

AWS (SAA-C02): Practice Test 1

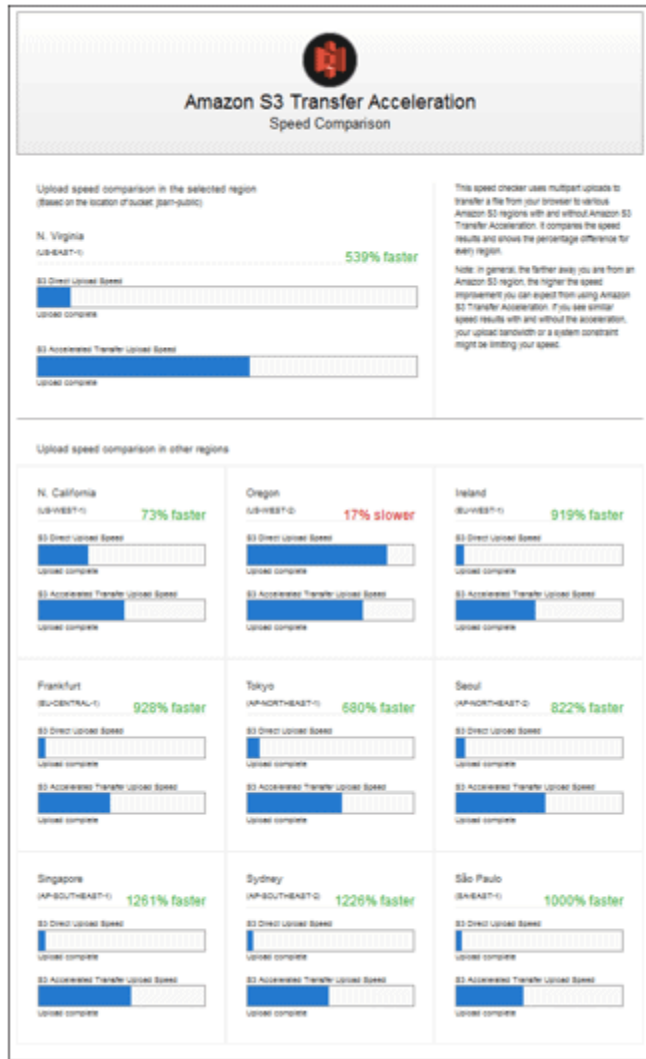
Question 1. A company collects atmospheric data such as temperature, air pressure, and humidity from different countries. Each site location is equipped with various weather instruments and a high-speed Internet connection. The average collected data in each location is around 500 GB and will be analyzed by a weather forecasting application hosted in Northern Virginia. As the Solutions Architect, you need to aggregate all the data in the fastest way.

Which of the following options can satisfy the given requirement?

- 1. ☐ A. Upload the data to the closest S3 bucket. Set up a cross-region replication and copy the objects to the destination bucket.
- 2. ☐ B. Use AWS Snowball Edge to transfer large amounts of data.
- 3. ☐ C. Enable Transfer Acceleration in the destination bucket and upload the collected data using Multipart Upload.
- 4. ☐ D. Set up a Site-to-Site VPN connection.

Correct Answer: – C

Explanation: – Amazon S3 is object storage built to store and retrieve any amount of data from anywhere on the Internet. It's a simple storage service that offers industry-leading durability, availability, performance, security, and virtually unlimited scalability at very low costs. Amazon S3 is also designed to be highly flexible. Store any type and amount of data that you want; read the same piece of data a million times or only for emergency disaster recovery; build a simple FTP application or a sophisticated web application.



Since the weather forecasting application is located in N. Virginia, you need to transfer all the data in the same AWS Region. With Amazon S3 Transfer Acceleration, you can speed up content transfers to and from Amazon S3 by as much as 50-500% for long-distance transfer of larger objects. Multipart upload allows you to upload a single object as a set of parts. After all the parts of your object are uploaded, Amazon S3 then presents the data as a single object. This approach is the fastest way to aggregate all the data.

Hence, the correct answer is: **Enable Transfer Acceleration in the destination bucket and upload the collected data using Multipart Upload.**

The option that says: **Upload the data to the closest S3 bucket. Set up a cross-region replication and copy the objects to the destination bucket** is incorrect because replicating the objects to the destination bucket takes about 15 minutes. Take note that the requirement in the scenario is to aggregate the data in the fastest way.

The option that says: **Use AWS Snowball Edge to transfer large amounts of data** is incorrect because the end-to-end time to transfer up to 80 TB of data into AWS Snowball Edge is approximately one week.

The option that says: **Set up a Site-to-Site VPN connection** is incorrect because setting up a VPN connection is not needed in this scenario. Site-to-Site VPN is just used for establishing secure connections between an on-premises network and Amazon VPC. Also, this approach is not the fastest way to transfer your data. You must use Amazon S3 Transfer Acceleration.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html>

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

Question 2. A company has a cloud architecture that is composed of Linux and Windows EC2 instances that process high volumes of financial data 24 hours a day, 7 days a week. To ensure high availability of the systems, the Solutions Architect needs to create a solution that allows them to monitor the memory and disk utilization metrics of all the instances.

Which of the following is the most suitable monitoring solution to implement?

- 1. ☐ A. Install the CloudWatch agent to all the EC2 instances that gathers the memory and disk utilization data. View the custom metrics in the Amazon CloudWatch console.
- 2. ☐ B. Use Amazon Inspector and install the Inspector agent to all EC2 instances.
- 3. ☐ C. Use the default CloudWatch configuration to EC2 instances where the memory and disk utilization metrics are already available. Install the AWS Systems Manager (SSM) Agent to all the EC2 instances.
- 4. ☐ D. Enable the Enhanced Monitoring option in EC2 and install CloudWatch agent to all the EC2 instances to be able to view the memory and disk utilization in the CloudWatch dashboard.

Correct Answer: – A

Explanation: – Amazon CloudWatch has available Amazon EC2 Metrics for you to use for monitoring CPU utilization, Network utilization, Disk performance, and Disk Reads/Writes. In case you need to monitor the below items, you need to prepare a custom metric using a Perl or other shell script, as there are no ready to use metrics for:

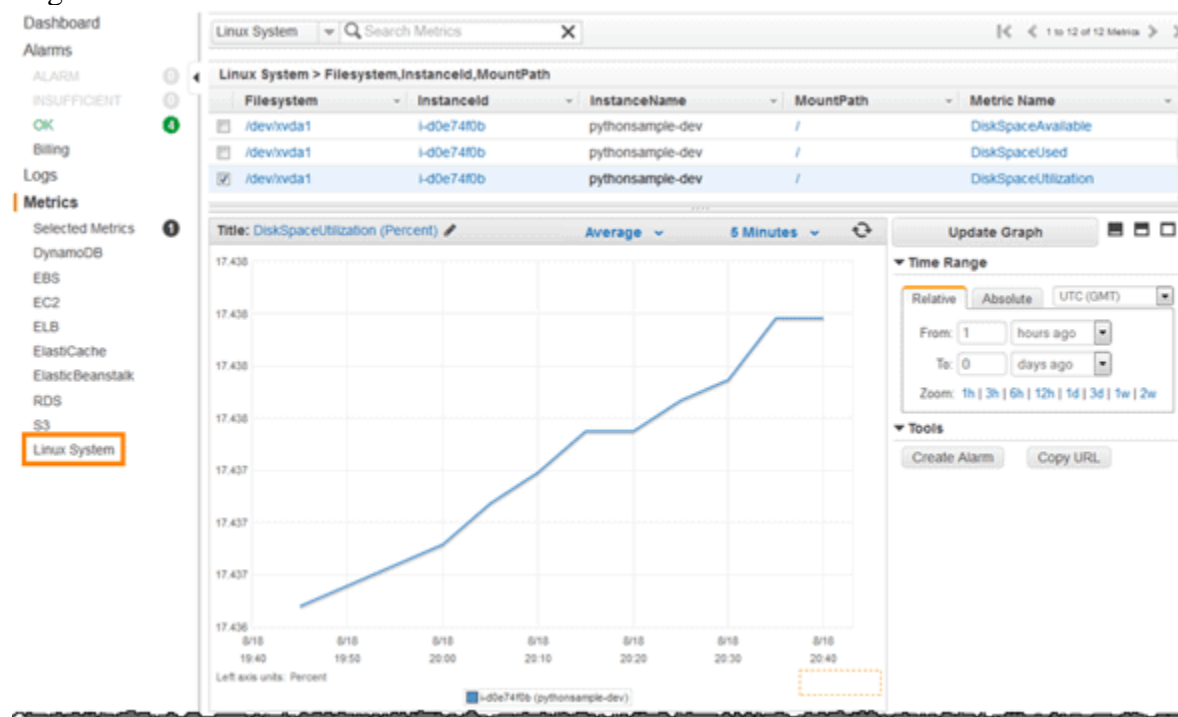
Memory utilization

Disk swap utilization

Disk space utilization

Page file utilization

Log collection



Take note that there is a multi-platform CloudWatch agent that can be installed on both Linux and Windows-based instances. You can use a single agent to collect both system metrics and log files from Amazon EC2 instances and on-premises servers. This agent supports both Windows Server and Linux and enables you to select the metrics to be collected, including sub-resource metrics such as per-CPU core. It is recommended that you use the new agent instead of the older monitoring scripts to collect metrics and logs.

Hence, the correct answer is: **Install the CloudWatch agent to all the EC2 instances that gather the memory and disk utilization data. View the custom metrics in the Amazon CloudWatch console.**

The option that says: **Use the default CloudWatch configuration to EC2 instances where the memory and disk utilization metrics are already available. Install the AWS Systems Manager (SSM) Agent to all the EC2 instances** is incorrect because, by default, CloudWatch does not automatically provide memory and disk utilization metrics of your instances. You have to set up custom CloudWatch metrics to monitor the memory, disk swap, disk space, and page file utilization of your instances.

The option that says: **Enable the Enhanced Monitoring option in EC2 and install CloudWatch agent to all the EC2 instances to be able to view the memory and disk utilization in the CloudWatch dashboard** is incorrect because Enhanced Monitoring is a feature of Amazon RDS. By default, Enhanced Monitoring metrics are stored for 30 days in the CloudWatch Logs.

The option that says: **Use Amazon Inspector and install the Inspector agent to all EC2 instances** is incorrect because Amazon Inspector is an automated security assessment service

that helps you test the network accessibility of your Amazon EC2 instances and the security state of your applications running on the instances. It does not provide a custom metric to track the memory and disk utilization of each and every EC2 instance in your VPC.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_ec2.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html#using_put_script

Question 3. A company plans to launch an Amazon EC2 instance in a private subnet for its internal corporate web portal. For security purposes, the EC2 instance must send data to Amazon DynamoDB and Amazon S3 via private endpoints that don't pass through the public Internet.

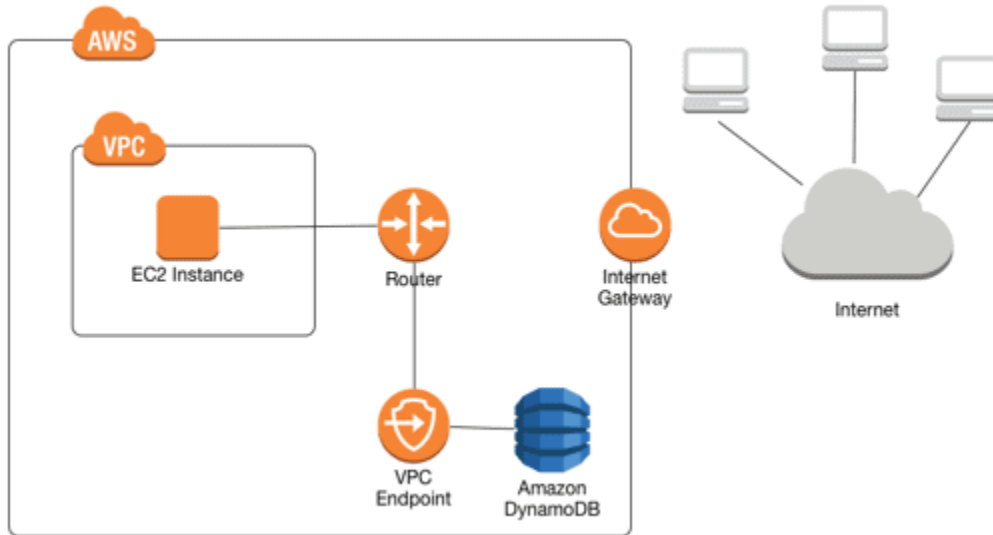
Which of the following can meet the above requirements?

- 1. ☐ A. Use AWS VPN CloudHub to route all access to S3 and DynamoDB via private endpoints.
- 2. ☐ B. Use VPC endpoints to route all access to S3 and DynamoDB via private endpoints.
- 3. ☐ C. Use AWS Direct Connect to route all access to S3 and DynamoDB via private endpoints.
- 4. ☐ D. Use AWS Transit Gateway to route all access to S3 and DynamoDB via private endpoints.

Correct Answer: – B

Explanation: – A **VPC endpoint** allows you to privately connect your VPC to supported AWS and VPC endpoint services powered by AWS PrivateLink without needing an Internet gateway, NAT computer, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

In the scenario, you are asked to configure private endpoints to send data to Amazon DynamoDB and Amazon S3 without accessing the public Internet. Among the options given, VPC endpoint is the most suitable service that will allow you to use private IP addresses to access both DynamoDB and S3 without any exposure to the public internet.



Hence, the correct answer is the option that says: **Use VPC endpoints to route all access to S3 and DynamoDB via private endpoints.**

The option that says: **Use AWS Transit Gateway to route all access in S3 and DynamoDB to a public endpoint** is incorrect because a Transit Gateway simply connects your VPC and on-premises networks through a central hub. It acts as a cloud router that allows you to integrate multiple networks.

The option that says: **Use AWS Direct Connect to route all access to S3 and DynamoDB via private endpoints** is incorrect because AWS Direct Connect is primarily used to establish a dedicated network connection from your premises to AWS. The scenario didn't say that the company is using its on-premises server or has a hybrid cloud architecture.

The option that says: **Use AWS VPN CloudHub to route all access in S3 and DynamoDB to a private endpoint** is incorrect because AWS VPN CloudHub is mainly used to provide secure communication between remote sites and not for creating a private endpoint to access Amazon S3 and DynamoDB within the Amazon network.

References:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html>

<https://docs.aws.amazon.com/glue/latest/dg/vpc-endpoints-s3.html>

Question 4. The company that you are working for has a highly available architecture consisting of an elastic load balancer and several EC2 instances configured with auto-scaling in three Availability Zones. You want to monitor your EC2 instances based on a particular metric, which is not readily available in CloudWatch.

Which of the following is a custom metric in CloudWatch which you have to manually set up?

- 1. ☐ A. Network packets out of an EC2 instance
- 2. ☐ B. Memory Utilization of an EC2 instance
- 3. ☐ C. Disk Reads activity of an EC2 instance
- 4. ☐ D. CPU Utilization of an EC2 instance

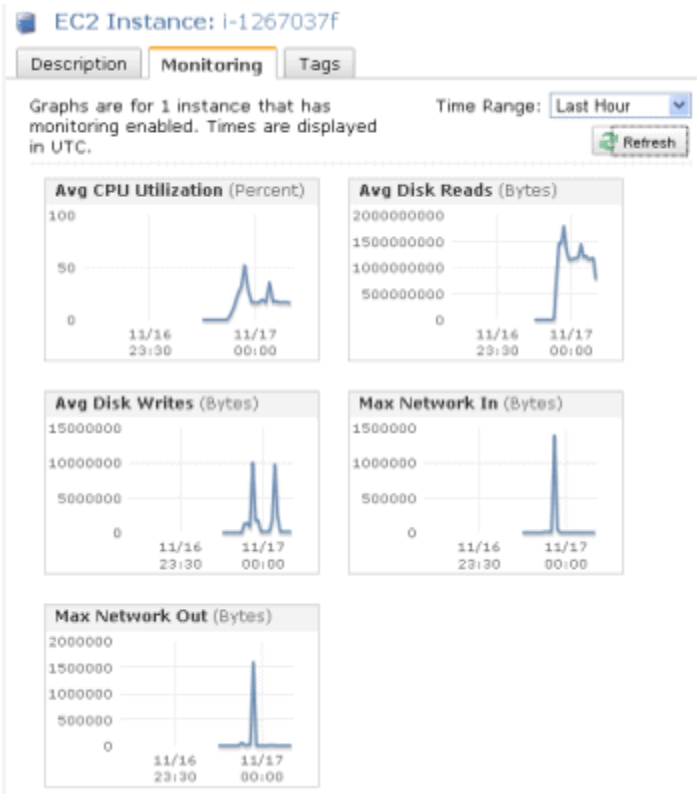
Correct Answer: – B

Explanation: – CloudWatch has available Amazon EC2 Metrics for you to use for monitoring. CPU Utilization identifies the processing power required to run an application upon a selected instance. Network Utilization identifies the volume of incoming and outgoing network traffic to a single instance. Disk Reads metric is used to determine the volume of the data the application reads from the hard disk of the instance. This can be used to determine the speed of the application. However, there are certain metrics that are not readily available in CloudWatch such as memory utilization, disk space utilization, and many others which can be collected by setting up a custom metric.

You need to prepare a custom metric using CloudWatch Monitoring Scripts which is written in Perl. You can also install CloudWatch Agent to collect more system-level metrics from Amazon EC2 instances. Here's the list of custom metrics that you can set up:

- Memory utilization
- Disk swap utilization
- Disk space utilization
- Page file utilization

– Log collection



CPU Utilization of an EC2 instance, Disk Reads activity of an EC2 instance, and Network packets out of an EC2 instance are all incorrect because these metrics are readily available in CloudWatch by default.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_ec2.html

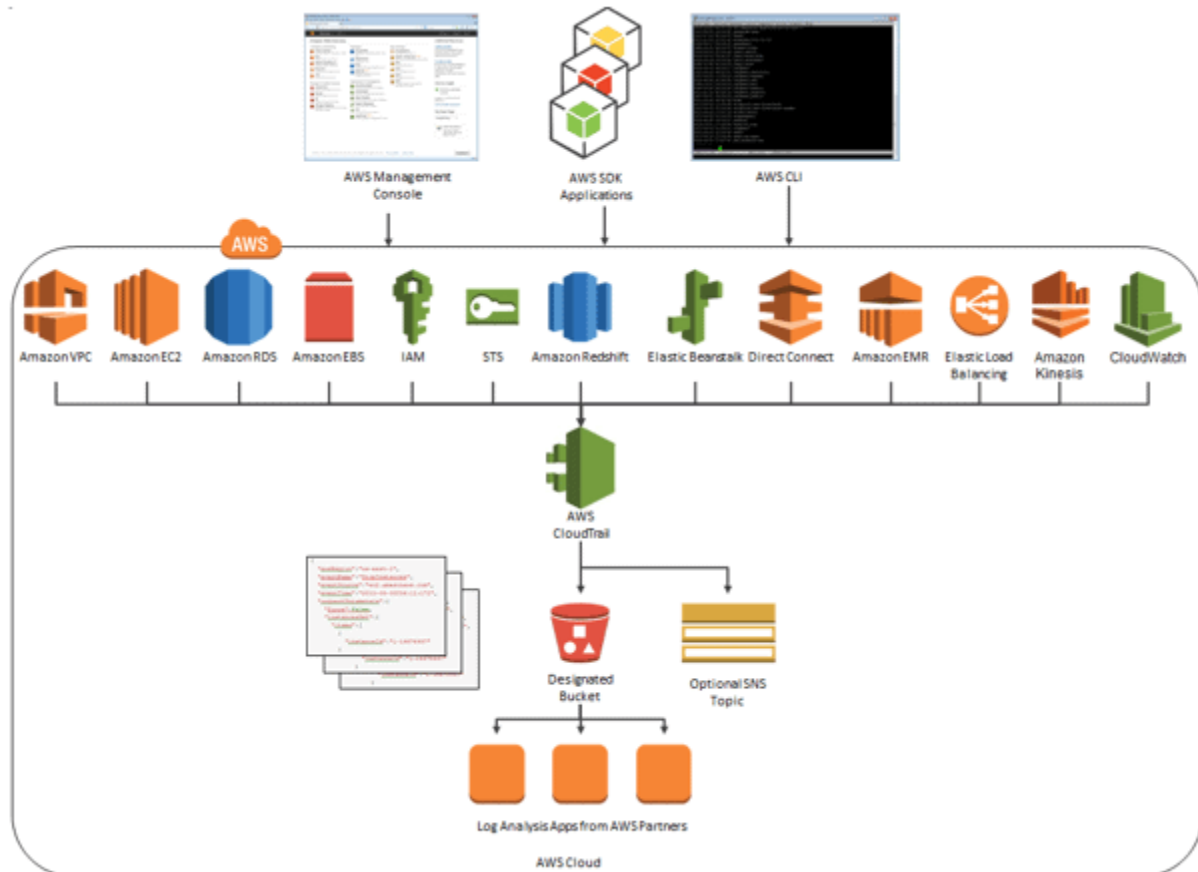
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html#using_put_script

Question 5. A company needs to design an online analytics application that uses Redshift Cluster for its data warehouse. Which of the following services allows them to monitor all API calls in Redshift instance and can also provide secured data for auditing and compliance purposes?

- 1. ☐ A. Amazon CloudWatch
- 2. ☐ B. AWS CloudTrail
- 3. ☐ C. AWS X-Ray
- 4. ☐ D. Amazon Redshift Spectrum

Correct Answer: – B

Explanation: – **AWS CloudTrail** is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. By default, CloudTrail is enabled on your AWS account when you create it. When activity occurs in your AWS account, that activity is recorded in a CloudTrail event. You can easily view recent events in the CloudTrail console by going to Event history.



CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, API calls, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

Hence, the correct answer is: **AWS CloudTrail**.

Amazon CloudWatch is incorrect. Although this is also a monitoring service, it cannot track the API calls to your AWS resources.

AWS X-Ray is incorrect because this is not a suitable service to use to track each API call to your AWS resources. It just helps you debug and analyze your microservices applications with request tracing so you can find the root cause of issues and performance.

Amazon Redshift Spectrum is incorrect because this is not a monitoring service but rather a feature of Amazon Redshift that enables you to query and analyze all of your data in Amazon S3 using the open data formats you already use, with no data loading or transformations needed.

References:

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

<https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/cloudtrail-user-guide.html>

Question 6. A company has decided to host its automobile sales website in Amazon EC2 and store the data in Amazon RDS. The listings will be automatically removed once the vehicle is sold. The Solutions Architect must implement a solution that monitors the automated DB snapshots and forwards the data to multiple target groups.

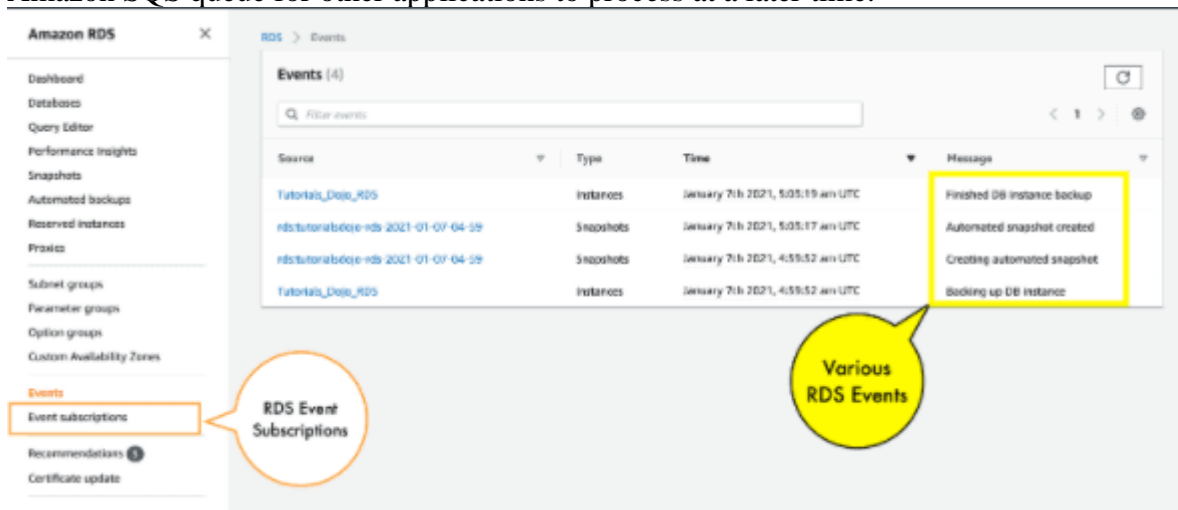
Which of the following options can satisfy the given requirement?

- 1. ☐ A. Create a native function or a stored procedure in Amazon RDS that invokes an AWS Lambda function. Configure the Lambda function to fanout the event notifications to multiple Amazon SNS topics to update the target groups.
- 2. ☐ B. Create an RDS event subscription and send the notifications to Amazon SQS. Configure the SQS queues to fanout the event notifications to multiple Amazon SNS topics. Update the target groups using a Lambda function.
- 3. ☐ C. Create an RDS event subscription and send the notifications to AWS Lambda. Configure the Lambda function to fanout the event notifications to multiple Amazon SQS queues to update the target groups.
- 4. ☐ D. Create an RDS event subscription and send the notifications to Amazon SNS. Configure the SNS topic to fanout the event notifications to multiple Amazon SQS queues. Update the target groups using a Lambda function.

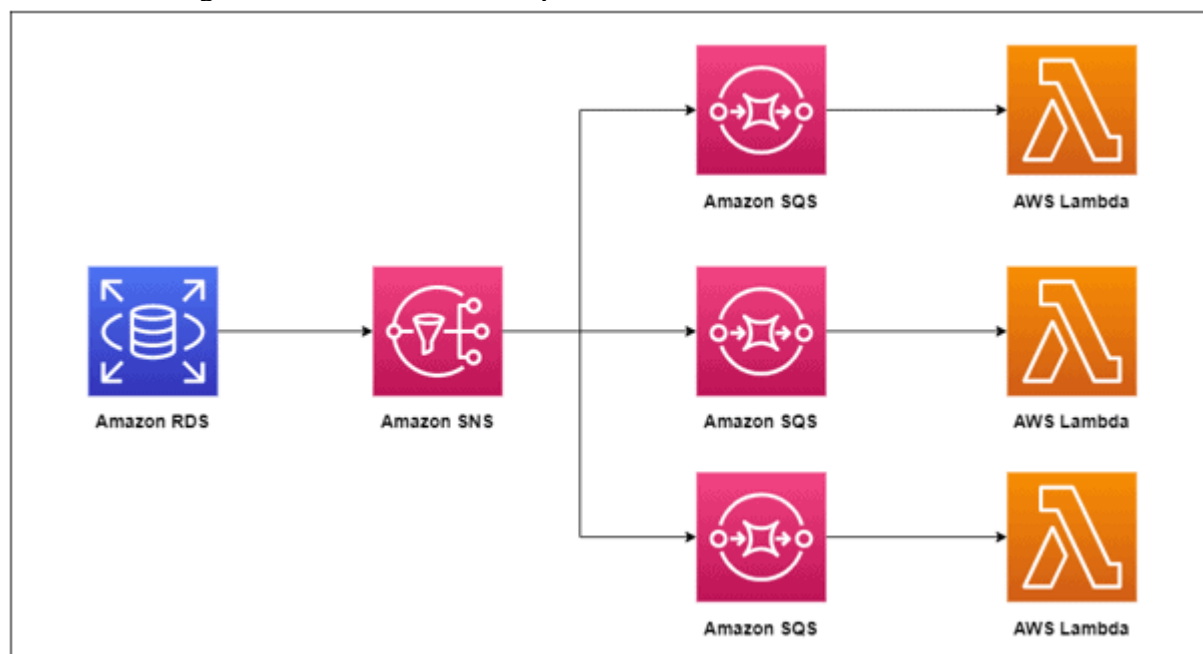
Correct Answer: – D

Explanation: – Amazon SNS works closely with Amazon Simple Queue Service (Amazon SQS). Both services provide different benefits for developers. Amazon SNS allows applications to send time-critical messages to multiple subscribers through a “push” mechanism, eliminating the need to periodically check or “poll” for updates. Amazon SQS is a message queue service used by distributed applications to exchange messages through a polling model and can be used to decouple sending and receiving components—without requiring each component to be concurrently available. Using Amazon SNS and Amazon SQS together, messages can be delivered to applications that require immediate notification of an event, and also persisted in an

Amazon SQS queue for other applications to process at a later time.



You can create an Amazon RDS event notification subscription so you can be notified when an event occurs for a given DB instance, DB snapshot, DB security group, or DB parameter group. The simplest way to create a subscription is with the RDS console. If you choose to create event notification subscriptions using the CLI or API, you must create an Amazon Simple Notification Service topic and subscribe to that topic with the Amazon SNS console or Amazon SNS API. You will also need to retain the Amazon Resource Name (ARN) of the topic because it is used when submitting CLI commands or API operations.



Amazon RDS uses Amazon SNS to send notifications of database events. Each event category applies to a source type, which can be a DB instance, DB snapshot, DB security group, or DB parameter group. The notifications can be in any form supported by Amazon SNS for an AWS Region, such as an email, a text message, or a call to an HTTP endpoint.

In this scenario, you can use Amazon SNS and Amazon SQS to implement fanout messaging. The messages from both of these services can be pushed to multiple subscribers. For example, you can send a message to a topic whenever the automated DB snapshot has been created. The SQS queues subscribed to that topic will receive identical notifications for that order. The Lambda function will process the event notifications and update the target groups.

Hence, the correct answer is: **Create an RDS event subscription and send the notifications to Amazon SNS. Configure the SNS topic to fanout the event notifications to multiple Amazon SQS queues. Update the target groups using a Lambda function.**

The option that says: **Create an RDS event subscription and send the notifications to Amazon SQS. Configure the SQS queues to fanout the event notifications to multiple Amazon SNS topics. Update the target groups using a Lambda function** is incorrect because RDS event subscription can only send notifications to an Amazon SNS topic and not directly to an SQS queue. You have to set up an SNS topic that will fanout the notifications to multiple Amazon SQS queues.

The option that says: **Create an RDS event subscription and send the notifications to AWS Lambda. Configure the Lambda function to fanout the event notifications to multiple Amazon SQS queues to update the target groups** is incorrect because an RDS event notification can only send data to an Amazon SNS topic, and not directly to a Lambda function. To fanout the notifications to multiple SQS queues, you need to use Amazon SNS. The SQS queues will invoke the Lambda function to send the information to multiple target groups.

The option that says: **Create a native function or a stored procedure in Amazon RDS that invokes an AWS Lambda function. Configure the Lambda function to fanout the event notifications to multiple Amazon SNS topics to update the target groups** is incorrect because you cannot directly invoke a Lambda function in Amazon RDS using a native function such as `lambda_sync()`. This is only applicable in Amazon Aurora and moreover, this is primarily used for data changes and not for monitoring automated snapshots.

References:

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

<https://docs.aws.amazon.com/sns/latest/dg/sns-sqs-as-subscriber.html>

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Lambda.html>

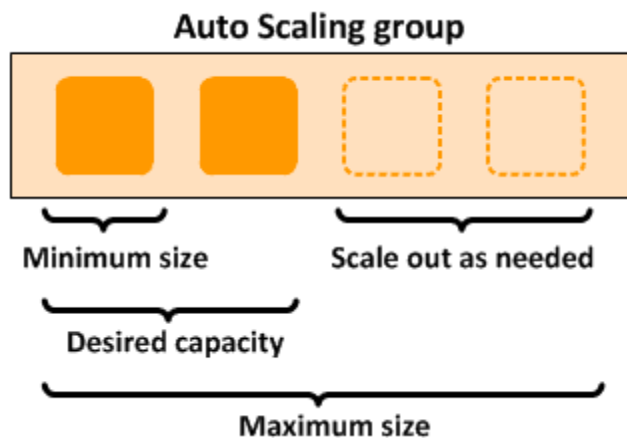
Question 7. A company needs to deploy at least 2 EC2 instances to support the normal workloads of its application and automatically scale up to 6 EC2 instances to handle the peak load. The architecture must be highly available and fault-tolerant as it is processing mission-critical workloads.

As the Solutions Architect of the company, what should you do to meet the above requirement?

- 1. ☐ A. Create an Auto Scaling group of EC2 instances and set the minimum capacity to 2 and the maximum capacity to 4. Deploy 2 instances in Availability Zone A and 2 instances in Availability Zone B.
- 2. ☐ B. Create an Auto Scaling group of EC2 instances and set the minimum capacity to 2 and the maximum capacity to 6. Deploy 4 instances in Availability Zone A.
- 3. ☐ C. Create an Auto Scaling group of EC2 instances and set the minimum capacity to 2 and the maximum capacity to 6. Use 2 Availability Zones and deploy 1 instance for each AZ.
- 4. ☐ D. Create an Auto Scaling group of EC2 instances and set the minimum capacity to 4 and the maximum capacity to 6. Deploy 2 instances in Availability Zone A and another 2 instances in Availability Zone B.

Correct Answer: – D

Explanation: – Amazon EC2 Auto Scaling helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application. You create collections of EC2 instances, called Auto Scaling groups. You can specify the minimum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes below this size. You can also specify the maximum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes above this size.



To achieve highly available and fault-tolerant architecture for your applications, you must deploy all your instances in different Availability Zones. This will help you isolate your resources if an outage occurs. Take note that to achieve fault tolerance, you need to have redundant resources in place to avoid any system degradation in the event of a server fault or an Availability Zone outage. Having a fault-tolerant architecture entails an extra cost in running additional resources than what is usually needed. This is to ensure that the mission-critical workloads are processed.

Since the scenario requires at least 2 instances to handle regular traffic, you should have 2 instances running all the time even if an AZ outage occurred. You can use an Auto Scaling Group to automatically scale your compute resources across two or more Availability Zones. You have to specify the minimum capacity to 4 instances and the maximum capacity to 6 instances. If each AZ has 2 instances running, even if an AZ fails, your system will still run a minimum of 2 instances.

Hence, the correct answer in this scenario is: **Create an Auto Scaling group of EC2 instances and set the minimum capacity to 4 and the maximum capacity to 6. Deploy 2 instances in Availability Zone A and another 2 instances in Availability Zone B.**

The option that says: **Create an Auto Scaling group of EC2 instances and set the minimum capacity to 2 and the maximum capacity to 6. Deploy 4 instances in Availability Zone A** is incorrect because the instances are only deployed in a single Availability Zone. It cannot protect your applications and data from datacentre or AZ failures.

The option that says: **Create an Auto Scaling group of EC2 instances and set the minimum capacity to 2 and the maximum capacity to 6. Use 2 Availability Zones and deploy 1 instance for each AZ** is incorrect because if an AZ outage occurred, there will only be 1 running instance left. The scenario requires you to run at least 2 EC2 instances to support the workload of their application.

The option that says: **Create an Auto Scaling group of EC2 instances and set the minimum capacity to 2 and the maximum capacity to 4. Deploy 2 instances in Availability Zone A and 2 instances in Availability Zone B** is incorrect. Although this fulfils the requirement of at least 2 EC2 instances and high availability, the maximum capacity setting is wrong. It should be set to 6 to properly handle the peak load. If an AZ outage occurs and the system is at its peak load, the number of running instances in this setup will only be 4 instead of 6 and this will affect the performance of your application.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html>

<https://docs.aws.amazon.com/documentdb/latest/developerguide/regions-and-azs.html>

Question 8. A financial application is composed of an Auto Scaling group of EC2 instances, an Application Load Balancer, and a MySQL RDS instance in a Multi-AZ Deployments configuration. To protect the confidential data of your customers, you have to ensure that your RDS database can only be accessed using the profile credentials specific to your EC2 instances via an authentication token.

As the Solutions Architect of the company, which of the following should you do to meet the above requirement?

- 1. ☐ A. Configure SSL in your application to encrypt the database connection to RDS.

- 2. ☐ B. Use a combination of IAM and STS to restrict access to your RDS instance via a temporary token.
- 3. ☐ C. Enable the IAM DB Authentication.
- 4. ☐ D. Create an IAM Role and assign it to your EC2 instances which will grant exclusive access to your RDS instance.

Correct Answer: – C

Explanation: – You can authenticate to your DB instance using AWS Identity and Access Management (IAM) database authentication. IAM database authentication works with MySQL and PostgreSQL. With this authentication method, you don't need to use a password when you connect to a DB instance. Instead, you use an authentication token.

An *authentication token* is a unique string of characters that Amazon RDS generates on request. Authentication tokens are generated using AWS Signature Version 4. Each token has a lifetime of 15 minutes. You don't need to store user credentials in the database, because authentication is managed externally using IAM. You can also still use standard database authentication.

Database options

DB cluster identifier

Info

If you do not provide one, a default identifier based on the instance identifier will be used.

Database name

Info

If you do not specify a database name, Amazon RDS does not create a database.

Port

Info

TCP/IP port the DB instance will use for application connections.

3306

DB parameter group

Info

default.aurora5.6

DB cluster parameter group

Info

default.aurora5.6

Option group

Info

default:aurora-5-6

IAM DB authentication

Info

☒ Enable IAM DB authentication

Manage your database user credentials through AWS IAM users and roles.

☐ Disable

IAM database authentication provides the following benefits:

Network traffic to and from the database is encrypted using Secure Sockets Layer (SSL).

You can use IAM to centrally manage access to your database resources, instead of managing access individually on each DB instance.

For applications running on Amazon EC2, you can use profile credentials specific to your EC2 instance to access your database instead of a password, for greater security.

Hence, **enabling IAM DB Authentication** is the correct answer based on the above reference.

Configuring SSL in your application to encrypt the database connection to RDS is incorrect because an SSL connection is not using an authentication token from IAM. Although configuring SSL to your application can improve the security of your data in flight, it is still not a suitable option to use in this scenario.

Creating an IAM Role and assigning it to your EC2 instances which will grant exclusive access to your RDS instance is incorrect because although you can create and assign an IAM Role to your EC2 instances, you still need to configure your RDS to use IAM DB Authentication.

Using a combination of IAM and STS to restrict access to your RDS instance via a temporary token is incorrect because you have to use IAM DB Authentication for this scenario, and not a combination of an IAM and STS. Although STS is used to send temporary tokens for authentication, this is not a compatible use case for RDS.

Reference:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html>

Question 9. A company requires all the data stored in the cloud to be encrypted at rest. To easily integrate this with other AWS services, they must have full control over the encryption of the created keys and also the ability to immediately remove the key material from AWS KMS. The solution should also be able to audit the key usage independently of AWS CloudTrail.

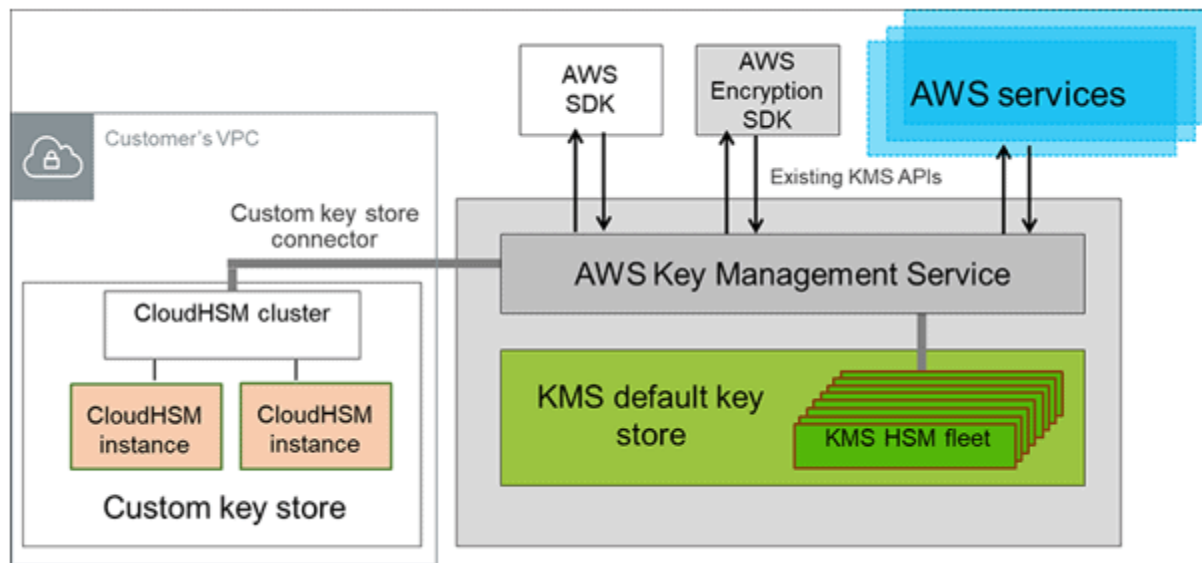
Which of the following options will meet this requirement?

- 1. ☐ A. Use AWS Key Management Service to create a CMK in a custom key store and store the non-extractable key material in Amazon S3.
- 2. ☐ B. Use AWS Key Management Service to create AWS-owned CMKs and store the non-extractable key material in AWS CloudHSM.
- 3. ☐ C. Use AWS Key Management Service to create a CMK in a custom key store and store the non-extractable key material in AWS CloudHSM.
- 4. ☐ D. Use AWS Key Management Service to create AWS-managed CMKs and store the non-extractable key material in AWS CloudHSM.

Correct Answer: – C

Explanation: – The **AWS Key Management Service (KMS)** custom key store feature combines the controls provided by **AWS CloudHSM** with the integration and ease of use of AWS KMS. You can configure your own CloudHSM cluster and authorize AWS KMS to use it as a dedicated key store for your keys rather than the default AWS KMS key store. When you create keys in AWS KMS you can choose to generate the key material in your CloudHSM cluster. CMKs that are generated in your custom key store never leave the HSMs in the CloudHSM cluster in plaintext and all AWS KMS operations that use those keys are only

performed in your HSMs.



AWS KMS can help you integrate with other AWS services to encrypt the data that you store in these services and control access to the keys that decrypt it. To immediately remove the key material from AWS KMS, you can use a custom key store. Take note that each custom key store is associated with an AWS CloudHSM cluster in your AWS account. Therefore, when you create an AWS KMS CMK in a custom key store, AWS KMS generates and stores the non-extractable key material for the CMK in an AWS CloudHSM cluster that you own and manage. This is also suitable if you want to be able to audit the usage of all your keys independently of AWS KMS or AWS CloudTrail.

Since you control your AWS CloudHSM cluster, you have the option to manage the lifecycle of your CMKs independently of AWS KMS. There are four reasons why you might find a custom key store useful:

You might have keys that are explicitly required to be protected in a single-tenant HSM or in an HSM over which you have direct control.

You might have keys that are required to be stored in an HSM that have been validated to FIPS 140-2 level 3 overall (the HSMs used in the standard AWS KMS key store are either validated or in the process of being validated to level 2 with level 3 in multiple categories).

You might need the ability to immediately remove key material from AWS KMS and to prove you have done so by independent means.

You might have a requirement to be able to audit all use of your keys independently of AWS KMS or AWS CloudTrail.

Hence, the correct answer in this scenario is: **Use AWS Key Management Service to create a CMK in a custom key store and store the non-extractable key material in AWS CloudHSM.**

The option that says: **Use AWS Key Management Service to create a CMK in a custom key store and store the non-extractable key material in Amazon S3** is incorrect because Amazon S3 is not a suitable storage service to use in storing encryption keys. You have to use AWS CloudHSM instead.

The options that say: **Use AWS Key Management Service to create AWS-owned CMKs and store the non-extractable key material in AWS CloudHSM** and **Use AWS Key Management Service to create AWS-managed CMKs and store the non-extractable key material in AWS CloudHSM** are both incorrect because the scenario requires you to have full control over the encryption of the created key. AWS-owned CMKs and AWS-managed CMKs are managed by AWS. Moreover, these options do not allow you to audit the key usage independently of AWS CloudTrail.

References:

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

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

<https://aws.amazon.com/blogs/security/are-kms-custom-key-stores-right-for-you/>

Question 10. In a government agency that you are working for, you have been assigned to put confidential tax documents on AWS cloud. However, there is a concern from a security perspective on what can be put on AWS.

What are the features in AWS that can ensure data security for your confidential documents? (Select TWO.)

- 1. ☐ A. Public Data Set Volume Encryption
- 2. ☐ B. S3 Server-Side Encryption
- 3. ☐ C. S3 On-Premises Data Encryption
- 4. ☐ D. EBS On-Premises Data Encryption
- 5. ☐ E. S3 Client-Side Encryption

Correct Answer: – B, E

Explanation: – You can secure the privacy of your data in AWS, both at rest and in-transit, through encryption. If your data is stored in EBS Volumes, you can enable EBS Encryption and if it is stored on Amazon S3, you can enable **client-side** and **server-side encryption**.

Public Data Set Volume Encryption is incorrect as public data sets are designed to be publicly accessible.

EBS On-Premises Data Encryption and **S3 On-Premises Data Encryption** are both incorrect as there is no such thing as On-Premises Data Encryption for S3 and EBS as these services are in the AWS cloud and not on your on-premises network.

References:

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

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

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-public-data-sets.html>

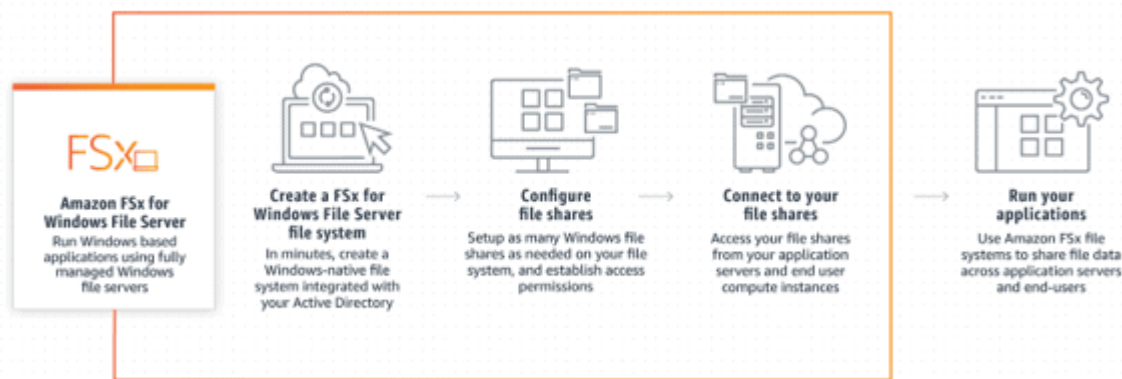
Question 11. A company has a web application that uses Internet Information Services (IIS) for Windows Server. A file share is used to store the application data on the network-attached storage of the company's on-premises data centre. To achieve a highly available system, they plan to migrate the application and file share to AWS.

Which of the following can be used to fulfill this requirement?

- 1. ☐ A. Migrate the existing file share configuration to Amazon EFS.
- 2. ☐ B. Migrate the existing file share configuration to AWS Storage Gateway.
- 3. ☐ C. Migrate the existing file share configuration to Amazon EBS.
- 4. ☐ D. Migrate the existing file share configuration to Amazon FSx for Windows File Server.

Correct Answer: – D

Explanation: – Amazon FSx for Windows File Server provides fully managed Microsoft Windows file servers, backed by a fully native Windows file system. Amazon FSx for Windows File Server has the features, performance, and compatibility to easily lift and shift enterprise applications to the AWS Cloud. It is accessible from Windows, Linux, and macOS compute instances and devices. Thousands of compute instances and devices can access a file system concurrently.



In this scenario, you need to migrate your existing file share configuration to the cloud. Among

the options given, the best possible answer is Amazon FSx. A file share is a specific folder in your file system, including the folder's subfolders, which you make accessible to your compute instances via the SMB protocol. To migrate file share configurations from your on-premises file system, you must migrate your files first to Amazon FSx before migrating your file share configuration.

Hence, the correct answer is: **Migrate the existing file share configuration to Amazon FSx for Windows File Server.**

The option that says: **Migrate the existing file share configuration to AWS Storage Gateway** is incorrect because AWS Storage Gateway is primarily used to integrate your on-premises network to AWS but not for migrating your applications. Using a file share in Storage Gateway implies that you will still keep your on-premises systems, and not entirely migrate it.

The option that says: **Migrate the existing file share configuration to Amazon EFS** is incorrect because it is stated in the scenario that the company is using a file share that runs on a Windows server. Remember that Amazon EFS only supports Linux workloads.

The option that says: **Migrate the existing file share configuration to Amazon EBS** is incorrect because EBS is primarily used as block storage for EC2 instances and not as a shared file system. A file share is a specific folder in a file system that you can access using a server message block (SMB) protocol. Amazon EBS does not support SMB protocol.

References:

<https://aws.amazon.com/fsx/windows/faqs/>

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-file-share-config-to-fsx.html>

Question 12. A Docker application, which is running on an Amazon ECS cluster behind a load balancer, is heavily using DynamoDB. You are instructed to improve the database performance by distributing the workload evenly and using the provisioned throughput efficiently.

Which of the following would you consider implementing for your DynamoDB table?

- 1. ☐ A. Avoid using a composite primary key, which is composed of a partition key and a sort key.
- 2. ☐ B. Use partition keys with high-cardinality attributes, which have a large number of distinct values for each item.
- 3. ☐ C. Use partition keys with low-cardinality attributes, which have a few number of distinct values for each item.
- 4. ☐ D. Reduce the number of partition keys in the DynamoDB table.

Correct Answer: – B

Explanation: – The partition key portion of a table’s primary key determines the logical partitions in which a table’s data is stored. This in turn affects the underlying physical partitions. Provisioned I/O capacity for the table is divided evenly among these physical partitions. Therefore, a partition key design that doesn’t distribute I/O requests evenly can create “hot” partitions that result in throttling and use your provisioned I/O capacity inefficiently.

The optimal usage of a table’s provisioned throughput depends not only on the workload patterns of individual items, but also on the partition-key design. This doesn’t mean that you must access all partition key values to achieve an efficient throughput level, or even that the percentage of accessed partition key values must be high. It does mean that the more distinct partition key values that your workload accesses, the more those requests will be spread across the partitioned space. In general, you will use your provisioned throughput more efficiently as the ratio of partition key values accessed to the total number of partition key values increases.

One example for this is the use of **partition keys with high-cardinality attributes, which have a large number of distinct values for each item.**

Reducing the number of partition keys in the DynamoDB table is incorrect because instead of doing this, you should actually add more to improve its performance to distribute the I/O requests evenly and not avoid “hot” partitions.

Using partition keys with low-cardinality attributes, which have a few numbers of distinct values for each item is incorrect because this is the exact opposite of the correct answer. Remember that the more distinct partition key values your workload accesses, the more those requests will be spread across the partitioned space. Conversely, the less distinct partition key values, the less evenly spread it would be across the partitioned space, which effectively slows the performance.

The option that says: **Avoid using a composite primary key, which is composed of a partition key and a sort key** is incorrect because as mentioned, a composite primary key will provide more partition for the table and in turn, improves the performance. Hence, it should be used and not avoided.

References:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-partition-key-uniform-load.html>

<https://aws.amazon.com/blogs/database/choosing-the-right-dynamodb-partition-key/>

Question 13. A travel photo-sharing website is using Amazon S3 to serve high-quality photos to visitors of your website. After a few days, you found out that there are other travel websites linking and using your photos. This resulted in financial losses for your business.

What is the MOST effective method to mitigate this issue?

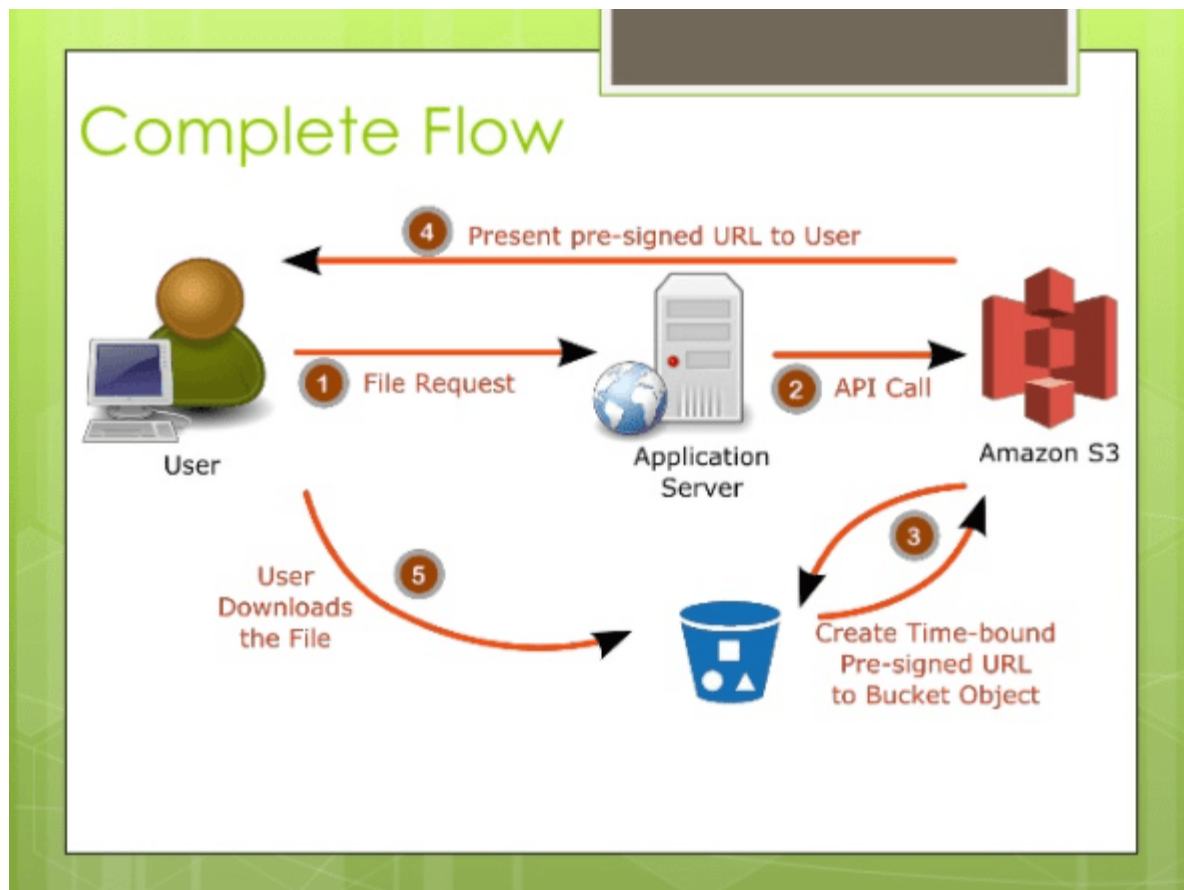
- 1. ☐ A. Use CloudFront distributions for your photos.
- 2. ☐ B. Configure your S3 bucket to remove public read access and use pre-signed URLs with expiry dates.
- 3. ☐ C. Block the IP addresses of the offending websites using NACL.
- 4. ☐ D. Store and privately serve the high-quality photos on Amazon WorkDocs instead.

Correct Answer: – B

Explanation: – In Amazon S3, all objects are private by default. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL, using their own security credentials, to grant time-limited permission to download the objects.

When you create a pre-signed URL for your object, you must provide your security credentials, specify a bucket name, an object key, specify the HTTP method (GET to download the object) and expiration date and time. The pre-signed URLs are valid only for the specified duration.

Anyone who receives the pre-signed URL can then access the object. For example, if you have a video in your bucket and both the bucket and the object are private, you can share the video with others by generating a pre-signed URL.



Using CloudFront distributions for your photos is incorrect. CloudFront is a content delivery network service that speeds up delivery of content to your customers.

Blocking the IP addresses of the offending websites using NACL is also incorrect. Blocking IP address using NACLs is not a very efficient method because a quick change in IP address would easily bypass this configuration.

Storing and privately serving the high-quality photos on Amazon WorkDocs instead is incorrect as WorkDocs is simply a fully managed, secure content creation, storage, and collaboration service. It is not a suitable service for storing static content. Amazon WorkDocs is more often used to easily create, edit, and share documents for collaboration and not for serving object data like Amazon S3.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ObjectOperations.html>

Question 14. A company plans to host a web application in an Auto Scaling group of Amazon EC2 instances. The application will be used globally by users to upload and store several types of files. Based on user trends, files that are older than 2 years must be stored

in a different storage class. The Solutions Architect of the company needs to create a cost-effective and scalable solution to store the old files yet still provide durability and high availability.

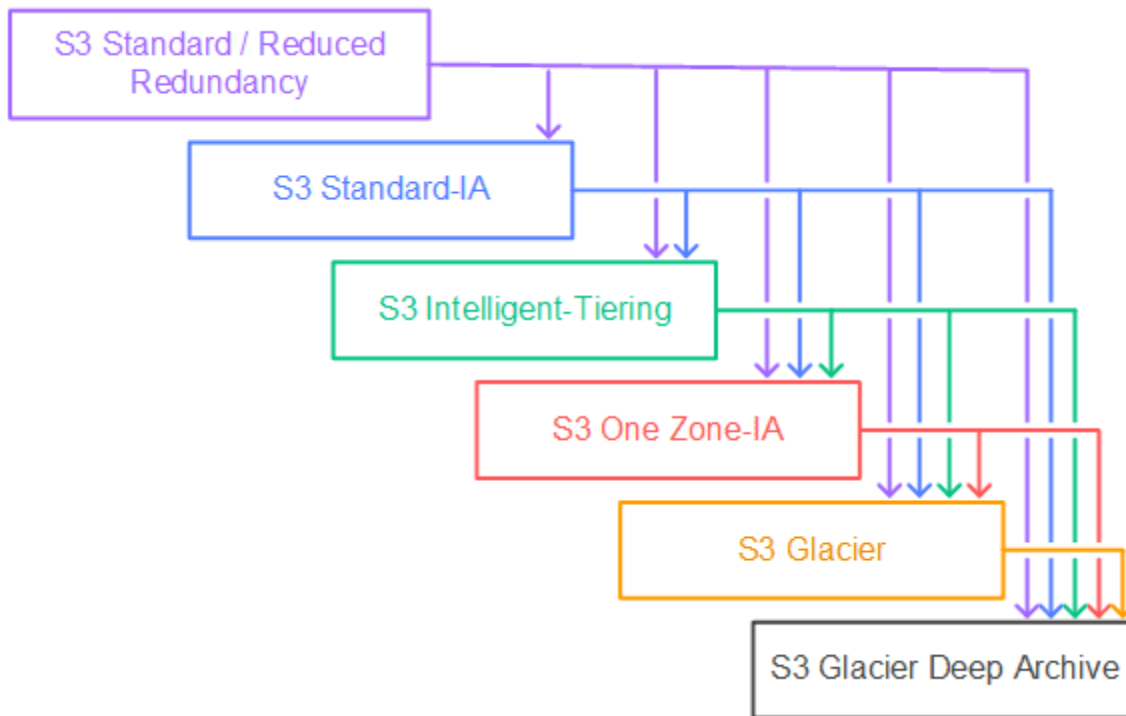
Which of the following approach can be used to fulfill this requirement? (Select TWO.)

- 1. ☐ A. Use Amazon S3 and create a lifecycle policy that will move the objects to Amazon S3 Standard-IA after 2 years.
- 2. ☐ B. Use Amazon S3 and create a lifecycle policy that will move the objects to Amazon S3 Glacier after 2 years.
- 3. ☐ C. Use a RAID 0 storage configuration that stripes multiple Amazon EBS volumes together to store the files. Configure the Amazon Data Lifecycle Manager (DLM) to schedule snapshots of the volumes after 2 years.
- 4. ☐ D. Use Amazon EFS and create a lifecycle policy that will move the objects to Amazon EFS-IA after 2 years.
- 5. ☐ E. Use Amazon EBS volumes to store the files. Configure the Amazon Data Lifecycle Manager (DLM) to schedule snapshots of the volumes after 2 years.

Correct Answer: – A, B

Explanation: – Amazon S3 stores data as objects within buckets. An object is a file and any optional metadata that describes the file. To store a file in Amazon S3, you upload it to a bucket. When you upload a file as an object, you can set permissions on the object and any metadata. Buckets are containers for objects. You can have one or more buckets. You can control access for each bucket, deciding who can create, delete, and list objects in it. You can also choose the geographical Region where Amazon S3 will store the bucket and its contents and view access

logs for the bucket and its objects.



To move a file to a different storage class, you can use Amazon S3 or Amazon EFS. Both services have lifecycle configurations. Take note that Amazon EFS can only transition a file to the IA storage class after 90 days. Since you need to move the files that are older than 2 years to a more cost-effective and scalable solution, you should use the Amazon S3 lifecycle configuration. With S3 lifecycle rules, you can transition files to S3 Standard IA or S3 Glacier. Using S3 Glacier expedited retrieval, you can quickly access your files within 1-5 minutes.

Hence, the correct answers are:

- Use Amazon S3 and create a lifecycle policy that will move the objects to Amazon S3 Glacier after 2 years.
- Use Amazon S3 and create a lifecycle policy that will move the objects to Amazon S3 Standard-IA after 2 years.

The option that says: **Use Amazon EFS and create a lifecycle policy that will move the objects to Amazon EFS-IA after 2 years** is incorrect because the maximum days for the EFS lifecycle policy is only 90 days. The requirement is to move the files that are older than 2 years or 730 days.

The option that says: **Use Amazon EBS volumes to store the files. Configure the Amazon Data Lifecycle Manager (DLM) to schedule snapshots of the volumes after 2 years** is incorrect because Amazon EBS costs more and is not as scalable as Amazon S3. It has some limitations when accessed by multiple EC2 instances. There are also huge costs involved in

using the multi-attach feature on a Provisioned IOPS EBS volume to allow multiple EC2 instances to access the volume.

The option that says: **Use a RAID 0 storage configuration that stripes multiple Amazon EBS volumes together to store the files. Configure the Amazon Data Lifecycle Manager (DLM) to schedule snapshots of the volumes after 2 years** is incorrect because RAID (Redundant Array of Independent Disks) is just a data storage virtualization technology that combines multiple storage devices to achieve higher performance or data durability. RAID 0 can stripe multiple volumes together for greater I/O performance than you can achieve with a single volume. On the other hand, RAID 1 can mirror two volumes together to achieve on-instance redundancy.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

<https://docs.aws.amazon.com/efs/latest/ug/lifecycle-management-efs.html>

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

Question 15. A startup is using Amazon RDS to store data from a web application. Most of the time, the application has low user activity, but it receives bursts of traffic within seconds whenever there is a new product announcement. The Solutions Architect needs to create a solution that will allow users around the globe to access the data using an API.

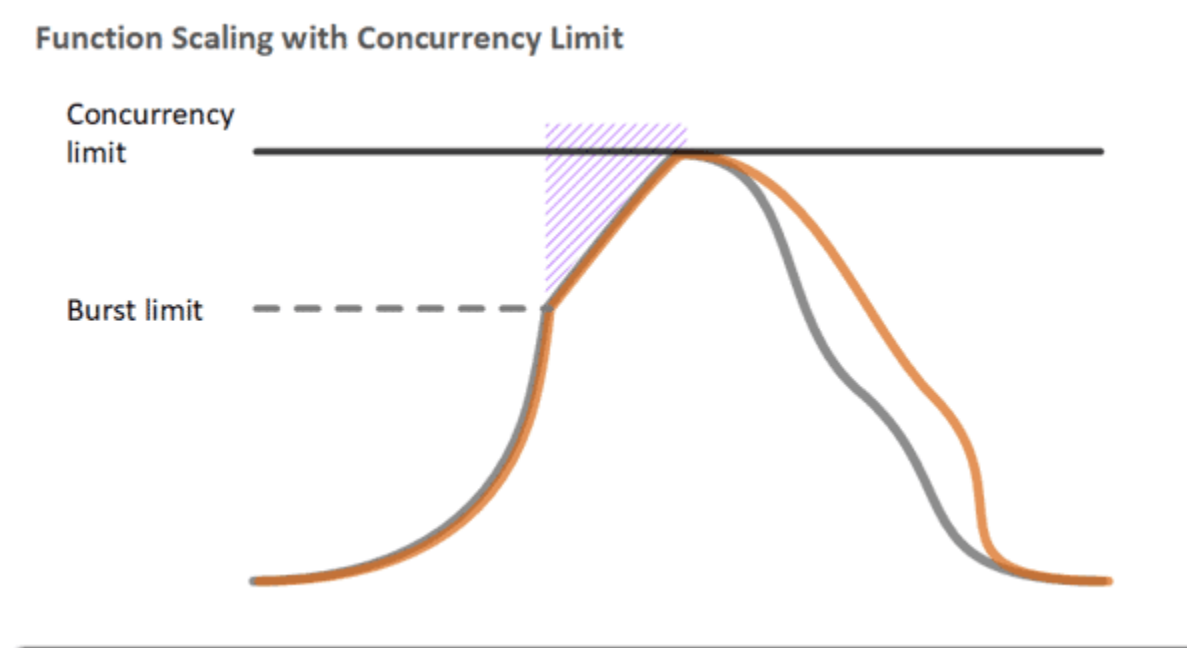
What should the Solutions Architect do meet the above requirement?

- 1. ☐ A. Create an API using Amazon API Gateway and use Amazon Elastic Beanstalk with Auto Scaling to handle the bursts of traffic in seconds.
- 2. ☐ B. Create an API using Amazon API Gateway and use AWS Lambda to handle the bursts of traffic in seconds.
- 3. ☐ C. Create an API using Amazon API Gateway and use an Auto Scaling group of Amazon EC2 instances to handle the bursts of traffic in seconds.
- 4. ☐ D. Create an API using Amazon API Gateway and use the Amazon ECS cluster with Service Auto Scaling to handle the bursts of traffic in seconds.

Correct Answer: – B

Explanation: – AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. With Lambda, you can run code for virtually any type of application or backend service – all with zero administration. Just upload your code, and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services or call it directly from any web or mobile app.

The first time you invoke your function, AWS Lambda creates an instance of the function and runs its handler method to process the event. When the function returns a response, it stays active and waits to process additional events. If you invoke the function again while the first event is being processed, Lambda initializes another instance, and the function processes the two events concurrently. As more events come in, Lambda routes them to available instances and creates new instances as needed. When the number of requests decreases, Lambda stops unused instances to free up the scaling capacity for other functions.



Your functions' *concurrency* is the number of instances that serve requests at a given time. For an initial burst of traffic, your functions' cumulative concurrency in a Region can reach an initial level of between 500 and 3000, which varies per Region.

Based on the given scenario, you need to create a solution that will satisfy the two requirements. The first requirement is to create a solution that will allow the users to access the data using an API. To implement this solution, you can use Amazon API Gateway. The second requirement is to handle the burst of traffic within seconds. You should use AWS Lambda in this scenario because Lambda functions can absorb reasonable bursts of traffic for approximately 15-30 minutes.

Lambda can scale faster than the regular Auto Scaling feature of Amazon EC2, Amazon Elastic Beanstalk, or Amazon ECS. This is because AWS Lambda is more lightweight than other computing services. Under the hood, Lambda can run your code to thousands of available AWS-managed EC2 instances (that could already be running) within seconds to accommodate traffic. This is faster than the Auto Scaling process of launching new EC2 instances that could take a few minutes or so. An alternative is to overprovision your compute capacity but that will incur significant costs. The best option to implement given the requirements is a combination of AWS Lambda and Amazon API Gateway.

Hence, the correct answer is: **Create an API using Amazon API Gateway and use AWS Lambda to handle the bursts of traffic.**

The option that says: **Create an API using Amazon API Gateway and use the Amazon ECS cluster with Service Auto Scaling to handle the bursts of traffic in seconds** is incorrect. AWS Lambda is a better option than Amazon ECS since it can handle a sudden burst of traffic within seconds and not minutes.

The option that says: **Create an API using Amazon API Gateway and use Amazon Elastic Beanstalk with Auto Scaling to handle the bursts of traffic in seconds** is incorrect because just like the previous option, the use of Auto Scaling has a delay of a few minutes as it launches new EC2 instances that will be used by Amazon Elastic Beanstalk.

The option that says: **Create an API using Amazon API Gateway and use an Auto Scaling group of Amazon EC2 instances to handle the bursts of traffic in seconds** is incorrect because the processing time of Amazon EC2 Auto Scaling to provision new resources takes minutes. Take note that in the scenario, a burst of traffic within seconds is expected to happen.

References:

<https://aws.amazon.com/blogs/startups/from-0-to-100-k-in-seconds-instant-scale-with-aws-lambda/>

<https://docs.aws.amazon.com/lambda/latest/dg/invoke-scaling.html>

Question 16. A company plans to migrate its on-premises workload to AWS. The current architecture is composed of a Microsoft SharePoint server that uses a Windows shared file storage. The Solutions Architect needs to use a cloud storage solution that is highly available and can be integrated with Active Directory for access control and authentication.

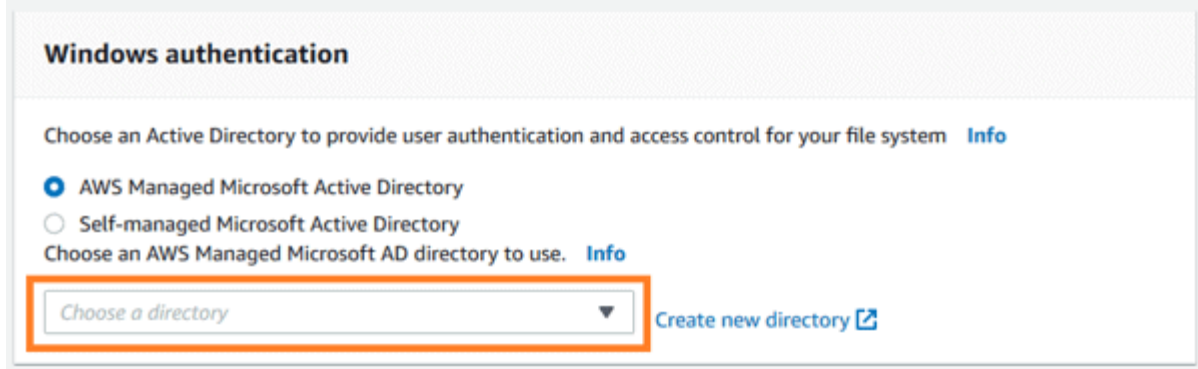
Which of the following options can satisfy the given requirement?

- 1. ☐ A. Launch an Amazon EC2 Windows Server to mount a new S3 bucket as a file volume.
- 2. ☐ B. Create a file system using Amazon EFS and join it to an Active Directory domain.
- 3. ☐ C. Create a file system using Amazon FSx for Windows File Server and join it to an Active Directory domain in AWS.
- 4. ☐ D. Create a Network File System (NFS) file share using AWS Storage Gateway.

Correct Answer: – C

Explanation: – Amazon FSx for Windows File Server provides fully managed, highly reliable, and scalable file storage that is accessible over the industry-standard Service Message Block

(SMB) protocol. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration. Amazon FSx is accessible from Windows, Linux, and MacOS compute instances and devices. Thousands of compute instances and devices can access a file system concurrently.



Amazon FSx works with Microsoft Active Directory to integrate with your existing Microsoft Windows environments. You have two options to provide user authentication and access control for your file system: AWS Managed Microsoft Active Directory and Self-managed Microsoft Active Directory.

Take note that after you create an Active Directory configuration for a file system, you can't change that configuration. However, you can create a new file system from a backup and change the Active Directory integration configuration for that file system. These configurations allow the users in your domain to use their existing identity to access the Amazon FSx file system and to control access to individual files and folders.

Hence, the correct answer is: **Create a file system using Amazon FSx for Windows File Server and join it to an Active Directory domain in AWS.**

The option that says: **Create a file system using Amazon EFS and join it to an Active Directory domain** is incorrect because Amazon EFS does not support Windows systems, only Linux OS. You should use Amazon FSx for Windows File Server instead to satisfy the requirement in the scenario.

The option that says: **Launch an Amazon EC2 Windows Server to mount a new S3 bucket as a file volume** is incorrect because you can't integrate Amazon S3 with your existing Active Directory to provide authentication and access control.

The option that says: **Create a Network File System (NFS) file share using AWS Storage Gateway** is incorrect because NFS file share is mainly used for Linux systems. Remember that the requirement in the scenario is to use a Windows shared file storage. Therefore, you must use an SMB file share instead, which supports Windows OS and Active Directory configuration. Alternatively, you can also use the Amazon FSx for the Windows File Server file system.

References:

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/aws-ad-integration-fsxW.html>

<https://aws.amazon.com/fsx/windows/faqs/>

<https://docs.aws.amazon.com/storagegateway/latest/userguide/CreatingAnSMBFileShare.html>

Question 17. An organization needs a persistent block storage volume that will be used for mission-critical workloads. The backup data will be stored in an object storage service and after 30 days, the data will be stored in a data archiving storage service.

What should you do to meet the above requirement?

- 1. ☐ A. Attach an instance store volume in your existing EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to Amazon S3 Glacier.
- 2. ☐ B. Attach an EBS volume in your EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to Amazon S3 One Zone-IA.
- 3. ☐ C. Attach an EBS volume in your EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to Amazon S3 Glacier.
- 4. ☐ D. Attach an instance store volume in your EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to Amazon S3 One Zone-IA.

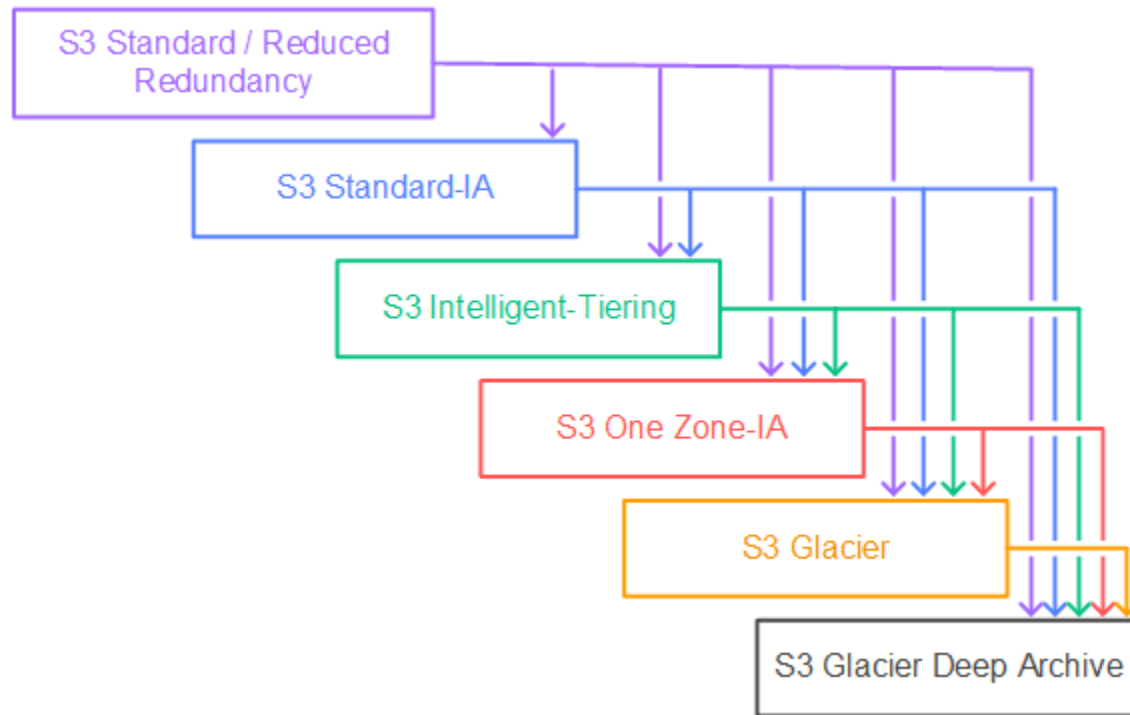
Correct Answer: – C

Explanation: – Amazon Elastic Block Store (EBS) is an easy to use, high performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction intensive workloads at any scale. A broad range of workloads, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS.

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics.

In an **S3 Lifecycle configuration**, you can define rules to transition objects from one storage class to another to save on storage costs. Amazon S3 supports a waterfall model for transitioning

between storage classes, as shown in the diagram below:



In this scenario, three services are required to implement this solution. The mission-critical workloads mean that you need to have a persistent block storage volume and the designed service for this is Amazon EBS volumes. The second workload needs to have an object storage service, such as Amazon S3, to store your backup data. Amazon S3 enables you to configure the lifecycle policy from S3 Standard to different storage classes. For the last one, it needs archive storage such as Amazon S3 Glacier.

Hence, the correct answer in this scenario is: **Attach an EBS volume in your EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to Amazon S3 Glacier.**

The option that says: **Attach an EBS volume in your EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to Amazon S3 One Zone-IA** is incorrect because this lifecycle policy will transition your objects into an infrequently accessed storage class and not a storage class for data archiving.

The option that says: **Attach an instance store volume in your existing EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to Amazon S3 Glacier** is incorrect because an Instance Store volume is simply a temporary block-level storage for EC2 instances. Also, you can't attach instance store volumes to an instance after you've launched it. You can specify the instance store volumes for your instance only when you launch it.

The option that says: **Attach an instance store volume in your EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to Amazon S3 One Zone-IA** is incorrect. Just like the previous option, the use of instance store volume is not suitable for mission-critical workloads because the data can be lost if the underlying disk drive fails, the instance stops, or if the instance is terminated. In addition, Amazon S3 Glacier is a more suitable option for data archival instead of Amazon S3 One Zone-IA.

References:

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

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

Question 18. A pharmaceutical company has resources hosted on both their on-premises network and in AWS cloud. They want all of their Software Architects to access resources on both environments using their on-premises credentials, which is stored in Active Directory.

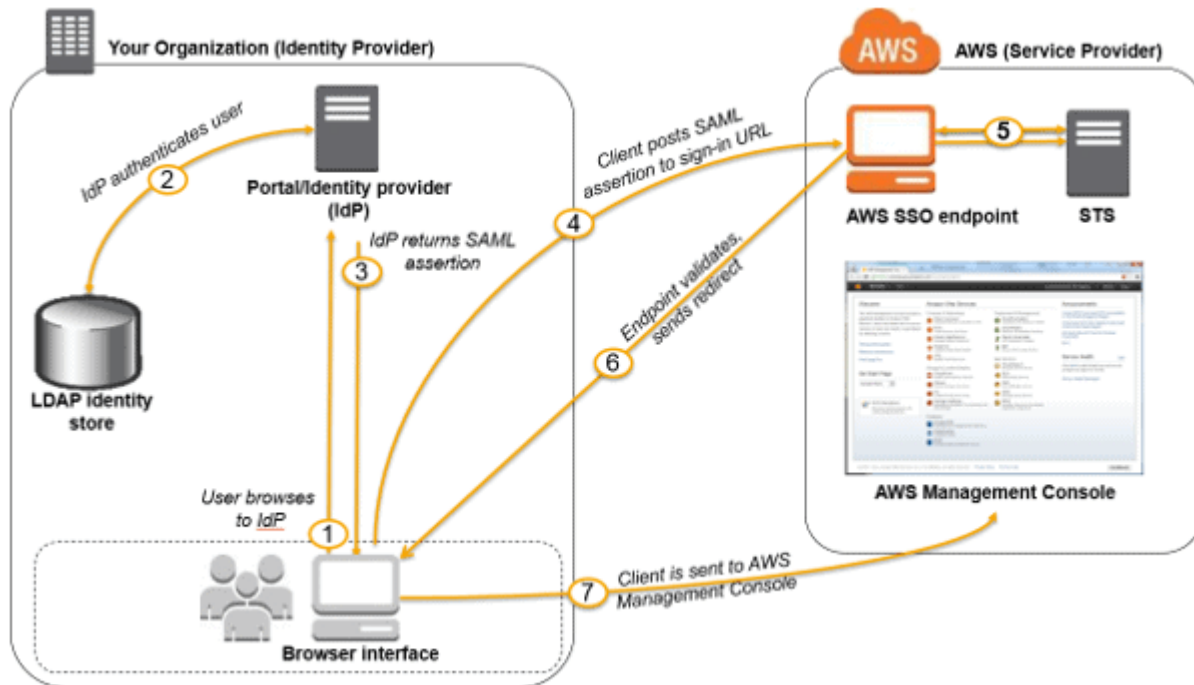
In this scenario, which of the following can be used to fulfill this requirement?

- 1. ☐ A. Set up SAML 2.0-Based Federation by using a Microsoft Active Directory Federation Service (AD FS).
- 2. ☐ B. Use IAM users
- 3. ☐ C. Set up SAML 2.0-Based Federation by using a Web Identity Federation.
- 4. ☐ D. Use Amazon VPC

Correct Answer: – A

Explanation: – Since the company is using Microsoft Active Directory which implements Security Assertion Markup Language (SAML), you can set up a SAML-Based Federation for API Access to your AWS cloud. In this way, you can easily connect to AWS using the login

credentials of your on-premises network.



AWS supports identity federation with SAML 2.0, an open standard that many identity providers (IdPs) use. This feature enables federated single sign-on (SSO), so users can log into the AWS Management Console or call the AWS APIs without you having to create an IAM user for everyone in your organization. By using SAML, you can simplify the process of configuring federation with AWS, because you can use the IdP's service instead of writing custom identity proxy code.

Before you can use SAML 2.0-based federation as described in the preceding scenario and diagram, you must configure your organization's IdP and your AWS account to trust each other. The general process for configuring this trust is described in the following steps. Inside your organization, you must have an IdP that supports SAML 2.0, like Microsoft Active Directory Federation Service (AD FS, part of Windows Server), Shibboleth, or another compatible SAML 2.0 provider.

Hence, the correct answer is: ***Set up SAML 2.0-Based Federation by using a Microsoft Active Directory Federation Service (AD FS).***

Setting up SAML 2.0-Based Federation by using a Web Identity Federation is incorrect because this is primarily used to let users sign in via a well-known external identity provider (IdP), such as Login with Amazon, Facebook, Google. It does not utilize Active Directory.

Using IAM users is incorrect because the situation requires you to use the existing credentials stored in their Active Directory, and not user accounts that will be generated by IAM.

Using Amazon VPC is incorrect because this only lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. This has nothing to do with user authentication or Active Directory.

References:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.html

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

Question 19. A Solutions Architect is working for a company which has multiple VPCs in various AWS regions. The Architect is assigned to set up a logging system which will track all of the changes made to their AWS resources in all regions, including the configurations made in IAM, CloudFront, AWS WAF, and Route 53. In order to pass the compliance requirements, the solution must ensure the security, integrity, and durability of the log data. It should also provide an event history of all API calls made in AWS Management Console and AWS CLI.

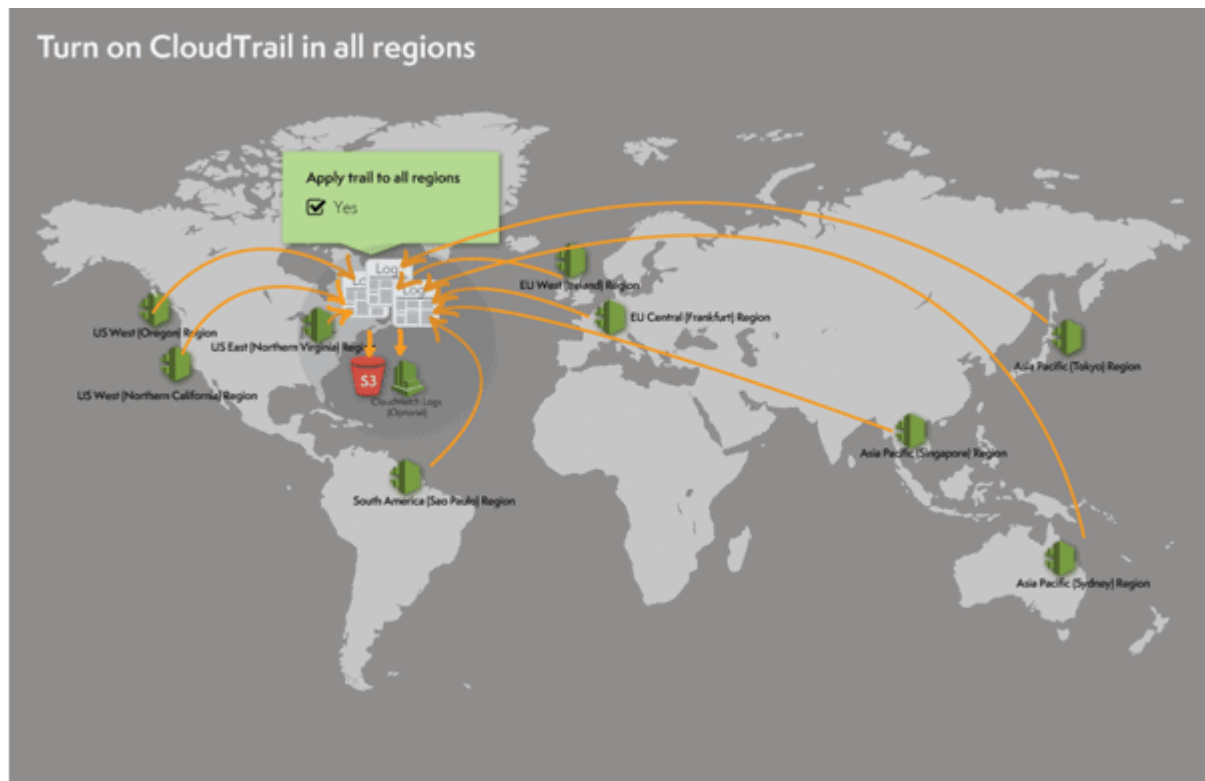
Which of the following solutions is the best fit for this scenario?

- 1. ☐ A. Set up a new CloudWatch trail in a new S3 bucket using the CloudTrail console and also pass the `--is-multi-region-trail` parameter then encrypt log files using KMS encryption. Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies.
- 2. ☐ B. Set up a new CloudWatch trail in a new S3 bucket using the AWS CLI and also pass both the `--is-multi-region-trail` and `--include-global-service-events` parameters then encrypt log files using KMS encryption. Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies.
- 3. ☐ C. Set up a new CloudTrail trail in a new S3 bucket using the AWS CLI and also pass both the `--is-multi-region-trail` and `--no-include-global-service-events` parameters then encrypt log files using KMS encryption. Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies.
- 4. ☐ D. Set up a new CloudTrail trail in a new S3 bucket using the AWS CLI and also pass both the `--is-multi-region-trail` and `--include-global-service-events` parameters then encrypt log files using KMS encryption. Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies.

Correct Answer: – D

Explanation: – An event in CloudTrail is the record of an activity in an AWS account. This activity can be an action taken by a user, role, or service that is monitorable by CloudTrail. CloudTrail events provide a history of both API and non-API account activity made through the

AWS Management Console, AWS SDKs, command line tools, and other AWS services. There are two types of events that can be logged in CloudTrail: management events and data events. By default, trails log management events, but not data events.



A trail can be applied to all regions or a single region. As a best practice, create a trail that applies to all regions in the AWS partition in which you are working. This is the default setting when you create a trail in the CloudTrail console.

For most services, events are recorded in the region where the action occurred. For global services such as AWS Identity and Access Management (IAM), AWS STS, Amazon CloudFront, and Route 53, events are delivered to any trail that includes global services, and are logged as occurring in US East (N. Virginia) Region.

In this scenario, the company requires a secure and durable logging solution that will track all of the activities of all AWS resources on all regions. CloudTrail can be used for this case with multi-region trail enabled, however, it will only cover the activities of the regional services (EC2, S3, RDS etc.) and not for global services such as IAM, CloudFront, AWS WAF, and Route 53. In order to satisfy the requirement, you have to add the `--include-global-service-events` parameter in your AWS CLI command.

The option that says: ***Set up a new CloudTrail trail in a new S3 bucket using the AWS CLI and also pass both the `--is-multi-region-trail` and `--include-global-service-events` parameters then encrypt log files using KMS encryption. Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the***

bucket policies is correct because it provides security, integrity, and durability to your log data and in addition, it has the `-include-global-service-events` parameter enabled which will also include activity from global services such as IAM, Route 53, AWS WAF, and CloudFront.

The option that says: *Set up a new CloudWatch trail in a new S3 bucket using the AWS CLI and also pass both the `-is-multi-region-trail` and `-include-global-service-events` parameters then encrypt log files using KMS encryption. Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies* is incorrect because you need to use CloudTrail instead of CloudWatch.

The option that says: *Set up a new CloudWatch trail in a new S3 bucket using the CloudTrail console and also pass the `-is-multi-region-trail` parameter then encrypt log files using KMS encryption. Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies* is incorrect because you need to use CloudTrail instead of CloudWatch. In addition, the `-include-global-service-events` parameter is also missing in this setup.

The option that says: *Set up a new CloudTrail trail in a new S3 bucket using the AWS CLI and also pass both the `-is-multi-region-trail` and `-no-include-global-service-events` parameters then encrypt log files using KMS encryption. Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies* is incorrect because the `-is-multi-region-trail` is not enough as you also need to add the `-include-global-service-events` parameter and not `-no-include-global-service-events`. Plus, you cannot enable the Global Service Events using the CloudTrail console but by using AWS CLI.

References:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-global-service-events>

<http://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html>

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-and-update-a-trail-by-using-the-aws-cli.html>

Question 20. A telecommunications company is planning to give AWS Console access to developers. Company policy mandates the use of identity federation and role-based access control. Currently, the roles are already assigned using groups in the corporate Active Directory.

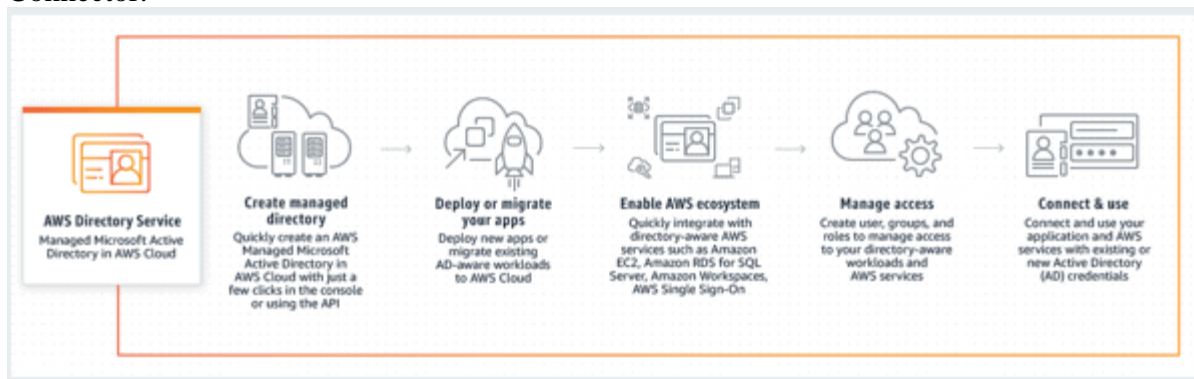
In this scenario, what combination of the following services can provide developers access to the AWS console? (Select TWO.)

- 1. ☐ A. IAM Groups

- 2. ☐ B. IAM Roles
- 3. ☐ C. AWS Directory Service Simple AD
- 4. ☐ D. Lambda
- 5. ☐ E. AWS Directory Service AD Connector

Correct Answer: – B, E

Explanation: – Considering that the company is using a corporate Active Directory, it is best to use **AWS Directory Service AD Connector** for easier integration. In addition, since the roles are already assigned using groups in the corporate Active Directory, it would be better to also use **IAM Roles**. Take note that you can assign an IAM Role to the users or groups from your Active Directory once it is integrated with your VPC via the AWS Directory Service AD Connector.



AWS Directory Service provides multiple ways to use Amazon Cloud Directory and Microsoft Active Directory (AD) with other AWS services. Directories store information about users, groups, and devices, and administrators use them to manage access to information and resources. AWS Directory Service provides multiple directory choices for customers who want to use existing Microsoft AD or Lightweight Directory Access Protocol (LDAP)–aware applications in the cloud. It also offers those same choices to developers who need a directory to manage users, groups, devices, and access.

AWS Directory Service Simple AD is incorrect because this just provides a **subset** of the features offered by AWS Managed Microsoft AD, including the ability to manage user accounts and group memberships, create and apply group policies, securely connect to Amazon EC2 instances, and provide Kerberos-based single sign-on (SSO). In this scenario, the more suitable component to use is the AD Connector since it is a directory gateway with which you can redirect directory requests to your on-premises Microsoft Active Directory.

IAM Groups is incorrect because this is just a collection of *IAM* users. *Groups* let you specify permissions for multiple users, which can make it easier to manage the permissions for those users. In this scenario, the more suitable one to use is IAM Roles in order for permissions to create AWS Directory Service resources.

Lambda is incorrect because this is primarily used for serverless computing.

Reference:

<https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/>

Question 21. A company hosts multiple applications in their VPC. While monitoring the system, they noticed that multiple port scans are coming in from a specific IP address block that is trying to connect to several AWS resources inside their VPC. The internal security team has requested that all offending IP addresses be denied for the next 24 hours for security purposes.

Which of the following is the best method to quickly and temporarily deny access from the specified IP addresses?

- 1. ☐ A. Modify the Network Access Control List associated with all public subnets in the VPC to deny access from the IP Address block.
- 2. ☐ B. Create a policy in IAM to deny access from the IP Address block.
- 3. ☐ C. Configure the firewall in the operating system of the EC2 instances to deny access from the IP address block.
- 4. ☐ D. Add a rule in the Security Group of the EC2 instances to deny access from the IP Address block.

Correct Answer: – A

Explanation: – To control the traffic coming in and out of your VPC network, you can use the **network access control list (ACL)**. It is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. This is the best solution among other options as you can easily add and remove the restriction in a matter of minutes.

Creating a policy in IAM to deny access from the IP Address block is incorrect as an IAM policy does not control the inbound and outbound traffic of your VPC.

Adding a rule in the Security Group of the EC2 instances to deny access from the IP Address block is incorrect as although a Security Group acts as a firewall, it will only control both inbound and outbound traffic at the instance level and not on the whole VPC.

Configuring the firewall in the operating system of the EC2 instances to deny access from the IP address block is incorrect because adding a firewall in the underlying operating system of the EC2 instance is not enough; the attacker can just connect to other AWS resources since the network access control list still allows them to do so.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

Question 22. An online cryptocurrency exchange platform is hosted in AWS which uses ECS Cluster and RDS in Multi-AZ Deployments configuration. The application is heavily using the RDS instance to process complex read and write database operations. To maintain the reliability, availability, and performance of your systems, you have to closely monitor how the different processes or threads on a DB instance use the CPU, including the percentage of the CPU bandwidth and total memory consumed by each process.

Which of the following is the most suitable solution to properly monitor your database?

- 1. ☐ A. Check the CPU% and MEM% metrics which are readily available in the Amazon RDS console that shows the percentage of the CPU bandwidth and total memory consumed by each database process of your RDS instance.
- 2. ☐ B. Use Amazon CloudWatch to monitor the CPU Utilization of your database.
- 3. ☐ C. Create a script that collects and publishes custom metrics to CloudWatch, which tracks the real-time CPU Utilization of the RDS instance, and then set up a custom CloudWatch dashboard to view the metrics.
- 4. ☐ D. Enable Enhanced Monitoring in RDS.

Correct Answer: – D

Explanation: – Amazon RDS provides metrics in real-time for the operating system (OS) that your DB instance runs on. You can view the metrics for your DB instance using the console or consume the Enhanced Monitoring JSON output from CloudWatch Logs in a monitoring system of your choice. By default, Enhanced Monitoring metrics are stored in the CloudWatch Logs for 30 days. To modify the amount of time the metrics are stored in the CloudWatch Logs, change the retention for the RDSOSMetrics log group in the CloudWatch console.

Take note that there are certain differences between CloudWatch and Enhanced Monitoring Metrics. CloudWatch gathers metrics about CPU utilization from the hypervisor for a DB instance, and Enhanced Monitoring gathers its metrics from an agent on the instance. As a result, you might find differences between the measurements, because the hypervisor layer performs a small amount of work. Hence, **enabling Enhanced Monitoring in RDS** is the correct answer in this specific scenario.

The differences can be greater if your DB instances use smaller instance classes, because then there are likely more virtual machines (VMs) that are managed by the hypervisor layer on a single physical instance. Enhanced Monitoring metrics are useful when you want to see how different processes or threads on a DB instance use the CPU.

Process List						
<input type="text" value="Filter process list"/>						
<div> < 1 2 > ⚙ </div>						
NAME ▼	VIRT ▼	RES ▼	CPU% ▼	MEM% ▼	VMLIMIT ▼	
▼ postgres [3181]†	283.55 MB	17.11 MB	0.02	1.72		
postgres: rdsadmin	384.7 MB	9.51 MB	0.02	0.95		
rdsadmin localhost(40156)						
idle [2953]†						

Using **Amazon CloudWatch to monitor the CPU Utilization of your database** is incorrect because although you can use this to monitor the CPU Utilization of your database instance, it does not provide the percentage of the CPU bandwidth and total memory consumed by each database process in your RDS instance. Take note that CloudWatch gathers metrics about CPU utilization from the hypervisor for a DB instance while RDS Enhanced Monitoring gathers its metrics from an agent on the instance.

The option that says: **Create a script that collects and publishes custom metrics to CloudWatch, which tracks the real-time CPU Utilization of the RDS instance and then set up a custom CloudWatch dashboard to view the metrics** is incorrect because although you can use Amazon CloudWatch Logs and CloudWatch dashboard to monitor the CPU Utilization of the database instance, using CloudWatch alone is still not enough to get the specific percentage of the CPU bandwidth and total memory consumed by each database processes. The data provided by CloudWatch is not as detailed as compared with the Enhanced Monitoring feature in RDS. Take note as well that you do not have direct access to the instances/servers of your RDS database instance, unlike with your EC2 instances where you can install a CloudWatch agent or a custom script to get CPU and memory utilization of your instance.

The option that says: **Check the CPU% and MEM% metrics which are readily available in the Amazon RDS console that shows the percentage of the CPU bandwidth and total memory consumed by each database process of your RDS instance** is incorrect because the CPU% and MEM% metrics are not readily available in the Amazon RDS console, which is contrary to what is being stated in this option.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Monitoring.OS.html#USER_Monitoring.OS.CloudWatchLogs

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/MonitoringOverview.html#monitoring-cloudwatch>

Question 23. An organization needs to provision a new Amazon EC2 instance with a persistent block storage volume to migrate data from its on-premises network to AWS. The required maximum performance for the storage volume is 64,000 IOPS.

In this scenario, which of the following can be used to fulfill this requirement?

- 1. ☐ A. Launch any type of Amazon EC2 instance and attach a Provisioned IOPS SSD EBS volume (io1) with 64,000 IOPS.
- 2. ☐ B. Launch an Amazon EFS file system and mount it to a Nitro-based Amazon EC2 instance and set the performance mode to Max I/O.
- 3. ☐ C. Launch a Nitro-based EC2 instance and attach a Provisioned IOPS SSD EBS volume (io1) with 64,000 IOPS.
- 4. ☐ D. Directly attach multiple Instance Store volumes in an EC2 instance to deliver maximum IOPS performance.

Correct Answer: – C

Explanation: – An **Amazon EBS volume** is a durable, block-level storage device that you can attach to your instances. After you attach a volume to an instance, you can use it as you would use a physical hard drive. EBS volumes are flexible.

The **AWS Nitro System** is the underlying platform for the latest generation of EC2 instances that enables AWS to innovate faster, further reduce the cost of the customers, and deliver added

benefits like increased security and new instance types.

	Solid-state drives (SSD)		
Volume type	General Purpose SSD (gp2)	Provisioned IOPS SSD	
		io2	io1
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	
Durability	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	99.999% durability (0.001% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)
Use cases	<ul style="list-style-type: none"> Recommended for most workloads System boot volumes Virtual desktops Low-latency interactive apps Development and test environments 	<ul style="list-style-type: none"> Critical business applications that require sustained IOPS performance, or more than 16,000 IOPS or 250 MB/s of throughput per volume Large database workloads, such as: <ul style="list-style-type: none"> MongoDB Cassandra Microsoft SQL Server MySQL PostgreSQL Oracle 	
Amazon EBS Multi-attach	Not supported	Not Supported	Supported
API name	gp2	io2	io1
Volume size	1 GiB - 16 TiB	4 GiB - 16 TiB	
Dominant performance	IOPS	IOPS	

Maximum IOPS and throughput are guaranteed only on Instances built on the Nitro System provisioned with more than 32,000

volume	
Max IOPS per instance ††	160,000
Max throughput per instance ††	4,750 MB/s

Amazon EBS is a persistent block storage volume. It can persist independently from the life of an instance. Since the scenario requires you to have an EBS volume with up to 64,000 IOPS, you have to launch a Nitro-based EC2 instance.

Hence, the correct answer in this scenario is: **Launch a Nitro-based EC2 instance and attach a Provisioned IOPS SSD EBS volume (io1) with 64,000 IOPS.**

The option that says: **Directly attach multiple Instance Store volumes in an EC2 instance to deliver maximum IOPS performance** is incorrect. Although an Instance Store is a block storage volume, it is not persistent and the data will be gone if the instance is restarted. An instance store provides temporary block-level storage for your instance. It means that the data in the instance store can be lost if the underlying disk drive fails, if the instance stops, and if the instance terminates.

The option that says: **Launch an Amazon EFS file system and mount it to a Nitro-based Amazon EC2 instance and set the performance mode to Max I/O** is incorrect. Although Amazon EFS can provide over 64,000 IOPS, this solution uses a file system and not a block storage volume which is what is asked in the scenario.

The option that says: **Launch an EC2 instance and attach an io1 EBS volume with 64,000 IOPS** is incorrect. In order to achieve the 64,000 IOPS for a provisioned IOPS SSD, you must provision a Nitro-based EC2 instance. The maximum IOPS and throughput are guaranteed only

on Instances built on the Nitro System provisioned with more than 32,000 IOPS. Other instances guarantee up to 32,000 IOPS only.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html#EBSVolumeTypes_piops

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

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html>

Question 24. An application hosted in EC2 consumes messages from an SQS queue and is integrated with SNS to send out an email to you once the process is complete. The Operations team received 5 orders but after a few hours, they saw 20 email notifications in their inbox.

Which of the following could be the possible culprit for this issue?

- 1. ☐ A. The web application is not deleting the messages in the SQS queue after it has processed them.
- 2. ☐ B. The web application is set to short polling so some messages are not being picked up
- 3. ☐ C. The web application does not have permission to consume messages in the SQS queue.
- 4. ☐ D. The web application is set for long polling so the messages are being sent twice.

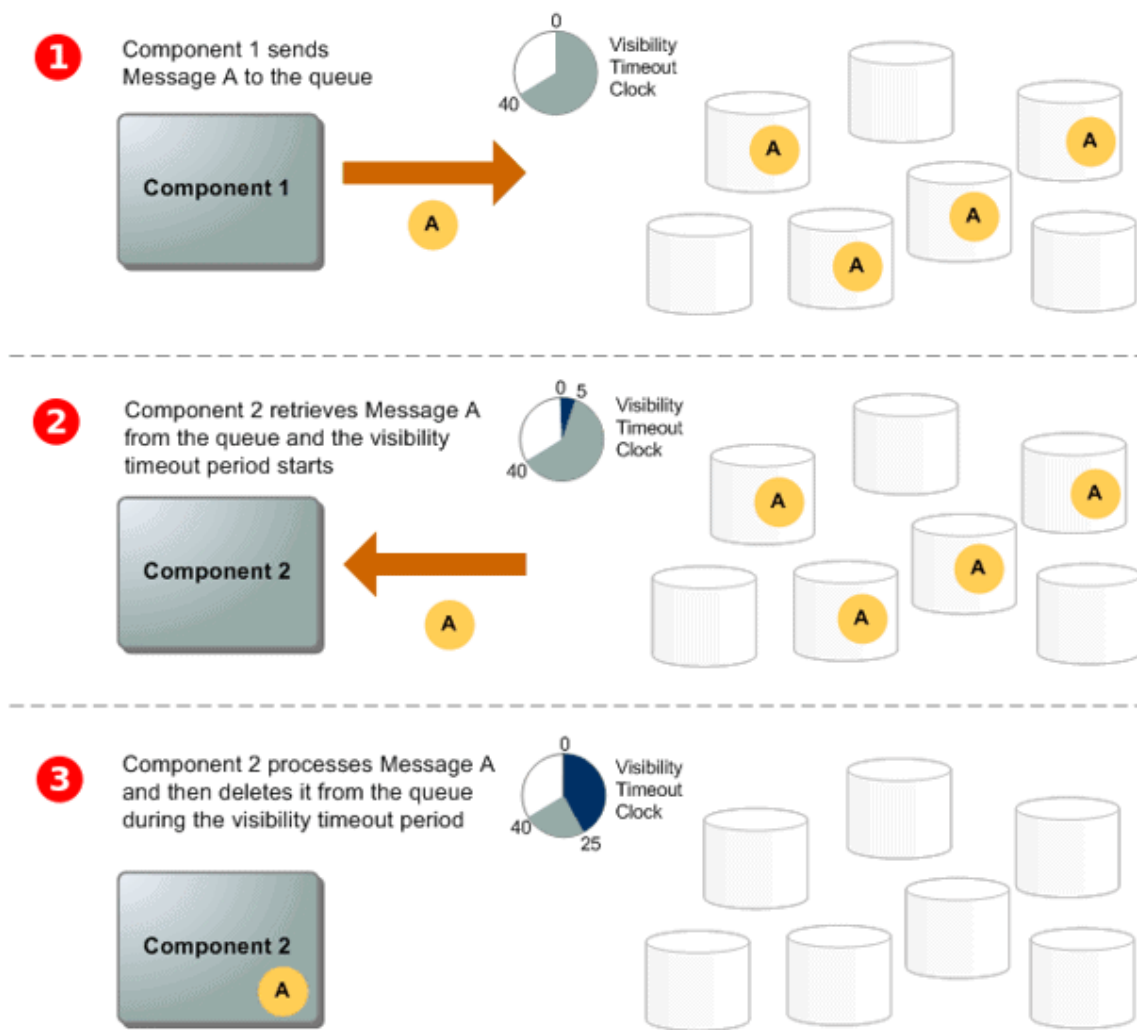
Correct Answer: – A

Explanation: – Always remember that the messages in the SQS queue will continue to exist even after the EC2 instance has processed it, until you delete that message. You have to ensure that you delete the message after processing to prevent the message from being received and processed again once the visibility timeout expires.

There are three main parts in a distributed messaging system:

1. The components of your distributed system (EC2 instances)
2. Your queue (distributed on Amazon SQS servers)
3. Messages in the queue.

You can set up a system which has several components that send messages to the queue and receive messages from the queue. The queue redundantly stores the messages across multiple Amazon SQS servers.



Refer to the third step of the SQS Message Lifecycle:

Component 1 sends Message A to a queue, and the message is distributed across the Amazon SQS servers redundantly.

When Component 2 is ready to process a message, it consumes messages from the queue, and Message A is returned. While Message A is being processed, it remains in the queue and isn't returned to subsequent receive requests for the duration of the visibility timeout.

Component 2 **deletes** Message A from the queue to prevent the message from being received and processed again once the visibility timeout expires.

The option that says: **The web application is set for long polling so the messages are being sent twice** is incorrect because long polling helps reduce the cost of using SQS by eliminating the number of empty responses (when there are no messages available for a ReceiveMessage request) and false empty responses (when messages are available but aren't included in a

response). Messages being sent twice in an SQS queue configured with long polling is quite unlikely.

The option that says: **The web application is set to short polling so some messages are not being picked up** is incorrect since you are receiving emails from SNS where messages are certainly being processed. Following the scenario, messages not being picked up won't result into 20 messages being sent to your inbox.

The option that says: **The web application does not have permission to consume messages in the SQS queue** is incorrect because not having the correct permissions would have resulted in a different response. The scenario says that messages were properly processed but there were over 20 messages that were sent, hence, there is no problem with the accessing the queue.

References:

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

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

Question 25. A popular social network is hosted in AWS and is using a DynamoDB table as its database. There is a requirement to implement a 'follow' feature where users can subscribe to certain updates made by a particular user and be notified via email. Which of the following is the most suitable solution that you should implement to meet the requirement?

- 1. ☐ A. Create a Lambda function that uses DynamoDB Streams Kinesis Adapter which will fetch data from the DynamoDB Streams endpoint. Set up an SNS Topic that will notify the subscribers via email when there is an update made by a particular user.
- 2. ☐ B. Enable DynamoDB Stream and create an AWS Lambda trigger, as well as the IAM role which contains all of the permissions that the Lambda function will need at runtime. The data from the stream record will be processed by the Lambda function which will then publish a message to SNS Topic that will notify the subscribers via email.
- 3. ☐ C. Using the Kinesis Client Library (KCL), write an application that leverages on DynamoDB Streams Kinesis Adapter that will fetch data from the DynamoDB Streams endpoint. When there are updates made by a particular user, notify the subscribers via email using SNS.
- 4. ☐ D. Set up a DAX cluster to access the source DynamoDB table. Create a new DynamoDB trigger and a Lambda function. For every update made in the user data, the trigger will send data to the Lambda function which will then notify the subscribers via email using SNS.

Correct Answer: – B

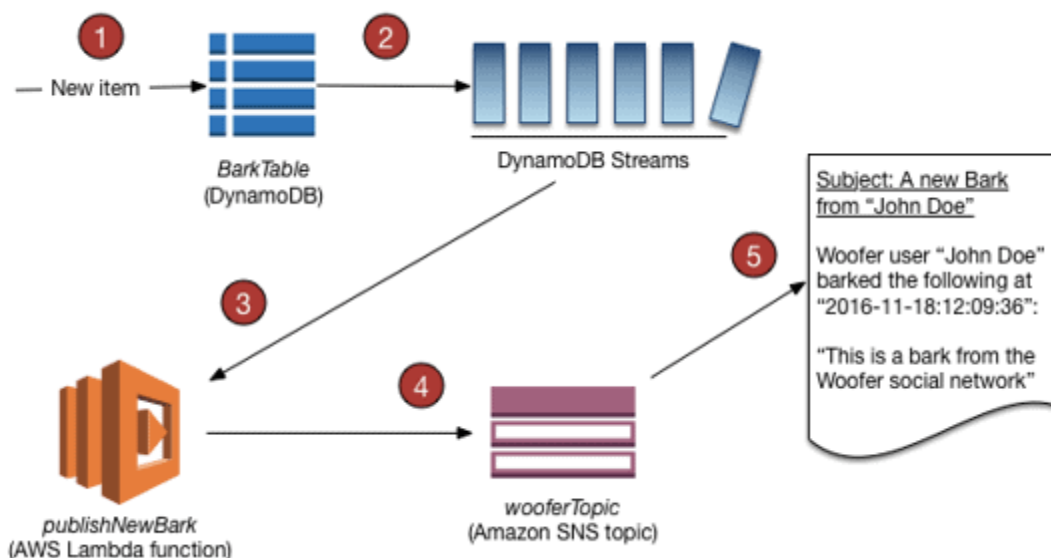
Explanation: – A **DynamoDB stream** is an ordered flow of information about changes to items in an Amazon DynamoDB table. When you enable a stream on a table, DynamoDB captures information about every modification to data items in the table.

Whenever an application creates, updates, or deletes items in the table, DynamoDB Streams writes a stream record with the primary key attribute(s) of the items that were modified. A *stream record* contains information about a data modification to a single item in a DynamoDB table. You can configure the stream so that the stream records capture additional information, such as the “before” and “after” images of modified items.

Amazon DynamoDB is integrated with AWS Lambda so that you can create *triggers*—pieces of code that automatically respond to events in DynamoDB Streams. With triggers, you can build applications that react to data modifications in DynamoDB tables.

If you enable DynamoDB Streams on a table, you can associate the stream ARN with a Lambda function that you write. Immediately after an item in the table is modified, a new record appears in the table’s stream. AWS Lambda polls the stream and invokes your Lambda function synchronously when it detects new stream records. The Lambda function can perform any actions you specify, such as sending a notification or initiating a workflow.

Hence, the correct answer in this scenario is the option that says: **Enable DynamoDB Stream and create an AWS Lambda trigger, as well as the IAM role which contains all of the permissions that the Lambda function will need at runtime. The data from the stream record will be processed by the Lambda function which will then publish a message to SNS Topic that will notify the subscribers via email.**



The option that says: **Using the Kinesis Client Library (KCL), write an application that leverages on DynamoDB Streams Kinesis Adapter that will fetch data from the DynamoDB Streams endpoint. When there are updates made by a particular user, notify the**

subscribers via email using SNS is incorrect because although this is a valid solution, it is missing a vital step which is to enable DynamoDB Streams. With the DynamoDB Streams Kinesis Adapter in place, you can begin developing applications via the KCL interface, with the API calls seamlessly directed at the DynamoDB Streams endpoint. Remember that the DynamoDB Stream feature is not enabled by default.

The option that says: **Create a Lambda function that uses DynamoDB Streams Kinesis Adapter which will fetch data from the DynamoDB Streams endpoint. Set up an SNS Topic that will notify the subscribers via email when there is an update made by a particular user** is incorrect because just like in the above, you have to manually enable DynamoDB Streams first before you can use its endpoint.

The option that says: **Set up a DAX cluster to access the source DynamoDB table. Create a new DynamoDB trigger and a Lambda function. For every update made in the user data, the trigger will send data to the Lambda function which will then notify the subscribers via email using SNS** is incorrect because the DynamoDB Accelerator (DAX) feature is primarily used to significantly improve the in-memory read performance of your database, and not to capture the time-ordered sequence of item-level modifications. You should use DynamoDB Streams in this scenario instead.

References:

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

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.Tutorial.html>

Question 26. An application is hosted in an AWS Fargate cluster that runs a batch job whenever an object is loaded on an Amazon S3 bucket. The minimum number of ECS Tasks is initially set to 1 to save on costs, and it will only increase the task count based on the new objects uploaded on the S3 bucket. Once processing is done, the bucket becomes empty and the ECS Task count should be back to 1.

Which is the most suitable option to implement with the LEAST amount of effort?

- 1. ☐ A. Set up a CloudWatch Event rule to detect S3 object PUT operations and set the target to a Lambda function that will run Amazon ECS API command to increase the number of tasks on ECS. Create another rule to detect S3 DELETE operations and run the Lambda function to reduce the number of ECS tasks.
- 2. ☐ B. Set up an alarm in CloudWatch to monitor CloudTrail since this S3 object-level operations are recorded on CloudTrail. Set two alarm actions to update ECS task count to scale-out/scale-in depending on the S3 event.
- 3. ☐ C. Set up a CloudWatch Event rule to detect S3 object PUT operations and set the target to the ECS cluster with the increased number of tasks. Create another rule to detect S3 DELETE operations and set the target to the ECS Cluster with 1 as the Task count.

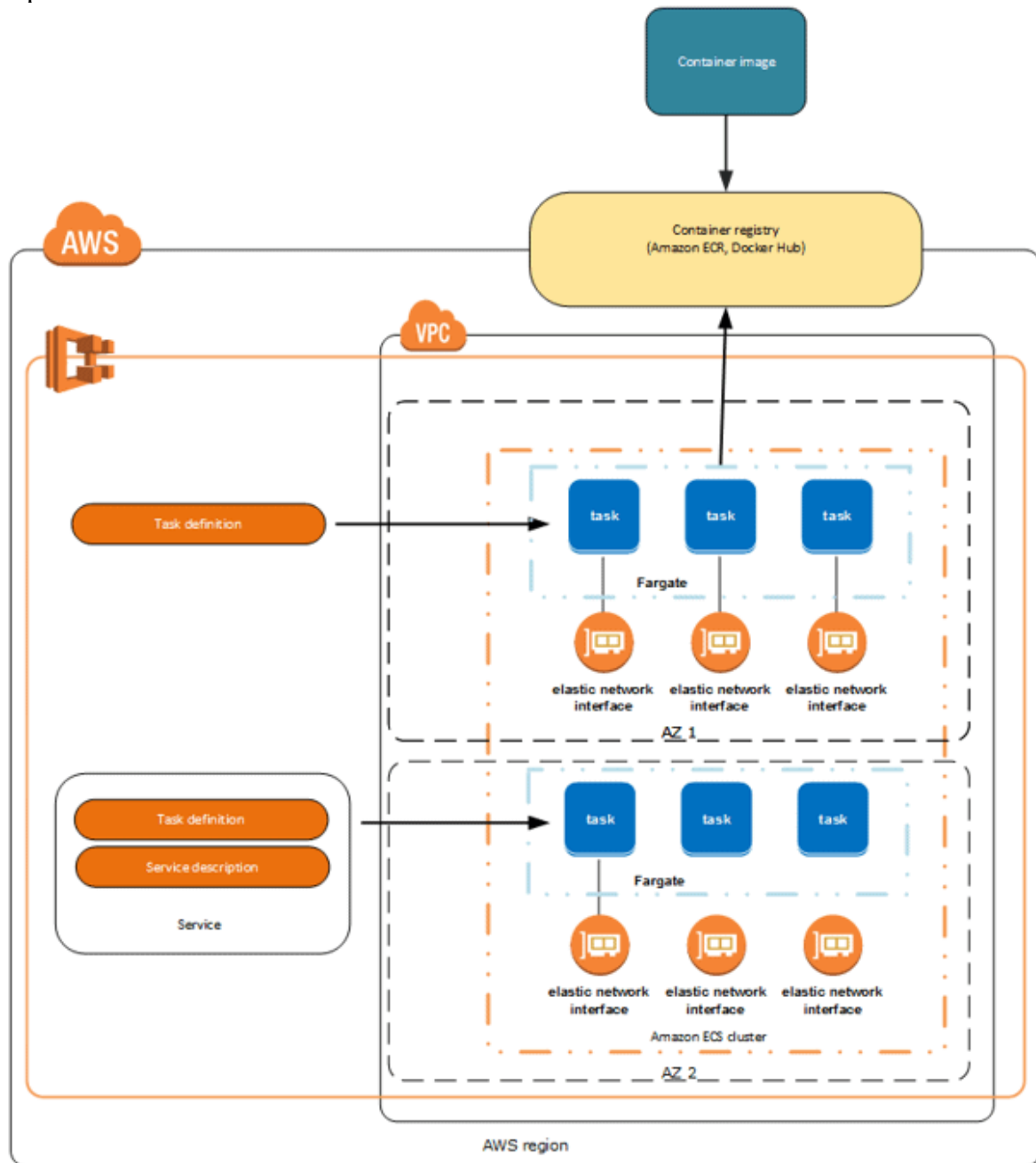
- 4. ☐ D. Set up an alarm in CloudWatch to monitor CloudTrail since the S3 object-level operations are recorded on CloudTrail. Create two Lambda functions for increasing/decreasing the ECS task count. Set these as respective targets for the CloudWatch Alarm depending on the S3 event.

Correct Answer: – C

Explanation: – You can use CloudWatch Events to run Amazon ECS tasks when certain AWS events occur. You can set up a CloudWatch Events rule that runs an Amazon ECS task whenever a file is uploaded to a certain Amazon S3 bucket using the Amazon S3 PUT operation. You can also declare a reduced number of ECS tasks whenever a file is deleted on the S3 bucket using the DELETE operation.

First, you must create a CloudWatch Events rule for the S3 service that will watch for object-level operations – PUT and DELETE objects. For object-level operations, it is required to create a CloudTrail trail first. On the Targets section, select the “ECS task” and input the needed values such as the cluster name, task definition and the task count. You need two rules – one for the

scale-up and another for the scale-down of the ECS task count.



Hence, the correct answer is: ***Set up a CloudWatch Event rule to detect S3 object PUT operations and set the target to the ECS cluster with the increased number of tasks. Create another rule to detect S3 DELETE operations and set the target to the ECS Cluster with 1 as the Task count.***

The option that says: ***Set up a CloudWatch Event rule to detect S3 object PUT operations and set the target to a Lambda function that will run Amazon ECS API command to increase the number of tasks on ECS. Create another rule to detect S3 DELETE operations and run the Lambda function to reduce the number of ECS tasks*** is incorrect because although this solution

meets the requirement, creating your own Lambda function for this scenario is not really necessary. It is much simpler to control ECS task directly as target for the CloudWatch Event rule. Take note that the scenario asks for a solution that is the easiest to implement.

The option that says: *Set up an alarm in CloudWatch to monitor CloudTrail since the S3 object-level operations are recorded on CloudTrail. Create two Lambda functions for increasing/decreasing the ECS task count. Set these as respective targets for the CloudWatch Alarm depending on the S3 event* is incorrect because using CloudTrail, CloudWatch Alarm, and two Lambda functions creates an unnecessary complexity to what you want to achieve. CloudWatch Events can directly target an ECS task on the Targets section when you create a new rule.

The option that says: *Set up an alarm in CloudWatch to monitor CloudTrail since this S3 object-level operations are recorded on CloudTrail. Set two alarm actions to update ECS task count to scale-out/scale-in depending on the S3 event* is incorrect because you can't directly set CloudWatch Alarms to update the ECS task count. You have to use CloudWatch Events instead.

References:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/CloudWatch-Events-tutorial-ECS.html>

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/Create-CloudWatch-Events-Rule.html>

Question 27. A cryptocurrency trading platform is using an API built in AWS Lambda and API Gateway. Due to the recent news and rumors about the upcoming price surge of Bitcoin, Ethereum and other cryptocurrencies, it is expected that the trading platform would have a significant increase in site visitors and new users in the coming days ahead.

In this scenario, how can you protect the backend systems of the platform from traffic spikes?

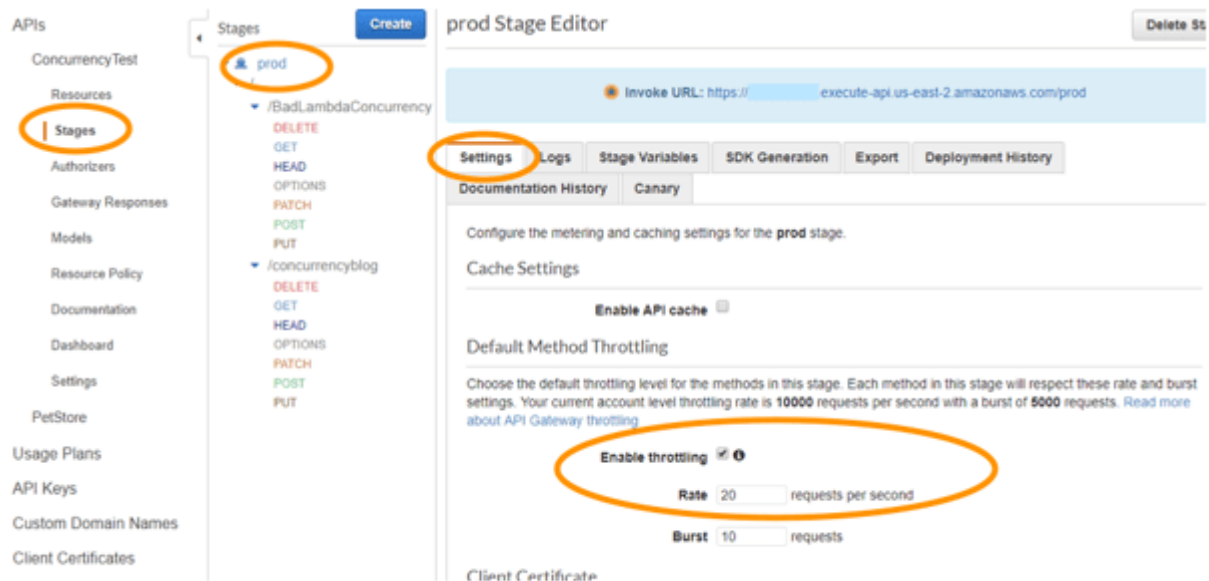
- 1. ☐ A. Switch from using AWS Lambda and API Gateway to a more scalable and highly available architecture using EC2 instances, ELB, and Auto Scaling.
- 2. ☐ B. Use CloudFront in front of the API Gateway to act as a cache.
- 3. ☐ C. Enable throttling limits and result caching in API Gateway.
- 4. ☐ D. Move the Lambda function in a VPC.

Correct Answer: – C

Explanation: – Amazon API Gateway provides throttling at multiple levels including global and by service call. Throttling limits can be set for standard rates and bursts. For example, API owners can set a rate limit of 1,000 requests per second for a specific method in their REST APIs, and also configure Amazon API Gateway to handle a burst of 2,000 requests per second

for a few seconds. Amazon API Gateway tracks the number of requests per second. Any request over the limit will receive a 429 HTTP response. The client SDKs generated by Amazon API Gateway retry calls automatically when met with this response. Hence, **enabling throttling limits and result caching in API Gateway** is the correct answer.

You can add caching to API calls by provisioning an Amazon API Gateway cache and specifying its size in gigabytes. The cache is provisioned for a specific stage of your APIs. This improves performance and reduces the traffic sent to your back end. Cache settings allow you to control the way the cache key is built and the time-to-live (TTL) of the data stored for each method. Amazon API Gateway also exposes management APIs that help you invalidate the cache for each stage.



The option that says: **Switch from using AWS Lambda and API Gateway to a more scalable and highly available architecture using EC2 instances, ELB, and Auto Scaling** is incorrect since there is no need to transfer your applications to other services.

Using CloudFront in front of the API Gateway to act as a cache is incorrect because CloudFront only speeds up content delivery which provides a better latency experience for your users. It does not help much for the backend.

Moving the Lambda function in a VPC is incorrect because this answer is irrelevant to what is being asked. A VPC is your own virtual private cloud where you can launch AWS services.

Reference:

<https://aws.amazon.com/api-gateway/faqs/>

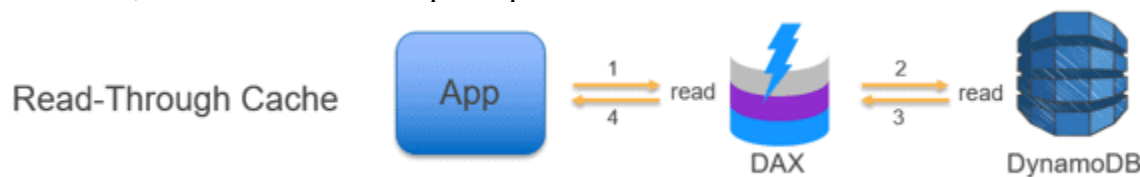
Question 28. A popular mobile game uses CloudFront, Lambda, and DynamoDB for its backend services. The player data is persisted on a DynamoDB table and the static assets are distributed by CloudFront. However, there are a lot of complaints that saving and retrieving player information is taking a lot of time.

To improve the game's performance, which AWS service can you use to reduce DynamoDB response times from milliseconds to microseconds?

- 1. ☐ A. Amazon DynamoDB Accelerator (DAX)
- 2. ☐ B. Amazon ElastiCache
- 3. ☐ C. AWS Device Farm
- 4. ☐ D. DynamoDB Auto Scaling

Correct Answer: – A

Explanation: – Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache that can reduce Amazon DynamoDB response times from milliseconds to microseconds, even at millions of requests per second.



Amazon ElastiCache is incorrect because although you may use ElastiCache as your database cache, it will not reduce the DynamoDB response time from milliseconds to microseconds as compared with DynamoDB DAX.

AWS Device Farm is incorrect because this is an app testing service that lets you test and interact with your Android, iOS, and web apps on many devices at once, or reproduce issues on a device in real time.

DynamoDB Auto Scaling is incorrect because this is primarily used to automate capacity management for your tables and global secondary indexes.

References:

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

<https://aws.amazon.com/device-farm>

Question 29. A company hosted an e-commerce website on an Auto Scaling group of EC2 instances behind an Application Load Balancer. The Solutions Architect noticed that the website is receiving a large number of illegitimate external requests from multiple systems with IP addresses that constantly change. To resolve the performance issues, the Solutions

Architect must implement a solution that would block the illegitimate requests with minimal impact on legitimate traffic.

Which of the following options fulfills this requirement?

- 1. ☐ A. Create a regular rule in AWS WAF and associate the web ACL to an Application Load Balancer.
- 2. ☐ B. Create a custom rule in the security group of the Application Load Balancer to block the offending requests.
- 3. ☐ C. Create a rate-based rule in AWS WAF and associate the web ACL to an Application Load Balancer.
- 4. ☐ D. Create a custom network ACL and associate it with the subnet of the Application Load Balancer to block the offending requests.

Correct Answer: – C

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

Rule Validate

Name
tutorialsdojo-rule
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Type
Rate-based rule

Request rate details

Rate limit
The rate limit is the maximum number of requests from a single IP address that are allowed in a five-minute period. This value is continually evaluated, and requests will be blocked once this limit is reached. The IP address is automatically unblocked after it falls below the limit.
100
Rate limit must be between 100 and 20,000,000.

IP address to use for rate limiting
When a request comes through a CDN or other proxy network, the source IP address identifies the proxy and the original IP address is sent in a header. Use caution with the option, IP address in header, because headers can be handled inconsistently by proxies and they can be modified to bypass inspection.

☒ Source IP address
☐ IP address in header

Criteria to count request towards rate limit
Choose whether to count all requests for each IP address or to only count requests that match the criteria of a rule statement.

☒ Consider all requests
☐ Only consider requests that match the criteria in a rule statement

A rate-based rule tracks the rate of requests for each originating IP address and triggers the rule action on IPs with rates that go over a limit. You set the limit as the number of requests per 5-minute time span. You can use this type of rule to put a temporary block on requests from an IP address that's sending excessive requests.

Based on the given scenario, the requirement is to limit the number of requests from the illegitimate requests without affecting the genuine requests. To accomplish this requirement, you can use AWS WAF web ACL. There are two types of rules in creating your own web ACL rule: regular and rate-based rules. You need to select the latter to add a rate limit to your web ACL. After creating the web ACL, you can associate it with ALB. When the rule action triggers, AWS WAF applies the action to additional requests from the IP address until the request rate falls below the limit.

Hence, the correct answer is: **Create a rate-based rule in AWS WAF and associate the web ACL to an Application Load Balancer.**

The option that says: **Create a regular rule in AWS WAF and associate the web ACL to an Application Load Balancer** is incorrect because a regular rule only matches the statement defined in the rule. If you need to add a rate limit to your rule, you should create a rate-based rule.

The option that says: **Create a custom network ACL and associate it with the subnet of the Application Load Balancer to block the offending requests** is incorrect. Although NACLs can help you block incoming traffic, this option wouldn't be able to limit the number of requests from a single IP address that is dynamically changing.

The option that says: **Create a custom rule in the security group of the Application Load Balancer to block the offending requests** is incorrect because the security group can only allow incoming traffic. Remember that you can't deny traffic using security groups. In addition, it is not capable of limiting the rate of traffic to your application unlike AWS WAF.

References:

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-rate-based.html>

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

Question 30. An AI-powered Forex trading application consumes thousands of data sets to train its machine learning model. The application's workload requires a high-performance, parallel hot storage to process the training datasets concurrently. It also needs cost-effective cold storage to archive those datasets that yield low profit.

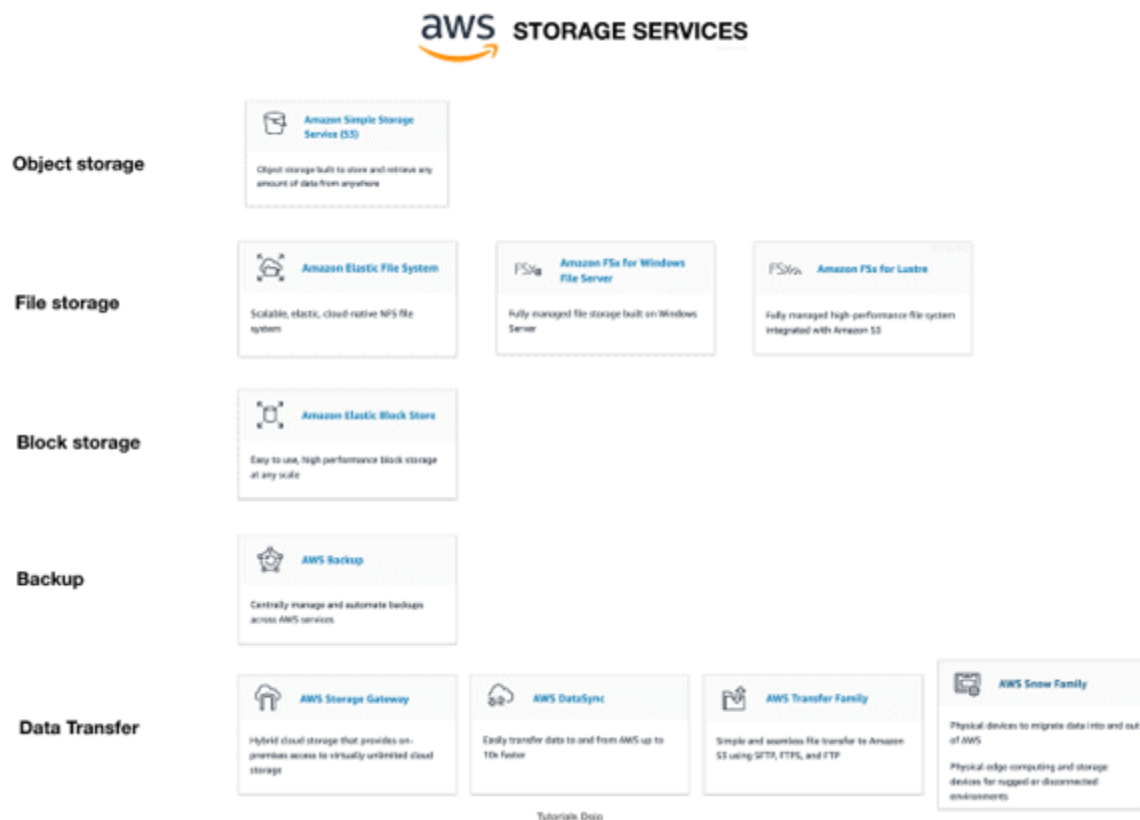
Which of the following Amazon storage services should the developer use?

- 1. ☐ A. Use Amazon Elastic File System and Amazon S3 for hot and cold storage respectively.
- 2. ☐ B. Use Amazon FSx For Windows File Server and Amazon S3 for hot and cold storage respectively.
- 3. ☐ C. Use Amazon FSx For Lustre and Amazon S3 for hot and cold storage respectively.
- 4. ☐ D. Use Amazon FSx For Lustre and Amazon EBS Provisioned IOPS SSD (io1) volumes for hot and cold storage respectively.

Correct Answer: – C

Explanation: – Hot storage refers to the storage that keeps frequently accessed data (hot data). **Warm storage** refers to the storage that keeps less frequently accessed data (warm data). **Cold storage** refers to the storage that keeps rarely accessed data (cold data). In terms of

pricing, the colder the data, the cheaper it is to store, and the costlier it is to access when needed.



Amazon FSx For Lustre is a high-performance file system for fast processing of workloads. Lustre is a popular open-source **parallel file system** which stores data across multiple network file servers to maximize performance and reduce bottlenecks.

Amazon FSx for Windows File Server is a fully managed Microsoft Windows file system with full support for the SMB protocol, Windows NTFS, Microsoft Active Directory (AD) Integration.

Amazon Elastic File System is a fully managed file storage service that makes it easy to set up and scale file storage in the Amazon Cloud.

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance. S3 offers different storage tiers for different use cases (frequently accessed data, infrequently accessed data, and rarely accessed data).

The question has two requirements:

High-performance, parallel hot storage to process the training datasets concurrently.

Cost-effective cold storage to keep the archived datasets that are accessed infrequently.

In this case, we can use **Amazon FSx For Lustre** for the first requirement, as it provides a high-performance, parallel file system for hot data. On the second requirement, we can use Amazon S3 for storing the cold data. Amazon S3 supports a cold storage system via Amazon S3 Glacier / Glacier Deep Archive.

Hence, the correct answer is **Use Amazon FSx For Lustre and Amazon S3 for hot and cold storage respectively**.

Using Amazon FSx For Lustre and Amazon EBS Provisioned IOPS SSD (io1) volumes for hot and cold storage respectively is incorrect because the Provisioned IOPS SSD (io1) volumes are designed as a hot storage to meet the needs of I/O-intensive workloads. EBS has a storage option called Cold HDD but it is not used for storing cold data. In addition, EBS Cold HDD is a lot more expensive than using Amazon S3 Glacier / Glacier Deep Archive.

Using Amazon Elastic File System and Amazon S3 for hot and cold storage respectively is incorrect because although EFS supports concurrent access to data, it does not have the high-performance ability that is required for machine learning workloads.

Using Amazon FSx For Windows File Server and Amazon S3 for hot and cold storage respectively is incorrect because Amazon FSx For Windows File Server does not have a parallel file system, unlike Lustre.

References:

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

<https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-storage-optimization/aws-storage-services.html>

<https://aws.amazon.com/blogs/startups/picking-the-right-data-store-for-your-workload/>

Question 31. You are using a combination of API Gateway and Lambda for the web services of your online web portal that is being accessed by hundreds of thousands of clients each day. Your company will be announcing a new revolutionary product and it is expected that your web portal will receive a massive number of visitors all around the globe. How can you protect your backend systems and applications from traffic spikes?

- 1. ☐ A. API Gateway will automatically scale and handle massive traffic spikes so you do not have to do anything.
- 2. ☐ B. Manually upgrade the EC2 instances being used by API Gateway
- 3. ☐ C. Deploy Multi-AZ in API Gateway with Read Replica
- 4. ☐ D. Use throttling limits in API Gateway

Correct Answer: – D

Explanation: – **Amazon API Gateway** provides throttling at multiple levels including global and by a service call. Throttling limits can be set for standard rates and bursts. For example, API owners can set a rate limit of 1,000 requests per second for a specific method in their REST APIs, and also configure Amazon API Gateway to handle a burst of 2,000 requests per second for a few seconds.

Amazon API Gateway tracks the number of requests per second. Any requests over the limit will receive a 429 HTTP response. The client SDKs generated by Amazon API Gateway retry calls automatically when met with this response.

The option that says: **API Gateway will automatically scale and handle massive traffic spikes so you do not have to do anything** is incorrect because although it can scale using AWS Edge locations, you still need to configure the throttling to further manage the bursts of your APIs.

Manually upgrading the EC2 instances being used by API Gateway is incorrect because API Gateway is a fully managed service and hence, you do not have access to its underlying resources.

Deploying Multi-AZ in API Gateway with Read Replica is incorrect because RDS has Multi-AZ and Read Replica capabilities, and not API Gateway.

Reference:

https://aws.amazon.com/api-gateway/faqs/#Throttling_and_Caching

Question 32. You are leading a software development team which uses serverless computing with AWS Lambda to build and run applications without having to set up or manage servers. You have a Lambda function that connects to a MongoDB Atlas, which is a popular Database as a Service (DBaaS) platform and also uses a third-party API to fetch certain data for your application. You instructed one of your junior developers to create the environment variables for the MongoDB database hostname, username, and password as well as the API credentials that will be used by the Lambda function for DEV, SIT, UAT and PROD environments.

Considering that the Lambda function is storing sensitive database and API credentials, how can you secure this information to prevent other developers in your team, or anyone, from seeing these credentials in plain text? Select the best option that provides the maximum security.

- 1. ☐ A. There is no need to do anything because, by default, AWS Lambda already encrypts the environment variables using the AWS Key Management Service.
- 2. ☐ B. Enable SSL encryption that leverages on AWS CloudHSM to store and encrypt the sensitive information.
- 3. ☐ C. Create a new KMS key and use it to enable encryption helpers that leverage on AWS Key Management Service to store and encrypt the sensitive information.

- 4. D. AWS Lambda does not provide encryption for the environment variables. Deploy your code to an EC2 instance instead.

Correct Answer: – C

Explanation: – When you create or update Lambda functions that use environment variables, AWS Lambda encrypts them using the AWS Key Management Service. When your Lambda function is invoked, those values are decrypted and made available to the Lambda code.

The first time you create or update Lambda functions that use environment variables in a region, a default service key is created for you automatically within AWS KMS. This key is used to encrypt environment variables. However, if you wish to use encryption helpers and use KMS to encrypt environment variables after your Lambda function is created, you must create your own AWS KMS key and choose it instead of the default key. The default key will give errors when chosen. Creating your own key gives you more flexibility, including the ability to create, rotate, disable, and define access controls, and to audit the encryption keys used to protect your data.

The option that says: **There is no need to do anything because, by default, AWS Lambda already encrypts the environment variables using the AWS Key Management Service** is incorrect because although Lambda encrypts the environment variables in your function by default, the sensitive information would still be visible to other users who have access to the Lambda console. This is because Lambda uses a default KMS key to encrypt the variables, which is usually accessible by other users. The best option in this scenario is to use encryption helpers to secure your environment variables.

The option that says: **Enable SSL encryption that leverages on AWS CloudHSM to store and encrypt the sensitive information** is also incorrect since enabling SSL would encrypt data only when in-transit. Your other teams would still be able to view the plaintext at-rest. Use AWS KMS instead.

The option that says: **AWS Lambda does not provide encryption for the environment variables. Deploy your code to an EC2 instance instead** is incorrect since, as mentioned, Lambda does provide encryption functionality of environment variables.

References:

https://docs.aws.amazon.com/lambda/latest/dg/env_variables.html#env_encrypt

https://docs.aws.amazon.com/lambda/latest/dg/tutorial-env_console.html

Question 33. An online medical system hosted in AWS stores sensitive Personally Identifiable Information (PII) of the users in an Amazon S3 bucket. Both the master keys and the unencrypted data should never be sent to AWS to comply with the strict compliance and regulatory requirements of the company.

Which S3 encryption technique should the Architect use?

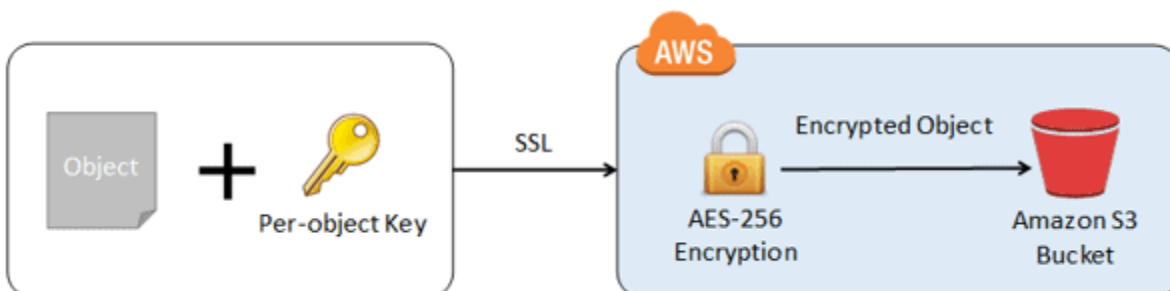
- 1. ☐ A. Use S3 client-side encryption with a client-side master key.
- 2. ☐ B. Use S3 server-side encryption with customer provided key.
- 3. ☐ C. Use S3 server-side encryption with a KMS managed key.
- 4. ☐ D. Use S3 client-side encryption with a KMS-managed customer master key.

Correct Answer: – A

Explanation: – **Client-side encryption** is the act of encrypting data before sending it to Amazon S3. To enable client-side encryption, you have the following options:

- Use an AWS KMS-managed customer master key.
- Use a client-side master key.

When using an AWS KMS-managed customer master key to enable client-side data encryption, you provide an AWS KMS customer master key ID (CMK ID) to AWS. On the other hand, when you use client-side master key for client-side data encryption, your client-side master keys and your unencrypted data are never sent to AWS. It's important that you safely manage your encryption keys because if you lose them, you can't decrypt your data.



This is how client-side encryption using client-side master key works:

When uploading an object – You provide a client-side master key to the Amazon S3 encryption client. The client uses the master key only to encrypt the data encryption key that it generates randomly. The process works like this:

1. The Amazon S3 encryption client generates a one-time-use symmetric key (also known as a data encryption key or data key) locally. It uses the data key to encrypt the data of a single Amazon S3 object. The client generates a separate data key for each object.
2. The client encrypts the data encryption key using the master key that you provide. The client uploads the encrypted data key and its material description as part of the object metadata. The client uses the material description to determine which client-side master key to use for decryption.
3. The client uploads the encrypted data to Amazon S3 and saves the encrypted data key as object metadata (x-amz-meta-x-amz-key) in Amazon S3.

When downloading an object – The client downloads the encrypted object from Amazon S3. Using the material description from the object's metadata, the client determines which master key to use to decrypt the data key. The client uses that master key to decrypt the data key and then uses the data key to decrypt the object.

Hence, the correct answer is to **use S3 client-side encryption with a client-side master key**.

Using S3 client-side encryption with a KMS-managed customer master key is incorrect because in client-side encryption with a KMS-managed customer master key, you provide an AWS KMS customer master key ID (CMK ID) to AWS. The scenario clearly indicates that both the master keys and the unencrypted data should never be sent to AWS.

Using S3 server-side encryption with a KMS managed key is incorrect because the scenario mentioned that the unencrypted data should never be sent to AWS, which means that you have to use client-side encryption in order to encrypt the data first before sending to AWS. In this way, you can ensure that there is no unencrypted data being uploaded to AWS. In addition, the master key used by Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS) is uploaded and managed by AWS, which directly violates the requirement of not uploading the master key.

Using S3 server-side encryption with customer provided key is incorrect because just as mentioned above, you have to use client-side encryption in this scenario instead of server-side encryption. For the S3 server-side encryption with customer-provided key (SSE-C), you actually provide the encryption key as part of your request to upload the object to S3. Using this key, Amazon S3 manages both the encryption (as it writes to disks) and decryption (when you access your objects).

References:

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

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

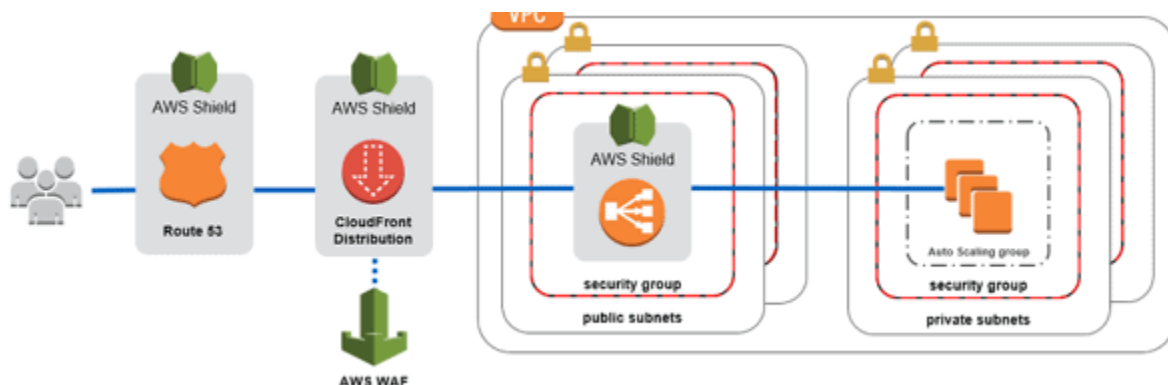
Question 34. You have identified a series of DDoS attacks while monitoring your VPC. As the Solutions Architect, you are responsible for fortifying your current cloud infrastructure to protect the data of your clients.

Which of the following is the most suitable solution to mitigate these kinds of attacks?

- 1. ☐ A. A combination of Security Groups and Network Access Control Lists to only allow authorized traffic to access your VPC.
- 2. ☐ B. Set up a web application firewall using AWS WAF to filter, monitor, and block HTTP traffic.
- 3. ☐ C. Use AWS Shield Advanced to detect and mitigate DDoS attacks.
- 4. ☐ D. Using the AWS Firewall Manager, set up a security layer that will prevent SYN floods, UDP reflection attacks, and other DDoS attacks.

Correct Answer: – C

Explanation: – For higher levels of protection against attacks targeting your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, and Amazon Route 53 resources, you can subscribe to AWS Shield Advanced. In addition to the network and transport layer protections that come with Standard, AWS Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF, a web application firewall.



AWS Shield Advanced also gives you 24×7 access to the AWS DDoS Response Team (DRT) and protection against DDoS related spikes in your Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing(ELB), Amazon CloudFront, and Amazon Route 53 charges.

Hence, the correct answer is: **Use AWS Shield Advanced to detect and mitigate DDoS attacks.**

The option that says: **Using the AWS Firewall Manager, set up a security layer that will prevent SYN floods, UDP reflection attacks and other DDoS attacks** is incorrect because the AWS Firewall Manager is mainly used to simplify your AWS WAF administration and maintenance tasks across multiple accounts and resources. It does not protect your VPC against DDoS attacks.

The option that says: **Set up a web application firewall using AWS WAF to filter, monitor, and block HTTP traffic** is incorrect because even though AWS WAF can help you block common attack patterns to your VPC such as SQL injection or cross-site scripting, this is still not enough to withstand DDoS attacks. It is better to use AWS Shield in this scenario.

The option that says: **A combination of Security Groups and Network Access Control Lists to only allow authorized traffic to access your VPC** is incorrect because although using a combination of Security Groups and NACLs are valid to provide security to your VPC, this is not enough to mitigate a DDoS attack. You should use AWS Shield for better security protection.

References:

https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

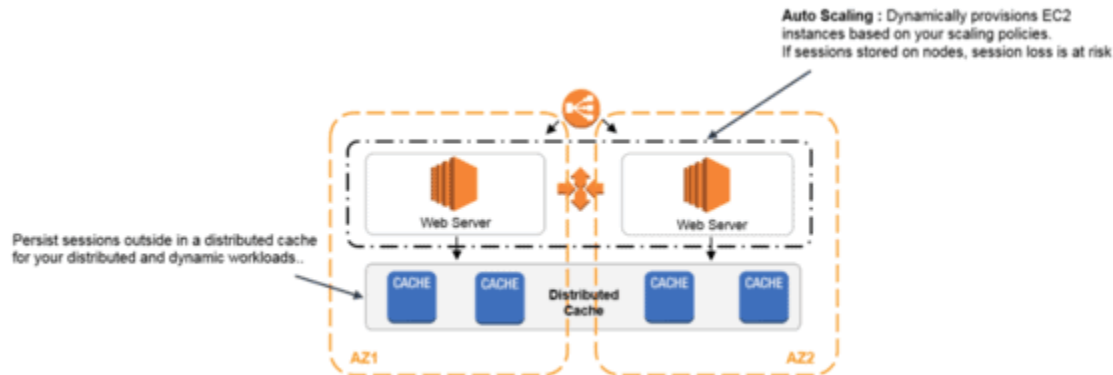
<https://aws.amazon.com/shield/>

Question 35. You are working for a large financial company as an IT consultant. Your role is to help their development team to build a highly available web application using stateless web servers. In this scenario, which AWS services are suitable for storing session state data? (Select TWO.)

- 1. ☐ A. RDS
- 2. ☐ B. ElastiCache
- 3. ☐ C. Glacier
- 4. ☐ D. Redshift Spectrum
- 5. ☐ E. DynamoDB

Correct Answer: – B, E

Explanation: – DynamoDB and ElastiCache are the correct answers. You can store session state data on both DynamoDB and ElastiCache. These AWS services provide high-performance storage of key-value pairs which can be used to build a highly available web application.



Redshift

Spectrum is incorrect since this is a data warehousing solution where you can directly query data from your data warehouse. Redshift is not suitable for storing session state, but more on analytics and OLAP processes.

RDS is incorrect as well since this is a relational database solution of AWS. This relational storage type might not be the best fit for session states, and it might not provide the performance you need compared to DynamoDB for the same cost.

S3 Glacier is incorrect as well since this is a low-cost cloud storage service for data archiving and long-term backup. The archival and retrieval speeds of Glacier is too slow for handling session states.

References:

<https://aws.amazon.com/caching/database-caching/>

<https://aws.amazon.com/caching/session-management/>

Question 36. A tech company that you are working for has undertaken a Total Cost Of Ownership (TCO) analysis evaluating the use of Amazon S3 versus acquiring more storage hardware. The result was that all 1200 employees would be granted access to use Amazon S3 for storage of their personal documents.

Which of the following will you need to consider so you can set up a solution that incorporates single sign-on feature from your corporate AD or LDAP directory and also restricts access for each individual user to a designated user folder in an S3 bucket? (Select TWO.)

1. ☐ A. Set up a matching IAM user for each of the 1200 users in your corporate directory that needs access to a folder in the S3 bucket.
2. ☐ B. Configure an IAM role and an IAM Policy to access the bucket.
3. ☐ C. Set up a Federation proxy or an Identity provider and use AWS Security Token Service to generate temporary tokens.

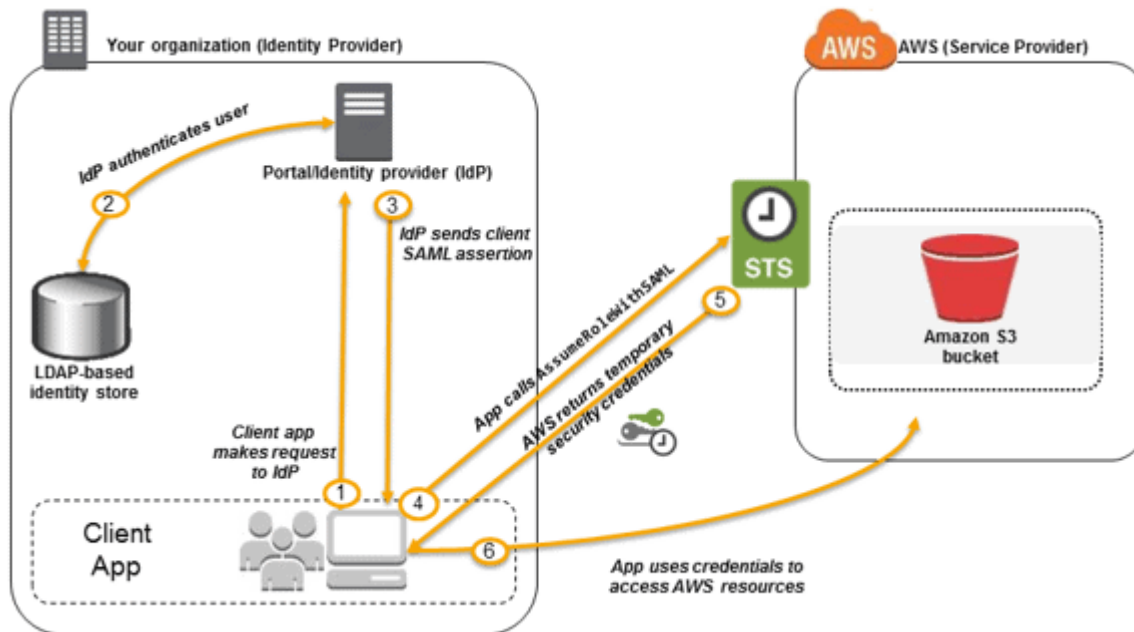
- 4. ☐ D. Map each individual user to a designated user folder in S3 using Amazon WorkDocs to access their personal documents.
- 5. ☐ E. Use 3rd party Single Sign-On solutions such as Atlassian Crowd, OKTA, OneLogin and many others.

Correct Answer: – B, C

Explanation: – The question refers to one of the common scenarios for temporary credentials in AWS. Temporary credentials are useful in scenarios that involve identity federation, delegation, cross-account access, and IAM roles. In this example, it is called **enterprise identity federation** considering that you also need to set up a single sign-on (SSO) capability.

The correct answers are:

- *Setup a Federation proxy or an Identity provider*
- *Setup an AWS Security Token Service to generate temporary tokens*
- *Configure an IAM role and an IAM Policy to access the bucket.*



In an enterprise identity federation, you can authenticate users in your organization's network, and then provide those users access to AWS without creating new AWS identities for them and requiring them to sign in with a separate user name and password. This is known as the *single sign-on* (SSO) approach to temporary access. AWS STS supports open standards like Security Assertion Markup Language (SAML) 2.0, with which you can use Microsoft AD FS to leverage your Microsoft Active Directory. You can also use SAML 2.0 to manage your own solution for federating user identities.

Using 3rd party Single Sign-On solutions such as Atlassian Crowd, OKTA, OneLogin and many others is incorrect since you don't have to use 3rd party solutions to provide the access. AWS already provides the necessary tools that you can use in this situation.

Mapping each individual user to a designated user folder in S3 using Amazon WorkDocs to access their personal documents is incorrect as there is no direct way of integrating Amazon S3 with Amazon WorkDocs for this particular scenario. Amazon WorkDocs is simply a fully managed, secure content creation, storage, and collaboration service. With Amazon WorkDocs, you can easily create, edit, and share content. And because it's stored centrally on AWS, you can access it from anywhere on any device.

Setting up a matching IAM user for each of the 1200 users in your corporate directory that needs access to a folder in the S3 bucket is incorrect since creating that many IAM users would be unnecessary. Also, you want the account to integrate with your AD or LDAP directory, hence, IAM Users does not fit these criteria.

References:

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

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

<https://aws.amazon.com/blogs/security/writing-iam-policies-grant-access-to-user-specific-folders-in-an-amazon-s3-bucket/>

Question 37. A multi-tiered application hosted in your on-premises data center is scheduled to be migrated to AWS. The application has a message broker service which uses industry standard messaging APIs and protocols that must be migrated as well, without rewriting the messaging code in your application.

Which of the following is the most suitable service that you should use to move your messaging service to AWS?

- 1. ☐ A. Amazon SNS
- 2. ☐ B. Amazon MQ
- 3. ☐ C. Amazon SQS
- 4. ☐ D. Amazon SWF

Correct Answer: – B

Explanation: – Amazon MQ, Amazon SQS, and Amazon SNS are messaging services that are suitable for anyone from startups to enterprises. If you're using messaging with existing applications and want to move your messaging service to the cloud quickly and easily, it is recommended that you consider Amazon MQ. It supports industry-standard APIs and protocols

so you can switch from any standards-based message broker to Amazon MQ without rewriting the messaging code in your applications.

Hence, **Amazon MQ** is the correct answer.

The screenshot displays the Amazon MQ managed message broker service page. At the top, it says 'APPLICATION INTEGRATION' and 'Amazon MQ managed message broker service for Apache ActiveMQ'. Below this, a description states: 'Amazon MQ is a managed message broker service for ActiveMQ that makes it easy to set up and operate message brokers in the cloud, so you can migrate your messaging and applications without rewriting code.'

On the right side, there is a 'Create a broker' section with a form for 'Broker name' (containing 'MyBroker') and a 'Next step' button.

Below the 'Create a broker' section is a 'Pricing & costs (US)' table:

Instance Type	Price
mq.t2.micro	\$0.03 per hour
mq.m4.large	\$0.3 per hour
Storage	\$0.3 per GB-month

Below the pricing table is a 'Learn more' link with an external link icon.

On the left side, there is a 'Benefits' section with three columns:

- Accelerate migration**: Amazon MQ supports industry-standard APIs and protocols so you can migrate messaging and applications without rewriting code.
- Offload operations**: Amazon MQ manages the administration and maintenance of ActiveMQ brokers and automatically provisions infrastructure for high availability.
- Reduce cost**: Amazon MQ provides cost-efficient and flexible messaging capacity - you pay for broker instance and storage usage as you go.

Below the 'Benefits' section is a 'Related services' section with two columns:

- Amazon SQS**: Amazon SQS is a fully managed and highly scalable message queuing service for distributed applications and systems.
- Amazon SNS**: Amazon SNS is a fully managed pub/sub messaging and mobile notification service with nearly unlimited throughput.

On the right side, below the 'Pricing & costs' section, is a 'Documentation' section with links to 'Developer Guide', 'API Reference', 'FAQs', and 'Support forums'.

If you are building brand new applications in the cloud, then it is highly recommended that you consider Amazon SQS and Amazon SNS. Amazon SQS and SNS are lightweight, fully managed message queue and topic services that scale almost infinitely and provide simple, easy-to-use APIs. You can use Amazon SQS and SNS to decouple and scale microservices, distributed systems, and serverless applications, and improve reliability.

Amazon SQS is incorrect because although this is a fully managed message queuing service, it does not support an extensive list of industry-standard messaging APIs and protocol, unlike

Amazon MQ. Moreover, using Amazon SQS requires you to do additional changes in the messaging code of applications to make it compatible.

Amazon SNS is incorrect because SNS is more suitable as a pub/sub messaging service instead of a message broker service.

Amazon SWF is incorrect because this is a fully-managed state tracker and task coordinator service and not a messaging service, unlike Amazon MQ, AmazonSQS and Amazon SNS.

References:

<https://aws.amazon.com/amazon-mq/faqs/>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html#sqs-difference-from-amazon-mq-sns>

Question 37. A multi-tiered application hosted in your on-premises data center is scheduled to be migrated to AWS. The application has a message broker service which uses industry standard messaging APIs and protocols that must be migrated as well, without rewriting the messaging code in your application.

Which of the following is the most suitable service that you should use to move your messaging service to AWS?

- 1. ☐ A. Amazon SNS
- 2. ☐ B. Amazon MQ
- 3. ☐ C. Amazon SQS
- 4. ☐ D. Amazon SWF

Correct Answer: – B

Explanation: – Amazon MQ, Amazon SQS, and Amazon SNS are messaging services that are suitable for anyone from startups to enterprises. If you're using messaging with existing applications and want to move your messaging service to the cloud quickly and easily, it is recommended that you consider Amazon MQ. It supports industry-standard APIs and protocols so you can switch from any standards-based message broker to Amazon MQ without rewriting the messaging code in your applications.

Hence, **Amazon MQ** is the correct answer.

APPLICATION INTEGRATION

Amazon MQ

managed message broker service for Apache ActiveMQ

Amazon MQ is a managed message broker service for ActiveMQ that makes it easy to set up and operate message brokers in the cloud, so you can migrate your messaging and applications without rewriting code.

Create a broker

Broker name

Next step

Benefits

Accelerate migration

Amazon MQ supports industry-standard APIs and protocols so you can migrate messaging and applications without rewriting code.

Offload operations


Amazon MQ manages the administration and maintenance of ActiveMQ brokers and automatically provisions infrastructure for high availability.

Reduce cost

Amazon MQ provides cost-efficient and flexible messaging capacity - you pay for broker instance and storage usage as you go.

Pricing & costs (US)

mq.t2.micro	\$0.03 per hour
mq.m4.large	\$0.3 per hour
Storage	\$0.3 per GB-month

[Learn more](#) 

Documentation

- [Developer Guide](#)
- [API Reference](#)
- [FAQs](#)
- [Support forums](#)

Related services

Amazon SQS

Amazon SQS is a fully managed and highly scalable message queuing service for distributed applications and systems.

Amazon SNS

Amazon SNS is a fully managed pub/sub messaging and mobile notification service with nearly unlimited throughput.

If you are building brand new applications in the cloud, then it is highly recommended that you consider Amazon SQS and Amazon SNS. Amazon SQS and SNS are lightweight, fully managed message queue and topic services that scale almost infinitely and provide simple, easy-to-use APIs. You can use Amazon SQS and SNS to decouple and scale microservices, distributed systems, and serverless applications, and improve reliability.

Amazon SQS is incorrect because although this is a fully managed message queuing service, it does not support an extensive list of industry-standard messaging APIs and protocol, unlike Amazon MQ. Moreover, using Amazon SQS requires you to do additional changes in the messaging code of applications to make it compatible.

Amazon SNS is incorrect because SNS is more suitable as a pub/sub messaging service instead of a message broker service.

Amazon SWF is incorrect because this is a fully-managed state tracker and task coordinator service and not a messaging service, unlike Amazon MQ, AmazonSQS and Amazon SNS.

References:

<https://aws.amazon.com/amazon-mq/faqs/>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html#sqs-difference-from-amazon-mq-sns>

Question 39. A suite of web applications is hosted in an Auto Scaling group of EC2 instances across three Availability Zones and is configured with default settings. There is an Application Load Balancer that forwards the request to the respective target group on the URL path. The scale-in policy has been triggered due to the low number of incoming traffic to the application.

Which EC2 instance will be the first one to be terminated by your Auto Scaling group?

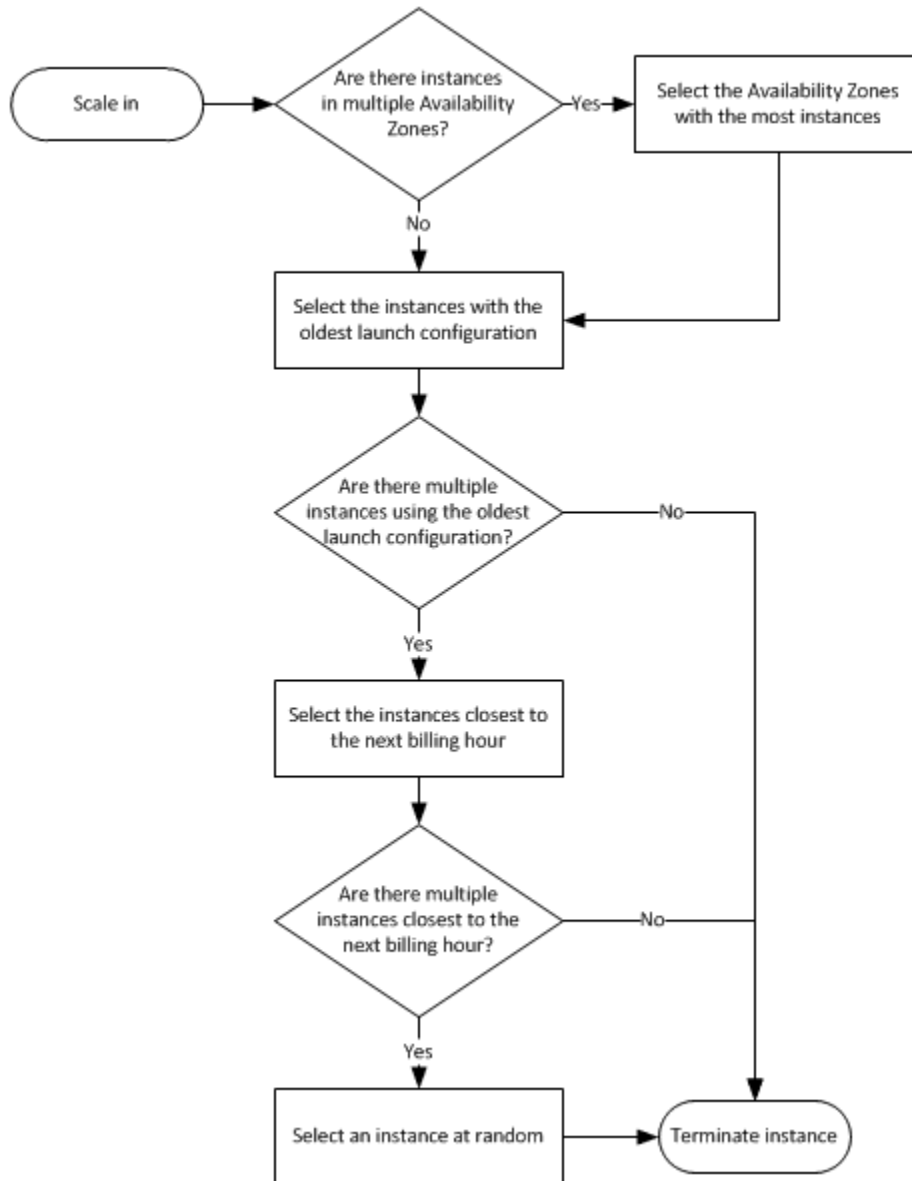
- 1. ☐ A. The EC2 instance which has the least number of user sessions
- 2. ☐ B. The EC2 instance which has been running for the longest time
- 3. ☐ C. The EC2 instance launched from the oldest launch configuration
- 4. ☐ D. The instance will be randomly selected by the Auto Scaling group

Correct Answer: – C

Explanation: – The default termination policy is designed to help ensure that your network architecture spans Availability Zones evenly. With the default termination policy, the behavior of the Auto Scaling group is as follows:

1. If there are instances in multiple Availability Zones, choose the Availability Zone with the most instances and at least one instance that is not protected from scale in. If there is more than one Availability Zone with this number of instances, choose the Availability Zone with the instances that use the oldest launch configuration.
2. Determine which unprotected instances in the selected Availability Zone use the oldest launch configuration. If there is one such instance, terminate it.
3. If there are multiple instances to terminate based on the above criteria, determine which unprotected instances are closest to the next billing hour. (This helps you maximize the use of your EC2 instances and manage your Amazon EC2 usage costs.) If there is one such instance, terminate it.
4. If there is more than one unprotected instance closest to the next billing hour, choose one of these instances at random.

The following flow diagram illustrates how the default termination policy works:



References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html#default-termination-policy>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html>

Question 40. There was an incident in your production environment where the user data stored in the S3 bucket has been accidentally deleted by one of the Junior DevOps Engineers. The issue was escalated to your manager and after a few days, you were instructed to improve the security and protection of your AWS resources.

What combination of the following options will protect the S3 objects in your bucket from both accidental deletion and overwriting? (Select TWO.)

- 1. ☐ A. Enable Amazon S3 Intelligent-Tiering
- 2. ☐ B. Provide access to S3 data strictly through pre-signed URL only
- 3. ☐ C. Enable Multi-Factor Authentication Delete
- 4. ☐ D. Disallow S3 Delete using an IAM bucket policy
- 5. ☐ E. Enable Versioning

Correct Answer: – C, E

Explanation: – By using Versioning and enabling MFA (Multi-Factor Authentication) Delete, you can secure and recover your S3 objects from accidental deletion or overwrite.

Versioning is a means of keeping multiple variants of an object in the same bucket. Versioning-enabled buckets enable you to recover objects from accidental deletion or overwrite. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures.

You can also optionally add another layer of security by configuring a bucket to enable MFA (Multi-Factor Authentication) Delete, which requires additional authentication for either of the following operations:

- Change the versioning state of your bucket
- Permanently delete an object version

MFA Delete requires two forms of authentication together:

- Your security credentials
- The concatenation of a valid serial number, a space, and the six-digit code displayed on an approved authentication device

Providing access to S3 data strictly through pre-signed URL only is incorrect since a pre-signed URL gives access to the object identified in the URL. Pre-signed URLs are useful when customers perform an object upload to your S3 bucket but does not help in preventing accidental deletes.

Disallowing S3 Delete using an IAM bucket policy is incorrect since you still want users to be able to delete objects in the bucket, and you just want to prevent accidental deletions. Disallowing S3 Delete using an IAM bucket policy will restrict all delete operations to your bucket.

Enabling Amazon S3 Intelligent-Tiering is incorrect since S3 intelligent tiering does not help in this situation.

Reference:

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

Question 41. A company has a hybrid cloud architecture that connects their on-premises data center and cloud infrastructure in AWS. They require a durable storage backup for their corporate documents stored on-premises and a local cache that provides low latency access to their recently accessed data to reduce data egress charges. The documents must be stored to and retrieved from AWS via the Server Message Block (SMB) protocol. These files must immediately be accessible within minutes for six months and archived for another decade to meet the data compliance.

Which of the following is the best and most cost-effective approach to implement in this scenario?

- 1. ☐ A. Use AWS Snowmobile to migrate all of the files from the on-premises network. Upload the documents to an S3 bucket and set up a lifecycle policy to move the data into Glacier for archival.
- 2. ☐ B. Launch a new file gateway that connects to your on-premises data center using AWS Storage Gateway. Upload the documents to the file gateway and set up a lifecycle policy to move the data into Glacier for data archival.
- 3. ☐ C. Establish a Direct Connect connection to integrate your on-premises network to your VPC. Upload the documents on Amazon EBS Volumes and use a lifecycle policy to automatically move the EBS snapshots to an S3 bucket, and then later to Glacier for archival.
- 4. ☐ D. Launch a new tape gateway that connects to your on-premises data center using AWS Storage Gateway. Upload the documents to the tape gateway and set up a lifecycle policy to move the data into Glacier for archival.

Correct Answer: – B

Explanation: – A file gateway supports a file interface into Amazon Simple Storage Service (Amazon S3) and combines a service and a virtual software appliance. By using this combination, you can store and retrieve objects in Amazon S3 using industry-standard file protocols such as Network File System (NFS) and Server Message Block (SMB). The software appliance, or gateway, is deployed into your on-premises environment as a virtual machine (VM) running on VMware ESXi, Microsoft Hyper-V, or Linux Kernel-based Virtual Machine (KVM) hypervisor.



The gateway provides access to objects in S3 as files or file share mount points. With a file gateway, you can do the following:

- You can store and retrieve files directly using the NFS version 3 or 4.1 protocol.
- You can store and retrieve files directly using the SMB file system version, 2 and 3 protocol.
- You can access your data directly in Amazon S3 from any AWS Cloud application or service.
- You can manage your Amazon S3 data using lifecycle policies, cross-region replication, and versioning. You can think of a file gateway as a file system mount on S3.

AWS Storage Gateway supports the Amazon S3 Standard, Amazon S3 Standard-Infrequent Access, Amazon S3 One Zone-Infrequent Access and Amazon Glacier storage classes. When you create or update a file share, you have the option to select a storage class for your objects. You can either choose the Amazon S3 Standard or any of the infrequent access storage classes such as S3 Standard IA or S3 One Zone IA. Objects stored in any of these storage classes can be transitioned to Amazon Glacier using a Lifecycle Policy.

Although you can write objects directly from a file share to the S3-Standard-IA or S3-One Zone-IA storage class, it is recommended that you use a Lifecycle Policy to transition your objects rather than write directly from the file share, especially if you're expecting to update or delete the object within 30 days of archiving it.

Therefore, the correct answer is: ***Launch a new file gateway that connects to your on-premises data center using AWS Storage Gateway. Upload the documents to the file gateway and set up a lifecycle policy to move the data into Glacier for data archival.***

The option that says: ***Launch a new tape gateway that connects to your on-premises data center using AWS Storage Gateway. Upload the documents to the tape gateway and set up a lifecycle policy to move the data into Glacier for archival*** is incorrect because although tape gateways provide cost-effective and durable archive backup data in Amazon Glacier, it does not meet the criteria of being retrievable immediately within minutes. It also doesn't maintain a local cache that provides low latency access to the recently accessed data and reduce data egress charges. Thus, it is still better to set up a file gateway instead.

The option that says: *Establish a Direct Connect connection to integrate your on-premises network to your VPC. Upload the documents on Amazon EBS Volumes and use a lifecycle policy to automatically move the EBS snapshots to an S3 bucket, and then later to Glacier for archival* is incorrect because EBS Volumes are not as durable compared with S3 and it would be more cost-efficient if you directly store the documents to an S3 bucket. An alternative solution is to use AWS Direct Connect with AWS Storage Gateway to create a connection for high-throughput workload needs, providing a dedicated network connection between your on-premises file gateway and AWS. But this solution is using EBS, hence, this option is still wrong.

The option that says: *Use AWS Snowmobile to migrate all of the files from the on-premises network. Upload the documents to an S3 bucket and set up a lifecycle policy to move the data into Glacier for archival* is incorrect because Snowmobile is mainly used to migrate the entire data of an on-premises data center to AWS. This is not a suitable approach as the company still has a hybrid cloud architecture which means that they will still use their on-premises data center along with their AWS cloud infrastructure.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

<https://docs.aws.amazon.com/storagegateway/latest/userguide/StorageGatewayConcepts.html>

Question 42. A tech company has a CRM application hosted on an Auto Scaling group of On-Demand EC2 instances. The application is extensively used during office hours from 9 in the morning till 5 in the afternoon. Their users are complaining that the performance of the application is slow during the start of the day but then works normally after a couple of hours.

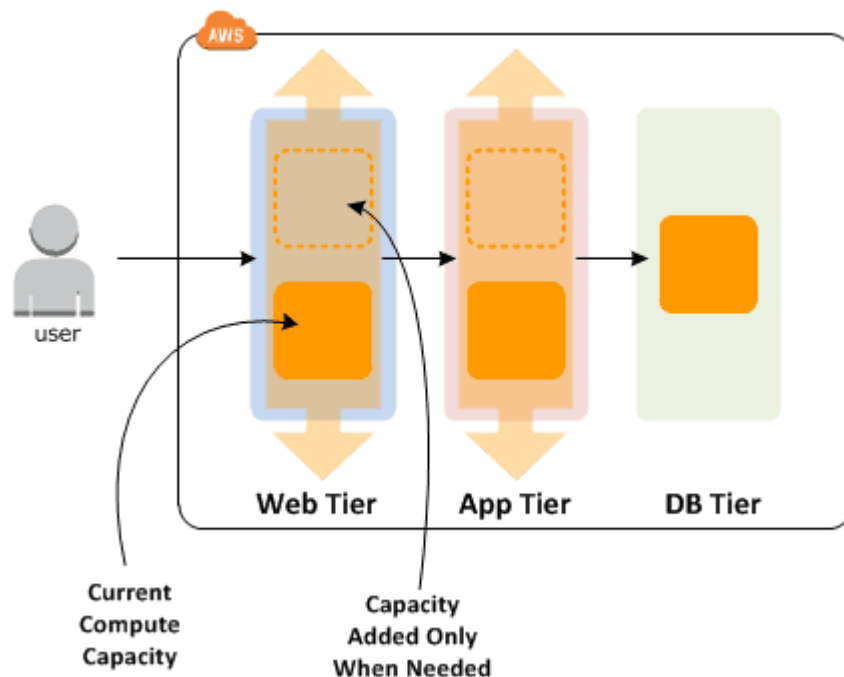
Which of the following can be done to ensure that the application works properly at the beginning of the day?

- 1. ☐ A. Configure a Scheduled scaling policy for the Auto Scaling group to launch new instances before the start of the day.
- 2. ☐ B. Set up an Application Load Balancer (ALB) to your architecture to ensure that the traffic is properly distributed on the instances.
- 3. ☐ C. Configure a Dynamic scaling policy for the Auto Scaling group to launch new instances based on the CPU utilization.
- 4. ☐ D. Configure a Dynamic scaling policy for the Auto Scaling group to launch new instances based on the Memory utilization.

Correct Answer: – A

Explanation: – Scaling based on a schedule allows you to scale your application in response to predictable load changes. For example, every week the traffic to your web application starts to

increase on Wednesday, remains high on Thursday, and starts to decrease on Friday. You can plan your scaling activities based on the predictable traffic patterns of your web application.



To configure your Auto Scaling group to scale based on a schedule, you create a scheduled action. The scheduled action tells Amazon EC2 Auto Scaling to perform a scaling action at specified times. To create a scheduled scaling action, you specify the start time when the scaling action should take effect, and the new minimum, maximum, and desired sizes for the scaling action. At the specified time, Amazon EC2 Auto Scaling updates the group with the values for minimum, maximum, and desired size specified by the scaling action. You can create scheduled actions for scaling one time only or for scaling on a recurring schedule.

Hence, **configuring a Scheduled scaling policy for the Auto Scaling group to launch new instances before the start of the day** is the correct answer. You need to configure a Scheduled scaling policy. This will ensure that the instances are already scaled up and ready before the start of the day since this is when the application is used the most.

Configuring a Dynamic scaling policy for the Auto Scaling group to launch new instances based on the CPU utilization and configuring a Dynamic scaling policy for the Auto Scaling group to launch new instances based on the Memory utilization are both incorrect because although these are valid solutions, it is still better to configure a Scheduled scaling policy as you already know the exact peak hours of your application. By the time either the CPU or Memory hits a peak, the application already has performance issues, so you need to ensure the scaling is done beforehand using a Scheduled scaling policy.

Setting up an Application Load Balancer (ALB) to your architecture to ensure that the traffic is properly distributed on the instances is incorrect. Although the Application load balancer can also balance the traffic, it cannot increase the instances based on demand.

Reference:

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

Question 43. A company plans to build a data analytics application in AWS which will be deployed in an Auto Scaling group of On-Demand EC2 instances and a MongoDB database. It is expected that the database will have high-throughput workloads performing small, random I/O operations. As the Solutions Architect, you are required to properly set up and launch the required resources in AWS.



Which of the following is the most suitable EBS type to use for your database?

- 1. ☐ A. Throughput Optimized HDD (st1)
- 2. ☐ B. Provisioned IOPS SSD (io1)
- 3. ☐ C. General Purpose SSD (gp2)
- 4. ☐ D. Cold HDD (sc1)

Correct Answer: – B

Explanation: – On a given volume configuration, certain I/O characteristics drive the performance behavior for your EBS volumes. SSD-backed volumes, such as General-Purpose SSD (gp2) and Provisioned IOPS SSD (io1), deliver consistent performance whether an I/O operation is random or sequential. HDD-backed volumes like Throughput Optimized HDD (st1) and Cold HDD (sc1) deliver optimal performance only when I/O operations are large and sequential.

In the exam, always consider the difference between SSD and HDD as shown on the table below. This will allow you to easily eliminate specific EBS-types in the options which are not SSD or not HDD, depending on whether the question asks for a storage type which has *small, random* I/O operations or *large, sequential* I/O operations.

FEATURES	SSD Solid State Drive	HDD Hard Disk Drive
Best for workloads with:	<i>small, random</i> I/O operations	<i>large, sequential</i> I/O operations
Can be used as a bootable volume?	Yes	No
Suitable Use Cases	<ul style="list-style-type: none"> - Best for transactional workloads - Critical business applications that require sustained IOPS performance - Large database workloads such as MongoDB, Oracle, Microsoft SQL Server and many others... 	<ul style="list-style-type: none"> - Best for large streaming workloads requiring consistent, fast throughput at a low price - Big data, Data warehouses, Log processing - Throughput-oriented storage for large volumes of data that is infrequently accessed
Cost	moderate / high 	low 
Dominant Performance Attribute	IOPS	Throughput (MiB/s)

Provisioned IOPS SSD (io1) volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads, that are sensitive to storage performance and consistency. Unlike gp2, which uses a bucket and credit model to calculate performance, an io1 volume allows you to specify a consistent IOPS rate when you create the volume, and Amazon EBS delivers within 10 percent of the provisioned IOPS performance 99.9 percent of the time over a given year.

	Solid-State Drives (SSD)		Hard Disk Drives (HDD)	
Volume Type	General Purpose SSD (gp2)*	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	Low-cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads
Use Cases	<ul style="list-style-type: none"> • Recommended for most workloads • System boot volumes • Virtual desktops • Low-latency interactive apps • Development and test environments 	<ul style="list-style-type: none"> • Critical business applications that require sustained IOPS performance, or more than 16,000 IOPS or 250 MiB/s of throughput per volume • Large database workloads, such as: <ul style="list-style-type: none"> ◦ MongoDB ◦ Cassandra ◦ Microsoft SQL Server ◦ MySQL ◦ PostgreSQL ◦ Oracle 	<ul style="list-style-type: none"> • Streaming workloads requiring consistent, fast throughput at a low price • Big data • Data warehouses • Log processing • Cannot be a boot volume 	<ul style="list-style-type: none"> • Throughput-oriented storage for large volumes of data that is infrequently accessed • Scenarios where the lowest storage cost is important • Cannot be a boot volume
API Name	gp2	io1	st1	sc1
Volume Size	1 GiB - 16 TiB	4 GiB - 16 TiB	500 GiB - 16 TiB	500 GiB - 16 TiB
Max. IOPS**/Volume	16,000***	64,000****	500	250
Max. Throughput*/Volume	250 MiB/s***	1,000 MiB/s†	500 MiB/s	250 MiB/s
Max. IOPS/Instance††	80,000	80,000	80,000	80,000
Max. Throughput/Instance††	1,750 MiB/s	1,750 MiB/s	1,750 MiB/s	1,750 MiB/s
Dominant Performance Attribute	IOPS	IOPS	MiB/s	MiB/s

General Purpose SSD (gp2) is incorrect because although General Purpose is a type of SSD that can handle small, random I/O operations, the Provisioned IOPS SSD volumes are much

more suitable to meet the needs of I/O-intensive database workloads such as MongoDB, Oracle, MySQL, and many others.

Throughput Optimized HDD (st1) and **Cold HDD (sc1)** are incorrect because HDD volumes (such as Throughput Optimized HDD and Cold HDD volumes) are more suitable for workloads with large, sequential I/O operations instead of small, random I/O operations.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_piops

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-io-characteristics.html>

Question 44. A content management system (CMS) is hosted on a fleet of auto-scaled, On-Demand EC2 instances which use Amazon Aurora as its database. Currently, the system stores the file documents that the users uploaded in one of the attached EBS Volumes. Your manager noticed that the system performance is quite slow, and he has instructed you to improve the architecture of the system.

In this scenario, what will you do to implement a scalable, high throughput POSIX-compliant file system?

- 1. ☐ A. Use EFS
- 2. ☐ B. Use ElastiCache
- 3. ☐ C. Create an S3 bucket and use this as a storage for CMS
- 4. ☐ D. Upgrade your existing EBS volumes to Provisioned IOPS SSD Volumes

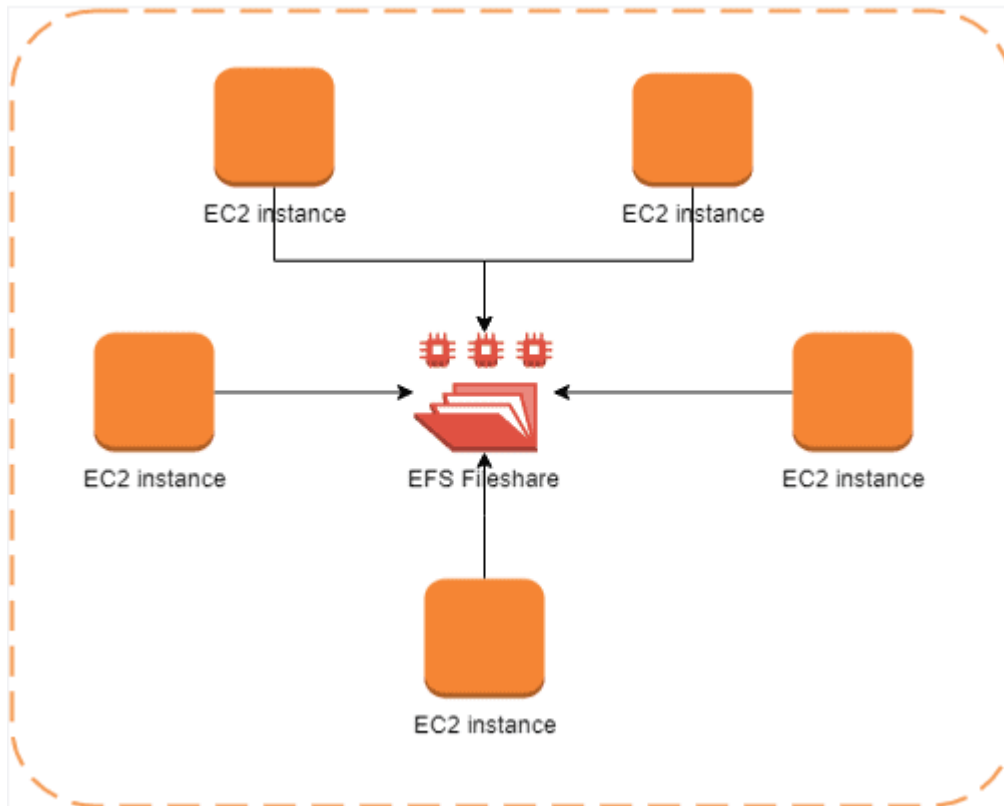
Correct Answer: – A

Explanation: – Amazon Elastic File System (Amazon EFS) provides simple, scalable, elastic file storage for use with AWS Cloud services and on-premises resources. When mounted on Amazon EC2 instances, an Amazon EFS file system provides a standard file system interface and file system access semantics, allowing you to seamlessly integrate Amazon EFS with your existing applications and tools. Multiple Amazon EC2 instances can access an Amazon EFS file system at the same time, allowing Amazon EFS to provide a common data source for workloads and applications running on more than one Amazon EC2 instance.

This particular scenario tests your understanding of EBS, EFS, and S3. In this scenario, there is a fleet of On-Demand EC2 instances that stores file documents from the users to one of the attached EBS Volumes. The system performance is quite slow because the architecture doesn't provide the EC2 instances a parallel shared access to the file documents.

Remember that an EBS Volume can be attached to one EC2 instance at a time, hence, no other EC2 instance can connect to that EBS Provisioned IOPS Volume. Take note as well that the type

of storage needed here is a “file storage” which means that **S3** is not the best service to use because it is mainly used for “object storage”, and S3 does not provide the notion of “folders” too. This is why **using EFS** is the correct answer.



Upgrading your existing EBS volumes to Provisioned IOPS SSD Volumes is incorrect because the scenario requires you to set up a scalable, high throughput storage system that will allow concurrent access from multiple EC2 instances. This is clearly not possible in EBS, even with Provisioned IOPS SSD Volumes. You have to use EFS instead.

Using ElastiCache is incorrect because this is an in-memory data store that improves the performance of your applications, which is not what you need since it is not a file storage.

Reference:

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

Question 45. An online shopping platform is hosted on an Auto Scaling group of Spot EC2 instances and uses Amazon Aurora PostgreSQL as its database. There is a requirement to optimize your database workloads in your cluster where you have to direct the write operations of the production traffic to your high-capacity instances and point the reporting queries sent by your internal staff to the low-capacity instances.

Which is the most suitable configuration for your application as well as your Aurora database cluster to achieve this requirement?

- 1. ☐ A. Create a custom endpoint in Aurora based on the specified criteria for the production traffic and another custom endpoint to handle the reporting queries.
- 2. ☐ B. In your application, use the instance endpoint of your Aurora database to handle the incoming production traffic and use the cluster endpoint to handle reporting queries.
- 3. ☐ C. Do nothing since by default, Aurora will automatically direct the production traffic to your high-capacity instances and the reporting queries to your low-capacity instances.
- 4. ☐ D. Configure your application to use the reader endpoint for both production traffic and reporting queries, which will enable your Aurora database to automatically perform load-balancing among all the Aurora Replicas.

Correct Answer: – A

Explanation: – Amazon Aurora typically involves a cluster of DB instances instead of a single instance. Each connection is handled by a specific DB instance. When you connect to an Aurora cluster, the host name and port that you specify point to an intermediate handler called an *endpoint*. Aurora uses the endpoint mechanism to abstract these connections. Thus, you don't have to hardcode all the hostnames or write your own logic for load-balancing and rerouting connections when some DB instances aren't available.

For certain Aurora tasks, different instances or groups of instances perform different roles. For example, the primary instance handles all data definition language (DDL) and data manipulation language (DML) statements. Up to 15 Aurora Replicas handle read-only query traffic.

Using endpoints, you can map each connection to the appropriate instance or group of instances based on your use case. For example, to perform DDL statements you can connect to whichever instance is the primary instance. To perform queries, you can connect to the reader endpoint, with Aurora automatically performing load-balancing among all the Aurora Replicas. For clusters with DB instances of different capacities or configurations, you can connect to custom endpoints associated with different subsets of DB instances. For diagnosis or tuning, you can connect to a specific instance endpoint to examine details about a specific DB instance.

The custom endpoint provides load-balanced database connections based on criteria other than the read-only or read-write capability of the DB instances. For example, you might define a custom endpoint to connect to instances that use a particular AWS instance class or a particular DB parameter group. Then you might tell particular groups of users about this custom endpoint. For example, you might direct internal users to low-capacity instances for report generation or ad hoc (one-time) querying, and direct production traffic to high-capacity instances.

Hence, **creating a custom endpoint in Aurora based on the specified criteria for the production traffic and another custom endpoint to handle the reporting queries** is the correct answer.

Configuring your application to use the reader endpoint for both production traffic and reporting queries, which will enable your Aurora database to automatically perform load-balancing among all the Aurora Replicas is incorrect because although it is true that a reader

endpoint enables your Aurora database to automatically perform load-balancing among all the Aurora Replicas, it is quite limited to doing read operations only. You still need to use a custom endpoint to load-balance the database connections based on the specified criteria.

The option that says: **In your application, use the instance endpoint of your Aurora database to handle the incoming production traffic and use the cluster endpoint to handle reporting queries** is incorrect because a cluster endpoint (also known as a writer endpoint) for an Aurora DB cluster simply connects to the current primary DB instance for that DB cluster. This endpoint can perform write operations in the database such as DDL statements, which is perfect for handling production traffic but not suitable for handling queries for reporting since there will be no write database operations that will be sent. Moreover, the endpoint does not point to lower-capacity or high-capacity instances as per the requirement. A better solution for this is to use a custom endpoint.

The option that says: **Do nothing since by default, Aurora will automatically direct the production traffic to your high-capacity instances and the reporting queries to your low-capacity instances** is incorrect because Aurora does not do this by default. You have to create custom endpoints in order to accomplish this requirement.

Reference:

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

Question 46. You have a requirement to make sure that an On-Demand EC2 instance can only be accessed from this IP address (110.238.98.71) via an SSH connection. Which configuration below will satisfy this requirement?

- 1. ☐ A. Security Group Inbound Rule: Protocol – TCP. Port Range – 22, Source 110.238.98.71/0
- 2. ☐ B. Security Group Inbound Rule: Protocol – TCP. Port Range – 22, Source 110.238.98.71/32
- 3. ☐ C. Security Group Inbound Rule: Protocol – UDP, Port Range – 22, Source 110.238.98.71/32
- 4. ☐ D. Security Group Inbound Rule: Protocol – UDP, Port Range – 22, Source 110.238.98.71/0

Correct Answer: – B

Explanation: – The SSH protocol uses TCP and port 22. Hence, **Protocol – UDP, Port Range – 22, Source 110.238.98.71/32** and **Protocol – UDP, Port Range – 22, Source 110.238.98.71/0** are incorrect as they are using UDP.

The following two options: **Protocol – TCP, Port Range – 22, Source 110.238.98.71/32** and **Protocol – TCP, Port Range – 22, Source 110.238.98.71/0** have one major difference and that is their CIDR block.

The requirement is to only allow the individual IP of the client and not the entire network. Therefore, the proper CIDR notation should be used. The **/32** denotes one IP address and the **/0** refers to the entire network. That is why **Protocol – TCP, Port Range – 22, Source 110.238.98.71/0** is incorrect as it allowed the entire network instead of a single IP.

Reference:

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

Question 47. A company is in the process of migrating their applications to AWS. One of their systems requires a database that can scale globally and handle frequent schema changes. The application should not have any downtime or performance issues whenever there is a schema change in the database. It should also provide a low latency response to high-traffic queries.

Which is the most suitable database solution to use to achieve this requirement?

- 1. ☐ A. An Amazon Aurora database with Read Replicas
- 2. ☐ B. An Amazon RDS instance in Multi-AZ Deployments configuration
- 3. ☐ C. Redshift
- 4. ☐ D. Amazon DynamoDB

Correct Answer: D

Explanation: Before we proceed in answering this question, we must first be clear with the actual definition of a “**schema**“. Basically, the english definition of a schema is: *a representation of a plan or theory in the form of an outline or model.*

Just think of a schema as the “structure” or a “model” of your data in your database. Since the scenario requires that the schema, or the structure of your data, changes frequently, then you have to pick a database which provides a non-rigid and flexible way of adding or removing new types of data. This is a classic example of choosing between a relational database and non-relational (NoSQL) database.

Characteristic	Relational Database Management System (RDBMS)	Amazon DynamoDB
Optimal Workloads	Ad hoc queries; data warehousing; OLAP (online analytical processing).	Web-scale applications, including social networks, gaming, media sharing, and IoT (Internet of Things).
Data Model	The relational model requires a well-defined schema, where data is normalized into tables, rows and columns. In addition, all of the relationships are defined among tables, columns, indexes, and other database elements.	DynamoDB is schemaless. Every table must have a primary key to uniquely identify each data item, but there are no similar constraints on other non-key attributes. DynamoDB can manage structured or semi-structured data, including JSON documents.
Data Access	SQL (Structured Query Language) is the standard for storing and retrieving data. Relational databases offer a rich set of tools for simplifying the development of database-driven applications, but all of these tools use SQL.	You can use the AWS Management Console or the AWS CLI to work with DynamoDB and perform ad hoc tasks. Applications can leverage the AWS software development kits (SDKs) to work with DynamoDB using object-based, document-centric, or low-level interfaces.
Performance	Relational databases are optimized for storage, so performance generally depends on the disk subsystem. Developers and database administrators must optimize queries, indexes, and table structures in order to achieve peak performance.	DynamoDB is optimized for compute, so performance is mainly a function of the underlying hardware and network latency. As a managed service, DynamoDB insulates you and your applications from these implementation details, so that you can focus on designing and building robust, high-performance applications.
Scaling	It is easiest to scale up with faster hardware. It is also possible for database tables to span across multiple hosts in a distributed system, but this requires additional investment. Relational databases have maximum sizes for the number and size of files, which imposes upper limits on scalability.	DynamoDB is designed to scale out using distributed clusters of hardware. This design allows increased throughput without increased latency. Customers specify their throughput requirements, and DynamoDB allocates sufficient resources to meet those requirements. There are no upper limits on the number of items per table, nor the total size of that table.

A relational database is known for having a rigid schema, with a lot of constraints and limits as to which (and what type of) data can be inserted or not. It is primarily used for scenarios where you have to support complex queries which fetch data across a number of tables. It is best for scenarios where you have complex table relationships but for use cases where you need to have a flexible schema, this is not a suitable database to use.

For NoSQL, it is not as rigid as a relational database because you can easily add or remove rows or elements in your table/collection entry. It also has a more flexible schema because it can store complex hierarchical data within a single item which, unlike a relational database, does not entail changing multiple related tables. Hence, the best answer to be used here is a NoSQL database, like DynamoDB. When your business requires a low-latency response to high-traffic queries, taking advantage of a NoSQL system generally makes technical and economic sense.

Amazon DynamoDB helps solve the problems that limit the relational system scalability by avoiding them. In DynamoDB, you design your schema specifically to make the most common and important queries as fast and as inexpensive as possible. Your data structures are tailored to the specific requirements of your business use cases.

Remember that a relational database system **does not scale** well for the following reasons:

- It normalizes data and stores it on multiple tables that require multiple queries to write to disk.
- It generally incurs the performance costs of an ACID-compliant transaction system.
- It uses expensive joins to reassemble required views of query results.

For DynamoDB, it scales well due to these reasons:

– Its **schema flexibility** lets DynamoDB store complex hierarchical data within a single item. DynamoDB is not a totally *schemeless* database since the very definition of a schema is just the model or structure of your data.

– Composite key design lets it store related items close together on the same table.

An Amazon RDS instance in Multi-AZ Deployments configuration and an Amazon Aurora database with Read Replicas are incorrect because both of them are a type of relational database.

Redshift is incorrect because it is primarily used for OLAP systems.

References:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-general-nosql-design.html>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-relational-modeling.html>

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

Question 48. A company is using Amazon S3 to store frequently accessed data. When an object is created or deleted, the S3 bucket will send an event notification to the Amazon SQS queue. A solutions architect needs to create a solution that will notify the development and operations team about the created or deleted objects.

Which of the following would satisfy this requirement?

- 1. ☐ A. Create a new Amazon SNS FIFO topic for the other team. Grant Amazon S3 permission to send the notification to the second SNS topic.
- 2. ☐ B. Set up an Amazon SNS topic and configure two Amazon SQS queues to poll the SNS topic. Grant Amazon S3 permission to send notifications to Amazon SNS and update the bucket to use the new SNS topic.
- 3. ☐ C. Create an Amazon SNS topic and configure two Amazon SQS queues to subscribe to the topic. Grant Amazon S3 permission to send notifications to Amazon SNS and update the bucket to use the new SNS topic.
- 4. ☐ D. Set up another Amazon SQS queue for the other team. Grant Amazon S3 permission to send a notification to the second SQS queue.

Correct Answer: C

Explanation: The **Amazon S3** notification feature enables you to receive notifications when certain events happen in your bucket. To enable notifications, you must first add a notification configuration that identifies the events you want Amazon S3 to publish and the destinations

where you want Amazon S3 to send the notifications. You store this configuration in the notification subresource that is associated with a bucket.

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

- Amazon Simple Notification Service (Amazon SNS) topic
- Amazon Simple Queue Service (Amazon SQS) queue
- AWS Lambda

In Amazon SNS, the *fanout* scenario is when a message published to an SNS topic is replicated and pushed to multiple endpoints, such as Amazon SQS queues, HTTP(S) endpoints, and Lambda functions. This allows for parallel asynchronous processing.



For example, you can develop an application that publishes a message to an SNS topic whenever an order is placed for a product. Then, SQS queues that are subscribed to the SNS topic receive identical notifications for the new order. An Amazon Elastic Compute Cloud (Amazon EC2) server instance attached to one of the SQS queues can handle the processing or fulfillment of the order. And you can attach another Amazon EC2 server instance to a data warehouse for analysis of all orders received.

Based on the given scenario, the existing setup sends the event notification to an SQS queue. Since you need to send the notification to the development and operations team, you can use a combination of Amazon SNS and SQS. By using the message fanout pattern, you can create a topic and use two Amazon SQS queues to subscribe to the topic. If Amazon SNS receives an event notification, it will publish the message to both subscribers.

Take note that Amazon S3 event notifications are designed to be delivered at least once and to one destination only. You cannot attach two or more SNS topics or SQS queues for S3 event notification. Therefore, you must send the event notification to Amazon SNS.

Hence, the correct answer is: **Create an Amazon SNS topic and configure two Amazon SQS queues to subscribe to the topic. Grant Amazon S3 permission to send notifications to Amazon SNS and update the bucket to use the new SNS topic.**

The option that says: **Set up another Amazon SQS queue for the other team. Grant Amazon S3 permission to send a notification to the second SQS queue** is incorrect because you can only add 1 SQS or SNS at a time for Amazon S3 events notification. If you need to send the events to multiple subscribers, you should implement a message fanout pattern with Amazon SNS and Amazon SQS.

The option that says: **Create a new Amazon SNS FIFO topic for the other team. Grant Amazon S3 permission to send the notification to the second SNS topic** is incorrect because just as mentioned in the previous option, you can only add 1 SQS or SNS at a time for Amazon S3 events notification. In addition, neither Amazon SNS FIFO topic nor Amazon SQS FIFO queue is warranted in this scenario. Both of them can be used together to provide strict message ordering and message deduplication. The FIFO capabilities of each of these services work together to act as a fully managed service to integrate distributed applications that require data consistency in near-real-time.

The option that says: **Set up an Amazon SNS topic and configure two Amazon SQS queues to poll the SNS topic. Grant Amazon S3 permission to send notifications to Amazon SNS and update the bucket to use the new SNS topic** is incorrect because you can't poll Amazon SNS. Instead of configuring queues to poll Amazon SNS, you should configure each Amazon SQS queue to subscribe to the SNS topic.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ways-to-add-notification-config-to-bucket.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html#notification-how-to-overview>

Question 50. An application that records weather data every minute is deployed in a fleet of Spot EC2 instances and uses a MySQL RDS database instance. Currently, there is only one RDS instance running in one Availability Zone. You plan to improve the database to ensure high availability by synchronous data replication to another RDS instance.

Which of the following performs synchronous data replication in RDS?

- 1. ☐ A. CloudFront running as a Multi-AZ deployment
- 2. ☐ B. RDS Read Replica
- 3. ☐ C. DynamoDB Read Replica
- 4. ☐ D. RDS DB instance running as a Multi-AZ deployment

Correct Answer: D

Explanation: When you create or modify your DB instance to run as a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous **standby** replica in a

different Availability Zone. Updates to your DB Instance are synchronously replicated across Availability Zones to the standby in order to keep both in sync and protect your latest database updates against DB instance failure.

Multi-AZ Deployments	Read Replicas
Synchronous replication – highly durable	Asynchronous replication – highly scalable
Only database engine on primary instance is active	All read replicas are accessible and can be used for read scaling
Automated backups are taken from standby	No backups configured by default
Always span two Availability Zones within a single Region	Can be within an Availability Zone, Cross-AZ, or Cross-Region
Database engine version upgrades happen on primary	Database engine version upgrade is independent from source instance
Automatic failover to standby when a problem is detected	Can be manually promoted to a standalone database instance

RDS Read Replica is incorrect as a Read Replica provides an asynchronous replication instead of synchronous.

DynamoDB Read Replica and **CloudFront running as a Multi-AZ deployment** are incorrect as both DynamoDB and CloudFront do not have a Read Replica feature.

Reference:

<https://aws.amazon.com/rds/details/multi-az/>

Question 51. A popular social media website uses a CloudFront web distribution to serve their static contents to their millions of users around the globe. They are receiving a number of complaints recently that their users take a lot of time to log into their website. There are also occasions when their users are getting HTTP 504 errors. You are instructed by your manager to significantly reduce the user's login time to further optimize the system.

Which of the following options should you use together to set up a cost-effective solution that can improve your application's performance? (Select TWO.)

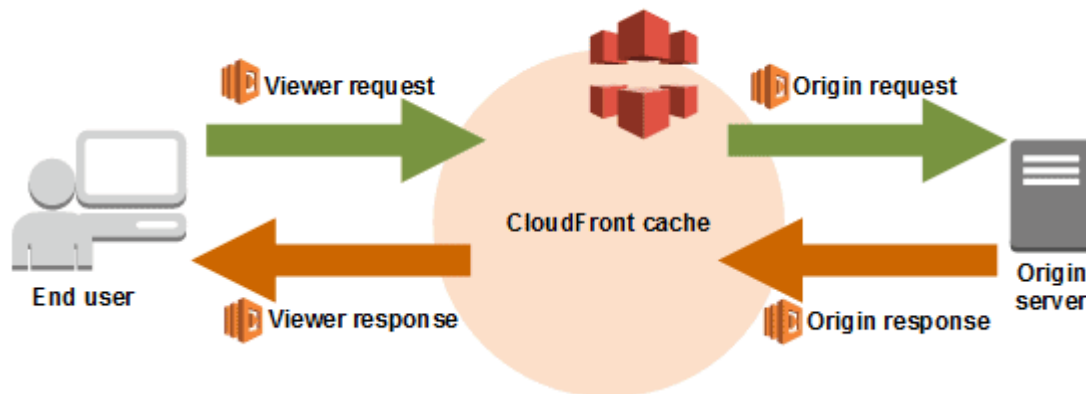
- 1. ☐ A. Set up an origin failover by creating an origin group with two origins. Specify one as the primary origin and the other as the second origin which CloudFront automatically switches to when the primary origin returns specific HTTP status code failure responses.
- 2. ☐ B. Customize the content that the CloudFront web distribution delivers to your users using Lambda@Edge, which allows your Lambda functions to execute the authentication process in AWS locations closer to the users.
- 3. ☐ C. Use multiple and geographically disperse VPCs to various AWS regions then create a transit VPC to connect all of your resources. In order to handle the requests faster, set up Lambda functions in each region using the AWS Serverless Application Model (SAM) service.

- 4. ☐ D. Deploy your application to multiple AWS regions to accommodate your users around the world. Set up a Route 53 record with latency routing policy to route incoming traffic to the region that provides the best latency to the user.
- 5. ☐ E. Configure your origin to add a Cache-Control max-age directive to your objects and specify the longest practical value for max-age to increase the cache hit ratio of your CloudFront distribution.

Correct Answer: A, B

Explanation: Lambda@Edge lets you run Lambda functions to customize the content that CloudFront delivers, executing the functions in AWS locations closer to the viewer. The functions run in response to CloudFront events, without provisioning or managing servers. You can use Lambda functions to change CloudFront requests and responses at the following points:

- After CloudFront receives a request from a viewer (viewer request)
- Before CloudFront forwards the request to the origin (origin request)
- After CloudFront receives the response from the origin (origin response)
- Before CloudFront forwards the response to the viewer (viewer response)



In the given scenario, you can use Lambda@Edge to allow your Lambda functions to customize the content that CloudFront delivers and to execute the authentication process in AWS locations closer to the users. In addition, you can set up an origin failover by creating an origin group with two origins with one as the primary origin and the other as the second origin which CloudFront automatically switches to when the primary origin fails. This will alleviate the occasional HTTP 504 errors that users are experiencing. Therefore, the correct answers are:

- **Customize the content that the CloudFront web distribution delivers to your users using Lambda@Edge, which allows your Lambda functions to execute the authentication process in AWS locations closer to the users.**

– Set up an origin failover by creating an origin group with two origins. Specify one as the primary origin and the other as the second origin which CloudFront automatically switches to when the primary origin returns specific HTTP status code failure responses.

The option that says: **Use multiple and geographically disperse VPCs to various AWS regions then create a transit VPC to connect all of your resources. In order to handle the requests faster, set up Lambda functions in each region using the AWS Serverless Application Model (SAM) service** is incorrect because of the same reason provided above. Although setting up multiple VPCs across various regions which are connected with a transit VPC is valid, this solution still entails higher setup and maintenance costs. A more cost-effective option would be to use Lambda@Edge instead.

The option that says: **Configure your origin to add a Cache-Control max-age directive to your objects and specify the longest practical value for max-age to increase the cache hit ratio of your CloudFront distribution** is incorrect because improving the cache hit ratio for the CloudFront distribution is irrelevant in this scenario. You can improve your cache performance by increasing the proportion of your viewer requests that are served from CloudFront edge caches instead of going to your origin servers for content. However, take note that the problem in the scenario is the sluggish authentication process of your global users and not just the caching of the static objects.

The option that says: **Deploy your application to multiple AWS regions to accommodate your users around the world. Set up a Route 53 record with latency routing policy to route incoming traffic to the region that provides the best latency to the user** is incorrect because although this may resolve the performance issue, this solution entails a significant implementation cost since you have to deploy your application to multiple AWS regions. Remember that the scenario asks for a solution that will improve the performance of the application with **minimal cost**.

References:

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

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-edge.html>

Question 52. A web application is using CloudFront to distribute their images, videos, and other static contents stored in their S3 bucket to its users around the world. The company has recently introduced a new member-only access to some of its high-quality media files. There is a requirement to provide access to multiple private media files only to their paying subscribers without having to change their current URLs.

Which of the following is the most suitable solution that you should implement to satisfy this requirement?

- 1. ☐ A. Create a Signed URL with a custom policy which only allows the members to see the private files.
- 2. ☐ B. Configure your CloudFront distribution to use Match Viewer as its Origin Protocol Policy which will automatically match the user request. This will allow access to the private content if the request is a paying member and deny it if it is not a member.
- 3. ☐ C. Configure your CloudFront distribution to use Field-Level Encryption to protect your private data and only allow access to members.
- 4. ☐ D. Use Signed Cookies to control who can access the private files in your CloudFront distribution by modifying your application to determine whether a user should have access to your content. For members, send the required Set-Cookie headers to the viewer which will unlock the content only to them.

Correct Answer: D

Explanation: CloudFront signed URLs and signed cookies provide the same basic functionality: they allow you to control who can access your content. If you want to serve private content through CloudFront and you're trying to decide whether to use signed URLs or signed cookies, consider the following:

Use **signed URLs** for the following cases:

- You want to use an RTMP distribution. Signed cookies aren't supported for RTMP distributions.
- You want to restrict access to individual files, for example, an installation download for your application.
- Your users are using a client (for example, a custom HTTP client) that doesn't support cookies.

Use **signed cookies** for the following cases:

- You want to provide access to multiple restricted files, for example, all of the files for a video in HLS format or all of the files in the subscribers' area of a website.
- You don't want to change your current URLs.

Hence, the correct answer for this scenario is the option that says: **Use Signed Cookies to control who can access the private files in your CloudFront distribution by modifying your application to determine whether a user should have access to your content. For members, send the required Set-Cookie headers to the viewer which will unlock the content only to them.**

The option that says: **Configure your CloudFront distribution to use Match Viewer as its Origin Protocol Policy which will automatically match the user request. This will allow access to the private content if the request is a paying member and deny it if it is not a**

member is incorrect because a Match Viewer is an Origin Protocol Policy which configures CloudFront to communicate with your origin using HTTP or HTTPS, depending on the protocol of the viewer request. CloudFront caches the object only once even if viewers make requests using both HTTP and HTTPS protocols.

The option that says: **Create a Signed URL with a custom policy which only allows the members to see the private files** is incorrect because Signed URLs are primarily used for providing access to individual files, as shown on the above explanation. In addition, the scenario explicitly says that they don't want to change their current URLs which is why implementing Signed Cookies is more suitable than Signed URL.

The option that says: **Configure your CloudFront distribution to use Field-Level Encryption to protect your private data and only allow access to members** is incorrect because Field-Level Encryption only allows you to securely upload user-submitted sensitive information to your web servers. It does not provide access to download multiple private files.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-choosing-signed-urls-cookies.html>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-cookies.html>

Question 53. A Solutions Architect is hosting a website in an Amazon S3 bucket named techstartup. The users load the website using the following URL: `http://techstartup.s3-website-us-east-1.amazonaws.com` and there is a new requirement to add a JavaScript on the webpages in order to make authenticated HTTP GET requests against the same bucket by using the Amazon S3 API endpoint (`techstartup.s3.amazonaws.com`). Upon testing, you noticed that the web browser blocks JavaScript from allowing those requests.

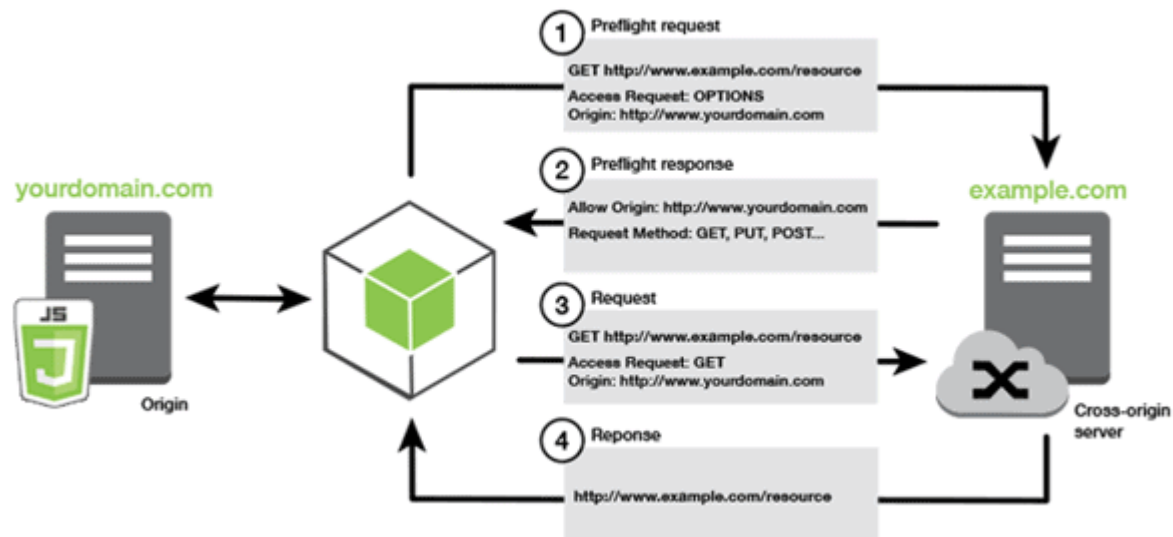
Which of the following options is the MOST suitable solution that you should implement for this scenario?

- 1. ☐ A. Enable Cross-Region Replication (CRR).
- 2. ☐ B. Enable cross-account access.
- 3. ☐ C. Enable Cross-origin resource sharing (CORS) configuration in the bucket.
- 4. ☐ D. Enable Cross-Zone Load Balancing.

Correct Answer: C

Explanation: Cross-origin resource sharing (CORS) defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. With CORS

support, you can build rich client-side web applications with Amazon S3 and selectively allow cross-origin access to your Amazon S3 resources.



Suppose that you are hosting a website in an Amazon S3 bucket named your-website and your users load the website endpoint `http://your-website.s3-website-us-east-1.amazonaws.com`. Now you want to use JavaScript on the webpages that are stored in this bucket to be able to make authenticated GET and PUT requests against the same bucket by using the Amazon S3 API endpoint for the bucket, `your-website.s3.amazonaws.com`. A browser would normally block JavaScript from allowing those requests, but with CORS you can configure your bucket to explicitly enable cross-origin requests from `your-website.s3-website-us-east-1.amazonaws.com`.

In this scenario, you can solve the issue by enabling the CORS in the S3 bucket. Hence, **enabling Cross-origin resource sharing (CORS) configuration in the bucket** is the correct answer.

Enabling cross-account access is incorrect because cross-account access is a feature in IAM and not in Amazon S3.

Enabling Cross-Zone Load Balancing is incorrect because Cross-Zone Load Balancing is only used in ELB and not in S3.

Enabling Cross-Region Replication (CRR) is incorrect because CRR is a bucket-level configuration that enables automatic, asynchronous copying of objects across buckets in different AWS Regions.

References:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ManageCorsUsing.html>

Question 54. A company hosted a web application in an Auto Scaling group of EC2 instances. The IT manager is concerned about the over-provisioning of the resources that can cause higher operating costs. A Solutions Architect has been instructed to create a cost-effective solution without affecting the performance of the application.

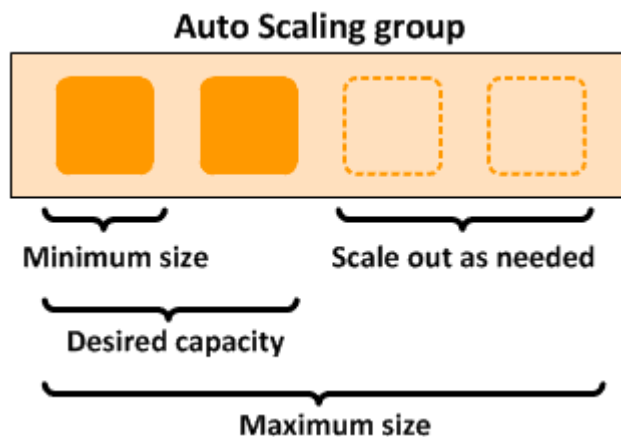
Which dynamic scaling policy should be used to satisfy this requirement?

- 1. ☐ A. Use simple scaling.
- 2. ☐ B. Use target tracking scaling.
- 3. ☐ C. Use suspend and resume scaling.
- 4. ☐ D. Use scheduled scaling.

Correct Answer: B

Explanation: An **Auto Scaling group** contains a collection of Amazon EC2 instances that are treated as a logical grouping for the purposes of automatic scaling and management. An Auto Scaling group also enables you to use Amazon EC2 Auto Scaling features such as health check replacements and scaling policies. Both maintaining the number of instances in an Auto Scaling group and automatic scaling are the core functionality of the Amazon EC2 Auto Scaling service. The size of an Auto Scaling group depends on the number of instances that you set as the desired capacity. You can adjust its size to meet demand, either manually or by using automatic scaling.

Step scaling policies and simple scaling policies are two of the dynamic scaling options available for you to use. Both require you to create CloudWatch alarms for the scaling policies. Both require you to specify the high and low thresholds for the alarms. Both require you to define whether to add or remove instances, and how many, or set the group to an exact size. The main difference between the policy types is the step adjustments that you get with step scaling policies. When step adjustments are applied, and they increase or decrease the current capacity of your Auto Scaling group, the adjustments vary based on the size of the alarm breach.



The primary issue with simple scaling is that after a scaling activity is started, the policy must wait for the scaling activity or health check replacement to complete and the cooldown period to

expire before responding to additional alarms. Cooldown periods help to prevent the initiation of additional scaling activities before the effects of previous activities are visible.

With a target tracking scaling policy, you can increase or decrease the current capacity of the group based on a target value for a specific metric. This policy will help resolve the over-provisioning of your resources. The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to changes in the metric due to a changing load pattern.

Hence, the correct answer is: **Use target tracking scaling.**

The option that says: **Use simple scaling** is incorrect because you need to wait for the cooldown period to complete before initiating additional scaling activities. Target tracking or step scaling policies can trigger a scaling activity immediately without waiting for the cooldown period to expire.

The option that says: **Use scheduled scaling** is incorrect because this policy is mainly used for predictable traffic patterns. You need to use the target tracking scaling policy to optimize the cost of your infrastructure without affecting the performance.

The option that says: **Use suspend and resume scaling** is incorrect because this type is used to temporarily pause scaling activities triggered by your scaling policies and scheduled actions.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html>

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

Question 55. A company has 3 DevOps engineers that are handling its software development and infrastructure management processes. One of the engineers accidentally deleted a file hosted in Amazon S3 which has caused disruption of service.

What can the DevOps engineers do to prevent this from happening again?

- 1. ☐ A. Create an IAM bucket policy that disables delete operation.
- 2. ☐ B. Set up a signed URL for all users.
- 3. ☐ C. Use S3 Infrequently Accessed storage to store the data.
- 4. ☐ D. Enable S3 Versioning and Multi-Factor Authentication Delete on the bucket.

Correct Answer: D

Explanation: To avoid accidental deletion in Amazon S3 bucket, you can:

- Enable Versioning
- Enable MFA (Multi-Factor Authentication) Delete

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures.

If the MFA (Multi-Factor Authentication) Delete is enabled, it requires additional authentication for either of the following operations:

- Change the versioning state of your bucket
- Permanently delete an object version

Using S3 Infrequently Accessed storage to store the data is incorrect. Switching your storage class to S3 Infrequent Access won't help mitigate accidental deletions.

Setting up a signed URL for all users is incorrect. Signed URLs give you more control over access to your content, so this feature deals more on accessing rather than deletion.

Creating an IAM bucket policy that disables delete operation is incorrect. If you create a bucket policy preventing deletion, other users won't be able to delete objects that should be deleted. You only want to prevent accidental deletion, not disable the action itself.

Reference:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html>

Question 56. A media company has an Amazon ECS Cluster, which uses the Fargate launch type, to host its news website. The database credentials should be supplied using environment variables, to comply with strict security compliance. As the Solutions Architect, you have to ensure that the credentials are secure and that they cannot be viewed in plaintext on the cluster itself.

Which of the following is the most suitable solution in this scenario that you can implement with minimal effort?

- 1. ☐ A. Store the database credentials in the ECS task definition file of the ECS Cluster and encrypt it with KMS. Store the task definition JSON file in a private S3 bucket and ensure that HTTPS is enabled on the bucket to encrypt the data in-flight. Create an IAM role to the ECS task definition script that allows access to the specific S3 bucket and then pass the `--cli-input-json` parameter when calling the ECS `register-task-definition`. Reference the task definition JSON file in the S3 bucket which contains the database credentials.

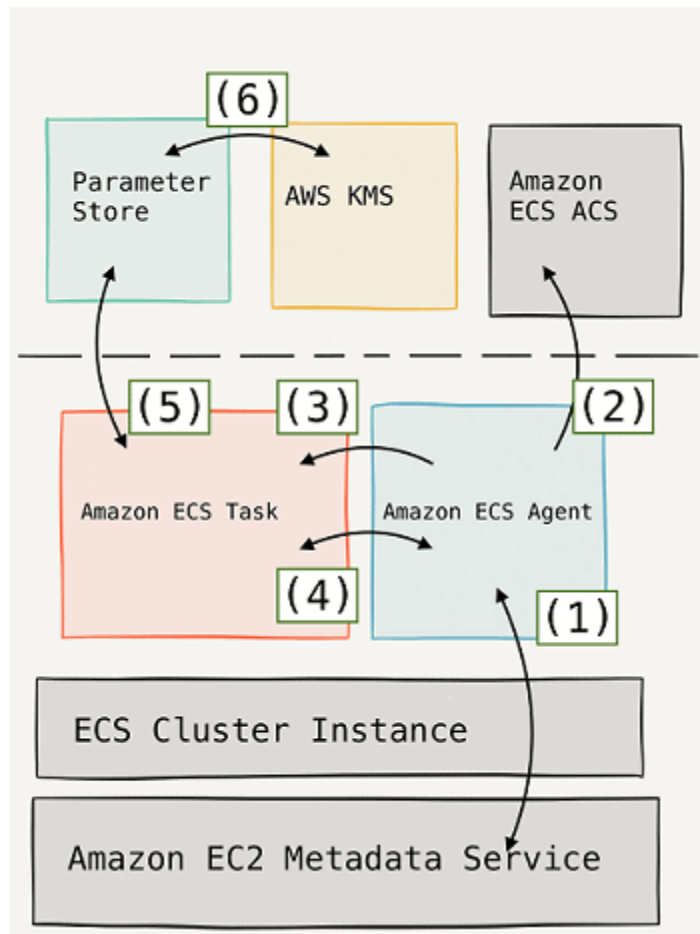
- 2. ☐ B. Use the AWS Systems Manager Parameter Store to keep the database credentials and then encrypt them using AWS KMS. Create an IAM Role for your Amazon ECS task execution role (taskRoleArn) and reference it with your task definition, which allows access to both KMS and the Parameter Store. Within your container definition, specify secrets with the name of the environment variable to set in the container and the full ARN of the Systems Manager Parameter Store parameter containing the sensitive data to present to the container.
- 3. ☐ C. In the ECS task definition file of the ECS Cluster, store the database credentials using Docker Secrets to centrally manage these sensitive data and securely transmit it to only those containers that need access to it. Secrets are encrypted during transit and at rest. A given secret is only accessible to those services which have been granted explicit access to it via IAM Role, and only while those service tasks are running.
- 4. ☐ D. Use the AWS Secrets Manager to store the database credentials and then encrypt them using AWS KMS. Create a resource-based policy for your Amazon ECS task execution role (taskRoleArn) and reference it with your task definition which allows access to both KMS and AWS Secrets Manager. Within your container definition, specify secrets with the name of the environment variable to set in the container and the full ARN of the Secrets Manager secret which contains the sensitive data, to present to the container.

Correct Answer: B

Explanation: Amazon ECS enables you to inject sensitive data into your containers by storing your sensitive data in either AWS Secrets Manager secrets or AWS Systems Manager Parameter Store parameters and then referencing them in your container definition. This feature is supported by tasks using both the EC2 and Fargate launch types.

Secrets can be exposed to a container in the following ways:

- To inject sensitive data into your containers as environment variables, use the secrets container definition parameter.
- To reference sensitive information in the log configuration of a container, use the secretOptions container definition parameter.



Within your container definition, specify secrets with the name of the environment variable to set in the container and the full ARN of either the Secrets Manager secret or Systems Manager Parameter Store parameter containing the sensitive data to present to the container. The parameter that you reference can be from a different Region than the container using it, but must be from within the same account.

Hence, the correct answer is the option that says: *Use the AWS Systems Manager Parameter Store to keep the database credentials and then encrypt them using AWS KMS. Create an IAM Role for your Amazon ECS task execution role (taskRoleArn) and reference it with your task definition, which allows access to both KMS and the Parameter Store. Within your container definition, specify secrets with the name of the environment variable to set in the container and the full ARN of the Systems Manager Parameter Store parameter containing the sensitive data to present to the container.*

The option that says: *In the ECS task definition file of the ECS Cluster, store the database credentials using Docker Secrets to centrally manage these sensitive data and securely transmit it to only those containers that need access to it. Secrets are encrypted during transit and at rest. A given secret is only accessible to those services which have been granted explicit access to it via IAM Role, and only while those service tasks are running* is incorrect because although you can use Docker Secrets to secure the sensitive database credentials, this feature is

only applicable in Docker Swarm. In AWS, the recommended way to secure sensitive data is either through the use of Secrets Manager or Systems Manager Parameter Store.

The option that says: *Store the database credentials in the ECS task definition file of the ECS Cluster and encrypt it with KMS. Store the task definition JSON file in a private S3 bucket and ensure that HTTPS is enabled on the bucket to encrypt the data in-flight. Create an IAM role to the ECS task definition script that allows access to the specific S3 bucket and then pass the `--cli-input-json` parameter when calling the ECS `register-task-definition`. Reference the task definition JSON file in the S3 bucket which contains the database credentials* is incorrect because although the solution may work, it is not recommended to store sensitive credentials in S3. This entails a lot of overhead and manual configuration steps which can be simplified by simply using the Secrets Manager or Systems Manager Parameter Store.

The option that says: *Use the AWS Secrets Manager to store the database credentials and then encrypt them using AWS KMS. Create a resource-based policy for your Amazon ECS task execution role (`taskRoleArn`) and reference it with your task definition which allows access to both KMS and AWS Secrets Manager. Within your container definition, specify secrets with the name of the environment variable to set in the container and the full ARN of the Secrets Manager secret which contains the sensitive data, to present to the container* is incorrect because although the use of Secrets Manager in securing sensitive data in ECS is valid, using an IAM Role is a more suitable choice over a resource-based policy for the Amazon ECS task execution role.

References:

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/specifying-sensitive-data.html>

<https://aws.amazon.com/blogs/mt/the-right-way-to-store-secrets-using-parameter-store/>

Question 57. An application consists of multiple EC2 instances in private subnets in different availability zones. The application uses a single NAT Gateway for downloading software patches from the Internet to the instances. There is a requirement to protect the application from a single point of failure when the NAT Gateway encounters a failure or if its availability zone goes down.

How should the Solutions Architect redesign the architecture to be more highly available and cost-effective.

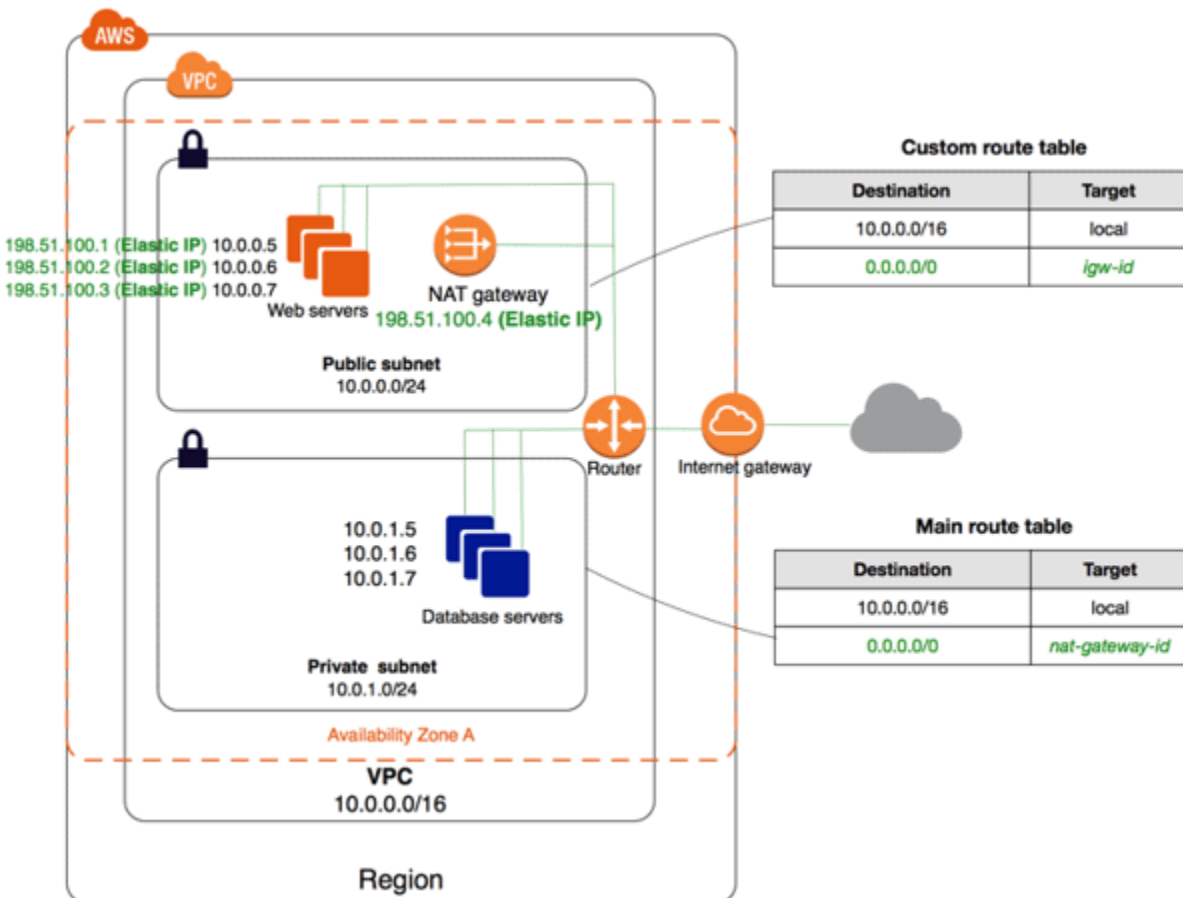
- 1. ☐ A. Create a NAT Gateway in each availability zone. Configure the route table in each public subnet to ensure that instances use the NAT Gateway in the same availability zone.
- 2. ☐ B. Create three NAT Gateways in each availability zone. Configure the route table in each private subnet to ensure that instances use the NAT Gateway in the same availability zone.

- 3. C. Create two NAT Gateways in each availability zone. Configure the route table in each public subnet to ensure that instances use the NAT Gateway in the same availability zone.
- 4. D. Create a NAT Gateway in each availability zone. Configure the route table in each private subnet to ensure that instances use the NAT Gateway in the same availability zone.

Correct Answer: D

Explanation: A **NAT Gateway** is a highly available, managed Network Address Translation (NAT) service for your resources in a private subnet to access the Internet. NAT gateway is created in a specific Availability Zone and implemented with redundancy in that zone.

You must create a NAT gateway on a public subnet to enable instances in a private subnet to connect to the Internet or other AWS services, but prevent the Internet from initiating a connection with those instances.



If you have resources in multiple Availability Zones and they share one NAT gateway, and if the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose Internet access. To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone.

Hence, the correct answer is: **Create a NAT Gateway in each availability zone. Configure the route table in each private subnet to ensure that instances use the NAT Gateway in the same availability zone.**

The option that says: **Create a NAT Gateway in each availability zone. Configure the route table in each public subnet to ensure that instances use the NAT Gateway in the same availability zone** is incorrect because you should configure the route table in the private subnet and not the public subnet to associate the right instances in the private subnet.

The options that say: **Create two NAT Gateways in each availability zone. Configure the route table in each public subnet to ensure that instances use the NAT Gateway in the same availability zone** and **Create three NAT Gateways in each availability zone. Configure the route table in each private subnet to ensure that instances use the NAT Gateway in the same availability zone** are both incorrect because a single NAT Gateway in each availability zone is enough. NAT Gateway is already redundant in nature, meaning, AWS already handles any failures that occur in your NAT Gateway in an availability zone.

References:

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

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html>

Question 58. A Forex trading platform, which frequently processes and stores global financial data every minute, is hosted in your on-premises data center and uses an Oracle database. Due to a recent cooling problem in their data center, the company urgently needs to migrate their infrastructure to AWS to improve the performance of their applications. As the Solutions Architect, you are responsible in ensuring that the database is properly migrated and should remain available in case of database server failure in the future.

Which of the following is the most suitable solution to meet the requirement?

- 1. ☐ A. Launch an Oracle Real Application Clusters (RAC) in RDS.
- 2. ☐ B. Launch an Oracle database instance in RDS with Recovery Manager (RMAN) enabled.
- 3. ☐ C. Convert the database schema using the AWS Schema Conversion Tool and AWS Database Migration Service. Migrate the Oracle database to a non-cluster Amazon Aurora with a single instance.
- 4. ☐ D. Create an Oracle database in RDS with Multi-AZ deployments.

Correct Answer: D

Explanation: Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB

Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable.

In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.

In this scenario, the best RDS configuration to use is an Oracle database in RDS with Multi-AZ deployments to ensure high availability even if the primary database instance goes down. Hence, **creating an Oracle database in RDS with Multi-AZ deployments** is the correct answer.

Launching an Oracle database instance in RDS with Recovery Manager (RMAN) enabled and **launching an Oracle Real Application Clusters (RAC) in RDS** are incorrect because Oracle RMAN and RAC are not supported in RDS.

The option that says: **Convert the database schema using the AWS Schema Conversion Tool and AWS Database Migration Service. Migrate the Oracle database to a non-cluster Amazon Aurora with a single instance** is incorrect because although this solution is feasible, it takes time to migrate your Oracle database to Aurora, which is not acceptable. Based on this option, the Aurora database is only using a single instance with no Read Replica and is not configured as an Amazon Aurora DB cluster, which could have improved the availability of the database.

References:

<https://aws.amazon.com/rds/details/multi-az/>

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

Question 59. You are designing a banking portal which uses Amazon ElastiCache for Redis as its distributed session management component. Since the other Cloud Engineers in your department have access to your ElastiCache cluster, you have to secure the session data in the portal by requiring them to enter a password before they are granted permission to execute Redis commands.

As the Solutions Architect, which of the following should you do to meet the above requirement?

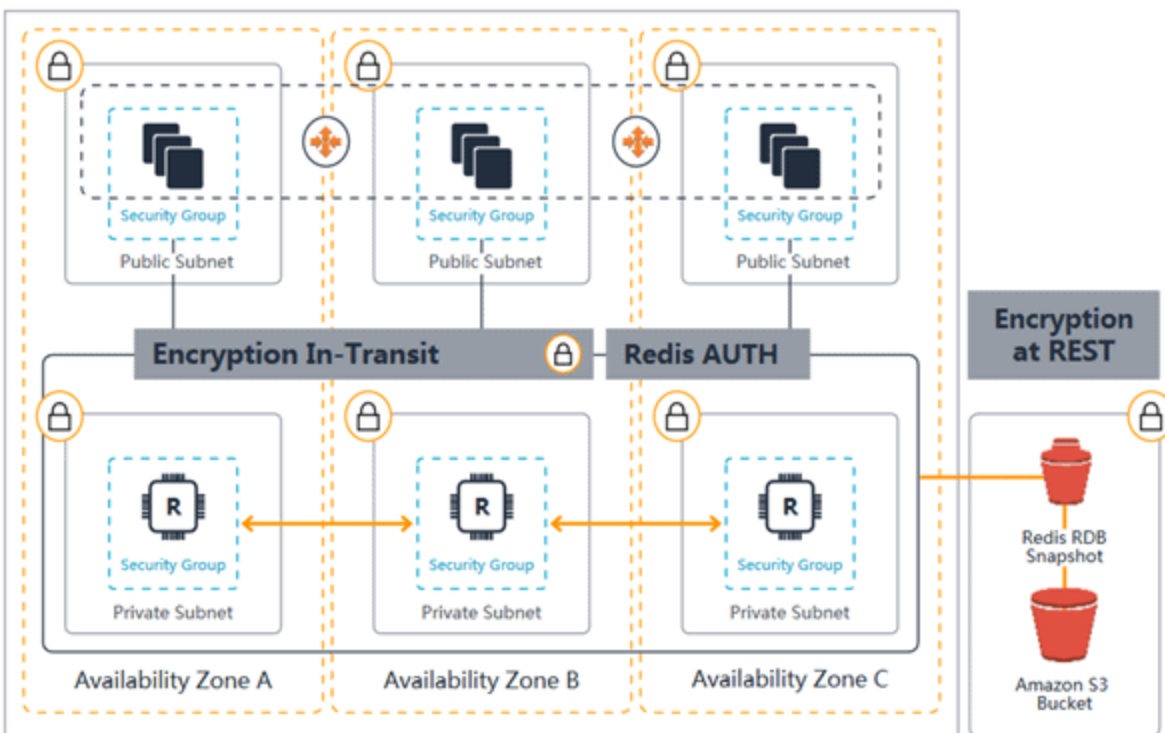
- 1. ☐ A. Enable the in-transit encryption for Redis replication groups.

- 2. ☐ B. Set up an IAM Policy and MFA which requires the Cloud Engineers to enter their IAM credentials and token before they can access the ElastiCache cluster.
- 3. ☐ C. Authenticate the users using Redis AUTH by creating a new Redis Cluster with both the `--transit-encryption-enabled` and `--auth-token` parameters enabled.
- 4. ☐ D. Set up a Redis replication group and enable the `AtRestEncryptionEnabled` parameter.

Correct Answer: C

Explanation: Using Redis AUTH command can improve data security by requiring the user to enter a password before they are granted permission to execute Redis commands on a password protected Redis server. Hence, the correct answer is: **Authenticate the users using Redis AUTH by creating a new Redis Cluster with both the `--transit-encryption-enabled` and `--auth-token` parameters enabled.**

To require that users enter a password on a password-protected Redis server, include the parameter `--auth-token` with the correct password when you create your replication group or cluster and on all subsequent commands to the replication group or cluster.



Setting up an IAM Policy and MFA which requires the Cloud Engineers to enter their IAM credentials and token before they can access the ElastiCache cluster is incorrect because this is not possible in IAM. You have to use the Redis AUTH option instead.

Setting up a Redis replication group and enabling the `AtRestEncryptionEnabled` parameter is incorrect because the Redis At-Rest Encryption

feature only secures the data inside the in-memory data store. You have to use Redis AUTH option instead.

Enabling the in-transit encryption for Redis replication groups is incorrect because although in-transit encryption is part of the solution, it is missing the most important thing which is the Redis AUTH option.

References:

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/auth.html>

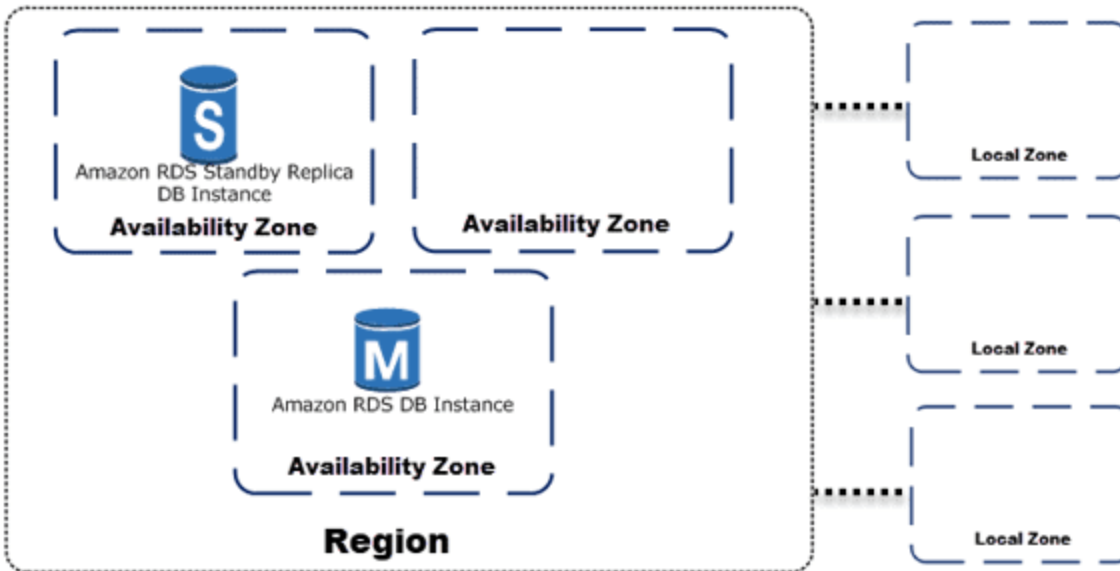
<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/encryption.html>

Question 60. There are a lot of outages in the Availability Zone of your RDS database instance to the point that you have lost access to the database. What could you do to prevent losing access to your database in case that this event happens again?

- 1. ☐ A. Enabled Multi-AZ failover
- 2. ☐ B. Increase the database instance size
- 3. ☐ C. Create a read replica
- 4. ☐ D. Make a snapshot of the database

Correct Answer: A

Explanation: Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. For this scenario, **enabling Multi-AZ failover** is the correct answer. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable.



In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete.

Making a snapshot of the database allows you to have a backup of your database, but it does not provide immediate availability in case of AZ failure. So this is incorrect.

Increasing the database instance size is not a solution for this problem. Doing this action addresses the need to upgrade your compute capacity but does not solve the requirement of providing access to your database even in the event of a loss of one of the Availability Zones.

Creating a read replica is incorrect because this simply provides enhanced performance for read-heavy database workloads. Although you can promote a read replica, its asynchronous replication might not provide you the latest version of your database.

Reference:

<https://aws.amazon.com/rds/details/multi-az/>

Question 61. A company conducted a surprise IT audit on all of the AWS resources being used in the production environment. During the audit activities, it was noted that you are using a combination of Standard and Scheduled Reserved EC2 instances in your applications. They argued that you should have used Spot EC2 instances instead as it is cheaper than the Reserved Instance.

Which of the following are the characteristics and benefits of using these two types of Reserved EC2 instances, which you can use as justification? (Select TWO.)

- 1. ☐ A. Standard Reserved Instances can be later exchanged for other Convertible Reserved Instances

- 2. ☐ B. Reserved Instances don't get interrupted unlike Spot instances in the event that there are not enough unused EC2 instances to meet the demand.
- 3. ☐ C. You can have capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term through Scheduled Reserved Instances
- 4. ☐ D. It can enable you to reserve capacity for your Amazon EC2 instances in multiple Availability Zones and multiple AWS Regions for any duration.
- 5. ☐ E. It runs in a VPC on hardware that's dedicated to a single customer.

Correct Answer: B, C

Explanation: Reserved Instances (RIs) provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. You have the flexibility to change families, OS types, and tenancies while benefiting from RI pricing when you use Convertible RIs. One important thing to remember here is that Reserved Instances are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account.

When your computing needs change, you can modify your Standard or Convertible Reserved Instances and continue to take advantage of the billing benefit. You can modify the Availability Zone, scope, network platform, or instance size (within the same instance type) of your Reserved Instance. You can also sell your unused instance on the Reserved Instance Marketplace.

The option that says: **Reserved Instances don't get interrupted unlike Spot instances in the event that there are not enough unused EC2 instances to meet the demand** is correct. Likewise, the option that says: **You can have capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term through Scheduled Reserved Instances** is correct. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.

The option that says: **Standard Reserved Instances can be later exchanged for other Convertible Reserved Instances** is incorrect because only Convertible Reserved Instances can be exchanged for other Convertible Reserved Instances.

The option that says: **It can enable you to reserve capacity for your Amazon EC2 instances in multiple Availability Zones and multiple AWS Regions for any duration** is incorrect because you can reserve capacity to a specific AWS Region (regional Reserved Instance) or specific Availability Zone (zonal Reserved Instance) only. You cannot reserve capacity to multiple AWS Regions in a single RI purchase.

The option that says: **It runs in a VPC on hardware that's dedicated to a single customer** is incorrect because that is the description of a Dedicated instance and not a Reserved Instance. A Dedicated instance runs in a VPC on hardware that's dedicated to a single customer.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-modifying.html>

<https://aws.amazon.com/ec2/pricing/reserved-instances/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/reserved-instances-types.html>

Question 62. A government entity is conducting a population and housing census in the city. Each household information uploaded on their online portal is stored in encrypted files in Amazon S3. The government assigned its Solutions Architect to set compliance policies that verify sensitive data in a manner that meets their compliance standards. They should also be alerted if there are compromised files detected containing personally identifiable information (PII), protected health information (PHI) or intellectual properties (IP).

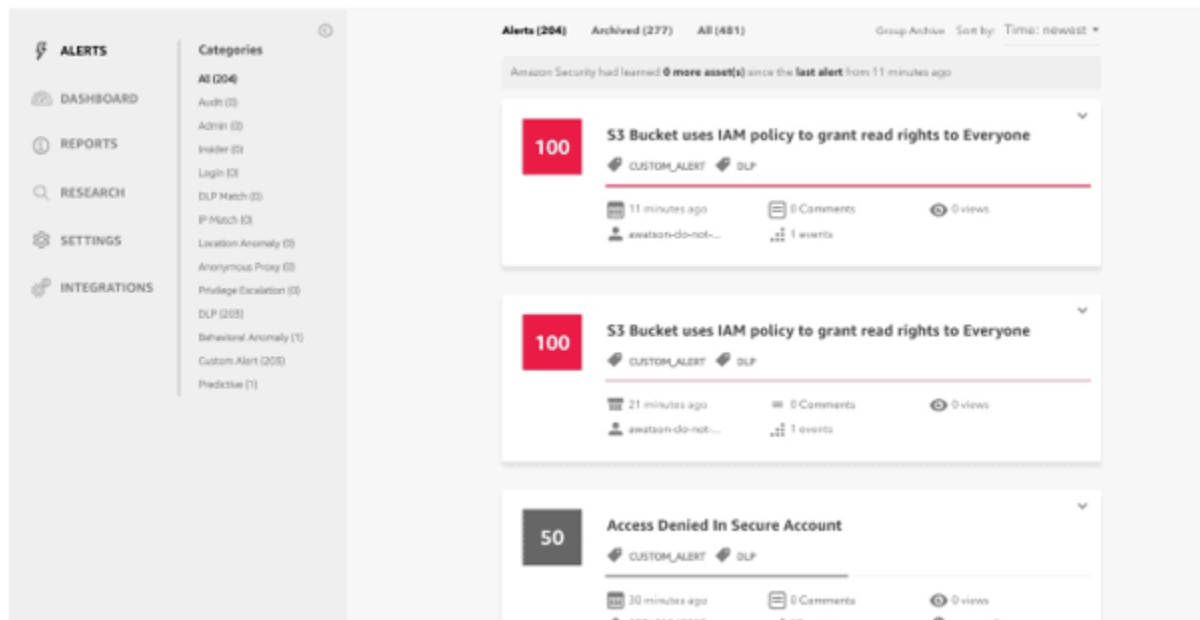
Which of the following should the Architect implement to satisfy this requirement?

- 1. ☐ A. Set up and configure Amazon Inspector to send out alert notifications whenever a security violation is detected on their Amazon S3 data.
- 2. ☐ B. Set up and configure Amazon Rekognition to monitor and recognize patterns on their Amazon S3 data.
- 3. ☐ C. Set up and configure Amazon Macie to monitor and detect usage patterns on their Amazon S3 data.
- 4. ☐ D. Set up and configure Amazon GuardDuty to monitor malicious activity on their Amazon S3 data.

Correct Answer: C

Explanation: Amazon Macie is an ML-powered security service that helps you prevent data loss by automatically discovering, classifying, and protecting sensitive data stored in Amazon S3. Amazon Macie uses machine learning to recognize sensitive data such as personally identifiable information (PII) or intellectual property, assigns a business value, and provides visibility into where this data is stored and how it is being used in your organization.

Amazon Macie continuously monitors data access activity for anomalies, and delivers alerts when it detects risk of unauthorized access or inadvertent data leaks. Amazon Macie has ability to detect global access permissions inadvertently being set on sensitive data, detect uploading of API keys inside source code, and verify sensitive customer data is being stored and accessed in a manner that meets their compliance standards.



Hence, the correct answer is: *Set up and configure Amazon Macie to monitor and detect usage patterns on their Amazon S3 data.*

The option that says: *Set up and configure Amazon Rekognition to monitor and recognize patterns on their Amazon S3 data* is incorrect because Rekognition is simply a service that can identify the objects, people, text, scenes, and activities, as well as detect any inappropriate content on your images or videos.

The option that says: *Set up and configure Amazon GuardDuty to monitor malicious activity on their Amazon S3 data* is incorrect because GuardDuty is just a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.

The option that says: *Set up and configure Amazon Inspector to send out alert notifications whenever a security violation is detected on their Amazon S3 data* is incorrect because Inspector is basically an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

References:

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

<https://aws.amazon.com/macie/faq/>

<https://docs.aws.amazon.com/macie/index.html>

Question 63. A retail website has intermittent, sporadic, and unpredictable transactional workloads throughout the day that are hard to predict. The website is currently hosted on-premises and is slated to be migrated to AWS. A new relational database is needed that

autoscales capacity to meet the needs of the application's peak load and scales back down when the surge of activity is over.

Which of the following option is the MOST cost-effective and suitable database setup in this scenario?

- 1. ☐ A. Launch a DynamoDB Global table with Auto Scaling enabled.
- 2. ☐ B. Launch an Amazon Redshift data warehouse cluster with Concurrency Scaling.
- 3. ☐ C. Launch an Amazon Aurora Provisioned DB cluster with burstable performance DB instance class types.
- 4. ☐ D. Launch an Amazon Aurora Serverless DB cluster then set the minimum and maximum capacity for the cluster.

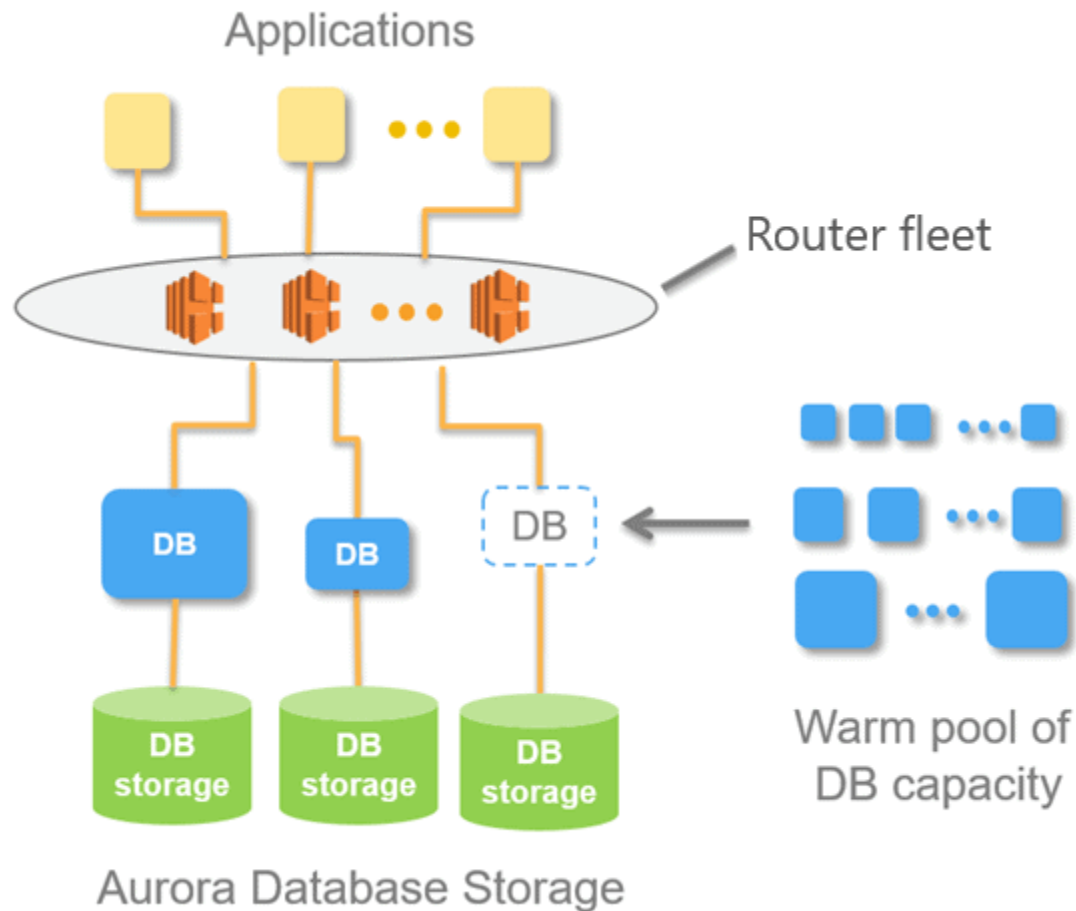
Correct Answer: D

Explanation: Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora. An Aurora Serverless DB cluster is a DB cluster that automatically starts up, shuts down, and scales up or down its compute capacity based on your application's needs. Aurora Serverless provides a relatively simple, cost-effective option for infrequent, intermittent, sporadic or unpredictable workloads. It can provide this because it automatically starts up, scales compute capacity to match your application's usage and shuts down when it's not in use.

Take note that a non-Serverless DB cluster for Aurora is called a provisioned DB cluster. Aurora Serverless clusters and provisioned clusters both have the same kind of high-capacity, distributed, and highly available storage volume.

When you work with Amazon Aurora without Aurora Serverless (provisioned DB clusters), you can choose your DB instance class size and create Aurora Replicas to increase read throughput. If your workload changes, you can modify the DB instance class size and change the number of Aurora Replicas. This model works well when the database workload is predictable, because you can adjust capacity manually based on the expected workload.

However, in some environments, workloads can be intermittent and unpredictable. There can be periods of heavy workloads that might last only a few minutes or hours, and also long periods of light activity, or even no activity. Some examples are retail websites with intermittent sales events, reporting databases that produce reports when needed, development and testing environments, and new applications with uncertain requirements. In these cases and many others, it can be difficult to configure the correct capacity at the right times. It can also result in higher costs when you pay for capacity that isn't used.



With Aurora Serverless, you can create a database endpoint without specifying the DB instance class size. You set the minimum and maximum capacity. With Aurora Serverless, the database endpoint connects to a *proxy fleet* that routes the workload to a fleet of resources that are automatically scaled. Because of the proxy fleet, connections are continuous as Aurora Serverless scales the resources automatically based on the minimum and maximum capacity specifications. Database client applications don't need to change to use the proxy fleet. Aurora Serverless manages the connections automatically. Scaling is rapid because it uses a pool of "warm" resources that are always ready to service requests. Storage and processing are separate, so you can scale down to zero processing and pay only for storage.

Aurora Serverless introduces a new serverless DB engine mode for Aurora DB clusters. Non-Serverless DB clusters use the provisioned DB engine mode.

Hence, the correct answer is: ***Launch an Amazon Aurora Serverless DB cluster then set the minimum and maximum capacity for the cluster.***

The option that says: ***Launch an Amazon Aurora Provisioned DB cluster with burstable performance DB instance class types*** is incorrect because an Aurora Provisioned DB cluster is not suitable for intermittent, sporadic, and unpredictable transactional workloads. This model works well when the database workload is predictable because you can adjust capacity manually

based on the expected workload. A better database setup here is to use an Amazon Aurora Serverless cluster.

The option that says: ***Launch a DynamoDB Global table with Auto Scaling enabled*** is incorrect because although it is using Auto Scaling, the scenario explicitly indicated that you need a relational database to handle your transactional workloads. DynamoDB is a NoSQL database and is not suitable for this use case. Moreover, the use of a DynamoDB Global table is not warranted since this is primarily used if you need a fully managed, multi-region, and multi-master database that provides fast, local, read and write performance for massively scaled, global applications.

The option that says: ***Launch an Amazon Redshift data warehouse cluster with Concurrency Scaling*** is incorrect because this type of database is primarily used for online analytical processing (OLAP) and not for online transactional processing (OLTP). Concurrency Scaling is simply an Amazon Redshift feature that automatically and elastically scales query processing power of your Redshift cluster to provide consistently fast performance for hundreds of concurrent queries.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless.how-it-works.html>

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

Question 64. A global IT company with offices around the world has multiple AWS accounts. To improve efficiency and drive costs down, the Chief Information Officer (CIO) wants to set up a solution that centrally manages their AWS resources. This will allow them to procure AWS resources centrally and share resources such as AWS Transit Gateways, AWS License Manager configurations, or Amazon Route 53 Resolver rules across their various accounts.

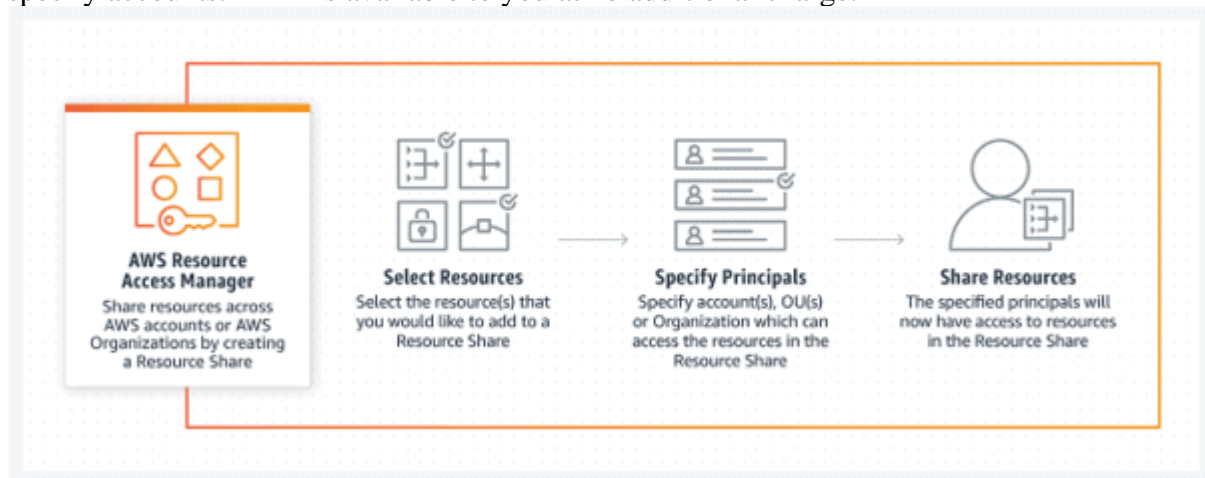
As the Solutions Architect, which combination of options should you implement in this scenario? (Select TWO.)

- 1. ☐ A. Use the AWS Resource Access Manager (RAM) service to easily and securely share your resources with your AWS accounts.
- 2. ☐ B. Consolidate all of the company's accounts using AWS ParallelCluster.
- 3. ☐ C. Consolidate all of the company's accounts using AWS Organizations.
- 4. ☐ D. Use AWS Control Tower to easily and securely share your resources with your AWS accounts.
- 5. ☐ E. Use the AWS Identity and Access Management service to set up cross-account access that will easily and securely share your resources with your AWS accounts.

Correct Answer: A, C

Explanation: AWS Resource Access Manager (RAM) is a service that enables you to easily and securely share AWS resources with any AWS account or within your AWS Organization. You can share AWS Transit Gateways, Subnets, AWS License Manager configurations, and Amazon Route 53 Resolver rules resources with RAM.

Many organizations use multiple accounts to create administrative or billing isolation, and limit the impact of errors. RAM eliminates the need to create duplicate resources in multiple accounts, reducing the operational overhead of managing those resources in every single account you own. You can create resources centrally in a multi-account environment, and use RAM to share those resources across accounts in three simple steps: create a Resource Share, specify resources, and specify accounts. RAM is available to you at no additional charge.



You can procure AWS resources centrally, and use RAM to share resources such as subnets or License Manager configurations with other accounts. This eliminates the need to provision duplicate resources in every account in a multi-account environment, reducing the operational overhead of managing those resources in every account.

AWS Organizations is an account management service that lets you consolidate multiple AWS accounts into an organization that you create and centrally manage. With Organizations, you can create member accounts and invite existing accounts to join your organization. You can organize those accounts into groups and attach policy-based controls.

Hence, the correct combination of options in this scenario is:

- ***Consolidate all of the company's accounts using AWS Organizations.***
- ***Use the AWS Resource Access Manager (RAM) service to easily and securely share your resources with your AWS accounts.***

The option that says: ***Use the AWS Identity and Access Management service to set up cross-account access that will easily and securely share your resources with your AWS accounts*** is incorrect because although you can delegate access to resources that are in different AWS accounts using IAM, this process is extremely tedious and entails a lot of operational overhead

since you have to manually set up cross-account access to each and every AWS account of the company. A better solution is to use AWS Resources Access Manager instead.

The option that says: ***Use AWS Control Tower to easily and securely share your resources with your AWS accounts*** is incorrect because AWS Control Tower simply offers the easiest way to set up and govern a new, secure, multi-account AWS environment. This is not the most suitable service to use to securely share your resources across AWS accounts or within your Organization. You have to use AWS Resources Access Manager (RAM) instead.

The option that says: ***Consolidate all of the company's accounts using AWS ParallelCluster*** is incorrect because AWS ParallelCluster is simply an AWS-supported open-source cluster management tool that makes it easy for you to deploy and manage High-Performance Computing (HPC) clusters on AWS. In this particular scenario, it is more appropriate to use AWS Organizations to consolidate all of your AWS accounts.

References:

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

<https://docs.aws.amazon.com/ram/latest/userguide/shareable.html>