



# Amazon-Web-Services

## Exam Questions SAA-C03

AWS Certified Solutions Architect - Associate (SAA-C03)

### NEW QUESTION 1

- (Exam Topic 1)

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

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

**Answer:** B

#### Explanation:

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

### NEW QUESTION 2

- (Exam Topic 1)

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

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

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

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

**Answer:** AB

#### Explanation:

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

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

Amazon SQS is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message-oriented middleware, and empowers developers to focus on differentiating work. When new images are uploaded to the S3 bucket, SQS will trigger the Lambda function to process the image and compress it. Once the image is processed, the SQS message is deleted, ensuring that the Lambda function is stateless and durable.

### NEW QUESTION 3

- (Exam Topic 1)

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

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

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

**Answer:** A

#### Explanation:

You might want to use Transfer Acceleration on a bucket for various reasons, including the following: You have customers that upload to a centralized bucket from all over the world.

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

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

<https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html> [https://aws.amazon.com/s3/transfer-acceleration/#:~:text=S3%20Transfer%20Acceleration%20\(S3TA\)%20redu](https://aws.amazon.com/s3/transfer-acceleration/#:~:text=S3%20Transfer%20Acceleration%20(S3TA)%20redu) "Amazon S3 Transfer Acceleration can speed up content transfers to and from Amazon S3 by as much as 50-500% for long-distance transfer of larger objects. Customers who have either web or mobile applications with widespread users or applications hosted far away from their S3 bucket can experience long and variable upload and download speeds over the Internet"

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/mpuoverview.html> "Improved throughput - You can upload parts in parallel to improve throughput."

#### NEW QUESTION 4

- (Exam Topic 1)

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

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 5

- (Exam Topic 1)

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

What should a solutions architect recommend?

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

**Answer:** A

#### NEW QUESTION 6

- (Exam Topic 1)

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

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

- A. Use the EC2 serial console to directly access the terminal interface of each instance for administration.
- B. Attach the appropriate IAM role to each existing instance and new instance
- C. Use AWS Systems Manager Session Manager to establish a remote SSH session.
- D. Create an administrative SSH key pair
- E. Load the public key into each EC2 instance
- F. Deploy a bastion host in a public subnet to provide a tunnel for administration of each instance.
- G. Establish an AWS Site-to-Site VPN connection
- H. Instruct administrators to use their local on-premises machines to connect directly to the instances by using SSH keys across the VPN tunnel.

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 7

- (Exam Topic 1)

A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon EC2 instance in a public subnet of a VPC A solutions architect needs to connect from the on-premises network, through the company's internet connection to the bastion host and to the application servers The solutions architect must make sure that the security groups of all the EC2 instances will allow that access

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

- A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances
- B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company
- C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company
- D. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host
- E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host

**Answer:** CD

#### Explanation:

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

#### NEW QUESTION 8

- (Exam Topic 1)

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

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

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

**Answer: D**

**Explanation:**

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

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

**NEW QUESTION 9**

- (Exam Topic 1)

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

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

- A. Make the encrypted AMI and snapshots publicly available
- B. Modify the CMK's key policy to allow the MSP Partner's AWS account to use the key
- C. Modify the launchPermission property of the AMI
- D. Share the AMI with the MSP Partner's AWS account only
- E. Modify the CMK's key policy to allow the MSP Partner's AWS account to use the key.
- F. Modify the launchPermission property of the AMI Share the AMI with the MSP Partner's AWS account only
- G. Modify the CMK's key policy to trust a new CMK that is owned by the MSP Partner for encryption.
- H. Export the AMI from the source account to an Amazon S3 bucket in the MSP Partner's AWS account. Encrypt the S3 bucket with a CMK that is owned by the MSP Partner Copy and launch the AMI in the MSP Partner's AWS account.

**Answer: B**

**Explanation:**

Share the existing KMS key with the MSP external account because it has already been used to encrypt the AMI snapshot.

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

**NEW QUESTION 10**

- (Exam Topic 1)

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

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

Which solution will meet these requirements?

- A. Take EBS snapshots of the production EBS volume
- B. Restore the snapshots onto EC2 instance store volumes in the test environment.
- C. Configure the production EBS volumes to use the EBS Multi-Attach feature
- D. Take EBS snapshots of the production EBS volume
- E. Attach the production EBS volumes to the EC2 instances in the test environment.
- F. Take EBS snapshots of the production EBS volume
- G. Create and initialize new EBS volume
- H. Attach the new EBS volumes to EC2 instances in the test environment before restoring the volumes from the production EBS snapshots.
- I. Take EBS snapshots of the production EBS volume
- J. Turn on the EBS fast snapshot restore feature on the EBS snapshot
- K. Restore the snapshots into new EBS volume
- L. Attach the new EBS volumes to EC2 instances in the test environment.

**Answer: C**

**NEW QUESTION 10**

- (Exam Topic 1)

A company is storing backup files by using Amazon S3 Standard storage. The files are accessed frequently for 1 month. However, the files are not accessed after 1 month. The company must keep the files indefinitely.

Which storage solution will meet these requirements MOST cost-effectively?

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

**Answer: B**

**NEW QUESTION 12**

- (Exam Topic 1)

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

Which solution will meet these requirements?



- A. Create an S3 bucket Create an IAM role that has permissions to write to the S3 bucket
- B. Use the AWS CLI to copy all files locally to the S3 bucket.
- C. Create an AWS Snowball Edge job
- D. Receive a Snowball Edge device on premise
- E. Use the Snowball Edge client to transfer data to the device
- F. Return the device so that AWS can import the data into Amazon S3.
- G. Deploy an S3 File Gateway on premise
- H. 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
- I. Transfer the data from the existing NFS file share to the S3 File Gateway.
- J. Set up an AWS Direct Connect connection between the on-premises network and AWS
- K. Deploy an S3 File Gateway on premise
- L. Create a public virtual interface (VIF) to connect to the S3 File Gateway
- M. Create an S3 bucket
- N. Create a new NFS file share on the S3 File Gateway
- O. Point the new file share to the S3 bucket
- P. Transfer the data from the existing NFS file share to the S3 File Gateway.

**Answer: B**

#### NEW QUESTION 17

- (Exam Topic 1)

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

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

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

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

**Answer: B**

#### NEW QUESTION 21

- (Exam Topic 1)

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

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

Which solution meets these requirements with the LEAST operational overhead?

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

**Answer: C**

#### Explanation:

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

The SNS topic publishes the event to an SQS queue in the central Region.

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

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

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/subscribe-a-lambda-function-to-event-notifications.html>

#### NEW QUESTION 23

- (Exam Topic 1)

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

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

What should a solutions architect do to meet these requirements?

- A. Enable HTTP health checks on the NLB
- B. supplying the URL of the company's application.

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

**Answer:** C

#### NEW QUESTION 26

- (Exam Topic 1)

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

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

**Answer:** B

#### Explanation:

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

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

There is no interaction with databases.

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

=====

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

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

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

#### NEW QUESTION 30

- (Exam Topic 1)

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

Which solution will meet these requirements?

- A. Share the dashboard from the CloudWatch consol
- B. Enter the product manager's email address, and complete the sharing step
- C. Provide a shareable link for the dashboard to the product manager.
- D. Create an IAM user specifically for the product manage
- E. Attach the CloudWatch Read Only Access managed policy to the use
- F. Share the new login credential with the product manage
- G. Share the browser URL of the correct dashboard with the product manager.
- H. Create an IAM user for the company's employees, Attach the View Only Access AWS managed policy to the IAM use
- I. Share the new login credentials with the product manage
- J. Ask the product manager to navigate to the CloudWatch console and locate the dashboard by name in the Dashboards section.
- K. Deploy a bastion server in a public subne
- L. When the product manager requires access to the dashboard, start the server and share the RDP credential
- M. On the bastion server, ensure that the browser is configured to open the dashboard URL with cached AWS credentials that have appropriate permissions to view the dashboard.

**Answer:** B

#### NEW QUESTION 31

- (Exam Topic 1)

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

Which solution will satisfy these requirements?

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

**Answer:** D

#### NEW QUESTION 35

- (Exam Topic 1)

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

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

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

**Answer: D**

**Explanation:**

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

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

**NEW QUESTION 38**

- (Exam Topic 1)

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

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

- A. Create AWS Secrets Manager secrets for encrypted certificate
- B. Manually update the certificates as neede
- C. Control access to the data by using fine-grained IAM access.
- D. Create an AWS Lambda function that uses the Python cryptography library to receive and perform encryption operation
- E. Store the function in an Amazon S3 bucket.
- F. Create an AWS Key Management Service (AWS KMS) customer managed ke
- G. Allow the EC2 role to use the KMS key for encryption operation
- H. Store the encrypted data on Amazon S3.
- I. Create an AWS Key Management Service (AWS KMS) customer managed ke
- J. Allow the EC2 role to use the KMS key for encryption operation
- K. Store the encrypted data on Amazon Elastic Block Store (Amazon EBS) volumes.

**Answer: D**

**NEW QUESTION 39**

- (Exam Topic 1)

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

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

**Answer: D**

**Explanation:**

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

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

**NEW QUESTION 42**

- (Exam Topic 1)

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

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

Which solution will meet these requirements?

- A. Deploy a Network Load Balancer (NLB) and an associated target grou
- B. Associate the target group with the Auto Scaling grou
- C. Use the NLB as an AWS Global Accelerator endpoint in each Region.
- D. Deploy an Application Load Balancer (ALB) and an associated target grou
- E. Associate the target group with the Auto Scaling grou
- F. Use the ALB as an AWS Global Accelerator endpoint in each Region.
- G. Deploy a Network Load Balancer (NLB) and an associated target grou
- H. Associate the target group with the Auto Scaling grou



- I. Create an Amazon Route 53 latency record that points to aliases for each NL
- J. Create an Amazon CloudFront distribution that uses the latency record as an origin.
- K. Deploy an Application Load Balancer (ALB) and an associated target group
- L. Associate the target group with the Auto Scaling group
- M. Create an Amazon Route 53 weighted record that points to aliases for each AL
- N. Deploy an Amazon CloudFront distribution that uses the weighted record as an origin.

**Answer:** D

**Explanation:**

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

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

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

**NEW QUESTION 45**

- (Exam Topic 1)

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

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

Which solution will meet these requirements?

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

**Answer:** D

**Explanation:**

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

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

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

**NEW QUESTION 46**

- (Exam Topic 1)

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

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

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

**Answer:** AC

**Explanation:**

"Security groups create an outbound rule for every inbound rule." Not completely right. Stateful 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](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#SecurityGroupRules)

**NEW QUESTION 50**

- (Exam Topic 1)

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

What should the solutions architect recommend?

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

**Answer:** C

**Explanation:**

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

You can now create a CloudFront distribution using a custom origin. Each distribution will can point to an S3 or to a custom origin. This could be another storage



service, or it could be something more interesting and more dynamic, such as an EC2 instance or even an Elastic Load Balancer

#### NEW QUESTION 51

- (Exam Topic 1)

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

- A. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console
- B. 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.
- C. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console
- D. 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.
- E. Use AWS Directory Service
- F. Create a two-way trust relationship with the company's self-managed Microsoft Active Directory.
- G. Deploy an identity provider (IdP) on premise
- H. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.

**Answer:** A

#### NEW QUESTION 53

- (Exam Topic 1)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 54

- (Exam Topic 1)

A company needs the ability to analyze the log files of its proprietary application. The logs are stored in JSON format in an Amazon S3 bucket. Queries will be simple and will run on-demand. A solutions architect needs to perform the analysis with minimal changes to the existing architecture. What should the solutions architect do to meet these requirements with the LEAST amount of operational overhead?

- A. Use Amazon Redshift to load all the content into one place and run the SQL queries as needed
- B. Use Amazon CloudWatch Logs to store the logs. Run SQL queries as needed from the Amazon CloudWatch console
- C. Use Amazon Athena directly with Amazon S3 to run the queries as needed
- D. Use AWS Glue to catalog the logs. Use a transient Apache Spark cluster on Amazon EMR to run the SQL queries as needed

**Answer:** C

#### Explanation:

Amazon Athena can be used to query JSON in S3

#### NEW QUESTION 55

- (Exam Topic 1)

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

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

What is the effect of this policy?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 57**

- (Exam Topic 1)

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

Which solution meets these requirements MOST cost-effectively?

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

**Answer:** A

**NEW QUESTION 60**

- (Exam Topic 1)

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

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

- A. Create an Auto Scaling group so that EC2 instances can scale out
- B. Configure an S3 event notification to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.
- C. Create an Amazon AppFlow flow to transfer data between each SaaS source and the S3 bucket. 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.
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for each SaaS source to send output data
- E. Configure the S3 bucket as the rule's target
- F. Create a second EventBridge (CloudWatch Events) rule to send events when the upload to the S3 bucket is complete

- G. Configure an Amazon Simple Notification Service (Amazon SNS) topic as the second rule's target.
- H. Create a Docker container to use instead of an EC2 instance
- I. Host the containerized application on Amazon Elastic Container Service (Amazon ECS). Configure Amazon CloudWatch Container Insights to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.

**Answer: B**

**Explanation:**

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

**NEW QUESTION 63**

- (Exam Topic 1)

A company needs to configure a real-time data ingestion architecture for its application. The company needs an API, a process that transforms data as the data is streamed, and a storage solution for the data.

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

- A. Deploy an Amazon EC2 instance to host an API that sends data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source
- B. Use AWS Lambda functions to transform the data
- C. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
- D. Deploy an Amazon EC2 instance to host an API that sends data to AWS Glue
- E. Stop source/destination checking on the EC2 instance
- F. Use AWS Glue to transform the data and to send the data to Amazon S3.
- G. Configure an Amazon API Gateway API to send data to an Amazon Kinesis data stream
- H. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source
- I. Use AWS Lambda functions to transform the data
- J. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
- K. Configure an Amazon API Gateway API to send data to AWS Glue
- L. Use AWS Lambda functions to transform the data
- M. Use AWS Glue to send the data to Amazon S3.

**Answer: C**

**NEW QUESTION 66**

- (Exam Topic 1)

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

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

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

- A. Use AWS DataSync to move the data. Create a custom transformation job by using AWS Glue.
- B. Order an AWS Snowcone device to move the data. Deploy the transformation application to the device.
- C. Order an AWS Snowball Edge Storage Optimized device.
- D. Copy the data to the device.
- E. Create a custom transformation job by using AWS Glue.
- F. Order an AWS 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.
- G. Snowball Edge Storage Optimized device that includes Amazon EC2 compute. Copy the data to the device. Create a new EC2 instance on AWS to run the transformation application.

**Answer: C**

**NEW QUESTION 69**

- (Exam Topic 1)

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

Which solution meets these requirements?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 73**

- (Exam Topic 1)

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

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

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

- A. Set up long polling in the SQS queue by increasing the ReceiveMessage wait time to 30 seconds.
- B. Change the SQS standard queue to an SQS FIFO queue
- C. Use the message deduplication ID to discard duplicate messages.
- D. 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.
- E. Modify the Lambda function to delete each message from the SQS queue immediately after the message is read before processing.

**Answer:** C

#### NEW QUESTION 75

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 78

- (Exam Topic 1)

A solutions architect must design a highly available infrastructure for a website. The website is powered by Windows web servers that run on Amazon EC2 instances. The solutions architect must implement a solution that can mitigate a large-scale DDoS attack that originates from thousands of IP addresses. Downtime is not acceptable for the website.

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

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

**Answer:** AC

#### Explanation:

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

#### NEW QUESTION 80

- (Exam Topic 1)

A company has more than 5 TB of file data on Windows file servers that run on premises. Users and applications interact with the data each day. The company is moving its Windows workloads to AWS. As the company continues this process, the company requires access to AWS and on-premises file storage with minimum latency. The company needs a solution that minimizes operational overhead and requires no significant changes to the existing file access patterns. The company uses an AWS Site-to-Site VPN connection for connectivity to AWS. What should a solutions architect do to meet these requirements?

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

**Answer:** D

#### NEW QUESTION 82

- (Exam Topic 1)

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

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

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



- C. Use Amazon CloudWatch metrics to analyze the application performance history to determine the server's peak utilization during the performance failure
- D. Increase the size of the application server's Amazon EC2 instances to meet the peak requirements.
- E. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group
- F. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.
- G. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group
- H. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

**Answer:** A

**Explanation:**

<https://aws.amazon.com/getting-started/hands-on/build-serverless-web-app-lambda-apigateway-s3-dynamodb-c/> 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

**NEW QUESTION 83**

- (Exam Topic 1)

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

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

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

- A. Edit the job to use job bookmarks.
- B. Edit the job to delete data after the data is processed
- C. Edit the job by setting the NumberOfWorkers field to 1.
- D. Use a FindMatches machine learning (ML) transform.

**Answer:** C

**Explanation:**

This is the purpose of bookmarks: "AWS Glue tracks data that has already been processed during a previous run of an ETL job by persisting state information from the job run. This persisted state information is called a job bookmark. Job bookmarks help AWS Glue maintain state information and prevent the reprocessing of old data." <https://docs.aws.amazon.com/glue/latest/dg/monitor-continuations.html>

**NEW QUESTION 87**

- (Exam Topic 1)

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

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 92**

- (Exam Topic 1)

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

How can the solutions architect meet this requirement?

- A. Deploy Amazon API Gateway into a public subnet and adjust the route table to route S3 calls through it.
- B. Deploy a NAT gateway into a public subnet and attach an 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.

**Answer:** D

**NEW QUESTION 95**

- (Exam Topic 1)

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

What should a solutions architect do to meet these requirements?

- A. Create an Amazon CloudFront distribution that has the S3 bucket and the ALB as origins. Configure Route 53 to route traffic to the CloudFront distribution.
- B. Create an Amazon CloudFront distribution that has the ALB as an origin. Create an AWS Global Accelerator standard accelerator that has the S3 bucket as an endpoint.
- C. Configure Route 53 to route traffic to the CloudFront distribution.
- D. 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.
- E. Create an Amazon CloudFront distribution that has the ALB as an origin.
- F. Create an AWS Global Accelerator standard accelerator that has the S3 bucket as an endpoint. Create two domain names.

G. Point one domain name to the CloudFront DNS name for dynamic content, Point the other domain name to the accelerator DNS name for static content Use the domain names as endpoints for the web application.

**Answer:** C

**Explanation:**

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

<https://aws.amazon.com/blogs/networking-and-content-delivery/improving-availability-and-performance-for-ap>

**NEW QUESTION 99**

- (Exam Topic 1)

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

What should a solutions architect do to meet this requirement?

- A. Update the ALB's network ACL to accept only HTTPS traffic
- B. Create a rule that replaces the HTTP in the URL with HTTPS.
- C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.
- D. Replace the ALB with a Network Load Balancer configured to use Server Name Indication (SNI).

**Answer:** C

**Explanation:**

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

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

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

**NEW QUESTION 100**

- (Exam Topic 1)

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

What should a solutions architect do to meet these requirements?

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

**Answer:** A

**NEW QUESTION 104**

- (Exam Topic 1)

A company has an application that generates a large number of files, each approximately 5 MB in size. The files are stored in Amazon S3. Company policy requires the files to be stored for 4 years before they can be

deleted Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce. The files are frequently accessed in the first 30 days of the object creation but are rarely accessed after the first 30 days

Which storage solution is MOST cost-effective?

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

**Answer:** B

**Explanation:**

[https://aws.amazon.com/s3/storage-classes/?trk=66264cd8-3b73-416c-9693-ea7cf4fe846a&sc\\_channel=ps&s\\_k](https://aws.amazon.com/s3/storage-classes/?trk=66264cd8-3b73-416c-9693-ea7cf4fe846a&sc_channel=ps&s_k)

**NEW QUESTION 106**

- (Exam Topic 1)

An application runs on an Amazon EC2 instance in a VPC. The application processes logs that are stored in an Amazon S3 bucket. The EC2 instance needs to access the S3 bucket without connectivity to the internet.

Which solution will provide private network connectivity to Amazon S3?

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 111

- (Exam Topic 1)

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

What should a solutions architect do to meet these requirements?

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

**Answer:** D

#### NEW QUESTION 112

- (Exam Topic 1)

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

Which solution addresses this performance issue?

- A. Change the storage type to Provisioned IOPS SSD
- B. Change the DB instance to a memory optimized instance class
- C. Change the DB instance to a burstable performance instance class
- D. Enable Multi-AZ RDS read replicas with MySQL native asynchronous replication.

**Answer:** A

#### Explanation:

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

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

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

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Storage.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html)

#### NEW QUESTION 115

- (Exam Topic 1)

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

The company wants a highly available solution. However, the company needs to minimize costs and does not want to manage additional infrastructure. 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

**Answer:** A

#### Explanation:

<https://aws.amazon.com/kinesis/data-firehose/features/?nc=sn&loc=2#:~:text=into%20Amazon%20S3%2C%20>

#### NEW QUESTION 116

- (Exam Topic 1)

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

**Answer:** AB

#### NEW QUESTION 118

- (Exam Topic 2)

A company runs a global web application on Amazon EC2 instances behind an Application Load Balancer. The application stores data in Amazon Aurora. The company needs to create a disaster recovery solution and can tolerate up to 30 minutes of downtime and potential data loss. The solution does not need to handle the load when the primary infrastructure is healthy.

What should a solutions architect do to meet these requirements?

- A. Deploy the application with the required infrastructure elements in place. Use Amazon Route 53 to configure active-passive failover. Create an Aurora Replica in a second AWS Region.
- B. Host a scaled-down deployment of the application in a second AWS Region. Use Amazon Route 53 to configure active-active failover. Create an Aurora Replica in the second Region.
- C. Replicate the primary infrastructure in a second AWS Region. Use Amazon Route 53 to configure active-active failover. Create an Aurora database that is restored from the latest snapshot.
- D. Back up data with AWS Backup. Use the backup to create the required infrastructure in a second AWS Region. Use Amazon Route 53 to configure active-passive failover. Create an Aurora second primary instance in the second Region.

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 122

- (Exam Topic 2)

A company stores its application logs in an Amazon CloudWatch Logs log group. A new policy requires the company to store all application logs in Amazon OpenSearch Service (Amazon Elasticsearch Service) in near-real time.

Which solution will meet this requirement with the LEAST operational overhead?

- A. Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).
- B. Create an AWS Lambda function.
- C. Use the log group to invoke the function to write the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).
- D. Create an Amazon Kinesis Data Firehose delivery stream.
- E. Configure the log group as the delivery stream's source.
- F. Configure Amazon OpenSearch Service (Amazon Elasticsearch Service) as the delivery stream's destination.
- G. Install and configure Amazon Kinesis Agent on each application server to deliver the logs to Amazon Kinesis Data Stream.
- H. Configure Kinesis Data Streams to deliver the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).

**Answer:** B

#### Explanation:

<https://computingforgeeks.com/stream-logs-in-aws-from-cloudwatch-to-elasticsearch/>

#### NEW QUESTION 127

- (Exam Topic 2)

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

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

Which solution meets these requirements MOST cost-effectively?

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

**Answer:** B

#### NEW QUESTION 129

- (Exam Topic 2)

A company needs to move data from an Amazon EC2 instance to an Amazon S3 bucket. The company must ensure that no API calls and no data are routed through public internet routes. Only the EC2 instance can have access to upload data to the S3 bucket.

Which solution will meet these requirements?

- A. Create an interface VPC endpoint for Amazon S3 in the subnet where the EC2 instance is located. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
- B. Create a gateway VPC endpoint for Amazon S3 in the Availability Zone where the EC2 instance is located.
- C. Attach appropriate security groups to the endpoint.
- D. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
- E. Run the nslookup tool from inside the EC2 instance to obtain the private IP address of the S3 bucket's service API endpoint.
- F. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket.
- G. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
- H. Use the AWS-provided, publicly available ip-ranges.json file to obtain the private IP address of the S3 bucket's service API endpoint.



- I. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket
- J. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.

**Answer:** A

**Explanation:**

(<https://aws.amazon.com/blogs/security/how-to-restrict-amazon-s3-bucket-access-to-a-specific-iam-role/>)

**NEW QUESTION 134**

- (Exam Topic 2)

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

The company wants to make all the data available to various teams so that the teams can perform analytics.

The solution must provide the ability to manage fine-grained permissions for the data and must minimize operational overhead.

Which solution will meet these requirements?

- A. Migrate the purchase data to write directly to Amazon RD
- B. Use RDS access controls to limit access.
- C. Schedule an AWS Lambda function to periodically copy data from Amazon RDS to Amazon S3. Create an AWS Glue crawle
- D. Use Amazon Athena to query the dat
- E. Use S3 policies to limit access.
- F. Create a data lake by using AWS Lake Formatio
- G. Create an AWS Glue JDBC connection to Amazon RD
- H. Register (he S3 bucket in Lake Formatio
- I. Use Lake Formation access controls to limit access.
- J. Create an Amazon Redshift cluste
- K. Schedule an AWS Lambda function to periodically copy data from Amazon S3 and Amazon RDS to Amazon Redshif
- L. Use Amazon Redshift access controls to limit access.

**Answer:** D

**NEW QUESTION 138**

- (Exam Topic 2)

A company is migrating its on-premises PostgreSQL database to Amazon Aurora PostgreSQL. The

on-premises database must remain online and accessible during the migration. The Aurora database must remain synchronized with the on-premises database.

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

- A. Create an ongoing replication task.
- B. Create a database backup of the on-premises database
- C. Create an AWS Database Migration Service (AWS DMS) replication server
- D. Convert the database schema by using the AWS Schema Conversion Tool (AWS SCT).
- E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to monitor the database synchronization

**Answer:** CD

**NEW QUESTION 142**

- (Exam Topic 2)

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

What should a solutions architect do to meet these requirements?

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

**Answer:** B

**NEW QUESTION 145**

- (Exam Topic 2)

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

Which solution will meet these requirements?

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

**Answer:** D

**NEW QUESTION 147**

- (Exam Topic 2)

A company is migrating an application from on-premises servers to Amazon EC2 instances. As part of the migration design requirements, a solutions architect

must implement infrastructure metric alarms. The company does not need to take action if CPU utilization increases to more than 50% for a short burst of time. However, if the CPU utilization increases to more than 50% and read IOPS on the disk are high at the same time, the company needs to act as soon as possible. The solutions architect also must reduce false alarms. What should the solutions architect do to meet these requirements?

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

**Answer:** A

#### NEW QUESTION 149

- (Exam Topic 2)

A company wants to run applications in containers in the AWS Cloud. These applications are stateless and can tolerate disruptions within the underlying infrastructure. The company needs a solution that minimizes cost and operational overhead. What should a solutions architect do to meet these requirements?

- A. Use Spot Instances in an Amazon EC2 Auto Scaling group to run the application containers.
- B. Use Spot Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.
- C. Use On-Demand Instances in an Amazon EC2 Auto Scaling group to run the application containers.
- D. Use On-Demand Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.

**Answer:** A

#### Explanation:

<https://aws.amazon.com/cn/blogs/compute/cost-optimization-and-resilience-eks-with-spot-instances/>

#### NEW QUESTION 153

- (Exam Topic 2)

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

- A. Create a VPC peering connection between the company's VPC and the provider's VPC.
- B. Update the route table to connect to the target service.
- C. Ask the provider to create a virtual private gateway in its VPC.
- D. Use AWS PrivateLink to connect to the target service.
- E. Create a NAT gateway in a public subnet of the company's VPC.
- F. Update the route table to connect to the target service.
- G. Ask the provider to create a VPC endpoint for the target service.
- H. Use AWS PrivateLink to connect to the target service.

**Answer:** D

#### NEW QUESTION 156

- (Exam Topic 2)

A solutions architect is designing a customer-facing application for a company. The application's database will have a clearly defined access pattern throughout the year and will have a variable number of reads and writes that depend on the time of year. The company must retain audit records for the database for 7 days. The recovery point objective (RPO) must be less than 5 hours. Which solution meets these requirements?

- A. Use Amazon DynamoDB with auto scaling. Use on-demand backups and Amazon DynamoDB Streams.
- B. Use Amazon Redshift.
- C. Configure concurrency scaling.
- D. Activate audit logging.
- E. Perform database snapshots every 4 hours.
- F. Use Amazon RDS with Provisioned IOPS. Activate the database auditing parameter. Perform database snapshots every 5 hours.
- G. Use Amazon Aurora MySQL with auto scaling.
- H. Activate the database auditing parameter.

**Answer:** B

#### NEW QUESTION 160

- (Exam Topic 2)

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

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

**Answer:** B

**Explanation:**

Q: What does Amazon RDS manage on my behalf?

Amazon RDS manages the work involved in setting up a relational database: from provisioning the infrastructure capacity you request to installing the database software. Once your database is up and running, Amazon RDS automates common administrative tasks such as performing backups and patching the software that powers your database. With optional Multi-AZ deployments, Amazon RDS also manages synchronous data replication across Availability Zones with automatic failover.

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

**NEW QUESTION 163**

- (Exam Topic 2)

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

What should the solutions architect recommend?

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

**Answer:** A

**NEW QUESTION 165**

- (Exam Topic 2)

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

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

- A. Move the data to the S3 bucket
- B. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use the built-in key rotation behavior of SSE-S3 encryption keys.
- C. Create an AWS Key Management Service (AWS KMS) customer managed key
- D. Enable automatic key rotation
- E. Set the S3 bucket's default encryption behavior to use the customer managed KMS key
- F. Move the data to the S3 bucket.
- G. Create an AWS Key Management Service (AWS KMS) customer managed key
- H. Set the S3 bucket's default encryption behavior to use the customer managed KMS key
- I. Move the data to the S3 bucket
- J. Manually rotate the KMS key every year.
- K. Encrypt the data with customer key material before moving the data to the S3 bucket
- L. Create an AWS Key Management Service (AWS KMS) key without key material
- M. Import the customer key material into the KMS key
- N. Enable automatic key rotation.

**Answer:** C

**NEW QUESTION 166**

- (Exam Topic 2)

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

Which action should the solutions architect take?

- A. Configure a CloudFront signed URL.
- B. Configure a CloudFront signed cookie.
- C. Configure a CloudFront field-level encryption profile.
- D. Configure CloudFront and set the Origin Protocol Policy setting to HTTPS Only for the Viewer Protocol Policy.

**Answer:** C

**Explanation:**

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

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

**NEW QUESTION 170**

- (Exam Topic 2)

A company runs a web-based portal that provides users with global breaking news, local alerts, and weather updates. The portal delivers each user a personalized view by using a mixture of static and dynamic content. Content is served over HTTPS through an API server running on an Amazon EC2 instance behind an Application Load Balancer (ALB). The company wants the portal to provide this content to its users across the world as quickly as possible.

How should a solutions architect design the application to ensure the LEAST amount of latency for all users?

- A. Deploy the application stack in a single AWS Region
- B. Use Amazon CloudFront to serve all static and dynamic content by specifying the ALB as an origin.
- C. Deploy the application stack in two AWS Regions
- D. Use an Amazon Route 53 latency routing policy to serve all content from the ALB in the closest Region.
- E. Deploy the application stack in a single AWS Region
- F. Use Amazon CloudFront to serve the static content
- G. Serve the dynamic content directly from the ALB.
- H. Deploy the application stack in two AWS Regions

I. Use an Amazon Route 53 geolocation routing policy to serve all content from the ALB in the closest Region.

**Answer:** A

**Explanation:**

<https://aws.amazon.com/blogs/networking-and-content-delivery/deliver-your-apps-dynamic-content-using-amaz>

#### NEW QUESTION 172

- (Exam Topic 2)

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

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

**Answer:** B

**Explanation:**

<https://aws.amazon.com/kms/faqs/#:~:text=If%20you%20are%20a%20developer%20who%20needs%20to%20d>

#### NEW QUESTION 173

- (Exam Topic 2)

A company has two applications: a sender application that sends messages with payloads to be processed and a processing application intended to receive the messages with payloads. The company wants to implement an AWS service to handle messages between the two applications. The sender application can send about 1.000 messages each hour. The messages may take up to 2 days to be processed. If the messages fail to process, they must be retained so that they do not impact the processing of any remaining messages.

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

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

**Answer:** C

**Explanation:**

<https://aws.amazon.com/blogs/compute/building-loosely-coupled-scalable-c-applications-with-amazon-sqs-and-https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.htm>

#### NEW QUESTION 174

- (Exam Topic 2)

A solutions architect needs to implement a solution to reduce a company's storage costs. All the company's data is in the Amazon S3 Standard storage class. The company must keep all data for at least 25 years. Data from the most recent 2 years must be highly available and immediately retrievable.

Which solution will meet these requirements?

- A. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive immediately.
- B. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 2 years.
- C. Use S3 Intelligent-Tierin
- D. Activate the archiving option to ensure that data is archived in S3 Glacier Deep Archive.
- E. Set up an S3 Lifecycle policy to transition objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately and to S3 Glacier Deep Archive after 2 years.

**Answer:** B

#### NEW QUESTION 177

- (Exam Topic 2)

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

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

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

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

**Answer:** AC



#### NEW QUESTION 180

- (Exam Topic 2)

A company has a legacy data processing application that runs on Amazon EC2 instances. Data is processed sequentially, but the order of results does not matter. The application uses a monolithic architecture. The only way that the company can scale the application to meet increased demand is to increase the size of the instances.

The company's developers have decided to rewrite the application to use a microservices architecture on Amazon Elastic Container Service (Amazon ECS). What should a solutions architect recommend for communication between the microservices?

- A. Create an Amazon Simple Queue Service (Amazon SQS) queue
- B. Add code to the data producers, and send data to the queue
- C. Add code to the data consumers to process data from the queue.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic
- E. Add code to the data producers, and publish notifications to the topic
- F. Add code to the data consumers to subscribe to the topic.
- G. Create an AWS Lambda function to pass message
- H. Add code to the data producers to call the Lambda function with a data object
- I. Add code to the data consumers to receive a data object that is passed from the Lambda function.
- J. Create an Amazon DynamoDB table
- K. Enable DynamoDB Stream
- L. Add code to the data producers to insert data into the table
- M. Add code to the data consumers to use the DynamoDB Streams API to detect new table entries and retrieve the data.

**Answer:** A

#### Explanation:

Queue has Limited throughput (300 msg/s without batching, 3000 msg/s with batching whereby up-to 10 msg per batch operation; Msg duplicates not allowed in the queue (exactly-once delivery); Msg order is preserved (FIFO); Queue name must end with .fifo

#### NEW QUESTION 181

- (Exam Topic 2)

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

What should a solutions architect do to meet these requirements?

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

**Answer:** D

#### Explanation:

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

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

#### NEW QUESTION 186

- (Exam Topic 2)

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

Which solution meets these requirements MOST cost-effectively?

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

**Answer:** C

#### NEW QUESTION 189

- (Exam Topic 2)

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 194

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 197

- (Exam Topic 2)

A medical records company is hosting an application on Amazon EC2 instances. The application processes customer data files that are stored on Amazon S3. The EC2 instances are hosted in public subnets. The EC2 instances access Amazon S3 over the internet, but they do not require any other network access. A new requirement mandates that the network traffic for file transfers take a private route and not be sent over the internet. Which change to the network architecture should a solutions architect recommend to meet this requirement?

- A. Create a NAT gateway
- B. Configure the route table for the public subnets to send traffic to Amazon S3 through the NAT gateway.
- C. Configure the security group for the EC2 instances to restrict outbound traffic so that only traffic to the S3 prefix list is permitted.
- D. Move the EC2 instances to private subnet
- E. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets
- F. Remove the internet gateway from the VPC
- G. Set up an AWS Direct Connect connection, and route traffic to Amazon S3 over the Direct Connect connection.

**Answer:** C

#### NEW QUESTION 201

- (Exam Topic 2)

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

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

**Answer:** A

#### Explanation:

You can use CloudFront to deliver video on demand (VOD) or live streaming video using any HTTP origin. One way you can set up video workflows in the cloud is by using CloudFront together with AWS Media Services.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streaming-video.html>

#### NEW QUESTION 204

- (Exam Topic 2)

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

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

**Answer:** A

#### Explanation:

Cloudfront for rapid response and s3 to minimize infrastructure.

#### NEW QUESTION 206

- (Exam Topic 2)

A company wants to migrate its existing on-premises monolithic application to AWS.

The company wants to keep as much of the front-end code and the backend code as possible. However, the company wants to break the application into smaller applications. A different team will manage each application. The company needs a highly scalable solution that minimizes operational overhead.

Which solution will meet these requirements?

- A. Host the application on AWS Lambda. Integrate the application with Amazon API Gateway.
- B. Host the application with AWS Amplify
- C. Connect the application to an Amazon API Gateway API that is integrated with AWS Lambda.
- D. Host the application on Amazon EC2 instance
- E. Set up an Application Load Balancer with EC2 instances in an Auto Scaling group as targets.
- F. Host the application on Amazon Elastic Container Service (Amazon ECS). Set up an Application Load Balancer with Amazon ECS as the target.

**Answer:** D

**Explanation:**

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

**NEW QUESTION 210**

- (Exam Topic 2)

A company has implemented a self-managed DNS solution on three Amazon EC2 instances behind a Network Load Balancer (NLB) in the us-west-2 Region. Most of the company's users are located in the United States and Europe. The company wants to improve the performance and availability of the solution. The company launches and configures three EC2 instances in the eu-west-1 Region and adds the EC2 instances as targets for a new NLB.

Which solution can the company use to route traffic to all the EC2 instances?

- A. Create an Amazon Route 53 geolocation routing policy to route requests to one of the two NLB
- B. Create an Amazon CloudFront distributio
- C. Use the Route 53 record as the distribution's origin.
- D. Create a standard accelerator in AWS Global Accelerato
- E. Create endpoint groups in us-west-2 and eu-west-1. Add the two NLBs as endpoints for the endpoint groups.
- F. Attach Elastic IP addresses to the six EC2 instance
- G. Create an Amazon Route 53 geolocation routing policy to route requests to one of the six EC2 instance
- H. Create an Amazon CloudFront distributio
- I. Use the Route 53 record as the distribution's origin.
- J. 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 ALB
- K. Create an Amazon CloudFront distributio
- L. Use the Route 53 record as the distribution's origin.

**Answer:** B

**Explanation:**

For standard accelerators, Global Accelerator uses the AWS global network to route traffic to the optimal regional endpoint based on health, client location, and policies that you configure, which increases the availability of your applications. Endpoints for standard accelerators can be Network Load Balancers, Application Load Balancers, Amazon EC2 instances, or Elastic IP addresses that are located in one AWS Region or multiple Regions.

<https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html>

**NEW QUESTION 214**

- (Exam Topic 2)

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

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

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

**Answer:** D

**NEW QUESTION 215**

- (Exam Topic 2)

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

What should a solutions architect do to accomplish this?

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

**Answer:** D

**Explanation:**

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

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scp.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html).

**NEW QUESTION 216**

- (Exam Topic 2)

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

Which solution meets these requirements MOST cost-effectively?

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

D. Use Reserved Instances for the baseline capacity and use On-Demand Instances to handle additional capacity.

**Answer:** D

**Explanation:**

We recommend that you use On-Demand Instances for applications with short-term, irregular workloads that cannot be interrupted.  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-on-demand-instances.html>

**NEW QUESTION 219**

- (Exam Topic 2)

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

Which configuration will meet this requirement?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 221**

- (Exam Topic 2)

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

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 222**

- (Exam Topic 2)

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

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

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

- A. Create a Lambda function to copy the files to the analysis S3 bucket
- B. Create an S3 event notification for the analysis S3 bucket
- C. Configure Lambda and SageMaker Pipelines as destinations of the event notification
- D. Configure s3objectCreated:Put as the event type.
- E. Create a Lambda function to copy the files to the analysis S3 bucket
- F. 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.
- G. Configure S3 replication between the S3 bucket
- H. Create an S3 event notification for the analysis S3 bucket
- I. Configure Lambda and SageMaker Pipelines as destinations of the event notification
- J. Configure s3objectCreated:Put as the event type.
- K. Configure S3 replication between the S3 bucket
- L. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge (Amazon CloudWatch Events). Configure an ObjectCreated rule in EventBridge (CloudWatch Events). Configure Lambda and SageMaker Pipelines as targets for the rule.

**Answer:** A

**NEW QUESTION 227**

- (Exam Topic 2)

A company wants to move its application to a serverless solution. The serverless solution needs to analyze existing and new data by using SL. The company stores the data in an Amazon S3 bucket. The data requires encryption and must be replicated to a different AWS Region.



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

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

**Answer:** A

#### NEW QUESTION 229

- (Exam Topic 2)

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

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

**Answer:** A

#### Explanation:

The details are revealed in below url: <https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html>

FIFO (First-In-First-Out) queues are designed to enhance messaging between applications when the order of operations and events is critical, or where duplicates can't be tolerated. Examples of situations where you might use FIFO queues include the following: To make sure that user-entered commands are run in the right order. To display the correct product price by sending price modifications in the right order. To prevent a student from enrolling in a course before registering for an account.

#### NEW QUESTION 231

- (Exam Topic 2)

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

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

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

**Answer:** A

#### Explanation:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-placementgroup.html> "A cluster placement group is a logical grouping of instances within a single Availability Zone that benefit from low network latency, high network throughput"

#### NEW QUESTION 232

- (Exam Topic 2)

A gaming company is designing a highly available architecture. The application runs on a modified Linux kernel and supports only UDP-based traffic. The company needs the front-end tier to provide the best possible user experience. That tier must have low latency, route traffic to the nearest edge location, and provide static IP addresses for entry into the application endpoints.

What should a solutions architect do to meet these requirements?

- A. Configure Amazon Route 53 to forward requests to an Application Load Balance
- B. Use AWS Lambda for the application in AWS Application Auto Scaling.
- C. Configure Amazon CloudFront to forward requests to a Network Load Balance
- D. Use AWS Lambda for the application in an AWS Application Auto Scaling group.
- E. Configure AWS Global Accelerator to forward requests to a Network Load Balance
- F. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.
- G. Configure Amazon API Gateway to forward requests to an Application Load Balance
- H. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.

**Answer:** C

#### NEW QUESTION 237

- (Exam Topic 2)

A company has an ecommerce checkout workflow that writes an order to a database and calls a service to process the payment. Users are experiencing timeouts during the checkout process. When users resubmit the checkout form, multiple unique orders are created for the same desired transaction. How should a solutions architect refactor this workflow to prevent the creation of multiple orders?

- A. Configure the web application to send an order message to Amazon Kinesis Data Firehose
- B. Set the payment service to retrieve the message from Kinesis Data Firehose and process the order.
- C. 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.
- D. Store the order in the database
- E. Send a message that includes the order number to Amazon Simple Notification Service (Amazon SNS). Set the payment service to poll Amazon SNS
- F. retrieve the message, and process the order.
- G. Store the order in the database
- H. Send a message that includes the order number to an Amazon Simple Queue Service (Amazon SQS) FIFO queue
- I. Set the payment service to retrieve the message and process the order
- J. Delete the message from the queue.

**Answer:** D

**Explanation:**

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

**NEW QUESTION 240**

- (Exam Topic 2)

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

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

**Answer:** B

**Explanation:**

<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>

**NEW QUESTION 241**

- (Exam Topic 2)

A corporation has recruited a new cloud engineer who should not have access to the CompanyConfidential Amazon S3 bucket. The cloud engineer must have read and write permissions on an S3 bucket named AdminTools. Which IAM policy will satisfy these criteria?

- A. Text, letter Description automatically generated

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

- B. Text Description automatically generated

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

C. Text, application Description automatically generated

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

D. Text, application Description automatically generated

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

**Answer: A**

**Explanation:**

[https://docs.amazonaws.cn/en\\_us/IAM/latest/UserGuide/reference\\_policies\\_examples\\_s3\\_rw-bucket.html](https://docs.amazonaws.cn/en_us/IAM/latest/UserGuide/reference_policies_examples_s3_rw-bucket.html)

## NEW QUESTION 245

- (Exam Topic 2)

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

Which solution meets the availability requirement MOST cost-effectively?

- A. Use all EC2 Spot Instance
- B. Stop the RDS database when it is not in use.
- C. Purchase EC2 Instance Savings Plans to cover five EC2 instance

- D. Purchase an RDS Reserved DB Instance
- E. Purchase two EC2 Reserved Instances Use up to three additional EC2 Spot Instances as needed
- F. Stop the RDS database when it is not in use.
- G. Purchase EC2 Instance Savings Plans to cover two EC2 instances
- H. Use up to three additional EC2 On-Demand Instances as needed
- I. Purchase an RDS Reserved DB Instance.

**Answer:** D

#### NEW QUESTION 247

.....



## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### SAA-C03 Practice Exam Features:

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

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