon Cognito for authentication. Use AWS Lambda for authorization. Use Amazon S3 Transfer Acceleration to 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.

Correct Answer: A

Explanation

QUESTION 102

A solutions architect must secure a VPC network that hosts Amazon EC2 instances. The EC2 instances contain highly sensitive data and run in a private subnet. According to company policy, the EC2 instances that run in 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 rules. 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

Correct Answer: A

Explanation

Explanation/Reference:

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>

Exam D

QUESTION 1

A company has a business system that generates hundreds of reports each day. The business system saves the reports to a network share in CSV format. The company needs to store this data in the AWS Cloud in near-real time for analysis.

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

- A. Use AWS DataSync to transfer the files to Amazon S3. Create a scheduled task that runs at the end of each day.
- B. Create an Amazon S3 File Gateway. Update the business system to use a new network share from the S3 File Gateway.
- C. Use AWS DataSync to transfer the files to Amazon S3. Create an application that uses the DataSync API in the automation workflow.
- D. Deploy an AWS Transfer for SFTP endpoint. Create a script that checks for new files on the network share and uploads the new files by using SFTP.

Correct Answer: B

Explanation

Explanation/Reference:

1. It presents a simple network file share interface that the business system can write to, just like a standard network share. This requires minimal changes to the business system.
2. The S3 File Gateway automatically uploads all files written to the share to an S3 bucket in the background. This handles the transfer and upload to S3 without requiring any scheduled tasks, scripts or automation.
3. All ongoing management like monitoring, scaling, patching etc. is handled by AWS for the S3 File Gateway.

QUESTION 2

A company is storing petabytes of data in Amazon S3 Standard. The data is stored in multiple S3 buckets and is accessed with varying frequency. The company does not know access patterns for all the data. The company needs to implement a solution for each S3 bucket to optimize the cost of S3 usage.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering.
- B. Use the S3 storage class analysis tool to determine the correct tier for each object in the S3 bucket. Move each object to the identified storage tier.
- C. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Glacier Instant Retrieval.
- D. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 One Zone-Infrequent Access (S3 One Zone-IA).

Correct Answer: A

Explanation

Explanation/Reference:

Creating an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering would be the most efficient solution to optimize the cost of S3 usage. S3 Intelligent-Tiering is a storage class that automatically moves objects between two access tiers (frequent and infrequent) based on changing access patterns. It is a cost-effective solution that does not require any manual intervention to move data to different storage classes, unlike the other options.

QUESTION 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? (Choose 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 read replica for the RDS DB instance.
- E. Configure a Multi-AZ deployment for the RDS DB instance.

Correct Answer: BD

Explanation

Explanation/Reference:

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.

QUESTION 4

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 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 an EC2 Instance 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 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 functions 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.

Correct Answer: C

Explanation

Explanation/Reference:

Answer C is the best solution that meets the company's requirements.

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.

QUESTION 5

A solutions architect needs to allow team members to access Amazon S3 buckets in two different AWS accounts: a development account and a production account. The team currently has access to S3 buckets in the development account by using unique IAM users that are assigned to an IAM group that has appropriate permissions in the account.

The solutions architect has created an IAM role in the production account. The role has a policy that grants access to an S3 bucket in the production account.

Which solution will meet these requirements while complying with the principle of least privilege?

- A. Attach the Administrator Access policy to the development account users.
- B. Add the development account as a principal in the trust policy of the role in the production account.
- C. Turn off the S3 Block Public Access feature on the S3 bucket in the production account.
- D. Create a user in the production account with unique credentials for each team member.

Correct Answer: B

Explanation

Explanation/Reference:

By adding the development account as a principal in the trust policy of the IAM role in the production account, you are allowing users from the development account to assume the role in the production account. This allows the team members to access the S3 bucket in the production account without granting them unnecessary privileges.

QUESTION 6

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 IAM 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? (Choose two.)

- A. In the Amazon EC2 console, select the EBS encryption account attribute and define a default encryption key.
- B. Create an IAM 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 SCP. 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 IAM 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.

Correct Answer: CE

Explanation

Explanation/Reference:

SCPs are a great way to enforce policies across an entire AWS Organization, preventing users from creating resources that do not comply with the set policies.

In AWS Management Console, one can go to EC2 dashboard -> Settings -> Data encryption -> Check "Always encrypt new EBS volumes" and choose a default KMS key. This ensures that every new EBS volume created will be encrypted by default, regardless of how it is created.

QUESTION 7

A company wants to use an Amazon RDS for PostgreSQL DB cluster to simplify time-consuming database administrative tasks for production database workloads. The company wants to ensure that its database is highly available and will provide automatic failover support in most scenarios in less than 40 seconds. The company wants to offload reads off of the primary instance and keep costs as low as possible.

Which solution will meet these requirements?

- A. Use an Amazon RDS Multi-AZ DB instance deployment. Create one read replica and point the read workload to the read replica.
- B. Use an Amazon RDS Multi-AZ DB cluster deployment. Create two read replicas and point the read workload to the read replicas.
- C. Use an Amazon RDS Multi-AZ DB instance deployment. Point the read workload to the secondary instances in the Multi-AZ pair.
- D. Use an Amazon RDS Multi-AZ DB cluster deployment. Point the read workload to the reader endpoint.

Correct Answer: D

Explanation**Explanation/Reference:**

The company wants high availability, automatic failover support in less than 40 seconds, read offloading from the primary instance, and cost-effectiveness.

Answer D is the best choice for several reasons:

1. Amazon RDS Multi-AZ deployments provide high availability and automatic failover support.
2. In a Multi-AZ DB cluster, Amazon RDS automatically provisions and maintains a standby in a different Availability Zone. If a failure occurs, Amazon RDS performs an automatic failover to the standby, minimizing downtime.
3. The "Reader endpoint" for an Amazon RDS DB cluster provides load-balancing support for read-only connections to the DB cluster. Directing read traffic to the reader endpoint helps in offloading read operations from the primary instance.

QUESTION 8

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.

Correct Answer: B

Explanation

Explanation/Reference:

EFS is serverless. There is no reference in S3 about IOPS

QUESTION 9

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 S3 at startup and load the data into memory. Users access the models through an asynchronous API. Users can send a request or a batch of requests and specify where the results should be sent.

The company provides models to hundreds of users. The usage patterns for the models are irregular. Some models could be unused for days or weeks. Other models could receive batches of thousands of requests at a time.

Which 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.

Correct Answer: D

Explanation

Explanation/Reference:

asynchronous=SQS, microservices=ECS.

Use AWS Auto Scaling to adjust the number of ECS services.

QUESTION 10

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? (Choose two.)

- A. Role
- B. Group
- C. Organization
- D. Amazon Elastic Container Service (Amazon ECS) resource
- E. Amazon EC2 resource

Correct Answer: AB

Explanation

Explanation/Reference:

identity-based policy used for role and group

QUESTION 11

A company is running a custom application on Amazon EC2 On-Demand Instances. The application has frontend nodes that need to run 24 hours a day, 7 days a week and backend nodes that need to run only for a short time based on workload. The number of backend nodes varies during the day.

The company needs to scale out and scale in more instances based on workload.

Which solution will meet these requirements MOST cost-effectively?

- A. Use Reserved Instances for the frontend nodes. Use AWS Fargate for the backend nodes.
- B. Use Reserved Instances for the frontend nodes. Use Spot Instances for the backend nodes.
- C. Use Spot Instances for the frontend nodes. Use Reserved Instances for the backend nodes.
- D. Use Spot Instances for the frontend nodes. Use AWS Fargate for the backend nodes.

Correct Answer: B

Explanation

Explanation/Reference:

short time = SPOT

QUESTION 12

A company uses high block storage capacity to runs its workloads on premises. The company's daily peak input and output transactions per second are not more than 15,000 IOPS. The company wants to migrate the workloads to Amazon EC2 and to provision disk performance independent of storage capacity.

Which Amazon Elastic Block Store (Amazon EBS) volume type will meet these requirements MOST cost-effectively?

- A. GP2 volume type
- B. io2 volume type
- C. GP3 volume type
- D. io1 volume type

Correct Answer: C

Explanation

Explanation/Reference:

The GP3 (General Purpose SSD) volume type in Amazon Elastic Block Store (EBS) is the most cost-effective option for the given requirements. GP3 volumes offer a balance of price and performance and are suitable for a wide range of workloads, including those with moderate I/O needs.

GP3 volumes allow you to provision performance independently from storage capacity, which means you can adjust the baseline performance (measured in IOPS) and throughput (measured in MiB/s) separately from the volume size. This flexibility allows you to optimize your costs while meeting the workload requirements.

In this case, since the company's daily peak input and output transactions per second are not more than 15,000 IOPS, GP3 volumes provide a suitable and cost-effective option for their workloads.

QUESTION 13

A company needs to store data from its healthcare application. The application's data frequently changes. A new regulation requires audit 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 S3. 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.

Correct Answer: A

Explanation

Explanation/Reference:

AWS DataSync is a service designed specifically for securely and efficiently transferring large amounts of data between on-premises storage systems and AWS services like Amazon S3. It provides a reliable and optimized way to migrate data while maintaining data integrity.

AWS CloudTrail, on the other hand, is a service that logs and monitors management events in your AWS account. While it can capture data events for certain services, its primary focus is on tracking management actions like API calls and configuration changes.

Therefore, using AWS DataSync to transfer the existing data to Amazon S3 and leveraging AWS CloudTrail to log data events aligns with the requirement of securely migrating the data and ensuring audit access at all levels, as specified by the new regulation.

QUESTION 14

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.

Correct Answer: B

Explanation

Explanation/Reference:

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.

QUESTION 15

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 IAM 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 IAM 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 IAM 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 IAM 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.

Correct Answer: B

Explanation

Explanation/Reference:

Role key word and trusted service lambda

QUESTION 16

The following IAM policy is attached to an IAM group. This is the only policy applied to the group.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "1",
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:Region": "us-east-1"
        }
      }
    },
    {
      "Sid": "2",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {
        "BoolIfExists": {"aws:MultiFactorAuthPresent": false}
      }
    }
  ]
}

```

What are the effective IAM permissions of this policy for group members?

- A. Group members are permitted any Amazon EC2 action within the us-east-1 Region. Statements after the Allow permission are not applied.
- B. Group members are denied any Amazon EC2 permissions in the us-east-1 Region unless they are logged in with multi-factor authentication (MFA).
- C. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for all Regions when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action.
- D. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action within the us-east-1 Region.

Correct Answer: D
Explanation

QUESTION 17

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? (Choose 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).

Correct Answer: BC

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/amazonglacier/latest/dev/introduction.html>

QUESTION 18

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

What should a solutions architect do to meet these requirements?

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

Correct Answer: B

Explanation

Explanation/Reference:

<https://aws.amazon.com/jp/blogs/news/building-a-real-time-gaming-leaderboard-with-amazon-elasticache-for-redis/>

QUESTION 19

An ecommerce company wants to use machine learning (ML) algorithms to build and train models. The company will use the models to visualize complex scenarios and to detect trends in customer data. The architecture team wants to integrate its ML models with a reporting platform to analyze the augmented data and use the data directly in its business intelligence dashboards.

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

- A. Use AWS Glue to create an ML transform to build and train models. Use Amazon OpenSearch Service to visualize the data.
- B. Use Amazon SageMaker to build and train models. Use Amazon QuickSight to visualize the data.
- C. Use a pre-built ML Amazon Machine Image (AMI) from the AWS Marketplace to build and train models. Use Amazon OpenSearch Service to visualize the data.
- D. Use Amazon QuickSight to build and train models by using calculated fields. Use Amazon QuickSight to visualize the data.

Correct Answer: B

Explanation

Explanation/Reference:

Business intelligence, visualiations = AmazonQuickSight
ML = Amazon SageMaker

QUESTION 20

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 authorized principals.
- D. Create custom Amazon CloudWatch logs to prevent tag modification.

Correct Answer: C

Explanation**Explanation/Reference:**

https://docs.aws.amazon.com/ja_jp/organizations/latest/userguide/orgs_manage_policies_scps_examples_tagging.html

QUESTION 21

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.

Correct Answer: A

Explanation**Explanation/Reference:**

By configuring the DynamoDB table as a global table, you can replicate the table data across multiple AWS Regions, including the primary Region and the disaster recovery Region. This ensures that data is available in both Regions and can be seamlessly accessed during a failover event.

QUESTION 22

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 with 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.

Correct Answer: A

Explanation

QUESTION 23

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.

Correct Answer: A

Explanation

QUESTION 24

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

What should a solutions architect recommend?

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

Correct Answer: B

Explanation

Explanation/Reference:

AWS WAF (Web Application Firewall) is a service that provides protection for web applications against common web exploits. By associating AWS WAF with the Application Load Balancer (ALB), you can inspect incoming traffic and define rules to allow or block requests based on various criteria.

QUESTION 25

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 S3 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.

Correct Answer: D

Explanation

Explanation/Reference:

Option D (Creating an encrypted snapshot of the database, sharing the snapshot, and allowing access to the AWS Key Management Service encryption key) is generally considered a better option for sharing the database with the auditor in terms of security and control.

QUESTION 26

A solutions architect configured a VPC that has a small range of IP addresses. The number of Amazon EC2 instances that are in the VPC is increasing, and there is an insufficient number of IP addresses for future workloads.

Which solution resolves this issue with the LEAST operational overhead?

- A. Add an additional IPv4 CIDR block to increase the number of IP addresses and create additional subnets in the VPC. Create new resources in the new subnets by using the new CIDR.
- B. Create a second VPC with additional subnets. Use a peering connection to connect the second VPC with the first VPC. Update the routes and create new resources in the subnets of the second VPC.
- C. Use AWS Transit Gateway to add a transit gateway and connect a second VPC with the first VPC. Update the routes of the transit gateway and VPCs. Create new resources in the subnets of the second VPC.
- D. Create a second VPC. Create a Site-to-Site VPN connection between the first VPC and the second VPC by using a VPN-hosted solution on Amazon EC2 and a virtual private gateway. Update the route between VPCs to the traffic through the VPN. Create new resources in the subnets of the second VPC.

Correct Answer: A

Explanation

Explanation/Reference:

You assign a single CIDR IP address range as the primary CIDR block when you create a VPC and can add up to four secondary CIDR blocks after creation of the VPC.

QUESTION 27

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? (Choose 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.

Correct Answer: AC

Explanation

Explanation/Reference:

Migrating data from MySQL by using an Amazon S3 bucket

You can copy the full and incremental backup files from your source MySQL version 5.7 database to an Amazon S3 bucket, and then restore an Amazon Aurora MySQL DB cluster from those files.

This option can be considerably faster than migrating data using mysqldump, because using mysqldump replays all of the commands to recreate the schema and data from your source database in your new Aurora MySQL DB cluster.

By copying your source MySQL data files, Aurora MySQL can immediately use those files as the data for an Aurora MySQL DB cluster.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Migrating.ExtMySQL.html>

QUESTION 28

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.

Correct Answer: C

Explanation

Explanation/Reference:

Static Web Content = S3 Always.

CloudFront = Closer to the users locations since it will cache in the Edge nodes.

QUESTION 29

A company stores several petabytes of data across multiple AWS accounts. The company uses AWS Lake Formation to manage its data lake. The company's data science team wants to securely share selective data from its accounts with the company's engineering team for analytical purposes.

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

- A. Copy the required data to a common account. Create an IAM access role in that account. Grant access by specifying a permission policy that includes users from the engineering team accounts as trusted entities.
- B. Use the Lake Formation permissions Grant command in each account where the data is stored to allow the required engineering team users to access the data.
- C. Use AWS Data Exchange to privately publish the required data to the required engineering team accounts.
- D. Use Lake Formation tag-based access control to authorize and grant cross-account permissions for the required data to the engineering team accounts.

Correct Answer: D

Explanation

Explanation/Reference:

By utilizing Lake Formation's tag-based access control, you can define tags and tag-based policies to grant selective access to the required data for the engineering team accounts. This approach allows you to control access at a granular level without the need to copy or move the data to a common account or manage permissions individually in each account. It provides a centralized and scalable solution for securely sharing data across accounts with minimal operational overhead.

QUESTION 30

A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world. Application users will be able to download and upload unique data up to gigabytes in size.

The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.

What should a solutions architect do to accomplish this?

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

Correct Answer: A

Explanation

Explanation/Reference:

Amazon S3 (Simple Storage Service) is a highly scalable object storage service provided by AWS. It allows you to store and retrieve any amount of data from anywhere on the web. With Amazon S3, you can host static websites, store and deliver large media files, and manage data for backup and restore.

Transfer Acceleration is a feature of Amazon S3 that utilizes the AWS global infrastructure to accelerate file transfers to and from Amazon S3. It uses optimized network paths and parallelization techniques to speed up data transfer, especially for large files and over long distances.

By using Amazon S3 with Transfer Acceleration, the web application can benefit from faster upload and download speeds, reducing latency and improving overall performance for users in different geographic regions. This solution is cost-effective as it leverages the existing Amazon S3 infrastructure and eliminates the need for additional compute resources.

QUESTION 31

A company has hired a solutions architect to design a reliable architecture for its application. The application consists of one Amazon RDS DB instance and two manually provisioned Amazon EC2 instances that run web servers. The EC2 instances are located in a single Availability Zone.

An employee recently deleted the DB instance, and the application was unavailable for 24 hours as a result. The company is concerned with the overall reliability of its environment.

What should the solutions architect do to maximize reliability of the application's infrastructure?

- A. Delete one EC2 instance and enable termination protection on the other EC2 instance. Update the DB instance to be Multi-AZ, and enable deletion protection.
- B. Update the DB instance to be Multi-AZ, and enable deletion protection. Place the EC2 instances behind an Application Load Balancer, and run them in an EC2 Auto Scaling group across multiple Availability Zones.
- C. Create an additional DB instance along with an Amazon API Gateway and an AWS Lambda function. Configure the application to invoke the Lambda function through API Gateway. Have the Lambda function write the data to the two DB instances.
- D. Place the EC2 instances in an EC2 Auto Scaling group that has multiple subnets located in multiple Availability Zones. Use Spot Instances instead of On-Demand Instances. Set up Amazon CloudWatch alarms to monitor the health of the instances. Update the DB instance to be Multi-AZ, and enable

deletion protection.

Correct Answer: B

Explanation

Explanation/Reference:

HA ensured by DB in Multi-AZ and EC2 in AG

QUESTION 32

A company is storing 700 terabytes of data on a large network-attached storage (NAS) system in its 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.

Correct Answer: A

Explanation

Explanation/Reference:

By leveraging AWS DataSync in combination with AWS Direct Connect, the company can efficiently and securely transfer its 700 terabytes of data to an Amazon S3 bucket without disruption. The solution allows continued access and updates to the data during the transfer window, ensuring business continuity throughout the migration process.

QUESTION 33

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 Versioning 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.

Correct Answer: D

Explanation

Explanation/Reference:

You need AWS Batch to re-apply certain config to files that were already in S3, like encryption

QUESTION 34

A company has a stateless web application that runs on AWS Lambda functions that are invoked by Amazon API Gateway. The company wants to deploy the application across multiple AWS Regions to

provide Regional failover capabilities.

What should a solutions architect do to route traffic to multiple Regions?

- A. 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.

Correct Answer: A

Explanation

Explanation/Reference:

To route traffic to multiple AWS Regions and provide regional failover capabilities for a stateless web application running on AWS Lambda functions invoked by Amazon API Gateway, you can use Amazon Route 53 with an active-active failover configuration.

By creating Amazon Route 53 health checks for each Region and configuring an active-active failover configuration, Route 53 can monitor the health of the endpoints in each Region and route traffic to healthy endpoints. In the event of a failure in one Region, Route 53 automatically routes traffic to the healthy endpoints in other Regions.

This setup ensures high availability and failover capabilities for your web application across multiple AWS Regions.

QUESTION 35

A company has two VPCs named Management and Production. The Management VPC uses VPNs through a customer gateway to connect to a single device in the data center. The Production VPC uses a virtual private gateway with two attached AWS Direct Connect connections. The Management and Production VPCs both use a single VPC peering connection to allow communication between the applications.

What should a solutions architect do to mitigate any single point of failure in this architecture?

- A. Add a set of VPNs between the Management and Production VPCs.
- B. Add a second virtual private gateway and attach it to the Management VPC.
- C. Add a second set of VPNs to the Management VPC from a second customer gateway device.
- D. Add a second VPC peering connection between the Management VPC and the Production VPC.

Correct Answer: C

Explanation

Explanation/Reference:

Redundant VPN connections: Instead of relying on a single device in the data center, the Management VPC should have redundant VPN connections established through multiple customer gateways. This will ensure high availability and fault tolerance in case one of the VPN connections or customer gateways fails.

QUESTION 36

A company runs its application on an Oracle database. The company plans to quickly migrate to AWS because of limited resources for the database, backup administration, and data center maintenance. The application uses third-party database features that require privileged access.

Which solution will help the company migrate the database to AWS MOST cost-effectively?

- A. Migrate the database to Amazon RDS for Oracle. Replace third-party features with cloud services.
- B. Migrate the database to Amazon RDS Custom for Oracle. Customize the database settings to support third-party features.
- C. Migrate the database to an Amazon EC2 Amazon Machine Image (AMI) for Oracle. Customize the

database settings to support third-party features.

- D. Migrate the database to Amazon RDS for PostgreSQL by rewriting the application code to remove dependency on Oracle APEX.

Correct Answer: B

Explanation

Explanation/Reference:

<https://aws.amazon.com/about-aws/whats-new/2021/10/amazon-rds-custom-oracle/>

QUESTION 37

A company has a three-tier web application that is in a single server. The company wants to migrate the application to the AWS Cloud. The company also wants the application to align with the AWS Well-Architected Framework and to be consistent with AWS recommended best practices for security, scalability, and resiliency.

Which combination of solutions will meet these requirements? (Choose three.)

- A. Create a VPC across two Availability Zones with the application's existing architecture. Host the application with existing architecture on an Amazon EC2 instance in a private subnet in each Availability Zone with EC2 Auto Scaling groups.
Secure the EC2 instance with security groups and network access control lists (network ACLs).
- B. Set up security groups and network access control lists (network ACLs) to control access to the database layer. Set up a single Amazon RDS database in a private subnet.
- C. Create a VPC across two Availability Zones. Refactor the application to host the web tier, application tier, and database tier. Host each tier on its own private subnet with Auto Scaling groups for the web tier and application tier.
- D. Use a single Amazon RDS database. Allow database access only from the application tier security group.
- E. Use Elastic Load Balancers in front of the web tier. Control access by using security groups containing references to each layer's security groups.
- F. Use an Amazon RDS database Multi-AZ cluster deployment in private subnets. Allow database access only from application tier security groups.

Correct Answer: CEF

Explanation

Explanation/Reference:

C. This solution follows the recommended architecture pattern of separating the web, application, and database tiers into different subnets. It provides better security, scalability, and fault tolerance. E. By using Elastic Load Balancers (ELBs), you can distribute traffic to multiple instances of the web tier, increasing scalability and availability. Controlling access through security groups allows for fine-grained control and ensures only authorized traffic reaches each layer.

F. Deploying an Amazon RDS database in a Multi-AZ configuration provides high availability and automatic failover. Placing the database in private subnets enhances security. Allowing database access only from the application tier security groups limits exposure and follows the principle of least privilege.

QUESTION 38

A company is migrating its applications and databases to the AWS Cloud. The company will use Amazon Elastic Container Service (Amazon ECS), AWS Direct Connect, and Amazon RDS.

Which activities will be managed by the company's operational team? (Choose three.)

- A. Management of the Amazon RDS infrastructure layer, operating system, and platforms
- B. Creation of an Amazon RDS DB instance and configuring the scheduled maintenance window
- C. Configuration of additional software components on Amazon ECS for monitoring, patch management, log management, and host intrusion detection
- D. Installation of patches for all minor and major database versions for Amazon RDS
- E. Ensure the physical security of the Amazon RDS infrastructure in the data center
- F. Encryption of the data that moves in transit through Direct Connect

Correct Answer: BCF

Explanation

Explanation/Reference:

B: Mentioned RDS

C: Mentioned ECS

F: Mentioned Direct connect

QUESTION 39

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.

Correct Answer: B

Explanation

Explanation/Reference:

AWS Lambda automatically scales resources to handle the workload, so you don't have to worry about managing the underlying infrastructure. It provisions the necessary compute resources based on the configured memory size (1 GB in this case) and executes the job in a serverless environment.

By using Amazon EventBridge, you can create a scheduled rule to trigger the Lambda function every hour, ensuring that the job runs on the desired interval.

QUESTION 40

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.

Correct Answer: D

Explanation

Explanation/Reference:

Must not alter the files for the duration of the retention period = Compliance Mode

<https://docs.aws.amazon.com/aws-backup/latest/devguide/vault-lock.html>

QUESTION 41

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 inventory. 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.

Correct Answer: C

Explanation

Explanation/Reference:

Workload Discovery on AWS is a service that helps visualize and understand the architecture of your workloads across multiple AWS accounts and Regions. It automatically discovers and maps the relationships between resources, providing an accurate representation of the architecture.

QUESTION 42

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? (Choose 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 IAM user for AWS Budgets to run budget actions with the required permissions.
- D. Create an IAM 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 IAM 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 IAM identity created with the appropriate service control policy (SCP) to prevent provisioning of additional resources.

Correct Answer: BDF

Explanation

Explanation/Reference:

https://docs.aws.amazon.com/ja_jp/awsaccountbilling/latest/aboutv2/view-billing-dashboard.html

QUESTION 43

A company runs applications on Amazon EC2 instances in one AWS Region. The company wants to back up the EC2 instances to a second Region. The company also wants to provision EC2 resources in the second Region and manage the EC2 instances centrally from one AWS account.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a disaster recovery (DR) plan that has a similar number of EC2 instances in the second Region. Configure data replication.
- B. Create point-in-time Amazon Elastic Block Store (Amazon EBS) snapshots of the EC2 instances. Copy the snapshots to the second Region periodically.
- C. Create a backup plan by using AWS Backup. Configure cross-Region backup to the second Region for the EC2 instances.
- D. Deploy a similar number of EC2 instances in the second Region. Use AWS DataSync to transfer the

data from the source Region to the second Region.

Correct Answer: C

Explanation

Explanation/Reference:

Using AWS Backup, you can create backup plans that automate the backup process for your EC2 instances. By configuring cross-Region backup, you can ensure that backups are replicated to the second Region, providing a disaster recovery capability. This solution is cost-effective as it leverages AWS Backup's built-in features and eliminates the need for manual snapshot management or deploying and managing additional EC2 instances in the second Region.

QUESTION 44

A company that uses AWS is building an application to transfer data to a product manufacturer. The company has its own identity provider (IdP). The company wants the IdP to authenticate application users while the users use the application to transfer data. The company must use Applicability Statement 2 (AS2) protocol.

Which solution will meet these requirements?

- A. Use AWS DataSync to transfer the data. Create an AWS Lambda function for IdP authentication.
- B. Use Amazon AppFlow flows to transfer the data. Create an Amazon Elastic Container Service (Amazon ECS) task for IdP authentication.
- C. Use AWS Transfer Family to transfer the data. Create an AWS Lambda function for IdP authentication.
- D. Use AWS Storage Gateway to transfer the data. Create an Amazon Cognito identity pool for IdP authentication.

Correct Answer: C

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/transfer/latest/userguide/custom-identity-provider-users.html>

QUESTION 45

A solutions architect is designing a RESTAPI 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? (Choose two.)

- A. Amazon EC2
- B. AWS Lambda
- C. Amazon RDS
- D. Amazon DynamoDB
- E. Amazon Elastic Kubernetes Services (Amazon EKS)

Correct Answer: BC

Explanation

Explanation/Reference:

"The application will require that the data is in a relational format" so DynamoDB is out. RDS is the choice. Lambda is serverless.

QUESTION 46

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.

Correct Answer: A

Explanation

Explanation/Reference:

By activating a user-defined cost allocation tag named "department" and creating a cost report in Cost Explorer that groups by the tag name and filters by EC2, the accounting team will be able to track and attribute costs to specific departments across all AWS accounts within the organization. This approach allows for consistent cost allocation and reporting regardless of the AWS account structure.

QUESTION 47

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.

- 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.

Correct Answer: C

Explanation

Explanation/Reference:

Amazon AppFlow is a fully managed integration service that allows you to securely transfer data between different SaaS applications and AWS services. It provides built-in encryption options and supports encryption in transit using SSL/TLS protocols. With AppFlow, you can configure the data transfer flow from Salesforce to Amazon S3, ensuring data encryption at rest by utilizing AWS KMS CMKs.

QUESTION 48

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.

Correct Answer: B

Explanation

Explanation/Reference:

AWS Global Accelerator is a better solution for the mobile gaming app than CloudFront

QUESTION 49

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.

Correct Answer: B

Explanation

Explanation/Reference:

By decoupling the write operation from the processing operation using SQS, you ensure that the orders are reliably stored in the queue, regardless of the processing capacity of the EC2 instances. This allows the processing to be performed at a scalable rate based on the available EC2 instances, improving the overall reliability and speed of order processing.

QUESTION 50

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 Scala job
- 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

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 51

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

Which solution meets these requirements?

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

Correct Answer: A

Explanation

Explanation/Reference:

Compared to other solutions that involve creating new instances, restoring snapshots, or setting up replication manually, converting to a Multi-AZ deployment is a simpler and more streamlined approach with lower overhead.

Overall, option A offers a cost-effective and efficient way to minimize database downtime without requiring significant changes or additional complexities.

QUESTION 52

A company is developing an application to support customer demands. The company wants to deploy the application on multiple Amazon EC2 Nitro-based instances within the same Availability Zone. The company also wants to give the application the ability to write to multiple block storage volumes in multiple EC2 Nitro-based instances simultaneously to achieve higher application availability.

Which solution will meet these requirements?

- A. Use General Purpose SSD (gp3) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
- B. Use Throughput Optimized HDD (st1) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
- C. Use Provisioned IOPS SSD (io2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
- D. Use General Purpose SSD (gp2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach

Correct Answer: C

Explanation

Explanation/Reference:

C. Use Provisioned IOPS SSD (io2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach.

While both option C and option D can support Amazon EBS Multi-Attach, using Provisioned IOPS SSD (io2) EBS volumes provides higher performance and lower latency compared to General Purpose SSD (gp2) volumes. This makes io2 volumes better suited for demanding and mission-critical applications where performance is crucial.

If the goal is to achieve higher application availability and ensure optimal performance, using Provisioned IOPS SSD (io2) EBS volumes with Multi-Attach will provide the best results.

QUESTION 53

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

Correct Answer: A

Explanation

Explanation/Reference:

By combining Multi-AZ EC2 Auto Scaling and an Application Load Balancer, you achieve high availability for the EC2 instances hosting your stateless two-tier application.

QUESTION 54

A company uses AWS Organizations. A member account has purchased a Compute Savings Plan. Because of changes in the workloads inside the member account, the account no longer receives the full benefit of the Compute Savings Plan commitment. The company uses less than 50% of its purchased compute power.

- A. Turn on discount sharing from the Billing Preferences section of the account console in the member account that purchased the Compute Savings Plan.
- B. Turn on discount sharing from the Billing Preferences section of the account console in the company's Organizations management account.
- C. Migrate additional compute workloads from another AWS account to the account that has the Compute Savings Plan.
- D. Sell the excess Savings Plan commitment in the Reserved Instance Marketplace.

Correct Answer: B

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ri-turn-off.html>

Sign in to the AWS Management Console and open the AWS Billing console at <https://console.aws.amazon.com/billing/>

Note

Ensure you're logged in to the management account of your AWS Organizations.

QUESTION 55

A company is developing a microservices application that will provide a search catalog for customers. The company must use REST APIs to present the frontend of the application to users. The REST APIs must access the backend services that the company hosts in containers in private VPC subnets.

Which solution will meet these requirements?

- A. Design a WebSocket API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a private VPC link for API Gateway to access Amazon ECS.
- B. Design a REST API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a private VPC link for API Gateway to access

Amazon ECS.

- C. Design a WebSocket API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a security group for API Gateway to access Amazon ECS.
- D. Design a REST API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a security group for API Gateway to access Amazon ECS.

Correct Answer: B

Explanation

Explanation/Reference:

REST API with Amazon API Gateway: REST APIs are the appropriate choice for providing the frontend of the microservices application. Amazon API Gateway allows you to design, deploy, and manage REST APIs at scale.

Amazon ECS in a Private Subnet: Hosting the application in Amazon ECS in a private subnet ensures that the containers are securely deployed within the VPC and not directly exposed to the public internet.

Private VPC Link: To enable the REST API in API Gateway to access the backend services hosted in Amazon ECS, you can create a private VPC link. This establishes a private network connection between the API Gateway and ECS containers, allowing secure communication without traversing the public internet.

QUESTION 56

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 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-IA)
- B. Use S3 Lifecycle rules to transition objects from S3 Standard to Standard-Infrequent Access (S3 Standard-IA)
- C. Use S3 Lifecycle rules to 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

Correct Answer: C

Explanation

Explanation/Reference:

S3 Inventory can't move files to another class

QUESTION 57

A company has applications hosted on Amazon EC2 instances with IPv6 addresses. The applications must initiate communications with other external applications using the internet. However the company's security policy states that any external service cannot initiate a connection to the EC2 instances.

What should a solutions architect recommend to resolve this issue?

- A. Create a NAT gateway and make it the destination of the subnet's route table
- B. Create an internet gateway and make it the destination of the subnet's route table
- C. Create a virtual private gateway and make it the destination of the subnet's route table
- D. Create an egress-only internet gateway and make it the destination of the subnet's route table

Correct Answer: D

Explanation

Explanation/Reference:

An egress-only internet gateway (EIGW) is specifically designed for IPv6-only VPCs and provides outbound IPv6 internet access while blocking inbound IPv6 traffic. It satisfies the requirement of preventing external services from initiating connections to the EC2 instances while allowing the instances to initiate outbound communications.

QUESTION 58

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

Correct Answer: C

Explanation**Explanation/Reference:**

Gateway VPC Endpoint: A gateway VPC endpoint enables private connectivity between a VPC and Amazon S3. It allows direct access to Amazon S3 without the need for internet gateways, NAT devices, VPN connections, or AWS Direct Connect.

Minimize Internet Traffic: By creating a gateway VPC endpoint for Amazon S3 and associating it with all route tables in the VPC, the traffic between the VPC and Amazon S3 will be kept within the AWS network. This helps in minimizing data transfer costs and prevents the need for traffic to traverse the internet.

Cost-Effective: With a gateway VPC endpoint, the data transfer between the application running in the VPC and the S3 bucket stays within the AWS network, reducing the need for data transfer across the internet. This can result in cost savings, especially when dealing with large amounts of data.

QUESTION 59

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

Which method should the solutions architect select?

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

Correct Answer: A

Explanation**Explanation/Reference:**

Amazon DynamoDB Accelerator (DAX): DAX is an in-memory cache for DynamoDB that provides low-latency access to frequently accessed data. By configuring DAX for the new messages table, read requests for the table will be served from the DAX cache, significantly reducing the latency.

Minimal Application Changes: With DAX, the application code can be updated to use the DAX endpoint instead of the standard DynamoDB endpoint. This change is relatively minimal and does not require extensive modifications to the application's data access logic.

Low Latency: DAX caches frequently accessed data in memory, allowing subsequent read requests for the same data to be served with minimal latency. This ensures that new messages can be read by users with minimal delay.

QUESTION 60

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.

- 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

Correct Answer: A

Explanation

Explanation/Reference:

Amazon CloudFront: CloudFront is a content delivery network (CDN) service that caches content at edge locations worldwide. By creating a CloudFront distribution, static content from the website can be cached at edge locations, reducing the load on the EC2 instances and improving the overall performance.

Caching Static Files: Since the website serves static content, caching these files at CloudFront edge locations can significantly reduce the number of requests forwarded to the EC2 instances. This helps to lower the overall cost by offloading traffic from the instances and reducing the data transfer costs.

QUESTION 61

A company has multiple VPCs across AWS Regions to support and run workloads that are isolated from workloads in other Regions. Because of a recent application launch requirement, the company's VPCs must communicate with all other VPCs across all Regions.

Which solution will meet these requirements with the LEAST amount of administrative effort?

- A. Use VPC peering to manage VPC communication in a single Region. Use VPC peering across Regions to manage VPC communications.
- B. Use AWS Direct Connect gateways across all Regions to connect VPCs across regions and manage VPC communications.
- C. Use AWS Transit Gateway to manage VPC communication in a single Region and Transit Gateway peering across Regions to manage VPC communications.
- D. Use AWS PrivateLink across all Regions to connect VPCs across Regions and manage VPC communications

Correct Answer: C

Explanation

Explanation/Reference:

AWS Transit Gateway: Transit Gateway is a highly scalable service that simplifies network connectivity between VPCs and on-premises networks. By using a Transit Gateway in a single Region, you can centralize VPC communication management and reduce administrative effort.

Transit Gateway Peering: Transit Gateway supports peering connections across AWS Regions, allowing you to establish connectivity between VPCs in different Regions without the need for complex VPC peering configurations. This simplifies the management of VPC communications across Regions.

QUESTION 62

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

Correct Answer: C

Explanation

Explanation/Reference:

AWS Backup can manage replication of EFS to another region as mentioned below
<https://docs.aws.amazon.com/efs/latest/ug/awsbackup.html>

EFS Replication can replicate your file system data to another Region or within the same Region without requiring additional infrastructure or a custom process. Amazon EFS Replication automatically and transparently replicates your data to a second file system in a Region or AZ of your choice. You can use the Amazon EFS console, AWS CLI, and APIs to activate replication on an existing file system. EFS Replication is continual and provides a recovery point objective (RPO) and a recovery time objective (RTO) of minutes, helping you meet your compliance and business continuity goals.

QUESTION 63

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 IAM groups. The solutions architect will add the new users to IAM 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 IAM groups
- C. Create an IAM policy that grants least privilege permission. Attach the policy to the IAM groups
- D. Create IAM roles. Associate the roles with a permissions boundary that defines the maximum permissions

Correct Answer: C

Explanation

Explanation/Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups_manage_attach-policy.html

Attaching a policy to an IAM user group

QUESTION 64

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


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

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

```

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

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

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

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

```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Correct Answer: D
Explanation

QUESTION 65

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 IAM permissions to any AWS principals that access the S3 bucket until the designated date.
- B. Create a new Amazon S3 bucket with S3 Versioning enabled. Use S3 Object Lock with a retention period in accordance with the designated date. Configure the S3 bucket for static website hosting. Set an S3 bucket policy to allow read- only access to the objects.

- C. Create a new Amazon S3 bucket with S3 Versioning enabled. Configure an event trigger to run an AWS Lambda function in case of object modification or deletion. Configure the Lambda function to replace the objects with the original versions from a private S3 bucket.
- D. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Select the folder that contains the files. Use S3 Object Lock with a retention period in accordance with the designated date. Grant read-only IAM permissions to any AWS principals that access the S3 bucket.

Correct Answer: B

Explanation

Explanation/Reference:

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

QUESTION 66

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.

Correct Answer: B

Explanation

QUESTION 67

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

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

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

Correct Answer: B

Explanation

Explanation/Reference:

A VPC endpoint enables you to privately access AWS services without requiring internet gateways, NAT gateways, VPN connections, or AWS Direct Connect connections. It allows you to connect your VPC directly to supported AWS services, such as Amazon S3, over a private connection within the AWS network.

By creating a VPC endpoint for Amazon S3, the traffic between your EC2 instances and S3 will stay within the AWS network and won't traverse the public internet. This provides a more secure and compliant solution, as the data transfer remains within the private network boundaries.

QUESTION 68

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

Correct Answer: B

Explanation

Explanation/Reference:

In the write-through caching strategy, when a customer adds or updates an item in the database, the application first writes the data to the database and then updates the cache with the same data. This ensures that the cache is always synchronized with the database, as every write operation triggers an update to the cache.

QUESTION 69

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

Correct Answer: B

Explanation

Explanation/Reference:

AWS DataSync is a fully managed data transfer service that simplifies and automates the process of moving data between on-premises storage and Amazon S3. It provides secure and efficient data transfer with built-in encryption, ensuring that the data is encrypted in transit.

By using AWS DataSync, the company can easily migrate the 100 GB of historical data from their on-premises location to an S3 bucket. DataSync will handle the encryption of data in transit and ensure secure transfer.

QUESTION 70

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.

Correct Answer: C

Explanation

Explanation/Reference:

By using Amazon ECS on AWS Fargate, you can run the job in a containerized environment while benefiting from the serverless nature of Fargate, where you only pay for the resources used during the job's execution. Creating a scheduled task based on the container image of the job ensures that it runs every 10 minutes, meeting the required schedule. This solution provides flexibility, scalability, and cost-effectiveness.

QUESTION 71

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? (Choose 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 IAM 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 IAM 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 IAM Identity Center (AWS Single Sign-On) in the organization. Configure IAM Identity Center, and integrate it with the company's corporate directory service.

Correct Answer: AE

Explanation

Explanation/Reference:

A. By creating a new organization in AWS Organizations, you can establish a consolidated multi-account architecture. This allows you to create and manage multiple AWS accounts for different business units under a single organization.

E. Setting up AWS IAM Identity Center (AWS Single Sign-On) within the organization enables you to integrate it with the company's corporate directory service. This integration allows for centralized authentication, where users can sign in using their corporate credentials and access the AWS accounts within the organization.

Together, these actions create a centralized, multi-account architecture that leverages AWS Organizations for account management and AWS IAM Identity Center (AWS Single Sign-On) for authentication and access control.

QUESTION 72

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

What is the MOST cost-effective solution?

- A. Store the video archives in Amazon S3 Glacier and use Expedited retrievals.
- B. Store the video archives in Amazon S3 Glacier and use Standard retrievals.
- C. Store the video archives in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).

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

Correct Answer: A

Explanation

Explanation/Reference:

By choosing Expedited retrievals in Amazon S3 Glacier, you can reduce the retrieval time to minutes, making it suitable for scenarios where quick access is required. Expedited retrievals come with a higher cost per retrieval compared to standard retrievals but provide faster access to your archived data.

QUESTION 73

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.

Correct Answer: A

Explanation

Explanation/Reference:

Amazon S3 is a highly scalable and cost-effective storage service that can be used to host static website content. It provides durability, high availability, and low latency access to the static files.

Amazon ECS with AWS Fargate eliminates the need to manage the underlying infrastructure. It allows you to run containerized applications without provisioning or managing EC2 instances. This reduces operational overhead and provides scalability.

By using a managed Amazon RDS cluster for the database, you can offload the management tasks such as backups, patching, and monitoring to AWS. This reduces the operational burden and ensures high availability and durability of the database.

QUESTION 74

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

Correct Answer: C

Explanation

Explanation/Reference:

Amazon EFS is a fully managed file system service that provides scalable, shared storage for Amazon EC2 instances. It supports the Network File System version 4 (NFSv4) protocol, which is a native protocol

for Linux-based systems. EFS is designed to be highly available, durable, and scalable.

QUESTION 75

A 4-year-old media company is using the AWS Organizations all features feature set to organize its AWS accounts. According to the 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.

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 76

An ecommerce company runs an application in the AWS Cloud that is integrated with an on-premises warehouse solution. The company uses Amazon Simple Notification Service (Amazon SNS) to send order messages to an on-premises HTTPS endpoint so the warehouse application can process the orders. The local data center team has detected that some of the order messages were not received.

A solutions architect needs to retain messages that are not delivered and analyze the messages for up to 14 days.

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

- A. Configure an Amazon SNS dead letter queue that has an Amazon Kinesis Data Stream target with a retention period of 14 days.
- B. Add an Amazon Simple Queue Service (Amazon SQS) queue with a retention period of 14 days between the application and Amazon SNS.
- C. Configure an Amazon SNS dead letter queue that has an Amazon Simple Queue Service (Amazon SQS) target with a retention period of 14 days.
- D. Configure an Amazon SNS dead letter queue that has an Amazon DynamoDB target with a TTL attribute set for a retention period of 14 days.

Correct Answer: C

Explanation

Explanation/Reference:

The message retention period in Amazon SQS can be set between 1 minute and 14 days (the default is 4 days). Therefore, you can configure your SQS DLQ to retain undelivered SNS messages for 14 days. This

will enable you to analyze undelivered messages with the least development effort.

QUESTION 77

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.

Correct Answer: B

Explanation

Explanation/Reference:

Continuous Backups: DynamoDB provides a feature called continuous backups, which automatically backs up your table data. Enabling continuous backups ensures that your table data is continuously backed up without the need for additional coding or manual interventions.

Export to Amazon S3: With continuous backups enabled, DynamoDB can directly export the backups to an Amazon S3 bucket. This eliminates the need for custom coding to export the data.

Minimal Coding: Option B requires the least amount of coding effort as continuous backups and the export to Amazon S3 functionality are built-in features of DynamoDB.

No Impact on Availability and RCUs: Enabling continuous backups and exporting data to Amazon S3 does not affect the availability of your application or the read capacity units (RCUs) defined for the table. These operations happen in the background and do not impact the table's performance or consume additional RCUs.

QUESTION 78

A solutions architect is designing an asynchronous application to process credit card data validation requests for a bank. The application must be secure and be able to process each request at least once.

Which solution will meet these requirements MOST cost-effectively?

- A. Use AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) standard queues as the event source. Use AWS Key Management Service (SSE-KMS) for encryption. Add the kms:Decrypt permission for the Lambda execution role.
- B. Use AWS Lambda event source mapping. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues as the event source. Use SQS managed encryption keys (SSE-SQS) for encryption. Add the encryption key invocation permission for the Lambda function.
- C. Use the AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) FIFO queues as the event source. Use AWS KMS keys (SSE-KMS). Add the kms:Decrypt permission for the Lambda execution role.
- D. Use the AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) standard queues as the event source. Use AWS KMS keys (SSE-KMS) for encryption. Add the encryption key invocation permission for the Lambda function.

Correct Answer: A

Explanation

Explanation/Reference:

Key word - at least once and cost effective suggests SQS standard

QUESTION 79

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.

Correct Answer: B

Explanation

Explanation/Reference:

AWS Organizations: AWS Organizations is a service that helps you centrally manage multiple AWS accounts. It enables you to group accounts into organizational units (OUs) and apply policies across those accounts.

Service Control Policies (SCPs): SCPs in AWS Organizations allow you to define fine-grained permissions and restrictions at the account or OU level. By attaching an SCP to the development accounts, you can control the creation and usage of EC2 instance types.

Least Development Effort: Option B requires minimal development effort as it leverages the built-in features of AWS Organizations and SCPs. You can define the SCP to restrict the use of oversized EC2 instance types and apply it to the appropriate OUs or accounts.

QUESTION 80

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? (Choose 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.

Correct Answer: DEF

Explanation

Explanation/Reference:

Amazon Transcribe will convert the audio recordings into text, **Amazon Translate** will translate the text into English, and **Amazon Comprehend** will perform sentiment analysis on the translated text to generate sentiment analysis reports.

QUESTION 81

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.

Correct Answer: D

Explanation

Explanation/Reference:

"aws:SourceIP" indicates the IP address that is trying to perform the action.

QUESTION 82

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.

Correct Answer: C

Explanation

Explanation/Reference:

Amazon Macie is a service that helps discover, classify, and protect sensitive data stored in AWS. It uses machine learning algorithms and managed identifiers to detect various types of sensitive information, including personally identifiable information (PII) and financial information. By configuring Amazon Macie to run a data discovery job with the appropriate managed identifiers for the required data types (such as passport numbers and credit card numbers), the company can identify and classify any sensitive data present in the S3 bucket.

QUESTION 83

A company uses on-premises servers to host its applications. The company is running out of storage capacity. The applications use both block storage and NFS storage. The company needs a high-performing solution that supports local caching without re-architecting its existing applications.

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

- A. Mount Amazon S3 as a file system to the on-premises servers.
- B. Deploy an AWS Storage Gateway file gateway to replace NFS storage.
- C. Deploy AWS Snowball Edge to provision NFS mounts to on-premises servers.
- D. Deploy an AWS Storage Gateway volume gateway to replace the block storage.
- E. Deploy Amazon Elastic File System (Amazon EFS) volumes and mount them to on-premises servers.

Correct Answer: BD

Explanation

Explanation/Reference:

By combining the deployment of an AWS Storage Gateway file gateway and an AWS Storage Gateway volume gateway, the company can address both its block storage and NFS storage needs, while leveraging local caching capabilities for improved performance.

QUESTION 84

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.

Correct Answer: C

Explanation

Explanation/Reference:

A VPC gateway endpoint allows you to privately access Amazon S3 from within your VPC without using a NAT gateway or NAT instance. By provisioning a VPC gateway endpoint for S3, the service in the private

subnet can directly communicate with S3 without incurring data transfer costs for traffic going through a NAT gateway.

QUESTION 85

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 of 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.

Correct Answer: A

Explanation

Explanation/Reference:

S3 Lifecycle policies allow you to define rules that automatically transition or expire objects based on their age or other criteria. By configuring an S3 Lifecycle policy to delete expired object versions and retain only the two most recent versions, you can effectively manage the storage costs while maintaining the desired retention policy. This solution is highly automated and requires minimal operational overhead as the lifecycle management is handled by S3 itself.

QUESTION 86

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.

Correct Answer: D

Explanation

Explanation/Reference:

For Dedicated Connections, 1 Gbps, 10 Gbps, and 100 Gbps ports are available. For Hosted Connections, connection speeds of 50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps and 10 Gbps may be ordered from approved AWS Direct Connect Partners. See AWS Direct Connect Partners for more information.

QUESTION 87

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? (Choose 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.

Correct Answer: AD

Explanation

Explanation/Reference:

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.

QUESTION 88

A company wants to ingest customer payment data into the company's data lake in Amazon S3. The company receives payment data every minute on average. The company wants to analyze the payment data in real time. Then the company wants to ingest the data into the data lake.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Use Amazon Kinesis Data Streams to ingest data. Use AWS Lambda to analyze the data in real time.
- B. Use AWS Glue to ingest data. Use Amazon Kinesis Data Analytics to analyze the data in real time.
- C. Use Amazon Kinesis Data Firehose to ingest data. Use Amazon Kinesis Data Analytics to analyze the data in real time.
- D. Use Amazon API Gateway to ingest data. Use AWS Lambda to analyze the data in real time.

Correct Answer: C

Explanation

Explanation/Reference:

By leveraging the combination of Amazon Kinesis Data Firehose and Amazon Kinesis Data Analytics, you can efficiently ingest and analyze the payment data in real time without the need for manual processing or additional infrastructure management. This solution provides a streamlined and scalable approach to handle continuous data ingestion and analysis requirements.

QUESTION 89

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? (Choose 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.

Correct Answer: CE

Explanation

Explanation/Reference:

By combining the use of Amazon EFS for shared file storage and Amazon CloudFront for content delivery, you can achieve improved performance and resilience for the website.

QUESTION 90

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 IAM 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 IAM 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 IAM role with read-only EC2 and CloudWatch permissions. Encrypt and store the Amazon Cognito user and password in a secrets management system.

Correct Answer: A

Explanation

Explanation/Reference:

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.

QUESTION 91

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.

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 92

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.

Correct Answer: C

Explanation

Explanation/Reference:

Purchasing a 1-year Savings Plan (option A) or a 1-year Reserved Instance (option B) may provide cost savings, but they are more suitable for long-running, steady-state workloads. Since your batch jobs run for a specific period each day, using Spot Instances with the ability to scale out based on CPU usage is a more cost-effective choice.

QUESTION 93

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.

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 94

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.

Correct Answer: A

Explanation

Explanation/Reference:

Using DynamoDB's global tables feature, you can achieve a globally consistent reservation database with low latency on updates, making it suitable for serving a global user base. The automatic replication provided by DynamoDB eliminates the need for manual synchronization between Regions.

QUESTION 95

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? (Choose 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.

Correct Answer: BD

Explanation

Explanation/Reference:

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.

QUESTION 96

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.

Correct Answer: B

Explanation

Explanation/Reference:

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.

QUESTION 97

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.

Correct Answer: B

Explanation

Explanation/Reference:

Option B suggests configuring a VPC peering connection between the ap-southeast-2 VPC and the eu-west-1 VPC. By establishing this peering connection, the VPCs can communicate with each other over their private IP addresses.

Additionally, updating the subnet route tables is necessary to ensure that the traffic destined for the remote VPC is correctly routed through the VPC peering connection.

To secure the communication, an inbound rule is created in the ap-southeast-2 database security group. This rule references the security group ID of the application servers in the eu-west-1 VPC, allowing traffic only from those instances.

This approach ensures that only the authorized application servers can access the databases in the ap-southeast-2 VPC.

QUESTION 98

A company is developing software that uses a PostgreSQL database schema. The company needs to configure multiple development environments and databases for the company's developers. On average, each development environment is used for half of the 8-hour workday.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure each development environment with its own Amazon Aurora PostgreSQL database
- B. Configure each development environment with its own Amazon RDS for PostgreSQL Single-AZ DB instances
- C. Configure each development environment with its own Amazon Aurora On-Demand PostgreSQL-Compatible database
- D. Configure each development environment with its own Amazon S3 bucket by using Amazon S3 Object Select

Correct Answer: C

Explanation

Explanation/Reference:

Amazon Aurora On-Demand is a pay-per-use deployment option for Amazon Aurora that allows you to create and destroy database instances as needed. This is ideal for development environments that are only used for part of the day, as you only pay for the database instance when it is in use.

The other options are not as cost-effective. Option A, configuring each development environment with its own Amazon Aurora PostgreSQL database, would require you to pay for the database instance even when it is not in use. Option B, configuring each development environment with its own Amazon RDS for PostgreSQL Single-AZ DB instance, would also require you to pay for the database instance even when it is not in use. Option D, configuring each development environment with its own Amazon S3 bucket by using Amazon S3 Object Select, is not a viable option as Amazon S3 is not a database.

QUESTION 99

A company uses AWS Organizations with resources tagged by account. The company also uses AWS Backup to back up its AWS infrastructure resources. The company needs to back up all AWS resources.

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

- A. Use AWS Config to identify all untagged resources. Tag the identified resources programmatically. Use tags in the backup plan.
- B. Use AWS Config to identify all resources that are not running. Add those resources to the backup vault.
- C. Require all AWS account owners to review their resources to identify the resources that need to be backed up.
- D. Use Amazon Inspector to identify all noncompliant resources.

Correct Answer: A

Explanation

Explanation/Reference:

This solution allows you to leverage AWS Config to identify any untagged resources within your AWS Organizations accounts. Once identified, you can programmatically apply the necessary tags to indicate the backup requirements for each resource. By using tags in the backup plan configuration, you can ensure that only the tagged resources are included in the backup process, reducing operational overhead.

and ensuring all necessary resources are backed up.

QUESTION 100

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.

Correct Answer: A

Explanation

Explanation/Reference:

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.

QUESTION 101

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 (IAM) to the AmazonEKSNodeRole IAM 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.

Correct Answer: B

Explanation

Explanation/Reference:

By creating interface VPC endpoints, you can enable the necessary communication between the Amazon EKS control plane and the nodes in private subnets. This solution ensures that the control plane maintains endpoint private access (set to true) and endpoint public access (set to false) for security compliance.

QUESTION 102

A company is migrating an on-premises application to AWS. The company wants to use Amazon Redshift as a solution.

Which use cases are suitable for Amazon Redshift in this scenario? (Choose three.)

- A. Supporting data APIs to access data with traditional, containerized, and event-driven applications
- B. Supporting client-side and server-side encryption
- C. Building analytics workloads during specified hours and when the application is not active
- D. Caching data to reduce the pressure on the backend database
- E. Scaling globally to support petabytes of data and tens of millions of requests per minute
- F. Creating a secondary replica of the cluster by using the AWS Management Console

Correct Answer: BCE

Explanation

Explanation/Reference:

B. Supporting client-side and server-side encryption: Amazon Redshift supports both client-side and server-side encryption for improved data security.

C. Building analytics workloads during specified hours and when the application is not active: Amazon Redshift is optimized for running complex analytic queries against very large datasets, making it a good choice for this use case.

E. Scaling globally to support petabytes of data and tens of millions of requests per minute: Amazon Redshift is designed to handle petabytes of data, and to deliver fast query and I/O performance for virtually any size dataset.

QUESTION 103

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.

Correct Answer: B

Explanation

Explanation/Reference:

In the context of the given scenario, where the company wants low latency and consistent performance for their API during peak usage times, it would be more suitable to use provisioned concurrency. By allocating a specific number of concurrent executions, the company can ensure that there are enough function instances available to handle the expected load and minimize the impact of cold starts. This will result in lower latency and improved performance for the API.

QUESTION 104

A company wants to send all AWS Systems Manager Session Manager logs to an Amazon S3 bucket for archival purposes.

Which solution will meet this requirement with the MOST operational efficiency?

- A. Enable S3 logging in the Systems Manager console. Choose an S3 bucket to send the session data to.
- B. Install the Amazon CloudWatch agent. Push all logs to a CloudWatch log group. Export the logs to an S3 bucket from the group for archival purposes.

- C. Create a Systems Manager document to upload all server logs to a central S3 bucket. Use Amazon EventBridge to run the Systems Manager document against all servers that are in the account daily.
- D. Install an Amazon CloudWatch agent. Push all logs to a CloudWatch log group. Create a CloudWatch logs subscription that pushes any incoming log events to an Amazon Kinesis Data Firehose delivery stream. Set Amazon S3 as the destination.

Correct Answer: A

Explanation

Explanation/Reference:

option A does not involve CloudWatch, while option D does. Therefore, in terms of operational overhead, option A would generally have less complexity and operational overhead compared to option D.

Option A simply enables S3 logging in the Systems Manager console, allowing you to directly send session logs to an S3 bucket. This approach is straightforward and requires minimal configuration.

On the other hand, option D involves installing and configuring the Amazon CloudWatch agent, creating a CloudWatch log group, setting up a CloudWatch Logs subscription, and configuring an Amazon Kinesis Data Firehose delivery stream to store logs in an S3 bucket. This requires additional setup and management compared to option A.

QUESTION 105

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

Correct Answer: A

Explanation

Explanation/Reference:

Enabling storage autoscaling allows RDS to automatically adjust the storage capacity based on the application's needs. When the storage usage exceeds a predefined threshold, RDS will automatically increase the allocated storage without requiring manual intervention or causing downtime. This ensures that the RDS database has sufficient disk space to handle the increasing storage requirements.

QUESTION 106

A consulting company provides professional services to customers worldwide. The company provides solutions and tools for customers to expedite gathering and analyzing data on AWS. The company needs to centrally manage and deploy a common set of solutions and tools for customers to use for self-service purposes.

Which solution will meet these requirements?

- A. Create AWS CloudFormation templates for the customers.
- B. Create AWS Service Catalog products for the customers.
- C. Create AWS Systems Manager templates for the customers.
- D. Create AWS Config items for the customers.

Correct Answer: B

Explanation

Explanation/Reference:

AWS Service Catalog allows you to create and manage catalogs of IT services that can be deployed within your organization. With Service Catalog, you can define a standardized set of products (solutions and tools

in this case) that customers can self-service provision. By creating Service Catalog products, you can control and enforce the deployment of approved and validated solutions and tools.

QUESTION 107

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. The 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.

Correct Answer: B

Explanation

Explanation/Reference:

AWS Service Catalog allows you to create and manage catalogs of IT services that can be deployed within your organization. With Service Catalog, you can define a standardized set of products (solutions and tools in this case) that customers can self-service provision. By creating Service Catalog products, you can control and enforce the deployment of approved and validated solutions and tools.

QUESTION 108

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 IAM user that has programmatic access. Configure the application to use the correct IAM user access key ID and secret access key to authenticate and read the DynamoDB table. Manually rotate IAM access keys every 30 days.
- C. In every business account, create an IAM 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 crossaccount 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.

Correct Answer: C

Explanation

Explanation/Reference:

IAM Roles: IAM roles provide a secure way to grant permissions to entities within AWS. By creating an IAM role in each business account named BU_ROLE with the necessary permissions to access the DynamoDB table, the access can be controlled at the IAM role level.

Cross-Account Access: By configuring a trust policy in the BU_ROLE that trusts a specific role in the inventory application account (APP_ROLE), you establish a trusted relationship between the two accounts. Least Privilege: By creating a specific IAM role (BU_ROLE) in each business account and granting it access only to the required DynamoDB table, you can ensure that each team's table is accessed with the least privilege principle. Security Token Service (STS): The use of STS AssumeRole API operation in the inventory application account allows the application to assume the cross-account role (BU_ROLE) in each business account.

QUESTION 109

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? (Choose 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.

Correct Answer: BC

Explanation

Explanation/Reference:

By combining the Kubernetes Cluster Autoscaler (option C) to manage the number of nodes in the cluster and enabling horizontal pod autoscaling (option B) with the Kubernetes Metrics Server, you can achieve automatic scaling of your EKS cluster and container applications based on workload demand. This approach minimizes operational overhead as it leverages built-in Kubernetes functionality and automation mechanisms.

QUESTION 110

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. AWS AppSync 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

Correct Answer: B

Explanation

Explanation/Reference:

Cloud front was build specifically to resolve performance issues.

Exam E

QUESTION 1

A company collects data for temperature, humidity, and atmospheric pressure in cities across multiple continents. The average volume of data that the company collects from each site daily is 500 GB. Each site has a high-speed Internet connection.

The company wants to aggregate the data from all these global sites as quickly as possible in a single Amazon S3 bucket. The solution must minimize operational complexity.

Which solution meets these requirements?

- A. Turn on S3 Transfer Acceleration on the destination S3 bucket. Use multipart uploads to directly upload site data to the destination S3 bucket.
- B. Upload the data from each site to an S3 bucket in the closest Region. Use S3 Cross-Region Replication to copy objects to the destination S3 bucket. Then remove the data from the origin S3 bucket.
- C. Schedule AWS Snowball Edge Storage Optimized device jobs daily to transfer data from each site to the closest Region. Use S3 Cross-Region Replication to copy objects to the destination S3 bucket.
- D. Upload the data from each site to an Amazon EC2 instance in the closest Region. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. At regular intervals, take an EBS snapshot and copy it to the Region that contains the destination S3 bucket. Restore the EBS volume in that Region.

Correct Answer: A

Explanation

Explanation/Reference:

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

QUESTION 2

A solutions architect is developing a VPC architecture that includes multiple subnets. The architecture will host applications that use Amazon EC2 instances and Amazon RDS DB instances. The architecture consists of six subnets in two Availability Zones. Each Availability Zone includes a public subnet, a private subnet, and a dedicated subnet for databases. Only EC2 instances that run in the private subnets can have access to the RDS databases.

Which solution will meet these requirements?

- A. Create a new route table that excludes the route to the public subnets' CIDR blocks. Associate the route table with the database subnets.
- B. Create a security group that denies inbound traffic from the security group that is assigned to instances in the public subnets. Attach the security group to the DB instances.
- C. Create a security group that allows inbound traffic from the security group that is assigned to instances in the private subnets. Attach the security group to the DB instances.
- D. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.

Correct Answer: C

Explanation

Explanation/Reference:

The solution that meets the requirements described in the question is option C: Create a security group that allows inbound traffic from the security group that is assigned to instances in the private subnets. Attach the security group to the DB instances.

In this solution, the security group applied to the DB instances allows inbound traffic from the security group assigned to instances in the private subnets. This ensures that only EC2 instances running in the private subnets can have access to the RDS databases.

QUESTION 3

A company is implementing a shared storage solution for a gaming application that is hosted in an on-premises data center. The company needs the ability to use Lustre clients to access data. The solution must be fully managed.

Which solution meets these requirements?

- A. Create an AWS Storage Gateway file gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
- 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 Elastic File System (Amazon EFS) file system, and configure it to support Lustre. Attach the file system to the origin server. Connect the application server to the file system.
- D. Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.

Correct Answer: D

Explanation

Explanation/Reference:

Lustre in the question is only available as FSx

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

QUESTION 4

A company wants to migrate an on-premises data center to AWS. The data center 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.

Which combination of steps should a solutions architect take to automate this task? (Choose two.)

- A. Launch the EC2 instance into the same Availability Zone as the EFS file system.
- B. Install an AWS DataSync agent in the on-premises data center.
- C. Create a secondary Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instance for 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 on-premises SFTP server.

Correct Answer: BE

Explanation

Explanation/Reference:

B-Install an AWS DataSync agent in the on-premises data center.

E-Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server.

To automate the process of transferring the data from the on-premises SFTP server to an EC2 instance with an EFS file system, you can use AWS DataSync. AWS DataSync is a fully managed data transfer service that simplifies, automates, and accelerates transferring data between on-premises storage systems and Amazon S3, Amazon EFS, or Amazon FSx for Windows File Server. To use AWS DataSync for this task, you should first install an AWS DataSync agent in the on-premises data center. This agent is a lightweight software application that you install on your on-premises data source. The agent communicates with the AWS DataSync service to transfer data between the data source and target locations.

QUESTION 5

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.

Correct Answer: D

Explanation

Explanation/Reference:

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.

QUESTION 6

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.

Correct Answer: A

Explanation

Explanation/Reference:

Cross-Region backup

Using AWS Backup, you can copy backups to multiple different AWS Regions on demand or automatically as part of a scheduled backup plan. Cross-Region backup is particularly valuable if you have business continuity or compliance requirements to store backups a minimum distance away from your production data.

<https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html>

QUESTION 7

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? (Choose 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.

Correct Answer: BD

Explanation

Explanation/Reference:

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>

QUESTION 8

A company needs to run a critical application on AWS. The company needs to use Amazon EC2 for the application's database. The database must be highly available and must fail over automatically if a disruptive event occurs.

Which solution will meet these requirements?

- A. Launch two EC2 instances, each in a different Availability Zone in the same AWS Region. Install the database on both EC2 instances. Configure the EC2 instances as a cluster. Set up database replication.
- B. Launch an EC2 instance in an Availability Zone. Install the database on the EC2 instance. Use an Amazon Machine Image (AMI) to back up the data. Use AWS CloudFormation to automate provisioning of the EC2 instance if a disruptive event occurs.
- C. Launch two EC2 instances, each in a different AWS Region. Install the database on both EC2 instances. Set up database replication. Fail over the database to a second Region.
- D. Launch an EC2 instance in an Availability Zone. Install the database on the EC2 instance. Use an Amazon Machine Image (AMI) to back up the data. Use EC2 automatic recovery to recover the instance if a disruptive event occurs.

Correct Answer: A

Explanation

Explanation/Reference:

ECS Spread placement strategy

ECS groups available capacity used to place Tasks into ECS Clusters with ECS Tasks being launched into an ECS Cluster. An ECS Clusters configured to use EC2 will have EC2 Instances registered with it and each EC2 instance resides in a single Availability Zone. You should be ensuring that you have EC2 instances registered with your Cluster from multiple Availability Zones. <https://aws.amazon.com/blogs/containers/amazon-ecs-availability-best-practices/#:~:text=An%20ECS%20Clusters%20configured%20to,Cluster%20from%20multiple%20Availability%20Zones>

QUESTION 9

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.

Correct Answer: D

Explanation

Explanation/Reference:

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.

QUESTION 10

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.

Correct Answer: B

Explanation

Explanation/Reference:

By creating Amazon Machine Images (AMIs) to back up the EC2 instances and copying them to a secondary AWS Region, the company can ensure that they have a reliable backup in the event of a disaster. By using AWS CloudFormation to automate infrastructure deployment in the secondary Region, the company can minimize the amount of time and effort required to set up the DR solution. https://docs.aws.amazon.com/zh_cn/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html#backup-and-restore

QUESTION 11

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.

Correct Answer: B

Explanation

Explanation/Reference:

configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB. This ensures that only the traffic originating from the ALB is allowed access to the EC2 instances in the private subnet, while denying any other traffic from other sources. The other options do not provide a suitable solution to meet the stated requirements.

QUESTION 12

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.

Correct Answer: D

Explanation

Explanation/Reference:

Amazon FSx for NetApp ONTAP is a fully-managed shared storage service built on NetApp's popular ONTAP file system. Amazon FSx for NetApp ONTAP provides the popular features, performance, and APIs of ONTAP file systems with the agility, scalability, and simplicity of a fully managed AWS service, making it easier for customers to migrate on-premises applications that rely on NAS appliances to AWS. FSx for ONTAP file systems are similar to on-premises NetApp clusters. Within each file system that you create, you also create one or more storage virtual machines (SVMs). These are isolated file servers each with their own endpoints for NFS, SMB, and management access, as well as authentication (for both administration and end-user data access). In turn, each SVM has one or more volumes which store your data.

<https://aws.amazon.com/de/blogs/storage/getting-started-cloud-file-storage-with-amazon-fsx-for-netapp-ontap-using-netapp-management-tools/>

QUESTION 13

A company hosts its static website by using Amazon S3. The company wants to add a contact form to its webpage. The contact form will have dynamic server-side 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 endpoint 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 Lightsail. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail.
- D. 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.

Correct Answer: B

Explanation

Explanation/Reference:

This solution is the most cost-efficient for the anticipated 100 monthly visits because:

API Gateway charges are based on API calls. With only 100 visits, charges would be minimal.

AWS Lambda provides compute time for the backend code in increments of 100ms, so charges would also be negligible for this workload. Amazon SES is used only for sending emails from the submitted contact forms. SES has a generous free tier of 62,000 emails per month, so there would be no charges for sending the contact emails.

No EC2 instances or other infrastructure needs to be run and paid for.

<https://aws.amazon.com/blogs/architecture/create-dynamic-contact-forms-for-s3-static-websites-using-aws-lambda-amazon-api-gateway-and-amazon-ses/>

QUESTION 14

A company has a static website that is hosted on Amazon CloudFront in front of Amazon S3. The static website uses a database backend. The company notices that the website does not reflect updates that have been made in the website's Git repository. The company checks the continuous integration and continuous delivery (CI/CD) pipeline between the Git repository and Amazon S3. The company verifies that the webhooks are configured properly and that the CI/CD pipeline is sending messages that indicate successful deployments.

A solutions architect needs to implement a solution that displays the updates on the website.

Which solution will meet these requirements?

- A. Add an Application Load Balancer.
- B. Add Amazon ElastiCache for Redis or Memcached to the database layer of the web application.
- C. Invalidate the CloudFront cache.
- D. Use AWS Certificate Manager (ACM) to validate the website's SSL certificate.

Correct Answer: C

Explanation

Explanation/Reference:

Problem is the CF cache. After invalidating the CloudFront cache, CF will be forced to read the updated static page from the S3 and the S3 changes will start being visible.

QUESTION 15

A media company uses Amazon CloudFront for its publicly available streaming video content. The company wants to secure the video content that is hosted in Amazon S3 by controlling who has access. Some of the company's users are using a custom HTTP client that does not support cookies. Some of the company's users are unable to change the hardcoded URLs that they are using for access.

Which services or methods will meet these requirements with the LEAST impact to the users? (Choose two.)

- A. Signed cookies
- B. Signed URLs
- C. AWS AppSync
- D. JSON Web Token (JWT)
- E. AWS Secrets Manager

Correct Answer: AB

Explanation

Explanation/Reference:

Signed cookies would allow the media company to authorize access to related content (like HLS video

segments) with a single signature, minimizing implementation overhead. This works for users that can support cookies. Signed URLs would allow the media company to sign each URL individually to control access, supporting users that cannot use cookies. By embedding the signature in the URL, existing hardcoded URLs would not need to change.

QUESTION 16

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.

Correct Answer: AB

Explanation

Explanation/Reference:

DMS can move data from DBs to streaming services and cannot natively handle streaming data. Hence A.B makes sense. Also AWS Glue/ETL can handle MSK streaming <https://docs.aws.amazon.com/glue/latest/dg/add-job-streaming.html>.

QUESTION 17

A university research laboratory needs to migrate 30 TB of data from an on-premises Windows file server to Amazon FSx for Windows File Server. The laboratory has a 1 Gbps network link that many other departments in the university share.

The laboratory wants to implement a data migration service that will maximize the performance of the data transfer. However, the laboratory needs to be able to control the amount of bandwidth that the service uses to minimize the impact on other departments. The data migration must take place within the next 5 days.

Which AWS solution will meet these requirements?

- A. AWS Snowcone
- B. Amazon FSx File Gateway
- C. AWS DataSync
- D. AWS Transfer Family

Correct Answer: C

Explanation

Explanation/Reference:

AWS DataSync is a data transfer service that can copy large amounts of data between on-premises storage and Amazon FSx for Windows File Server at high speeds. It allows you to control the amount of bandwidth used during data transfer. DataSync uses agents at the source and destination to automatically copy files and file metadata over the network. This optimizes the data transfer and minimizes the impact on

your network bandwidth. DataSync allows you to schedule data transfers and configure transfer rates to suit your needs. You can transfer 30 TB within 5 days while controlling bandwidth usage. DataSync can resume interrupted transfers and validate data to ensure integrity. It provides detailed monitoring and reporting on the progress and performance of data transfers.

QUESTION 18

A company uses an Amazon EC2 instance to run a script to poll for and process messages in an Amazon Simple Queue Service (Amazon SQS) queue. The company wants to reduce operational costs while maintaining its ability to process a growing number of messages that are added to the queue.

What should a solutions architect recommend to meet these requirements?

- A. Increase the size of the EC2 instance to process messages faster.
- B. Use Amazon EventBridge to turn off the EC2 instance when the instance is underutilized.
- C. Migrate the script on the EC2 instance to an AWS Lambda function with the appropriate runtime.
- D. Use AWS Systems Manager Run Command to run the script on demand.

Correct Answer: C

Explanation

Explanation/Reference:

AWS Lambda is a serverless compute service that allows you to run your code without provisioning or managing servers. By migrating the script to an AWS Lambda function, you can eliminate the need to maintain an EC2 instance, reducing operational costs. Additionally, Lambda automatically scales to handle the increasing number of messages in the SQS queue.

QUESTION 19

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.

Correct Answer: D

Explanation

Explanation/Reference:

Amazon Inspector is a security assessment service that helps improve the security and compliance of applications deployed on Amazon Web Services (AWS). It automatically assesses applications for vulnerabilities or deviations from best practices. Amazon Inspector can be used to identify security issues and recommend fixes for them. It is an ideal solution for running regular security scans across a large fleet of EC2 instances.

AWS Systems Manager Patch Manager is a service that helps you automate the process of patching Windows and Linux instances. It provides a simple, automated way to patch your instances with the latest security patches and updates. Patch Manager helps you maintain compliance with security policies and regulations by providing detailed reports on the patch status of your instances.

QUESTION 20

A company wants to give a customer the ability to use on-premises Microsoft Active Directory to download files that are stored in Amazon S3. The customer's application uses an SFTP client to download the files.

Which solution will meet these requirements with the LEAST operational overhead and no changes to the customer's application?

- A. Set up AWS Transfer Family with SFTP for Amazon S3. Configure integrated Active Directory authentication.
- B. Set up AWS Database Migration Service (AWS DMS) to synchronize the on-premises client with Amazon S3. Configure integrated Active Directory authentication.
- C. Set up AWS DataSync to synchronize between the on-premises location and the S3 location by using AWS IAM Identity Center (AWS Single Sign-On).
- D. Set up a Windows Amazon EC2 instance with SFTP to connect the on-premises client with Amazon S3. Integrate AWS Identity and Access Management (IAM).

Correct Answer: A

Explanation

Explanation/Reference:

using AWS Batch to LEAST operational overhead

and have SFTP to no changes to the customer's application

<https://aws.amazon.com/vi/blogs/architecture/managed-file-transfer-using-aws-transfer-family-and-amazon-s3/>

QUESTION 21

A company has a Java application that uses Amazon Simple Queue Service (Amazon SQS) to parse messages. The application cannot parse messages that are larger than 256 KB in size. The company wants to implement a solution to give the application the ability to parse messages as large as 50 MB.

Which solution will meet these requirements with the FEWEST changes to the code?

- A. Use the Amazon SQS Extended Client Library for Java to host messages that are larger than 256 KB in Amazon S3.
- B. Use Amazon EventBridge to post large messages from the application instead of Amazon SQS.
- C. Change the limit in Amazon SQS to handle messages that are larger than 256 KB.
- D. Store messages that are larger than 256 KB in Amazon Elastic File System (Amazon EFS). Configure Amazon SQS to reference this location in the messages.

Correct Answer: A

Explanation

Explanation/Reference:

Amazon SQS has a limit of 256 KB for the size of messages. To handle messages larger than 256 KB, the Amazon SQS Extended Client Library for Java can be used. This library allows messages larger than 256 KB to be stored in Amazon S3 and provides a way to retrieve and process them. Using this solution, the application code can remain largely unchanged while still being able to process messages up to 50 MB in size.

QUESTION 22

A company wants to restrict access to the content of one of its main web applications and to protect the content by using authorization techniques available on AWS. The company wants to implement a serverless architecture and an authentication solution for fewer than 100 users. The solution needs to integrate with the main web application and serve web content globally. The solution must also scale as the company's user base grows while providing the lowest login latency possible.

Which solution will meet these requirements MOST cost-effectively?

- A. Use Amazon Cognito for authentication. Use Lambda@Edge for authorization. Use Amazon CloudFront to serve the web application globally.
- B. Use AWS Directory Service for Microsoft Active Directory for authentication. Use AWS Lambda for authorization. Use an Application Load Balancer to serve the web application globally.

- C. Use Amazon Cognito for authentication. Use AWS Lambda for authorization. Use Amazon S3 Transfer Acceleration to 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 globally.

Correct Answer: A

Explanation

Explanation/Reference:

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.

QUESTION 23

A company has an aging network-attached storage (NAS) array in its data center. The NAS array presents SMB shares and NFS shares to client workstations. The company does not want to purchase a new NAS array. The company also does not want to incur the cost of renewing the NAS array's support contract. Some of the data is accessed frequently, but much of the data is inactive.

A solutions architect needs to implement a solution that migrates the data to Amazon S3, uses S3 Lifecycle policies, and maintains the same look and feel for the client workstations. The solutions architect has identified AWS Storage Gateway as part of the solution.

Which type of storage gateway should the solutions architect provision to meet these requirements?

- A. Volume Gateway
- B. Tape Gateway
- C. Amazon FSx File Gateway
- D. Amazon S3 File Gateway

Correct Answer: D

Explanation

Explanation/Reference:

Amazon S3 File Gateway provides a file interface to objects stored in S3. It can be used for a file-based interface with S3, which allows the company to migrate their NAS array data to S3 while maintaining the same look and feel for client workstations. Amazon S3 File Gateway supports SMB and NFS protocols, which will allow clients to continue to access the data using these protocols. Additionally, Amazon S3 Lifecycle policies can be used to automate the movement of data to lower-cost storage tiers, reducing the storage cost of inactive data.

QUESTION 24

A company has an application that is running on Amazon EC2 instances. A solutions architect has standardized the company on a particular instance family and various instance sizes based on the current needs of the company.

The company wants to maximize cost savings for the application over the next 3 years. The company needs to be able to change the instance family and sizes in the next 6 months based on application popularity and usage.

Which solution will meet these requirements MOST cost-effectively?

- A. Compute Savings Plan
- B. EC2 Instance Savings Plan
- C. Zonal Reserved Instances
- D. Standard Reserved Instances

Correct Answer: A
Explanation

Explanation/Reference:

Savings Plans offer a flexible pricing model that provides savings on AWS usage. You can save up to 72 percent on your AWS compute workloads. Compute Savings Plans provide lower prices on Amazon EC2 instance usage regardless of instance family, size, OS, tenancy, or AWS Region. This also applies to AWS Fargate and AWS Lambda usage. SageMaker Savings Plans provide you with lower prices for your Amazon SageMaker instance usage, regardless of your instance family, size, component, or AWS Region. <https://docs.aws.amazon.com/savingsplans/latest/userguide/what-is-savings-plans.html>

QUESTION 25

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?

- 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.

Correct Answer: B
Explanation

Explanation/Reference:

an interface endpoint is a horizontally scaled, redundant VPC endpoint that provides private connectivity to a service. It is an elastic network interface with a private IP address that serves as an entry point for traffic destined to the AWS service. Interface endpoints are used to connect VPCs with AWS services

QUESTION 26

A company is building a game system that needs to send unique events to separate leaderboard, matchmaking, and authentication services concurrently. The company needs an AWS event-driven system that guarantees the order of the events.

Which solution will meet these requirements?

- A. Amazon EventBridge event bus
- B. Amazon Simple Notification Service (Amazon SNS) FIFO topics
- C. Amazon Simple Notification Service (Amazon SNS) standard topics
- D. Amazon Simple Queue Service (Amazon SQS) FIFO queues

Correct Answer: B
Explanation

Explanation/Reference:

Amazon SNS is a highly available and durable publish-subscribe messaging service that allows applications to send messages to multiple subscribers through a topic. SNS FIFO topics are designed to ensure that messages are delivered in the order in which they are sent. This makes them ideal for situations where message order is important, such as in the case of the company's game system.

QUESTION 27

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 frequently.

The reporting process takes a few hours with the use of relational queries. The reporting process must not prevent any document modifications or the addition of new documents. A solutions architect needs to implement a solution to speed up the reporting process.

Which solution will meet these requirements with the LEAST amount of change to the application code?

- 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 Aurora PostgreSQL DB cluster that includes an Aurora Replica. Issue queries to the Aurora Replica to generate the reports.
- C. Set up a new Amazon RDS for PostgreSQL Multi-AZ DB instance. Configure the reporting module to query the secondary RDS node so that the reporting module does not affect the primary node.
- D. 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.

Correct Answer: B

Explanation

Explanation/Reference:

Aurora is a relational database, it supports PostgreSQL and with the help of read replicas we can issue the reporting process that take several hours to the replica, therefore not affecting the primary node which can handle new writes or document modifications.

QUESTION 28

A company is implementing a shared storage solution for a gaming application that is hosted in the AWS Cloud. The company needs the ability to use Lustre clients to access data. The solution must be fully managed.

Which 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 AWS Storage Gateway file gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
- C. Create an Amazon Elastic File System (Amazon EFS) file system, and configure it to support Lustre. Attach the file system to the origin server. Connect the application server to the file system.
- D. Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.

Correct Answer: D

Explanation

Explanation/Reference:

To meet the requirements of a shared storage solution for a gaming application that can be accessed using Lustre clients and is fully managed, the best solution would be to use Amazon FSx for Lustre. Amazon FSx for Lustre is a fully managed file system that is optimized for compute-intensive workloads, such as high-performance computing, machine learning, and gaming. It provides a POSIX-compliant file system that can be accessed using Lustre clients and offers high performance, scalability, and data durability.

This solution provides a highly available, scalable, and fully managed shared storage solution that can be accessed using Lustre clients. Amazon FSx for Lustre is optimized for compute-intensive workloads and provides high performance and durability.

QUESTION 29

A company wants to analyze and troubleshoot Access Denied errors and Unauthorized errors that are related to IAM 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.

Correct Answer: C

Explanation

QUESTION 30

A company wants to add its existing AWS usage cost to its operation cost dashboard. A solutions architect needs to recommend a solution that will give the company access to its usage cost programmatically. The company must be able to access cost data for the current year and forecast costs for the next 12 months.

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

- A. Access usage cost-related data by using the AWS Cost Explorer API with pagination.
- B. Access usage cost-related data by using downloadable AWS Cost Explorer report .csv files.
- C. Configure AWS Budgets actions to send usage cost data to the company through FTP.
- D. Create AWS Budgets reports for usage cost data. Send the data to the company through SMTP.

Correct Answer: A

Explanation

Explanation/Reference:

From AWS Documentation*:

"You can view your costs and usage using the Cost Explorer user interface free of charge. You can also access your data programmatically using the Cost Explorer API. Each paginated API request incurs a charge of \$0.01. You can't disable Cost Explorer after you enable it."

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

<https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-cost-explorer/interfaces/costexplorerpaginationconfiguration.html>

QUESTION 31

A solutions architect is reviewing the resilience of an application. The solutions architect notices that a database administrator recently failed over the application's Amazon Aurora PostgreSQL database writer instance as part of a scaling exercise. The failover resulted in 3 minutes of downtime for the application.

Which solution will reduce the downtime for scaling exercises with the LEAST operational overhead?

- A. Create more Aurora PostgreSQL read replicas in the cluster to handle the load during failover.
- B. Set up a secondary Aurora PostgreSQL cluster in the same AWS Region. During failover, update the application to use the secondary cluster's writer endpoint.
- C. Create an Amazon ElastiCache for Memcached cluster to handle the load during failover.
- D. Set up an Amazon RDS proxy for the database. Update the application to use the proxy endpoint.

Correct Answer: D

Explanation

QUESTION 32

A company is migrating its workloads to AWS. The company has transactional and sensitive data in its databases. The company wants to use AWS Cloud solutions to increase security and reduce operational overhead for the databases.

Which solution will meet these requirements?

- A. Migrate the databases to Amazon EC2. Use an AWS Key Management Service (AWS KMS) AWS managed key for encryption.
- B. Migrate the databases to Amazon RDS Configure encryption at rest.
- C. Migrate the data to Amazon S3 Use Amazon Macie for data security and protection

D. Migrate the database to Amazon RDS. Use Amazon CloudWatch Logs for data security and protection.

Correct Answer: B

Explanation

QUESTION 33

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.

Correct Answer: C

Explanation

Explanation/Reference:

UDP and TCP is AWS Global accelerator as it works in the Transportation layer.
Now this with NLB is perfect.

QUESTION 34

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? (Choose 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).

Correct Answer: ADF

Explanation

Explanation/Reference:

Step A involves registering the required domain in a registrar and creating a wildcard custom domain name in a Route 53 hosted zone. This allows you to map individual and secure URLs for all customers to your API Gateway endpoints. Step D is to request a wildcard certificate from AWS Certificate Manager (ACM) that matches the custom domain name you created in Step A. This wildcard certificate will cover all subdomains and ensure secure HTTPS communication. Step F is to create a custom domain name in API Gateway for your REST API. This allows you to associate the custom domain name with your API Gateway endpoints and import the certificate from ACM for secure communication.

QUESTION 35

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:S3Object/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.

Correct Answer: A

Explanation

Explanation/Reference:

SNS is more suitable for this option as a pub/sub service, we subscribe the security team and then they will receive the notifications.

QUESTION 36

A company wants to build a logging solution for its multiple AWS accounts. The company currently stores the logs from all accounts in a centralized account. The company has created an Amazon S3 bucket in the centralized account to store the VPC flow logs and AWS CloudTrail logs. All logs must be highly available for 30 days for frequent analysis, retained for an additional 60 days for backup purposes, and deleted 90 days after creation.

Which solution will meet these requirements MOST cost-effectively?

- A. Transition objects to the S3 Standard storage class 30 days after creation. Write an expiration action that directs Amazon S3 to delete objects after 90 days.
- B. Transition objects to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class 30 days after creation. Move all objects to the S3 Glacier Flexible Retrieval storage class after 90 days. Write an expiration action that directs Amazon S3 to delete objects after 90 days.
- C. Transition objects to the S3 Glacier Flexible Retrieval storage class 30 days after creation. Write an expiration action that directs Amazon S3 to delete objects after 90 days.
- D. Transition objects to the S3 One Zone-Infrequent Access (S3 One Zone-IA) storage class 30 days after creation. Move all objects to the S3 Glacier Flexible Retrieval storage class after 90 days. Write an expiration action that directs Amazon S3 to delete objects after 90 days.

Correct Answer: C

Explanation

Explanation/Reference:

After 30 days is backup only, doesn't specify frequent access.

Therefore we must transition the items after 30 days to Glacier Flexible Retrieval.

Also it says deletion after 90 days, so all answers specifying a transition after 90 days makes no sense.

QUESTION 37

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 alias/aws/ebs alias. Enable default Amazon Elastic Block Store (Amazon EBS) volume encryption for the account.

Correct Answer: B

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/eks/latest/userguide/enable-kms.html>

QUESTION 38

A company wants to provide data scientists with near real-time read-only access to the company's production Amazon RDS for PostgreSQL database. The database is currently configured as a Single-AZ database. The data scientists use complex queries that will not affect the production database. The company needs a solution that is highly available.

Which solution will meet these requirements MOST cost-effectively?

- A. Scale the existing production database in a maintenance window to provide enough power for the data scientists.
- B. Change the setup from a Single-AZ to a Multi-AZ instance deployment with a larger secondary standby instance. Provide the data scientists access to the secondary instance.
- C. Change the setup from a Single-AZ to a Multi-AZ instance deployment. Provide two additional read replicas for the data scientists.
- D. Change the setup from a Single-AZ to a Multi-AZ cluster deployment with two readable standby instances. Provide read endpoints to the data scientists.

Correct Answer: D

Explanation

Explanation/Reference:

Amazon RDS now offers Multi-AZ deployments with readable standby instances (also called Multi-AZ DB cluster deployments) in preview. You should consider using Multi-AZ DB cluster deployments with two readable DB instances if you need additional read capacity in your Amazon RDS Multi-AZ deployment and if your application workload has strict transaction latency requirements such as single-digit milliseconds transactions.

<https://aws.amazon.com/blogs/database/readable-standby-instances-in-amazon-rds-multi-az-deployments-a-new-high-availability-option/>

QUESTION 39

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.

Correct Answer: A

Explanation

Explanation/Reference:

Memcached is best suited for caching data, while Redis is better for storing data that needs to be persisted. If you need to store data that needs to be accessed frequently, such as user profiles, session data, and application settings, then Redis is the better choice

QUESTION 40

A global video streaming company uses Amazon CloudFront as a content distribution network (CDN). The company wants to roll out content in a phased manner across multiple countries. The company needs to ensure that viewers who are outside the countries to which the company rolls out content are not able to view the content.

Which solution will meet these requirements?

- A. Add geographic restrictions to the content in CloudFront by using an allow list. Set up a custom error message.
- B. Set up a new URL for restricted content. Authorize access by using a signed URL and cookies. Set up a custom error message.
- C. Encrypt the data for the content that the company distributes. Set up a custom error message.
- D. Create a new URL for restricted content. Set up a time-restricted access policy for signed URLs.

Correct Answer: A

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html>

QUESTION 41

A company wants to use the AWS Cloud to improve its on-premises disaster recovery (DR) configuration. The company's core production business application uses Microsoft SQL Server Standard, which runs on a virtual machine (VM). The application has a recovery point objective (RPO) of 30 seconds or fewer and a recovery time objective (RTO) of 60 minutes. The DR solution needs to minimize costs wherever possible. Which solution will meet these requirements?

- A. Configure a multi-site active/active setup between the on-premises server and AWS by using Microsoft SQL Server Enterprise with Always On availability groups.
- B. Configure a warm standby Amazon RDS for SQL Server database on AWS. Configure AWS Database Migration Service (AWS DMS) to use change data capture (CDC).
- C. Use AWS Elastic Disaster Recovery configured to replicate disk changes to AWS as a pilot light.
- D. Use third-party backup software to capture backups every night. Store a secondary set of backups in Amazon S3.

Correct Answer: C

Explanation

Explanation/Reference:

QUESTION 42

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.

Correct Answer: C

Explanation

QUESTION 43

A company wants to 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? (Choose 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 Cognito 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.

Correct Answer: ACF

Explanation

Explanation/Reference:

Check the difference between user pools and identity pools.

A = Lambda, we pay for our use only, if it is idle it won't cost, ECS will always cost.

C = Identity pool for users to sign in.

F = It uses S3 to host website which is better cost related and with CloudFront to serve content.

QUESTION 44

A media company uses an Amazon CloudFront distribution to deliver content over the internet. The company wants only premium customers to have access to the media streams and file content. The company stores all content in an Amazon S3 bucket. The company also delivers content on demand to customers for a specific purpose, such as movie rentals or music downloads.

Which solution will meet these requirements?

- A. Generate and provide S3 signed cookies to premium customers.
- B. Generate and provide CloudFront signed URLs to premium customers.
- C. Use origin access control (OAC) to limit the access of non-premium customers.
- D. Generate and activate field-level encryption to block non-premium customers.

Correct Answer: B
Explanation

Explanation/Reference:

Signed URLs

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>

QUESTION 45

A company runs Amazon EC2 instances in multiple AWS accounts that are individually billed. The company recently purchased a Savings Plan. Because of changes in the company's business requirements, the company has decommissioned a large number of EC2 instances. The company wants to use its Savings Plan discounts on its other AWS accounts.

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

- A. From the AWS Account Management Console of the management account, turn on discount sharing from the billing preferences section.
- B. From the AWS Account Management Console of the account that purchased the existing Savings Plan, turn on discount sharing from the billing preferences section. Include all accounts.
- C. From the AWS Organizations management account, use AWS Resource Access Manager (AWS RAM) to share the Savings Plan with other accounts.
- D. Create an organization in AWS Organizations in a new payer account. Invite the other AWS accounts to join the organization from the management account.
- E. Create an organization in AWS Organizations in the existing AWS account with the existing EC2 instances and Savings Plan. Invite the other AWS accounts to join the organization from the management account.

Correct Answer: AE
Explanation

QUESTION 46

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.

Correct Answer: A
Explanation

Explanation/Reference:

keyword: "latest versions on an api"

Canary release is a software development strategy in which a "new version of an API" (as well as other software) is deployed for testing purposes.

QUESTION 47

A company deploys an application on five Amazon EC2 instances. An Application Load Balancer (ALB) distributes traffic to the instances by using a target group. The average CPU usage on each of the instances 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 existing 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%. Add the EC2 instances to the Auto Scaling group.
- C. Create an EC2 Auto Scaling. Select the existing 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 state when the average CPUUtilization metric is below 20%. Configure the second CloudWatch alarm to enter the ALARM state when the average CPUUtilization metric is above 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.

Correct Answer: B

Explanation

Explanation/Reference:

1. 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.
2. 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.
3. 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.
4. A minimum of 2 and maximum of 6 instances provides the ability to scale between 3 and 6 instances as needed based on demand.
5. 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.

QUESTION 48

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.

Correct Answer: C

Explanation

Explanation/Reference:

This solution satisfies the needs in the following ways:

1. EFS provides a fully managed elastic network file system that can be mounted on multiple EC2 instances concurrently.
2. The EFS file system appears as a standard file system mount on the Linux web servers, requiring no application changes. The servers can access shared files as if they were on local storage.
3. EFS is highly available, durable, and scalable, providing a robust shared storage solution.

QUESTION 49

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

Which Amazon EC2 pricing option is the MOST cost-effective?

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

Correct Answer: A

Explanation

Explanation/Reference:

Dedicated Host Reservations provide a billing discount compared to running On-Demand Dedicated Hosts. Reservations are available in three payment options.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-hosts-overview.html>

QUESTION 50

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.

Correct Answer: D

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html>

QUESTION 51

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.

Correct Answer: B

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html>

QUESTION 52

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 Standard-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 for the S3 Docket
- D. Use Amazon CloudFront to handle all the requests to the S3 bucket

Correct Answer: D

Explanation

QUESTION 53

A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods for IAM user passwords

What should the solutions architect do to accomplish this?

- A. Set an overall password policy for the entire AWS account
- B. Set a password policy for each IAM user in the AWS account
- C. Use third-party vendor software to set password requirements
- D. Attach an Amazon CloudWatch rule to the Create_newuser event to set the password with the appropriate requirements

Correct Answer: A

Explanation

Explanation/Reference:

To accomplish this, the solutions architect should set an overall password policy for the entire AWS account. This policy will apply to all IAM users in the account, including new users.

QUESTION 54

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.

Correct Answer: B

Explanation

Explanation/Reference:

<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.

QUESTION 55

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.

Correct Answer: BC

Explanation

Explanation/Reference:

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:

1. Amazon CloudFront distribution
2. Amazon API Gateway REST API
3. Application Load Balancer
4. AWS AppSync GraphQL API
5. Amazon Cognito user pool

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

QUESTION 56

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 DB 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 0/0 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

Correct Answer: CD

Explanation

Explanation/Reference:

To meet the requirements of allowing access to the web servers in the public subnet on port 443 and the Amazon RDS for MySQL DB instance in the database subnet on port 3306, the best solution would be to create a security group for the web servers and another security group for the DB instance, and then define the appropriate inbound and outbound rules for each security group.

1. Create a security group for the web servers in the public subnet. Add a rule to allow traffic from 0.0.0.0/0 on port 443.
2. Create a security group for the DB instance. Add a rule to allow traffic from the web servers' security group on port 3306.

This will allow the web servers in the public subnet to receive traffic from the internet on port 443, and the Amazon RDS for MySQL DB instance in the database subnet to receive traffic only from the web servers on port 3306.

QUESTION 57

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 periodic basis.

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)

Correct Answer: A

Explanation

Explanation/Reference:

AWS DataSync is a fully managed data transfer service that simplifies moving large amounts of data between on-premises storage systems and AWS services. It can also transfer data between different AWS services, including different AWS Regions. DataSync provides a simple, scalable, and automated solution to transfer data, and it minimizes the operational overhead because it is fully managed by AWS.

QUESTION 58

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.

Correct Answer: D

Explanation

Explanation/Reference:

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

QUESTION 59

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 meet 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 Buckets Configure email notifications In Trusted Advisor when a change is detected manually change the S3 bucket policy if it allows public access
- C. Use AWS Resource Access Manager to find publicly accessible S3 buckets Use Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function when a change is detected. Deploy a Lambda function that programmatically remediates the change.
- D. Use the S3 Block Public Access feature on the account level. Use AWS Organizations to create a service control policy (SCP) that prevents IAM users from changing the setting Apply the SCP to the account

Correct Answer: D

Explanation

Explanation/Reference:

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.

QUESTION 60

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 solution 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 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.

Correct Answer: BE

Explanation

QUESTION 61

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.

Correct Answer: C

Explanation

QUESTION 62

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.

Correct Answer: C

Explanation

Explanation/Reference:

<https://aws.amazon.com/blogs/big-data/manage-fine-grained-access-control-using-aws-lake-formation/>

QUESTION 63

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 scaling metric

Correct Answer: AD

Explanation**Explanation/Reference:**

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

QUESTION 64

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 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.
- 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 tiering policy to NONE. Import the raw data into the file system. Mount the file system on the EC2 instances.

Correct Answer: B

Explanation**Explanation/Reference:**

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.

QUESTION 65

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.

Correct Answer: D

Explanation

Explanation/Reference:

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>

QUESTION 66

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.

Correct Answer: AC

Explanation

Explanation/Reference:

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/>

QUESTION 67

A meteorological startup company has a custom web application to sell weather data to its users online.

The company uses Amazon DynamoDB to store its data and wants to build a new service that sends an alert to the managers of four internal teams every time a new weather event is recorded. The company does not want the new service to affect the performance of the current application.

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

- A. Use DynamoDB transactions to write new event data to the table. Configure the transactions to notify internal teams.
- B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.
- C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.
- D. Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SQS) queue to which the teams can subscribe.

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 68

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 reads 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 ElastiCache for Redis
- C. Use Amazon Route 53 DNS caching
- D. Use Amazon ElastiCache for Memcached

Correct Answer: A

Explanation

QUESTION 69

A company is running a multi-tier e-commerce web application in the AWS Cloud. The application runs on Amazon EC2 instances with an Amazon RDS for MySQL Multi-AZ DB instance. Amazon RDS is configured with the latest generation DB instance with 2,000 GB of storage in a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. The database performance affects the application during periods of high demand.

A database administrator analyzes the logs in Amazon CloudWatch Logs and discovers that the application performance 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.

Correct Answer: B
Explanation

Explanation/Reference:

DB storage size for gp3 above 400 G support up to 64,000 IOPS, please check the below link:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

QUESTION 70

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.

Correct Answer: B
Explanation

Explanation/Reference:

This is the most cost-effective option because:

1. Versioning has caused the number of objects to increase over time, even as current objects are deleted after 3 years. By deleting previous versions as well, this will clean up old object versions and reduce storage costs.
2. An S3 Lifecycle policy incurs no additional charges and requires no additional resources to configure and run. It is a native S3 tool for managing object lifecycles cost-effectively.

<https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/best-practices-security.html#:~:text=The%20CloudTrail%20trail,time%20has%20passed.>

QUESTION 71

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

Which service should a solutions architect recommend?

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

Correct Answer: B
Explanation

Explanation/Reference:

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.

QUESTION 72

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.

Correct Answer: D

Explanation

Explanation/Reference:

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.

QUESTION 73

A company hosts its static website by using Amazon S3. The company wants to add a contact form to its webpage. The contact form will have dynamic server-side 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 endpoint 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 Lightsail. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail.
- D. 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.

Correct Answer: D

Explanation

Explanation/Reference:

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/>

QUESTION 74

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.

Correct Answer: B

Explanation

Explanation/Reference:

key words - UDP, non-relational data

answers - NLB for UDP application, DynamoDB for non-relational data

QUESTION 75

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.

Correct Answer: A

Explanation

Explanation/Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html

QUESTION 76

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

Correct Answer: C

Explanation

Explanation/Reference:

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

QUESTION 77

A company is hosting a three-tier ecommerce application in the AWS Cloud. The company hosts the website on Amazon S3 and integrates the website with an API that handles sales requests. The company hosts the API on three Amazon EC2 instances behind an Application Load Balancer (ALB). The API consists of static and dynamic front-end content along with backend workers that process sales requests asynchronously.

The company is expecting a significant and sudden increase in the number of sales requests during events for the launch of new products

What should a solutions architect recommend to ensure that all the requests are processed successfully?

- A. Add an Amazon CloudFront distribution for the dynamic content. Increase the number of EC2 instances to handle the increase in traffic.
- B. Add an Amazon CloudFront distribution for the static content. Place the EC2 instances in an Auto Scaling group to launch new instances based on network traffic.
- C. Add an Amazon CloudFront distribution for the dynamic content. Add an Amazon ElastiCache instance in front of the ALB to reduce traffic for the API to handle.
- D. Add an Amazon CloudFront distribution for the static content. Add an Amazon Simple Queue Service (Amazon SQS) queue to receive requests from the website for later processing by the EC2 instances.

Correct Answer: D

Explanation

Explanation/Reference:

An SQS queue acts as a buffer between the frontend (website) and backend (API). Web requests can dump messages into the queue at a high throughput, then the queue handles delivering those messages to the API at a controlled rate that it can sustain. This prevents the API from being overwhelmed.

QUESTION 78

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

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

Correct Answer: D

Explanation

Explanation/Reference:

To encrypt an object at the time of upload, you need to add a header called x-amz-server-side-encryption to the request to tell S3 to encrypt the object using SSE-C, SSE-S3, or SSE-KMS. The following code example shows a Put request using SSE-S3.

<https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/>

QUESTION 79

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 requirements 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 scheduled 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.

Correct Answer: C

Explanation

Explanation/Reference:

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

QUESTION 80

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 libraries. 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 retrieval of similar datasets.
- D. Increase the size of the database to increase the number of connections Lambda can establish at one time.

Correct Answer: B

Explanation

Explanation/Reference:

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/>

QUESTION 81

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 to 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 Elasticsearch 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.

Correct Answer: C

Explanation

Explanation/Reference:

Quote types need to be separated: SNS message filtering can be used to publish messages to the appropriate SQS queue based on the quote type, ensuring that quotes are separated by type. Quotes must be responded to within 24 hours and must not get lost: SQS provides reliable and scalable queuing for messages, ensuring that quotes will not get lost and can be processed in a timely manner. Additionally, each backend application server can use its own SQS queue, ensuring that quotes are processed efficiently without any delay.

Operational efficiency and minimizing maintenance: Using a single SNS topic and multiple SQS queues is a scalable and cost-effective approach, which can help to maximize operational efficiency and minimize maintenance. Additionally, SNS and SQS are fully managed services, which means that the company will not need to worry about maintenance tasks such as software updates, hardware upgrades, or scaling the infrastructure.

<https://aws.amazon.com/getting-started/hands-on/filter-messages-published-to-topics/>

QUESTION 82

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 DB instance in multiple Availability Zones to process the business reporting queries.

Correct Answer: A

Explanation

Explanation/Reference:

that business reporting queries can run without impacting write operations to the production DB instance.

QUESTION 83

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

Correct Answer: C

Explanation

Explanation/Reference:

Autoscaling with ALB / scale up on demand using on demand and spot instance combination makes sense. Reserved will not fit the no-long term commitment clause.

QUESTION 84

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.

Correct Answer: C

Explanation

Explanation/Reference:

It suggests using Amazon Transcribe with PII redaction turned on. When an audio file is uploaded to the S3 bucket, an AWS Lambda function can be used to start the transcription job. The output can be stored in a separate S3 bucket to ensure that the PII redaction is applied to the transcript. Amazon Transcribe can redact PII such as credit card numbers, social security numbers, and phone numbers.

QUESTION 85

A telemarketing company is designing its customer call center functionality on AWS. The company needs a solution that provides multiple 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 purposes.

Which solution will meet these requirements?

- A. Use Amazon Rekognition for multiple speaker recognition. Store the transcript files in Amazon S3. Use machine learning models for transcript file analysis.
- B. Use Amazon Transcribe for multiple speaker recognition. Use Amazon Athena to query transcript file analysts.
- C. Use Amazon Translate for multiple speaker recognition. Store the transcript files in Amazon Redshift.

Use SQL queues for 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

Correct Answer: B

Explanation

Explanation/Reference:

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/>

QUESTION 86

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.

Correct Answer: A

Explanation

Explanation/Reference:

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>

QUESTION 87

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

Which solution meets these requirements?

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

Correct Answer: B

Explanation

Explanation/Reference:

Cost Explorer looks at the usage pattern or history

QUESTION 88

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 times 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 ElastiCache 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.

Correct Answer: A

Explanation

Explanation/Reference:

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/>)

QUESTION 89

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.

Correct Answer: D

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/tag-editor/latest/userguide/tagging.html>

QUESTION 90

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 the AWS CLI.

- 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.

Correct Answer: C

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/cli/latest/reference/transfer/describe-server.html>

QUESTION 91

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.

Correct Answer: AD

Explanation

Explanation/Reference:

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>

QUESTION 92

A financial company hosts a web application on AWS. The application uses an Amazon API Gateway Regional API endpoint to give users the ability to retrieve current stock prices. The company's security team has noticed an increase in the number of API requests. The security team is concerned that HTTP flood attacks might take the application offline.

A solutions architect must design a solution to protect the application from this type of attack.

Which solution meets these requirements with the LEAST operational overhead?

- A. Create an Amazon CloudFront distribution in front of the API Gateway Regional API endpoint with a maximum TTL of 24 hours
- B. Create a Regional AWS WAF web ACL with a rate-based rule. Associate the web ACL with the API Gateway stage.
- C. Use Amazon CloudWatch metrics to monitor the Count metric and alert the security team when the predefined rate is reached
- D. Create an Amazon CloudFront distribution with Lambda@Edge in front of the API Gateway Regional API endpoint. Create an AWS Lambda function to block requests from IP addresses that exceed the predefined rate.

Correct Answer: B

Explanation

Explanation/Reference:

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.

QUESTION 93

A company runs a fleet of web servers using an Amazon RDS for PostgreSQL DB instance. After a routine compliance check, the company sets a standard that requires a recovery point objective (RPO) of less than 1 second for all its production databases.

Which solution meets these requirements?

- A. Enable a Multi-AZ deployment for the DB Instance
- B. Enable auto scaling for the DB instance in one Availability Zone.
- C. Configure the DB instance in one Availability Zone and create multiple read replicas in a separate Availability Zone
- D. Configure the DB instance in one Availability Zone, and configure AWS Database Migration Service (AWS DMS) change data capture (CDC) tasks

Correct Answer: A

Explanation

Explanation/Reference:

Used for DR. Every single change is replicated in a standby AZ. If we lose the main AZ, (uses the same DNS name) standby becomes automatic failover and the new main DB.

QUESTION 94

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 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 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 to 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.

Correct Answer: A

Explanation

Explanation/Reference:

Provisioned concurrency -- Provisioned concurrency initializes a requested number of execution environments so that they are prepared to respond immediately to your function's invocations. Note that configuring provisioned concurrency incurs charges to your AWS account.

QUESTION 95

A company hosts a multi-tier web application that uses an Amazon Aurora MySQL DB cluster for storage. The application tier is hosted on Amazon EC2 instances. The company's IT security guidelines mandate that the database credentials be encrypted and rotated every 14 days.

What should a solutions architect do to meet this requirement with the LEAST operational effort?

- A. Create a new AWS Key Management Service (AWS KMS) encryption key. Use AWS Secrets Manager

to create a new secret that uses the KMS key with the appropriate credentials Associate the secret with the Aurora DB cluster Configure a custom rotation period of 14 days

- B. Create two parameters in AWS Systems Manager Parameter Store one for the user name as a string parameter and one that uses the SecureString type for the password Select AWS Key Management Service (AWS KMS) encryption for the password parameter, and load these parameters in the application tier Implement an AWS Lambda function that rotates the password every 14 days.
- C. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon Elastic File System (Amazon EFS) file system Mount the EFS file system in all EC2 instances of the application tier. Restrict the access to the file on the file system so that the application can read the file and that only super users can modify the file Implement an AWS Lambda function that rotates the key in Aurora every 14 days and writes new credentials into the file
- D. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon S3 bucket that the application uses to load the credentials Download the file to the application regularly to ensure that the correct credentials are used Implement an AWS Lambda function that rotates the Aurora credentials every 14 days and uploads these credentials to the file in the S3 bucket

Correct Answer: A

Explanation

Explanation/Reference:

AWS Secrets Manager allows you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. With this service, you can automate the rotation of secrets, such as database credentials, on a schedule that you choose. The solution allows you to create a new secret with the appropriate credentials and associate it with the Aurora DB cluster. You can then configure a custom rotation period of 14 days to ensure that the credentials are automatically rotated every two weeks, as required by the IT security guidelines. This approach requires the least amount of operational effort as it allows you to manage secrets centrally without modifying your application code or infrastructure.

QUESTION 96

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.

Correct Answer: D

Explanation

Explanation/Reference:

Simple use case, highly available, and scalable -> Choose DynamoDB over RDS in terms of cost.

QUESTION 97

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.

Correct Answer: C

Explanation

QUESTION 98

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

Correct Answer: C

Explanation

Explanation/Reference:

<https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ds/index.html>

QUESTION 99

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

Correct Answer: A

Explanation

Explanation/Reference:

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.

QUESTION 100

A company needs to export its database once a day to Amazon S3 for other teams to access. The exported object size varies 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)

Correct Answer: A

Explanation

Explanation/Reference:

S3 Intelligent-Tiering monitors access patterns and moves objects that have not been accessed for 30 consecutive days to the Infrequent Access tier and after 90 days of no access to the Archive Instant Access tier.

QUESTION 101

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

What should the solutions architect recommend?

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

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 102

A hospital is designing a new application that gathers symptoms from patients. The hospital has decided to use Amazon Simple Queue Service (Amazon SQS) and Amazon Simple Notification Service (Amazon SNS) in the architecture.

A solutions architect is reviewing the infrastructure design Data must be encrypted at rest 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 the 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 policy to allow only encrypted connections over TLS.
- D. Turn on server-side encryption on the SQS 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. Set a condition in the queue policy to allow only encrypted connections over TLS.

- E. Turn on server-side encryption on the SQS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply an IAM policy to restrict key usage to a set of authorized principals. Set a condition in the queue policy to allow only encrypted connections over TLS

Correct Answer: BD

Explanation

Explanation/Reference:

<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>

QUESTION 103

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 read replica for the RDS DB instance.
- E. Configure a Multi-AZ deployment for the RDS DB instance

Correct Answer: BD

Explanation

Explanation/Reference:

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.

QUESTION 104

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

Which solution will meet these requirements?

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

Correct Answer: C

Explanation

Explanation/Reference:

Since we have sporadic & unpredictable usage for DB, Aurora Serverless would be fit more cost-efficient for this case scenario than RDS MySQL.

<https://www.techtarget.com/searchcloudcomputing/answer/When-should-I-use-Amazon-RDS-vs-Aurora-Serverless>

QUESTION 105

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

Correct Answer: D

Explanation

Explanation/Reference:

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/>

QUESTION 106

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

Correct Answer: C

Explanation

Explanation/Reference:

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/>

QUESTION 107

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's 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.

Correct Answer: AC

Explanation

Explanation/Reference:

<https://medium.com/awesome-cloud/aws-difference-between-multi-az-and-read-replicas-in-amazon-rds-60fe848ef53a>

QUESTION 108

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

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

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

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 109

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 all 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 all 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

Correct Answer: A

Explanation

Explanation/Reference:

Minimize maintenance & Patching = Serverless
S3, DynamoDB are serverless

QUESTION 110

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.

Correct Answer: A

Explanation

Explanation/Reference:

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.

QUESTION 111

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.

Correct Answer: D

Explanation

Explanation/Reference:

By using Amazon S3 as the target for the VPC Flow Logs, the logs can be easily stored and accessed by the security team. Enabling an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days will automatically move the logs to a storage class that is optimized for infrequent access, reducing the storage costs for the company. The security team will still be able to access the logs as needed, even after they have been transitioned to S3 Standard-IA, but the storage cost will be optimized.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AWS-logs-and-resource-policy.html#AWS-logs-infrastructure-S3>

QUESTION 112

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.

Correct Answer: D

Explanation

Explanation/Reference:

Stored Volume Gateway will retain ALL data locally whereas Cached Volume Gateway retains frequently accessed data locally

QUESTION 113

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.

Correct Answer: BD

Explanation

QUESTION 114

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 certificate 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).

Correct Answer: A

Explanation

Explanation/Reference:

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>

QUESTION 115

A company is deploying a two-tier web application in a VPC. The web tier is using an Amazon EC2 Auto Scaling group with public subnets that span multiple Availability Zones. The database tier consists of an Amazon RDS for MySQL DB instance in separate private subnets. The web tier requires access to the database to retrieve product information.

The web application is not working as intended. The web application reports that it cannot connect to the database. The database is confirmed to be up and running. All configurations for the network ACLs, security groups, and route tables are still in their default states.

What should a solutions architect recommend to fix the application?

- A. Add an explicit rule to the private subnet's network ACL to allow traffic from the web tier's EC2 instances.
- B. Add a route in the VPC route table to allow traffic between the web tier's EC2 instances and the database tier.
- C. Deploy the web tier's EC2 instances and the database tier's RDS instance into two separate VPCs, and configure VPC peering.
- D. Add an inbound rule to the security group of the database tier's RDS instance to allow traffic from the web tier's security group.

Correct Answer: D

Explanation

Explanation/Reference:

By default, all inbound traffic to an RDS instance is blocked. Therefore, an inbound rule needs to be added to the security group of the RDS instance to allow traffic from the security group of the web tier's EC2 instances.

QUESTION 116

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

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

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

Correct Answer: C

Explanation**Explanation/Reference:**

The most resilient and durable replacement for the on-premises file share in this scenario would be Amazon FSx for Windows File Server.

Amazon FSx is a fully managed Windows file system service that is built on Windows Server and provides native support for the SMB protocol. It is designed to be highly available and durable, with built-in backup and restore capabilities. It is also fully integrated with AWS security services, providing encryption at rest and in transit, and it can be configured to meet compliance standards.

QUESTION 117

A company has an application that 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.

Correct Answer: B

Explanation**Explanation/Reference:**

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.

QUESTION 118

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 in 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 in 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

Correct Answer: B

Explanation

Explanation/Reference:

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.

QUESTION 119

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 Aurora 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 application tier to a second Region. Create an Aurora PostgreSQL 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.

Correct Answer: D

Explanation

Explanation/Reference:

Aws Aurora Global Database allows you to read and write from any region in the global cluster. This enables you to distribute read and write workloads globally, improving performance and reducing latency. Data is replicated synchronously across regions, ensuring strong consistency.

QUESTION 120

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.

Correct Answer: AD

Explanation

Explanation/Reference:

<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.

QUESTION 121

A company's order system sends requests from clients to Amazon EC2 instances. The EC2 instances process the orders and then 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 if a system outage occurs.

What should a solutions architect do to meet these requirements?

- A. Move the 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.

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 122

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 frequently 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 (S3 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).

Correct Answer: C

Explanation

QUESTION 123

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 securely to the employees' devices.

The files are stored in an on-premises Windows file server. However, due to an increase in remote usage, the file server is out of capacity.

Which solution will meet these requirements?

- A. Migrate the file server to an Amazon EC2 instance in a public subnet. Configure the security group to limit inbound traffic to the employees' IP addresses.
- B. Migrate the files to an Amazon FSx for Windows File Server file system. Integrate the Amazon FSx file system with the on-premises Active Directory. Configure AWS Client VPN.
- C. Migrate the files to Amazon S3, and create a private VPC endpoint. Create a signed URL to allow download.
- D. Migrate the files to Amazon S3, and create a public VPC endpoint. Allow employees to sign on with AWS IAM Identity Center (AWS Single Sign-On).

Correct Answer: B

Explanation

Explanation/Reference:

This solution addresses the need for secure access to confidential and sensitive files, as well as the increase in remote usage. Migrating the files to Amazon FSx for Windows File Server provides a scalable, fully managed file storage solution in the AWS Cloud that is accessible from on-premises and cloud environments. Integration with the on-premises Active Directory allows for a consistent user experience and centralized access control. AWS Client VPN provides a secure and managed VPN solution that can be used by employees to access the files securely.

QUESTION 124

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

Correct Answer: D

Explanation

Explanation/Reference:

1. Performs active vulnerability scans of EC2 instances. It looks for software vulnerabilities, unintended network accessibility, and other security issues.
2. Requires installing an agent on EC2 instances to perform scans. The agent must be deployed to each instance.
3. Provides scheduled scan reports detailing any findings of security risks or vulnerabilities. These reports can be used to patch or remediate issues.
4. Is best suited for proactively detecting security weaknesses and misconfigurations in your AWS environment.

QUESTION 125

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 SQS) queue Send the requests to the queue Configure the queue as an event source for Lambda.

Correct Answer: D

Explanation

Explanation/Reference:

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.

QUESTION 126

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.

Correct Answer: C

Explanation

Explanation/Reference:

Amazon EC2 Reserved Instances allow for significant cost savings compared to On-Demand instances for long-running, steady-state workloads like this one. Reserved Instances provide a capacity reservation, so the instances are guaranteed to be available for the duration of the reservation period.

Amazon Aurora is a highly scalable, cloud-native relational database service that is designed to be compatible with MySQL and PostgreSQL. It can automatically scale up to meet growing storage requirements, so it can accommodate the application's database storage needs over time. By using Reserved Instances for Aurora, the cost savings will be significant over the long term.

QUESTION 127

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.

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 128

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

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

Correct Answer: A

Explanation

Explanation/Reference:

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.

QUESTION 129

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.

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 130

A solution architect needs to assign a new microservice for a company's application. Clients must be able to call an HTTPS endpoint to reach the microservice. The microservice also must use AWS identity and Access Management (IAM) to authentication calls. The solutions 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 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 distribuon. Deploy the function to CloudFront Functions. Specify AWS_IAM as the authentication type.

Correct Answer: A

Explanation

Explanation/Reference:

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.

QUESTION 131

A company collects data from a large number of participants who use wearable devices. 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.

Which 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 units (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.

Correct Answer: B

Explanation

QUESTION 132

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

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

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

Correct Answer: AE

Explanation

QUESTION 133

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.

Correct Answer: B

Explanation

Explanation/Reference:

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.

QUESTION 134

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 if 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

Correct Answer: B

Explanation

Explanation/Reference:

Note: The difference between pilot light and warm standby can sometimes be difficult to understand. Both include an environment in your DR Region with copies of your primary Region assets. The distinction is that pilot light cannot process requests without additional action taken first, whereas warm standby can handle traffic (at reduced capacity levels) immediately. The pilot light approach requires you to "turn on" servers, possibly deploy additional (non-core) infrastructure, and scale up, whereas warm standby only requires you to scale up (everything is already deployed and running). Use your RTO and RPO needs to help you choose between these approaches.

<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>

QUESTION 135

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.

Correct Answer: AC

Explanation

Explanation/Reference:

<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>

QUESTION 136

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 requirements? (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 SQS). 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.

Correct Answer: AE

Explanation

Explanation/Reference:

"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)

QUESTION 137

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.

Correct Answer: B

Explanation

Explanation/Reference:

To reduce the cost associated with data transfers and maintain or improve performance, a solutions architect should use Amazon CloudFront, a content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.

Deploying a CloudFront distribution with the existing S3 bucket as the origin will allow the company to serve the data to customers from edge locations that are closer to them, reducing data transfer costs and improving performance.

Directing customer requests to the CloudFront URL and switching to CloudFront signed URLs for access control will enable customers to access the data securely and efficiently.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>

QUESTION 138

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 to 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 that contain the new site features for testing

Correct Answer: B

Explanation

Explanation/Reference:

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.

QUESTION 139

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 authorizer 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.

Correct Answer: D

Explanation

Explanation/Reference:

KEYWORD: LEAST operational overhead

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.

QUESTION 140

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 scaling 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 experience additional lag during periods of peak load. A solutions architect must reduce the replication lag as much as possible. The solutions 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

Correct Answer: A

Explanation

QUESTION 141

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.

Correct Answer: D

Explanation

Explanation/Reference:

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>

QUESTION 142

A company is launching a new application deployed on an Amazon Elastic Container Service (Amazon ECS) cluster and is using the Fargate launch type for ECS tasks. The company is monitoring CPU and

memory usage because it is expecting high traffic to the application upon its launch. However, the company wants to reduce costs when utilization decreases.

What should a solutions architect recommend?

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

Correct Answer: D

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/autoscaling/application/userguide/what-is-application-auto-scaling.html>

QUESTION 143

A company is moving its on-premises Oracle database to Amazon Aurora PostgreSQL. The database has several applications that write to the same tables. The applications need to be migrated one by one with a month in between each migration. Management has expressed concerns that the database has a high number of reads and writes. The data must be kept in sync across both databases throughout the migration.

What should a solutions architect recommend?

- A. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a change data capture (CDC) replication task and a table mapping to select all tables.
- B. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
- C. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a memory optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
- D. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a compute optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select the largest tables.

Correct Answer: C

Explanation

Explanation/Reference:

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_ReplicationInstance.Types.html

QUESTION 144

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.

Correct Answer: B

Explanation

Explanation/Reference:

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.

QUESTION 145

A company is using Amazon Route 53 latency-based routing to route requests to its UDP-based application for users around the world. The application is hosted on redundant servers in the company's on-premises data centers in the United States, Asia, and Europe. The company's compliance requirements state that the application must be hosted on premises. The company wants to improve the performance and availability of the application.

What should a solutions architect do to meet these requirements?

- A. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the NLBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
- B. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator and register the ALBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
- C. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three NLBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.
- D. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three ALBs and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.

Correct Answer: A

Explanation

Explanation/Reference:

C - D: CloudFront doesn't support UDP/TCP.

B: Global Accelerator doesn't support ALB.

QUESTION 146

A company has a three-tier environment on AWS that ingests sensor data from its users' devices. The traffic flows through a Network Load Balancer (NLB) then to Amazon EC2 instances for the web tier and finally to EC2 instances for the application tier that makes database calls.

What should a solutions architect do to improve the security of data in transit to the web tier?

- A. Configure a TLS listener and add the server certificate on the NLB.
- B. Configure AWS Shield Advanced and enable AWS WAF on the NLB.
- C. Change the load balancer to an Application Load Balancer and attach AWS WAF to it.
- D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances using AWS Key Management Service (AWS KMS).

Correct Answer: A

Explanation

QUESTION 147

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.

Correct Answer: B

Explanation

Explanation/Reference:

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.

QUESTION 148

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 serverside 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.

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 149

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.

Correct Answer: B

Explanation

Explanation/Reference:

<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.

QUESTION 150

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.

Correct Answer: BD

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/awssupport/latest/user/organizational-view.html>

<https://docs.aws.amazon.com/awssupport/latest/user/cost-optimization-checks.html#amazon-rds-idle-dbs-instances>

QUESTION 151

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.

Correct Answer: A

Explanation

Explanation/Reference:

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.

QUESTION 152

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

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

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

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

- A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: D

Explanation

QUESTION 153

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

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

- A. AWS Key Management Service (AWS KMS)

- B. VPC endpoint
- C. Private subnet
- D. Virtual private gateway

Correct Answer: B

Explanation

Explanation/Reference:

A VPC endpoint enables you to privately access AWS services without requiring internet gateways, NAT gateways, VPN connections, or AWS Direct Connect connections. It allows you to connect your VPC directly to supported AWS services, such as Amazon S3, over a private connection within the AWS network.

By creating a VPC endpoint for Amazon S3, the traffic between your EC2 instances and S3 will stay within the AWS network and won't traverse the public internet. This provides a more secure and compliant solution, as the data transfer remains within the private network boundaries.

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints.html>

QUESTION 154

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.

Correct Answer: C

Explanation

Explanation/Reference:

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.

QUESTION 155

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

What is the MOST cost-effective solution?

- A. Store the video archives in Amazon S3 Glacier and use Expedited retrievals.
- B. Store the video archives in Amazon S3 Glacier and use Standard retrievals.
- C. Store the video archives in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).
- D. Store the video archives in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: A

Explanation

Explanation/Reference:

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? minutes and are suitable for Active Archive use cases. Standard retrievals typically complete within 3? hours and are suitable for less urgent needs. Bulk retrievals typically complete within 5?2 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? 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/>

QUESTION 156

A company has applications hosted on Amazon EC2 instances with IPv6 addresses. The applications must initiate communications with other external applications using the internet.

However, the company's security policy states that any external service cannot initiate a connection to the EC2 instances.

What should a solutions architect recommend to resolve this issue?

- A. Create a NAT gateway and make it the destination of the subnet's route table.
- B. Create an internet gateway and make it the destination of the subnet's route table
- C. Create a virtual private gateway and make it the destination of the subnet's route table.
- D. Create an egress-only internet gateway and make it the destination of the subnet's route table.

Correct Answer: D

Explanation

Explanation/Reference:

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:

<https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html>

<https://dev.to/aws-builders/what-is-an-egress-only-internet-gateways-in-aws-7gp>

<https://docs.aws.amazon.com/vpc/latest/userguide/route-table-options.html>

QUESTION 157

A company hosts an online shopping application that stores all orders in an Amazon RDS for PostgreSQL Single-AZ DB instance. Management wants to eliminate single points of 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.

Correct Answer: A

Explanation

Explanation/Reference:

<https://aws.amazon.com/rds/features/multi-az/> To convert an existing Single-AZ DB Instance to a Multi-AZ deployment, use the "Modify" option corresponding to your DB Instance in the AWS Management Console.

QUESTION 158

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 Versioning 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.

Correct Answer: D

Explanation

Explanation/Reference:

You need AWS Batch to re-apply certain config to files that were already in S3, like encryption.

QUESTION 159

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.

Correct Answer: A

Explanation

Explanation/Reference:

By combining Multi-AZ EC2 Auto Scaling and an Application Load Balancer, you achieve high availability.

for the EC2 instances hosting your stateless two-tier application.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-availability-zone.html>

QUESTION 160

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 the 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.

Correct Answer: BE

Explanation

Explanation/Reference:

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>

QUESTION 161

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

Which method should the solutions architect select?

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

Correct Answer: A

Explanation

Explanation/Reference:

<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 replicas 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/>

QUESTION 162

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 IAM 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 IAM 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 IAM Identity Center (AWS Single Sign-On) in the organization. Configure IAM Identity Center, and integrate it with the company's corporate directory service.

Correct Answer: AE

Explanation

Explanation/Reference:

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 IAM 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 IAM Identity 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

QUESTION 163

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

Correct Answer: C

Explanation

Explanation/Reference:

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/>

QUESTION 164

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 determine 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 to 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.

Correct Answer: C

Explanation

Explanation/Reference:

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 tier. 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-1A).

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>

QUESTION 165

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.

Correct Answer: C

Explanation

Explanation/Reference:

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/>

QUESTION 166

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.

Correct Answer: A

Explanation

Explanation/Reference:

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 Lambda 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](https://docs.aws.amazon.com/lambda/latest/dg/lambda-api-permissions-ref.html)

QUESTION 167

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)

Correct Answer: BC

Explanation

Explanation/Reference:

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 Go¹. 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/>

QUESTION 168

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.

Correct Answer: B

Explanation

Explanation/Reference:

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. Ensure 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

QUESTION 169

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 inventory[^]. 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

Correct Answer: C

Explanation

Explanation/Reference:

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 workloads 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/>

QUESTION 170

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.

Correct Answer: AB

Explanation

Explanation/Reference:

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/>

QUESTION 171

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.

Correct Answer: B

Explanation

Explanation/Reference:

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 protocol². 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/>

QUESTION 172

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 all buckets.
- B. Design a bucket policy that gives read-only access to users. Specify IAM entities as principals
- C. Create a cross-account IAM role that has a read-only access policy specified for the IAM role.
- D. Create a user policy and vendor user groups that give read-only access to vendor users

Correct Answer: C

Explanation

Explanation/Reference:

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

QUESTION 173

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

Correct Answer: B

Explanation

Explanation/Reference:

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:

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

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html>

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-what-is-concepts.html>

Exam F

QUESTION 1

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

What should a solutions architect recommend?

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

Correct Answer: D

Explanation

Explanation/Reference:

https://aws.amazon.com/storagegateway/vtl/?nc1=h_ls

QUESTION 2

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.

Correct Answer: A

Explanation

Explanation/Reference:

Data collection in near real time = Amazon Kinesis Data Firehose

QUESTION 3

A company has separate AWS accounts for its finance, data analytics, and development departments. Because of costs and security concerns, the company wants to control which services each AWS account can use.

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

- A. Use AWS Systems Manager templates to control which AWS services each department can use.
- B. Create organization units (OUs) for each department in AWS Organizations. Attach service control policies (SCPs) to the OUs.
- C. Use AWS CloudFormation to automatically provision only the AWS services that each department can use.
- D. Set up a list of products in AWS Service Catalog in the AWS accounts to manage and control the usage of specific AWS services.

Correct Answer: B

Explanation

Explanation/Reference:

To control different AWS account you required AWS Organisation

QUESTION 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.

Correct Answer: B

Explanation

Explanation/Reference:

NAT Gateway is safe

QUESTION 5

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.

Correct Answer: BD

Explanation

QUESTION 6

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.

Correct Answer: A

Explanation

QUESTION 7

A company needs to optimize the cost of its Amazon EC2 instances. The company also needs to change the type and family of its EC2 instances every 2-3 months.

What should the company do to meet these requirements?

- A. Purchase Partial Upfront Reserved Instances for a 3-year term.
- B. Purchase a No Upfront Compute Savings Plan for a 1-year term.
- C. Purchase All Upfront Reserved Instances for a 1-year term.
- D. Purchase an All Upfront EC2 Instance Savings Plan for a 1-year term.

Correct Answer: B

Explanation

Explanation/Reference:

"EC2 Instance Savings Plans give you the flexibility to change your usage between instances WITHIN a family in that region. "

<https://aws.amazon.com/savingsplans/compute-pricing/>

QUESTION 8

A solutions architect needs to review a company's Amazon S3 buckets to discover personally identifiable information (PII). The company stores the PII data in the us-east-1 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.

Correct Answer: A

Explanation

Explanation/Reference:

AWS Macie = PII detection

QUESTION 9

A company's SAP application has a backend SQL Server database in an on-premises environment. The company wants to migrate its on-premises application and database server to AWS. The company needs an instance type that meets the high demands of its SAP database. On-premises performance data shows that both the SAP application and the database have high memory utilization.

Which solution will meet these requirements?

- A. Use the compute optimized instance family for the application. Use the memory optimized instance family for the database.
- B. Use the storage optimized instance family for both the application and the database.
- C. Use the memory optimized instance family for both the application and the database.
- D. Use the high performance computing (HPC) optimized instance family for the application. Use the memory optimized instance family for the database.

Correct Answer: C

Explanation

QUESTION 10

A company runs an application in a VPC with public and private subnets. The VPC extends across multiple

Availability Zones. The application runs on Amazon EC2 instances in private subnets. The application uses an Amazon Simple Queue Service (Amazon SQS) queue.

A solutions architect needs to design a secure solution to establish a connection between the EC2 instances and the SQS queue.

Which solution will meet these requirements?

- A. Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the private subnets. Add to the endpoint a security group that has an inbound access rule that allows traffic from the EC2 instances that are in the private subnets.
- B. Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the public subnets. Attach to the interface endpoint a VPC endpoint policy that allows access from the EC2 instances that are in the private subnets.
- C. Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the public subnets. Attach an Amazon SQS access policy to the interface VPC endpoint that allows requests from only a specified VPC endpoint.
- D. Implement a gateway endpoint for Amazon SQS. Add a NAT gateway to the private subnets. Attach an IAM role to the EC2 instances that allows access to the SQS queue.

Correct Answer: A

Explanation

QUESTION 11

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.

Correct Answer: A

Explanation

QUESTION 12

A solutions architect manages an analytics application. The application stores large amounts of semistructured data in an Amazon S3 bucket. The solutions architect wants to use parallel data processing to process the data more quickly. The solutions architect also wants to use information that is stored in an Amazon Redshift database to enrich the data.

Which solution will meet these requirements?

- A. Use Amazon Athena to process the S3 data. Use AWS Glue with the Amazon Redshift data to enrich the S3 data.
- B. Use Amazon EMR to process the S3 data. Use Amazon EMR with the Amazon Redshift data to enrich the S3 data.

- C. Use Amazon EMR to process the S3 data. Use Amazon Kinesis Data Streams to move the S3 data into Amazon Redshift so that the data can be enriched.
- D. Use AWS Glue to process the S3 data. Use AWS Lake Formation with the Amazon Redshift data to enrich the S3 data.

Correct Answer: D

Explanation

QUESTION 13

A company has two VPCs that are located in the us-west-2 Region within the same AWS account. The company needs to allow network traffic between these VPCs. Approximately 500 GB of data transfer will occur between the VPCs each month.

What is the MOST cost-effective solution to connect these VPCs?

- A. Implement AWS Transit Gateway to connect the VPCs. Update the route tables of each VPC to use the transit gateway for inter-VPC communication.
- B. Implement an AWS Site-to-Site VPN tunnel between the VPCs. Update the route tables of each VPC to use the VPN tunnel for inter-VPC communication.
- C. Set up a VPC peering connection between the VPCs. Update the route tables of each VPC to use the VPC peering connection for inter-VPC communication.
- D. Set up a 1 GB AWS Direct Connect connection between the VPCs. Update the route tables of each VPC to use the Direct Connect connection for inter-VPC communication.

Correct Answer: C

Explanation

Explanation/Reference:

VPC peering is the most cost-effective way to connect two VPCs within the same region and AWS account. There are no additional charges for VPC peering beyond standard data transfer rates.

Transit Gateway and VPN add additional hourly and data processing charges that are not necessary for simple VPC peering.

Direct Connect provides dedicated network connectivity, but is overkill for the relatively low inter-VPC data transfer needs described here. It has high fixed costs plus data transfer rates.

For occasional inter-VPC communication of moderate data volumes within the same region and account, VPC peering is the most cost-effective solution. It provides simple private connectivity without transfer charges or network appliances.

QUESTION 14

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? (Choose 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.

Correct Answer: BE

Explanation

Explanation/Reference:

"Only a management account in an organization and single accounts that aren't members of an organization have access to the cost allocation tags manager in the Billing and Cost Management console."

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html>

QUESTION 15

A company's solutions architect is designing an AWS multi-account solution that uses AWS Organizations. The solutions architect has organized the company's accounts into organizational units (OUs).

The solutions architect needs a solution that will identify any changes to the OU hierarchy. The solution also needs to notify the company's operations team of any changes.

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

- A. Provision the AWS accounts by using AWS Control Tower. Use account drift notifications to identify the changes to the OU hierarchy.
- B. Provision the AWS accounts by using AWS Control Tower. Use AWS Config aggregated rules to identify the changes to the OU hierarchy.
- C. Use AWS Service Catalog to create accounts in Organizations. Use an AWS CloudTrail organization trail to identify the changes to the OU hierarchy.
- D. Use AWS CloudFormation templates to create accounts in Organizations. Use the drift detection operation on a stack to identify the changes to the OU hierarchy.

Correct Answer: A

Explanation**Explanation/Reference:**

<https://docs.aws.amazon.com/controltower/latest/userguide/what-is-control-tower.html>

<https://docs.aws.amazon.com/controltower/latest/userguide/prevention-and-notification.html>

QUESTION 16

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.

Correct Answer: A

Explanation**Explanation/Reference:**

DynamoDB = DAX

QUESTION 17

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.

Correct Answer: AB

Explanation

QUESTION 18

A company runs its applications on both Amazon Elastic Kubernetes Service (Amazon EKS) clusters and on-premises Kubernetes clusters. The company wants to view all clusters and workloads from a central location.

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

- A. Use Amazon CloudWatch Container Insights to collect and group the cluster information.
- B. Use Amazon EKS Connector to register and connect all Kubernetes clusters.
- C. Use AWS Systems Manager to collect and view the cluster information.
- D. Use Amazon EKS Anywhere as the primary cluster to view the other clusters with native Kubernetes commands.

Correct Answer: B

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/eks/latest/userguide/eks-connector.html>

QUESTION 19

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.

Correct Answer: B

Explanation

Explanation/Reference:

"even from database administrators" -> "Client Side encryption"

QUESTION 20

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.

Correct Answer: C

Explanation

Explanation/Reference:

Aurora is better in autoscaling than RDS

QUESTION 21

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 (io2) Amazon Elastic Block Store (Amazon EBS) volume. Attach the EBS volume to all the EC2 instances.
- D. Create file systems on Amazon Elastic Block Store (Amazon EBS) volumes that are attached to each EC2 instance. Synchronize the EBS volumes across the different EC2 instances.

Correct Answer: B

Explanation

Explanation/Reference:

How is Amazon EFS different than Amazon S3?

Amazon EFS provides shared access to data using a traditional file sharing permissions model and hierarchical directory structure via the NFSv4 protocol. Applications that access data using a standard file system interface provided through the operating system can use Amazon EFS to take advantage of the scalability and reliability of file storage in the cloud without writing any new code or adjusting applications.

Amazon S3 is an object storage platform that uses a simple API for storing and accessing data.

Applications that do not require a file system structure and are designed to work with object storage can use Amazon S3 as a massively scalable, durable, low-cost object storage solution.

QUESTION 22

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.

Correct Answer: A
Explanation

Explanation/Reference:

"The workload will receive more features in the future ..." -> DynamoDB

QUESTION 23

A solutions architect is designing the storage architecture for a new web application used for storing and viewing engineering drawings. All application components will be deployed on the AWS infrastructure.

The application design must support caching to minimize the amount of time that users wait for the engineering drawings to load. The application must be able to store petabytes of data.

Which combination of storage and caching should the solutions architect use?

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

Correct Answer: A
Explanation

Explanation/Reference:

B : Glacier for archiving

C : i dont think EBS scale to petabytes (I am not sure about that)

D : it incorrect because All application components will be deployed on the AWS infrastructure

QUESTION 24

An Amazon EventBridge rule targets a third-party API. The third-party API has not received any incoming traffic. A solutions architect needs to determine whether the rule conditions are being met and if the rule's target is being invoked.

Which solution will meet these requirements?

- A. Check for metrics in Amazon CloudWatch in the namespace for AWS/Events.
- B. Review events in the Amazon Simple Queue Service (Amazon SQS) dead-letter queue.
- C. Check for the events in Amazon CloudWatch Logs.
- D. Check the trails in AWS CloudTrail for the EventBridge events.

Correct Answer: A
Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/CloudWatch-Events-Monitoring-CloudWatch-Metrics.html>

QUESTION 25

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.

Correct Answer: B
Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html>

QUESTION 26

A company is creating a REST API. The company has strict requirements for the use of TLS. The company requires TLSv1.3 on the API endpoints. The company also requires a specific public third-party certificate authority (CA) to sign the TLS certificate.

Which solution will meet these requirements?

- A. Use a local machine to create a certificate that is signed by the third-party CA. Import the certificate into AWS Certificate Manager (ACM). Create an HTTP API in Amazon API Gateway with a custom domain. Configure the custom domain to use the certificate.
- B. Create a certificate in AWS Certificate Manager (ACM) that is signed by the third-party CA. Create an HTTP API in Amazon API Gateway with a custom domain. Configure the custom domain to use the certificate.
- C. Use AWS Certificate Manager (ACM) to create a certificate that is signed by the third-party CA. Import the certificate into AWS Certificate Manager (ACM). Create an AWS Lambda function with a Lambda function URL. Configure the Lambda function URL to use the certificate.
- D. Create a certificate in AWS Certificate Manager (ACM) that is signed by the third-party CA. Create an AWS Lambda function with a Lambda function URL. Configure the Lambda function URL to use the certificate.

Correct Answer: B
Explanation

Explanation/Reference:

AWS Certificate Manager (ACM) is a service that lets you easily provision, manage, and deploy SSL/TLS certificates for use with AWS services and your internal resources. By creating a certificate in ACM that is signed by the third-party CA, the company can meet its requirement for a specific public third-party CA to sign the TLS certificate.

QUESTION 27

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.

Correct Answer: C
Explanation

Explanation/Reference:

Instead of provisioning and managing database servers, you specify Aurora capacity units (ACUs). Each ACU is a combination of approximately 2 gigabytes (GB) of memory, corresponding CPU, and networking. Database storage automatically scales from 10 gibibytes (GiB) to 128 tebibytes (TiB), the same as storage in a standard Aurora DB cluster.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v1.how-it-works.html>
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v2.html>

QUESTION 28

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.

Correct Answer: D

Explanation

Explanation/Reference:

Lambda SnapStart for Java can improve startup performance for latency-sensitive applications by up to 10x at no extra cost, typically with no changes to your function code. The largest contributor to startup latency (often referred to as cold start time) is the time that Lambda spends initializing the function, which includes loading the function's code, starting the runtime, and initializing the function code.

<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html>

QUESTION 29

A financial services company launched a new application that uses an Amazon RDS for MySQL database. The company uses the application to track stock market trends. The company needs to operate the application for only 2 hours at the end of each week. The company needs to optimize the cost of running the database.

Which solution will meet these requirements MOST cost-effectively?

- A. Migrate the existing RDS for MySQL database to an Aurora Serverless v2 MySQL database cluster.
- B. Migrate the existing RDS for MySQL database to an Aurora MySQL database cluster.
- C. Migrate the existing RDS for MySQL database to an Amazon EC2 instance that runs MySQL.
Purchase an instance reservation for the EC2 instance.
- D. Migrate the existing RDS for MySQL database to an Amazon Elastic Container Service (Amazon ECS) cluster that uses MySQL container images to run tasks.

Correct Answer: A

Explanation

QUESTION 30

A company deploys its applications on Amazon Elastic Kubernetes Service (Amazon EKS) behind an Application Load Balancer in an AWS Region. The application needs to store data in a PostgreSQL database engine. The company wants the data in the database to be highly available. The company also needs increased capacity for read workloads.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Create an Amazon DynamoDB database table configured with global tables.
- B. Create an Amazon RDS database with Multi-AZ deployments.
- C. Create an Amazon RDS database with Multi-AZ DB cluster deployment.
- D. Create an Amazon RDS database configured with cross-Region read replicas.

Correct Answer: C

Explanation

Explanation/Reference:

DB cluster deployment can scale read workloads by adding read replicas. This provides increased capacity for read workloads without impacting the write workload.

QUESTION 31

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-optimized endpoint

Correct Answer: D

Explanation

Explanation/Reference:

API Gateway - Endpoint Types

? Edge-Optimized (default): For global clients

? Requests are routed through the CloudFront Edge locations (improves latency)

? The API Gateway still lives in only one region

? Regional:

? For clients within the same region

? Could manually combine with CloudFront (more control over the caching strategies and the distribution)

? Private:

? Can only be accessed from your VPC using an interface VPC endpoint (ENI)

? Use a resource policy to define access

QUESTION 32

A company uses an Amazon CloudFront distribution to serve content pages for its website. The company needs to ensure that clients use a TLS certificate when accessing the company's website. The company wants to automate the creation and renewal of the TLS certificates.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Use a CloudFront security policy to create a certificate.
- B. Use a CloudFront origin access control (OAC) to create a certificate.
- C. Use AWS Certificate Manager (ACM) to create a certificate. Use DNS validation for the domain.
- D. Use AWS Certificate Manager (ACM) to create a certificate. Use email validation for the domain.

Correct Answer: C

Explanation

Explanation/Reference:

"DNS Validation is preferred for automation purposes" -- Stephane's course on Udemy

QUESTION 33

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.

Correct Answer: A

Explanation

Explanation/Reference:

Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for Amazon DynamoDB that delivers up to a 10 times performance improvement—from milliseconds to microseconds—even at millions of requests per second.

[https://aws.amazon.com/dynamodb/dax/#:~:text=Amazon%20DynamoDB%20Accelerator%20\(DAX\)%20is,millions%20of%20requests%20per%20second.](https://aws.amazon.com/dynamodb/dax/#:~:text=Amazon%20DynamoDB%20Accelerator%20(DAX)%20is,millions%20of%20requests%20per%20second.)

QUESTION 34

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.

Correct Answer: A

Explanation

Explanation/Reference:

<https://aws.amazon.com/solutions/implementations/instance-scheduler-on-aws/>

QUESTION 35

A company uses locally attached storage to run a latency-sensitive application on premises. The company is using a lift and shift method to move the application to the AWS Cloud. The company does not want to change the application architecture.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure an Auto Scaling group with an Amazon EC2 instance. Use an Amazon FSx for Lustre file system to run the application.
- B. Host the application on an Amazon EC2 instance. Use an Amazon Elastic Block Store (Amazon EBS) GP2 volume to run the application.
- C. Configure an Auto Scaling group with an Amazon EC2 instance. Use an Amazon FSx for OpenZFS file system to run the application.
- D. Host the application on an Amazon EC2 instance. Use an Amazon Elastic Block Store (Amazon EBS) GP3 volume to run the application.

Correct Answer: B

Explanation

QUESTION 36

A company runs a stateful production application on Amazon EC2 instances. The application requires at least two EC2 instances to always be running.

A solutions architect needs to design a highly available and fault-tolerant architecture for the application. The solutions architect creates an Auto Scaling group of EC2 instances.

Which set of additional steps should the solutions architect take to meet these requirements?

- A. Set the Auto Scaling group's minimum capacity to two. Deploy one On-Demand Instance in one Availability Zone and one On-Demand Instance in a second Availability Zone.
- B. Set the Auto Scaling group's minimum capacity to four. Deploy two On-Demand Instances in one Availability Zone and two On-Demand Instances in a second Availability Zone.
- C. Set the Auto Scaling group's minimum capacity to two. Deploy four Spot Instances in one Availability Zone.
- D. Set the Auto Scaling group's minimum capacity to four. Deploy two On-Demand Instances in one Availability Zone and two Spot Instances in a second Availability Zone.

Correct Answer: B

Explanation

Explanation/Reference:

By setting the Auto Scaling group's minimum capacity to four, the architect ensures that there are always at least two running instances. Deploying two On-Demand Instances in each of two Availability Zones ensures that the application is highly available and fault-tolerant. If one Availability Zone becomes unavailable, the application can still run in the other Availability Zone.

QUESTION 37

An ecommerce company uses Amazon Route 53 as its DNS provider. The company hosts its website on premises and in the AWS Cloud. The company's on-premises data center is near the us-west-1 Region. The company uses the eu-central-1 Region to host the website. The company wants to minimize load time for the website as much as possible.

Which solution will meet these requirements?

- A. Set up a geolocation routing policy. Send the traffic that is near us-west-1 to the on-premises data center. Send the traffic that is near eu-central-1 to eu-central-1.
- B. Set up a simple routing policy that routes all traffic that is near eu-central-1 to eu-central-1 and routes all traffic that is near the on-premises datacenter to the on-premises data center.
- C. Set up a latency routing policy. Associate the policy with us-west-1.
- D. Set up a weighted routing policy. Split the traffic evenly between eu-central-1 and the on-premises data center.

Correct Answer: A

Explanation

QUESTION 38

A company has 5 PB of archived data on physical tapes. The company needs to preserve the data on the tapes for another 10 years for compliance purposes. The company wants to migrate to AWS in the next 6 months. The data center that stores the tapes has a 1 Gbps uplink internet connectivity.

Which solution will meet these requirements MOST cost-effectively?

- A. Read the data from the tapes on premises. Stage the data in a local NFS storage. Use AWS DataSync to migrate the data to Amazon S3 Glacier Flexible Retrieval.
- B. Use an on-premises backup application to read the data from the tapes and to write directly to Amazon S3 Glacier Deep Archive.
- C. Order multiple AWS Snowball devices that have Tape Gateway. Copy the physical tapes to virtual tapes in Snowball. Ship the Snowball devices to AWS. Create a lifecycle policy to move the tapes to Amazon S3 Glacier Deep Archive.
- D. Configure an on-premises Tape Gateway. Create virtual tapes in the AWS Cloud. Use backup software to copy the physical tape to the virtual tape.

Correct Answer: C

Explanation

QUESTION 39

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.

Correct Answer: B

Explanation**Explanation/Reference:**

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.

QUESTION 40

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.

Correct Answer: A

Explanation**Explanation/Reference:**

Clearly the right choice, with a read replica all the queries needed for a report are done in the replica, leaving the primary on best performance for write

QUESTION 41

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.

Correct Answer: B

Explanation

Explanation/Reference:

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.

QUESTION 42

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.

Correct Answer: B

Explanation

Explanation/Reference:

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.

QUESTION 43

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 networking 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

Correct Answer: ACF

Explanation

Explanation/Reference:

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/>

QUESTION 44

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.

Correct Answer: C

Explanation

Explanation/Reference:

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/>

QUESTION 45

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.

Correct Answer: C

Explanation

Explanation/Reference:

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 needed¹. 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: <https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-on-demand.html>

QUESTION 46

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.

Correct Answer: B

Explanation

Explanation/Reference:

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>

QUESTION 47

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.

Correct Answer: B

Explanation

Explanation/Reference:

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>

QUESTION 48

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) turned 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.

Correct Answer: A

Explanation

Explanation/Reference:

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>

QUESTION 49

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.

Correct Answer: A

Explanation

Explanation/Reference:

Spread Placement Group strictly places a small group of instances across distinct underlying hardware to reduce correlated failures.

QUESTION 50

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.

Correct Answer: C

Explanation

Explanation/Reference:

When separating a business unit from an AWS Organizations structure, best practice is to:

Create a new AWS account dedicated for the business unit in the new organization

Migrate resources from the old account to the new account

Remove the old account from the original organization

This allows a clean break between the organizations and avoids any linking between them after separation.

QUESTION 51

A solutions architect is designing a disaster recovery (DR) strategy to provide Amazon EC2 capacity in a failover AWS Region. Business requirements state that the DR strategy must meet capacity in the failover Region.

Which solution will meet these requirements?

- A. Purchase On-Demand Instances in the failover Region.
- B. Purchase an EC2 Savings Plan in the failover Region.
- C. Purchase regional Reserved Instances in the failover Region.
- D. Purchase a Capacity Reservation in the failover Region.

Correct Answer: D

Explanation

Explanation/Reference:

Capacity Reservations allocate EC2 capacity in a specific AWS Region for you to launch instances.

The capacity is reserved and available to be utilized when needed, meeting the requirement to provide EC2 capacity in the failover region.

Other options do not reserve capacity. On-Demand provides flexible capacity but does not reserve capacity upfront.

Savings Plans and Reserved Instances provide discounts but do not reserve capacity.

Capacity Reservations allow defining instance attributes like instance type, platform, Availability Zone so the reserved capacity matches the production environment.

QUESTION 52

A company runs a web application on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer that has sticky sessions enabled. The web server currently hosts the user session state. The company wants to ensure high availability and avoid user session state loss in the event of a web server outage.

Which solution will meet these requirements?

- A. Use an Amazon ElastiCache for Memcached instance to store the session data. Update the application to use ElastiCache for Memcached to store the session state.
- B. Use Amazon ElastiCache for Redis to store the session state. Update the application to use ElastiCache for Redis to store the session state.
- C. Use an AWS Storage Gateway cached volume to store session data. Update the application to use AWS Storage Gateway cached volume to store the session state.
- D. Use Amazon RDS to store the session state. Update the application to use Amazon RDS to store the session state.

Correct Answer: B

Explanation

Explanation/Reference:

ElastiCache Redis provides in-memory caching that can deliver microsecond latency for session data.

Redis supports replication and multi-AZ which can provide high availability for the cache.

The application can be updated to store session data in ElastiCache Redis rather than locally on the web servers.

If a web server fails, the user can be routed via the load balancer to another web server which can retrieve their session data from the highly available ElastiCache Redis cluster.

QUESTION 53

A company plans to migrate to AWS 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.

Correct Answer: C

Explanation

Explanation/Reference:

Hibernation saves the in-memory state of the EC2 instance to persistent storage and shuts the instance

down. When the instance is started again, the in-memory state is restored, which launches much faster than launching a new instance.

Warm pools pre-initialize EC2 instances and keep them ready to fulfill requests, reducing launch time. The hibernated instances can be added to a warm pool.

When auto scaling scales out during the next testing phase, it will be able to launch instances from the warm pool rapidly since they are already initialized

QUESTION 54

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.

Correct Answer: D

Explanation

Explanation/Reference:

API Gateway is a fully managed service that makes it easy for you to create, publish, maintain, monitor, and secure APIs at any scale. API Gateway provides an entry point to your microservices

QUESTION 55

A company uses AWS and sells access to copyrighted images. The company's global customer base needs to be able to access these images quickly. The company must deny access to users from specific countries. The company wants to minimize costs as much as possible.

Which solution will meet these requirements?

- A. Use Amazon S3 to store the images. Turn on multi-factor authentication (MFA) and public bucket access. Provide customers with a link to the S3 bucket.
- B. Use Amazon S3 to store the images. Create an IAM user for each customer. Add the users to a group that has permission to access the S3 bucket.
- C. Use Amazon EC2 instances that are behind Application Load Balancers (ALBs) to store the images. Deploy the instances only in the countries the company services. Provide customers with links to the ALBs for their specific country's instances.
- D. Use Amazon S3 to store the images. Use Amazon CloudFront to distribute the images with geographic restrictions. Provide a signed URL for each customer to access the data in CloudFront.

Correct Answer: D

Explanation

Explanation/Reference:

Use Amazon S3 to store the images. Use Amazon CloudFront to distribute the images with geographic restrictions. Provide a signed URL for each customer to access the data in CloudFront.

QUESTION 56

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.

Correct Answer: A

Explanation

Explanation/Reference:

Aurora Serverless v2 got autoscaling, highly available and cheaper when compared to the other options.

QUESTION 57

A company runs its critical database on an Amazon RDS for PostgreSQL DB instance. The company wants to migrate to Amazon Aurora PostgreSQL with minimal downtime and data loss.

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

- A. Create a DB snapshot of the RDS for PostgreSQL DB instance to populate a new Aurora PostgreSQL DB cluster.
- B. Create an Aurora read replica of the RDS for PostgreSQL DB instance. Promote the Aurora read replicate to a new Aurora PostgreSQL DB cluster.
- C. Use data import from Amazon S3 to migrate the database to an Aurora PostgreSQL DB cluster.
- D. Use the `pg_dump` utility to back up the RDS for PostgreSQL database. Restore the backup to a new Aurora PostgreSQL DB cluster.

Correct Answer: B

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraPostgreSQL.Migrating.html>

QUESTION 58

An ecommerce company wants a disaster recovery solution for its Amazon RDS DB instances that run Microsoft SQL Server Enterprise Edition. The company's current recovery point objective (RPO) and recovery time objective (RTO) are 24 hours.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a cross-Region read replica and promote the read replica to the primary instance.
- B. Use AWS Database Migration Service (AWS DMS) to create RDS cross-Region replication.
- C. Use cross-Region replication every 24 hours to copy native backups to an Amazon S3 bucket.
- D. Copy automatic snapshots to another Region every 24 hours.

Correct Answer: D

Explanation

Explanation/Reference:

This is the most cost-effective solution because it does not require any additional AWS services. Amazon RDS automatically creates snapshots of your DB instances every hour. You can copy these snapshots to another Region every 24 hours to meet your RPO and RTO requirements.

The other solutions are more expensive because they require additional AWS services. For example, AWS DMS is a more expensive service than AWS RDS.

QUESTION 59

A company recently migrated to the AWS Cloud. The company wants a serverless solution for large-scale parallel on-demand processing of a semistructured dataset. The data consists of logs, media files, sales transactions, and IoT sensor data that is stored in Amazon S3. The company wants the solution to process thousands of items in the dataset in parallel.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Use the AWS Step Functions Map state in Inline mode to process the data in parallel.
- B. Use the AWS Step Functions Map state in Distributed mode to process the data in parallel.
- C. Use AWS Glue to process the data in parallel.
- D. Use several AWS Lambda functions to process the data in parallel.

Correct Answer: B

Explanation

Explanation/Reference:

With Step Functions, you can orchestrate large-scale parallel workloads to perform tasks, such as on-demand processing of semi-structured data. These parallel workloads let you concurrently process large-scale data sources stored in Amazon S3. <https://docs.aws.amazon.com/step-functions/latest/dg/concepts-orchestrate-large-scale-parallel-workloads.html>

QUESTION 60

A company's infrastructure consists of hundreds of Amazon EC2 instances that use Amazon Elastic Block Store (Amazon EBS) storage. A solutions architect must ensure that every EC2 instance can be recovered after a disaster.

What should the solutions architect do to meet this requirement with the LEAST amount of effort?

- A. Take a snapshot of the EBS storage that is attached to each EC2 instance. Create an AWS CloudFormation template to launch new EC2 instances from the EBS storage.
- B. Take a snapshot of the EBS storage that is attached to each EC2 instance. Use AWS Elastic Beanstalk to set the environment based on the EC2 template and attach the EBS storage.
- C. Use AWS Backup to set up a backup plan for the entire group of EC2 instances. Use the AWS Backup API or the AWS CLI to speed up the restore process for multiple EC2 instances.
- D. Create an AWS Lambda function to take a snapshot of the EBS storage that is attached to each EC2 instance and copy the Amazon Machine Images (AMIs). Create another Lambda function to perform the restores with the copied AMIs and attach the EBS storage.

Correct Answer: C

Explanation

Explanation/Reference:

Going with Backup. Can restore programmatically using Backup API.

QUESTION 61

A company is planning to migrate a TCP-based application into the company's VPC. The application is publicly accessible on a nonstandard TCP port through a hardware appliance in the company's data center. This public endpoint can process up to 3 million requests per second with low latency. The company requires the same level of performance for the new public endpoint in AWS.

What should a solutions architect recommend to meet this requirement?

- A. Deploy a Network Load Balancer (NLB). Configure the NLB to be publicly accessible over the TCP port that the application requires.
- B. Deploy an Application Load Balancer (ALB). Configure the ALB to be publicly accessible over the TCP port that the application requires.
- C. Deploy an Amazon CloudFront distribution that listens on the TCP port that the application requires. Use an Application Load Balancer as the origin.
- D. Deploy an Amazon API Gateway API that is configured with the TCP port that the application requires. Configure AWS Lambda functions with provisioned concurrency to process the requests.

Correct Answer: A

Explanation

Explanation/Reference:

NLBs handle millions of requests per second. NLBs can handle general TCP traffic.

QUESTION 62

A company has several on-premises Internet Small Computer Systems Interface (iSCSI) network storage servers. The company wants to reduce the number of these servers by moving to the AWS Cloud. A solutions architect must provide low-latency access to frequently used data and reduce the dependency on on-premises servers with a minimal number of infrastructure changes.

Which solution will meet these requirements?

- A. Deploy an Amazon S3 File Gateway.
- B. Deploy Amazon Elastic Block Store (Amazon EBS) storage with backups to Amazon S3.
- C. Deploy an AWS Storage Gateway volume gateway that is configured with stored volumes.
- D. Deploy an AWS Storage Gateway volume gateway that is configured with cached volumes.

Correct Answer: D

Explanation

Explanation/Reference:

iSCSI=Volume Gateway.

low-latency access to frequently used data = cached volumes

An AWS Storage Gateway volume gateway is a hybrid storage solution that connects your on-premises applications to your cloud storage. It provides low-latency access to frequently used data while storing your entire dataset in the cloud.

When you configure an AWS Storage Gateway volume gateway with cached volumes, the gateway stores a copy of frequently accessed data locally. This allows you to provide low-latency access to your frequently accessed data while reducing your dependency on on-premises servers.

QUESTION 63

A company will migrate 10 PB of data to Amazon S3 in 6 weeks. The current data center has a 500 Mbps uplink to the internet. Other on-premises applications share the uplink. The company can use 80% of the internet bandwidth for this one-time migration task.

Which solution will meet these requirements?

- A. Configure AWS DataSync to migrate the data to Amazon S3 and to automatically verify the data.
- B. Use rsync to transfer the data directly to Amazon S3.
- C. Use the AWS CLI and multiple copy processes to send the data directly to Amazon S3.
- D. Order multiple AWS Snowball devices. Copy the data to the devices. Send the devices to AWS to copy the data to Amazon S3.

Correct Answer: D

Explanation

QUESTION 64

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 an 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? (Choose 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 File 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. Setup Amazon Athena to query the data that is in Amazon S3. Provide access to analysts.

Correct Answer: ACF

Explanation

Explanation/Reference:

<https://docs.aws.amazon.com/glue/latest/dg/aws-glue-programming-etl-format-csv-home.html>
<https://aws.amazon.com/blogs/aws/amazon-athena-interactive-sql-queries-for-data-in-amazon-s3/>
<https://aws.amazon.com/storagegateway/faqs/>

QUESTION 65

A company has migrated a two-tier application from its on-premises data center to the AWS Cloud. The data tier is a Multi-AZ deployment of Amazon RDS for Oracle with 12 TB of General Purpose SSD Amazon Elastic Block Store (Amazon EBS) storage. The application is designed to process and store documents in the database as binary large objects (blobs) with an average document size of 6 MB.

The database size has grown over time, reducing the performance and increasing the cost of storage. The company must improve the database performance and needs a solution that is highly available and resilient.

Which solution will meet these requirements MOST cost-effectively?

- A. Reduce the RDS DB instance size. Increase the storage capacity to 24 TiB. Change the storage type to Magnetic.
- B. Increase the RDS DB instance size. Increase the storage capacity to 24 TiB. Change the storage type to Provisioned IOPS.
- C. Create an Amazon S3 bucket. Update the application to store documents in the S3 bucket. Store the object metadata in the existing database.
- D. Create an Amazon DynamoDB table. Update the application to use DynamoDB. Use AWS Database Migration Service (AWS DMS) to migrate data from the Oracle database to DynamoDB.

Correct Answer: C

Explanation

Explanation/Reference:

Storing the blobs in the db is more expensive than S3 with references in the db.

QUESTION 66

A company has an application that runs on Amazon EC2 instances in a private subnet. The application needs to process sensitive information from an Amazon S3 bucket. The application must not use the internet to connect to the S3 bucket.

Which solution will meet these requirements?

- A. Configure an internet gateway. Update the S3 bucket policy to allow access from the internet gateway. Update the application to use the new internet gateway.
- B. Configure a VPN connection. Update the S3 bucket policy to allow access from the VPN connection. Update the application to use the new VPN connection.
- C. Configure a NAT gateway. Update the S3 bucket policy to allow access from the NAT gateway. Update the application to use the new NAT gateway.
- D. Configure a VPC endpoint. Update the S3 bucket policy to allow access from the VPC endpoint. Update the application to use the new VPC endpoint.

Correct Answer: D

Explanation

Explanation/Reference:

A VPC endpoint is a managed endpoint in your VPC that is connected to a public AWS service. It provides a private connection between your VPC and the service, and it does not require an internet gateway or a NAT device.

QUESTION 67

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 function 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).

Correct Answer: B

Explanation

Explanation/Reference:

Enabling secrets encryption in the EKS cluster by using AWS Key Management Service (AWS KMS) is the least operationally overhead way to encrypt the sensitive information in the Kubernetes secrets object. When you enable secrets encryption in the EKS cluster, AWS KMS encrypts the secrets before they are stored in the EKS cluster. You do not need to make any changes to your container application or implement any additional Lambda functions.

QUESTION 68

A solutions architect is designing an application that will allow business users to upload objects to Amazon S3. The solution needs to maximize object durability. Objects also must be readily available at any time and for any length of time. Users will access objects frequently within the first 30 days after the objects are uploaded, but users are much less likely to access objects that are older than 30 days.

Which solution meets these requirements MOST cost-effectively?

- A. Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 Glacier after 30 days.
- B. Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
- C. Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
- D. Store all the objects in S3 Intelligent-Tiering with an S3 Lifecycle rule to transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.

Correct Answer: B

Explanation

QUESTION 69

A company deploys Amazon EC2 instances that run in a VPC. The EC2 instances load source data into Amazon S3 buckets so that the data can be processed in the future. According to compliance laws, the data must not be transmitted over the public internet. Servers in the company's on-premises data center will consume the output from an application that runs on the EC2 instances.

Which solution will meet these requirements?

- A. Deploy an interface VPC endpoint for Amazon EC2. Create an AWS Site-to-Site VPN connection between the company and the VPC.
- B. Deploy a gateway VPC endpoint for Amazon S3. Set up an AWS Direct Connect connection between the on-premises network and the VPC.
- C. Set up an AWS Transit Gateway connection from the VPC to the S3 buckets. Create an AWS Site-to-Site VPN connection between the company and the VPC.
- D. Set up proxy EC2 instances that have routes to NAT gateways. Configure the proxy EC2 instances to fetch S3 data and feed the application instances.

Correct Answer: B

Explanation

Explanation/Reference:

Gateway VPC Endpoint = no internet to access S3. Direct Connect = secure access to VPC.

QUESTION 70

A company is designing a new multi-tier web application that consists of the following components:

1. Web and application servers that run on Amazon EC2 instances as part of Auto Scaling groups
2. An Amazon RDS DB instance for data storage

A solutions architect needs to limit access to the application servers so that only the web servers can access them.

Which solution will meet these requirements?

- A. Deploy AWS PrivateLink in front of the application servers. Configure the network ACL to allow only the web servers to access the application servers.
- B. Deploy a VPC endpoint in front of the application servers. Configure the security group to allow only the web servers to access the application servers.
- C. Deploy a Network Load Balancer with a target group that contains the application servers' Auto Scaling group. Configure the network ACL to allow only the web servers to access the application servers.
- D. Deploy an Application Load Balancer with a target group that contains the application servers' Auto Scaling group. Configure the security group to allow only the web servers to access the application servers.

Correct Answer: D

Explanation

Explanation/Reference:

QUESTION 71

A company wants to use Amazon FSx for Windows File Server for its Amazon EC2 instances that have an SMB file share mounted as a volume in the us-east-1 Region. The company has a recovery point objective (RPO) of 5 minutes for planned system maintenance or unplanned service disruptions. The company needs to replicate the file system to the us-west-2 Region. The replicated data must not be deleted by any user for 5 years.

Which solution will meet these requirements?

- A. Create an FSx for Windows File Server file system in us-east-1 that has a Single-AZ 2 deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in compliance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.
- B. Create an FSx for Windows File Server file system in us-east-1 that has a Multi-AZ deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in governance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.
- C. Create an FSx for Windows File Server file system in us-east-1 that has a Multi-AZ deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in compliance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.
- D. Create an FSx for Windows File Server file system in us-east-1 that has a Single-AZ 2 deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in governance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.

Correct Answer: C

Explanation

QUESTION 72

A company has an application that serves clients that are deployed in more than 20,000 retail storefront locations around the world. The application consists of backend web services that are exposed over HTTPS on port 443. The application is hosted on Amazon EC2 instances behind an Application Load Balancer (ALB). The retail locations communicate with the web application over the public internet. The company allows each retail location to register the IP address that the retail location has been allocated by its local ISP.

The company's security team recommends to increase the security of the application endpoint by restricting access to only the IP addresses registered by the retail locations.

What should a solutions architect do to meet these requirements?

- A. Associate an AWS WAF web ACL with the ALB. Use IP rule sets on the ALB to filter traffic. Update the IP addresses in the rule to include the registered IP addresses.
- B. Deploy AWS Firewall Manager to manage the ALB. Configure firewall rules to restrict traffic to the ALB. Modify the firewall rules to include the registered IP addresses.
- C. Store the IP addresses in an Amazon DynamoDB table. Configure an AWS Lambda authorization function on the ALB to validate that incoming requests are from the registered IP addresses.
- D. Configure the network ACL on the subnet that contains the public interface of the ALB. Update the ingress rules on the network ACL with entries for each of the registered IP addresses.

Correct Answer: A

Explanation

QUESTION 73

A company wants to migrate an on-premises data center to AWS. The data center hosts a storage server that stores data in an NFS-based file system. The storage server holds 200 GB of data. The company needs to migrate the data without interruption to existing services. Multiple resources in AWS must be able to access the data by using the NFS protocol.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

- A. Create an Amazon FSx for Lustre file system.
- B. Create an Amazon Elastic File System (Amazon EFS) file system.
- C. Create an Amazon S3 bucket to receive the data.
- D. Manually use an operating system copy command to push the data into the AWS destination.
- E. Install an AWS DataSync agent in the on-premises data center. Use a DataSync task between the on-premises location and AWS.

Correct Answer: BE

Explanation

Explanation/Reference:

NFS file system = EFS, Use DataSync for the migration with NFS support.

QUESTION 74

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 Macie 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.

Correct Answer: C

Explanation

Explanation/Reference:

Guard duty is a threat detection service for accounts and workloads.

QUESTION 75

A company runs a critical, customer-facing application on Amazon Elastic Kubernetes Service (Amazon EKS). The application has a microservices architecture. The company needs to implement a solution that collects, aggregates, and summarizes metrics and logs from the application in a centralized location.

Which solution meets these requirements?

- A. Run the Amazon CloudWatch agent in the existing EKS cluster. View the metrics and logs in the CloudWatch console.
- B. Run AWS App Mesh in the existing EKS cluster. View the metrics and logs in the App Mesh console.
- C. Configure AWS CloudTrail to capture data events. Query CloudTrail by using Amazon OpenSearch Service.
- D. Configure Amazon CloudWatch Container Insights in the existing EKS cluster. View the metrics and logs in the CloudWatch console.

Correct Answer: D

Explanation

Explanation/Reference:

Amazon CloudWatch Container Insights is a service that collects, aggregates, and summarizes metrics and logs from containerized applications. It is designed to work with Amazon EKS and Kubernetes.

QUESTION 76

A company is planning to deploy a business-critical application in the AWS Cloud. The application requires durable storage with consistent, low-latency performance.

Which type of storage should a solutions architect recommend to meet these requirements?

- A. Instance store volume
- B. Amazon ElastiCache for Memcached cluster
- C. Provisioned IOPS SSD Amazon Elastic Block Store (Amazon EBS) volume
- D. Throughput Optimized HDD Amazon Elastic Block Store (Amazon EBS) volume

Correct Answer: C

Explanation

QUESTION 77

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

Which action meets these requirements?

- A. Create an IAM policy that prohibits changes to CloudTrail. and attach it to the root user.
- B. Create a new trail in CloudTrail from within the developer accounts with the organization trails option enabled.
- C. Create a service control policy (SCP) that prohibits changes to CloudTrail, and attach it the developer

accounts.

- D. Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the management account.

Correct Answer: C

Explanation

QUESTION 78

A company is designing a solution to capture customer activity in different web applications to process analytics and make predictions. Customer activity in the web applications is unpredictable and can increase suddenly. The company requires a solution that integrates with other web applications. The solution must include an authorization step for security purposes.

Which solution will meet these requirements?

- A. Configure a Gateway Load Balancer (GWLB) in front of an Amazon Elastic Container Service (Amazon ECS) container instance that stores the information that the company receives in an Amazon Elastic File System (Amazon EFS) file system. Authorization is resolved at the GWLB.
- B. Configure an Amazon API Gateway endpoint in front of an Amazon Kinesis data stream that stores the information that the company receives in an Amazon S3 bucket. Use an AWS Lambda function to resolve authorization.
- C. Configure an Amazon API Gateway endpoint in front of an Amazon Kinesis Data Firehose that stores the information that the company receives in an Amazon S3 bucket. Use an API Gateway Lambda authorizer to resolve authorization.
- D. Configure a Gateway Load Balancer (GWLB) in front of an Amazon Elastic Container Service (Amazon ECS) container instance that stores the information that the company receives on an Amazon Elastic File System (Amazon EFS) file system. Use an AWS Lambda function to resolve authorization.

Correct Answer: C

Explanation

Explanation/Reference:

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

QUESTION 79

An online photo-sharing company stores its photos in an Amazon S3 bucket that exists in the us-west-1 Region. The company needs to store a copy of all new photos in the us-east-1 Region.

Which solution will meet this requirement with the LEAST operational effort?

- A. Create a second S3 bucket in us-east-1. Use S3 Cross-Region Replication to copy photos from the existing S3 bucket to the second S3 bucket.
- B. Create a cross-origin resource sharing (CORS) configuration of the existing S3 bucket. Specify us-east-1 in the CORS rule's AllowedOrigin element.
- C. Create a second S3 bucket in us-east-1 across multiple Availability Zones. Create an S3 Lifecycle rule to save photos into the second S3 bucket.
- D. Create a second S3 bucket in us-east-1. Configure S3 event notifications on object creation and update events to invoke an AWS Lambda function to copy photos from the existing S3 bucket to the second S3 bucket.

Correct Answer: A

Explanation

Explanation/Reference:

S3 Cross-Region Replication is least operational overhead.

QUESTION 80

A company is creating a new web application for its subscribers. The application will consist of a static single page and a persistent database layer. The application will have millions of users for 4 hours in the morning, but the application will have only a few thousand users during the rest of the day. The company's

data architects have requested the ability to rapidly evolve their schema.

Which solutions will meet these requirements and provide the MOST scalability? (Choose two.)

- A. Deploy Amazon DynamoDB as the database solution. Provision on-demand capacity.
- B. Deploy Amazon Aurora as the database solution. Choose the serverless DB engine mode.
- C. Deploy Amazon DynamoDB as the database solution. Ensure that DynamoDB auto scaling is enabled.
- D. Deploy the static content into an Amazon S3 bucket. Provision an Amazon CloudFront distribution with the S3 bucket as the origin.
- E. Deploy the web servers for static content across a fleet of Amazon EC2 instances in Auto Scaling groups. Configure the instances to periodically refresh the content from an Amazon Elastic File System (Amazon EFS) volume.

Correct Answer: CD

Explanation

Explanation/Reference:

Static content = S3 + CloudFront. Radidly scale and rapidly evolve schema = DynamoDB with auto-scaling enabled (which it is by default).

QUESTION 81

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

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

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

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

Correct Answer: A

Explanation

Explanation/Reference:

For near-real time data ingest and processing, Kinesis and Lambda are most scalable choice.

QUESTION 82

A company uses Amazon API Gateway to manage its REST APIs that third-party service providers access. The company must protect the REST APIs from SQL injection and cross-site scripting attacks.

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

- A. Configure AWS Shield.
- B. Configure AWS WAF.
- C. Set up API Gateway with an Amazon CloudFront distribution. Configure AWS Shield in CloudFront.
- D. Set up API Gateway with an Amazon CloudFront distribution. Configure AWS WAF in CloudFront.

Correct Answer: B

Explanation

Explanation/Reference:

WAF helps with layer 7 attacks like SQL injection and XSS. Shield is helpful for DDOS attacks.

About CertBus.com

As a professional IT exam study guide provider, CertBus.com provides our candidates with the most accurate and high quality IT exam training material.

[Cisco](#)
[EMC](#)
[LPI](#)

[Citrix](#)
[EXIN](#)
[Nortel](#)

[CompTIA](#)
[HP](#)
[Oracle](#)

[Check Point](#)
[Juniper](#)
[VMware](#)

and so on, you can find all kinds of exam questions, study guides, practice tests here. Our aim is to be your assistance on your way to be successful in your IT certifications. We provide our customers with the 100% Pass Guaranteed or Full Refund.



We spare no efforts to help you to pass any IT Certification exams at the first try. Do not hesitate to contact us if you need any help on the products, payments or questions about IT exams.

You can reach us on:

[**https://www.certbus.com/contact-us.html**](https://www.certbus.com/contact-us.html)

We will get in touch with you in 24 hours. Your satisfaction is the recognition for us. You could rely upon us anytime you need help. We are at your service.



 90 Days Free Update Free update is available within 90 days after your purchase. And we are proud to boast a 24/7 efficient Customer Support system via Email.	 Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.	 Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.
--	---	--

Guarantee & Policy | Privacy & Policy | Terms & Conditions

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.

Copyright © CertBus.com, All Rights Reserved.