



**Exam** SAA-C03

**Title** AWS Certified Solutions Architect  
Associate Practice Tests for SAA-C02 /  
SAA-C03 Exam

**Version** 5.0

**Product Type** 385 Q&A with explanations



## QUESTION 1

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?

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

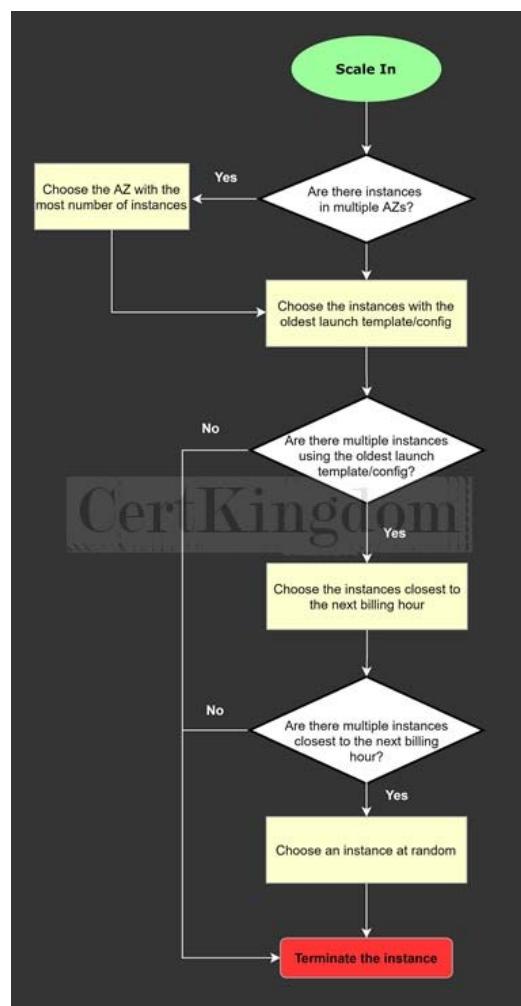
Answer: B

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>

Check out this AWS Auto Scaling Cheat Sheet:

<https://tutorialsdojo.com/aws-auto-scaling/>

## QUESTION 2

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?

A. Use CloudFront in front of the API Gateway to act as a cache.

B. Enable throttling limits and result caching in API Gateway.

C. Switch from using AWS Lambda and API Gateway to a more scalable and highly available architecture using EC2 instances, ELB, and Auto Scaling.

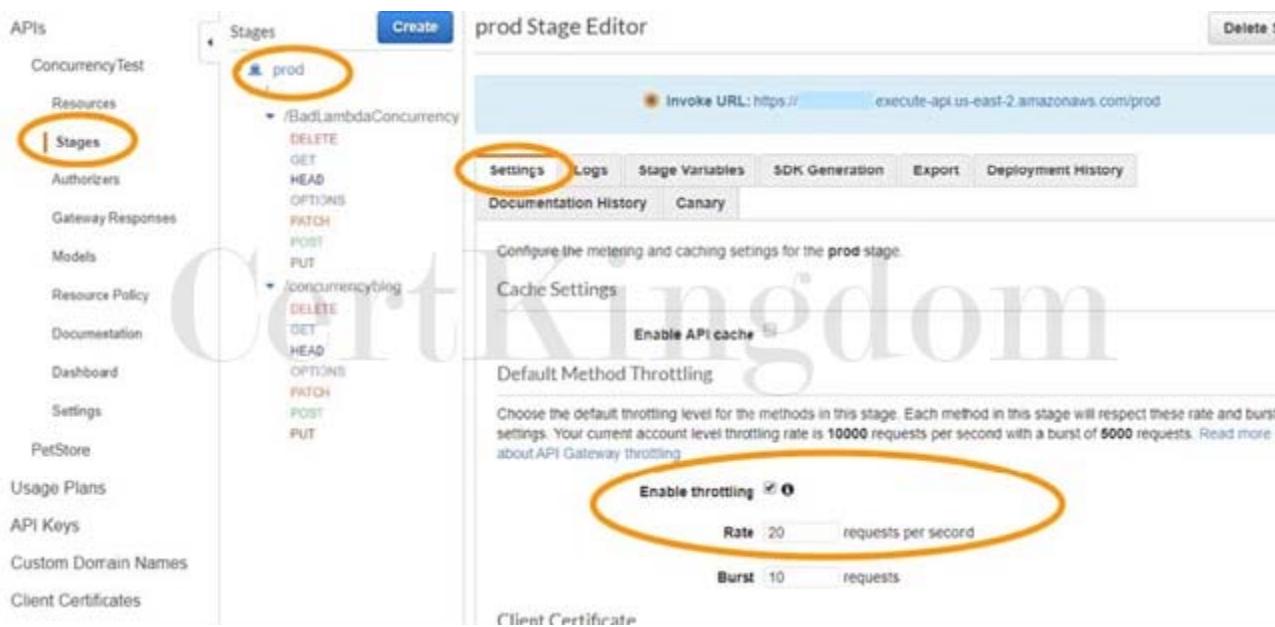
D. Move the Lambda function in a VPC.

Answer: B

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/>

Check out this Amazon API Gateway Cheat Sheet:

<https://tutorialsdojo.com/amazon-api-gateway/>

Here is an in-depth tutorial on Amazon API Gateway:

<https://youtu.be/XwfpPEFHkTQ>

---

### QUESTION 3

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 Convertible Reserved EC2 instances in your applications.

Which of the following are the characteristics and benefits of using these two types of Reserved EC2 instances? (Select TWO.)

- A. Unused Convertible Reserved Instances can later be sold at the Reserved Instance Marketplace.
- B. It runs in a VPC on hardware that's dedicated to a single customer.
- C. Convertible Reserved Instances allow you to exchange for another convertible reserved instance of a different instance family.
- D. It can enable you to reserve capacity for your Amazon EC2 instances in multiple Availability Zones and multiple AWS Regions for any duration.
- E. Unused Standard Reserved Instances can later be sold at the Reserved Instance Marketplace.

Answer: C,E

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.

The offering class of a Reserved Instance is either Standard or Convertible. A Standard Reserved Instance provides a more significant discount than a Convertible Reserved Instance, but you can't exchange a Standard Reserved Instance unlike Convertible Reserved Instances. You can modify Standard and Convertible Reserved Instances. Take note that in Convertible Reserved Instances, you are allowed to exchange another Convertible Reserved instance with a different instance type and tenancy.

The configuration of a Reserved Instance comprises a single instance type, platform, scope, and tenancy over a term. If your computing needs change, you might be able to modify or exchange your Reserved Instance.

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 for Standard RIs but not Convertible RIs on the Reserved Instance Marketplace.

Hence, the correct options are:

- Unused Standard Reserved Instances can later be sold at the Reserved Instance Marketplace.
- Convertible Reserved Instances allow you to exchange for another convertible reserved instance of a different instance family.

The option that says: Unused Convertible Reserved Instances can later be sold at the Reserved Instance Marketplace is incorrect. This is not possible. Only Standard RIs can be sold at the Reserved Instance Marketplace.

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>

Amazon EC2 Overview:

[https://youtu.beVsGIHT\\_jQE](https://youtu.beVsGIHT_jQE)

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

#### QUESTION 4

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.

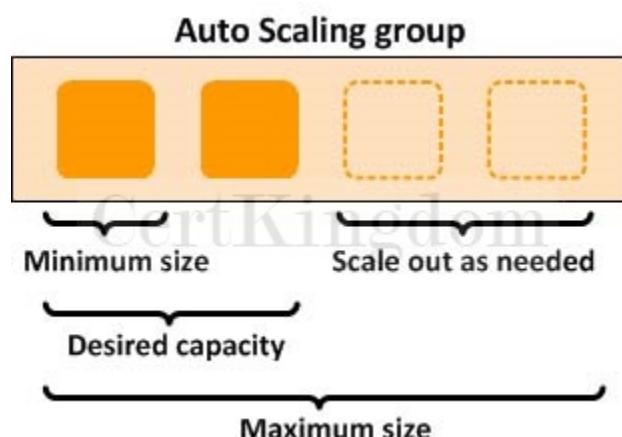
As the Solutions Architect of the company, what should you do to meet the above requirement?

- 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.
- B. 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.
- C. 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.
- D. 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.

Answer: B

Explanation:

Amazon EC2 Auto Scaling helps 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 datacenter 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.

It is required to have 2 instances running all the time. If an AZ outage happened, ASG will launch a new instance on the unaffected AZ. This provisioning does not happen instantly, which means that for a certain period of time, there will only be 1 running instance left.

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 fulfills 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>

Check out this AWS Auto Scaling Cheat Sheet:

<https://tutorialsdojo.com/aws-auto-scaling/>

---

## QUESTION 5

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?

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

Answer: B

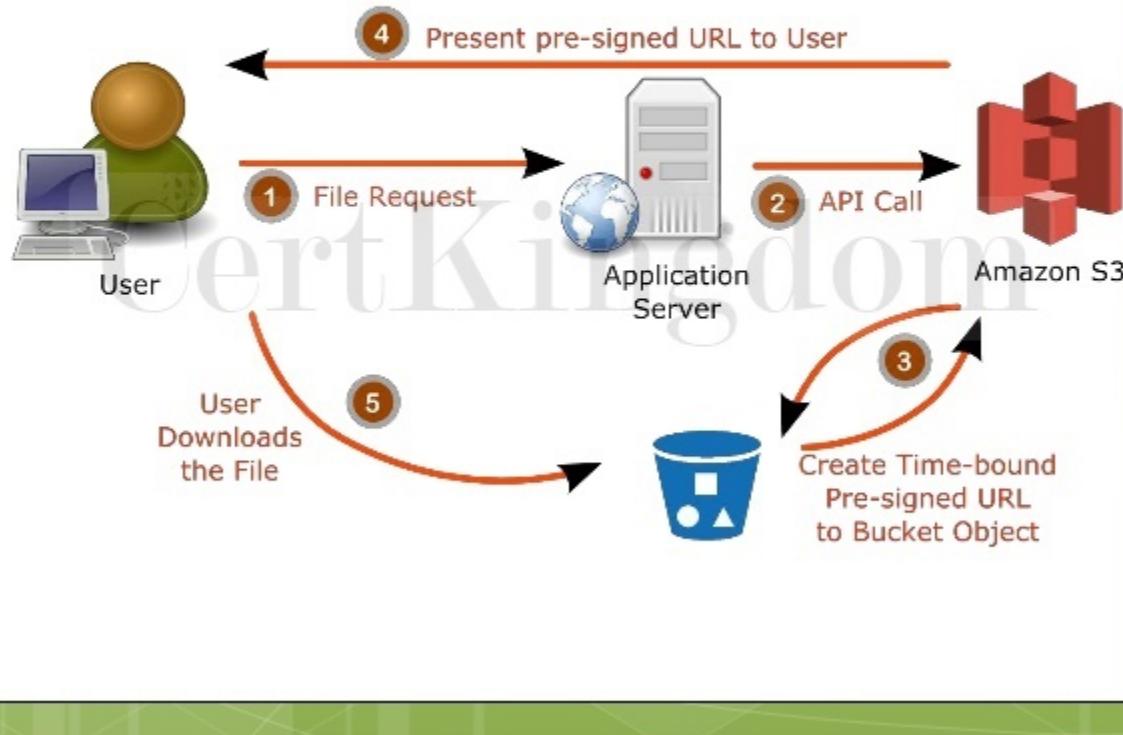
Explanation:

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.

# Complete Flow



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>

Check out this Amazon CloudFront Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudfront/>

S3 Pre-signed URLs vs CloudFront Signed URLs vs Origin Access Identity (OAI)

<https://tutorialsdojo.com/s3-pre-signed-urls-vs-cloudfront-signed-urls-vs-origin-access-identity-oai/>

Comparison of AWS Services Cheat Sheets:

<https://tutorialsdojo.com/comparison-of-aws-services/>

## QUESTION 6

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 the storage of their personal documents.

Which of the following will you need to consider so you can set up a solution that incorporates a 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.)

- 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.
- Set up a Federation proxy or an Identity provider, and use AWS Security Token Service to generate temporary tokens.

- C. Use 3rd party Single Sign-On solutions such as Atlassian Crowd, OKTA, OneLogin and many others.
- D. Configure an IAM role and an IAM Policy to access the bucket.
- E. Map each individual user to a designated user folder in S3 using Amazon WorkDocs to access their personal documents.

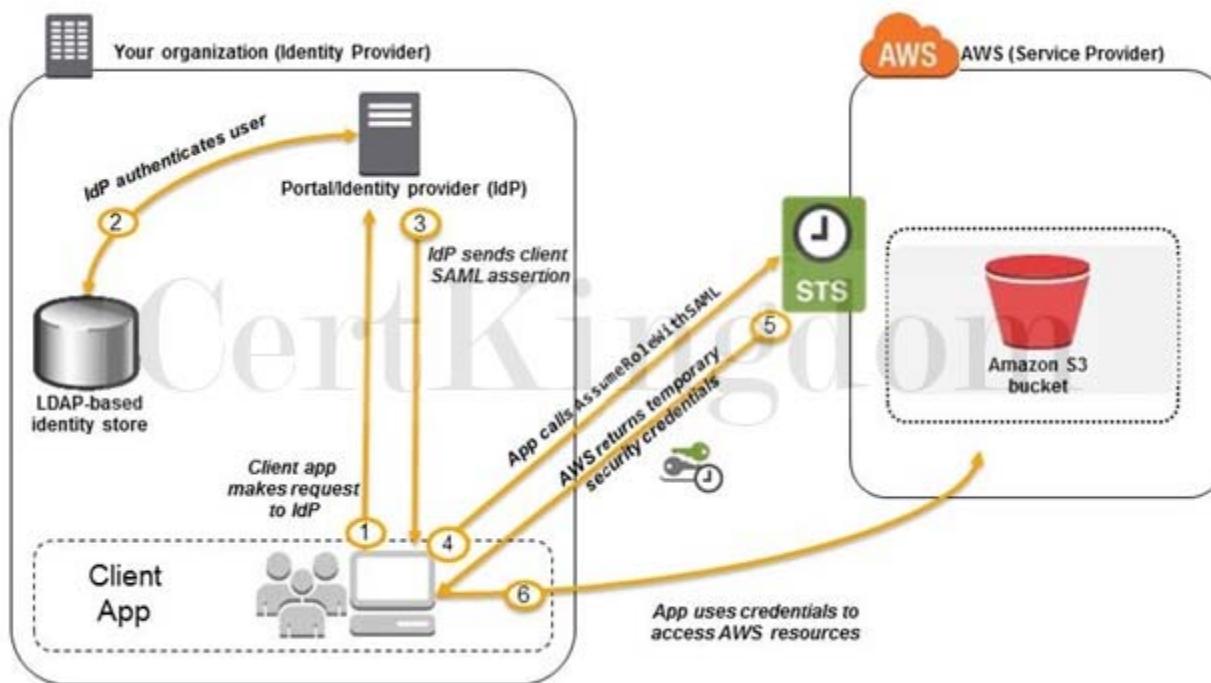
Answer: B,D

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_saml.html)

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_providers\\_oidc.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html)

<https://aws.amazon.com/premiumsupport/knowledge-center/iam-s3-user-specific-folder/>

AWS Identity Services Overview:

<https://youtu.be/AIdUw0i8rr0>

Check out this AWS IAM Cheat Sheet:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

---

## QUESTION 7

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?

- A. Disk Reads activity of an EC2 instance
- B. Memory Utilization of an EC2 instance
- C. Network packets out of an EC2 instance
- D. CPU Utilization of an EC2 instance

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.

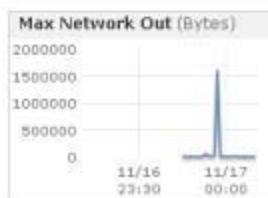
Here's the list of custom metrics that you can set up:

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

[Description](#) [Monitoring](#) [Tags](#)

Graphs are for 1 instance that has monitoring enabled. Times are displayed in UTC.

Time Range: Last Hour



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/monitoring_ec2.html)

[https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html#using\\_put\\_script](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html#using_put_script)

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Check out this Amazon CloudWatch Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudwatch/>

## QUESTION 8

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?

- Set up a new CloudTrail trail in a new S3 bucket using the AWS CLI and also pass both the `--ismulti-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.
- 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.
- Set up a new CloudTrail trail in a new S3 bucket using the AWS CLI and also pass both the `--ismulti-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.
- Set up a new CloudWatch trail in a new S3 bucket using the AWS CLI and also pass both the `--ismulti-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.

Answer: A

## 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, commandline 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.

### Turn on CloudTrail in all regions



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 in 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.

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>

Check out this AWS CloudTrail Cheat Sheet:

<https://tutorialsdojo.com/aws-cloudtrail/>

---

## QUESTION 9

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?

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

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

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

### Type

Select  
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.

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/>

Check out this AWS WAF Cheat Sheet:

<https://tutorialsdojo.com/aws-waf/>

## QUESTION 10

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.)

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

Answer: B,C

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>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

---

## QUESTION 11

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 to implement for your DynamoDB table?

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

Answer: C

#### 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. 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 number 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/>

Check out this Amazon DynamoDB Cheat Sheet:

<https://tutorialsdojo.com/amazon-dynamodb/>

Amazon DynamoDB Overview:

<https://www.youtube.com/watch?v=3ZOyUNIeorU>

---

## QUESTION 12

A car dealership website hosted in Amazon EC2 stores car listings in an Amazon Aurora database managed by Amazon RDS. Once a vehicle has been sold, its data must be removed from the current listings and forwarded to a distributed processing system.

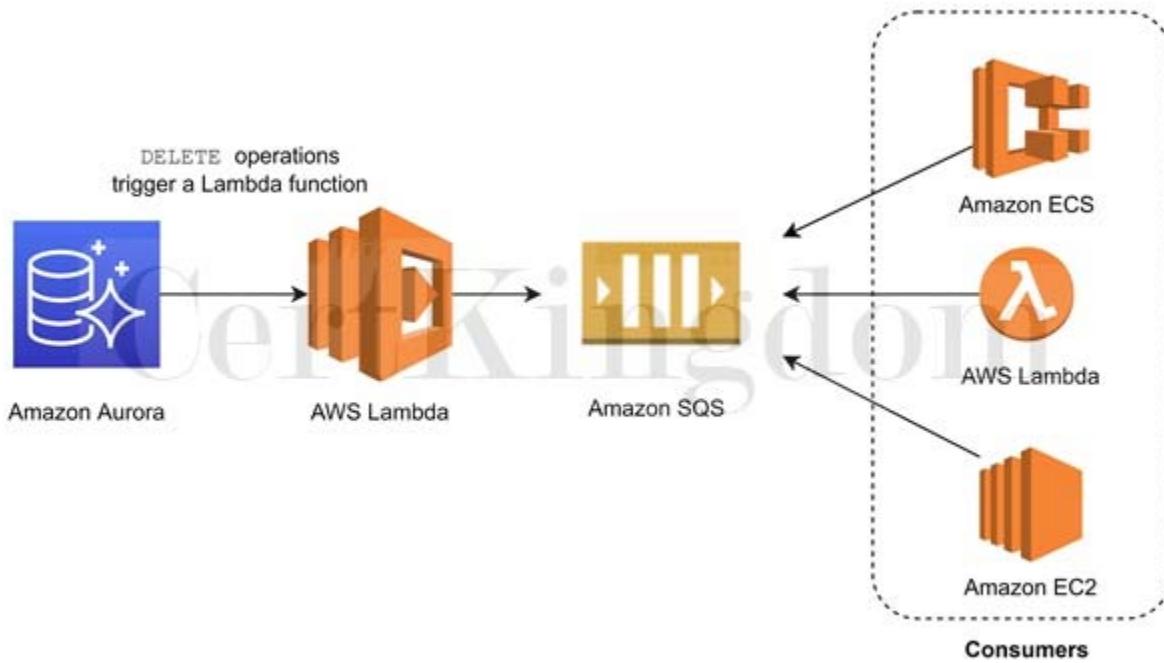
Which of the following options can satisfy the given requirement?

- A. Create an RDS event subscription and send the notifications to Amazon SQS. Configure the SQS queues to fan out the event notifications to multiple Amazon SNS topics. Process the data using Lambda functions.
- B. Create an RDS event subscription and send the notifications to AWS Lambda. Configure the Lambda function to fan out the event notifications to multiple Amazon SQS queues to update the processing system.
- C. Create a native function or a stored procedure that invokes a Lambda function. Configure the Lambda function to send event notifications to an Amazon SQS queue for the processing system to consume.
- D. Create an RDS event subscription and send the notifications to Amazon SNS. Configure the SNS topic to fan out the event notifications to multiple Amazon SQS queues. Process the data using Lambda functions.

Answer: C

#### Explanation:

You can invoke an AWS Lambda function from an Amazon Aurora MySQL-Compatible Edition DB cluster with a native function or a stored procedure. This approach can be useful when you want to integrate your database running on Aurora MySQL with other AWS services. For example, you might want to capture data changes whenever a row in a table is modified in your database.



In the scenario, you can trigger a Lambda function whenever a listing is deleted from the database. You can then write the logic of the function to send the listing data to an SQS queue and have different processes consume it.

Hence, the correct answer is: Create a native function or a stored procedure that invokes a Lambda function. Configure the Lambda function to send event notifications to an Amazon SQS queue for the processing system to consume.

RDS events only provide operational events such as DB instance events, DB parameter group events, DB security group events, and DB snapshot events. What we need in the scenario is to capture datamodifying events (INSERT, DELETE, UPDATE) which can be achieved thru native functions or stored procedures. Hence, the following options are incorrect:

- Create an RDS event subscription and send the notifications to Amazon SQS. Configure the SQS queues to fan out the event notifications to multiple Amazon SNS topics. Process the data using Lambda functions.
- Create an RDS event subscription and send the notifications to AWS Lambda. Configure the Lambda function to fan out the event notifications to multiple Amazon SQS queues to update the processing system.
- Create an RDS event subscription and send the notifications to Amazon SNS. Configure the SNS topic to fan out the event notifications to multiple Amazon SQS queues. Process the data using Lambda functions.

References:

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

<https://aws.amazon.com/blogs/database/capturing-data-changes-in-amazon-aurora-using-aws-lambda/>

Amazon Aurora Overview:

<https://youtu.be/iwS1h7rLNQ>

Check out this Amazon Aurora Cheat Sheet:

<https://tutorialsdojo.com/amazon-aurora/>

### QUESTION 13

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?

- 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.
- B. Use Amazon CloudWatch to monitor the CPU Utilization of your database.
- C. Enable Enhanced Monitoring in RDS.
- D. 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.

Answer: C

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"/> Filter process list						
NAME	VIRT	RES	CPU%	MEM%	VMLIMIT	
postgres [3181] <sup>!</sup>	283.55 MB	17.11 MB	0.02	1.72		
postgres: rdsadmin rdsadmin localhost(40156) idle [2953] <sup>!</sup>	384.7 MB	9.51 MB	0.02	0.95		

Using Amazon CloudWatch to monitor the CPU Utilization of your database is incorrect. 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.

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/USER_Monitoring.OS.html#USER_Monitoring.OS.CloudWatchLogs)

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

Check out this Amazon CloudWatch Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudwatch/>

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

---

## QUESTION 14

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?

- A. 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.
- B. Create a new Amazon SNS FIFO topic for the other team. Grant Amazon S3 permission to send the notification to the second SNS topic.
- C. 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.
- D. Set up another Amazon SQS queue for the other team. Grant Amazon S3 permission to send a notification to the second SQS queue.

Answer: A

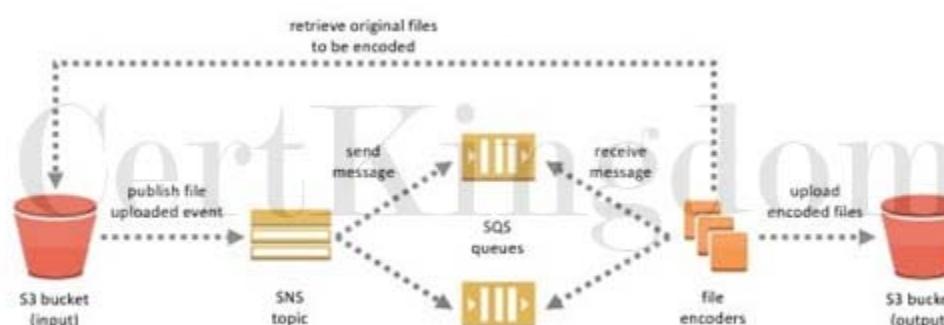
### Explanation:

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. 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>

<https://docs.aws.amazon.com/sns/latest/dg/welcome.html>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

Amazon SNS Overview:

<https://youtu.be/ft5R45lEUJ8>

---

## QUESTION 15

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?

- A. Amazon DynamoDB Accelerator (DAX)
- B. DynamoDB Auto Scaling
- C. Amazon ElastiCache
- D. AWS Device Farm

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>

Check out this Amazon DynamoDB Cheat Sheet:

<https://tutorialsdojo.com/amazon-dynamodb/>

## QUESTION 16

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?

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

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>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

## QUESTION 17

A company collects atmospheric data such as temperature, air pressure, and humidity from different . 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?

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

Answer: C

Explanation:

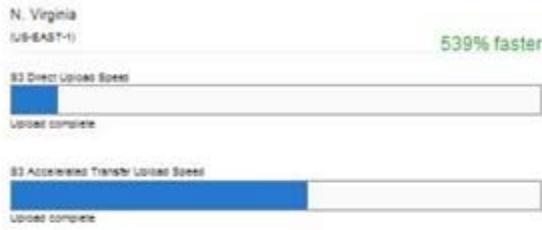
Amazon S3 is object storage built to store and retrieve any amount of data from anywhere on the Internet. It's a simple storage service that offers industry-leading durability, availability, performance, security, and virtually unlimited scalability at very low costs. Amazon S3 is also designed to be 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.



## Amazon S3 Transfer Acceleration

### Speed Comparison

Upload speed comparison in the selected region  
(Based on the location of bucket: us-east-1)



This speed checker uses multipart uploads to transfer a file from your browser to various Amazon S3 regions with and without Amazon S3 Transfer Acceleration. It compares the speed results and shows the percentage difference for every region.

Note: In general, the farther away you are from an Amazon S3 region, the higher the speed improvement you can expect from using Amazon S3 Transfer Acceleration. If you see similar speed results with and without the acceleration, your upload bandwidth or a system constraint might be limiting your speed.

Upload speed comparison in other regions:

N. California (US-WEST-1) <b>73% faster</b>	Oregon (US-WEST-2) <b>17% slower</b>	Ireland (EU-WEST-1) <b>919% faster</b>
S3 Direct Upload Speed	S3 Direct Upload Speed	S3 Direct Upload Speed
Upload complete	Upload complete	Upload complete
S3 Accelerated Transfer Upload Speed	S3 Accelerated Transfer Upload Speed	S3 Accelerated Transfer Upload Speed
Upload complete	Upload complete	Upload complete
Frankfurt (EU-CENTRAL-1) <b>928% faster</b>	Tokyo (AP-NORTHEAST-1) <b>680% faster</b>	Seoul (AP-NORTHEAST-2) <b>822% faster</b>
S3 Direct Upload Speed	S3 Direct Upload Speed	S3 Direct Upload Speed
Upload complete	Upload complete	Upload complete
S3 Accelerated Transfer Upload Speed	S3 Accelerated Transfer Upload Speed	S3 Accelerated Transfer Upload Speed
Upload complete	Upload complete	Upload complete
Singapore (AP-SOUTHEAST-1) <b>1261% faster</b>	Sydney (AP-SOUTHEAST-2) <b>1226% faster</b>	São Paulo (SA-EAST-1) <b>1000% faster</b>
S3 Direct Upload Speed	S3 Direct Upload Speed	S3 Direct Upload Speed
Upload complete	Upload complete	Upload complete
S3 Accelerated Transfer Upload Speed	S3 Accelerated Transfer Upload Speed	S3 Accelerated Transfer Upload Speed
Upload complete	Upload complete	Upload complete

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>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

## QUESTION 18

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?

- A. 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.
- B. 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.
- C. Use Amazon Inspector and install the Inspector agent to all EC2 instances.
- 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.

Answer: B

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:

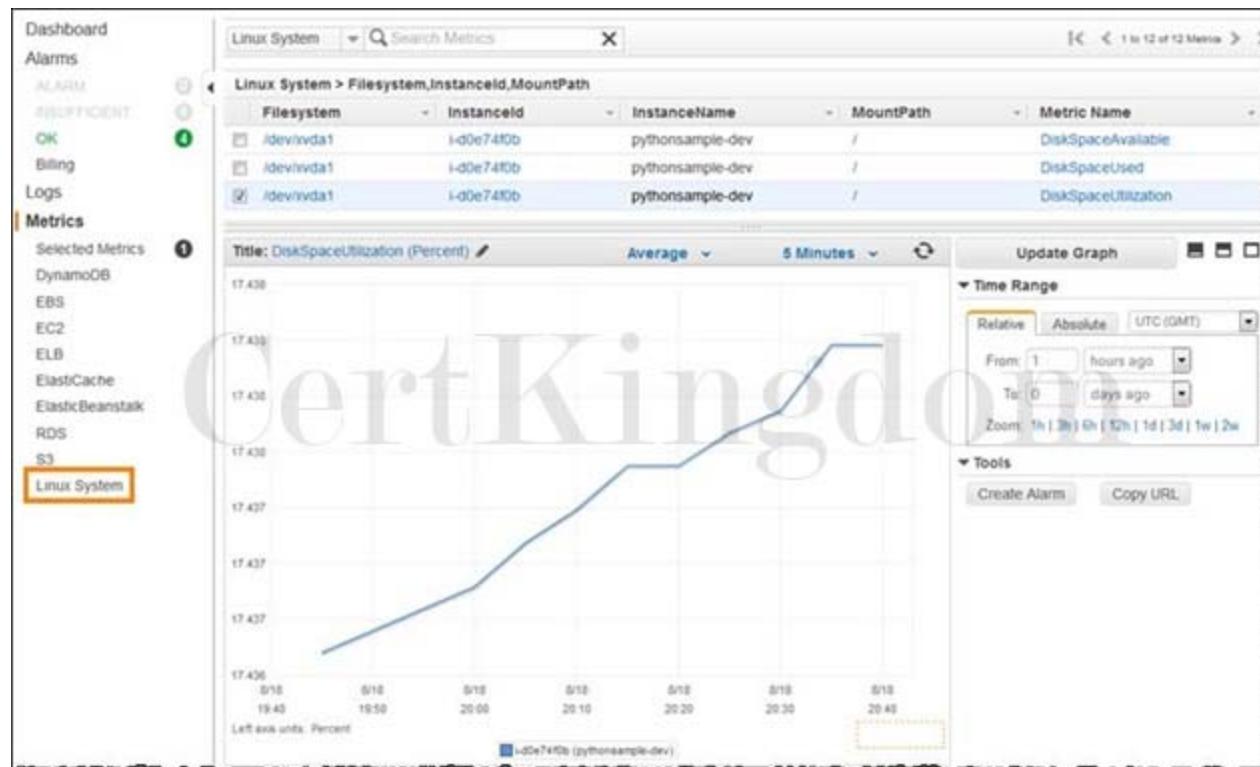
Memory utilization

Disk swap utilization

Disk space utilization

Page file utilization

Log collection



Take note that there is a multi-platform CloudWatch agent which 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 gathers 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/monitoring_ec2.html)

[https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html#using\\_put\\_script](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html#using_put_script)

Check out this Amazon CloudWatch Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudwatch/>

CloudWatch Agent vs SSM Agent vs Custom Daemon Scripts:

<https://tutorialsdojo.com/cloudwatch-agent-vs-ssm-agent-vs-custom-daemon-scripts/>

Comparison of AWS Services Cheat Sheets:

<https://tutorialsdojo.com/comparison-of-aws-services/>

---

## QUESTION 19

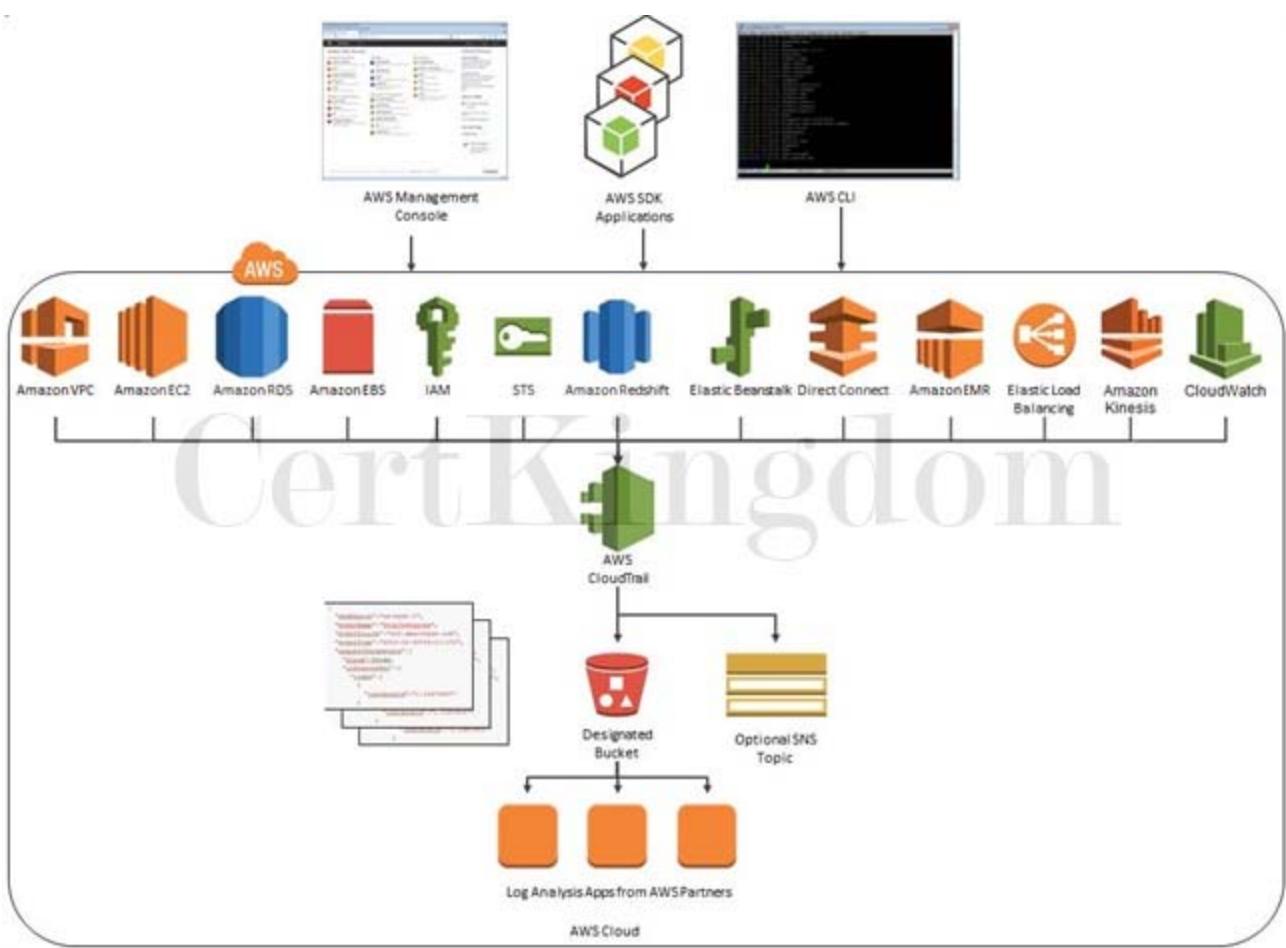
A company needs to design an online analytics application that uses Redshift Cluster for its data warehouse. Which of the following services allows them to monitor all API calls in Redshift instance and can also provide secured data for auditing and compliance purposes?

- A. Amazon Redshift Spectrum
- B. AWS CloudTrail
- C. AWS X-Ray
- D. Amazon CloudWatch

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/awscloudtrail/latest/userguide/cloudtrail-user-guide.html>

Check out this AWS CloudTrail Cheat Sheet:

<https://tutorialsdojo.com/aws-cloudtrail/>

## QUESTION 20

A Solutions Architect needs to set up a relational database and come up with a disaster recovery plan to mitigate multi-region failure. The solution requires a Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of less than 1 minute.

Which of the following AWS services can fulfill this requirement?

- A. Amazon Timestream
- B. Amazon Aurora Global Database
- C. Amazon RDS for PostgreSQL with cross-region read replicas
- D. Amazon Quantum Ledger Database (Amazon QLDB)

Answer: B

## Explanation:

Amazon Aurora Global Database is designed for globally distributed applications, allowing a single Amazon Aurora database to span multiple AWS regions. It replicates your data with no impact on database performance, enables fast local reads with low latency in each region, and provides disaster recovery from region-wide outages.

The screenshot shows the Amazon RDS console under the 'Databases' section. There are two global databases listed: 'global-database-1' and 'global-database-2'. Each database has multiple clusters and instances across different regions. For 'global-database-1', there is one cluster with one instance in us-east-1, and another cluster with one instance in us-east-1a. For 'global-database-2', there are two clusters: one with one instance in us-east-1 and another with one instance in us-east-1a. All instances are marked as 'Available'.

DB Identifier	Role	Engine	Region & AZ	Size	Status	CPU	Current DB
global-database-1	Global	Aurora MySQL	1 region	1 cluster	Available	-	1
global-database-1	Primary	Aurora MySQL	us-east-1	1 instance	Available	-	1
global-database-1	Writer	Aurora MySQL	us-east-1a	db.r5.1.large	Available	-	1
global-database-2	Global	Aurora PostgreSQL	2 regions	2 clusters	Available	-	2
global-database-2	Primary	Aurora PostgreSQL	us-east-1	1 instance	Available	-	1
global-database-2	Writer	Aurora PostgreSQL	us-east-1a	db.r5.1.large	Available	-	1
global-database-2	Secondary	Aurora PostgreSQL	us-east-2	1 instance	Available	-	1
global-database-2	Reader	Aurora PostgreSQL	us-east-2a	db.r5.1.large	Available	100%	1

Aurora Global Database supports storage-based replication that has a latency of less than 1 second. If there is an unplanned outage, one of the secondary regions you assigned can be promoted to read and write capabilities in less than 1 minute. This feature is called Cross-Region Disaster Recovery. An RPO of 1 second and an RTO of less than 1 minute provide you a strong foundation for a global business continuity plan.

Hence, the correct answer is: Amazon Aurora Global Database.

Amazon Quantum Ledger Database (Amazon QLDB) is incorrect because it is stated in the scenario that the Solutions Architect needs to create a relational database and not a ledger database. An Amazon Quantum Ledger Database (QLDB) is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log. Moreover, QLDB cannot provide an RPO of 1 second and an RTO of less than 1 minute.

Multi-AZ Amazon RDS database with cross-region read replicas is incorrect because a Multi-AZ deployment is only applicable inside a single region and not in a multi-region setup. This database setup is not capable of providing an RPO of 1 second and an RTO of less than 1 minute. Moreover, the crossregion RDS Read Replica replication is not as fast as Amazon Aurora Global Databases.

Amazon Timestream is incorrect because this is a serverless time series database service that is commonly used for IoT and operational applications. The most suitable solution for this scenario is to use the Amazon Aurora Global Database since it can provide the required RPO and RTO.

## References:

<https://aws.amazon.com/rds/aurora/global-database/>

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

## Amazon Aurora Overview:

<https://youtu.be/iwS1h7rLNQ>

## Check out this Amazon Aurora Cheat Sheet:

<https://tutorialsdojo.com/amazon-aurora/>

## QUESTION 21

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.

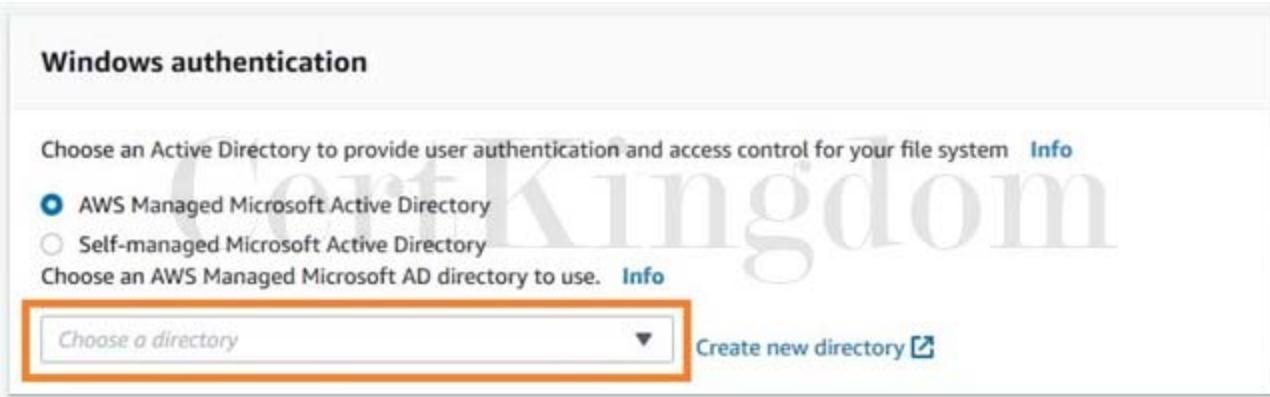
Which of the following options can satisfy the given requirement?

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

Answer: A

## 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.



The screenshot shows the 'Windows authentication' section of the AWS FSx configuration interface. It asks to choose an Active Directory for user authentication. Two options are available: 'AWS Managed Microsoft Active Directory' (selected) and 'Self-managed Microsoft Active Directory'. Below this, it says 'Choose an AWS Managed Microsoft AD directory to use.' There is a 'Create new directory' button at the bottom of the dropdown menu, which is highlighted with a red box.

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 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>

Check out this Amazon FSx Cheat Sheet:

<https://tutorialsdojo.com/amazon-fsx/>

## QUESTION 22

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?

- Create a custom endpoint in Aurora based on the specified criteria for the production traffic and another custom endpoint to handle the reporting queries.
- 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.

C. 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.

D. Do nothing since by default, Aurora will automatically direct the production traffic to your highcapacity instances and the reporting queries to your low-capacity instances.

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.

The screenshot shows the AWS RDS Cluster Overview page for a cluster named 'tutorialsdojo-1'. The top table lists three DB instances: 'tutorialsdojo-1' (Cluster, Aurora MySQL, db.t2.small, Available), 'tutorialsdojo' (Writer, Aurora MySQL, db.t2.small, Available, 9.33% CPU), and 'tutorialsdojo-ap-southeast-2b' (Reader, Aurora MySQL, db.t2.small, Available, 7.70% CPU). Below this is a navigation bar with tabs: Connectivity & security (selected), Monitoring, Logs & events, Configuration, Maintenance & backups, and Tags. Under the 'Connectivity & security' tab, there is a section titled 'Endpoints (2)' with a 'Create custom endpoint' button. A search bar labeled 'Filter endpoint' is present. The bottom table lists two endpoints: 'tutorialsdojo-1.cluster-ro-cerpn6ov4bsw.ap-southeast-2.rds.amazonaws.com' (Available, Reader, Port 3306) and 'tutorialsdojo-1.cluster-cerpn6ov4bsw.ap-southeast-2.rds.amazonaws.com' (Available, Writer, Port 3306).

DB identifier	Role	Engine	Class	Status	CPU	Current
tutorialsdojo-1	Cluster	Aurora MySQL	-	Available		
tutorialsdojo	Writer	Aurora MySQL	db.t2.small	Available	9.33%	
tutorialsdojo-ap-southeast-2b	Reader	Aurora MySQL	db.t2.small	Available	7.70%	

Endpoints (2)			
Endpoint name	Status	Type	Port
tutorialsdojo-1.cluster-ro-cerpn6ov4bsw.ap-southeast-2.rds.amazonaws.com	Available	Reader	3306
tutorialsdojo-1.cluster-cerpn6ov4bsw.ap-southeast-2.rds.amazonaws.com	Available	Writer	3306

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. 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>

Amazon Aurora Overview:

<https://youtu.be/iwS1h7rLNQ>

Check out this Amazon Aurora Cheat Sheet:

<https://tutorialsdojo.com/amazon-aurora/>

---

### QUESTION 23

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?

- A. Amazon SWF
- B. Amazon SQS
- C. Amazon SNS
- D. Amazon MQ

Answer: D

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.

# 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.

### 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.

#### 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.

Create a broker

Broker name  
MyBroker

**Next step**

#### Pricing & costs (US)

mq.t2.micro	\$0.03 per hour
mq.m4.large	\$0.3 per hour
Storage	\$0.5 per GB-month

[Learn more](#)

#### Documentation

[Developer Guide](#)

[API Reference](#)

[FAQs](#)

[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. 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#sqsdifference-from-amazon-mq-sns>

Check out this Amazon MQ Cheat Sheet:

<https://tutorialsdojo.com/amazon-mq/>

### QUESTION 24

An IT consultant is working for a large financial company. The role of the consultant is to help the development team build a highly available web application using stateless web servers.

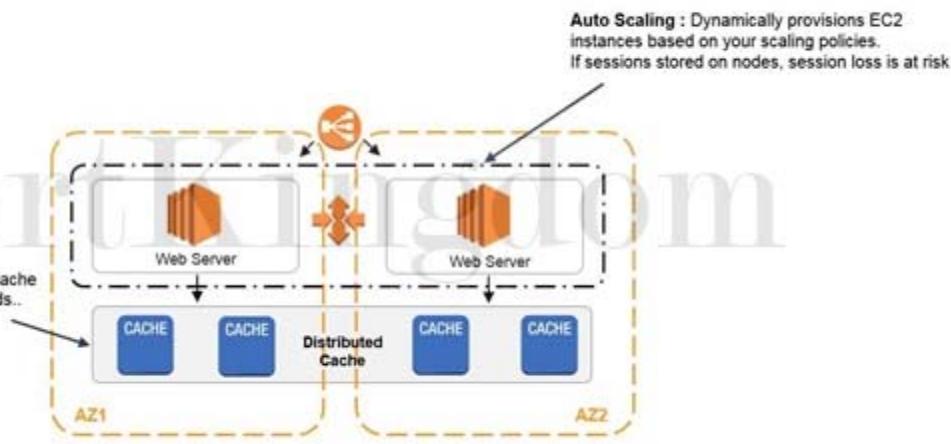
In this scenario, which AWS services are suitable for storing session state data? (Select TWO.)

- A. ElastiCache
- B. Redshift Spectrum
- C. RDS
- D. Glacier
- E. DynamoDB

Answer: A,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 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/>

Check out this Amazon ElastiCache Cheat Sheet:

<https://tutorialsdojo.com/amazon-elasticsearch/>

## QUESTION 25

A company is designing a banking portal that 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?

- A. Authenticate the users using Redis AUTH by creating a new Redis Cluster with both the --transitencryption- enabled and --auth-token parameters enabled.
- B. Set up a Redis replication group and enable the AtRestEncryptionEnabled parameter.
- C. 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.

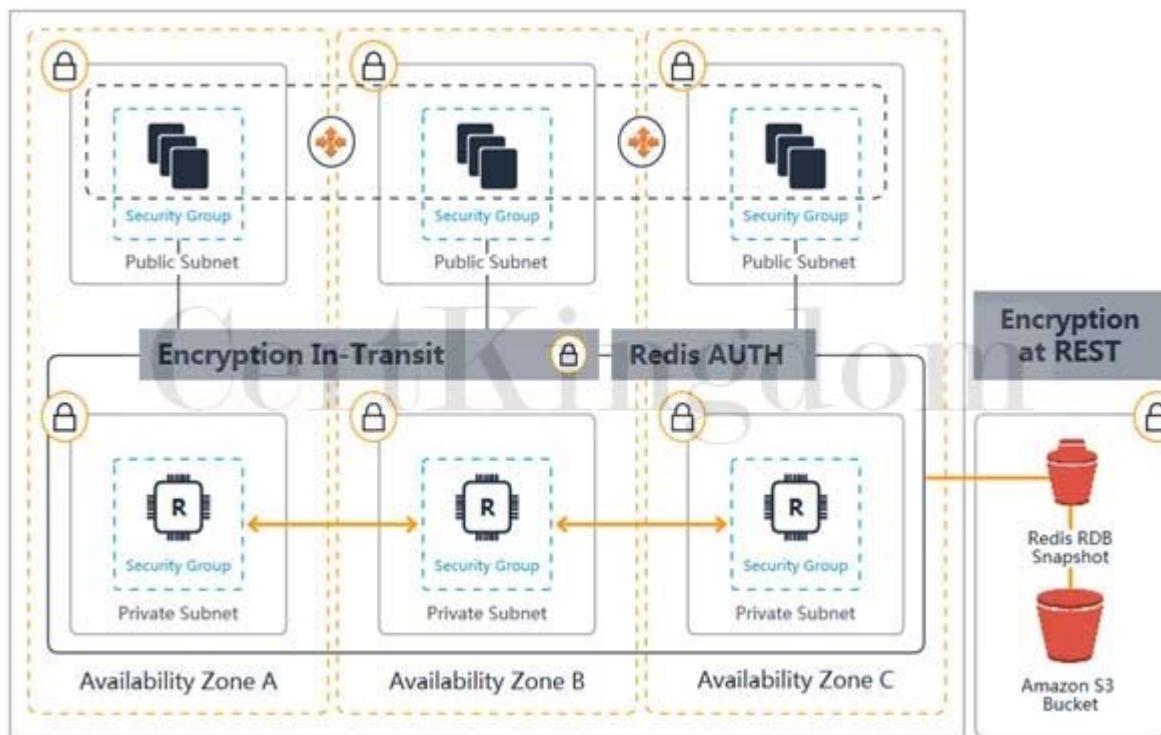
D. Enable the in-transit encryption for Redis replication groups.

Answer: A

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. 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>

Check out this Amazon ElastiCache Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastichache/>

Redis (cluster mode enabled vs disabled) vs Memcached:

<https://tutorialsdojo.com/redis-cluster-mode-enabled-vs-disabled-vs-memcached/>

## QUESTION 26

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.

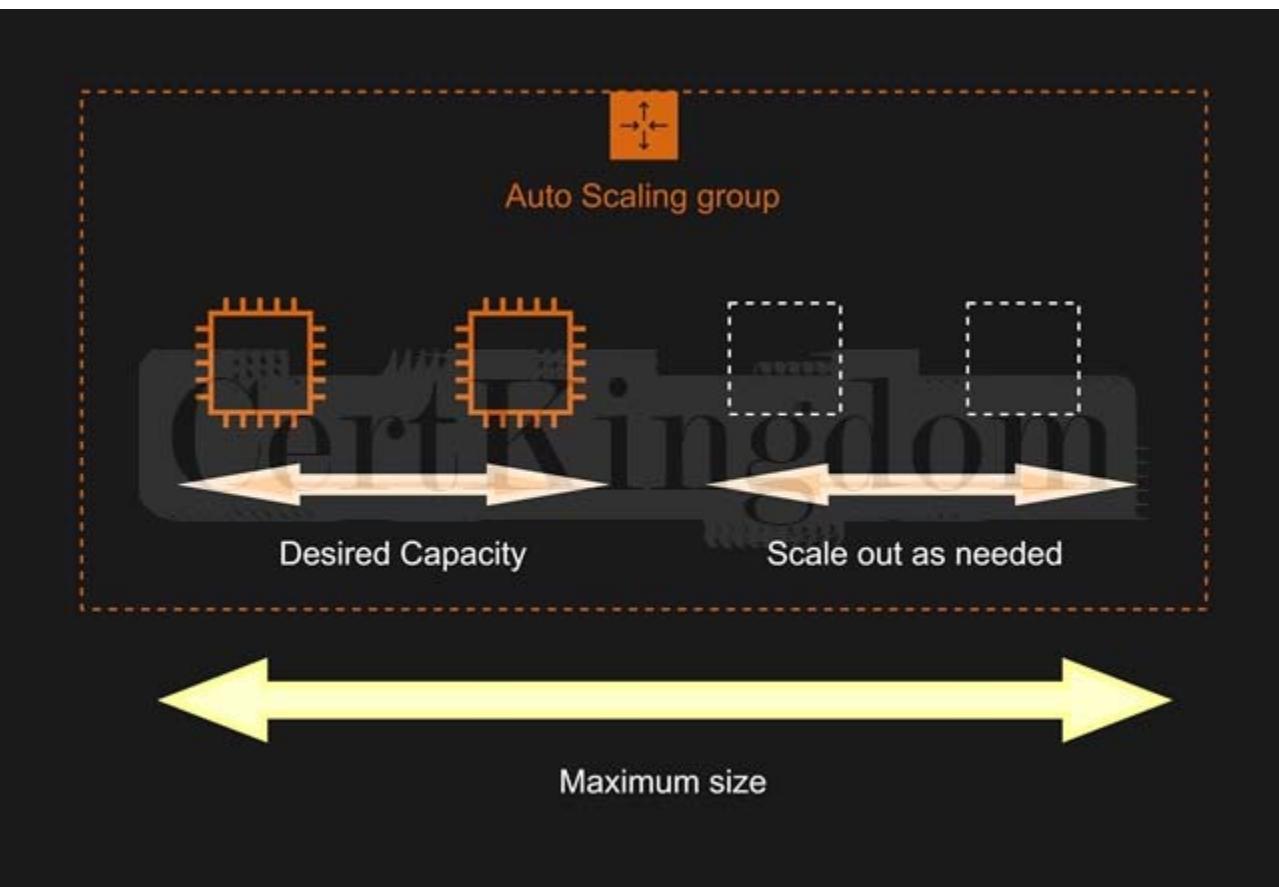
Which of the following can be done to ensure that the application works properly at the beginning of the day?

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

Answer: B

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

Check out this AWS Auto Scaling Cheat Sheet:

<https://tutorialsdojo.com/aws-auto-scaling/>

---

## QUESTION 27

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?

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

Answer: B

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 schemaless 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>

Also check the AWS Certified Solutions Architect Official Study Guide: Associate Exam 1st Edition and turn to page 161 which talks about NoSQL Databases.

Check out this Amazon DynamoDB Cheat Sheet:

<https://tutorialsdojo.com/amazon-dynamodb>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

---

## QUESTION 28

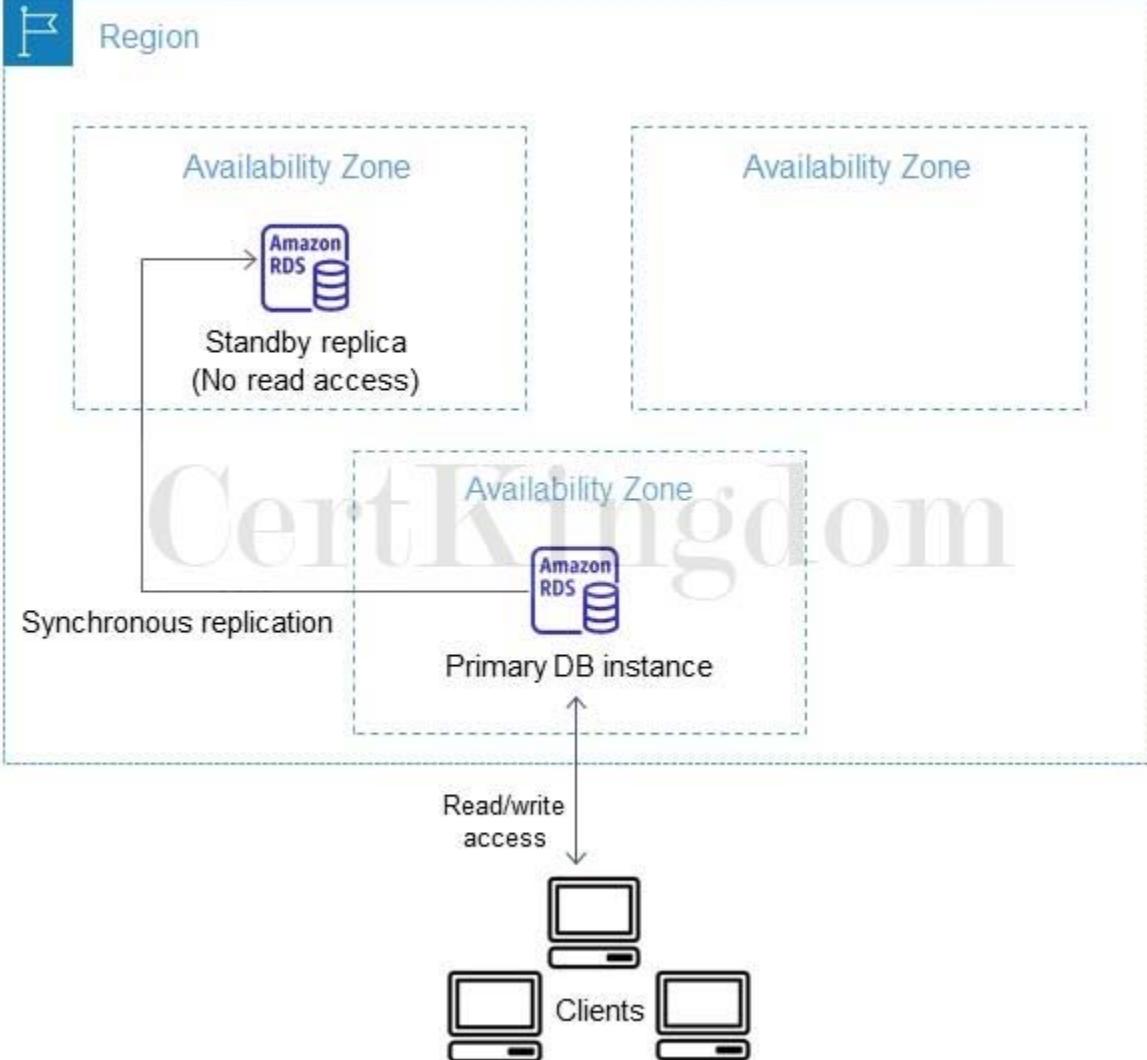
There are a lot of outages in the Availability Zone of your RDS database instance to the point that you have lost access to the database. What could you do to prevent losing access to your database in case that this event happens again?

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

Answer: C

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/>

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

## QUESTION 29

A company wishes to query data that resides in multiple AWS accounts from a central data lake. Each account has its own Amazon S3 bucket that stores data unique to its business function. Users from different accounts must be granted access to the data lake based on their roles.

Which solution will minimize overhead and costs while meeting the required access patterns?

- A. Use AWS Kinesis Firehose to consolidate data from multiple accounts into a single account.
- B. Use AWS Central Tower to centrally manage each account's S3 buckets.

- C. Create a scheduled Lambda function for transferring data from multiple accounts to the S3 buckets of a central account  
D. Use AWS Lake Formation to consolidate data from multiple accounts into a single account.

Answer: D

Explanation:

AWS Lake Formation is a service that makes it easy to set up a secure data lake in days. A data lake is a centralized, curated, and secured repository that stores all your data, both in its original form and prepared for analysis. A data lake enables you to break down data silos and combine different types of analytics to gain insights and guide better business decisions. Amazon S3 forms the storage layer for Lake Formation. If you already use S3, you typically begin by registering existing S3 buckets that contain your data. Lake Formation creates new buckets for the data lake and import data into them. AWS always stores this data in your account, and only you have direct access to it.

The screenshot shows the AWS Lake Formation console. On the left, there's a navigation sidebar with options like 'Dashboard', 'Data catalog', 'Databases', 'Tables' (which is selected and highlighted in green), 'Settings', 'Register and ingest', 'Permissions', and various sub-options for each. The main content area is titled 'AWS Lake Formation > Tables'. It shows a table with two entries: 'Tutorials Dojo Manila' and 'Tutorials Dojo Cabanatuan'. Both entries are associated with the 'sampledb' database and the owner account '12061898'. There are also columns for 'Shared resource' and 'Shared resource ...'. At the top of this section, there's a search bar labeled 'Find table by properties' and a 'Create table' button. A green box highlights the 'Create table using a crawler' button.

AWS Lake Formation is integrated with AWS Glue which you can use to create a data catalog that describes available datasets and their appropriate business applications. Lake Formation lets you define policies and control data access with simple grant and revoke permissions to data sets at granular levels. You can assign permissions to IAM users, roles, groups, and Active Directory users using federation. You specify permissions on catalog objects (like tables and columns) rather than on buckets and objects.

Thus, the correct answer is: Use AWS Lake Formation to consolidate data from multiple accounts into a single account.

The option that says: Use AWS Kinesis Firehose to consolidate data from multiple accounts into a single account is incorrect. Setting up a Kinesis Firehose in each and every account to move data into a single location is costly and impractical. A better approach is to set up cross-account sharing which is free with AWS Lake Formation.

The option that says: Create a scheduled Lambda function for transferring data from multiple accounts to the S3 buckets of a central account is incorrect. This could be done by utilizing the AWS SDK, but implementation would be difficult and quite challenging to manage. Remember that the scenario explicitly mentioned that the solution must minimize management overhead.

The option that says: Use AWS Central Tower to centrally manage each account's S3 buckets is incorrect because the AWS Central Tower service is primarily used to manage and govern multiple AWS accounts and not just S3 buckets. Using the AWS Lake Formation service is a more suitable choice.

References:

<https://aws.amazon.com/blogs/big-data/building-securign-and-managing-data-lakes-with-aws-lake-formation/>

<https://docs.aws.amazon.com/lake-formation/latest/dg/how-it-works.html>

## QUESTION 30

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?

- A. 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.
- B. Create an API using Amazon API Gateway and use AWS Lambda to handle the bursts of traffic in seconds.
- C. 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.
- D. Create an API using Amazon API Gateway and use Amazon Elastic Beanstalk with Auto Scaling to handle the bursts of traffic in seconds.

Answer: B

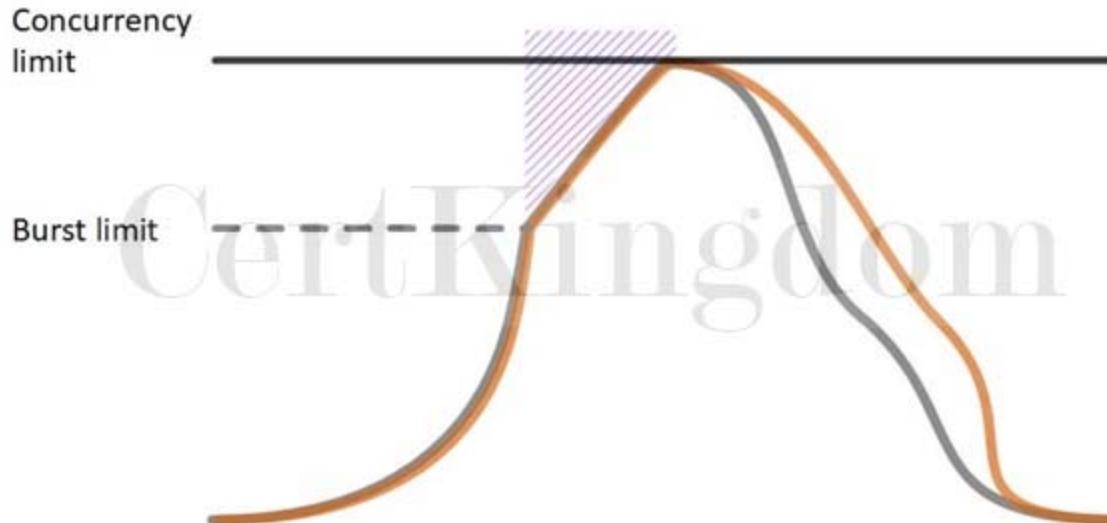
Explanation:

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.

### Function Scaling with Concurrency Limit



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/invocation-scaling.html>

Check out this AWS Lambda Cheat Sheet:

<https://tutorialsdojo.com/aws-lambda/>

---

### QUESTION 31

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?

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

Answer: C

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

Amazon VPC Overview:

<https://www.youtube.com/watch?v=oIDHKeNvxQQ>

Check out this Amazon VPC Cheat Sheet:  
<https://tutorialsdojo.com/amazon-vpc/>

## QUESTION 32

A Solutions Architect is hosting a website in an Amazon S3 bucket named tutorialsdojo. The users load the website using the following URL: <http://tutorialsdojo.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 ([tutorialsdojo.s3.amazonaws.com](http://tutorialsdojo.s3.amazonaws.com)). Upon testing, you noticed that the web browser blocks JavaScript from allowing those requests.

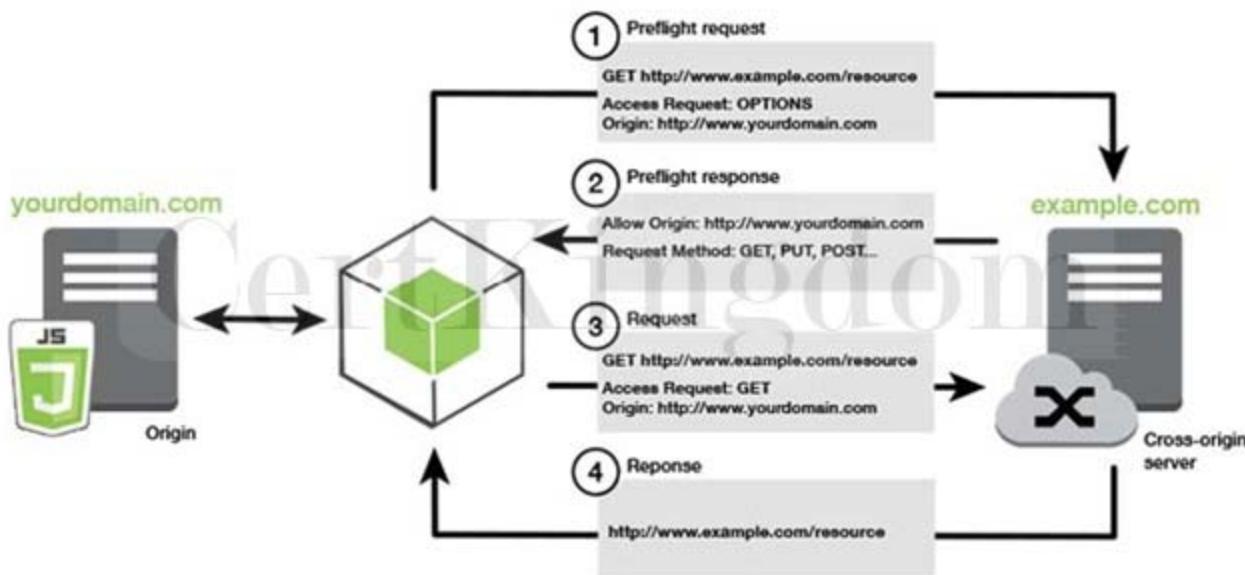
Which of the following options is the MOST suitable solution that you should implement for this scenario?

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

Answer: D

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 clientside 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, `yourwebsite.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 `yourwebsite.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 Crossorigin 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 33

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?

- A. Configure your CloudFront distribution to use Field-Level Encryption to protect your private data and only allow access to members.
- 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.
- C. 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.
- D. Create a Signed URL with a custom policy which only allows the members to see the private files.

Answer: C

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>

Check out this Amazon CloudFront Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudfront/>

---

## QUESTION 34

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?

- 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.
- B. 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.
- C. 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.
- D. 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.

Answer: D

Explanation:

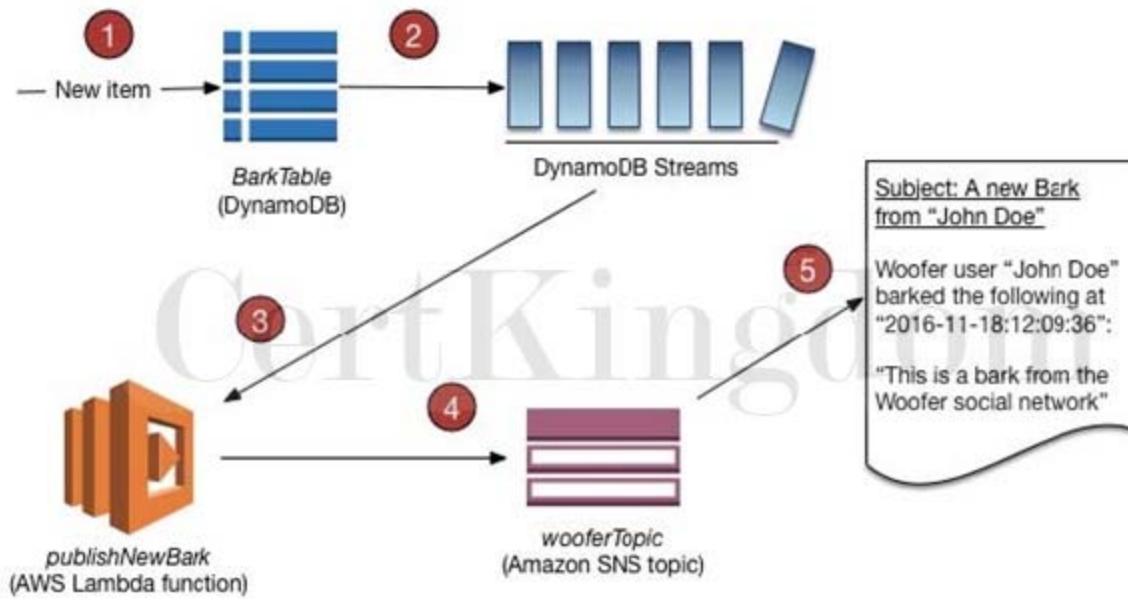
A DynamoDB stream is an ordered flow of information about changes to items in an Amazon DynamoDB table. When you enable a stream on a table, DynamoDB captures information about every modification to data items in the table.

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. 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 inmemory 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>

Check out this Amazon DynamoDB Cheat Sheet:

<https://tutorialsdojo.com/amazon-dynamodb/>

---

### QUESTION 35

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?

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

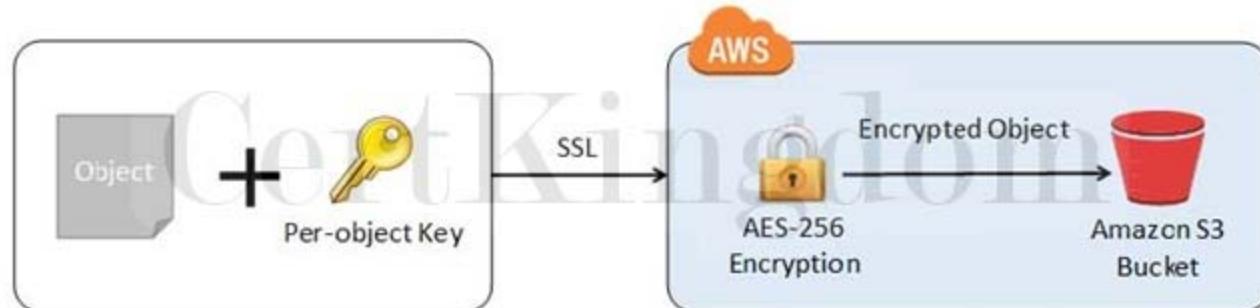
Answer: B

## 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 36

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.

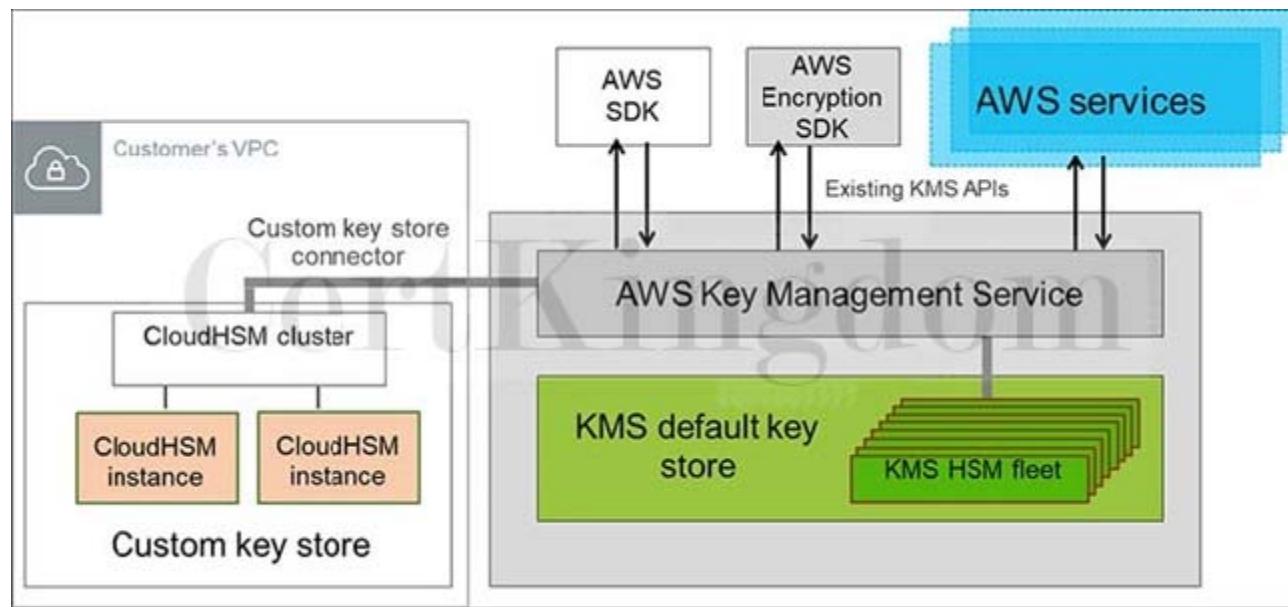
Which of the following options will meet this requirement?

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

Answer: B

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 has 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/>

Check out this AWS KMS Cheat Sheet:

<https://tutorialsdojo.com/aws-key-management-service-aws-kms/>

---

## QUESTION 37

A Solutions Architect identified a series of DDoS attacks while monitoring the VPC. The Architect needs to fortify the current cloud infrastructure to protect the data of the clients.

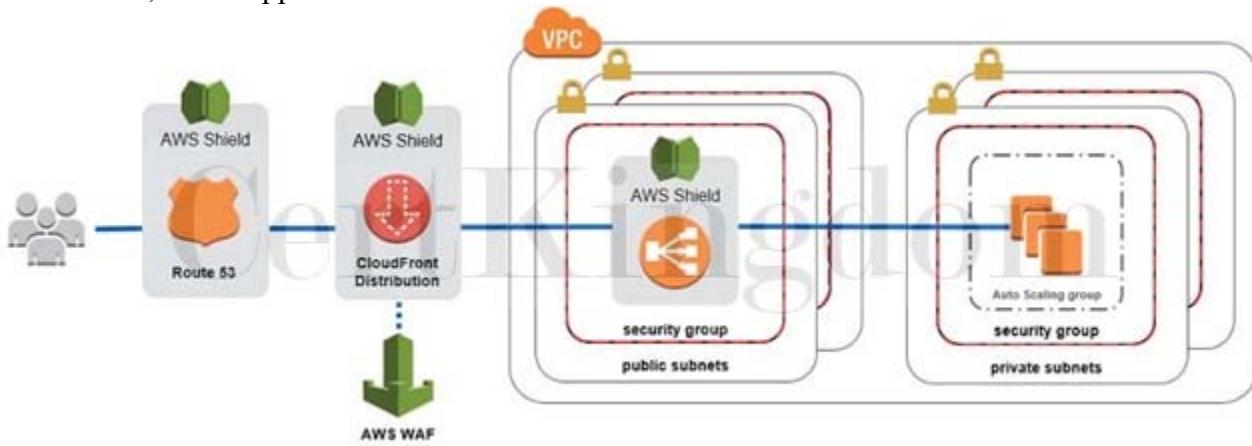
Which of the following is the most suitable solution to mitigate these kinds of attacks?

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

Answer: D

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 Shield Advanced also gives you 24x7 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 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. 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. 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://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf)

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

Check out this AWS Shield Cheat Sheet:

<https://tutorialsdojo.com/aws-shield/>

AWS Security Services Overview - WAF, Shield, CloudHSM, KMS:

<https://youtu.be/-1S-RdeAmMo>

## QUESTION 38

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?

- A. Configure SSL in your application to encrypt the database connection to RDS.
- B. Create an IAM Role and assign it to your EC2 instances which will grant exclusive access to your RDS instance.
- C. Use a combination of IAM and STS to restrict access to your RDS instance via a temporary token.
- D. Enable the IAM DB Authentication.

Answer: D

## 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](#)  
tutorialsdojo  
If you do not provide one, a default identifier based on the instance identifier will be used.

**Database name** [Info](#)  
tutorialsdojo  
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>

Check out this Amazon RDS cheat sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

---

### QUESTION 39

A software development company is using serverless computing with AWS Lambda to build and run applications without having to set up or manage servers. They 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 their application. One of the developers was instructed 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 this information be secured to prevent other developers in the team, or anyone, from seeing these credentials in plain text? Select the best option that provides maximum security.

- A. There is no need to do anything because, by default, AWS Lambda already encrypts the environment variables using the AWS Key Management Service.
- B. 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.
- C. AWS Lambda does not provide encryption for the environment variables. Deploy your code to an EC2 instance instead.
- D. Enable SSL encryption that leverages on AWS CloudHSM to store and encrypt the sensitive information.

Answer: B

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.

## Environment variables

You can define environment variables as key-value pairs that are accessible from your function code. These are useful to store configuration settings without the need to change function code. [Learn more](#)

password	AQjCAHgdCwJ7eNzGOcBk9Q6nDD21wrmtICsvWz2AsE75No	Encrypt	Code	Remove
Key	Value	Encrypt	Code	Remove

▼ Encryption configuration

Enable helpers for encryption in transit [Info](#)

AWS KMS key to encrypt in transit  [rkey/2defc6c2-ab8a-499f-87de-](#) [X](#)

**⚠️ AWS KMS call failed for reason: User: arn:aws:iam::84205 /user/koko is not authorized to perform: kms:Encrypt on resource: arn:aws:kms:us-east-1:84205 2defc6c2-ab8a-499f-87de-**

AWS KMS key to encrypt at rest [Info](#)  
Choose an AWS KMS key to encrypt the environment variables at rest, or simply let Lambda manage the encryption.

(default) aws/lambda  
 Use a customer master key

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. 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/env_variables.html#env_encrypt)

[https://docs.aws.amazon.com/lambda/latest/dg/tutorial-env\\_console.html](https://docs.aws.amazon.com/lambda/latest/dg/tutorial-env_console.html)

Check out this AWS Lambda Cheat Sheet:

<https://tutorialsdojo.com/aws-lambda/>

AWS Lambda Overview - Serverless Computing in AWS:

<https://youtu.be/bPVX1zHwAnY>

## QUESTION 40

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.

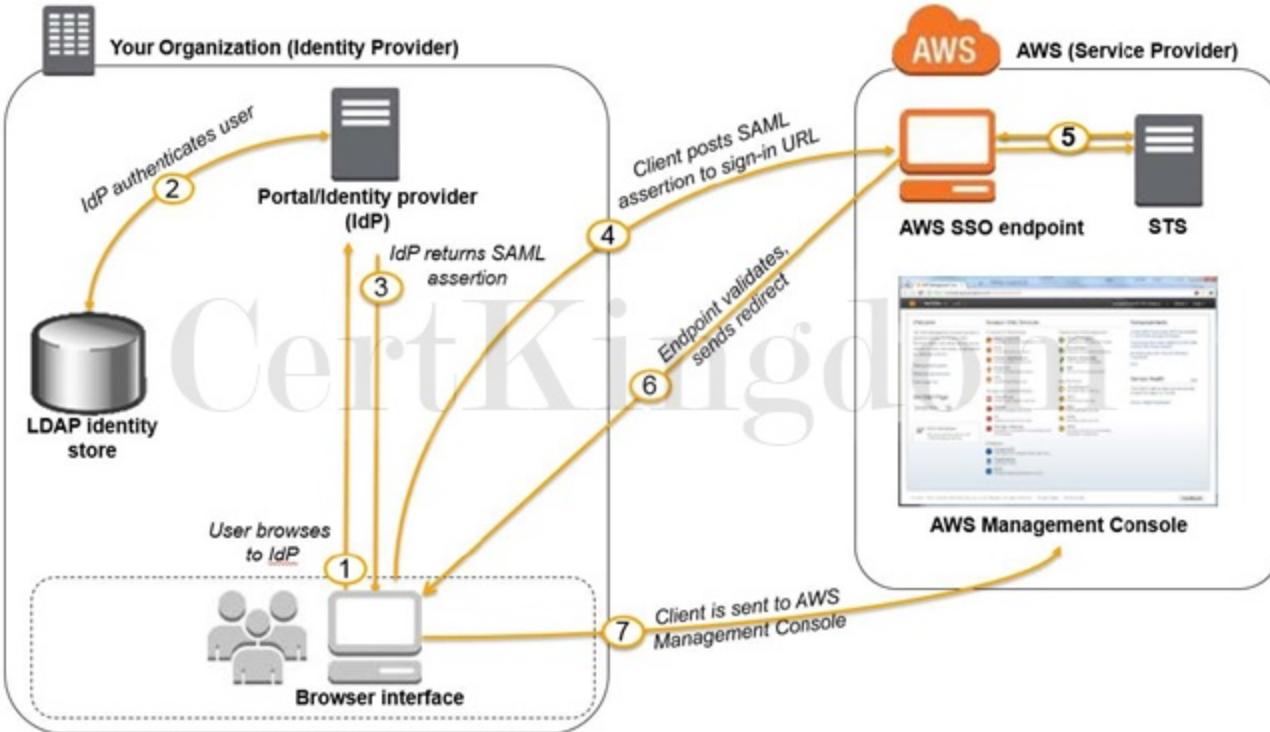
In this scenario, which of the following can be used to fulfill this requirement?

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

Answer: C

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

Check out this AWS IAM Cheat Sheet:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

## QUESTION 41

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?

- Use Amazon FSx For Windows File Server and Amazon S3 for hot and cold storage respectively.
- Use Amazon FSx For Lustre and Amazon S3 for hot and cold storage respectively.

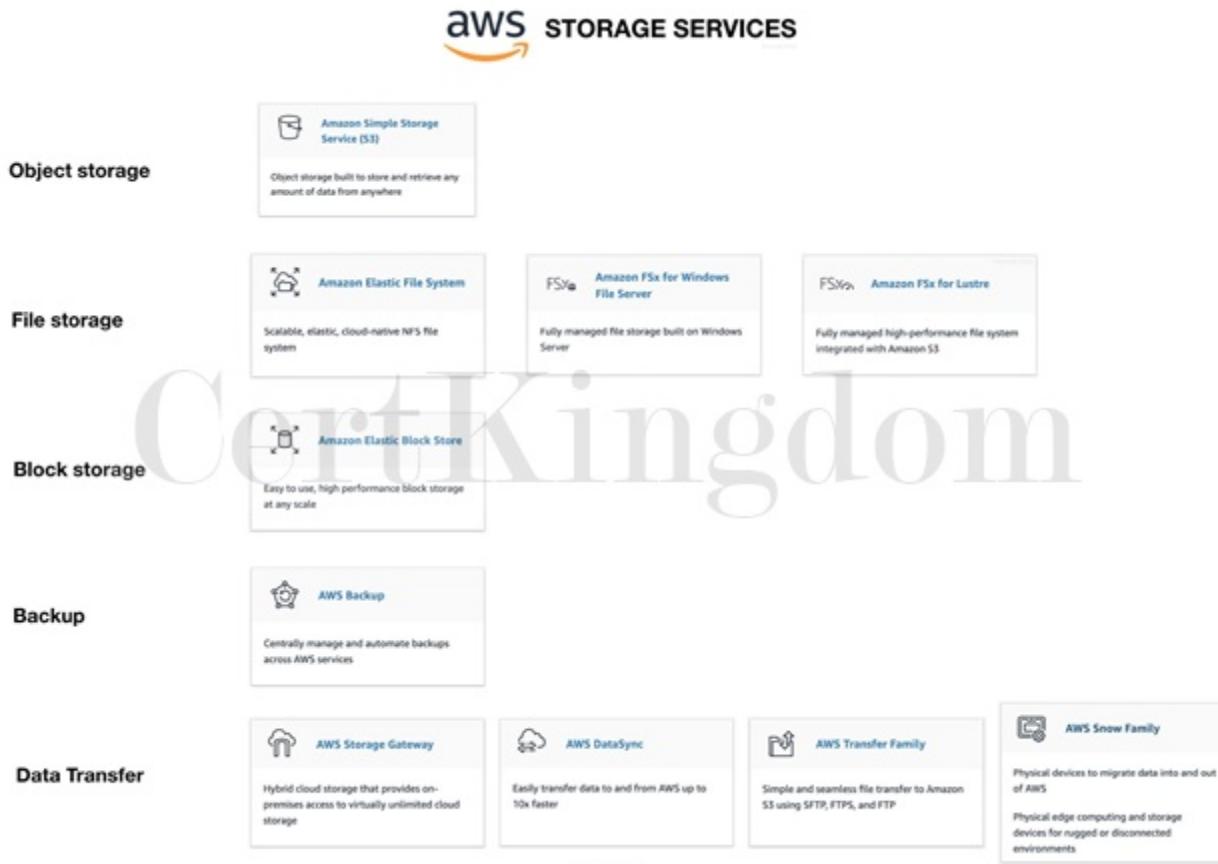
C. Use Amazon FSx For Lustre and Amazon EBS Provisioned IOPS SSD (io1) volumes for hot and cold storage respectively.

D. Use Amazon Elastic File System and Amazon S3 for hot and cold storage respectively.

Answer: B

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 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 for storing hot data (data that are frequently accessed) used in I/O-intensive workloads. EBS has a storage option called "Cold HDD," but due to its price, it is not ideal for data archiving. EBS Cold HDD is much more expensive than Amazon S3 Glacier / Glacier Deep Archive and is often utilized in applications where sequential cold data is read less frequently.

Using Amazon Elastic File System and Amazon S3 for hot and cold storage respectively is incorrect. 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/>

Check out this Amazon FSx Cheat Sheet:

<https://tutorialsdojo.com/amazon-fsx/>

---

## QUESTION 42

A Solutions Architect needs to make sure that the 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?

- A. Security Group Inbound Rule: Protocol “ UDP, Port Range “ 22, Source 110.238.98.71
- B. Security Group Inbound Rule: Protocol “ UDP, Port Range “ 22, Source 110.238.98.71/0
- C. Security Group Inbound Rule: Protocol “ TCP, Port Range “ 22, Source 110.238.98.71
- D. Security Group Inbound Rule: Protocol “ TCP, Port Range “ 22, Source 110.238.98.71/0

Answer: C

Explanation:

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC can be assigned to a different set of security groups.

The screenshot shows the 'Inbound rules' section of a CloudFormation stack. There are three rules listed:

- HTTP:** Protocol: TCP, Port range: 80, Source: 0.0.0.0/0
- HTTPS:** Protocol: TCP, Port range: 443, Source: Anywhere
- SSH:** Protocol: TCP, Port range: 22, Source: 110.238.98.71/32

The 'SSH' rule is highlighted with a green border, indicating it is the correct answer.

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 denotes one IP address and the /0 refers to the entire network. Take note that the SSH protocol uses TCP and port 22.

Hence, the correct answer is: Protocol “ TCP, Port Range “ 22, Source 110.238.98.71

Protocol “ UDP, Port Range “ 22, Source 110.238.98.71 and Protocol “ UDP, Port Range “ 22, Source 110.238.98.71/0 are incorrect as they are using UDP.

Protocol ““ TCP, Port Range ““ 22, Source 110.238.98.71/0 is incorrect because it uses a /0 CIDR notation.

Protocol ““ TCP, Port Range ““ 22, Source 110.238.98.71/0 is incorrect because it allows the entire network instead of a single IP.

Reference:

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

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

---

### QUESTION 43

A government agency plans to store confidential tax documents on AWS. Due to the sensitive information in the files, the Solutions Architect must restrict the data access requests made to the storage solution to a specific Amazon VPC only. The solution should also prevent the files from being deleted or overwritten to meet the regulatory requirement of having a write-once-read-many (WORM) storage model.

Which combination of the following options should the Architect implement? (Select TWO.)

- A. Create a new Amazon S3 bucket with the S3 Object Lock feature enabled. Store the documents in the bucket and set the Legal Hold option for object retention.
- B. Configure an Amazon S3 Access Point for the S3 bucket to restrict data access to a particular Amazon VPC only.
- C. Set up a new Amazon S3 bucket to store the tax documents and integrate it with AWS Network Firewall. Configure the Network Firewall to only accept data access requests from a specific Amazon VPC.
- D. Store the tax documents in the Amazon S3 Glacier Instant Retrieval storage class to restrict fast data retrieval to a particular Amazon VPC of your choice.
- E. Enable Object Lock but disable Object Versioning on the new Amazon S3 bucket to comply with the write-once-read-many (WORM) storage model requirement.

Answer: A,B

Explanation:

Amazon S3 access points simplify data access for any AWS service or customer application that stores data in S3. Access points are named network endpoints that are attached to buckets that you can use to perform S3 object operations, such as GetObject and PutObject.

Each access point has distinct permissions and network controls that S3 applies for any request that is made through that access point. Each access point enforces a customized access point policy that works in conjunction with the bucket policy that is attached to the underlying bucket. You can configure any access point to accept requests only from a virtual private cloud (VPC) to restrict Amazon S3 data access to a private network. You can also configure custom block public access settings for each access point.

The screenshot shows the AWS S3 Access Points Properties page. The 'Bucket name' field is highlighted with a yellow box. The 'Network origin' section, which includes options for 'Virtual private cloud (VPC)', 'No internet access', and 'Internet', is also highlighted with a green box. A blue callout bubble points to the 'VPC ID' field, which contains 'vpc-0612abacada1898'. The 'Block Public Access settings for this Access Point' section is partially visible at the bottom.

You can also use Amazon S3 Multi-Region Access Points to provide a global endpoint that applications can use to fulfill requests from S3 buckets located in multiple AWS Regions. You can use Multi-Region Access Points to build multi-Region applications with the same simple architecture used in a single Region, and then run those applications anywhere in the world. Instead of sending requests over the congested public internet, Multi-Region Access Points provide built-in network resilience with acceleration of internet-based requests to Amazon S3. Application requests made to a Multi-Region Access Point global endpoint use AWS Global Accelerator to automatically route over the AWS global network to the S3 bucket with the lowest network latency.

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

Before you lock any objects, you have to enable a bucket to use S3 Object Lock. You enable Object Lock when you create a bucket. After you enable Object Lock on a bucket, you can lock objects in that bucket. When you create a bucket with Object Lock enabled, you can't disable Object Lock or suspend versioning for that bucket.

Hence, the correct answers are:

- Configure an Amazon S3 Access Point for the S3 bucket to restrict data access to a particular Amazon VPC only.
- Create a new Amazon S3 bucket with the S3 Object Lock feature enabled. Store the documents in the bucket and set the Legal Hold option for object retention.

The option that says: Set up a new Amazon S3 bucket to store the tax documents and integrate it with AWS Network Firewall. Configure the Network Firewall to only accept data access requests from a specific Amazon VPC is incorrect because you cannot directly use an AWS Network Firewall to restrict S3 bucket data access requests to a specific Amazon VPC only. You have to use an Amazon S3 Access Point instead for this particular use case. An AWS Network Firewall is commonly integrated to your Amazon VPC and not to an S3 bucket.

The option that says: Store the tax documents in the Amazon S3 Glacier Instant Retrieval storage class to restrict fast data retrieval to a particular Amazon VPC of your choice is incorrect because Amazon S3 Glacier Instant Retrieval is just an archive storage class that delivers the lowest-cost storage for long-lived data that is rarely accessed and requires retrieval in milliseconds. It neither provides write-once-read-many (WORM) storage nor a fine-grained network control that restricts S3 bucket access to a specific Amazon VPC.

The option that says: Enable Object Lock but disable Object Versioning on the new Amazon S3 bucket to comply with the write-once-read-many (WORM) storage model requirement is incorrect. Although the Object Lock feature does provide write-once-read-many (WORM) storage, the Object Versioning feature must also be enabled too in order for this to work. In fact, you cannot manually disable the Object Versioning feature if you have already selected the Object Lock option.

#### References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-points.html>

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

---

## QUESTION 44

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 center. To achieve a highly available system, they plan to migrate the application and file share to AWS.

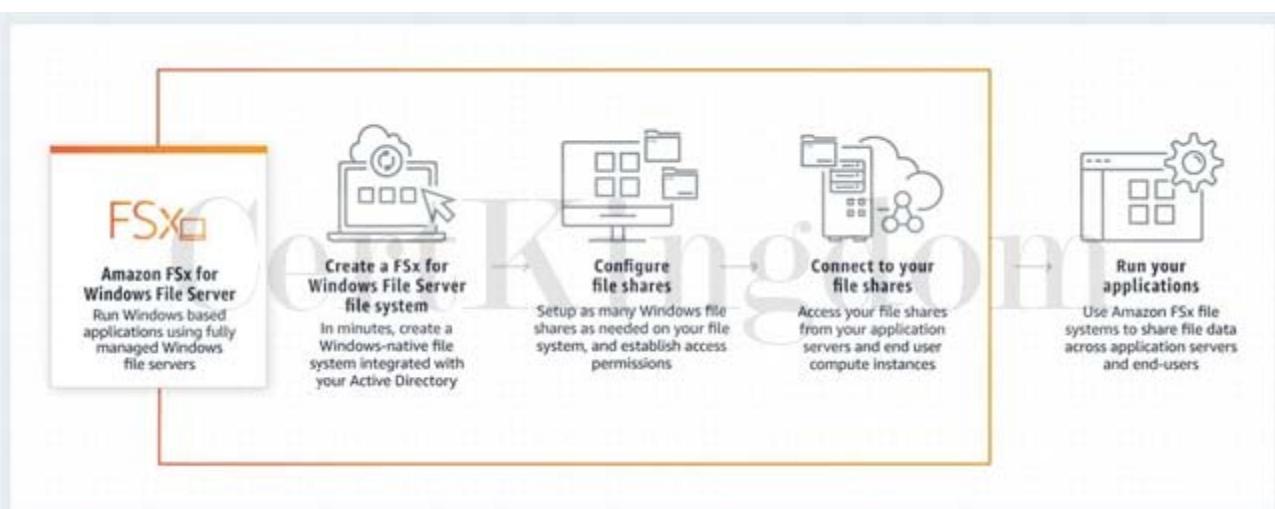
Which of the following can be used to fulfill this requirement?

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

Answer: A

#### 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>

Check out this Amazon FSx Cheat Sheet:

<https://tutorialsdojo.com/amazon-fsx/>

---

## QUESTION 45

A commercial bank has a forex trading application. They created an Auto Scaling group of EC2 instances that allow the bank to cope with the current traffic and achieve cost-efficiency. They want the Auto Scaling group to behave in such a way that it will follow a predefined set of parameters before it scales down the number of EC2 instances, which protects the system from unintended slowdown or unavailability.

Which of the following statements are true regarding the cooldown period? (Select TWO.)

- A. Its default value is 300 seconds.
- B. It ensures that the Auto Scaling group launches or terminates additional EC2 instances without any downtime.
- C. Its default value is 600 seconds.
- D. It ensures that before the Auto Scaling group scales out, the EC2 instances have ample time to cooldown.
- E. It ensures that the Auto Scaling group does not launch or terminate additional EC2 instances before the previous scaling activity takes effect.

Answer: A,E

Explanation:

In Auto Scaling, the following statements are correct regarding the cooldown period:

It ensures that the Auto Scaling group does not launch or terminate additional EC2 instances before the previous scaling activity takes effect.

Its default value is 300 seconds.

It is a configurable setting for your Auto Scaling group.

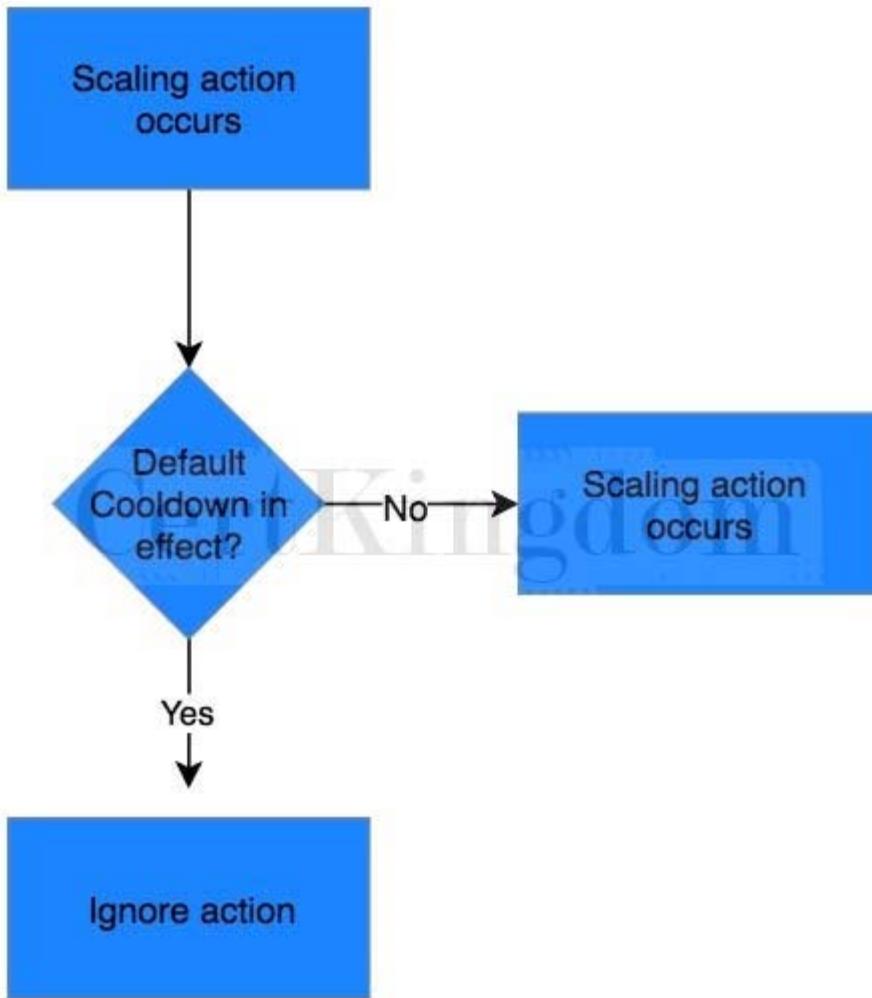
The following options are incorrect:

- It ensures that before the Auto Scaling group scales out, the EC2 instances have ample time to cooldown.
- It ensures that the Auto Scaling group launches or terminates additional EC2 instances without any downtime.
- Its default value is 600 seconds.

These statements are inaccurate and don't depict what the word "cooldown" actually means for Auto Scaling. The cooldown period is a configurable setting for your Auto Scaling group that helps to ensure that it doesn't launch or terminate additional instances before the previous scaling activity takes effect.

After the Auto Scaling group dynamically scales using a simple scaling policy, it waits for the cooldown period to complete before resuming scaling activities.

The figure below demonstrates the scaling cooldown:



Reference:

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

Check out this AWS Auto Scaling Cheat Sheet:

<https://tutorialsdojo.com/aws-auto-scaling/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

#### QUESTION 46

A Solutions Architect is building a cloud infrastructure where EC2 instances require access to various AWS services such as S3 and Redshift. The Architect will also need to provide access to system administrators so they can deploy and test their changes.

Which configuration should be used to ensure that the access to the resources is secured and not compromised? (Select TWO.)

- A. Store the AWS Access Keys in the EC2 instance.
- B. Assign an IAM role to the Amazon EC2 instance.
- C. Store the AWS Access Keys in ACM.
- D. Enable Multi-Factor Authentication.
- E. Assign an IAM user for each Amazon EC2 Instance.

Answer: B,D

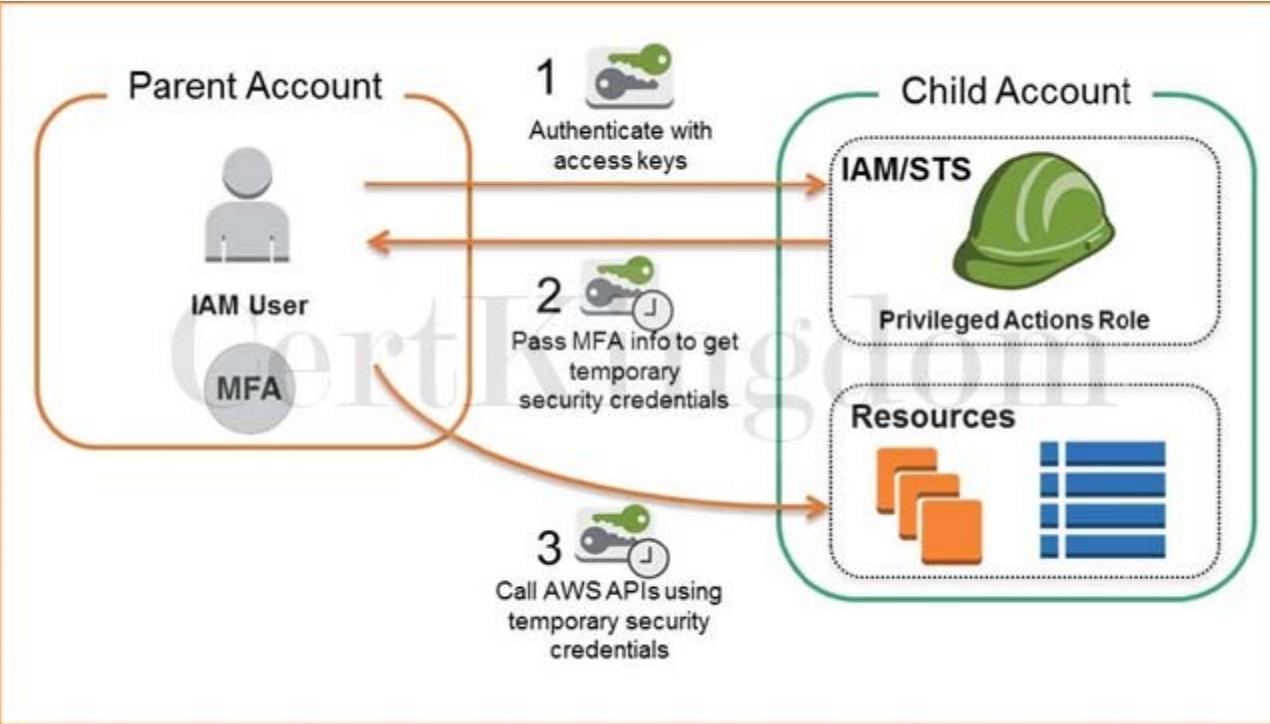
Explanation:

In this scenario, the correct answers are:

- Enable Multi-Factor Authentication

## - Assign an IAM role to the Amazon EC2 instance

Always remember that you should associate IAM roles to EC2 instances and not an IAM user, for the purpose of accessing other AWS services. IAM roles are designed so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use. Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles.



AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password. With MFA enabled, when a user signs in to an AWS website, they will be prompted for their user name and password (the first factor "what they know"), as well as for an authentication code from their AWS MFA device (the second factor "what they have"). Taken together, these multiple factors provide increased security for your AWS account settings and resources. You can enable MFA for your AWS account and for individual IAM users you have created under your account. MFA can also be used to control access to AWS service APIs.

Storing the AWS Access Keys in the EC2 instance is incorrect. This is not recommended by AWS as it can be compromised. Instead of storing access keys on an EC2 instance for use by applications that run on the instance and make AWS API requests, you can use an IAM role to provide temporary access keys for these applications.

Assigning an IAM user for each Amazon EC2 Instance is incorrect because there is no need to create an IAM user for this scenario since IAM roles already provide greater flexibility and easier management. Storing the AWS Access Keys in ACM is incorrect because ACM is just a service that lets you easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources. It is not used as a secure storage for your access keys.

References:

<https://aws.amazon.com/iam/details/mfa/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

Check out this AWS IAM Cheat Sheet:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

## QUESTION 47

A solutions architect is instructed to host a website that consists of HTML, CSS, and some Javascript files. The web pages will display several high-resolution images. The website should have optimal loading times and be able to respond to high request rates.

Which of the following architectures can provide the most cost-effective and fastest loading experience?

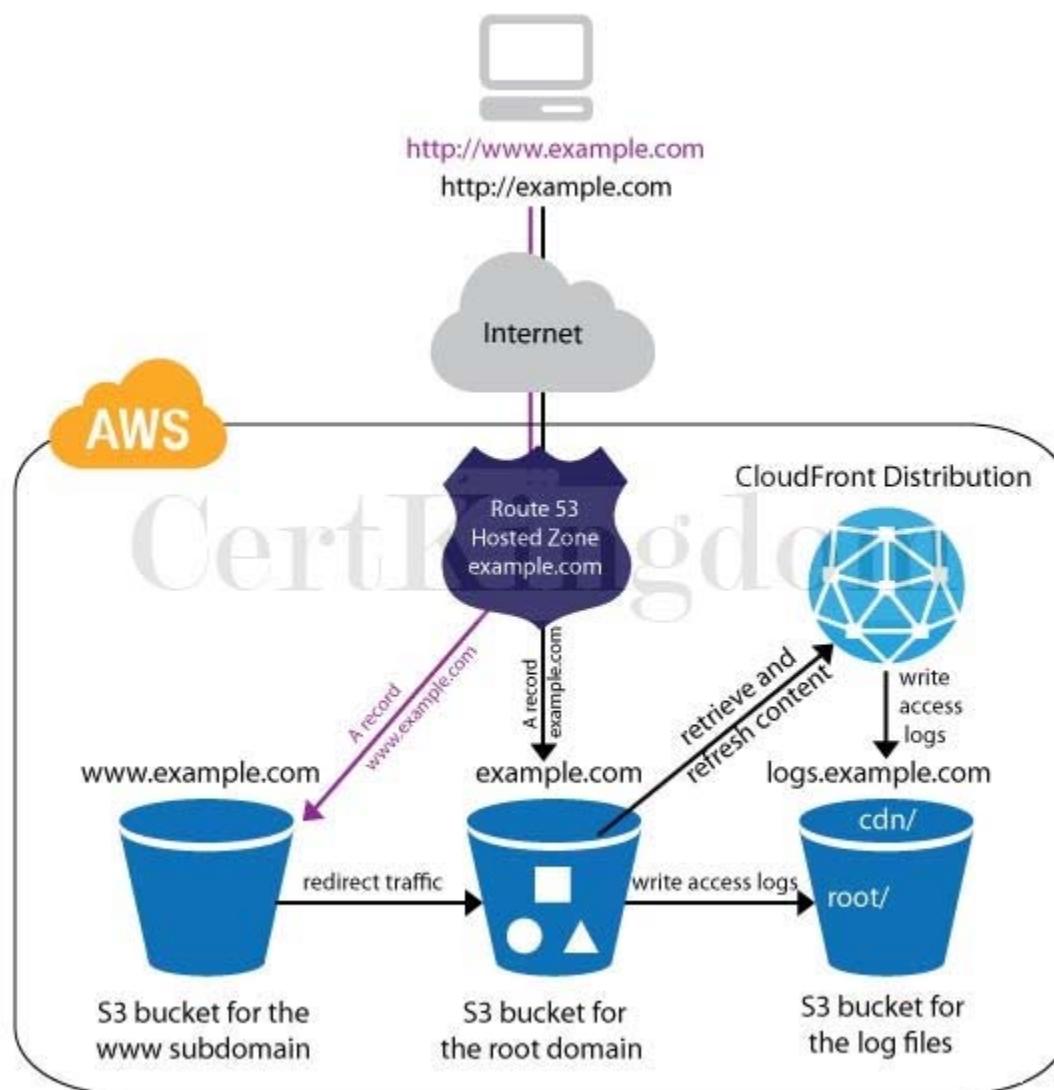
- A. Host the website using an Nginx server in an EC2 instance. Upload the images in an S3 bucket. Use CloudFront as a CDN to deliver the images closer to end-users.
- B. Host the website in an AWS Elastic Beanstalk environment. Upload the images in an S3 bucket. Use CloudFront as a CDN to deliver the images closer to your end-users.
- C. Upload the HTML, CSS, Javascript, and the images in a single bucket. Then enable website hosting. Create a CloudFront distribution and point the domain on the S3 website endpoint.
- D. Launch an Auto Scaling Group using an AMI that has a pre-configured Apache web server, then configure the scaling policy accordingly. Store the images in an Elastic Block Store. Then, point your instance's endpoint to AWS Global Accelerator.

Answer: C

Explanation:

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance. Additionally, You can use Amazon S3 to host a static website. On a static website, individual webpages include static content. Amazon S3 is highly scalable and you only pay for what you use, you can start small and grow your application as you wish, with no compromise on performance or reliability.

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds. CloudFront can be integrated with Amazon S3 for fast delivery of data originating from an S3 bucket to your end-users. By design, delivering data out of CloudFront can be more cost-effective than delivering it from S3 directly to your users.



In the scenario, Since we are only dealing with static content, we can leverage the web hosting feature of

S3. Then we can improve the architecture further by integrating it with CloudFront. This way, users will be able to load both the web pages and images faster than if we hosted them on a webserver that we built from scratch.

Hence, the correct answer is: Upload the HTML, CSS, Javascript, and the images in a single bucket. Then enable website hosting. Create a CloudFront distribution and point the domain on the S3 website endpoint.

The option that says: Host the website using an Nginx server in an EC2 instance. Upload the images in an S3 bucket. Use CloudFront as a CDN to deliver the images closer to end-users is incorrect. Creating your own web server to host a static website in AWS is a costly solution. Web Servers on an EC2 instance are usually used for hosting applications that require server-side processing (connecting to a database, data validation, etc.). Since static websites contain web pages with fixed content, we should use S3 website hosting instead.

The option that says: Launch an Auto Scaling Group using an AMI that has a pre-configured Apache web server, then configure the scaling policy accordingly. Store the images in an Elastic Block Store. Then, point your instance's endpoint to AWS Global Accelerator is incorrect. This is how we serve static websites in the old days. Now, with the help of S3 website hosting, we can host our static contents from a durable, high-availability, and highly scalable environment without managing any servers. Hosting static websites in S3 is cheaper than hosting it in an EC2 instance. In addition, Using ASG for scaling instances that host a static website is an over-engineered solution that carries unnecessary costs. S3 automatically scales to high requests and you only pay for what you use.

The option that says: Host the website in an AWS Elastic Beanstalk environment. Upload the images in an S3 bucket. Use CloudFront as a CDN to deliver the images closer to your end-users is incorrect. AWS Elastic Beanstalk simply sets up the infrastructure (EC2 instance, load balancer, auto-scaling group) for your application. It's a more expensive and a bit of an overkill solution for hosting a bunch of client-side files.

References:

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

<https://aws.amazon.com/blogs/networking-and-content-delivery/amazon-s3-amazon-cloudfront-a-matchmade-in-the-cloud/>

Check out these Amazon S3 and CloudFront Cheat Sheets:

<https://tutorialsdojo.com/amazon-s3/>

<https://tutorialsdojo.com/amazon-cloudfront/>

---

## QUESTION 48

A company recently adopted a hybrid architecture that integrates its on-premises data center to AWS cloud. You are assigned to configure the VPC and implement the required IAM users, IAM roles, IAM groups, and IAM policies.

In this scenario, what is the best practice when creating IAM policies?

- A. Grant all permissions to any EC2 user.
- B. Determine what users need to do and then craft policies for them that let the users perform those tasks including additional administrative operations.
- C. Use the principle of least privilege which means granting only the least number of people with full root access.
- D. Use the principle of least privilege which means granting only the permissions required to perform a task.

Answer: D

Explanation:

One of the best practices in AWS IAM is to grant least privilege.

When you create IAM policies, follow the standard security advice of granting least privilege”that is, granting only the permissions required to perform a task. Determine what users need to do and then craft policies for them that let the users perform only those tasks.

Therefore, using the principle of least privilege which means granting only the permissions required to

perform a task is the correct answer.

Start with a minimum set of permissions and grant additional permissions as necessary. Defining the right set of permissions requires some understanding of the user's objectives. Determine what is required for the specific task, what actions a particular service supports, and what permissions are required in order to perform those actions.

Granting all permissions to any EC2 user is incorrect since you don't want your users to gain access to everything and perform unnecessary actions. Doing so is not a good security practice.

Using the principle of least privilege which means granting only the least number of people with full root access is incorrect because this is not the correct definition of what the principle of least privilege is.

Determining what users need to do and then craft policies for them that let the users perform those tasks including additional administrative operations is incorrect since there are some users who you should not give administrative access to. You should follow the principle of least privilege when providing permissions and accesses to your resources.

Reference:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#use-groups-for-permissions>

Check out this AWS IAM Cheat Sheet:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

Service Control Policies (SCP) vs IAM Policies:

<https://tutorialsdojo.com/service-control-policies-scp-vs-iam-policies/>

Comparison of AWS Services Cheat Sheets:

<https://tutorialsdojo.com/comparison-of-aws-services/>

---

## QUESTION 49

A software company has resources hosted in AWS and on-premises servers. You have been requested to create a decoupled architecture for applications which make use of both resources.

Which of the following options are valid? (Select TWO.)

- A. Use DynamoDB to utilize both on-premises servers and EC2 instances for your decoupled application
- B. Use SQS to utilize both on-premises servers and EC2 instances for your decoupled application
- C. Use SWF to utilize both on-premises servers and EC2 instances for your decoupled application
- D. Use RDS to utilize both on-premises servers and EC2 instances for your decoupled application
- E. Use VPC peering to connect both on-premises servers and EC2 instances for your decoupled application

Answer: B,C

Explanation:

Amazon Simple Queue Service (SQS) and Amazon Simple Workflow Service (SWF) are the services that you can use for creating a decoupled architecture in AWS. Decoupled architecture is a type of computing architecture that enables computing components or layers to execute independently while still interfacing with each other.

Amazon SQS offers reliable, highly-scalable hosted queues for storing messages while they travel between applications or microservices. Amazon SQS lets you move data between distributed application components and helps you decouple these components. Amazon SWF is a web service that makes it easy to coordinate work across distributed application components.

Using RDS to utilize both on-premises servers and EC2 instances for your decoupled application and using DynamoDB to utilize both on-premises servers and EC2 instances for your decoupled application are incorrect as RDS and DynamoDB are database services.

Using VPC peering to connect both on-premises servers and EC2 instances for your decoupled application is incorrect because you can't create a VPC peering for your on-premises network and AWS VPC.

References:

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

<http://docs.aws.amazon.com/amazonswf/latest/developerguide/swf-welcome.html>

Check out this Amazon SQS Cheat Sheet:

<https://tutorialsdojo.com/amazon-sqs/>

Amazon Simple Workflow (SWF) vs AWS Step Functions vs Amazon SQS:

<https://tutorialsdojo.com/amazon-simple-workflow-swf-vs-aws-step-functions-vs-amazon-sqs/>

Comparison of AWS Services Cheat Sheets:

<https://tutorialsdojo.com/comparison-of-aws-services/>

## QUESTION 50

A company has a dynamic web app written in MEAN stack that is going to be launched in the next month. There is a probability that the traffic will be quite high in the first couple of weeks. In the event of a load failure, how can you set up DNS failover to a static website?

- A. Use Route 53 with the failover option to a static S3 website bucket or CloudFront distribution.
- B. Add more servers in case the application fails.
- C. Duplicate the exact application architecture in another region and configure DNS weight-based routing.
- D. Enable failover to an application hosted in an on-premises data center.

Answer: A

Explanation:

For this scenario, using Route 53 with the failover option to a static S3 website bucket or CloudFront distribution is correct. You can create a new Route 53 with the failover option to a static S3 website bucket or CloudFront distribution as an alternative.

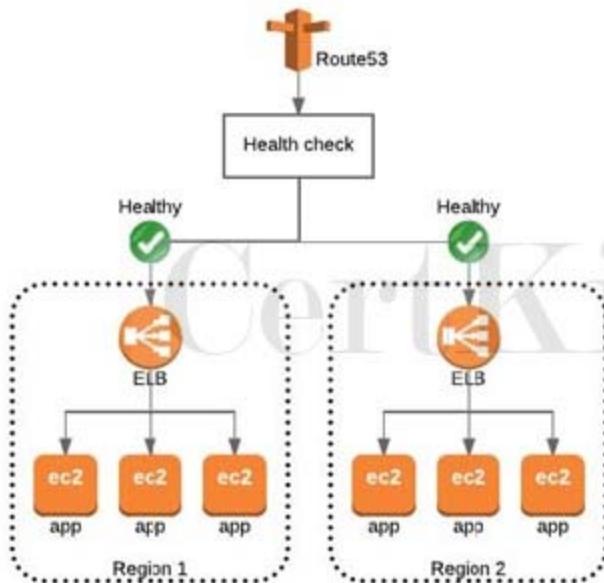


Figure 1 - Both regions operating normally

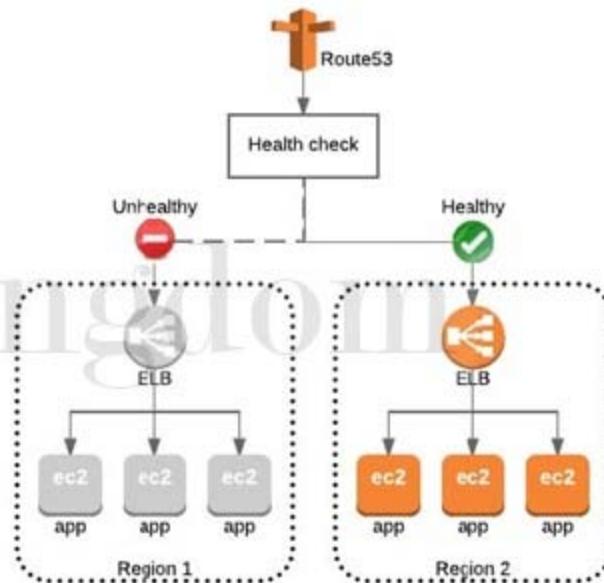


Figure 2 - region 1 experiencing issues

Duplicating the exact application architecture in another region and configuring DNS weight-based routing is incorrect because running a duplicate system is not a cost-effective solution. Remember that you are trying to build a failover mechanism for your web app, not a distributed setup.

Enabling failover to an application hosted in an on-premises data center is incorrect. Although you can set up failover to your on-premises data center, you are not maximizing the AWS environment such as using Route 53 failover.

Adding more servers in case the application fails is incorrect because this is not the best way to handle a failover event. If you add more servers only in case the application fails, then there would be a period of downtime in which your application is unavailable. Since there are no running servers on that period, your application will be unavailable for a certain period of time until your new server is up and running.

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/fail-over-s3-r53/>

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

Check out this Amazon Route 53 Cheat Sheet:

<https://tutorialsdojo.com/amazon-route-53/>

## QUESTION 51

One of your EC2 instances is reporting an unhealthy system status check. The operations team is looking for an easier way to monitor and repair these instances instead of fixing them manually. How will you automate the monitoring and repair of the system status check failure in an AWS environment?

- A. Write a python script that queries the EC2 API for each instance status check
- B. Create CloudWatch alarms that stop and start the instance based on status check alarms.
- C. Write a shell script that periodically shuts down and starts instances based on certain stats.
- D. Buy and implement a third party monitoring tool.

Answer: B

Explanation:

Using Amazon CloudWatch alarm actions, you can create alarms that automatically stop, terminate, reboot, or recover your EC2 instances. You can use the stop or terminate actions to help you save money when you no longer need an instance to be running. You can use the reboot and recover actions to automatically reboot those instances or recover them onto new hardware if a system impairment occurs.

Writing a python script that queries the EC2 API for each instance status check, writing a shell script that periodically shuts down and starts instances based on certain stats, and buying and implementing a third party monitoring tool are all incorrect because it is unnecessary to go through such lengths when CloudWatch Alarms already has such a feature for you, offered at a low cost.

Reference:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html>

Check out this Amazon CloudWatch Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudwatch/>

---

## QUESTION 52

A company launched a website that accepts high-quality photos and turns them into a downloadable video montage. The website offers a free and a premium account that guarantees faster processing. All requests by both free and premium members go through a single SQS queue and then processed by a group of EC2 instances that generate the videos. The company needs to ensure that the premium users who paid for the service have higher priority than the free members.

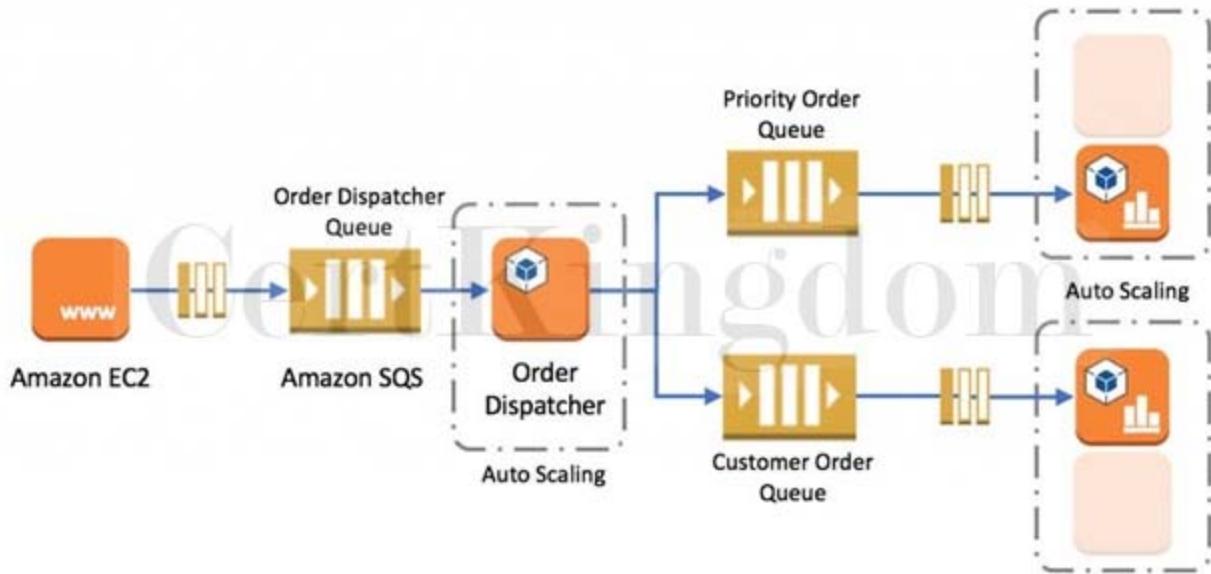
How should the company re-design its architecture to address this requirement?

- A. For the requests made by premium members, set a higher priority in the SQS queue so it will be processed first compared to the requests made by free members.
- B. Use Amazon Kinesis to process the photos and generate the video montage in real-time.
- C. Create an SQS queue for free members and another one for premium members. Configure your EC2 instances to consume messages from the premium queue first and if it is empty, poll from the free members' SQS queue.
- D. Use Amazon S3 to store and process the photos and then generate the video montage afterward.

Answer: C

Explanation:

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message-oriented middleware and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume without losing messages or requiring other services to be available.



In this scenario, it is best to create 2 separate SQS queues for each type of member. The SQS queues for the premium members can be polled first by the EC2 Instances and once completed, the messages from the free members can be processed next.

Hence, the correct answer is: Create an SQS queue for free members and another one for premium members. Configure your EC2 instances to consume messages from the premium queue first and if it is empty, poll from the free members' SQS queue.

The option that says: For the requests made by premium members, set a higher priority in the SQS queue so it will be processed first compared to the requests made by free members is incorrect as you cannot set a priority to individual items in the SQS queue.

The option that says: Using Amazon Kinesis to process the photos and generate the video montage in real time is incorrect as Amazon Kinesis is used to process streaming data and it is not applicable in this scenario.

The option that says: Using Amazon S3 to store and process the photos and then generating the video montage afterward is incorrect as Amazon S3 is used for durable storage and not for processing data.

Reference:

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

Check out this Amazon SQS Cheat Sheet:

<https://tutorialsdojo.com/amazon-sqs/>

## QUESTION 53

A company needs to assess and audit all the configurations in their AWS account. It must enforce strict compliance by tracking all configuration changes made to any of its Amazon S3 buckets. Publicly accessible S3 buckets should also be identified automatically to avoid data breaches.

Which of the following options will meet this requirement?

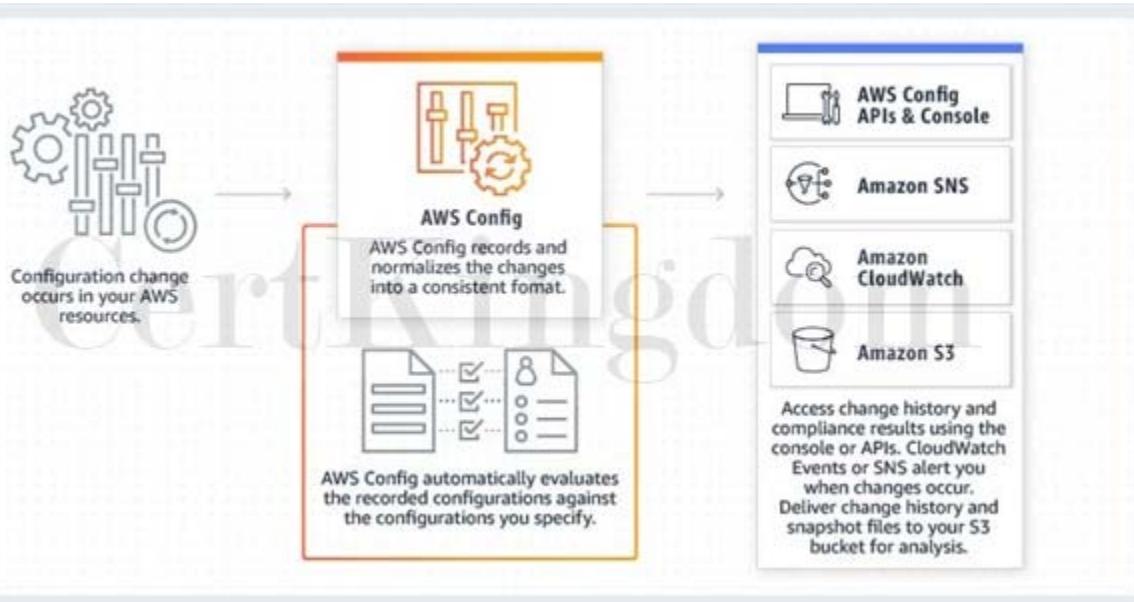
- A. Use AWS Trusted Advisor to analyze your AWS environment.
- B. Use AWS IAM to generate a credential report.
- C. Use AWS Config to set up a rule in your AWS account.
- D. Use AWS CloudTrail and review the event history of your AWS account.

Answer: C

Explanation:

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you

can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.



You can use AWS Config to evaluate the configuration settings of your AWS resources. By creating an AWS Config rule, you can enforce your ideal configuration in your AWS account. It also checks if the applied configuration in your resources violates any of the conditions in your rules. The AWS Config dashboard shows the compliance status of your rules and resources. You can verify if your resources comply with your desired configurations and learn which specific resources are noncompliant.

Hence, the correct answer is: Use AWS Config to set up a rule in your AWS account.

The option that says: Use AWS Trusted Advisor to analyze your AWS environment is incorrect because AWS Trusted Advisor only provides best practice recommendations. It cannot define rules for your AWS resources.

The option that says: Use AWS IAM to generate a credential report is incorrect because this report will not help you evaluate resources. The IAM credential report is just a list of all IAM users in your AWS account.

The option that says: Use AWS CloudTrail and review the event history of your AWS account is incorrect. Although it can track changes and store a history of what happened to your resources, this service still cannot enforce rules to comply with your organization's policies.

#### References:

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

<https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config.html>

Check out this AWS Config Cheat Sheet:

<https://tutorialsdojo.com/aws-config/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

## QUESTION 5

A Solutions Architect of a multinational gaming company develops video games for PS4, Xbox One, and Nintendo Switch consoles, plus a number of mobile games for Android and iOS. Due to the wide range of their products and services, the architect proposed that they use API Gateway.

What are the key features of API Gateway that the architect can tell to the client? (Select TWO.)

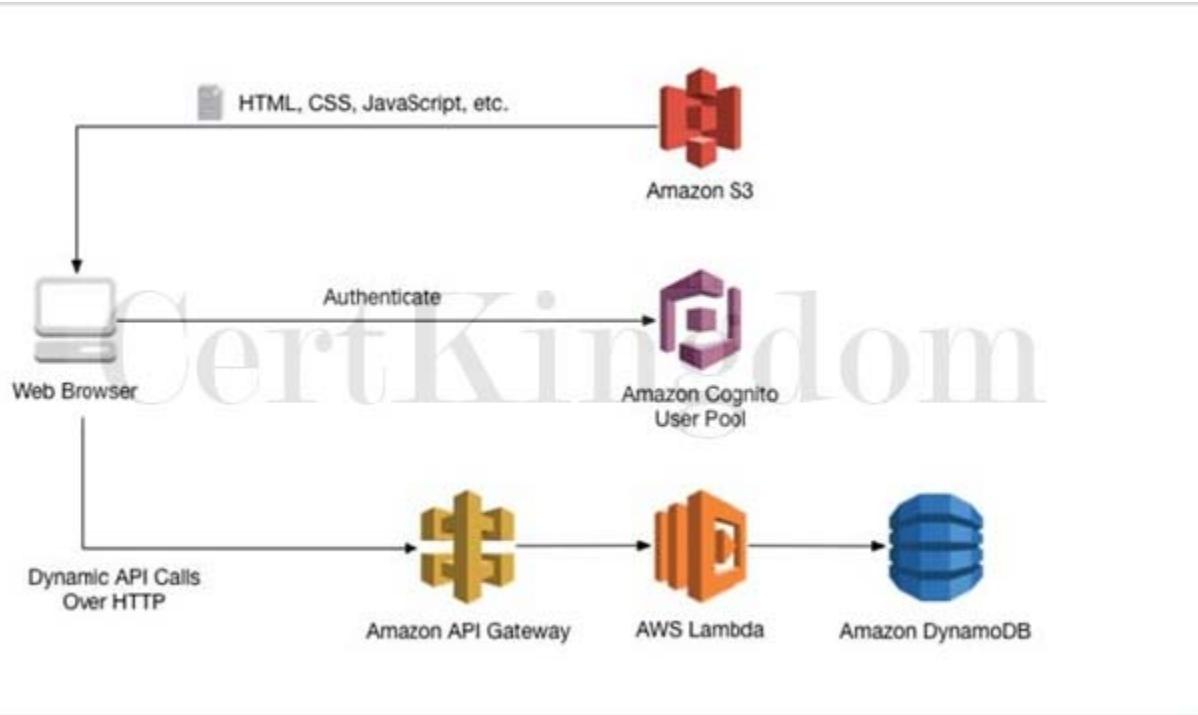
- A. It automatically provides a query language for your APIs similar to GraphQL.
- B. Enables you to build RESTful APIs and WebSocket APIs that are optimized for serverless workloads.
- C. Enables you to run applications requiring high levels of inter-node communications at scale on AWS through its custom-built operating system (OS) bypass hardware interface.

- D. You pay only for the API calls you receive and the amount of data transferred out.  
E. Provides you with static anycast IP addresses that serve as a fixed entry point to your applications hosted in one or more AWS Regions.

Answer: B,D

Explanation:

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. With a few clicks in the AWS Management Console, you can create an API that acts as a front door' for applications to access data, business logic, or functionality from your back-end services, such as workloads running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, or any web application. Since it can use AWS Lambda, you can run your APIs without servers.



Amazon API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management. Amazon API Gateway has no minimum fees or startup costs. You pay only for the API calls you receive and the amount of data transferred out.

Hence, the correct answers are:

- Enables you to build RESTful APIs and WebSocket APIs that are optimized for serverless workloads
- You pay only for the API calls you receive and the amount of data transferred out.

The option that says: It automatically provides a query language for your APIs similar to GraphQL is incorrect because this is not provided by API Gateway.

The option that says: Provides you with static anycast IP addresses that serve as a fixed entry point to your applications hosted in one or more AWS Regions is incorrect because this is a capability of AWS Global Accelerator and not API Gateway.

The option that says: Enables you to run applications requiring high levels of inter-node communications at scale on AWS through its custom-built operating system (OS) bypass hardware interface is incorrect because this is a capability of Elastic Fabric Adapter and not API Gateway.

References:

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

Check out this Amazon API Gateway Cheat Sheet:

<https://tutorialsdojo.com/amazon-api-gateway/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

## QUESTION 55

An organization stores and manages financial records of various companies in its on-premises data center, which is almost out of space. The management decided to move all of their existing records to a cloud storage service. All future financial records will also be stored in the cloud. For additional security, all records must be prevented from being deleted or overwritten.

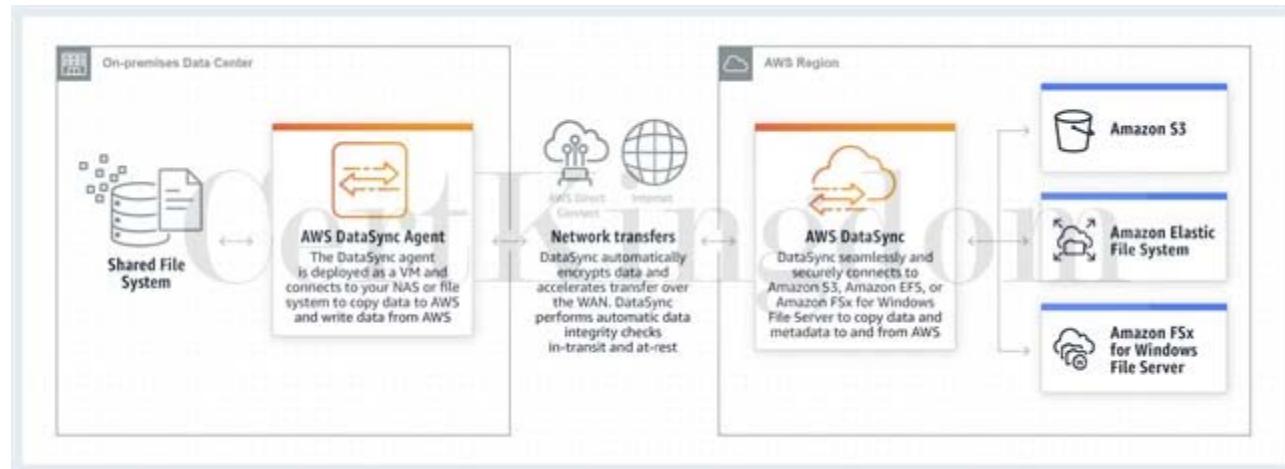
Which of the following should you do to meet the above requirement?

- A. Use AWS DataSync to move the data. Store all of your data in Amazon S3 and enable object lock.
- B. Use AWS Storage Gateway to establish hybrid cloud storage. Store all of your data in Amazon S3 and enable object lock.
- C. Use AWS Storage Gateway to establish hybrid cloud storage. Store all of your data in Amazon EBS and enable object lock.
- D. Use AWS DataSync to move the data. Store all of your data in Amazon EFS and enable object lock.

Answer: A

Explanation:

AWS DataSync allows you to copy large datasets with millions of files, without having to build custom solutions with open source tools, or license and manage expensive commercial network acceleration software. You can use DataSync to migrate active data to AWS, transfer data to the cloud for analysis and processing, archive data to free up on-premises storage capacity, or replicate data to AWS for business continuity.



AWS DataSync enables you to migrate your on-premises data to Amazon S3, Amazon EFS, and Amazon FSx for Windows File Server. You can configure DataSync to make an initial copy of your entire dataset, and schedule subsequent incremental transfers of changing data towards Amazon S3. Enabling S3 Object Lock prevents your existing and future records from being deleted or overwritten.

AWS DataSync is primarily used to migrate existing data to Amazon S3. On the other hand, AWS Storage Gateway is more suitable if you still want to retain access to the migrated data and for ongoing updates from your on-premises file-based applications.

Hence, the correct answer in this scenario is: Use AWS DataSync to move the data. Store all of your data in Amazon S3 and enable object lock.

The option that says: Use AWS DataSync to move the data. Store all of your data in Amazon EFS and enable object lock is incorrect because Amazon EFS only supports file locking. Object lock is a feature of Amazon S3 and not Amazon EFS.

The option that says: Use AWS Storage Gateway to establish hybrid cloud storage. Store all of your data in Amazon S3 and enable object lock is incorrect because the scenario requires that all of the existing records must be migrated to AWS. The future records will also be stored in AWS and not in the on-premises network. This means that setting up a hybrid cloud storage is not necessary since the on-premises storage will no longer be used.

The option that says: Use AWS Storage Gateway to establish hybrid cloud storage. Store all of your data in Amazon EBS and enable object lock is incorrect because Amazon EBS does not support object lock.

Amazon S3 is the only service capable of locking objects to prevent an object from being deleted or overwritten.

References:

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

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

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

Check out this AWS DataSync Cheat Sheet:

<https://tutorialsdojo.com/aws-datasync/>

AWS Storage Gateway vs DataSync:

<https://www.youtube.com/watch?v=tmfe1rO-AUs>

Amazon S3 vs EBS vs EFS Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3-vs-ebs-vs-efs/>

---

## QUESTION 56

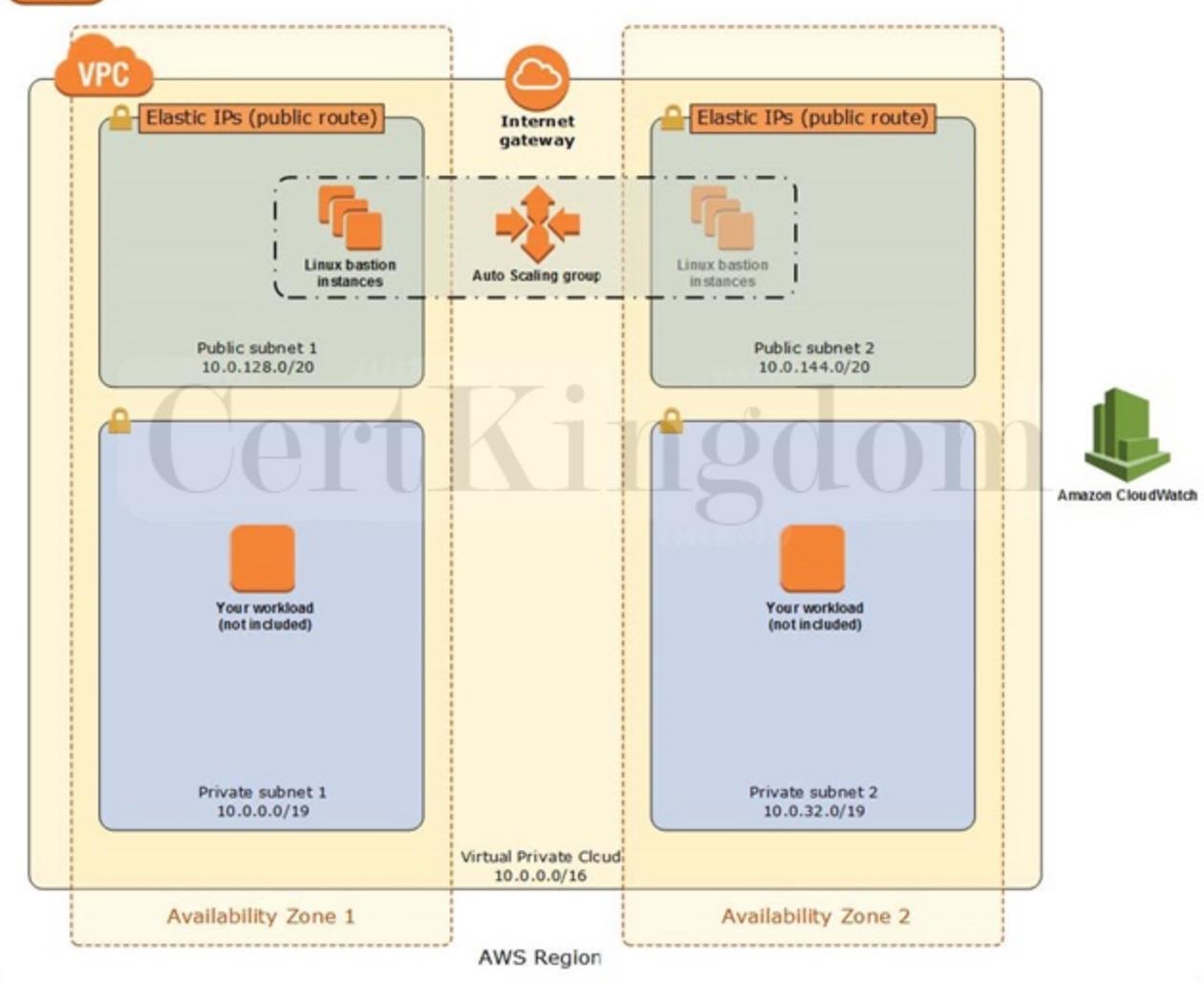
A Solutions Architect needs to set up a bastion host in Amazon VPC. It should only be accessed from the corporate data center via SSH. What is the best way to achieve this?

- A. Create a large EC2 instance with a security group which only allows access on port 22 via the IP address of the corporate data center. Use a private key (.pem) file to connect to the bastion host.
- B. Create a large EC2 instance with a security group which only allows access on port 22 using your own pre-configured password.
- C. Create a small EC2 instance with a security group which only allows access on port 22 using your own pre-configured password.
- D. Create a small EC2 instance with a security group which only allows access on port 22 via the IP address of the corporate data center. Use a private key (.pem) file to connect to the bastion host.

Answer: D

Explanation:

The best way to implement a bastion host is to create a small EC2 instance which should only have a security group from a particular IP address for maximum security. This will block any SSH Brute Force attacks on your bastion host. It is also recommended to use a small instance rather than a large one because this host will only act as a jump server to connect to other instances in your VPC and nothing else.



Therefore, there is no point of allocating a large instance simply because it doesn't need that much computing power to process SSH (port 22) or RDP (port 3389) connections. It is possible to use SSH with an ordinary user ID and a pre-configured password as credentials but it is more secure to use public key pairs for SSH authentication for better security.

Hence, the right answer for this scenario is the option that says: Create a small EC2 instance with a security group which only allows access on port 22 via the IP address of the corporate data center. Use a private key (.pem) file to connect to the bastion host.

Creating a large EC2 instance with a security group which only allows access on port 22 using your own pre-configured password and creating a small EC2 instance with a security group which only allows access on port 22 using your own pre-configured password are incorrect. Even though you have your own pre-configured password, the SSH connection can still be accessed by anyone over the Internet, which poses as a security vulnerability.

The option that says: Create a large EC2 instance with a security group which only allows access on port 22 via the IP address of the corporate data center. Use a private key (.pem) file to connect to the bastion host is incorrect because you don't need a large instance for a bastion host as it does not require much CPU resources.

#### References:

<https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html>

<https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-established-through-a-bastion-host/>

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

## QUESTION 57

A company has multiple VPCs with IPv6 enabled for its suite of web applications. The Solutions Architect tried to deploy a new Amazon EC2 instance but she received an error saying that there is no IP address

available on the subnet.

How should the Solutions Architect resolve this problem?

- A. Ensure that the VPC has IPv6 CIDRs only. Remove any IPv4 CIDRs associated with the VPC.
- B. Set up a new IPv6-only subnet with a large CIDR range. Associate the new subnet with the VPC then launch the instance.
- C. Set up a new IPv4 subnet with a larger CIDR range. Associate the new subnet with the VPC and then launch the instance.
- D. Disable the IPv4 support in the VPC and use the available IPv6 addresses.

Answer: C

Explanation:

Amazon Virtual Private Cloud (VPC) is a service that lets you launch AWS resources in a logically isolated virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 for most resources in your virtual private cloud, helping to ensure secure and easy access to resources and applications.

A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a specified subnet. When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a CIDR block. Each subnet must reside entirely within one Availability Zone and cannot span zones. You can also optionally assign an IPv6 CIDR block to your VPC, and assign IPv6 CIDR blocks to your subnets.

The screenshot shows the AWS VPC console for a Default VPC. Key details include:

- VPC ID:** vpc-f2bf5897
- Tenancy:** Default
- Default VPC:** Yes
- Owner ID:** 1206189812345
- State:** Available
- DNS hostnames:** Enabled
- Route table:** rtb-45b15d26
- IPv4 CIDR:** 172.31.0.0/16
- IPv6 pool:** Amazon (Associated)
- DNS resolution:** Enabled
- Network ACL:** acl-870beee2 / TutorialsDojo
- IPv6 CIDR (Network border group):** 2600:1f18:15b3:bff0::/56 (us-east-1) (Associated)

If you have an existing VPC that supports IPv4 only and resources in your subnet that are configured to use IPv4 only, you can enable IPv6 support for your VPC and resources. Your VPC can operate in dualstack mode – your resources can communicate over IPv4, or IPv6, or both. IPv4 and IPv6 communication are independent of each other. You cannot disable IPv4 support for your VPC and subnets since this is the default IP addressing system for Amazon VPC and Amazon EC2.

By default, a new EC2 instance uses an IPv4 addressing protocol. To fix the problem in the scenario, you need to create a new IPv4 subnet and deploy the EC2 instance in the new subnet.

Hence, the correct answer is: Set up a new IPv4 subnet with a larger CIDR range. Associate the new subnet with the VPC and then launch the instance.

The option that says: Set up a new IPv6-only subnet with a large CIDR range. Associate the new subnet

with the VPC then launch the instance is incorrect because you need to add IPv4 subnet first before you can create an IPv6 subnet.

The option that says: Ensure that the VPC has IPv6 CIDRs only. Remove any IPv4 CIDRs associated with the VPC is incorrect because you can't have a VPC with IPv6 CIDRs only. The default IP addressing system in VPC is IPv4. You can only change your VPC to dual-stack mode where your resources can communicate over IPv4, or IPv6, or both, but not exclusively with IPv6 only.

The option that says: Disable the IPv4 support in the VPC and use the available IPv6 addresses is incorrect because you cannot disable the IPv4 support for your VPC and subnets since this is the default IP addressing system.

#### References:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-migrate-ipv6.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ip-addressing.html>

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

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

---

## QUESTION 58

An organization is currently using a tape backup solution to store its application data on-premises. They plan to use a cloud storage service to preserve the backup data for up to 10 years that may be accessed about once or twice a year.

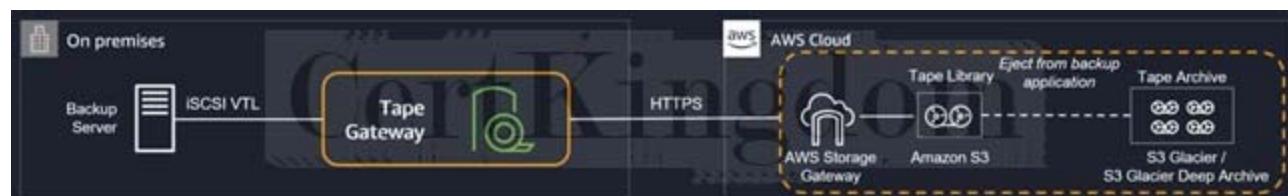
Which of the following is the most cost-effective option to implement this solution?

- A. Order an AWS Snowball Edge appliance to import the backup directly to Amazon S3 Glacier.
- B. Use AWS Storage Gateway to backup the data directly to Amazon S3 Glacier.
- C. Use Amazon S3 to store the backup data and add a lifecycle rule to transition the current version to Amazon S3 Glacier.
- D. Use AWS Storage Gateway to backup the data directly to Amazon S3 Glacier Deep Archive.

Answer: D

#### Explanation:

Tape Gateway enables you to replace using physical tapes on-premises with virtual tapes in AWS without changing existing backup workflows. Tape Gateway supports all leading backup applications and caches virtual tapes on-premises for low-latency data access. Tape Gateway encrypts data between the gateway and AWS for secure data transfer and compresses data and transitions virtual tapes between Amazon S3 and Amazon S3 Glacier, or Amazon S3 Glacier Deep Archive, to minimize storage costs.



The scenario requires you to backup your application data to a cloud storage service for long-term retention of data that will be retained for 10 years. Since it uses a tape backup solution, an option that uses AWS Storage Gateway must be the possible answer. Tape Gateway can move your virtual tapes archived in Amazon S3 Glacier or Amazon S3 Glacier Deep Archive storage class, enabling you to further reduce the monthly cost to store long-term data in the cloud by up to 75%.

Hence, the correct answer is: Use AWS Storage Gateway to backup the data directly to Amazon S3 Glacier Deep Archive.

The option that says: Use AWS Storage Gateway to backup the data directly to Amazon S3 Glacier is incorrect. Although this is a valid solution, moving to S3 Glacier is more expensive than directly backing it up to Glacier Deep Archive.

The option that says: Order an AWS Snowball Edge appliance to import the backup directly to Amazon S3 Glacier is incorrect because Snowball Edge can't directly integrate backups to S3 Glacier. Moreover, you have to use the Amazon S3 Glacier Deep Archive storage class as it is more cost-effective than the

regular Glacier class.

The option that says: Use Amazon S3 to store the backup data and add a lifecycle rule to transition the current version to Amazon S3 Glacier is incorrect. Although this is a possible solution, it is difficult to directly integrate a tape backup solution to S3 without using Storage Gateway.

References:

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

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

AWS Storage Gateway Overview:

<https://www.youtube.com/watch?v=pNb7xOBJjHE>

Check out this AWS Storage Gateway Cheat Sheet:

<https://tutorialsdojo.com/aws-storage-gateway/>

---

## QUESTION 59

A company runs a messaging application in the ap-northeast-1 and ap-southeast-2 region. A Solutions Architect needs to create a routing policy wherein a larger portion of traffic from the Philippines and North India will be routed to the resource in the ap-northeast-1 region.

Which Route 53 routing policy should the Solutions Architect use?

- A. Latency Routing
- B. Weighted Routing
- C. Geoproximity Routing
- D. Geolocation Routing

Answer: C

Explanation:

Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service. You can use Route 53 to perform three main functions in any combination: domain registration, DNS routing, and health checking. After you create a hosted zone for your domain, such as example.com, you create records to tell the Domain Name System (DNS) how you want traffic to be routed for that domain.

For example, you might create records that cause DNS to do the following:

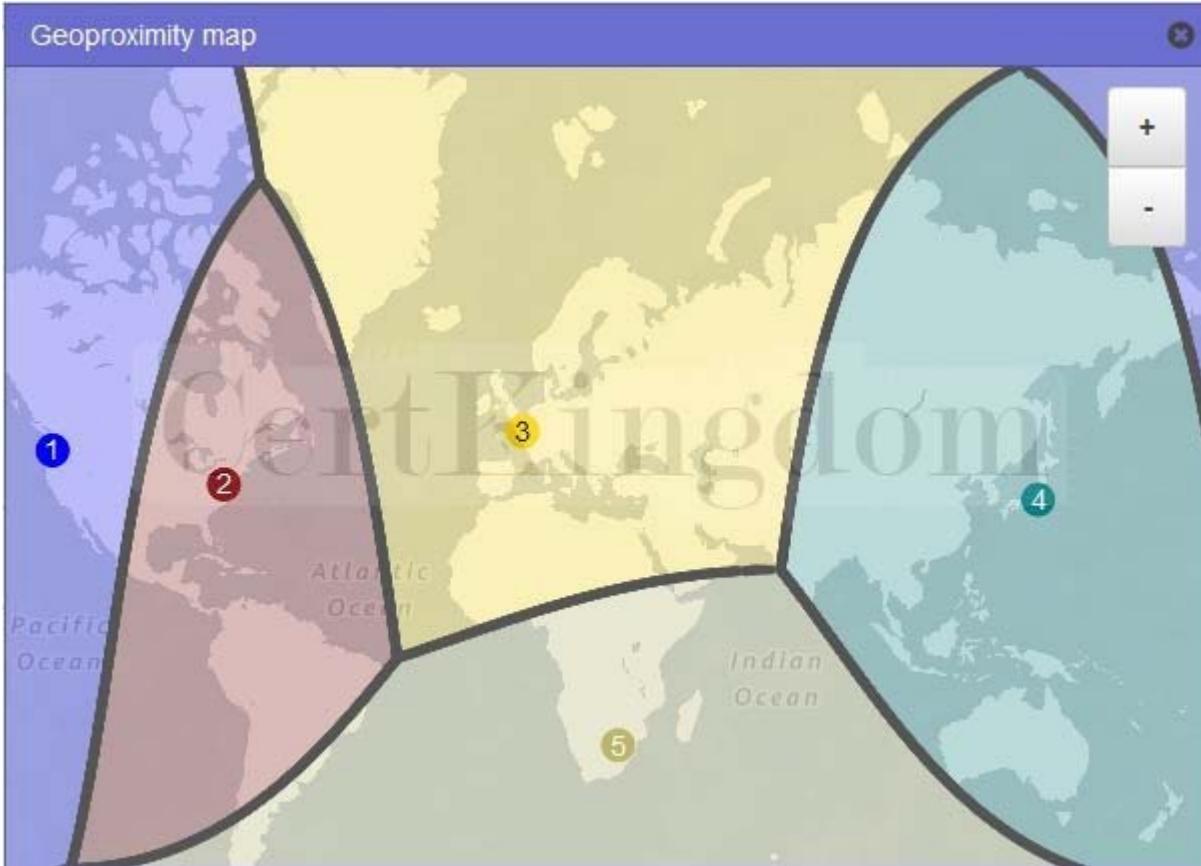
Route Internet traffic for example.com to the IP address of a host in your data center.

Route email for that domain (jose.rizal@tutorialsdojo.com) to a mail server (mail.tutorialsdojo.com).

Route traffic for a subdomain called operations.manila.tutorialsdojo.com to the IP address of a different host.

Each record includes the name of a domain or a subdomain, a record type (for example, a record with a type of MX routes email), and other information applicable to the record type (for MX records, the hostname of one or more mail servers and a priority for each server).

## Geoproximity map



Route 53 has different routing policies that you can choose from. Below are some of the policies:  
Latency Routing lets Amazon Route 53 serve user requests from the AWS Region that provides the lowest latency. It does not, however, guarantee that users in the same geographic region will be served from the same location.

Geoproximity Routing lets Amazon Route 53 route traffic to your resources based on the geographic location of your users and your resources. You can also optionally choose to route more traffic or less to a given resource by specifying a value, known as a bias. A bias expands or shrinks the size of the geographic region from which traffic is routed to a resource.

Geolocation Routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from.

Weighted Routing lets you associate multiple resources with a single domain name (tutorialsdojo.com) or subdomain name (subdomain.tutorialsdojo.com) and choose how much traffic is routed to each resource.

In this scenario, the problem requires a routing policy that will let Route 53 route traffic to the resource in the Tokyo region from a larger portion of the Philippines and North India.

## Geoproximity map



You need to use Geoproximity Routing and specify a bias to control the size of the geographic region from which traffic is routed to your resource. The sample image above uses a bias of -40 in the Tokyo region and a bias of 1 in the Sydney Region. Setting up the bias configuration in this manner would cause Route 53 to route traffic coming from the middle and northern part of the Philippines, as well as the northern part of India to the resource in the Tokyo Region.

Hence, the correct answer is: Geoproximity Routing.

Geolocation Routing is incorrect because you cannot control the coverage size from which traffic is routed to your instance in Geolocation Routing. It just lets you choose the instances that will serve traffic based on the location of your users.

Latency Routing is incorrect because it is mainly used for improving performance by letting Route 53 serve user requests from the AWS Region that provides the lowest latency.

Weighted Routing is incorrect because it is used for routing traffic to multiple resources in proportions that you specify. This can be useful for load balancing and testing new versions of a software.

References:

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

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/rrsets-working-with.html>

Latency Routing vs Geoproximity Routing vs Geolocation Routing:

<https://tutorialsdojo.com/latency-routing-vs-geoproximity-routing-vs-geolocation-routing/>

## QUESTION 60

A company plans to conduct a network security audit. The web application is hosted on an Auto Scaling group of EC2 Instances with an Application Load Balancer in front to evenly distribute the incoming traffic. A Solutions Architect has been tasked to enhance the security posture of the company's cloud infrastructure and minimize the impact of DDoS attacks on its resources.

Which of the following is the most effective solution that should be implemented?

- A. Configure Amazon CloudFront distribution and set a Network Load Balancer as the origin. Use Amazon GuardDuty to block suspicious hosts based on its security findings. Set up a custom AWS Lambda function that processes the security logs and invokes Amazon SNS for notification.

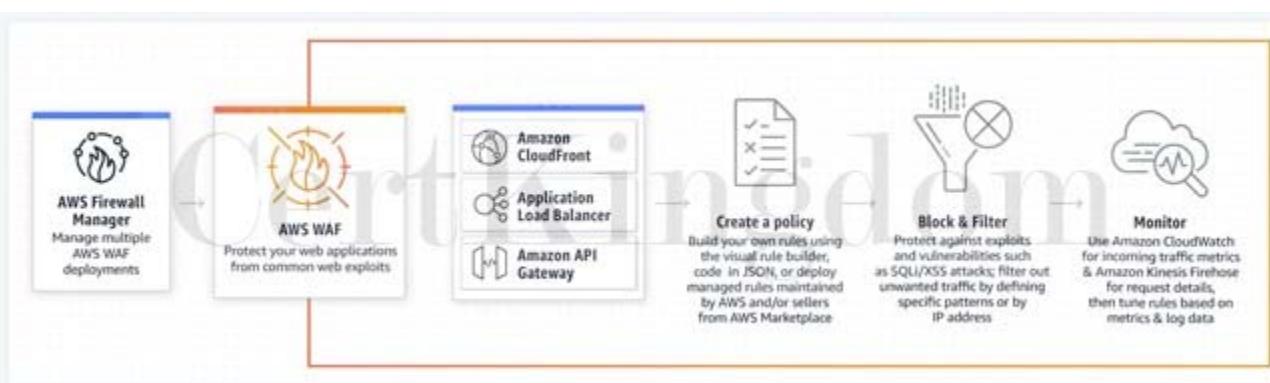
- B. Configure Amazon CloudFront distribution and set Application Load Balancer as the origin. Create a rate-based web ACL rule using AWS WAF and associate it with Amazon CloudFront.
- C. Configure Amazon CloudFront distribution and set a Network Load Balancer as the origin. Use VPC Flow Logs to monitor abnormal traffic patterns. Set up a custom AWS Lambda function that processes the flow logs and invokes Amazon SNS for notification.
- D. Configure Amazon CloudFront distribution and set an Application Load Balancer as the origin. Create a security group rule and deny all the suspicious addresses. Use Amazon SNS for notification.

Answer: B

Explanation:

AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic patterns you define. You can deploy AWS WAF on Amazon CloudFront as part of your CDN solution, the Application Load Balancer that fronts your web servers or origin servers running on EC2, or Amazon API Gateway for your APIs.

To detect and mitigate DDoS attacks, you can use AWS WAF in addition to AWS Shield. AWS WAF is a web application firewall that helps detect and mitigate web application layer DDoS attacks by inspecting traffic inline. Application layer DDoS attacks use well-formed but malicious requests to evade mitigation and consume application resources. You can define custom security rules that contain a set of conditions, rules, and actions to block attacking traffic. After you define web ACLs, you can apply them to CloudFront distributions, and web ACLs are evaluated in the priority order you specified when you configured them.



By using AWS WAF, you can configure web access control lists (Web ACLs) on your CloudFront distributions or Application Load Balancers to filter and block requests based on request signatures. Each Web ACL consists of rules that you can configure to string match or regex match one or more request attributes, such as the URI, query-string, HTTP method, or header key. In addition, by using AWS WAF's rate-based rules, you can automatically block the IP addresses of bad actors when requests matching a rule exceed a threshold that you define. Requests from offending client IP addresses will receive 403 Forbidden error responses and will remain blocked until request rates drop below the threshold. This is useful for mitigating HTTP flood attacks that are disguised as regular web traffic.

It is recommended that you add web ACLs with rate-based rules as part of your AWS Shield Advanced protection. These rules can alert you to sudden spikes in traffic that might indicate a potential DDoS event. A rate-based rule counts the requests that arrive from any individual address in any five-minute period. If the number of requests exceeds the limit that you define, the rule can trigger an action such as sending you a notification.

Hence, the correct answer is: Configure Amazon CloudFront distribution and set Application Load Balancer as the origin. Create a rate-based web ACL rule using AWS WAF and associate it with Amazon CloudFront.

The option that says: Configure Amazon CloudFront distribution and set a Network Load Balancer as the origin. Use VPC Flow Logs to monitor abnormal traffic patterns. Set up a custom AWS Lambda function that processes the flow logs and invokes Amazon SNS for notification is incorrect because this option only allows you to monitor the traffic that is reaching your instance. You can't use VPC Flow Logs to

mitigate DDoS attacks.

The option that says: Configure Amazon CloudFront distribution and set an Application Load Balancer as the origin. Create a security group rule and deny all the suspicious addresses. Use Amazon SNS for notification is incorrect. To deny suspicious addresses, you must manually insert the IP addresses of these hosts. This is a manual task which is not a sustainable solution. Take note that attackers generate large volumes of packets or requests to overwhelm the target system. Using a security group in this scenario won't help you mitigate DDoS attacks.

The option that says: Configure Amazon CloudFront distribution and set a Network Load Balancer as the origin. Use Amazon GuardDuty to block suspicious hosts based on its security findings. Set up a custom AWS Lambda function that processes the security logs and invokes Amazon SNS for notification is incorrect because Amazon GuardDuty is just a threat detection service. You should use AWS WAF and create your own AWS WAF rate-based rules for mitigating HTTP flood attacks that are disguised as regular web traffic.

References:

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html>

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-get-started-rate-based-rules.html>

[https://d0.awsstatic.com/whitepapers/Security/DDoS\\_White\\_Paper.pdf](https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf)

Check out this AWS WAF Cheat Sheet:

<https://tutorialsdojo.com/aws-waf/>

AWS Security Services Overview - WAF, Shield, CloudHSM, KMS:

<https://www.youtube.com/watch?v=-1S-RdeAmMo>

---

## QUESTION 61

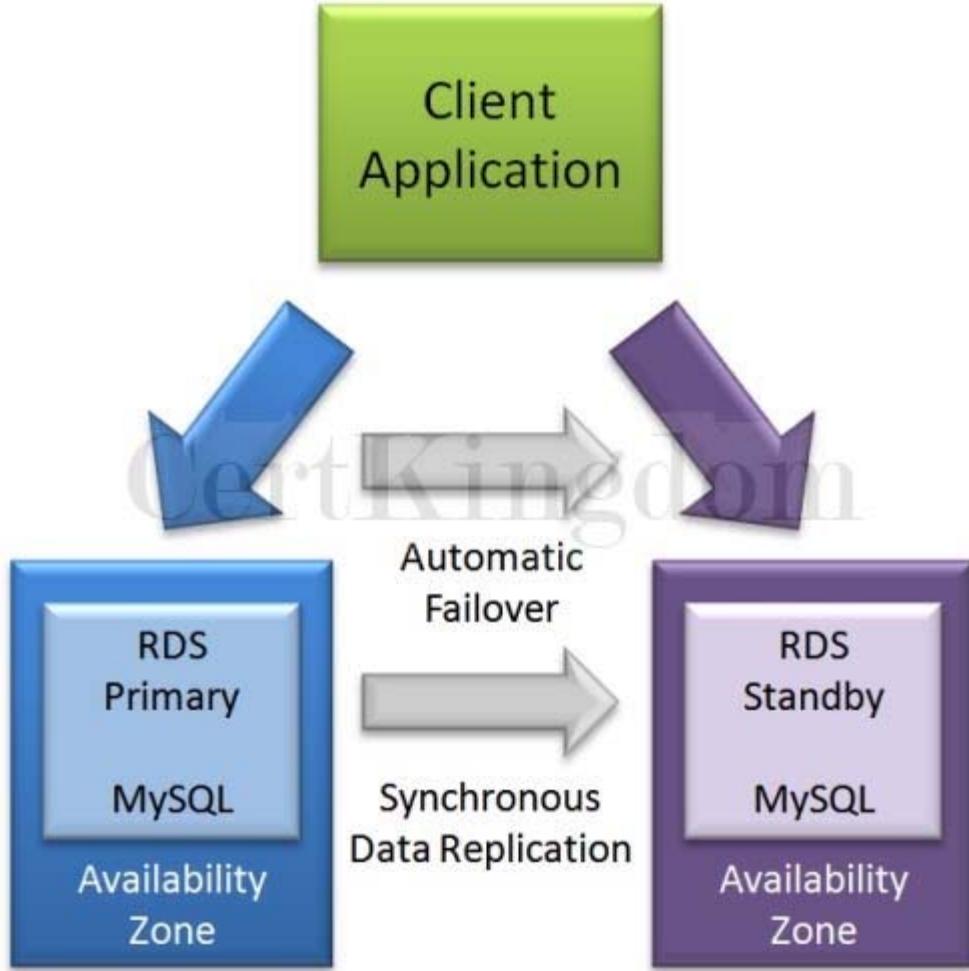
An accounting application uses an RDS database configured with Multi-AZ deployments to improve availability. What would happen to RDS if the primary database instance fails?

- A. The IP address of the primary DB instance is switched to the standby DB instance.
- B. The primary database instance will reboot.
- C. A new database instance is created in the standby Availability Zone.
- D. The canonical name record (CNAME) is switched from the primary to standby instance.

Answer: D

Explanation:

In Amazon RDS, failover is automatically handled so that you can resume database operations as quickly as possible without administrative intervention in the event that your primary database instance goes down. When failing over, Amazon RDS simply flips the canonical name record (CNAME) for your DB instance to point at the standby, which is in turn promoted to become the new primary.



The option that says: The IP address of the primary DB instance is switched to the standby DB instance is incorrect since IP addresses are per subnet, and subnets cannot span multiple AZs.

The option that says: The primary database instance will reboot is incorrect since in the event of a failure, there is no database to reboot with.

The option that says: A new database instance is created in the standby Availability Zone is incorrect since with multi-AZ enabled, you already have a standby database in another AZ.

References:

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

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

Amazon RDS Overview:

<https://youtu.be/aZmpL18K1UU>

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

## QUESTION 62

A music publishing company is building a mult-tier web application that requires a key-value store which will save the document models. Each model is composed of band ID, album ID, song ID, composer ID, lyrics, and other data. The web tier will be hosted in an Amazon ECS cluster with AWS Fargate launch type.

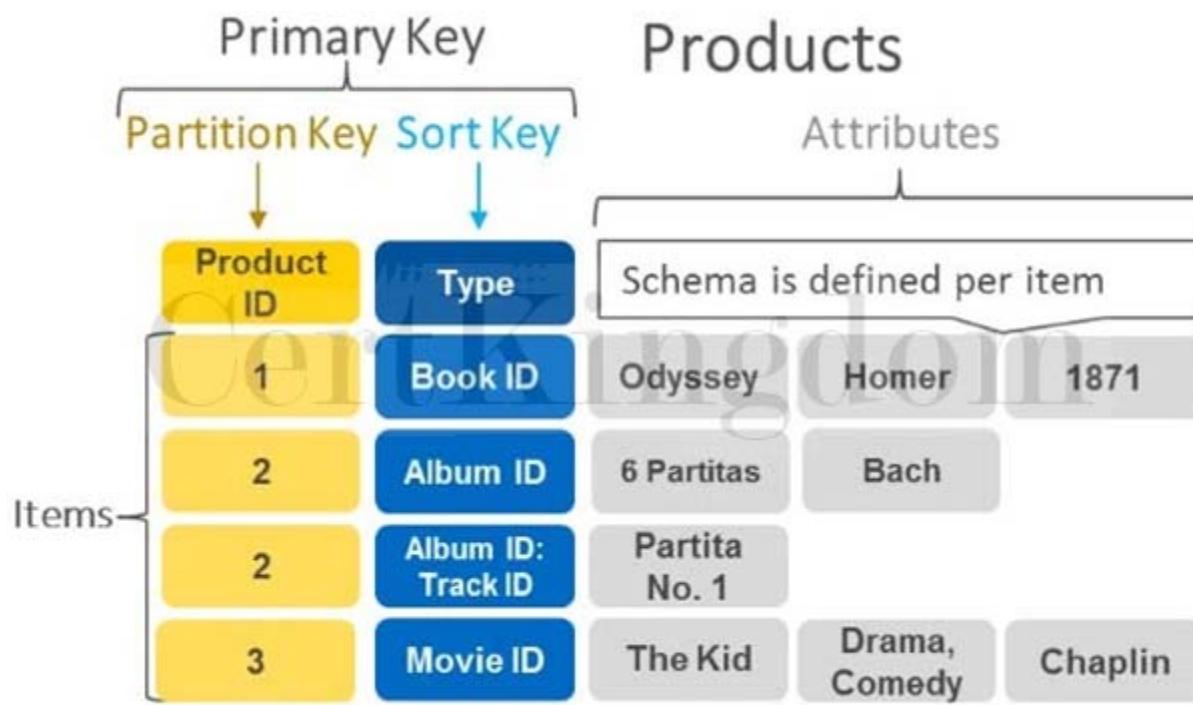
Which of the following is the MOST suitable setup for the database-tier?

- A. Launch an Amazon RDS database with Read Replicas.
- B. Use Amazon WorkDocs to store the document models.
- C. Launch a DynamoDB table.
- D. Launch an Amazon Aurora Serverless database.

Answer: C

## Explanation:

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed cloud database and supports both document and key-value store models. Its flexible data model, reliable performance, and automatic scaling of throughput capacity makes it a great fit for mobile, web, gaming, ad tech, IoT, and many other applications.



Hence, the correct answer is: Launch a DynamoDB table.

The option that says: Launch an Amazon RDS database with Read Replicas is incorrect because this is a relational database. This is not suitable to be used as a key-value store. A better option is to use DynamoDB as it supports both document and key-value store models.

The option that says: Use Amazon WorkDocs to store the document models is incorrect because Amazon WorkDocs simply enables you to share content, provide rich feedback, and collaboratively edit documents. It is not a key-value store like DynamoDB.

The option that says: Launch an Amazon Aurora Serverless database is incorrect because this type of database is not suitable to be used as a key-value store. Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora where the database will automatically start-up, shut down, and scale capacity up or down based on your application's needs. It enables you to run your database in the cloud without managing any database instances. It's a simple, cost-effective option for infrequent, intermittent, or unpredictable workloads and not as a key-value store.

References:

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

<https://aws.amazon.com/nosql/key-value/>

Check out this Amazon DynamoDB Cheat Sheet:

<https://tutorialsdojo.com/amazon-dynamodb/>

Amazon DynamoDB Overview:

<https://www.youtube.com/watch?v=3ZOyUNIeorU>

## QUESTION 63

An insurance company utilizes SAP HANA for its day-to-day ERP operations. Since they can't migrate this database due to customer preferences, they need to integrate it with the current AWS workload in the VPC in which they are required to establish a site-to-site VPN connection.

What needs to be configured outside of the VPC for them to have a successful site-to-site VPN

connection?

- A. An EIP to the Virtual Private Gateway
- B. A dedicated NAT instance in a public subnet
- C. An Internet-routable IP address (static) of the customer gateway's external interface for the onpremises network
- D. The main route table in your VPC to route traffic through a NAT instance

Answer: C

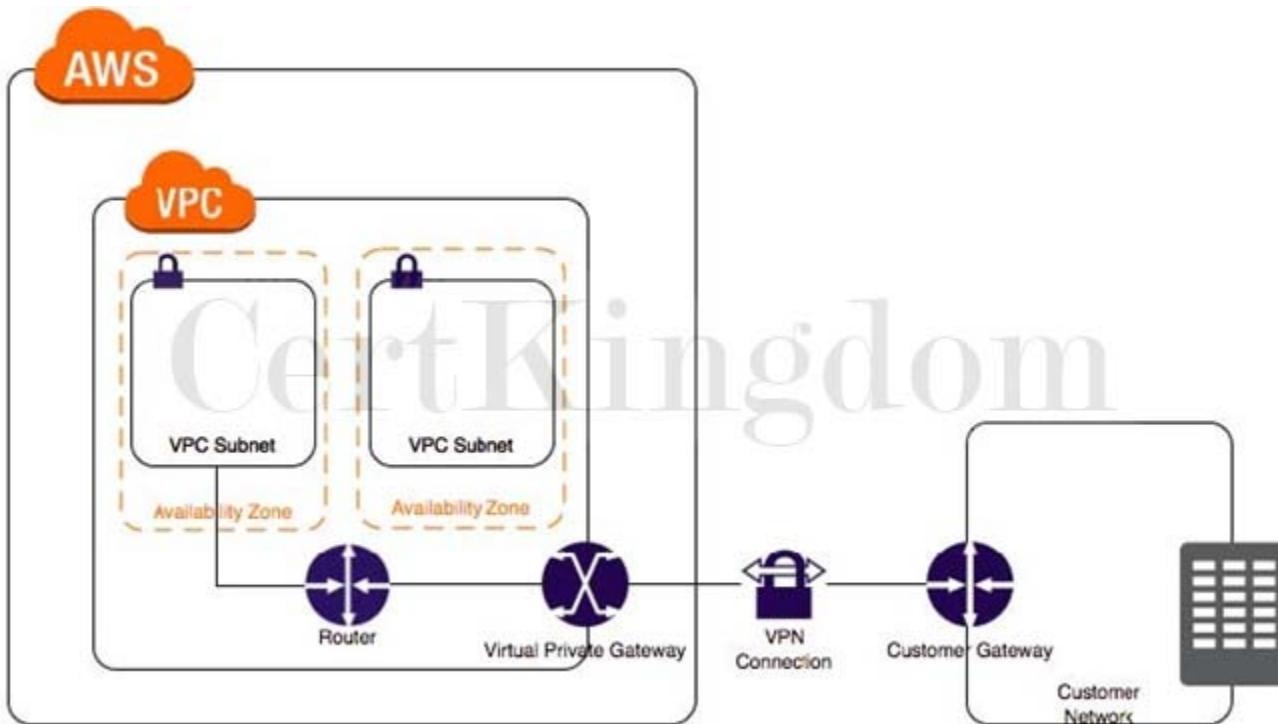
Explanation:

By default, instances that you launch into a virtual private cloud (VPC) can't communicate with your own network. You can enable access to your network from your VPC by attaching a virtual private gateway to the VPC, creating a custom route table, updating your security group rules, and creating an AWS managed VPN connection.

Although the term VPN connection is a general term, in the Amazon VPC documentation, a VPN connection refers to the connection between your VPC and your own network. AWS supports Internet Protocol security (IPsec) VPN connections.

A customer gateway is a physical device or software application on your side of the VPN connection. To create a VPN connection, you must create a customer gateway resource in AWS, which provides information to AWS about your customer gateway device. Next, you have to set up an Internet-routable IP address (static) of the customer gateway's external interface.

The following diagram illustrates single VPN connections. The VPC has an attached virtual private gateway, and your remote network includes a customer gateway, which you must configure to enable the VPN connection. You set up the routing so that any traffic from the VPC bound for your network is routed to the virtual private gateway.



The options that say: A dedicated NAT instance in a public subnet and the main route table in your VPC to route traffic through a NAT instance are incorrect since you don't need a NAT instance for you to be able to create a VPN connection.

An EIP to the Virtual Private Gateway is incorrect since you do not attach an EIP to a VPG.

References:

[https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_VPN.html](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html)

<https://docs.aws.amazon.com/vpc/latest/userguide/SetUpVPNConnections.html>

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

## QUESTION 64

As part of the Business Continuity Plan of your company, your IT Director instructed you to set up an automated backup of all of the EBS Volumes for your EC2 instances as soon as possible.  
What is the fastest and most cost-effective solution to automatically back up all of your EBS Volumes?

- A. Set your Amazon Storage Gateway with EBS volumes as the data source and store the backups in your on-premises servers through the storage gateway.
- B. Use an EBS-cycle policy in Amazon S3 to automatically back up the EBS volumes.
- C. For an automated solution, create a scheduled job that calls the "create-snapshot" command via the AWS CLI to take a snapshot of production EBS volumes periodically.
- D. Use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation of EBS snapshots.

Answer: D

Explanation:

You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots taken to back up your Amazon EBS volumes. Automating snapshot management helps you to:

- Protect valuable data by enforcing a regular backup schedule.
- Retain backups as required by auditors or internal compliance.
- Reduce storage costs by deleting outdated backups.

Combined with the monitoring features of Amazon CloudWatch Events and AWS CloudTrail, Amazon DLM provides a complete backup solution for EBS volumes at no additional cost.

Hence, using Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation of EBS snapshots is the correct answer as it is the fastest and most cost-effective solution that provides an automated way of backing up your EBS volumes.

The option that says: For an automated solution, create a scheduled job that calls the "create-snapshot" command via the AWS CLI to take a snapshot of production EBS volumes periodically is incorrect because even though this is a valid solution, you would still need additional time to create a scheduled job that calls the "create-snapshot" command. It would be better to use Amazon Data Lifecycle Manager (Amazon DLM) instead as this provides you the fastest solution which enables you to automate the creation, retention, and deletion of the EBS snapshots without having to write custom shell scripts or creating scheduled jobs.

Setting your Amazon Storage Gateway with EBS volumes as the data source and storing the backups in your on-premises servers through the storage gateway is incorrect as the Amazon Storage Gateway is used only for creating a backup of data from your on-premises server and not from the Amazon Virtual Private Cloud.

Using an EBS-cycle policy in Amazon S3 to automatically back up the EBS volumes is incorrect as there is no such thing as EBS-cycle policy in Amazon S3.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html>  
<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html>

Check out this Amazon EBS Cheat Sheet:

<https://tutorialsdojo.com/amazon-ebs/>

Amazon EBS Overview - SSD vs HDD:

<https://www.youtube.com/watch?v=LW7x8wyLFvw&t=8s>

## QUESTION 65

A solutions architect is designing a cost-efficient, highly available storage solution for company data. One of the requirements is to ensure that the previous state of a file is preserved and retrievable if a modified version of it is uploaded. Also, to meet regulatory compliance, data over 3 years must be retained in an archive and will only be accessible once a year.

How should the solutions architect build the solution?

- A. Create an S3 Standard bucket with object-level versioning enabled and configure a lifecycle rule

- that transfers files to Amazon S3 Glacier Deep Archive after 3 years.
- B. Create an S3 Standard bucket and enable S3 Object Lock in governance mode.
  - C. Create an S3 Standard bucket with S3 Object Lock in compliance mode enabled then configure a lifecycle rule that transfers files to Amazon S3 Glacier Deep Archive after 3 years.
  - D. Create a One-Zone-IA bucket with object-level versioning enabled and configure a lifecycle rule that transfers files to Amazon S3 Glacier Deep Archive after 3 years.

Answer: A

Explanation:

Versioning in Amazon S3 is a means of keeping multiple variants of an object in the same bucket. You can use the S3 Versioning feature to preserve, retrieve, and restore every version of every object stored in your buckets. With versioning, you can recover more easily from both unintended user actions and application failures. After versioning is enabled for a bucket, if Amazon S3 receives multiple write requests for the same object simultaneously, it stores all of those objects.

Hence, the correct answer is: Create an S3 Standard bucket with object-level versioning enabled and configure a lifecycle rule that transfers files to Amazon S3 Glacier Deep Archive after 3 years.

The S3 Object Lock feature allows you to store objects using a write-once-read-many (WORM) model. In the scenario, changes to objects are allowed but their previous versions should be preserved and remain retrievable. If you enable the S3 Object Lock feature, you won't be able to upload new versions of an object. This feature is only helpful when you want to prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely.

Therefore, the following options are incorrect:

- Create an S3 Standard bucket and enable S3 Object Lock in governance mode.
- Create an S3 Standard bucket with S3 Object Lock in compliance mode enabled then configure a lifecycle rule that transfers files to Amazon S3 Glacier Deep Archive after 3 years.

The option that says: Create a One-Zone-IA bucket with object-level versioning enabled and configure a lifecycle rule that transfers files to Amazon S3 Glacier Deep Archive after 3 years is incorrect. One-Zone-IA is not highly available as it only relies on one availability zone for storing data.

References:

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

<https://aws.amazon.com/blogs/aws/new-amazon-s3-storage-class-glacier-deep-archive/>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

---

## QUESTION 66

A Solutions Architect is working for a financial company. The manager wants to have the ability to automatically transfer obsolete data from their S3 bucket to a low-cost storage system in AWS.

What is the best solution that the Architect can provide to them?

- A. Use Lifecycle Policies in S3 to move obsolete data to Glacier.
- B. Use CloudEndure Migration.
- C. Use Amazon SQS.
- D. Use an EC2 instance and a scheduled job to transfer the obsolete data from their S3 location to Amazon S3 Glacier.

Answer: A

Explanation:

In this scenario, you can use lifecycle policies in S3 to automatically move obsolete data to Glacier.

Lifecycle configuration in Amazon S3 enables you to specify the lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects.

These actions can be classified as follows:

Transition actions “ In which you define when objects transition to another storage class. For example, you may choose to transition objects to the STANDARD\_IA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.

Expiration actions “ In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.

The option that says: Use an EC2 instance and a scheduled job to transfer the obsolete data from their S3 location to Amazon S3 Glacier is incorrect because you don't need to create a scheduled job in EC2 as you can simply use the lifecycle policy in S3.

The option that says: Use Amazon SQS is incorrect as SQS is not a storage service. Amazon SQS is primarily used to decouple your applications by queueing the incoming requests of your application.

The option that says: Use CloudEndure Migration is incorrect because this service is just a highly automated lift-and-shift (rehost) solution that simplifies, expedites, and reduces the cost of migrating applications to AWS. You cannot use this to automatically transition your S3 objects to a cheaper storage class.

References:

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

<https://aws.amazon.com/blogs/aws/archive-s3-to-glacier/>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

## QUESTION 67

A company needs to use Amazon Aurora as the Amazon RDS database engine of their web application. The Solutions Architect has been instructed to implement a 90-day backup retention policy.

Which of the following options can satisfy the given requirement?

- Create a daily scheduled event using CloudWatch Events and AWS Lambda to directly download the RDS automated snapshot to an S3 bucket. Archive snapshots older than 90 days to Glacier.
- Configure an automated backup and set the backup retention period to 90 days.
- Create an AWS Backup plan to take daily snapshots with a retention period of 90 days.
- Configure RDS to export the automated snapshot automatically to Amazon S3 and create a lifecycle policy to delete the object after 90 days.

Answer: C

Explanation:

AWS Backup is a centralized backup service that makes it easy and cost-effective for you to backup your application data across AWS services in the AWS Cloud, helping you meet your business and regulatory backup compliance requirements. AWS Backup makes protecting your AWS storage volumes, databases, and file systems simple by providing a central place where you can configure and audit the AWS resources you want to backup, automate backup scheduling, set retention policies, and monitor all recent backup and restore activity.



In this scenario, you can use AWS Backup to create a backup plan with a retention period of 90 days. A backup plan is a policy expression that defines when and how you want to back up your AWS resources. You assign resources to backup plans, and AWS Backup then automatically backs up and retains backups for those resources according to the backup plan.

Hence, the correct answer is: Create an AWS Backup plan to take daily snapshots with a retention period of 90 days.

The option that says: Configure an automated backup and set the backup retention period to 90 days is incorrect because the maximum backup retention period for automated backup is only 35 days.

The option that says: Configure RDS to export the automated snapshot automatically to Amazon S3 and create a lifecycle policy to delete the object after 90 days is incorrect because you can't export an automated snapshot automatically to Amazon S3. You must export the snapshot manually.

The option that says: Create a daily scheduled event using CloudWatch Events and AWS Lambda to directly download the RDS automated snapshot to an S3 bucket. Archive snapshots older than 90 days to Glacier is incorrect because you cannot directly download or export an automated snapshot in RDS to Amazon S3. You have to copy the automated snapshot first for it to become a manual snapshot, which you can move to an Amazon S3 bucket. A better solution for this scenario is to simply use AWS Backup.

References:

<https://docs.aws.amazon.com/aws-backup/latest/devguide/create-a-scheduled-backup.html>

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

Check out these AWS Cheat Sheets:

<https://tutorialsdojo.com/links-to-all-aws-cheat-sheets/>

## QUESTION 68

A Solutions Architect is working for a large IT consulting firm. One of the clients is launching a file sharing web application in AWS which requires a durable storage service for hosting their static contents such as PDFs, Word Documents, high-resolution images, and many others.

Which type of storage service should the Architect use to meet this requirement?

- A. Amazon EBS volume
- B. Amazon S3
- C. Amazon EC2 instance store
- D. Amazon RDS instance

Answer: B

## Explanation:

Amazon S3 is storage for the Internet. It's a simple storage service that offers software developers a durable, highly-scalable, reliable, and low-latency data storage infrastructure at very low costs. Amazon S3 provides customers with a highly durable storage infrastructure. Versioning offers an additional level of protection by providing a means of recovery when customers accidentally overwrite or delete objects. Remember that the scenario requires a durable storage for static content. These two keywords are actually referring to S3, since it is highly durable and suitable for storing static content. Hence, Amazon S3 is the correct answer.

Storage Need	Solution	AWS Services
Temporary storage	Consider using local instance store volumes for needs such as scratch disks, buffers, queues, and caches.	<a href="#">Amazon Local Instance Store</a>
Multi-instance storage	Amazon EBS volumes can only be attached to one EC2 instance at a time. If you need multiple EC2 instances accessing volume data at the same time, consider using Amazon EFS as a file system.	<a href="#">Amazon EFS</a>
Highly durable storage	If you need very highly durable storage, use S3 or Amazon EFS. Amazon S3 Standard storage is designed for 99.99999999 percent (11 nines) annual durability per object. You can even decide to take a snapshot of the EBS volumes. Such a snapshot then gets saved in Amazon S3, thus providing you the durability of Amazon S3. For more information on EBS durability, see the <a href="#">Durability and Availability</a> section. EFS is designed for high durability and high availability, with data stored in multiple Availability Zones within an AWS Region.	<a href="#">Amazon S3</a> <a href="#">Amazon EFS</a>
Static data or web content	If your data doesn't change that often, Amazon S3 might represent a more cost-effective and scalable solution for storing this fixed information. Also, web content served out of Amazon EBS requires a web server running on Amazon EC2; in contrast, you can deliver web content directly out of Amazon S3 or from multiple EC2 instances using Amazon EFS.	<a href="#">Amazon S3</a> <a href="#">Amazon EFS</a>

Amazon EBS volume is incorrect because this is not as durable compared with S3. In addition, it is best to store the static contents in S3 rather than EBS.

Amazon EC2 instance store is incorrect because it is definitely not suitable - the data it holds will be wiped out immediately once the EC2 instance is restarted.

Amazon RDS instance is incorrect because an RDS instance is just a database and not suitable for storing static content. By default, RDS is not durable, unless you launch it to be in Multi-AZ deployments configuration.

Reference:

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

<https://d1.awsstatic.com/whitepapers/Storage/AWS%20Storage%20Services%20Whitepaper-v9.pdf#page=24>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

## QUESTION 69

A company is hosting an application on EC2 instances that regularly pushes and fetches data in Amazon S3. Due to a change in compliance, the instances need to be moved on a private subnet. Along with this change, the company wants to lower the data transfer costs by configuring its AWS resources. How can this be accomplished in the MOST cost-efficient manner?

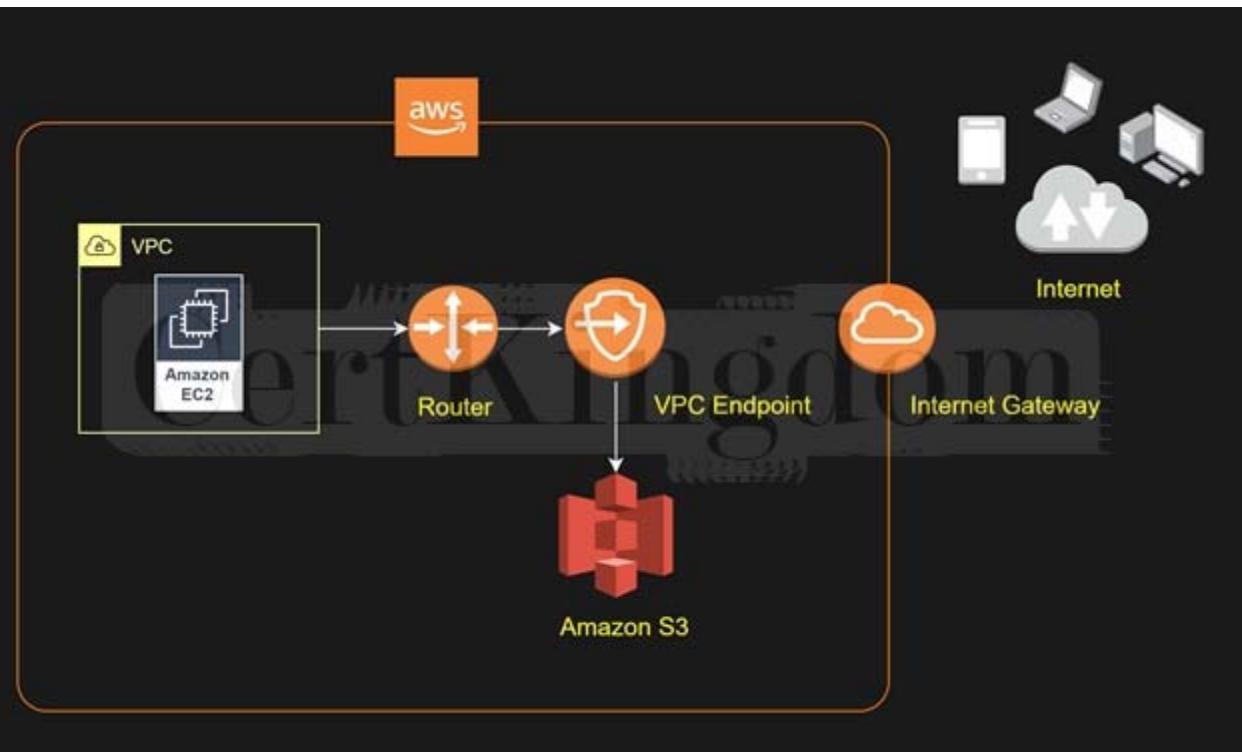
- A. Set up a NAT Gateway in the public subnet to connect to Amazon S3.
- B. Set up an AWS Transit Gateway to access Amazon S3.
- C. Create an Amazon S3 interface endpoint to enable a connection between the instances and Amazon S3.
- D. Create an Amazon S3 gateway endpoint to enable a connection between the instances and Amazon S3.

Answer: D

Explanation:

VPC endpoints for Amazon S3 simplify access to S3 from within a VPC by providing configurable and highly reliable secure connections to S3 that do not require an internet gateway or Network Address Translation (NAT) device. When you create an S3 VPC endpoint, you can attach an endpoint policy to it that controls access to Amazon S3.

You can use two types of VPC endpoints to access Amazon S3: gateway endpoints and interface endpoints. A gateway endpoint is a gateway that you specify in your route table to access Amazon S3 from your VPC over the AWS network. Interface endpoints extend the functionality of gateway endpoints by using private IP addresses to route requests to Amazon S3 from within your VPC, on-premises, or from a different AWS Region. Interface endpoints are compatible with gateway endpoints. If you have an existing gateway endpoint in the VPC, you can use both types of endpoints in the same VPC.



There is no additional charge for using gateway endpoints. However, standard charges for data transfer and resource usage still apply.

Hence, the correct answer is: Create an Amazon S3 gateway endpoint to enable a connection between the instances and Amazon S3.

The option that says: Set up a NAT Gateway in the public subnet to connect to Amazon S3 is incorrect. This will enable a connection between the private EC2 instances and Amazon S3 but it is not the most cost-efficient solution. NAT Gateways are charged on an hourly basis even for idle time.

The option that says: Create an Amazon S3 interface endpoint to enable a connection between the instances and Amazon S3 is incorrect. This is also a possible solution but it's not the most cost-effective solution. You pay an hourly rate for every provisioned Interface endpoint.

The option that says: Set up an AWS Transit Gateway to access Amazon S3 is incorrect because this service is mainly used for connecting VPCs and on-premises networks through a central hub.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html>

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

Check out this Amazon S3 Cheat Sheet:  
<https://tutorialsdojo.com/amazon-s3/>

## QUESTION 70

A company is hosting EC2 instances that are on non-production environment and processing non-priority batch loads, which can be interrupted at any time.

What is the best instance purchasing option which can be applied to your EC2 instances in this case?

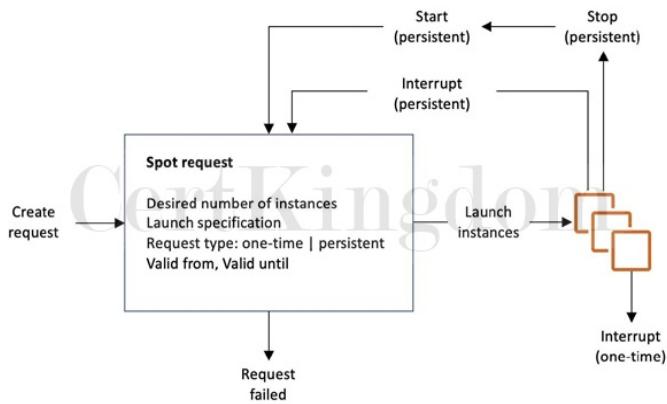
- A. On-Demand Instances
- B. Spot Instances
- C. Reserved Instances
- D. On-Demand Capacity Reservations

Answer: B

Explanation:

Amazon EC2 Spot instances are spare compute capacity in the AWS cloud available to you at steep discounts compared to On-Demand prices. It can be interrupted by AWS EC2 with two minutes of notification when the EC2 needs the capacity back.

To use Spot Instances, you create a Spot Instance request that includes the number of instances, the instance type, the Availability Zone, and the maximum price that you are willing to pay per instance hour. If your maximum price exceeds the current Spot price, Amazon EC2 fulfills your request immediately if capacity is available. Otherwise, Amazon EC2 waits until your request can be fulfilled or until you cancel the request.



References:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html>

<https://aws.amazon.com/ec2/spot/>

Amazon EC2 Overview:

[https://youtu.be/VsGIHT\\_jQE](https://youtu.be/VsGIHT_jQE)

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

## QUESTION 71

A company currently has an Augment Reality (AR) mobile game that has a serverless backend. It is using a DynamoDB table which was launched using the AWS CLI to store all the user data and information gathered from the players and a Lambda function to pull the data from DynamoDB. The game is being used by millions of users each day to read and store data.

How would you design the application to improve its overall performance and make it more scalable while keeping the costs low? (Select TWO.)

- A. Use AWS SSO and Cognito to authenticate users and have them directly access DynamoDB using

single-sign on. Manually set the provisioned read and write capacity to a higher RCU and WCU.

B. Configure CloudFront with DynamoDB as the origin; cache frequently accessed data on the client device using ElastiCache.

C. Use API Gateway in conjunction with Lambda and turn on the caching on frequently accessed data and enable DynamoDB global replication.

D. Enable DynamoDB Accelerator (DAX) and ensure that the Auto Scaling is enabled and increase the maximum provisioned read and write capacity.

E. Since Auto Scaling is enabled by default, the provisioned read and write capacity will adjust automatically. Also enable DynamoDB Accelerator (DAX) to improve the performance from milliseconds to microseconds.

Answer: C,D

Explanation:

The correct answers are the options that say:

- Enable DynamoDB Accelerator (DAX) and ensure that the Auto Scaling is enabled and increase the maximum provisioned read and write capacity.

- Use API Gateway in conjunction with Lambda and turn on the caching on frequently accessed data and enable DynamoDB global replication.

Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB that delivers up to a 10x performance improvement ““ from milliseconds to microseconds ““ even at millions of requests per second. DAX does all the heavy lifting required to add in-memory acceleration to your DynamoDB tables, without requiring developers to manage cache invalidation, data population, or cluster management.

## Scaling activities

### Provisioned capacity

Read capacity units

Table

5

Write capacity units

5

! Consumed read capacity >= 4 for 5 minutes

Estimated cost \$2.91 / month ([Capacity calculator](#))

### Auto Scaling

<input checked="" type="checkbox"/> Read capacity	<input type="checkbox"/> Write capacity
Target utilization	70 %

Minimum provisioned capacity 5 units

Maximum provisioned capacity 40000 units

Apply same settings to global secondary indexes

**IAM Role** I authorize DynamoDB to scale capacity using the following role:

- New role: DynamoDBAutoscaleRole
- Existing role with pre defined policies [[Instructions](#)]

Role Name\*

[Save](#) [Cancel](#)

Amazon API Gateway lets you create an API that acts as a "front door" for applications to access data, business logic, or functionality from your back-end services, such as code running on AWS Lambda. Amazon API Gateway handles all of the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management. Amazon API Gateway has no minimum fees or startup costs. AWS Lambda scales your functions automatically on your behalf. Every time an event notification is received for your function, AWS Lambda quickly locates free capacity within its compute fleet and runs your code. Since your code is stateless, AWS Lambda can start as many copies of your function as needed without lengthy deployment and configuration delays.

The option that says: Configure CloudFront with DynamoDB as the origin; cache frequently accessed data on the client device using ElastiCache is incorrect. Although CloudFront delivers content faster to your users using edge locations, you still cannot integrate DynamoDB table with CloudFront as these two are incompatible.

The option that says: Use AWS SSO and Cognito to authenticate users and have them directly access DynamoDB using single-sign on. Manually set the provisioned read and write capacity to a higher RCU and WCU is incorrect because AWS Single Sign-On (SSO) is a cloud SSO service that just makes it easy to centrally manage SSO access to multiple AWS accounts and business applications. This will not be of much help on the scalability and performance of the application. It is costly to manually set the provisioned read and write capacity to a higher RCU and WCU because this capacity will run round the clock and will still be the same even if the incoming traffic is stable and there is no need to scale.

The option that says: Since Auto Scaling is enabled by default, the provisioned read and write capacity will adjust automatically. Also enable DynamoDB Accelerator (DAX) to improve the performance from

milliseconds to microseconds is incorrect because, by default, Auto Scaling is not enabled in a DynamoDB table which is created using the AWS CLI.

References:

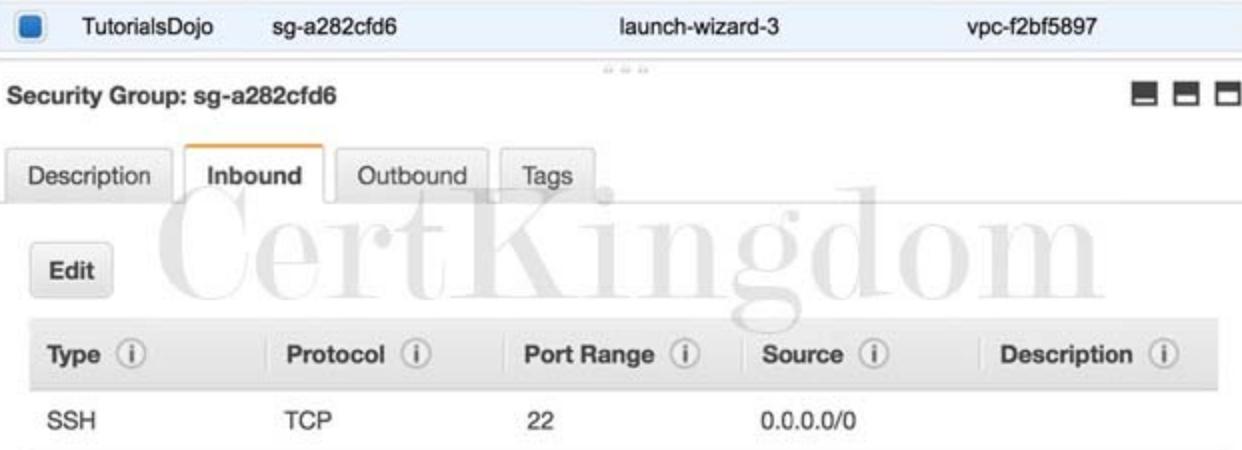
<https://aws.amazon.com/lambda/faqs/>  
<https://aws.amazon.com/api-gateway/faqs/>  
<https://aws.amazon.com/dynamodb/dax/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

## QUESTION 72

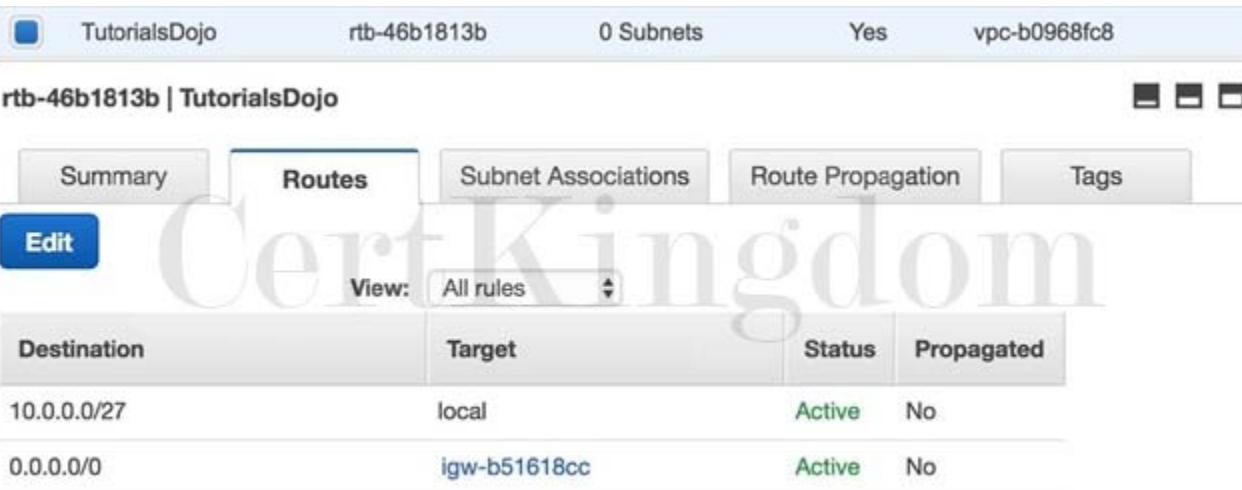
A company has an On-Demand EC2 instance located in a subnet in AWS that hosts a web application. The security group attached to this EC2 instance has the following Inbound Rules:



The screenshot shows the AWS Security Groups console for a security group named 'sg-a282cf6'. The 'Inbound' tab is selected. An inbound rule is listed with the following details:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	

The Route table attached to the VPC is shown below. You can establish an SSH connection into the EC2 instance from the Internet. However, you are not able to connect to the web server using your Chrome browser.



The screenshot shows the AWS Route Tables console for a route table named 'rtb-46b1813b'. The 'Routes' tab is selected. Two routes are listed:

Destination	Target	Status	Propagated
10.0.0.0/27	local	Active	No
0.0.0.0/0	igw-b51618cc	Active	No

Which of the below steps would resolve the issue?

- A. In the Route table, add this new route entry: 0.0.0.0 -> igw-b51618cc
- B. In the Route table, add this new route entry: 10.0.0.0 -> local
- C. In the Security Group, remove the SSH rule.
- D. In the Security Group, add an Inbound HTTP rule.

Answer: D

## Explanation:

In this particular scenario, you can already connect to the EC2 instance via SSH. This means that there is no problem in the Route Table of your VPC. To fix this issue, you simply need to update your Security Group and add an Inbound rule to allow HTTP traffic.

**Create Security Group**

Security group name	Web Server Security Group
Description	Security for production web server.
VPC	vpc-e68d9c81   DefaultVPC (default)

Security group rules:

Inbound    Outbound

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Anywhere	Admin access.
HTTP	TCP	80	Anywhere	Web traffic.
HTTPS	TCP	443	Custom	Secure web traffic.

Add Rule

Cancel    Create

The option that says: In the Security Group, remove the SSH rule is incorrect as doing so will not solve the issue. It will just disable SSH traffic that is already available.

The options that say: In the Route table, add this new route entry: 0.0.0.0 -> igw-b51618cc and In the Route table, add this new route entry: 10.0.0.0 -> local are incorrect as there is no need to change the Route Tables.

Reference:

[http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_SecurityGroups.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html)

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

## QUESTION 73

A company installed sensors to track the number of people who visit the park. The data is sent every day to an Amazon Kinesis stream with default settings for processing, in which a consumer is configured to process the data every other day. You noticed that the S3 bucket is not receiving all of the data that is being sent to the Kinesis stream. You checked the sensors if they are properly sending the data to Amazon Kinesis and verified that the data is indeed sent every day.

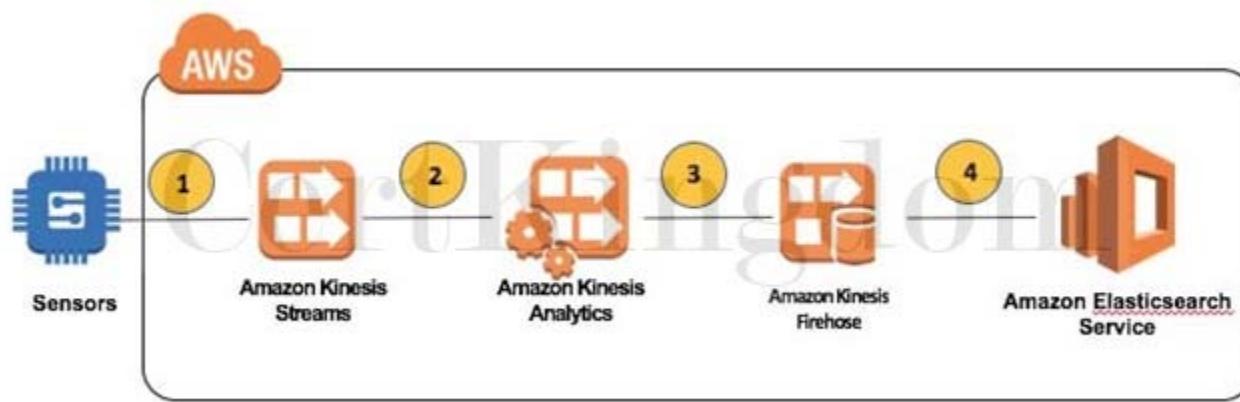
What could be the reason for this?

- A. There is a problem in the sensors. They probably had some intermittent connection hence, the data is not sent to the stream.
- B. By default, the data records are only accessible for 24 hours from the time they are added to a Kinesis stream.
- C. By default, Amazon S3 stores the data for 1 day and moves it to Amazon Glacier.
- D. Your AWS account was hacked and someone has deleted some data in your Kinesis stream.

Answer: B

## Explanation:

Kinesis Data Streams supports changes to the data record retention period of your stream. A Kinesis data stream is an ordered sequence of data records meant to be written to and read from in real-time. Data records are therefore stored in shards in your stream temporarily.



The time period from when a record is added to when it is no longer accessible is called the retention period. A Kinesis data stream stores records from 24 hours by default to a maximum of 8760 hours (365 days).

This is the reason why there are missing data in your S3 bucket. To fix this, you can either configure your sensors to send the data everyday instead of every other day or alternatively, you can increase the retention period of your Kinesis data stream.

The option that says: There is a problem in the sensors. They probably had some intermittent connection hence, the data is not sent to the stream is incorrect. You already verified that the sensors are working as they should be hence, this is not the root cause of the issue.

The option that says: By default, Amazon S3 stores the data for 1 day and moves it to Amazon Glacier is incorrect because by default, Amazon S3 does not store the data for 1 day only and move it to Amazon Glacier.

The option that says: Your AWS account was hacked and someone has deleted some data in your Kinesis stream is incorrect. Although this could be a possibility, you should verify first if there are other more probable reasons for the missing data in your S3 bucket. Be sure to follow and apply security best practices as well to prevent being hacked by someone.

By default, the data records are only accessible for 24 hours from the time they are added to a Kinesis stream, which depicts the root cause of this issue.

Reference:

<http://docs.aws.amazon.com/streams/latest/dev/kinesis-extended-retention.html>

Check out this Amazon Kinesis Cheat Sheet:

<https://tutorialsdojo.com/amazon-kinesis/>

## QUESTION 74

A company is deploying a Microsoft SharePoint Server environment on AWS using CloudFormation. The Solutions Architect needs to install and configure the architecture that is composed of Microsoft Active Directory (AD) domain controllers, Microsoft SQL Server 2012, multiple Amazon EC2 instances to host the Microsoft SharePoint Server and many other dependencies. The Architect needs to ensure that the required components are properly running before the stack creation proceeds.

Which of the following should the Architect do to meet this requirement?

- A. Configure a CreationPolicy attribute to the instance in the CloudFormation template. Send a success signal after the applications are installed and configured using the cfn-signal helper script.
- B. Configure the UpdateReplacePolicy attribute in the CloudFormation template. Send a success signal after the applications are installed and configured using the cfn-signal helper script.
- C. Configure the DependsOn attribute in the CloudFormation template. Send a success signal after the applications are installed and configured using the cfn-init helper script.
- D. Configure a UpdatePolicy attribute to the instance in the CloudFormation template. Send a success signal after the applications are installed and configured using the cfn-signal helper script.

Answer: A

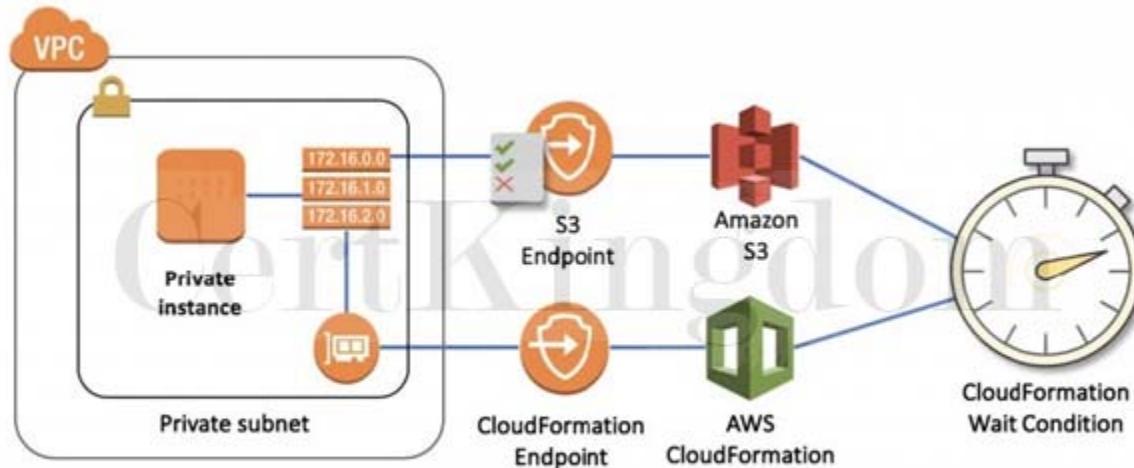
Explanation:

You can associate the `CreationPolicy` attribute with a resource to prevent its status from reaching `create complete` until AWS CloudFormation receives a specified number of success signals or the timeout period is exceeded. To signal a resource, you can use the `cfn-signal` helper script or `SignalResource` API. AWS CloudFormation publishes valid signals to the stack events so that you track the number of signals sent.

The creation policy is invoked only when AWS CloudFormation creates the associated resource.

Currently, the only AWS CloudFormation resources that support creation policies are

`AWS::AutoScaling::AutoScalingGroup`, `AWS::EC2::Instance`, and `AWS::CloudFormation::WaitCondition`.



Use the `CreationPolicy` attribute when you want to wait on resource configuration actions before stack creation proceeds. For example, if you install and configure software applications on an EC2 instance, you might want those applications to be running before proceeding. In such cases, you can add a `CreationPolicy` attribute to the instance, and then send a success signal to the instance after the applications are installed and configured.

Hence, the option that says: Configure a `CreationPolicy` attribute to the instance in the CloudFormation template. Send a success signal after the applications are installed and configured using the `cfn-signal` helper script is correct.

The option that says: Configure the `DependsOn` attribute in the CloudFormation template. Send a success signal after the applications are installed and configured using the `cfn-init` helper script is incorrect because the `cfn-init` helper script is not suitable to be used to signal another resource. You have to use `cfn-signal` instead. And although you can use the `DependsOn` attribute to ensure the creation of a specific resource follows another, it is still better to use the `CreationPolicy` attribute instead as it ensures that the applications are properly running before the stack creation proceeds.

The option that says: Configure a `UpdatePolicy` attribute to the instance in the CloudFormation template. Send a success signal after the applications are installed and configured using the `cfn-signal` helper script is incorrect because the `UpdatePolicy` attribute is primarily used for updating resources and for stack update rollback operations.

The option that says: Configure the `UpdateReplacePolicy` attribute in the CloudFormation template. Send a success signal after the applications are installed and configured using the `cfn-signal` helper script is incorrect because the `UpdateReplacePolicy` attribute is primarily used to retain or in some cases, back up the existing physical instance of a resource when it is replaced during a stack update operation.

References:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-creationpolicy.html>

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/deploying.applications.html#deployment-walkthrough-cfn-signal>

<https://aws.amazon.com/blogs/devops/use-a-creationpolicy-to-wait-for-on-instance-configurations/>

Check out this AWS CloudFormation Cheat Sheet:

<https://tutorialsdojo.com/aws-cloudformation/>

AWS CloudFormation - Templates, Stacks, Change Sets:

<https://www.youtube.com/watch?v=9Xpuprxg7aY>

---

## QUESTION 75

A company needs to launch an Amazon EC2 instance with persistent block storage to host its application. The stored data must be encrypted at rest.

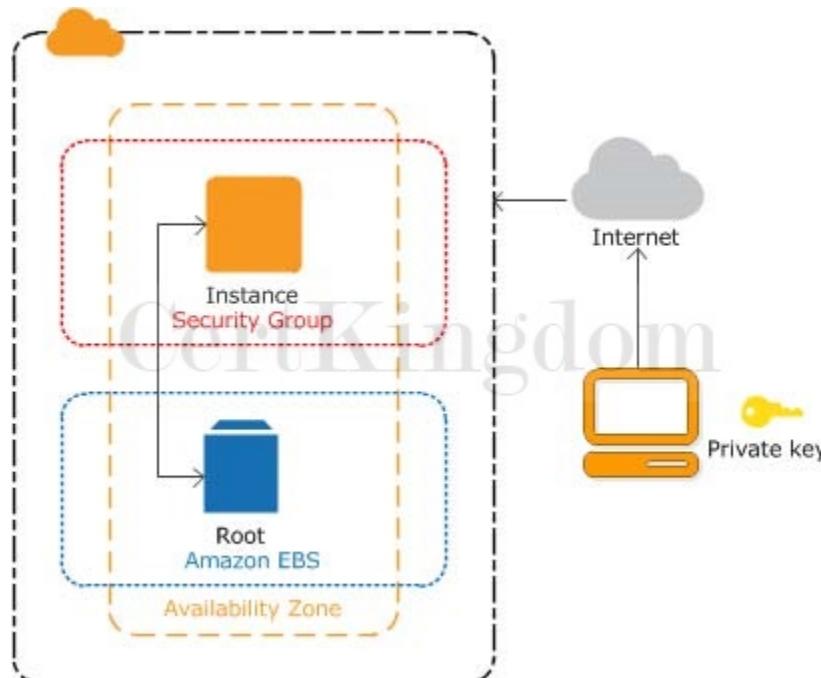
Which of the following is the most suitable storage solution in this scenario?

- A. Amazon EBS volume with server-side encryption (SSE) enabled.
- B. Encrypted Amazon EBS volume using AWS KMS.
- C. Encrypted Amazon EC2 Instance Store using AWS KMS.
- D. Amazon EC2 Instance Store with SSL encryption.

Answer: B

Explanation:

Amazon Elastic Block Store (Amazon EBS) provides block-level storage volumes for use with EC2 instances. EBS volumes behave like raw, unformatted block devices. You can mount these volumes as devices on your instances. EBS volumes that are attached to an instance are exposed as storage volumes that persist independently from the life of the instance.



Amazon EBS is the persistent block storage volume among the options given. It is mainly used as the root volume to store the operating system of an EC2 instance. To encrypt an EBS volume at rest, you can use AWS KMS customer master keys for the encryption of both the boot and data volumes of an EC2 instance.

Hence, the correct answer is: Encrypted Amazon EBS volume using AWS KMS.

The options that say: Amazon EC2 Instance Store with SSL encryption and Encrypted Amazon EC2 Instance Store using AWS KMS are both incorrect because the scenario requires persistent block storage and not temporary storage. Also, enabling SSL is not a requirement in the scenario as it is primarily used to encrypt data in transit.

The option that says: Amazon EBS volume with server-side encryption (SSE) enabled is incorrect because EBS volumes are only encrypted using AWS KMS. Server-side encryption (SSE) is actually an option for Amazon S3, but not for Amazon EC2.

References:

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

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

Check out this Amazon EBS Cheat Sheet:

<https://tutorialsdojo.com/amazon-ebs/>

---

## QUESTION 76

A company has an existing VPC which is quite unutilized for the past few months. The Business Manager instructed the Solutions Architect to integrate the company's on-premises data center and its VPC. The architect explained the list of tasks that he'll be doing and discussed the Virtual Private Network (VPN) connection. The Business Manager is not tech-savvy but he is interested to know what a VPN is and its benefits.

What is one of the major advantages of having a VPN in AWS?

- A. It enables you to establish a private and dedicated network connection between your network and your VPC
- B. It provides a cost-effective, hybrid connection from your VPC to your on-premises data centers which bypasses the public Internet.
- C. It provides a networking connection between two VPCs which enables you to route traffic between them using private IPv4 addresses or IPv6 addresses.
- D. It allows you to connect your AWS cloud resources to your on-premises data center using secure and private sessions with IP Security (IPSec) or Transport Layer Security (TLS) tunnels.

Answer: D

Explanation:

Amazon VPC offers you the flexibility to fully manage both sides of your Amazon VPC connectivity by creating a VPN connection between your remote network and a software VPN appliance running in your Amazon VPC network. This option is recommended if you must manage both ends of the VPN connection either for compliance purposes or for leveraging gateway devices that are not currently supported by Amazon VPC's VPN solution.

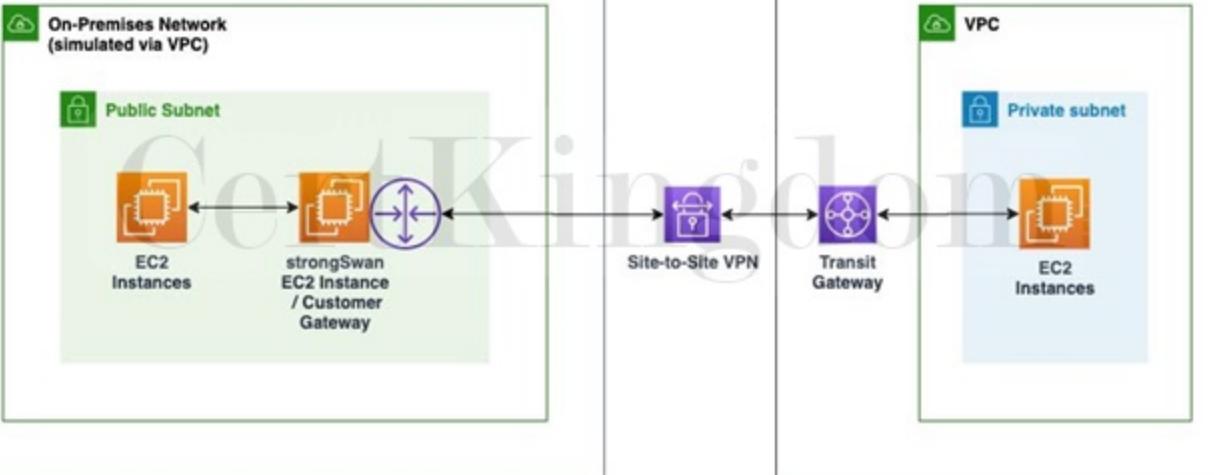
You can connect your Amazon VPC to remote networks and users using the following VPN connectivity options:

AWS Site-to-Site VPN - creates an IPsec VPN connection between your VPC and your remote network. On the AWS side of the Site-to-Site VPN connection, a virtual private gateway or transit gateway provides two VPN endpoints (tunnels) for automatic failover.

AWS Client VPN - a managed client-based VPN service that provides secure TLS VPN connections between your AWS resources and on-premises networks.

AWS VPN CloudHub - capable of wiring multiple AWS Site-to-Site VPN connections together on a virtual private gateway. This is useful if you want to enable communication between different remote networks that uses a Site-to-Site VPN connection.

Third-party software VPN appliance - You can create a VPN connection to your remote network by using an Amazon EC2 instance in your VPC that's running a third party software VPN appliance.



With a VPN connection, you can connect to an Amazon VPC in the cloud the same way you connect to your branches while establishing secure and private sessions with IP Security (IPSec) or Transport Layer Security (TLS) tunnels.

Hence, the correct answer is the option that says: It allows you to connect your AWS cloud resources to your on-premises data center using secure and private sessions with IP Security (IPSec) or Transport Layer Security (TLS) tunnels since one of the main advantages of having a VPN connection is that you will be able to connect your Amazon VPC to other remote networks securely.

The option that says: It provides a cost-effective, hybrid connection from your VPC to your on-premises data centers which bypasses the public Internet is incorrect. Although it is true that a VPN provides a cost-effective, hybrid connection from your VPC to your on-premises data centers, it certainly does not bypass the public Internet. A VPN connection actually goes through the public Internet, unlike the AWS Direct Connect connection which has a direct and dedicated connection to your on-premises network.

The option that says: It provides a networking connection between two VPCs which enables you to route traffic between them using private IPv4 addresses or IPv6 addresses is incorrect because this actually describes VPC Peering and not a VPN connection.

The option that says: It enables you to establish a private and dedicated network connection between your network and your VPC is incorrect because this is the advantage of an AWS Direct Connect connection and not a VPN.

#### References:

<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html>

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/software-vpn-network-toamazon.html>

#### Amazon VPC Overview:

<https://www.youtube.com/watch?v=oIDHKeN xvQQ>

#### Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

#### Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

## QUESTION 77

An aerospace engineering company recently adopted a hybrid cloud infrastructure with AWS. One of the Solutions Architect's tasks is to launch a VPC with both public and private subnets for their EC2 instances as well as their database instances.

Which of the following statements are true regarding Amazon VPC subnets? (Select TWO.)

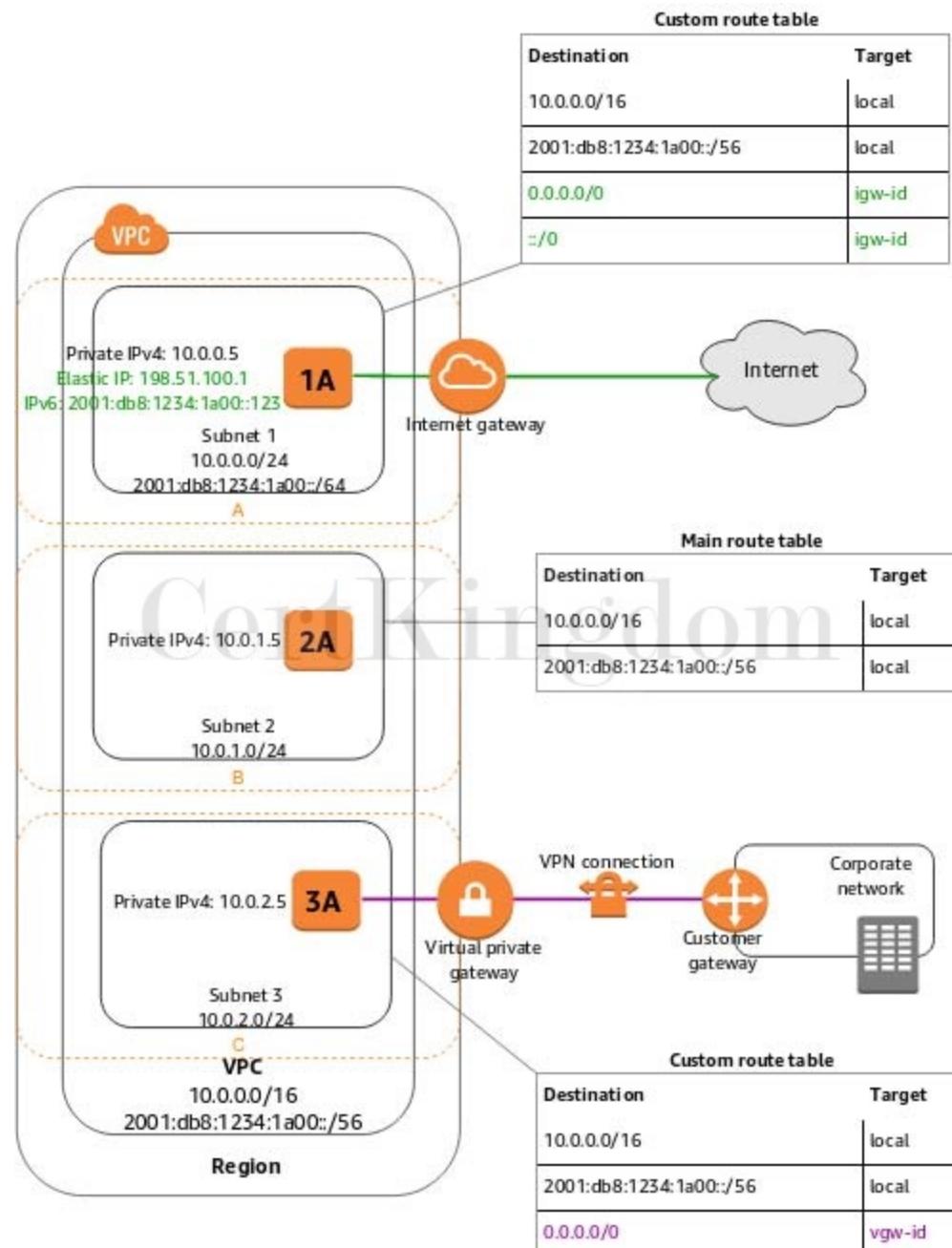
- A. Every subnet that you create is automatically associated with the main route table for the VPC.
- B. The allowed block size in VPC is between a netmask (65,536 IP addresses) and netmask (32 IP addresses).
- C. Each subnet spans to 2 Availability Zones.
- D. Each subnet maps to a single Availability Zone.

E. EC2 instances in a private subnet can communicate with the Internet only if they have an Elastic IP.

Answer: A,D

Explanation:

A VPC spans all the Availability Zones in the region. After creating a VPC, you can add one or more subnets in each Availability Zone. When you create a subnet, you specify the CIDR block for the subnet, which is a subset of the VPC CIDR block. Each subnet must reside entirely within one Availability Zone and cannot span zones. Availability Zones are distinct locations that are engineered to be isolated from failures in other Availability Zones. By launching instances in separate Availability Zones, you can protect your applications from the failure of a single location.



Below are the important points you have to remember about subnets:

- Each subnet maps to a single Availability Zone.
- Every subnet that you create is automatically associated with the main route table for the VPC.
- If a subnet's traffic is routed to an Internet gateway, the subnet is known as a public subnet.

The option that says: EC2 instances in a private subnet can communicate with the Internet only if they have an Elastic IP is incorrect. EC2 instances in a private subnet can communicate with the Internet not just by having an Elastic IP, but also with a public IP address via a NAT Instance or a NAT Gateway.

Take note that there is a distinction between private and public IP addresses. To enable communication

with the Internet, a public IPv4 address is mapped to the primary private IPv4 address through network address translation (NAT).

The option that says: The allowed block size in VPC is between a netmask (65,536 IP addresses) and netmask (32 IP addresses) is incorrect because the allowed block size in VPC is between a netmask (65,536 IP addresses) and netmask (16 IP addresses) and not netmask.

The option that says: Each subnet spans to 2 Availability Zones is incorrect because each subnet must reside entirely within one Availability Zone and cannot span zones.

References:

[https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Subnets.html](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html)

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ip-addressing.html>

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

---

## QUESTION 78

A company is generating confidential data that is saved on their on-premises data center. As a backup solution, the company wants to upload their data to an Amazon S3 bucket. In compliance with its internal security mandate, the encryption of the data must be done before sending it to Amazon S3. The company must spend time managing and rotating the encryption keys as well as controlling who can access those keys.

Which of the following methods can achieve this requirement? (Select TWO.)

- A. Set up Client-Side Encryption using a client-side master key.
- B. Set up Server-Side Encryption with keys stored in a separate S3 bucket.
- C. Set up Client-Side Encryption with Amazon S3 managed encryption keys.
- D. Set up Server-Side Encryption (SSE) with EC2 key pair.
- E. Set up Client-Side Encryption with a customer master key stored in AWS Key Management Service (AWS KMS).

Answer: A,E

Explanation:

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options for protecting data at rest in Amazon S3: Use Server-Side Encryption ““ You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

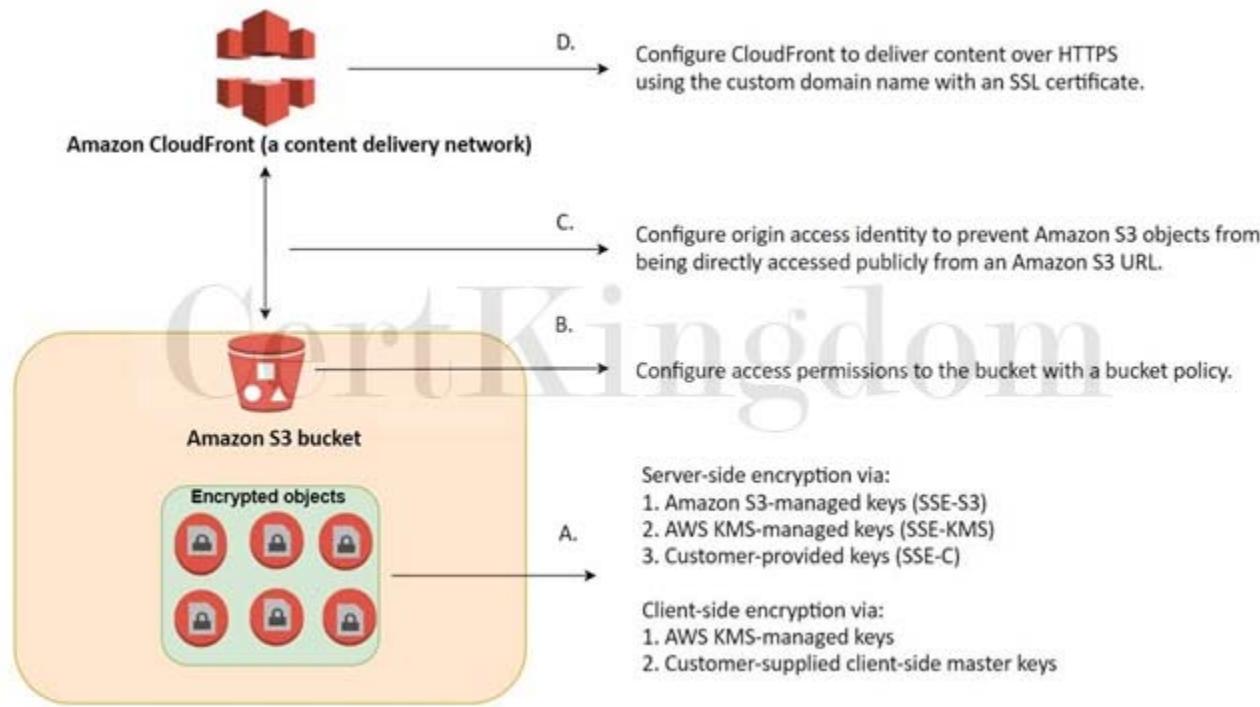
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Use Server-Side Encryption with Customer-Provided Keys (SSE-C)

Use Client-Side Encryption ““ You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Use Client-Side Encryption with AWS KMS’“Managed Customer Master Key (CMK)

Use Client-Side Encryption Using a Client-Side Master Key



Hence, the correct answers are:

- Set up Client-Side Encryption with a customer master key stored in AWS Key Management Service (AWS KMS).
- Set up Client-Side Encryption using a client-side master key.

The option that says: Set up Server-Side Encryption with keys stored in a separate S3 bucket is incorrect because you have to use AWS KMS to store your encryption keys or alternatively, choose an AWS-managed CMK instead to properly implement Server-Side Encryption in Amazon S3. In addition, storing any type of encryption key in Amazon S3 is actually a security risk and is not recommended.

The option that says: Set up Client-Side encryption with Amazon S3 managed encryption keys is incorrect because you can't have an Amazon S3 managed encryption key for client-side encryption. As its name implies, an Amazon S3 managed key is fully managed by AWS and also rotates the key automatically without any manual intervention. For this scenario, you have to set up a customer master key (CMK) in AWS KMS that you can manage, rotate, and audit or alternatively, use a client-side master key that you manually maintain.

The option that says: Set up Server-Side encryption (SSE) with EC2 key pair is incorrect because you can't use a key pair of your Amazon EC2 instance for encrypting your S3 bucket. You have to use a client-side master key or a customer master key stored in AWS KMS.

#### References:

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

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

## QUESTION 79

The media company that you are working for has a video transcoding application running on Amazon EC2. Each EC2 instance polls a queue to find out which video should be transcoded, and then runs a transcoding process. If this process is interrupted, the video will be transcoded by another instance based on the queuing system. This application has a large backlog of videos which need to be transcoded. Your manager would like to reduce this backlog by adding more EC2 instances, however, these instances are only needed until the backlog is reduced.

In this scenario, which type of Amazon EC2 instance is the most cost-effective type to use?

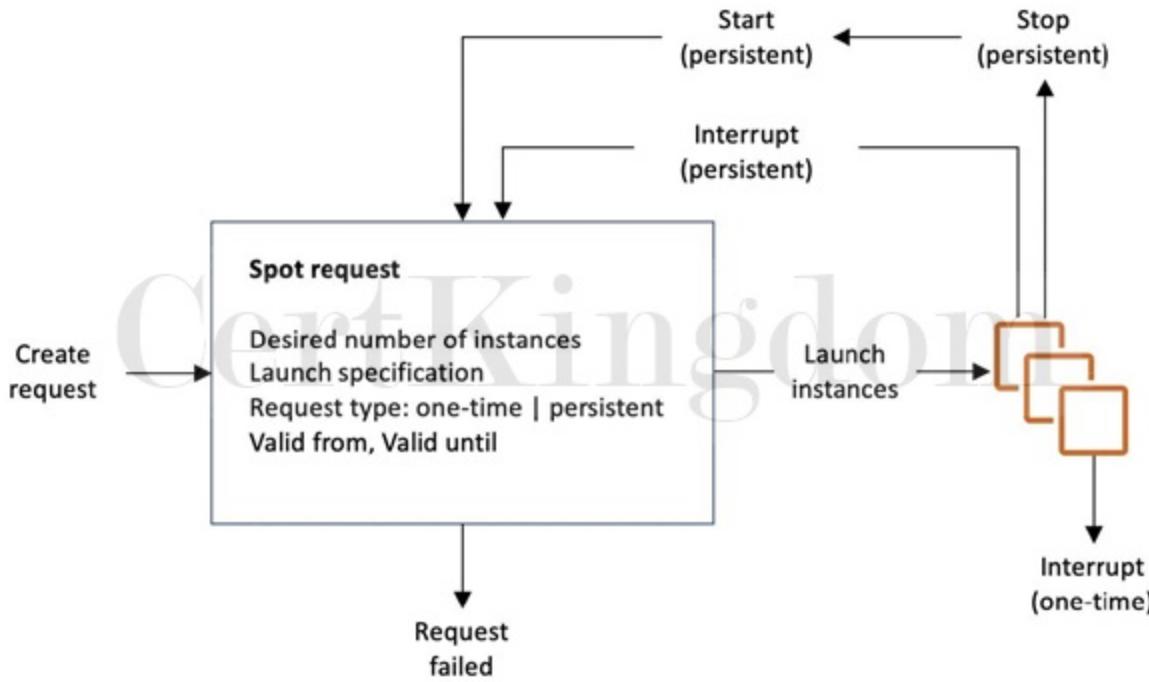
- Spot instances
- Reserved instances
- Dedicated instances

## D. On-demand instances

Answer: A

Explanation:

You require an instance that will be used not as a primary server but as a spare compute resource to augment the transcoding process of your application. These instances should also be terminated once the backlog has been significantly reduced. In addition, the scenario mentions that if the current process is interrupted, the video can be transcoded by another instance based on the queuing system. This means that the application can gracefully handle an unexpected termination of an EC2 instance, like in the event of a Spot instance termination when the Spot price is greater than your set maximum price. Hence, an Amazon EC2 Spot instance is the best and cost-effective option for this scenario.



Amazon EC2 Spot instances are spare compute capacity in the AWS cloud available to you at steep discounts compared to On-Demand prices. EC2 Spot enables you to optimize your costs on the AWS cloud and scale your application's throughput up to 10X for the same budget. By simply selecting Spot when launching EC2 instances, you can save up-to 90% on On-Demand prices. The only difference between On-Demand instances and Spot Instances is that Spot instances can be interrupted by EC2 with two minutes of notification when the EC2 needs the capacity back.

You can specify whether Amazon EC2 should hibernate, stop, or terminate Spot Instances when they are interrupted. You can choose the interruption behavior that meets your needs.

Take note that there is no "bid price" anymore for Spot EC2 instances since March 2018. You simply have to set your maximum price instead.

Reserved instances and Dedicated instances are incorrect as both do not act as spare compute capacity.

On-demand instances is a valid option but a Spot instance is much cheaper than On-Demand.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-interruptions.html>

[http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/how-spot-instances-work.html](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/how-spot-instances-work.html)

<https://aws.amazon.com/blogs/compute/new-amazon-ec2-spot-pricing>

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

## QUESTION 80

A Solutions Architect needs to set up a bastion host in the cheapest, most secure way. The Architect should be the only person that can access it via SSH.

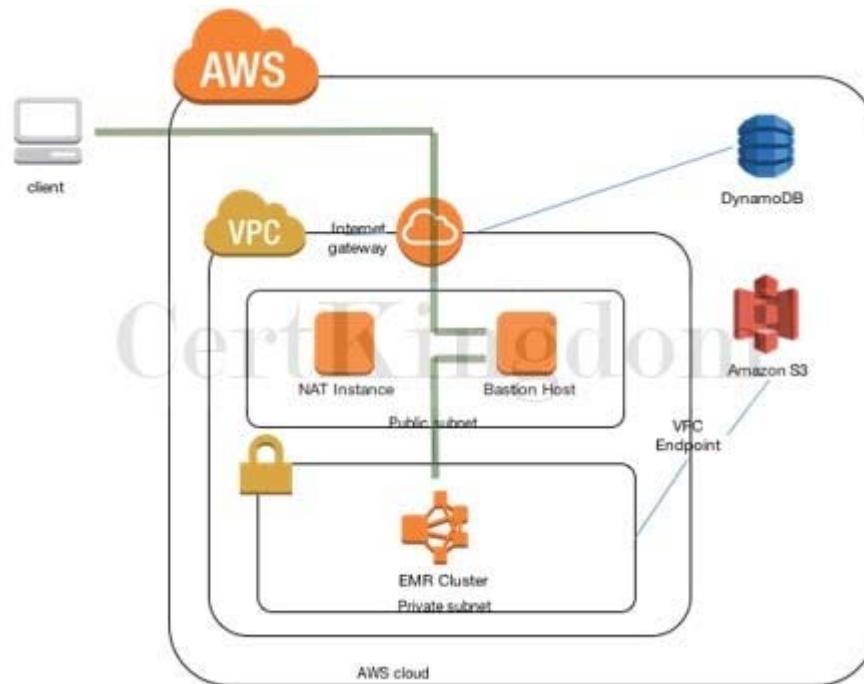
Which of the following steps would satisfy this requirement?

- A. Set up a small EC2 instance and a security group that only allows access on port 22 via your IP address
- B. Set up a small EC2 instance and a security group that only allows access on port 22
- C. Set up a large EC2 instance and a security group that only allows access on port 22 via your IP address
- D. Set up a large EC2 instance and a security group that only allows access on port 22

Answer: A

Explanation:

A bastion host is a server whose purpose is to provide access to a private network from an external network, such as the Internet. Because of its exposure to potential attack, a bastion host must minimize the chances of penetration.



To create a bastion host, you can create a new EC2 instance which should only have a security group from a particular IP address for maximum security. Since the cost is also considered in the question, you should choose a small instance for your host. By default, t2.micro instance is used by AWS but you can change these settings during deployment.

Setting up a large EC2 instance and a security group which only allows access on port 22 via your IP address is incorrect because you don't need to provision a large EC2 instance to run a single bastion host. At the same time, you are looking for the cheapest solution possible.

The options that say: Set up a large EC2 instance and a security group which only allows access on port 22 and Set up a small EC2 instance and a security group which only allows access on port 22 are both incorrect because you did not set your specific IP address to the security group rules, which possibly means that you publicly allow traffic from all sources in your security group. This is wrong as you should only be the one to have access to the bastion host.

References:

<https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html>

<https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-established-through-a-bastion-host/>

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

## QUESTION 81

A company has a web application that is relying entirely on slower disk-based databases, causing it to perform slowly. To improve its performance, the Solutions Architect integrated an in-memory data store to the web application using ElastiCache.

How does Amazon ElastiCache improve database performance?

- A. By caching database query results.
- B. It reduces the load on your database by routing read queries from your applications to the Read Replica.
- C. It securely delivers data to customers globally with low latency and high transfer speeds.
- D. It provides an in-memory cache that delivers up to 10x performance improvement from milliseconds to microseconds or even at millions of requests per second.

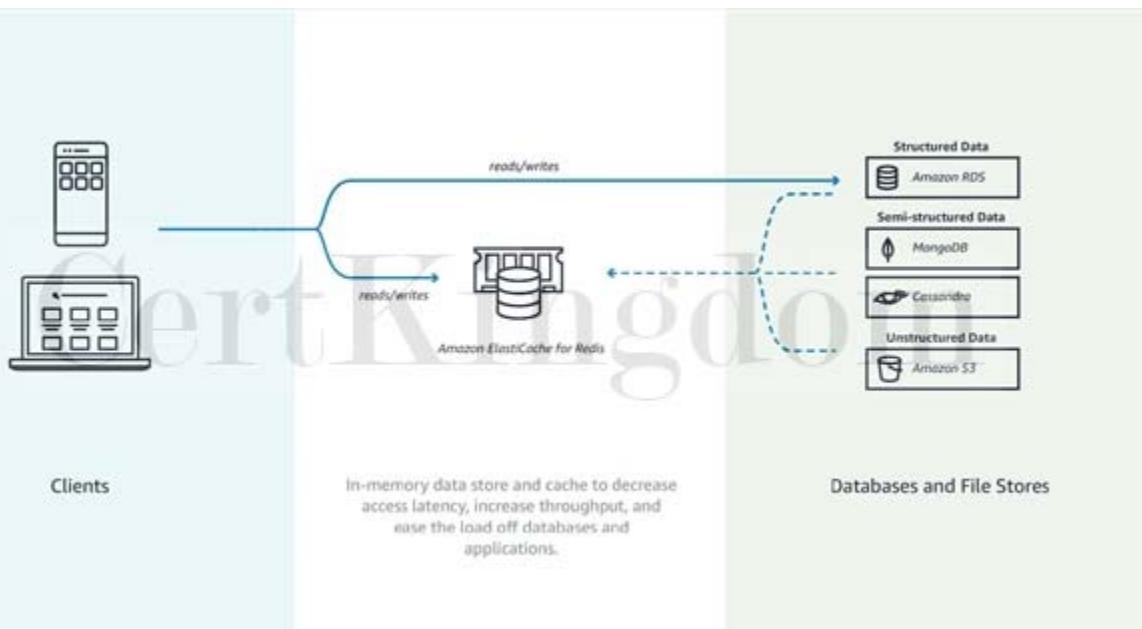
Answer: A

Explanation:

ElastiCache improves the performance of your database through caching query results.

The primary purpose of an in-memory key-value store is to provide ultra-fast (submillisecond latency) and inexpensive access to copies of data. Most data stores have areas of data that are frequently accessed but seldom updated. Additionally, querying a database is always slower and more expensive than locating a key in a key-value pair cache. Some database queries are especially expensive to perform, for example, queries that involve joins across multiple tables or queries with intensive calculations.

By caching such query results, you pay the price of the query once and then are able to quickly retrieve the data multiple times without having to re-execute the query.



The option that says: It securely delivers data to customers globally with low latency and high transfer speeds is incorrect because this option describes what CloudFront does and not ElastiCache.

The option that says: It provides an in-memory cache that delivers up to 10x performance improvement from milliseconds to microseconds or even at millions of requests per second is incorrect because this option describes what Amazon DynamoDB Accelerator (DAX) does and not ElastiCache. Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB. Amazon ElastiCache cannot provide a performance improvement from milliseconds to microseconds, let alone millions of requests per second like DAX can.

The option that says: It reduces the load on your database by routing read queries from your applications to the Read Replica is incorrect because this option describes what an RDS Read Replica does and not ElastiCache. Amazon RDS Read Replicas enable you to create one or more read-only copies of your database instance within the same AWS Region or in a different AWS Region.

References:

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

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

Check out this Amazon ElastiCache Cheat Sheet:

<https://tutorialsdojo.com/amazon-elasticache/>

---

## QUESTION 82

A production MySQL database hosted on Amazon RDS is running out of disk storage. The management has consulted its solutions architect to increase the disk space without impacting the database performance.

How can the solutions architect satisfy the requirement with the LEAST operational overhead?

- A. Modify the DB instance storage type to Provisioned IOPS.
- B. Increase the allocated storage for the DB instance.
- C. Change the default\_storage\_engine of the DB instance's parameter group to MyISAM.
- D. Modify the DB instance settings and enable storage autoscaling.

Answer: D

Explanation:

RDS Storage Auto Scaling automatically scales storage capacity in response to growing database workloads, with zero downtime.

Under-provisioning could result in application downtime, and over-provisioning could result in underutilized resources and higher costs. With RDS Storage Auto Scaling, you simply set your desired maximum storage limit, and Auto Scaling takes care of the rest.

RDS Storage Auto Scaling continuously monitors actual storage consumption, and scales capacity up automatically when actual utilization approaches provisioned storage capacity. Auto Scaling works with new and existing database instances. You can enable Auto Scaling with just a few clicks in the AWS Management Console. There is no additional cost for RDS Storage Auto Scaling. You pay only for the RDS resources needed to run your applications.

Hence, the correct answer is: Modify the DB instance settings and enable storage autoscaling.

The option that says: Increase the allocated storage for the DB instance is incorrect. Although this will solve the problem of low disk space, increasing the allocated storage might cause performance degradation during the change.

The option that says: Change the default\_storage\_engine of the DB instance's parameter group to MyISAM is incorrect. This is just a storage engine for MySQL. It won't increase the disk space in any way.

The option that says: Modify the DB instance storage type to Provisioned IOPS is incorrect. This may improve disk performance but it won't solve the problem of low database storage.

References:

<https://aws.amazon.com/about-aws/whats-new/06/rds-storage-auto-scaling/>

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_PIOPS.StorageTypes.html#USER\\_PIOPS.Autoscaling](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIOPS.StorageTypes.html#USER_PIOPS.Autoscaling)

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

---

## QUESTION 83

A tech startup is launching an on-demand food delivery platform using Amazon ECS cluster with an AWS Fargate serverless compute engine and Amazon Aurora. It is expected that the database read queries will significantly increase in the coming weeks ahead. A Solutions Architect recently launched two Read Replicas to the database cluster to improve the platform's scalability.

Which of the following is the MOST suitable configuration that the Architect should implement to load balance all of the incoming read requests equally to the two Read Replicas?

- A. Use the built-in Cluster endpoint of the Amazon Aurora database.

- B. Create a new Network Load Balancer to evenly distribute the read queries to the Read Replicas of the Amazon Aurora database.
- C. Use the built-in Reader endpoint of the Amazon Aurora database.
- D. Enable Amazon Aurora Parallel Query.

Answer: C

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 hostname 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.

Endpoint name	Status	Type	Port
Tutorials-Dojo-Tagaytay.cluster-cvkmnjhm7jiq.us-east-1.rds.amazonaws.com	Available	Writer	3306
Tutorials-Dojo-Tagaytay.cluster-ro-cvkmnjhm7jiq.us-east-1.rds.amazonaws.com	Available	Reader	3306

A reader endpoint for an Aurora DB cluster provides load-balancing support for read-only connections to the DB cluster. Use the reader endpoint for read operations, such as queries. By processing those statements on the read-only Aurora Replicas, this endpoint reduces the overhead on the primary instance. It also helps the cluster to scale the capacity to handle simultaneous SELECT queries, proportional to the number of Aurora Replicas in the cluster. Each Aurora DB cluster has one reader endpoint.

If the cluster contains one or more Aurora Replicas, the reader endpoint load-balances each connection request among the Aurora Replicas. In that case, you can only perform read-only statements such as SELECT in that session. If the cluster only contains a primary instance and no Aurora Replicas, the reader endpoint connects to the primary instance. In that case, you can perform write operations through the endpoint.

Hence, the correct answer is to use the built-in Reader endpoint of the Amazon Aurora database.

The option that says: Use the built-in Cluster endpoint of the Amazon Aurora database is incorrect because a cluster endpoint (also known as a writer endpoint) 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.

The option that says: Enable Amazon Aurora Parallel Query is incorrect because this feature simply enables Amazon Aurora to push down and distribute the computational load of a single query across thousands of CPUs in Aurora's storage layer. Take note that it does not load balance all of the incoming read requests equally to the two Read Replicas. With Parallel Query, query processing is pushed down

to the Aurora storage layer. The query gains a large amount of computing power, and it needs to transfer far less data over the network. In the meantime, the Aurora database instance can continue serving transactions with much less interruption. This way, you can run transactional and analytical workloads alongside each other in the same Aurora database, while maintaining high performance.

The option that says: Create a new Network Load Balancer to evenly distribute the read queries to the Read Replicas of the Amazon Aurora database is incorrect because a Network Load Balancer is not the suitable service/component to use for this requirement since an NLB is primarily used to distribute traffic to servers, not Read Replicas. You have to use the built-in Reader endpoint of the Amazon Aurora database instead.

References:

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

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

<https://aws.amazon.com/rds/aurora/parallel-query/>

Amazon Aurora Overview:

<https://youtu.be/iwS1h7rLNBQ>

Check out this Amazon Aurora Cheat Sheet:

<https://tutorialsdojo.com/amazon-aurora/>

---

## QUESTION 84

A company hosted a web application on a Linux Amazon EC2 instance in the public subnet that uses a default network ACL. The instance uses a default security group and has an attached Elastic IP address. The network ACL has been configured to block all traffic to the instance. The Solutions Architect must allow incoming traffic on port 443 to access the application from any source.

Which combination of steps will accomplish this requirement? (Select TWO.)

- A. In the Network ACL, update the rule to allow inbound TCP connection on port 443 from source 0.0.0.0/0 and outbound TCP connection on port 32768 - 65535 to destination 0.0.0.0/0
- B. In the Network ACL, update the rule to allow outbound TCP connection on port 32768 - 65535 to destination 0.0.0.0/0
- C. In the Security Group, create a new rule to allow TCP connection on port 443 to destination 0.0.0.0/0
- D. In the Network ACL, update the rule to allow both inbound and outbound TCP connection on port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0
- E. In the Security Group, add a new rule to allow TCP connection on port 443 from source 0.0.0.0/0

Answer: A,E

Explanation:

To enable the connection to a service running on an instance, the associated network ACL must allow both inbound traffic on the port that the service is listening on as well as allow outbound traffic from ephemeral ports. When a client connects to a server, a random port from the ephemeral port range (1024-65535) becomes the client's source port.

The designated ephemeral port then becomes the destination port for return traffic from the service, so outbound traffic from the ephemeral port must be allowed in the network ACL. By default, network ACLs allow all inbound and outbound traffic. If your network ACL is more restrictive, then you need to explicitly allow traffic from the ephemeral port range.

## acl-0f7a54f36f5c3a03f / Tutorials Dojo Network ACL - DAVAO

Actions ▾

**Details** Info

Network ACL ID  
acl-0f7a54f36f5c3a03f  
Owner  
8506121898

Default  
NoVPC ID  
vpc-23ad464a

Inbound rules

Outbound rules

Subnet associations

Tags

Outbound rules (3)

Edit outbound rules

Q Filter outbound rules

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
1	HTTPS (443)	TCP (6)	443	0.0.0.0/0	<input checked="" type="radio"/> Allow
2	Custom TCP	TCP (6)	32768 - 65535	0.0.0.0/0	<input checked="" type="radio"/> Allow
*	All traffic	All	All	0.0.0.0/0	<input type="radio"/> Deny

Ephemeral Ports

Tutorials Dojo

The client that initiates the request chooses the ephemeral port range. The range varies depending on the client's operating system.

- Many Linux kernels (including the Amazon Linux kernel) use ports 32768-61000.
- Requests originating from Elastic Load Balancing use ports 1024-65535.
- Windows operating systems through Windows Server 2003 use ports 1025-5000.
- Windows Server 2008 and later versions use ports 49152-65535.
- A NAT gateway uses ports 1024-65535.
- AWS Lambda functions use ports 1024-65535.

For example, if a request comes into a web server in your VPC from a Windows 10 client on the Internet, your network ACL must have an outbound rule to enable traffic destined for ports 49152 - 65535. If an instance in your VPC is the client initiating a request, your network ACL must have an inbound rule to enable traffic destined for the ephemeral ports specific to the type of instance (Amazon Linux, Windows Server 2008, and so on).

In this scenario, you only need to allow the incoming traffic on port 443. Since security groups are stateful, you can apply any changes to an incoming rule and it will be automatically applied to the outgoing rule.

To enable the connection to a service running on an instance, the associated network ACL must allow both inbound traffic on the port that the service is listening on as well as allow outbound traffic from ephemeral ports. When a client connects to a server, a random port from the ephemeral port range (32768 - 65535) becomes the client's source port.

Hence, the correct answers are:

- In the Security Group, add a new rule to allow TCP connection on port 443 from source 0.0.0.0/0.
- In the Network ACL, update the rule to allow inbound TCP connection on port 443 from source 0.0.0.0/0 and outbound TCP connection on port 32768 - 65535 to destination 0.0.0.0/0.

The option that says: In the Security Group, create a new rule to allow TCP connection on port 443 to destination 0.0.0.0/0 is incorrect because this step just allows outbound connections from the EC2 instance out to the public Internet which is unnecessary. Remember that a default security group already includes an outbound rule that allows all outbound traffic.

The option that says: In the Network ACL, update the rule to allow both inbound and outbound TCP connection on port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0 is incorrect because your network ACL must have an outbound rule to allow ephemeral ports (32768 - 65535). These are the specific ports that will be used as the client's source port for the traffic response.

The option that says: In the Network ACL, update the rule to allow outbound TCP connection on port 32768 - 65535 to destination 0.0.0.0/0 is incorrect because this step is just partially right. You still need to add an inbound rule from port 443 and not just the outbound rule for the ephemeral ports (32768 - 65535).

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/connect-http-https-ec2/>

[https://docs.amazonaws.cn/en\\_us/vpc/latest/userguide/vpc-network-acls.html#nacl-ephemeral-ports](https://docs.amazonaws.cn/en_us/vpc/latest/userguide/vpc-network-acls.html#nacl-ephemeral-ports)

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

---

### QUESTION 85

An online stocks trading application that stores financial data in an S3 bucket has a lifecycle policy that moves older data to Glacier every month. There is a strict compliance requirement where a surprise audit can happen at anytime and you should be able to retrieve the required data in under 15 minutes under all circumstances. Your manager instructed you to ensure that retrieval capacity is available when you need it and should handle up to 150 MB/s of retrieval throughput.

Which of the following should you do to meet the above requirement? (Select TWO.)

- A. Specify a range, or portion, of the financial data archive to retrieve.
- B. Purchase provisioned retrieval capacity.
- C. Retrieve the data using Amazon Glacier Select.
- D. Use Expedited Retrieval to access the financial data.
- E. Use Bulk Retrieval to access the financial data.

Answer: B,D

Explanation:

Expedited retrievals allow you to quickly access your data when occasional urgent requests for a subset of archives are required. For all but the largest archives (250 MB+), data accessed using Expedited retrievals are typically made available within 1–5 minutes. Provisioned Capacity ensures that retrieval capacity for Expedited retrievals is available when you need it.

To make an Expedited, Standard, or Bulk retrieval, set the Tier parameter in the Initiate Job (POST jobs) REST API request to the option you want, or the equivalent in the AWS CLI or AWS SDKs. If you have purchased provisioned capacity, then all expedited retrievals are automatically served through your provisioned capacity.

Provisioned capacity ensures that your retrieval capacity for expedited retrievals is available when you need it. Each unit of capacity provides that at least three expedited retrievals can be performed every five minutes and provides up to 150 MB/s of retrieval throughput. You should purchase provisioned retrieval capacity if your workload requires highly reliable and predictable access to a subset of your data in minutes. Without provisioned capacity Expedited retrievals are accepted, except for rare situations of unusually high demand. However, if you require access to Expedited retrievals under all circumstances, you must purchase provisioned retrieval capacity.



Retrieving the data using Amazon Glacier Select is incorrect because this is not an archive retrieval

option and is primarily used to perform filtering operations using simple Structured Query Language (SQL) statements directly on your data archive in Glacier.

Using Bulk Retrieval to access the financial data is incorrect because bulk retrievals typically complete within 5~12 hours hence, this does not satisfy the requirement of retrieving the data within 15 minutes. The provisioned capacity option is also not compatible with Bulk retrievals.

Specifying a range, or portion, of the financial data archive to retrieve is incorrect because using ranged archive retrievals is not enough to meet the requirement of retrieving the whole archive in the given timeframe. In addition, it does not provide additional retrieval capacity which is what the provisioned capacity option can offer.

References:

<https://docs.aws.amazon.com/amazonglacier/latest/dev/downloading-an-archive-two-steps.html>

<https://docs.aws.amazon.com/amazonglacier/latest/dev/glacier-select.html>

Check out this Amazon S3 Glacier Cheat Sheet:

<https://tutorialsdojo.com/amazon-glacier/>

---

## QUESTION 86

A company has a global online trading platform in which the users from all over the world regularly upload terabytes of transactional data to a centralized S3 bucket.

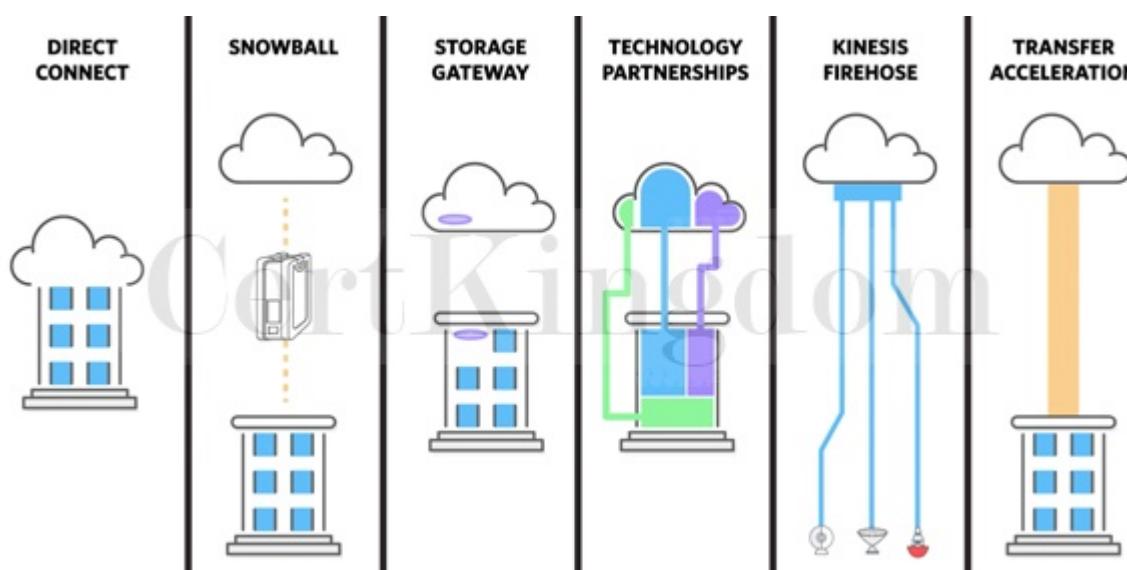
What AWS feature should you use in your present system to improve throughput and ensure consistently fast data transfer to the Amazon S3 bucket, regardless of your user's location?

- A. AWS Direct Connect
- B. Use CloudFront Origin Access Identity
- C. Amazon S3 Transfer Acceleration
- D. FTP

Answer: C

Explanation:

Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket. Transfer Acceleration leverages Amazon CloudFront's globally distributed AWS Edge Locations. As data arrives at an AWS Edge Location, data is routed to your Amazon S3 bucket over an optimized network path.



FTP is incorrect because the File Transfer Protocol does not guarantee fast throughput and consistent, fast data transfer.

AWS Direct Connect is incorrect because you have users all around the world and not just on your on-premises data center. Direct Connect would be too costly and is definitely not suitable for this purpose.

Using CloudFront Origin Access Identity is incorrect because this is a feature which ensures that only CloudFront can serve S3 content. It does not increase throughput and ensure fast delivery of content to

your customers.

Reference:

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

S3 Transfer Acceleration vs Direct Connect vs VPN vs Snowball vs Snowmobile:

<https://tutorialsdojo.com/s3-transfer-acceleration-vs-direct-connect-vs-vpn-vs-snowball-vs-snowmobile/>

Comparison of AWS Services Cheat Sheets:

<https://tutorialsdojo.com/comparison-of-aws-services/>

---

## QUESTION 87

A company is using multiple AWS accounts that are consolidated using AWS Organizations. They want to copy several S3 objects to another S3 bucket that belonged to a different AWS account which they also own. The Solutions Architect was instructed to set up the necessary permissions for this task and to ensure that the destination account owns the copied objects and not the account it was sent from.

How can the Architect accomplish this requirement?

- A. Connect the two S3 buckets from two different AWS accounts to Amazon WorkDocs. Set up crossaccount access to integrate the two S3 buckets. Use the Amazon WorkDocs console to copy the objects from one account to the other with modified object ownership assigned to the destination account.
- B. Configure cross-account permissions in S3 by creating an IAM customer-managed policy that allows an IAM user or role to copy objects from the source bucket in one account to the destination bucket in the other account. Then attach the policy to the IAM user or role that you want to use to copy objects between accounts.
- C. Enable the Requester Pays feature in the source S3 bucket. The fees would be waived through Consolidated Billing since both AWS accounts are part of AWS Organizations.
- D. Set up cross-origin resource sharing (CORS) in S3 by creating a bucket policy that allows an IAM user or role to copy objects from the source bucket in one account to the destination bucket in the other account.

Answer: B

Explanation:

By default, an S3 object is owned by the account that uploaded the object. That's why granting the destination account the permissions to perform the cross-account copy makes sure that the destination owns the copied objects. You can also change the ownership of an object by changing its access control list (ACL) to bucket-owner-full-control.

However, object ACLs can be difficult to manage for multiple objects, so it's a best practice to grant programmatic cross-account permissions to the destination account. Object ownership is important for managing permissions using a bucket policy. For a bucket policy to apply to an object in the bucket, the object must be owned by the account that owns the bucket. You can also manage object permissions using the object's ACL. However, object ACLs can be difficult to manage for multiple objects, so it's best practice to use the bucket policy as a centralized method for setting permissions.

## Bucket ARN

arn:aws:s3:::tutorialsdojo-media

## Policy

```
1 {  
2   "Version": "2008-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "PublicReadGetObject",  
6       "Effect": "Allow",  
7       "Principal": "*",  
8       "Action": "s3:GetObject",  
9       "Resource": "arn:aws:s3:::tutorialsdojo-media/*"  
10      }  
11    ]  
12  }  
13
```

To be sure that a destination account owns an S3 object copied from another account, grant the destination account the permissions to perform the cross-account copy. Follow these steps to configure cross-account permissions to copy objects from a source bucket in Account A to a destination bucket in Account B:

- Attach a bucket policy to the source bucket in Account A.
- Attach an AWS Identity and Access Management (IAM) policy to a user or role in Account B.
- Use the IAM user or role in Account B to perform the cross-account copy.

Hence, the correct answer is: Configure cross-account permissions in S3 by creating an IAM customermanaged policy that allows an IAM user or role to copy objects from the source bucket in one account to the destination bucket in the other account. Then attach the policy to the IAM user or role that you want to use to copy objects between accounts.

The option that says: Enable the Requester Pays feature in the source S3 bucket. The fees would be waived through Consolidated Billing since both AWS accounts are part of AWS Organizations is incorrect because the Requester Pays feature is primarily used if you want the requester, instead of the bucket owner, to pay the cost of the data transfer request and download from the S3 bucket. This solution lacks the necessary IAM Permissions to satisfy the requirement. The most suitable solution here is to configure cross-account permissions in S3.

The option that says: Set up cross-origin resource sharing (CORS) in S3 by creating a bucket policy that allows an IAM user or role to copy objects from the source bucket in one account to the destination bucket in the other account is incorrect because CORS simply defines a way for client web applications that are loaded in one domain to interact with resources in a different domain, and not on a different AWS account.

The option that says: Connect the two S3 buckets from two different AWS accounts to Amazon WorkDocs. Set up cross-account access to integrate the two S3 buckets. Use the Amazon WorkDocs console to copy the objects from one account to the other with modified object ownership assigned to the destination account is incorrect because Amazon WorkDocs is commonly used to easily collaborate, share content, provide rich feedback, and collaboratively edit documents with other users. There is no direct way for you to integrate WorkDocs and an Amazon S3 bucket owned by a different AWS account. A better solution here is to use cross-account permissions in S3 to meet the requirement.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroughs-managing-access-example2.html>

<https://aws.amazon.com/premiumsupport/knowledge-center/copy-s3-objects-account/>

<https://aws.amazon.com/premiumsupport/knowledge-center/cross-account-access-s3/>

## QUESTION 88

A media company is setting up an ECS batch architecture for its image processing application. It will be hosted in an Amazon ECS Cluster with two ECS tasks that will handle image uploads from the users and image processing. The first ECS task will process the user requests, store the image in an S3 input bucket, and push a message to a queue. The second task reads from the queue, parses the message containing the object name, and then downloads the object. Once the image is processed and transformed, it will upload the objects to the S3 output bucket. To complete the architecture, the Solutions Architect must create a queue and the necessary IAM permissions for the ECS tasks. Which of the following should the Architect do next?

- A. Launch a new Amazon AppStream 2.0 queue and configure the second ECS task to read from it. Create an IAM role that the ECS tasks can assume in order to get access to the S3 buckets and AppStream 2.0 queue. Declare the IAM Role (taskRoleArn) in the task definition.
- B. Launch a new Amazon Kinesis Data Firehose and configure the second ECS task to read from it. Create an IAM role that the ECS tasks can assume in order to get access to the S3 buckets and Kinesis Data Firehose. Specify the ARN of the IAM Role in the (taskDefinitionArn) field of the task definition.
- C. Launch a new Amazon SQS queue and configure the second ECS task to read from it. Create an IAM role that the ECS tasks can assume in order to get access to the S3 buckets and SQS queue. Declare the IAM Role (taskRoleArn) in the task definition.
- D. Launch a new Amazon MQ queue and configure the second ECS task to read from it. Create an IAM role that the ECS tasks can assume in order to get access to the S3 buckets and Amazon MQ queue. Set the (EnableTaskIAMRole) option to true in the task definition.

Answer: C

Explanation:

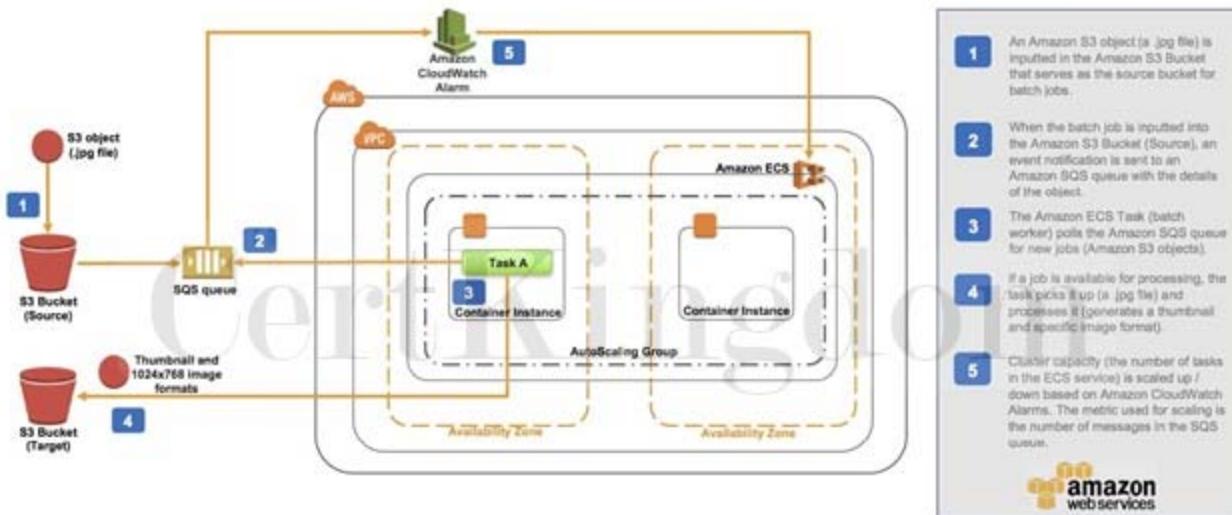
Docker containers are particularly suited for batch job workloads. Batch jobs are often short-lived and embarrassingly parallel. You can package your batch processing application into a Docker image so that you can deploy it anywhere, such as in an Amazon ECS task.

Amazon ECS supports batch jobs. You can use Amazon ECS Run Task action to run one or more tasks once. The Run Task action starts the ECS task on an instance that meets the task's requirements including CPU, memory, and ports.

## Amazon ECS Batch Processing

Build a batch processing framework to automate your batch jobs

This diagram shows how to use Amazon S3, Amazon SQS, and Amazon ECS to build an automated batch processing framework.



## AWS Reference Architectures

For example, you can set up an ECS Batch architecture for an image processing application. You can set up an AWS CloudFormation template that creates an Amazon S3 bucket, an Amazon SQS queue, an Amazon CloudWatch alarm, an ECS cluster, and an ECS task definition. Objects uploaded to the input S3 bucket trigger an event that sends object details to the SQS queue. The ECS task deploys a Docker container that reads from that queue, parses the message containing the object name and then downloads the object. Once transformed it will upload the objects to the S3 output bucket.

By using the SQS queue as the location for all object details, you can take advantage of its scalability and reliability as the queue will automatically scale based on the incoming messages and message retention can be configured. The ECS Cluster will then be able to scale services up or down based on the number of messages in the queue.

You have to create an IAM Role that the ECS task assumes in order to get access to the S3 buckets and SQS queue. Note that the permissions of the IAM role don't specify the S3 bucket ARN for the incoming bucket. This is to avoid a circular dependency issue in the CloudFormation template. You should always make sure to assign the least amount of privileges needed to an IAM role.

Hence, the correct answer is: Launch a new Amazon SQS queue and configure the second ECS task to read from it. Create an IAM role that the ECS tasks can assume in order to get access to the S3 buckets and SQS queue. Declare the IAM Role (taskRoleArn) in the task definition.

The option that says: Launch a new Amazon AppStream 2.0 queue and configure the second ECS task to read from it. Create an IAM role that the ECS tasks can assume in order to get access to the S3 buckets and AppStream 2.0 queue. Declare the IAM Role (taskRoleArn) in the task definition is incorrect because Amazon AppStream 2.0 is a fully managed application streaming service and can't be used as a queue. You have to use Amazon SQS instead.

The option that says: Launch a new Amazon Kinesis Data Firehose and configure the second ECS task to read from it. Create an IAM role that the ECS tasks can assume in order to get access to the S3 buckets and Kinesis Data Firehose. Specify the ARN of the IAM Role in the (taskDefinitionArn) field of the task definition is incorrect because Amazon Kinesis Data Firehose is a fully managed service for delivering real-time streaming data. Although it can stream data to an S3 bucket, it is not suitable to be used as a queue for a batch application in this scenario. In addition, the ARN of the IAM Role should be declared in the taskRoleArn and not in the taskDefinitionArn field.

The option that says: Launch a new Amazon MQ queue and configure the second ECS task to read from it. Create an IAM role that the ECS tasks can assume in order to get access to the S3 buckets and Amazon MQ queue. Set the (EnableTaskIAMRole) option to true in the task definition is incorrect because Amazon MQ is primarily used as a managed message broker service and not a queue. The EnableTaskIAMRole option is only applicable for Windows-based ECS Tasks that require extra configuration.

References:

<https://github.com/aws-samples/ecs-refarch-batch-processing>

[https://docs.aws.amazon.com/AmazonECS/latest/developerguide/common\\_use\\_cases.html](https://docs.aws.amazon.com/AmazonECS/latest/developerguide/common_use_cases.html)

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

## QUESTION 89

A Solutions Architect is working for an online hotel booking firm with terabytes of customer data coming from the websites and applications. There is an annual corporate meeting where the Architect needs to present the booking behavior and acquire new insights from the customers' data. The Architect is looking for a service to perform super-fast analytics on massive data sets in near real-time.

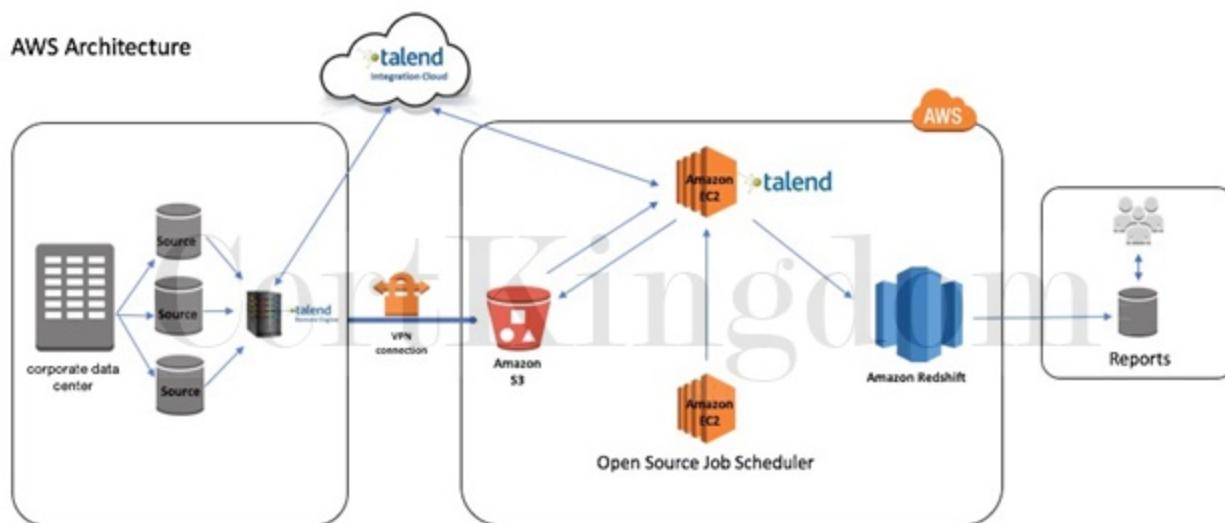
Which of the following services gives the Architect the ability to store huge amounts of data and perform quick and flexible queries on it?

- A. Amazon RDS
- B. Amazon DynamoDB
- C. Amazon Redshift
- D. Amazon ElastiCache

Answer: C

Explanation:

Amazon Redshift is a fast, scalable data warehouse that makes it simple and cost-effective to analyze all your data across your data warehouse and data lake. Redshift delivers ten times faster performance than other data warehouses by using machine learning, massively parallel query execution, and columnar storage on high-performance disk.



You can use Redshift to analyze all your data using standard SQL and your existing Business Intelligence (BI) tools. It also allows you to run complex analytic queries against terabytes to petabytes of structured and semi-structured data, using sophisticated query optimization, columnar storage on high-performance storage, and massively parallel query execution.

Hence, the correct answer is: Amazon Redshift.

Amazon DynamoDB is incorrect. DynamoDB is a NoSQL database which is based on key-value pairs

used for fast processing of small data that dynamically grows and changes. But if you need to scan large amounts of data (ie a lot of keys all in one query), the performance will not be optimal.

Amazon ElastiCache is incorrect because this is used to increase the performance, speed, and redundancy with which applications can retrieve data by providing an in-memory database caching system, and not for database analytical processes.

Amazon RDS is incorrect because this is mainly used for On-Line Transaction Processing (OLTP) applications and not for Online Analytics Processing (OLAP).

References:

<https://docs.aws.amazon.com/redshift/latest/mgmt/welcome.html>

<https://docs.aws.amazon.com/redshift/latest/gsg/getting-started.html>

Amazon Redshift Overview:

<https://youtu.be/jILERNzhHOg>

Check out this Amazon Redshift Cheat Sheet:

<https://tutorialsdojo.com/amazon-redshift/>

## QUESTION 90

A company has a data analytics application that updates a real-time foreign exchange dashboard and another separate application that archives data to Amazon Redshift. Both applications are configured to consume data from the same stream concurrently and independently by using Amazon Kinesis Data Streams. However, they noticed that there are a lot of occurrences where a shard iterator expires unexpectedly. Upon checking, they found out that the DynamoDB table used by Kinesis does not have enough capacity to store the lease data.

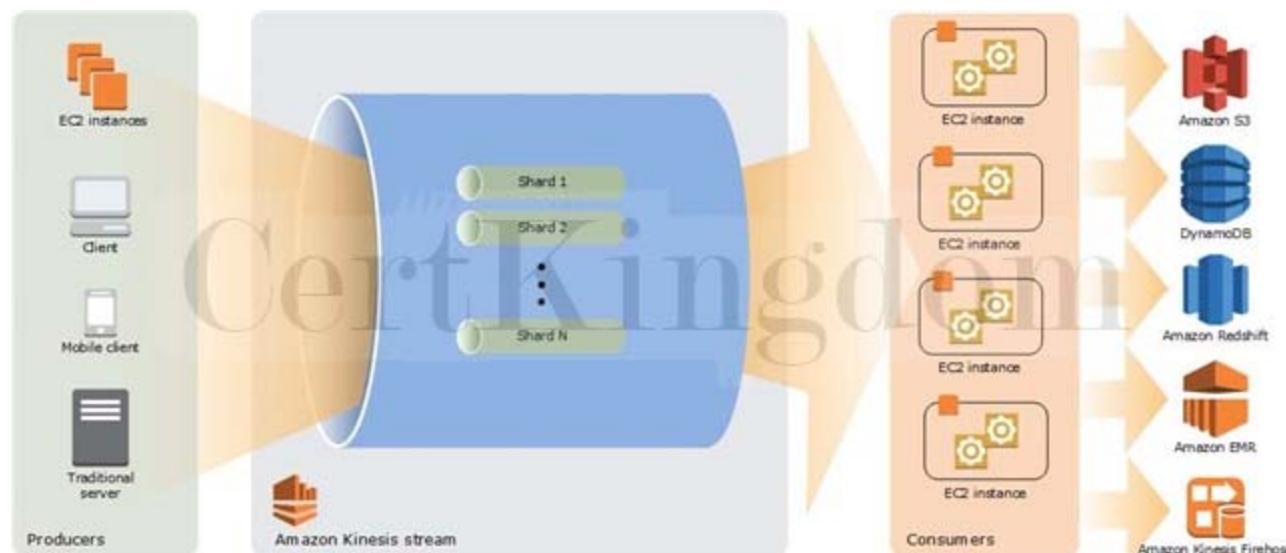
Which of the following is the most suitable solution to rectify this issue?

- A. Upgrade the storage capacity of the DynamoDB table.
- B. Use Amazon Kinesis Data Analytics to properly support the data analytics application instead of Kinesis Data Stream.
- C. Increase the write capacity assigned to the shard table.
- D. Enable In-Memory Acceleration with DynamoDB Accelerator (DAX).

Answer: C

Explanation:

A new shard iterator is returned by every GetRecords request (as NextShardIterator), which you then use in the next GetRecords request (as ShardIterator). Typically, this shard iterator does not expire before you use it. However, you may find that shard iterators expire because you have not called GetRecords for more than 5 minutes or because you've performed a restart of your consumer application.



If the shard iterator expires immediately before you can use it, this might indicate that the DynamoDB

table used by Kinesis does not have enough capacity to store the lease data. This situation is more likely to happen if you have a large number of shards. To solve this problem, increase the write capacity assigned to the shard table.

Hence, increasing the write capacity assigned to the shard table is the correct answer.

Upgrading the storage capacity of the DynamoDB table is incorrect because DynamoDB is a fully managed service that automatically scales its storage without setting it up manually. The scenario refers to the write capacity of the shard table as it says that the DynamoDB table used by Kinesis does not have enough capacity to store the lease data.

Enabling In-Memory Acceleration with DynamoDB Accelerator (DAX) is incorrect because the DAX feature is primarily used for read performance improvement of your DynamoDB table from milliseconds response time to microseconds. It does not have any relationship with Amazon Kinesis Data Stream in this scenario.

Using Amazon Kinesis Data Analytics to properly support the data analytics application instead of Kinesis Data Stream is incorrect. Although Amazon Kinesis Data Analytics can support a data analytics application, it is still not a suitable solution for this issue. You simply need to increase the write capacity assigned to the shard table in order to rectify the problem, which is why switching to Amazon Kinesis Data Analytics is not necessary.

Reference:

<https://docs.aws.amazon.com/streams/latest/dev/kinesis-record-processor-ddb.html>

<https://docs.aws.amazon.com/streams/latest/dev/troubleshooting-consumers.html>

Check out this Amazon Kinesis Cheat Sheet:

<https://tutorialsdojo.com/amazon-kinesis/>

---

## QUESTION 91

An online events registration system is hosted in AWS and uses ECS to host its front-end tier and an RDS configured with Multi-AZ for its database tier. What are the events that will make Amazon RDS automatically perform a failover to the standby replica? (Select TWO.)

- A. In the event of Read Replica failure
- B. Storage failure on secondary DB instance
- C. Compute unit failure on secondary DB instance
- D. Storage failure on primary
- E. Loss of availability in primary Availability Zone

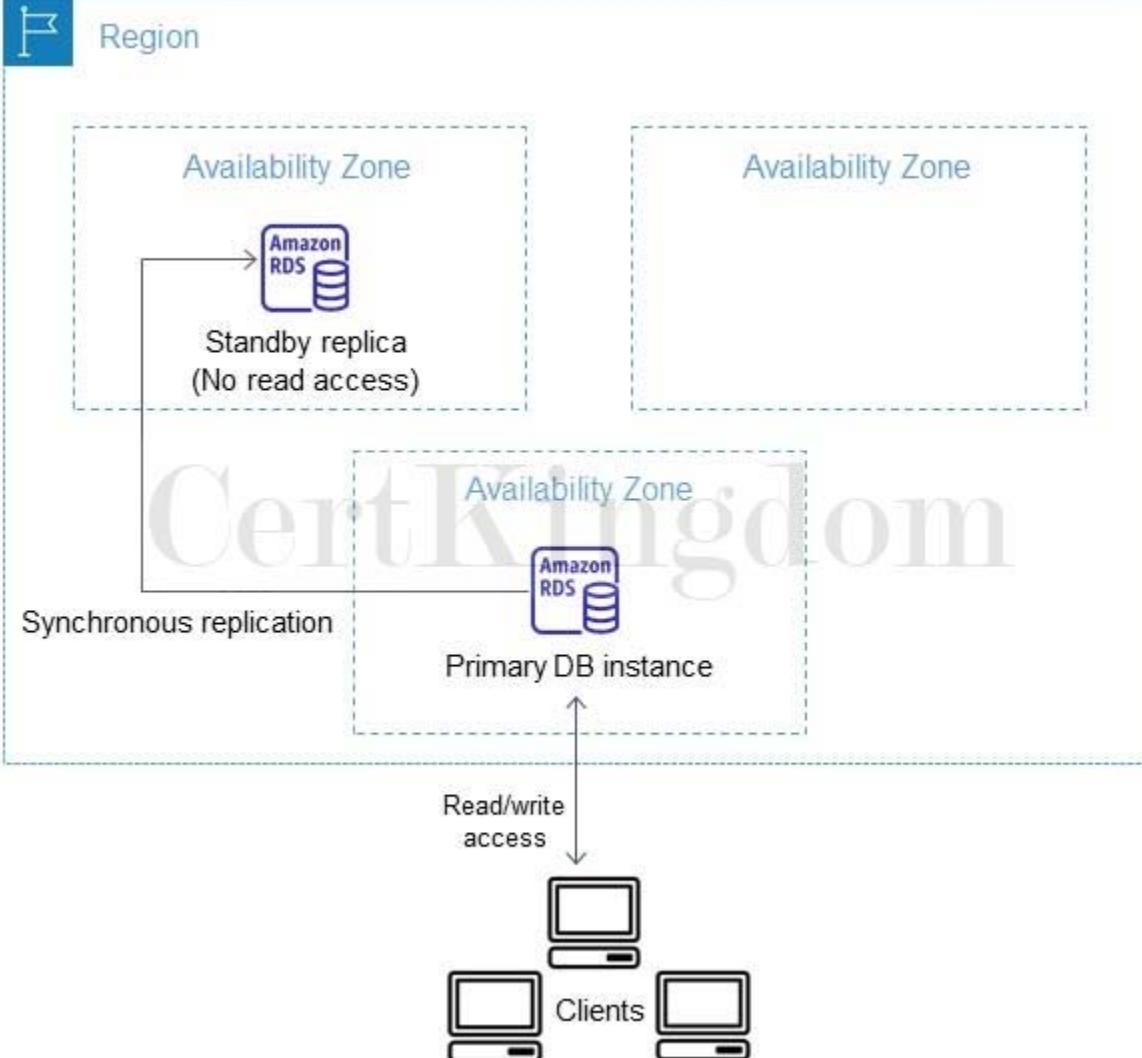
Answer: D,E

Explanation:

Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments. Amazon RDS uses several different technologies to provide failover support. Multi-AZ deployments for Oracle, PostgreSQL, MySQL, and MariaDB DB instances use Amazon's failover technology. SQL Server DB instances use SQL Server Database Mirroring (DBM).

In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance, and help protect your databases against DB instance failure and Availability Zone disruption.

Amazon RDS detects and automatically recovers from the most common failure scenarios for Multi-AZ deployments so that you can resume database operations as quickly as possible without administrative intervention.



The high-availability feature is not a scaling solution for read-only scenarios; you cannot use a standby replica to serve read traffic. To service read-only traffic, you should use a Read Replica.

Amazon RDS automatically performs a failover in the event of any of the following:

Loss of availability in primary Availability Zone.

Loss of network connectivity to primary.

Compute unit failure on primary.

Storage failure on primary.

Hence, the correct answers are:

- Loss of availability in primary Availability Zone

- Storage failure on primary

The following options are incorrect because all these scenarios do not affect the primary database.

Automatic failover only occurs if the primary database is the one that is affected.

- Storage failure on secondary DB instance

- In the event of Read Replica failure

- Compute unit failure on secondary DB instance

References:

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

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

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

## QUESTION 92

A company developed a web application and deployed it on a fleet of EC2 instances that uses Amazon SQS. The requests are saved as messages in the SQS queue, which is configured with the maximum message retention period. However, after thirteen days of operation, the web application suddenly

crashed and there are 10,000 unprocessed messages that are still waiting in the queue. Since they developed the application, they can easily resolve the issue but they need to send a communication to the users on the issue.

What information should they provide and what will happen to the unprocessed messages?

- A. Tell the users that the application will be operational shortly and all received requests will be processed after the web application is restarted.
- B. Tell the users that unfortunately, they have to resubmit all of the requests since the queue would not be able to process the 10,000 messages together.
- C. Tell the users that unfortunately, they have to resubmit all the requests again.
- D. Tell the users that the application will be operational shortly however, requests sent over three days ago will need to be resubmitted.

Answer: A

Explanation:

In Amazon SQS, you can configure the message retention period to a value from 1 minute to 14 days. The default is 4 days. Once the message retention limit is reached, your messages are automatically deleted.

A single Amazon SQS message queue can contain an unlimited number of messages. However, there is a 120,000 limit for the number of inflight messages for a standard queue and 20,000 for a FIFO queue. Messages are inflight after they have been received from the queue by a consuming component, but have not yet been deleted from the queue.

In this scenario, it is stated that the SQS queue is configured with the maximum message retention period. The maximum message retention in SQS is 14 days that is why the option that says: Tell the users that the application will be operational shortly and all received requests will be processed after the web application is restarted is the correct answer i.e. there will be no missing messages.

The options that say: Tell the users that unfortunately, they have to resubmit all the requests again and Tell the users that the application will be operational shortly, however, requests sent over three days ago will need to be resubmitted are incorrect as there are no missing messages in the queue thus, there is no need to resubmit any previous requests.

The option that says: Tell the users that unfortunately, they have to resubmit all of the requests since the queue would not be able to process the 10,000 messages together is incorrect as the queue can contain an unlimited number of messages, not just 10,000 messages.

Reference:

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

Check out this Amazon SQS Cheat Sheet:

<https://tutorialsdojo.com/amazon-sqs/>

---

## QUESTION 93

A company is hosting its web application in an Auto Scaling group of EC2 instances behind an Application Load Balancer. Recently, the Solutions Architect identified a series of SQL injection attempts and cross-site scripting attacks to the application, which had adversely affected their production data. Which of the following should the Architect implement to mitigate this kind of attack?

- A. Use Amazon GuardDuty to prevent any further SQL injection and cross-site scripting attacks in your application.
- B. Set up security rules that block SQL injection and cross-site scripting attacks in AWS Web Application Firewall (WAF). Associate the rules to the Application Load Balancer.
- C. Block all the IP addresses where the SQL injection and cross-site scripting attacks originated using the Network Access Control List.
- D. Using AWS Firewall Manager, set up security rules that block SQL injection and cross-site scripting attacks. Associate the rules to the Application Load Balancer.

Answer: B

## Explanation:

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer. AWS WAF also lets you control access to your content. Based on conditions that you specify, such as the IP addresses that requests originate from or the values of query strings, API Gateway, CloudFront or an Application Load Balancer responds to requests either with the requested content or with an HTTP 403 status code (Forbidden). You also can configure CloudFront to return a custom error page when a request is blocked.



At the simplest level, AWS WAF lets you choose one of the following behaviors:

Allow all requests except the ones that you specify ““ This is useful when you want CloudFront or an Application Load Balancer to serve content for a public website, but you also want to block requests from attackers.

Block all requests except the ones that you specify ““ This is useful when you want to serve content for a restricted website whose users are readily identifiable by properties in web requests, such as the IP addresses that they use to browse to the website.

Count the requests that match the properties that you specify ““ When you want to allow or block requests based on new properties in web requests, you first can configure AWS WAF to count the requests that match those properties without allowing or blocking those requests. This lets you confirm that you didn't accidentally configure AWS WAF to block all the traffic to your website. When you're confident that you specified the correct properties, you can change the behavior to allow or block requests.

Hence, the correct answer in this scenario is: Set up security rules that block SQL injection and crosssite scripting attacks in AWS Web Application Firewall (WAF). Associate the rules to the Application Load Balancer.

Using Amazon Guard?Duty to prevent any further SQL injection and cross-site scripting attacks in your application is incorrect because Amazon Guard?Duty is just a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. Using AWS Firewall Manager to set up security rules that block SQL injection and cross-site scripting attacks, then associating the rules to the Application Load Balancer is incorrect because AWS Firewall Manager just simplifies your AWS WAF and AWS Shield Advanced administration and maintenance tasks across multiple accounts and resources.

Blocking all the IP addresses where the SQL injection and cross-site scripting attacks originated using the Network Access Control List is incorrect because this 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. NACLs are not effective in blocking SQL injection and cross-site scripting attacks

References:

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

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

Check out this AWS WAF Cheat Sheet:

<https://tutorialsdojo.com/aws-waf/>

AWS Security Services Overview - WAF, Shield, CloudHSM, KMS:

<https://www.youtube.com/watch?v=-1S-RdeAmMo>

## QUESTION 94

A company is running a multi-tier web application farm in a virtual private cloud (VPC) that is not connected to their corporate network. They are connecting to the VPC over the Internet to manage the fleet of Amazon EC2 instances running in both the public and private subnets. The Solutions Architect has added a bastion host with Microsoft Remote Desktop Protocol (RDP) access to the application instance security groups, but the company wants to further limit administrative access to all of the instances in the VPC.

Which of the following bastion host deployment options will meet this requirement?

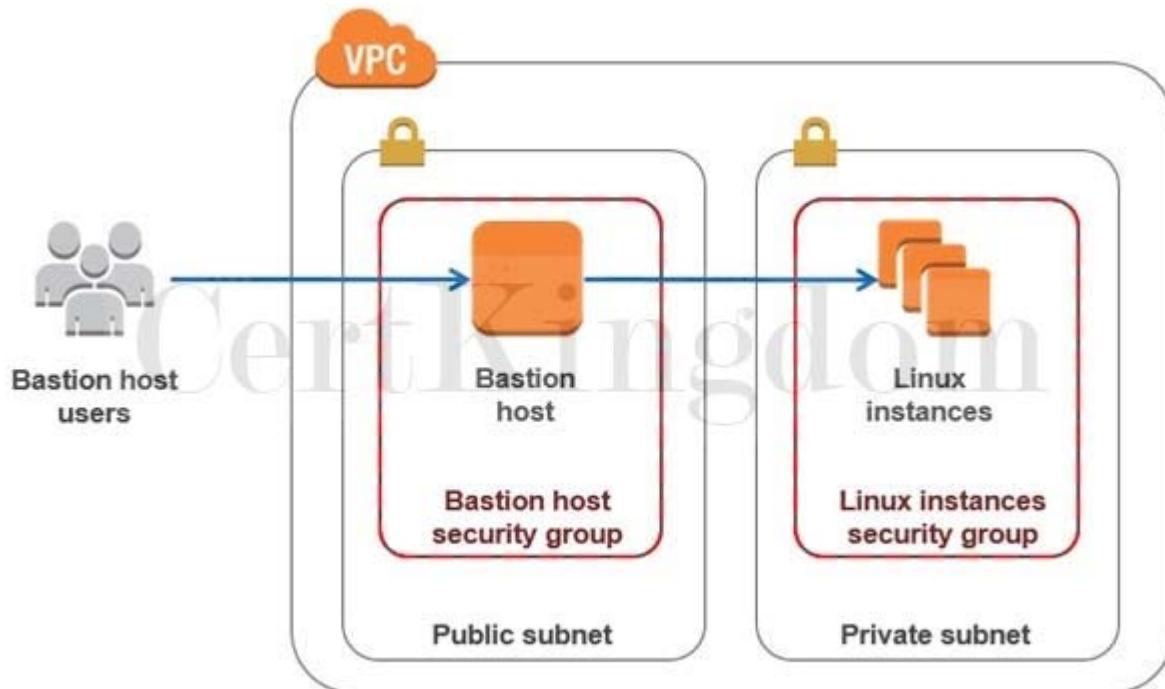
- A. Deploy a Windows Bastion host on the corporate network that has RDP access to all EC2 instances in the VPC.
- B. Deploy a Windows Bastion host with an Elastic IP address in the public subnet and allow RDP access to bastion only from the corporate IP addresses.
- C. Deploy a Windows Bastion host with an Elastic IP address in the private subnet, and restrict RDP access to the bastion from only the corporate public IP addresses.
- D. Deploy a Windows Bastion host with an Elastic IP address in the public subnet and allow SSH access to the bastion from anywhere.

Answer: B

Explanation:

The correct answer is to deploy a Windows Bastion host with an Elastic IP address in the public subnet and allow RDP access to bastion only from the corporate IP addresses.

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. If you have a bastion host in AWS, it is basically just an EC2 instance. It should be in a public subnet with either a public or Elastic IP address with sufficient RDP or SSH access defined in the security group. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets.



Deploying a Windows Bastion host on the corporate network that has RDP access to all EC2 instances in the VPC is incorrect since you do not deploy the Bastion host to your corporate network. It should be in the public subnet of a VPC.

Deploying a Windows Bastion host with an Elastic IP address in the private subnet, and restricting RDP access to the bastion from only the corporate public IP addresses is incorrect since it should be

deployed in a public subnet, not a private subnet.

Deploying a Windows Bastion host with an Elastic IP address in the public subnet and allowing SSH access to the bastion from anywhere is incorrect. Since it is a Windows bastion, you should allow RDP access and not SSH as this is mainly used for Linux-based systems.

Reference:

<https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html>

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

---

## QUESTION 95

A company has a serverless application made up of AWS Amplify, Amazon API Gateway and a Lambda function. The application is connected to an Amazon RDS MySQL database instance inside a private subnet. A Lambda Function URL is also implemented as the dedicated HTTPS endpoint for the function, which has the following value:

<https://june1898pillpinas.lambda-url.us-west-2.on.aws/>

There are times during peak loads when the database throws a too many connections' error preventing the users from accessing the application.

Which solution could the company take to resolve the issue?

- A. Increase the memory allocation of the Lambda function
- B. Provision an RDS Proxy between the Lambda function and RDS database instance
- C. Increase the concurrency limit of the Lambda function
- D. Increase the rate limit of API Gateway

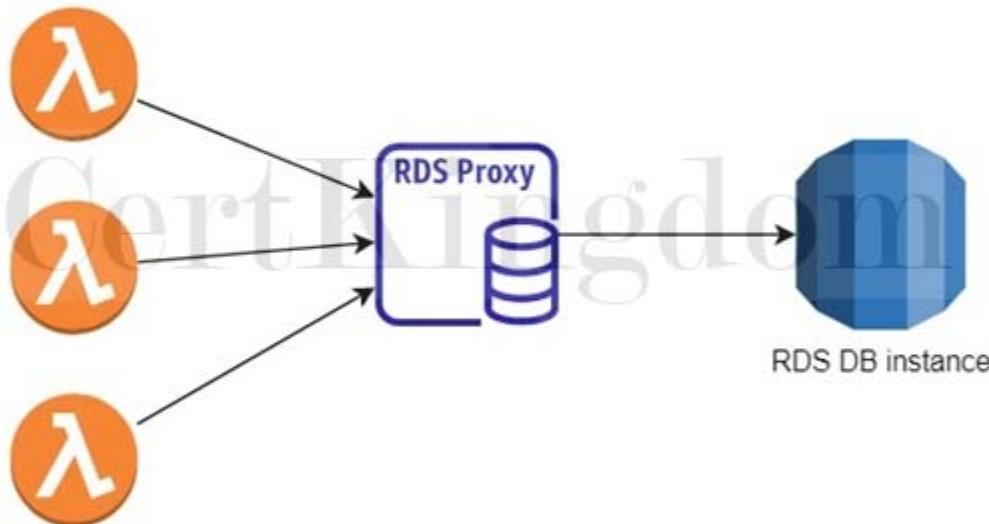
Answer: B

Explanation:

If a "Too Many Connections" error happens to a client connecting to a MySQL database, it means all available connections are in use by other clients. Opening a connection consumes resources on the database server. Since Lambda functions can scale to tens of thousands of concurrent connections, your database needs more resources to open and maintain connections instead of executing queries.

The maximum number of connections a database can support is largely determined by the amount of memory allocated to it. Upgrading to a database instance with higher memory is a straightforward way of solving the problem. Another approach would be to maintain a connection pool that clients can reuse.

This is where RDS Proxy comes in.



RDS Proxy helps you manage a large number of connections from Lambda to an RDS database by establishing a warm connection pool to the database. Your Lambda functions interact with RDS Proxy instead of your database instance. It handles the connection pooling necessary for scaling many simultaneous connections created by concurrent Lambda functions. This allows your Lambda applications to reuse existing connections, rather than creating new connections for every function invocation.

Thus, the correct answer is: Provision an RDS Proxy between the Lambda function and RDS database instance format

The option that says: Increase the concurrency limit of the Lambda function is incorrect. The concurrency limit refers to the maximum requests AWS Lambda can handle at the same time. Increasing the limit will allow for more requests to open a database connection, which could potentially worsen the problem.

The option that says: Increase the rate limit of API Gateway is incorrect. This won't fix the issue at all as all it does is increase the number of API requests a client can make.

The option that says: Increase the memory allocation of the Lambda function is incorrect. Increasing the Lambda function's memory would only make it run processes faster. It can help but it won't likely do any significant effect to get rid of the error. The "too many connections" error is a database-related issue.

Solutions that have to do with databases, like upgrading to a larger database instance or, in this case, creating a database connection pool using RDS Proxy have better chance of resolving the problem.

#### References:

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

<https://aws.amazon.com/blogs/compute/using-amazon-rds-proxy-with-aws-lambda/>

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

## QUESTION 96

A start-up company that offers an intuitive financial data analytics service has consulted you about their AWS architecture. They have a fleet of Amazon EC2 worker instances that process financial data and then outputs reports which are used by their clients. You must store the generated report files in a durable storage. The number of files to be stored can grow over time as the start-up company is expanding rapidly overseas and hence, they also need a way to distribute the reports faster to clients

located across the globe.

Which of the following is a cost-efficient and scalable storage option that you should use for this scenario?

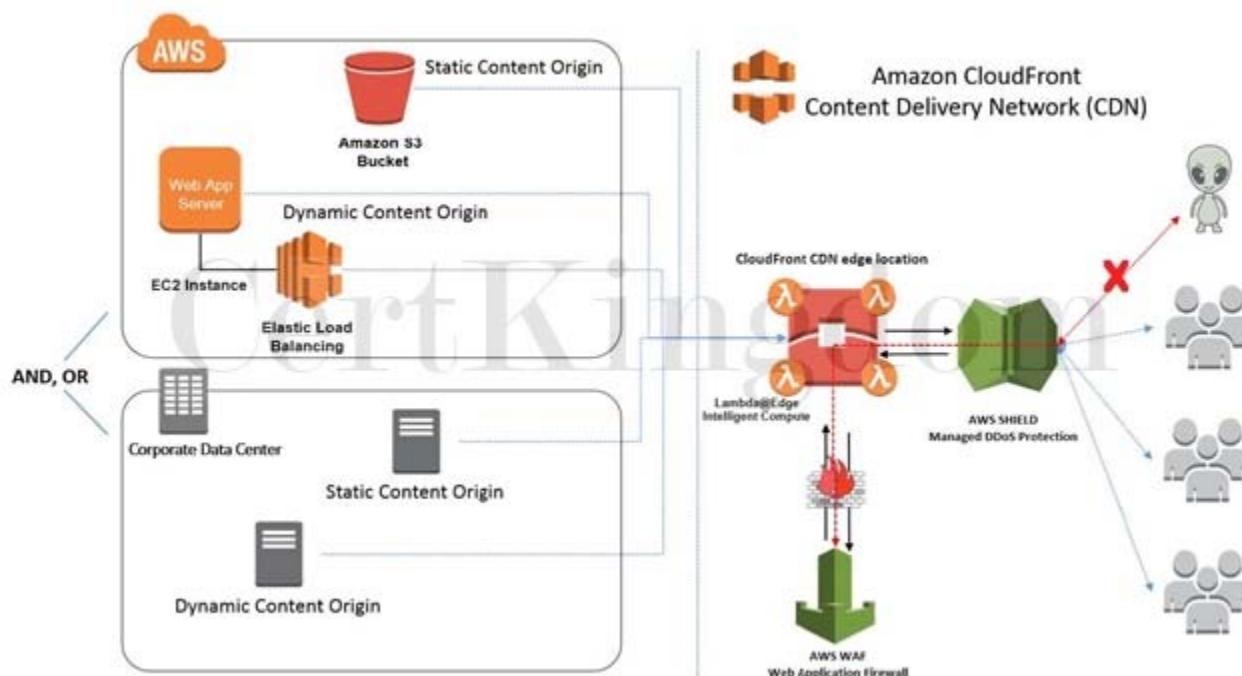
- A. Use multiple EC2 instance stores for data storage and ElastiCache as the CDN.
- B. Use Amazon S3 as the data storage and CloudFront as the CDN.
- C. Use Amazon Redshift as the data storage and CloudFront as the CDN.
- D. Use Amazon Glacier as the data storage and ElastiCache as the CDN.

Answer: B

Explanation:

A Content Delivery Network (CDN) is a critical component of nearly any modern web application. It used to be that CDN merely improved the delivery of content by replicating commonly requested files (static content) across a globally distributed set of caching servers. However, CDNs have become much more useful over time.

For caching, a CDN will reduce the load on an application origin and improve the experience of the requestor by delivering a local copy of the content from a nearby cache edge, or Point of Presence (PoP). The application origin is off the hook for opening the connection and delivering the content directly as the CDN takes care of the heavy lifting. The end result is that the application origins don't need to scale to meet demands for static content.



Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront is integrated with AWS “ both physical locations that are directly connected to the AWS global infrastructure, as well as other AWS services.

Amazon S3 offers a highly durable, scalable, and secure destination for backing up and archiving your critical data. This is the correct option as the start-up company is looking for a durable storage to store the audio and text files. In addition, ElastiCache is only used for caching and not specifically as a Global Content Delivery Network (CDN).

Using Amazon Redshift as the data storage and CloudFront as the CDN is incorrect as Amazon Redshift is usually used as a Data Warehouse.

Using Amazon S3 Glacier as the data storage and ElastiCache as the CDN is incorrect as Amazon S3 Glacier is usually used for data archives.

Using multiple EC2 instance stores for data storage and ElastiCache as the CDN is incorrect as data stored in an instance store is not durable.

References:

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

<https://aws.amazon.com/caching/cdn/>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

---

## QUESTION 97

An application is hosted in AWS Fargate and uses RDS database in Multi-AZ Deployments configuration with several Read Replicas. A Solutions Architect was instructed to ensure that all of their database credentials, API keys, and other secrets are encrypted and rotated on a regular basis to improve data security. The application should also use the latest version of the encrypted credentials when connecting to the RDS database.

Which of the following is the MOST appropriate solution to secure the credentials?

- A. Store the database credentials, API keys, and other secrets to AWS ACM.
- B. Use AWS Secrets Manager to store and encrypt the database credentials, API keys, and other secrets. Enable automatic rotation for all of the credentials.
- C. Store the database credentials, API keys, and other secrets in AWS KMS.
- D. Store the database credentials, API keys, and other secrets to Systems Manager Parameter Store each with a SecureString data type. The credentials are automatically rotated by default.

Answer: B

Explanation:

AWS Secrets Manager is an AWS service that makes it easier for you to manage secrets. Secrets can be database credentials, passwords, third-party API keys, and even arbitrary text. You can store and control access to these secrets centrally by using the Secrets Manager console, the Secrets Manager command line interface (CLI), or the Secrets Manager API and SDKs.

In the past, when you created a custom application that retrieves information from a database, you typically had to embed the credentials (the secret) for accessing the database directly in the application. When it came time to rotate the credentials, you had to do much more than just create new credentials. You had to invest time to update the application to use the new credentials. Then you had to distribute the updated application. If you had multiple applications that shared credentials and you missed updating one of them, the application would break. Because of this risk, many customers have chosen not to regularly rotate their credentials, which effectively substitutes one risk for another.



Secrets Manager enables you to replace hardcoded credentials in your code (including passwords), with an API call to Secrets Manager to retrieve the secret programmatically. This helps ensure that the secret can't be compromised by someone examining your code, because the secret simply isn't there. Also, you can configure Secrets Manager to automatically rotate the secret for you according to a schedule that you specify. This enables you to replace long-term secrets with short-term ones, which helps to

significantly reduce the risk of compromise.

Hence, the most appropriate solution for this scenario is: Use AWS Secrets Manager to store and encrypt the database credentials, API keys, and other secrets. Enable automatic rotation for all of the credentials.

The option that says: Store the database credentials, API keys, and other secrets to Systems Manager Parameter Store each with a SecureString data type. The credentials are automatically rotated by default is incorrect because Systems Manager Parameter Store doesn't rotate its parameters by default.

The option that says: Store the database credentials, API keys, and other secrets to AWS ACM is incorrect because it is just a managed private CA service that helps you easily and securely manage the lifecycle of your private certificates to allow SSL communication to your application. This is not a suitable service to store database or any other confidential credentials.

The option that says: Store the database credentials, API keys, and other secrets in AWS KMS is incorrect because this only makes it easy for you to create and manage encryption keys and control the use of encryption across a wide range of AWS services. This is primarily used for encryption and not for hosting your credentials.

References:

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

<https://aws.amazon.com/blogs/security/how-to-securely-provide-database-credentials-to-lambda-function-s-by-using-aws-secrets-manager/>

Check out these AWS Secrets Manager and Systems Manager Cheat Sheets:

<https://tutorialsdojo.com/aws-secrets-manager/>

<https://tutorialsdojo.com/aws-systems-manager/>

AWS Security Services Overview - Secrets Manager, ACM, Macie:

<https://www.youtube.com/watch?v=ogVamzF2Dzk>

---

## QUESTION 98

A digital media company shares static content to its premium users around the world and also to their partners who syndicate their media files. The company is looking for ways to reduce its server costs and securely deliver their data to their customers globally with low latency.

Which combination of services should be used to provide the MOST suitable and cost-effective architecture? (Select TWO.)

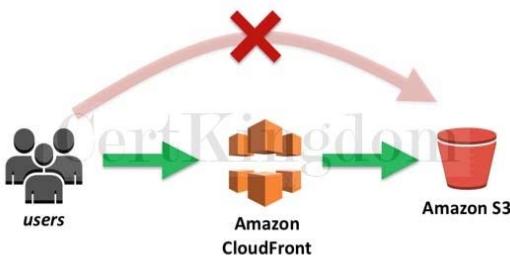
- A. Amazon CloudFront
- B. AWS Lambda
- C. AWS Fargate
- D. AWS Global Accelerator
- E. Amazon S3

Answer: A,E

Explanation:

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

CloudFront is integrated with AWS “ both physical locations that are directly connected to the AWS global infrastructure, as well as other AWS services. CloudFront works seamlessly with services including AWS Shield for DDoS mitigation, Amazon S3, Elastic Load Balancing or Amazon EC2 as origins for your applications, and Lambda@Edge to run custom code closer to customers’ users and to customize the user experience. Lastly, if you use AWS origins such as Amazon S3, Amazon EC2 or Elastic Load Balancing, you don’t pay for any data transferred between these services and CloudFront.



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 an extremely durable, highly available, and infinitely scalable data storage infrastructure at very low costs.

AWS Global Accelerator and Amazon CloudFront are separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable content (such as images and videos) and dynamic content (such as API acceleration and dynamic site delivery). Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. Both services integrate with AWS Shield for DDoS protection.

Hence, the correct options are Amazon CloudFront and Amazon S3.

AWS Fargate is incorrect because this service is just a serverless compute engine for containers that work with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Although this service is more cost-effective than its server-based counterpart, Amazon S3 still costs way less than Fargate, especially for storing static content.

AWS Lambda is incorrect because this simply lets you run your code serverless, without provisioning or managing servers. Although this is also a cost-effective service since you have to pay only for the compute time you consume, you can't use this to store static content or as a Content Delivery Network (CDN). A better combination is Amazon CloudFront and Amazon S3.

AWS Global Accelerator is incorrect because this service is more suitable for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. Moreover, there is no direct way that you can integrate AWS Global Accelerator with Amazon S3. It's more suitable to use Amazon CloudFront instead in this scenario.

#### References:

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/>  
<https://aws.amazon.com/blogs/networking-and-content-delivery/amazon-s3-amazon-cloudfront-a-matchmade-in-the-cloud/>  
<https://aws.amazon.com/global-accelerator/faqs/>

### QUESTION 99

A company has developed public APIs hosted in Amazon EC2 instances behind an Elastic Load Balancer. The APIs will be used by various clients from their respective on-premises data centers. A Solutions Architect received a report that the web service clients can only access trusted IP addresses whitelisted on their firewalls.

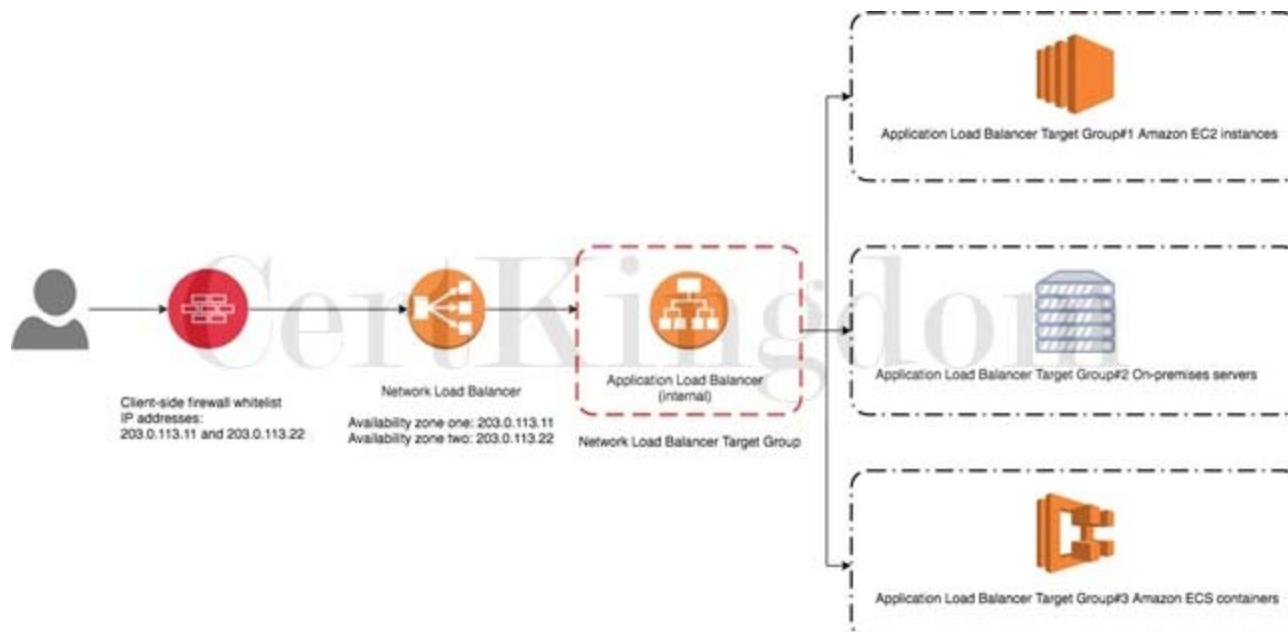
What should you do to accomplish the above requirement?

- A. Create an Alias Record in Route 53 which maps to the DNS name of the load balancer.
- B. Associate an Elastic IP address to a Network Load Balancer.
- C. Create a CloudFront distribution whose origin points to the private IP addresses of your web servers.
- D. Associate an Elastic IP address to an Application Load Balancer.

Answer: B

## Explanation:

A Network Load Balancer functions at the fourth layer of the Open Systems Interconnection (OSI) model. It can handle millions of requests per second. After the load balancer receives a connection request, it selects a target from the default rule's target group. It attempts to open a TCP connection to the selected target on the port specified in the listener configuration.



Based on the given scenario, web service clients can only access trusted IP addresses. To resolve this requirement, you can use the Bring Your Own IP (BYOIP) feature to use the trusted IPs as Elastic IP addresses (EIP) to a Network Load Balancer (NLB). This way, there's no need to re-establish the whitelists with new IP addresses.

Hence, the correct answer is: Associate an Elastic IP address to a Network Load Balancer.

The option that says: Associate an Elastic IP address to an Application Load Balancer is incorrect because you can't assign an Elastic IP address to an Application Load Balancer. The alternative method you can do is assign an Elastic IP address to a Network Load Balancer in front of the Application Load Balancer.

The option that says: Create a CloudFront distribution whose origin points to the private IP addresses of your web servers is incorrect because web service clients can only access trusted IP addresses. The fastest way to resolve this requirement is to attach an Elastic IP address to a Network Load Balancer.

The option that says: Create an Alias Record in Route 53 which maps to the DNS name of the load balancer is incorrect. This approach won't still allow them to access the application because of trusted IP addresses on their firewalls.

## References:

<https://aws.amazon.com/premiumsupport/knowledge-center/elb-attach-elastic-ip-to-public-nlb/>  
<https://aws.amazon.com/blogs/networking-and-content-delivery/using-static-ip-addresses-for-applicationload-balancers/>  
<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html>

Check out this AWS Elastic Load Balancing Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

## QUESTION 100

An advertising company is currently working on a proof of concept project that automatically provides SEO analytics for its clients. Your company has a VPC in AWS that operates in a dual-stack mode in which IPv4 and IPv6 communication is allowed. You deployed the application to an Auto Scaling group of EC2 instances with an Application Load Balancer in front that evenly distributes the incoming traffic. You are ready to go live but you need to point your domain name (tutorialsdojo.com) to the Application Load Balancer.

In Route 53, which record types will you use to point the DNS name of the Application Load Balancer? (Select TWO.)

- A. Alias with a type "A" record set
- B. Non-Alias with a type "A" record set
- C. Alias with a type of MX' record set
- D. Alias with a type "AAAA" record set
- E. Alias with a type "CNAME" record set

Answer: A,D

Explanation:

The correct answers are: Alias with a type "AAAA" record set and Alias with a type "A" record set. To route domain traffic to an ELB load balancer, use Amazon Route 53 to create an alias record that points to your load balancer. An alias record is a Route 53 extension to DNS. It's similar to a CNAME record, but you can create an alias record both for the root domain, such as tutorialsdojo.com, and for subdomains, such as portal.tutorialsdojo.com. (You can create CNAME records only for subdomains.) To enable IPv6 resolution, you would need to create a second resource record, tutorialsdojo.com ALIAS AAAA -> myelb.us-west-2.elb.amazonaws.com, this is assuming your Elastic Load Balancer has IPv6 support.

## Create Record Set

**Name:** tutorialsdojo.com.

**Type:** AAAA – IPv6 address

**Alias:**  Yes  No

**Alias Target:** dualstack.tutor-Appl-1ICKV12Q66A

**Alias Hosted Zone ID:** KTTL2X6KTTL2

You can also type the domain name for the resource. Examples:

- CloudFront distribution domain name: d111111abcdef8.cloudfront.net
- Elastic Beanstalk environment CNAME: example.elasticbeanstalk.com
- ELB load balancer DNS name: example-1.us-east-2.elb.amazonaws.com
- S3 website endpoint: s3-website.us-east-2.amazonaws.com
- Resource record set in this hosted zone: www.example.com
- VPC endpoint: example.us-east-2.vpce.amazonaws.com
- API Gateway custom regional API: d-abcd12345.execute-api.us-west-2.amazonaws.com

[Learn More](#)

**Routing Policy:** Simple

Route 53 responds to queries based only on the values in this record.

[Learn More](#)

**Evaluate Target Health:**  Yes  No

Non-Alias with a type "A" record set is incorrect because you only use Non-Alias with a type A' record set for IP addresses.

Alias with a type "CNAME" record set is incorrect because you can't create a CNAME record at the zone apex. For example, if you register the DNS name tutorialsdojo.com, the zone apex is tutorialsdojo.com.

Alias with a type of MX' record set is incorrect because an MX record is primarily used for mail servers. It includes a priority number and a domain name, for example: 10 mailserver.tutorialsdojo.com.

Reference:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-nonalias.html>

Check out this Amazon Route 53 Cheat Sheet:

<https://tutorialsdojo.com/amazon-route-53/>

### QUESTION 101

A company plans to migrate its suite of containerized applications running on-premises to a container

service in AWS. The solution must be cloud-agnostic and use an open-source platform that can automatically manage containerized workloads and services. It should also use the same configuration and tools across various production environments.

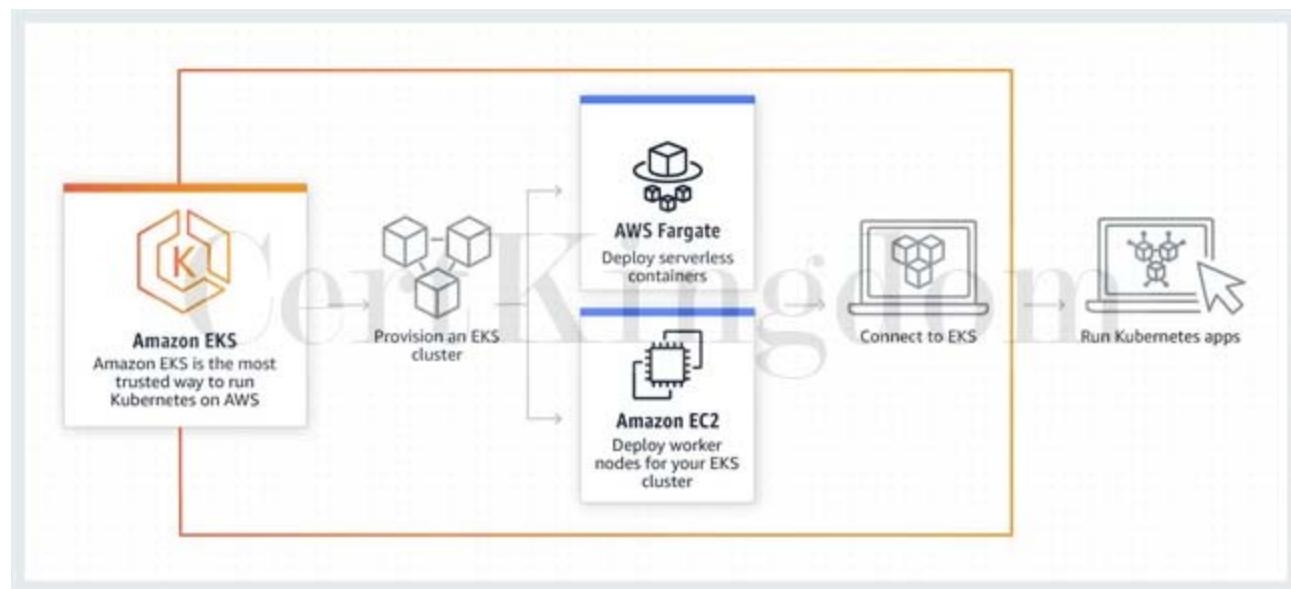
What should the Solution Architect do to properly migrate and satisfy the given requirement?

- A. Migrate the application to Amazon Container Registry (ECR) with Amazon EC2 instance worker nodes.
- B. Migrate the application to Amazon Elastic Container Service with ECS tasks that use the AWS Fargate launch type.
- C. Migrate the application to Amazon Elastic Container Service with ECS tasks that use the Amazon EC2 launch type.
- D. Migrate the application to Amazon Elastic Kubernetes Service with EKS worker nodes.

Answer: D

Explanation:

Amazon EKS provisions and scales the Kubernetes control plane, including the API servers and backend persistence layer, across multiple AWS availability zones for high availability and fault tolerance. Amazon EKS automatically detects and replaces unhealthy control plane nodes and provides patching for the control plane. Amazon EKS is integrated with many AWS services to provide scalability and security for your applications. These services include Elastic Load Balancing for load distribution, IAM for authentication, Amazon VPC for isolation, and AWS CloudTrail for logging.



To migrate the application to a container service, you can use Amazon ECS or Amazon EKS. But the key point in this scenario is cloud-agnostic and open-source platform. Take note that Amazon ECS is an AWS proprietary container service. This means that it is not an open-source platform. Amazon EKS is a portable, extensible, and open-source platform for managing containerized workloads and services.

Kubernetes is considered cloud-agnostic because it allows you to move your containers to other cloud service providers.

Amazon EKS runs up-to-date versions of the open-source Kubernetes software, so you can use all of the existing plugins and tools from the Kubernetes community. Applications running on Amazon EKS are fully compatible with applications running on any standard Kubernetes environment, whether running in on-premises data centers or public clouds. This means that you can easily migrate any standard Kubernetes application to Amazon EKS without any code modification required.

Hence, the correct answer is: Migrate the application to Amazon Elastic Kubernetes Service with EKS worker nodes.

The option that says: Migrate the application to Amazon Container Registry (ECR) with Amazon EC2 instance worker nodes is incorrect because Amazon ECR is just a fully-managed Docker container registry. Also, this option is not an open-source platform that can manage containerized workloads and services.

The option that says: Migrate the application to Amazon Elastic Container Service with ECS tasks that use the AWS Fargate launch type is incorrect because it is stated in the scenario that you have to migrate the application suite to an open-source platform. AWS Fargate is just a serverless compute engine for containers. It is not cloud-agnostic since you cannot use the same configuration and tools if you moved it to another cloud service provider such as Microsoft Azure or Google Cloud Platform (GCP).

The option that says: Migrate the application to Amazon Elastic Container Service with ECS tasks that use the Amazon EC2 launch type. is incorrect because Amazon ECS is an AWS proprietary managed container orchestration service. You should use Amazon EKS since Kubernetes is an open-source platform and is considered cloud-agnostic. With Kubernetes, you can use the same configuration and tools that you're currently using in AWS even if you move your containers to another cloud service provider.

References:

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

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

Check out our library of AWS Cheat Sheets:

<https://tutorialsdojo.com/links-to-all-aws-cheat-sheets/>

---

## QUESTION 102

A media company hosts large volumes of archive data that are about 250 TB in size on their internal servers. They have decided to move these data to S3 because of its durability and redundancy. The company currently has a 100 Mbps dedicated line connecting their head office to the Internet.

Which of the following is the FASTEST and the MOST cost-effective way to import all these data to Amazon S3?

- A. Order multiple AWS Snowball devices to upload the files to Amazon S3.
- B. Upload it directly to S3
- C. Use AWS Snowmobile to transfer the data over to S3.
- D. Establish an AWS Direct Connect connection then transfer the data over to S3.

Answer: A

Explanation:

AWS Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of the AWS cloud. Using Snowball addresses common challenges with large-scale data transfers, including high network costs, long transfer times, and security concerns.

Transferring data with Snowball is simple, fast, secure, and can be as little as one-fifth the cost of highspeed Internet.



Snowball is a strong choice for data transfer if you need to more securely and quickly transfer terabytes to many petabytes of data to AWS. Snowball can also be the right choice if you don't want to make expensive upgrades to your network infrastructure, if you frequently experience large backlogs of data, if you're located in a physically isolated environment, or if you're in an area where high-speed Internet connections are not available or cost-prohibitive.

As a rule of thumb, if it takes more than one week to upload your data to AWS using the spare capacity of your existing Internet connection, then you should consider using Snowball. For example, if you have a 100 Mb connection that you can solely dedicate to transferring your data and need to transfer 100 TB of data, it takes more than 100 days to complete data transfer over that connection. You can make the same transfer by using multiple Snowballs in about a week.

Available Internet Connection	Theoretical Min. Number of Days to Transfer 100TB at 80% Network Utilization	When to Consider AWS Snowball?
T3 (44.736Mbps)	269 days	2TB or more
100Mbps	120 days	5TB or more
1000Mbps	12 days	60TB or more

Hence, ordering multiple AWS Snowball devices to upload the files to Amazon S3 is the correct answer. Uploading it directly to S3 is incorrect since this would take too long to finish due to the slow Internet connection of the company.

Establishing an AWS Direct Connect connection then transferring the data over to S3 is incorrect since provisioning a line for Direct Connect would take too much time and might not give you the fastest data transfer solution. In addition, the scenario didn't warrant an establishment of a dedicated connection from your on-premises data center to AWS. The primary goal is to just do a one-time migration of data to AWS which can be accomplished by using AWS Snowball devices.

Using AWS Snowmobile to transfer the data over to S3 is incorrect because Snowmobile is more suitable if you need to move extremely large amounts of data to AWS or need to transfer up to 100PB of

data. This will be transported on a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck. Take note that you only need to migrate 250 TB of data, hence, this is not the most suitable and cost-effective solution.

References:

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

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

S3 Transfer Acceleration vs Direct Connect vs VPN vs Snowball vs Snowmobile:

<https://tutorialsdojo.com/s3-transfer-acceleration-vs-direct-connect-vs-vpn-vs-snowball-vs-snowmobile/>

Comparison of AWS Services Cheat Sheets:

<https://tutorialsdojo.com/comparison-of-aws-services/>

---

## QUESTION 103

For data privacy, a healthcare company has been asked to comply with the Health Insurance Portability and Accountability Act (HIPAA). The company stores all its backups on an Amazon S3 bucket. It is required that data stored on the S3 bucket must be encrypted.

What is the best option to do this? (Select TWO.)

- A. Store the data on EBS volumes with encryption enabled instead of using Amazon S3.
- B. Enable Server-Side Encryption on an S3 bucket to make use of AES-256 encryption.
- C. Before sending the data to Amazon S3 over HTTPS, encrypt the data locally first using your own encryption keys.
- D. Store the data in encrypted EBS snapshots.
- E. Enable Server-Side Encryption on an S3 bucket to make use of AES-128 encryption.

Answer: B,C

Explanation:

Server-side encryption is about data encryption at rest”that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects. For example, if you share your objects using a pre-signed URL, that URL works the same way for both encrypted and unencrypted objects.

You have three mutually exclusive options depending on how you choose to manage the encryption keys:

Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Use Server-Side Encryption with Customer-Provided Keys (SSE-C)

The options that say: Before sending the data to Amazon S3 over HTTPS, encrypt the data locally first using your own encryption keys and Enable Server-Side Encryption on an S3 bucket to make use of AES-256 encryption are correct because these options are using client-side encryption and Amazon S3-Managed Keys (SSE-S3) respectively. Client-side encryption is the act of encrypting data before sending it to Amazon S3 while SSE-S3 uses AES-256 encryption.

Storing the data on EBS volumes with encryption enabled instead of using Amazon S3 and storing the data in encrypted EBS snapshots are incorrect because both options use EBS encryption and not S3.

Enabling Server-Side Encryption on an S3 bucket to make use of AES-128 encryption is incorrect as S3 doesn't provide AES-128 encryption, only AES-256.

References:

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

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

## QUESTION 104

One member of your DevOps team consulted you about a connectivity problem in one of your Amazon EC2 instances. The application architecture is initially set up with four EC2 instances, each with an EIP address that all belong to a public non-default subnet. You launched another instance to handle the increasing workload of your application. The EC2 instances also belong to the same security group. Everything works well as expected except for one of the EC2 instances which is not able to send nor receive traffic over the Internet.

Which of the following is the MOST likely reason for this issue?

- A. The EC2 instance does not have a private IP address associated with it.
- B. The EC2 instance is running in an Availability Zone that is not connected to an Internet gateway.
- C. The route table is not properly configured to allow traffic to and from the Internet through the Internet gateway.
- D. The EC2 instance does not have a public IP address associated with it.

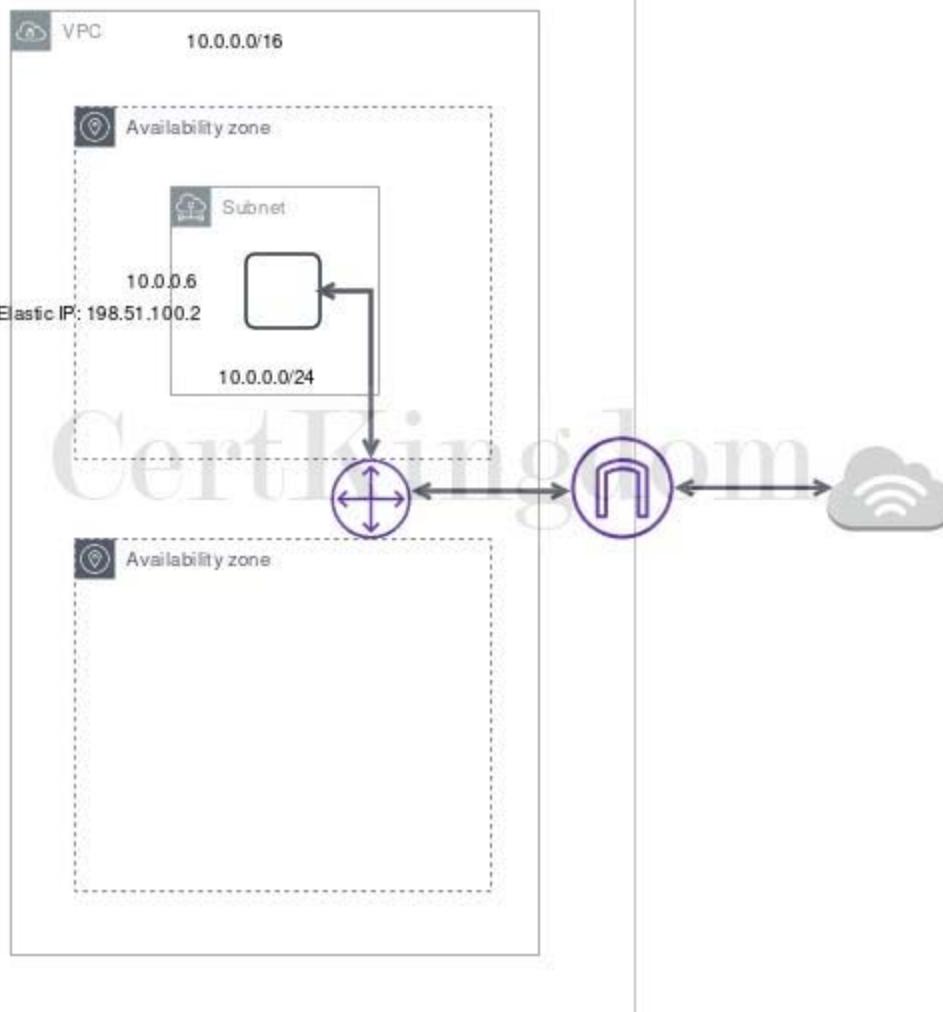
Answer: D

Explanation:

IP addresses enable resources in your VPC to communicate with each other and with resources over the Internet. Amazon EC2 and Amazon VPC support the IPv4 and IPv6 addressing protocols.

By default, Amazon EC2 and Amazon VPC use the IPv4 addressing protocol. When you create a VPC, you must assign it an IPv4 CIDR block (a range of private IPv4 addresses). Private IPv4 addresses are not reachable over the Internet. To connect to your instance over the Internet or to enable communication between your instances and other AWS services that have public endpoints, you can assign a globally-unique public IPv4 address to your instance.

You can optionally associate an IPv6 CIDR block with your VPC and subnets and assign IPv6 addresses from that block to the resources in your VPC. IPv6 addresses are public and reachable over the Internet.



All subnets have a modifiable attribute that determines whether a network interface created in that subnet is assigned a public IPv4 address and, if applicable, an IPv6 address. This includes the primary network interface (eth0) that's created for an instance when you launch an instance in that subnet. Regardless of the subnet attribute, you can still override this setting for a specific instance during launch. By default, nondefault subnets have the IPv4 public addressing attribute set to false, and default subnets have this attribute set to true. An exception is a nondefault subnet created by the Amazon EC2 launch instance wizard – the wizard sets the attribute to true. You can modify this attribute using the Amazon VPC console.

In this scenario, there are 5 EC2 instances that belong to the same security group that should be able to connect to the Internet. The main route table is properly configured but there is a problem connecting to one instance. Since the other four instances are working fine, we can assume that the security group and the route table are correctly configured. One possible reason for this issue is that the problematic instance does not have a public or an EIP address.

Take note as well that the four EC2 instances all belong to a public non-default subnet. This means that a new EC2 instance will not have a public IP address by default since the since IPv4 public addressing attribute is initially set to false.

Hence, the correct answer is the option that says: The EC2 instance does not have a public IP address associated with it.

The option that says: The route table is not properly configured to allow traffic to and from the Internet through the Internet gateway is incorrect because the other three instances, which are associated with the same route table and security group, do not have any issues.

The option that says: The EC2 instance is running in an Availability Zone that is not connected to an Internet gateway is incorrect because there is no relationship between the Availability Zone and the Internet Gateway (IGW) that may have caused the issue.

References:

[http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Scenario1.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html)

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

## QUESTION 105

An Intelligence Agency developed a missile tracking application that is hosted on both development and production AWS accounts. The Intelligence agency's junior developer only has access to the development account. She has received security clearance to access the agency's production account but the access is only temporary and only write access to EC2 and S3 is allowed.

Which of the following allows you to issue short-lived access tokens that act as temporary security credentials to allow access to your AWS resources?

- A. Use AWS SSO
- B. Use AWS Cognito to issue JSON Web Tokens (JWT)
- C. All of the given options are correct.
- D. Use AWS STS

Answer: D

Explanation:

AWS Security Token Service (AWS STS) is the service that you can use to create and provide trusted users with temporary security credentials that can control access to your AWS resources. Temporary security credentials work almost identically to the long-term access key credentials that your IAM users can use.

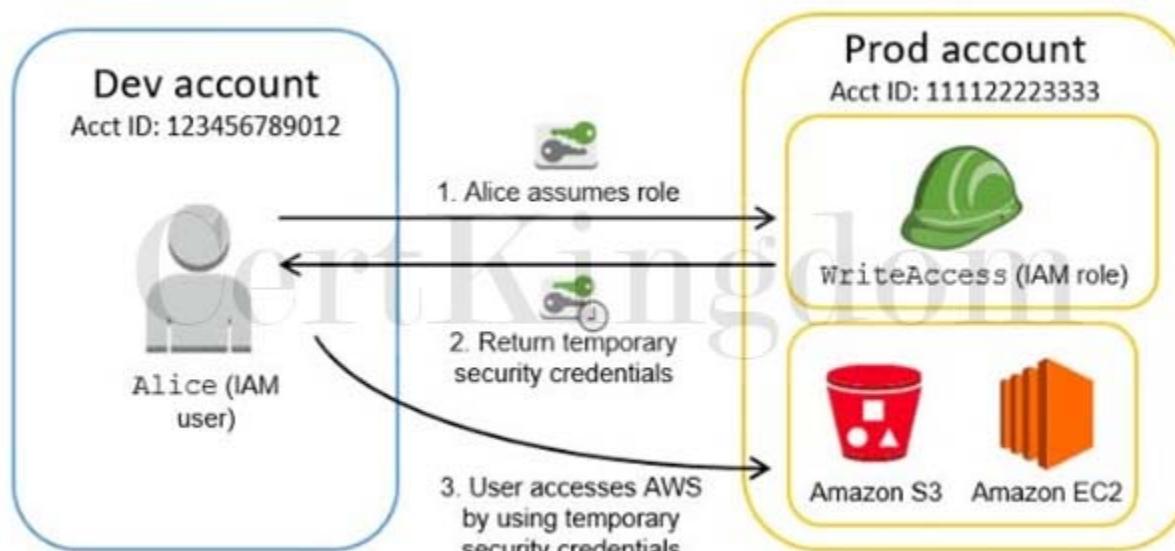
In this diagram, IAM user Alice in the Dev account (the role-assuming account) needs to access the Prod account (the role-owning account). Here's how it works:

Alice in the Dev account assumes an IAM role (WriteAccess) in the Prod account by calling AssumeRole.

STS returns a set of temporary security credentials.

Alice uses the temporary security credentials to access services and resources in the Prod account.

Alice could, for example, make calls to Amazon S3 and Amazon EC2, which are granted by the WriteAccess role.



Using AWS Cognito to issue JSON Web Tokens (JWT) is incorrect because the Amazon Cognito service is primarily used for user authentication and not for providing access to your AWS resources. A JSON Web Token (JWT) is meant to be used for user authentication and session management.

Using AWS SSO is incorrect. Although the AWS SSO service uses STS, it does not issue short-lived credentials by itself. AWS Single Sign-On (SSO) is a cloud SSO service that makes it easy to centrally manage SSO access to multiple AWS accounts and business applications.

The option that says All of the above is incorrect as only STS has the ability to provide temporary security credentials.

Reference:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_temp.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html)

AWS Identity Services Overview:

<https://www.youtube.com/watch?v=AIIdUw0i8rr0>

Check out this AWS IAM Cheat Sheet:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

---

## QUESTION 106

A company is planning to launch an application which requires a data warehouse that will be used for their infrequently accessed data. You need to use an EBS Volume that can handle large, sequential I/O operations.

Which of the following is the most cost-effective storage type that you should use to meet the requirement?

- A. Throughput Optimized HDD (st1)
- B. Provisioned IOPS SSD (io1)
- C. EBS General Purpose SSD (gp2)
- D. Cold HDD (sc1)

Answer: D

Explanation:

Cold HDD volumes provide low-cost magnetic storage that defines performance in terms of throughput rather than IOPS. With a lower throughput limit than Throughput Optimized HDD, this is a good fit ideal for large, sequential cold-data workloads. If you require infrequent access to your data and are looking to save costs, Cold HDD provides inexpensive block storage. Take note that bootable Cold HDD volumes are not supported.

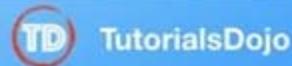
Volume Type	Solid-State Drives (SSD)		Hard Disk Drives (HDD)	
	General Purpose SSD (gp2)*	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume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

Cold HDD provides the lowest cost HDD volume and is designed for less frequently accessed workloads. Hence, Cold HDD (sc1) is the correct answer.

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"> <li>- Best for <b>transactional workloads</b></li> <li>- Critical business applications that require sustained IOPS performance</li> <li>- Large database workloads such as MongoDB, Oracle, Microsoft SQL Server and many others...</li> </ul>	<ul style="list-style-type: none"> <li>- Best for <i>large streaming workloads</i> requiring consistent, fast throughput at a low price</li> <li>- Big data, Data warehouses, Log processing</li> <li>- Throughput-oriented storage for large volumes of data that is <i>infrequently accessed</i></li> </ul>
Cost	moderate / high 	low 
Dominant Performance Attribute	IOPS	Throughput (MiB/s)



EBS General Purpose SSD (gp2) is incorrect because a General purpose SSD volume costs more and it is mainly used for a wide variety of workloads. It is recommended to be used as system boot volumes, virtual desktops, low-latency interactive apps, and many more.

Provisioned IOPS SSD (io1) is incorrect because this costs more than Cold HDD and thus, not costeffective for this scenario. It provides the highest performance SSD volume for mission-critical lowlatency or high-throughput workloads, which is not needed in the scenario.

Throughput Optimized HDD (st1) is incorrect because this is primarily used for frequently accessed, throughput-intensive workloads. In this scenario, Cold HDD perfectly fits the requirement as it is used for their infrequently accessed data and provides the lowest cost, unlike Throughput Optimized HDD.

References:

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

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

Check out this Amazon EBS Cheat Sheet:

<https://tutorialsdojo.com/amazon-ebs/>

## QUESTION 107

A company has an enterprise web application hosted on Amazon ECS Docker containers that use an Amazon FSx for Lustre filesystem for its high-performance computing workloads. A warm standby environment is running in another AWS region for disaster recovery. A Solutions Architect was assigned to design a system that will automatically route the live traffic to the disaster recovery (DR) environment only in the event that the primary application stack experiences an outage.

What should the Architect do to satisfy this requirement?

- A. Set up a Weighted routing policy configuration in Route 53 by adding health checks on both the primary stack and the DR environment. Configure the network access control list and the route table to allow Route 53 to send requests to the endpoints specified in the health checks. Enable the Evaluate

- Target Health option by setting it to Yes.
- B. Set up a failover routing policy configuration in Route 53 by adding a health check on the primary service endpoint. Configure Route 53 to direct the DNS queries to the secondary record when the primary resource is unhealthy. Configure the network access control list and the route table to allow Route 53 to send requests to the endpoints specified in the health checks. Enable the Evaluate Target Health option by setting it to Yes.
- C. Set up a CloudWatch Events rule to monitor the primary Route 53 DNS endpoint and create a custom Lambda function. Execute the ChangeResourceRecordSets API call using the function to initiate the failover to the secondary DNS record.
- D. Set up a CloudWatch Alarm to monitor the primary Route 53 DNS endpoint and create a custom Lambda function. Execute the ChangeResourceRecordSets API call using the function to initiate the failover to the secondary DNS record.

Answer: B

Explanation:

Use an active-passive failover configuration when you want a primary resource or group of resources to be available majority of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable. When responding to queries, Route 53 includes only the healthy primary resources. If all the primary resources are unhealthy, Route 53 begins to include only the healthy secondary resources in response to DNS queries.

To create an active-passive failover configuration with one primary record and one secondary record, you just create the records and specify Failover for the routing policy. When the primary resource is healthy, Route 53 responds to DNS queries using the primary record. When the primary resource is unhealthy, Route 53 responds to DNS queries using the secondary record.

You can configure a health check that monitors an endpoint that you specify either by IP address or by domain name. At regular intervals that you specify, Route 53 submits automated requests over the Internet to your application, server, or other resource to verify that it's reachable, available, and functional. Optionally, you can configure the health check to make requests similar to those that your users make, such as requesting a web page from a specific URL.

## Create Record Set

Name: example.com.

Type: A - IPv4 address

Alias:  Yes  No

Alias Target: [REDACTED].us-west-2.elb.amazonaws

Alias Hosted Zone ID: [REDACTED]

Routing Policy: Failover

Route 53 responds to queries using primary record sets if any are healthy, or using secondary record sets otherwise. [Learn More](#)

Failover Record Type:  Primary  Secondary

Set ID: Primary

Evaluate Target Health:  Yes  No

**Create Record Set**

When Route 53 checks the health of an endpoint, it sends an HTTP, HTTPS, or TCP request to the IP address and port that you specified when you created the health check. For a health check to succeed, your router and firewall rules must allow inbound traffic from the IP addresses that the Route 53 health checkers use.

Hence, the correct answer is: Set up a failover routing policy configuration in Route 53 by adding a health check on the primary service endpoint. Configure Route 53 to direct the DNS queries to the secondary record when the primary resource is unhealthy. Configure the network access control list and the route table to allow Route 53 to send requests to the endpoints specified in the health checks.

Enable the Evaluate Target Health option by setting it to Yes.

The option that says: Set up a Weighted routing policy configuration in Route 53 by adding health checks on both the primary stack and the DR environment. Configure the network access control list and the route table to allow Route 53 to send requests to the endpoints specified in the health checks. Enable the Evaluate Target Health option by setting it to Yes is incorrect because Weighted routing simply lets you associate multiple resources with a single domain name (tutorialsdojo.com) or subdomain name (blog.tutorialsdojo.com) and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load balancing and testing new versions of software, but not for a failover configuration. Remember that the scenario says that the solution should automatically route the live traffic to the disaster recovery (DR) environment only in the event that the primary application stack experiences an outage. This configuration is incorrectly distributing the traffic on both the primary and DR environment.

The option that says: Set up a CloudWatch Alarm to monitor the primary Route 53 DNS endpoint and create a custom Lambda function. Execute the ChangeResourceRecordSets API call using the function to initiate the failover to the secondary DNS record is incorrect because setting up a CloudWatch Alarm and using the Route 53 API is not applicable nor useful at all in this scenario. Remember that CloudWatch Alarms are primarily used for monitoring CloudWatch metrics. You have to use a Failover routing policy instead.

The option that says: Set up a CloudWatch Events rule to monitor the primary Route 53 DNS endpoint and create a custom Lambda function. Execute the ChangeResourceRecordSets API call using the function to initiate the failover to the secondary DNS record is incorrect because the Amazon CloudWatch Events service is commonly used to deliver a near real-time stream of system events that describe changes in some Amazon Web Services (AWS) resources. There is no direct way for

CloudWatch Events to monitor the status of your Route 53 endpoints. You have to configure a health check and a failover configuration in Route 53 instead to satisfy the requirement in this scenario.

References:

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

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

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

Check out this Amazon Route 53 Cheat Sheet:

<https://tutorialsdojo.com/amazon-route-53/>

---

### QUESTION 108

A start-up company has an EC2 instance that is hosting a web application. The volume of users is expected to grow in the coming months and hence, you need to add more elasticity and scalability in your AWS architecture to cope with the demand.

Which of the following options can satisfy the above requirement for the given scenario? (Select TWO.)

- A. Set up two EC2 instances and use Route 53 to route traffic based on a Weighted Routing Policy.
- B. Set up two EC2 instances and then put them behind an Elastic Load balancer (ELB).
- C. Set up an AWS WAF behind your EC2 Instance.
- D. Set up two EC2 instances deployed using Launch Templates and integrated with AWS Glue.
- E. Set up an S3 Cache in front of the EC2 instance.

Answer: A,B

Explanation:

Using an Elastic Load Balancer is an ideal solution for adding elasticity to your application. Alternatively, you can also create a policy in Route 53, such as a Weighted routing policy, to evenly distribute the traffic to 2 or more EC2 instances. Hence, setting up two EC2 instances and then put them behind an Elastic Load balancer (ELB) and setting up two EC2 instances and using Route 53 to route traffic based on a Weighted Routing Policy are the correct answers.

Setting up an S3 Cache in front of the EC2 instance is incorrect because doing so does not provide elasticity and scalability to your EC2 instances.

Setting up an AWS WAF behind your EC2 Instance is incorrect because AWS WAF is a web application firewall that helps protect your web applications from common web exploits. This service is more on providing security to your applications.

Setting up two EC2 instances deployed using Launch Templates and integrated with AWS Glue is incorrect because AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. It does not provide scalability or elasticity to your instances.

References:

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

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide>Welcome.html>

Check out this AWS Elastic Load Balancing (ELB) Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

Check out this Amazon Route 53 Cheat Sheet:

<https://tutorialsdojo.com/amazon-route-53/>

---

### QUESTION 109

A company plans to migrate all of their applications to AWS. The Solutions Architect suggested to store all the data to EBS volumes. The Chief Technical Officer is worried that EBS volumes are not appropriate for the existing workloads due to compliance requirements, downtime scenarios, and IOPS performance.

Which of the following are valid points in proving that EBS is the best service to use for migration? (Select TWO.)

- A. EBS volumes can be attached to any EC2 Instance in any Availability Zone.

B. Amazon EBS provides the ability to create snapshots (backups) of any EBS volume and write a copy of the data in the volume to Amazon RDS, where it is stored redundantly in multiple Availability Zones

C. When you create an EBS volume in an Availability Zone, it is automatically replicated on a separate AWS region to prevent data loss due to a failure of any single hardware component.

D. EBS volumes support live configuration changes while in production which means that you can modify the volume type, volume size, and IOPS capacity without service interruptions.

E. An EBS volume is off-instance storage that can persist independently from the life of an instance.

Answer: D,E

Explanation:

An Amazon EBS volume is a durable, block-level storage device that you can attach to a single EC2 instance. You can use EBS volumes as primary storage for data that requires frequent updates, such as the system drive for an instance or storage for a database application. You can also use them for throughput-intensive applications that perform continuous disk scans. EBS volumes persist independently from the running life of an EC2 instance.

Here is a list of important information about EBS Volumes:

- When you create an EBS volume in an Availability Zone, it is automatically replicated within that zone to prevent data loss due to a failure of any single hardware component.
- An EBS volume can only be attached to one EC2 instance at a time.
- After you create a volume, you can attach it to any EC2 instance in the same Availability Zone
- An EBS volume is off-instance storage that can persist independently from the life of an instance. You can specify not to terminate the EBS volume when you terminate the EC2 instance during instance creation.
- EBS volumes support live configuration changes while in production which means that you can modify the volume type, volume size, and IOPS capacity without service interruptions.
- Amazon EBS encryption uses 256-bit Advanced Encryption Standard algorithms (AES-256)
- EBS Volumes offer 99.999% SLA.

The option that says: When you create an EBS volume in an Availability Zone, it is automatically replicated on a separate AWS region to prevent data loss due to a failure of any single hardware component is incorrect because when you create an EBS volume in an Availability Zone, it is automatically replicated within that zone only, and not on a separate AWS region, to prevent data loss due to a failure of any single hardware component.

The option that says: EBS volumes can be attached to any EC2 Instance in any Availability Zone is incorrect as EBS volumes can only be attached to an EC2 instance in the same Availability Zone.

The option that says: Amazon EBS provides the ability to create snapshots (backups) of any EBS volume and write a copy of the data in the volume to Amazon RDS, where it is stored redundantly in multiple Availability Zones is almost correct. But instead of storing the volume to Amazon RDS, the EBS Volume snapshots are actually sent to Amazon S3.

References:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html>

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

Check out this Amazon EBS Cheat Sheet:

<https://tutorialsdojo.com/amazon-ebs/>

Here is a short video tutorial on EBS:

<https://youtu.be/ljYH5IHQdxo>

---

## QUESTION 110

A company has a top priority requirement to monitor a few database metrics and then afterward, send email notifications to the Operations team in case there is an issue. Which AWS services can accomplish this requirement? (Select TWO.)

- A. Amazon Simple Queue Service (SQS)
- B. Amazon Simple Notification Service (SNS)
- C. Amazon Simple Email Service

D. Amazon CloudWatch

E. Amazon EC2 Instance with a running Berkeley Internet Name Domain (BIND) Server.

Answer: B,D

Explanation:

Amazon CloudWatch and Amazon Simple Notification Service (SNS) are correct. In this requirement, you can use Amazon CloudWatch to monitor the database and then Amazon SNS to send the emails to the Operations team. Take note that you should use SNS instead of SES (Simple Email Service) when you want to monitor your EC2 instances.



CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing you with a unified view of AWS resources, applications, and services that run on AWS, and on-premises servers.

SNS is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications.

Amazon Simple Email Service is incorrect. SES is a cloud-based email sending service designed to send notifications and transactional emails.

Amazon Simple Queue Service (SQS) is incorrect. SQS is a fully-managed message queuing service. It does not monitor applications nor send email notifications, unlike SES.

Amazon EC2 Instance with a running Berkeley Internet Name Domain (BIND) Server is incorrect because BIND is primarily used as a Domain Name System (DNS) web service. This is only applicable if you have a private hosted zone in your AWS account. It does not monitor applications nor send email notifications.

References:

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

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

Check out this Amazon CloudWatch Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudwatch/>

## QUESTION 111

All objects uploaded to an Amazon S3 bucket must be encrypted for security compliance. The bucket will use server-side encryption with Amazon S3-Managed encryption keys (SSE-S3) to encrypt data using 256-bit Advanced Encryption Standard (AES-256) block cipher.

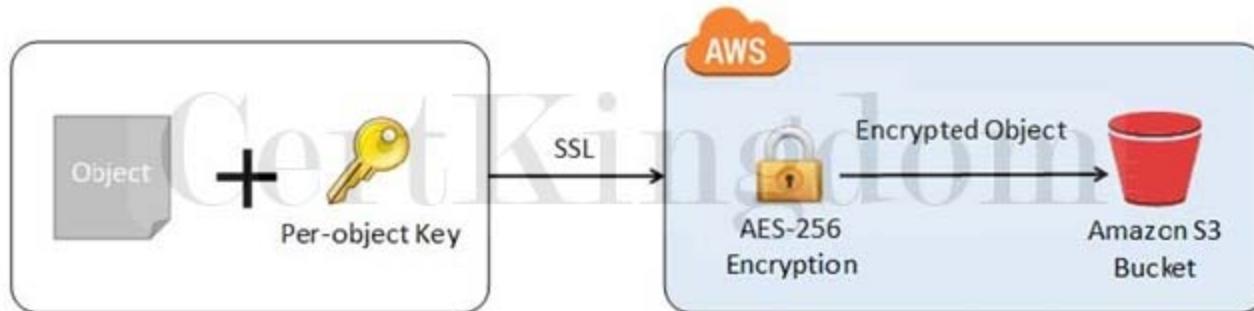
Which of the following request headers must be used?

- A. x-amz-server-side-encryption-customer-key
- B. x-amz-server-side-encryption-customer-algorithm
- C. x-amz-server-side-encryption-customer-key-MD5
- D. x-amz-server-side-encryption

Answer: D

Explanation:

Server-side encryption protects data at rest. If you use Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3), Amazon S3 will encrypt each object with a unique key and as an additional safeguard, it encrypts the key itself with a master key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.



If you need server-side encryption for all of the objects that are stored in a bucket, use a bucket policy. For example, the following bucket policy denies permissions to upload an object unless the request includes the x-amz-server-side-encryption header to request server-side encryption:

However, if you chose to use server-side encryption with customer-provided encryption keys (SSE-C), you must provide encryption key information using the following request headers:

x-amz-server-side-encryption-customer-algorithm

x-amz-server-side-encryption-customer-key

x-amz-server-side-encryption-customer-key-MD5

Hence, using the x-amz-server-side-encryption header is correct as this is the one being used for Amazon S3-Managed Encryption Keys (SSE-S3).

All other options are incorrect since they are used for SSE-C.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>

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

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

## QUESTION 112

A company wants to streamline the process of creating multiple AWS accounts within an AWS Organization. Each organization unit (OU) must be able to launch new accounts with preapproved configurations from the security team which will standardize the baselines and network configurations for all accounts in the organization.

Which solution entails the least amount of effort to implement?

- A. Set up an AWS Config aggregator on the root account of the organization to enable multi-account, multi-region data aggregation. Deploy conformance packs to standardize the baselines and network configurations for all accounts.
- B. Set up an AWS Control Tower Landing Zone. Enable pre-packaged guardrails to enforce policies or detect violations.
- C. Configure AWS Resource Access Manager (AWS RAM) to launch new AWS accounts as well as standardize the baselines and network configurations for each organization unit
- D. Centralized the creation of AWS accounts using AWS Systems Manager OpsCenter. Enforce policies and detect violations to all AWS accounts using AWS Security Hub.

Answer: B

Explanation:

AWS Control Tower provides a single location to easily set up your new well-architected multi-account environment and govern your AWS workloads with rules for security, operations, and internal

compliance. You can automate the setup of your AWS environment with best-practices blueprints for multi-account structure, identity, access management, and account provisioning workflow. For ongoing governance, you can select and apply pre-packaged policies enterprise-wide or to specific groups of accounts.

AWS Control Tower > Set up landing zone

Step 1  
Review pricing and select Regions

Step 2  
Configure organizational units (OUs)

Step 3  
Configure shared accounts and encryption

Step 4  
Review and set up landing zone

Configure organizational units (OUs) Info

**Foundational OU**

To start a well-planned OU structure in your landing zone, AWS Control Tower sets up a Security OU for you. This OU contains two shared accounts: the log archive account, and the security audit account (also referred to as the audit account).

Change OU name - optional  
"Security" is the default OU name for your shared accounts. OU names must be unique and can be edited after you set up your landing zone.

Tutorials Dojo Control Tower

**Additional OU**

To help set up a multi-account system, AWS Control Tower recommends you create a secondary OU when setting up your landing zone. This OU can be used to store any production or development accounts. You can create more OUs after setting up your landing zone.

Change OU name - optional  
"Sandbox" is the default OU name for your additional OU. OU names must be unique and can be edited after you set up your landing zone.

Philippine OU

Cancel Previous Next

AWS Control Tower provides three methods for creating member accounts:

- Through the Account Factory console that is part of AWS Service Catalog.
- Through the Enroll account feature within AWS Control Tower.
- From your AWS Control Tower landing zone's management account, using Lambda code and appropriate IAM roles.

AWS Control Tower offers "guardrails" for ongoing governance of your AWS environment. Guardrails provide governance controls by preventing the deployment of resources that don't conform to selected policies or detecting non-conformance of provisioned resources. AWS Control Tower automatically implements guardrails using multiple building blocks such as AWS CloudFormation to establish a baseline, AWS Organizations service control policies (SCPs) to prevent configuration changes, and AWS Config rules to continuously detect non-conformance.

In this scenario, the requirement is to simplify the creation of AWS accounts that have governance guardrails and a defined baseline in place. To save time and resources, you can use AWS Control Tower to automate account creation. With the appropriate user group permissions, you can specify standardized baselines and network configurations for all accounts in the organization.

Hence, the correct answer is: Set up an AWS Control Tower Landing Zone. Enable pre-packaged guardrails to enforce policies or detect violations.

The option that says: Configure AWS Resource Access Manager (AWS RAM) to launch new AWS accounts as well as standardize the baselines and network configurations for each organization unit is incorrect. The AWS Resource Access Manager (RAM) service simply helps you to securely share your resources across AWS accounts or within your organization or organizational units (OUs) in AWS Organizations. It is not capable of launching new AWS accounts with preapproved configurations. The option that says: Set up an AWS Config aggregator on the root account of the organization to enable multi-account, multi-region data aggregation. Deploy conformance packs to standardize the baselines and network configurations for all accounts is incorrect. AWS Config cannot provision

accounts. A conformance pack is only a collection of AWS Config rules and remediation actions that can be easily deployed as a single entity in an account and a Region or across an organization in AWS Organizations.

The option that says: Centralized the creation of AWS accounts using AWS Systems Manager OpsCenter. Enforce policies and detect violations to all AWS accounts using AWS Security Hub is incorrect. AWS Systems Manager is just a collection of services used to manage applications and infrastructure running in AWS that is usually in a single AWS account. The AWS Systems Manager OpsCenter service is just one of the capabilities of AWS Systems Manager, provides a central location where operations engineers and IT professionals can view, investigate, and resolve operational work items (OpsItems) related to AWS resources.

References:

<https://docs.aws.amazon.com/controlltower/latest/userguide/account-factory.html>

<https://aws.amazon.com/blogs/mt/how-to-automate-the-creation-of-multiple-accounts-in-aws-control-tower/>

<https://aws.amazon.com/blogs/aws/aws-control-tower-set-up-govern-a-multi-account-aws-environment/>

---

### QUESTION 113

A company developed a meal planning application that provides meal recommendations for the week as well as the food consumption of the users. The application resides on an EC2 instance which requires access to various AWS services for its day-to-day operations.

Which of the following is the best way to allow the EC2 instance to access the S3 bucket and other AWS services?

- A. Store the API credentials in a bastion host.
- B. Store the API credentials in the EC2 instance.
- C. Create a role in IAM and assign it to the EC2 instance.
- D. Add the API Credentials in the Security Group and assign it to the EC2 instance.

Answer: C

Explanation:

The best practice in handling API Credentials is to create a new role in the Identity Access Management (IAM) service and then assign it to a specific EC2 instance. In this way, you have a secure and centralized way of storing and managing your credentials.



Storing the API credentials in the EC2 instance, adding the API Credentials in the Security Group and assigning it to the EC2 instance, and storing the API credentials in a bastion host are incorrect because it is not secure to store nor use the API credentials from an EC2 instance. You should use IAM service instead.

Reference:

## QUESTION 114

A company is building an internal application that serves as a repository for images uploaded by a couple of users. Whenever a user uploads an image, it would be sent to Kinesis Data Streams for processing before it is stored in an S3 bucket. If the upload was successful, the application will return a prompt informing the user that the operation was successful. The entire processing typically takes about 5 minutes to finish.

Which of the following options will allow you to asynchronously process the request to the application from upload request to Kinesis, S3, and return a reply in the most cost-effective manner?

- A. Use a combination of SQS to queue the requests and then asynchronously process them using On-Demand EC2 Instances.
- B. Replace the Kinesis Data Streams with an Amazon SQS queue. Create a Lambda function that will asynchronously process the requests.
- C. Use a combination of SNS to buffer the requests and then asynchronously process them using On-Demand EC2 Instances.
- D. Use a combination of Lambda and Step Functions to orchestrate service components and asynchronously process the requests.

Answer: B

Explanation:

AWS Lambda supports the synchronous and asynchronous invocation of a Lambda function. You can control the invocation type only when you invoke a Lambda function. When you use an AWS service as a trigger, the invocation type is predetermined for each service. You have no control over the invocation type that these event sources use when they invoke your Lambda function. Since processing only takes 5 minutes, Lambda is also a cost-effective choice.



You can use an AWS Lambda function to process messages in an Amazon Simple Queue Service (Amazon SQS) queue. Lambda event source mappings support standard queues and first-in, first-out (FIFO) queues. With Amazon SQS, you can offload tasks from one component of your application by sending them to a queue and processing them asynchronously.

Kinesis Data Streams is a real-time data streaming service that requires the provisioning of shards.

Amazon SQS is a cheaper option because you only pay for what you use. Since there is no requirement for real-time processing in the scenario given, replacing Kinesis Data Streams with Amazon SQS would save more costs.

Hence, the correct answer is: Replace the Kinesis stream with an Amazon SQS queue. Create a Lambda function that will asynchronously process the requests.

Using a combination of Lambda and Step Functions to orchestrate service components and asynchronously process the requests is incorrect. The AWS Step Functions service lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly. Although this can be a valid solution, it is not cost-effective since the application does not have a lot of components to

orchestrate. Lambda functions can effectively meet the requirements in this scenario without using Step Functions. This service is not as cost-effective as Lambda.

Using a combination of SQS to queue the requests and then asynchronously processing them using On-Demand EC2 Instances and Using a combination of SNS to buffer the requests and then asynchronously processing them using On-Demand EC2 Instances are both incorrect as using On-Demand EC2 instances is not cost-effective. It is better to use a Lambda function instead.

References:

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

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

<https://aws.amazon.com/blogs/compute/new-aws-lambda-controls-for-stream-processing-and-asynchronous-invocations/>

AWS Lambda Overview - Serverless Computing in AWS:

<https://www.youtube.com/watch?v=bPVX1zHwAnY>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

---

## QUESTION 115

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.

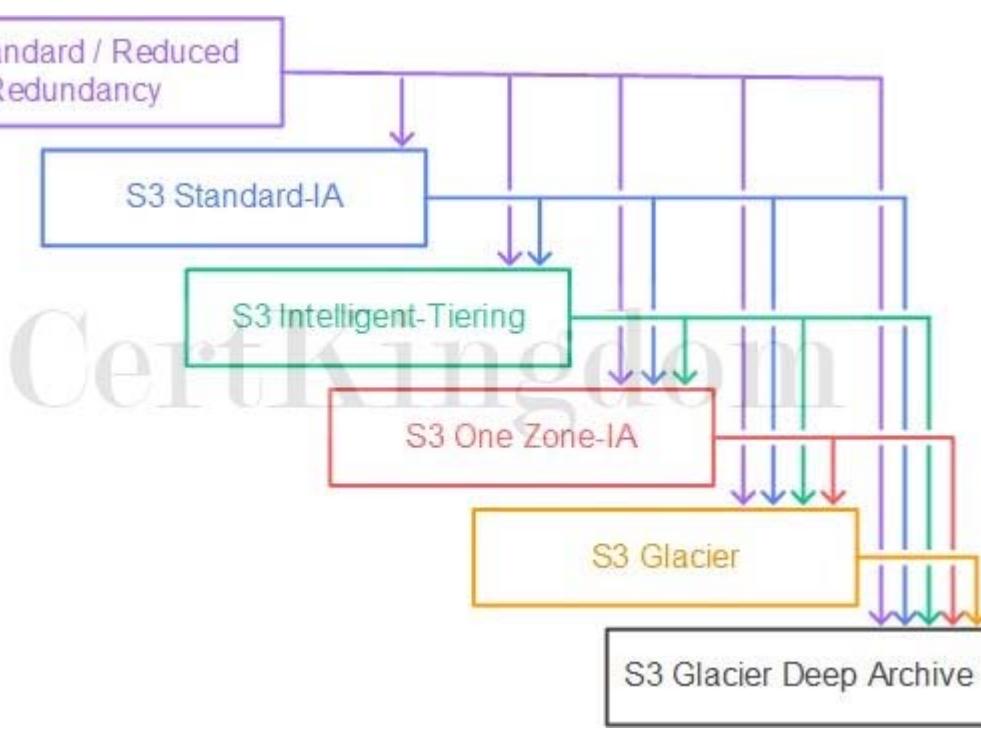
Which of the following approach can be used to fulfill this requirement? (Select TWO.)

- A. Use Amazon S3 and create a lifecycle policy that will move the objects to Amazon S3 Standard-IA after 2 years.
- B. Use Amazon EBS volumes to store the files. Configure the Amazon Data Lifecycle Manager (DLM) to schedule snapshots of the volumes after 2 years.
- 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.
- D. Use Amazon EFS and create a lifecycle policy that will move the objects to Amazon EFS-IA after 2 years.
- E. Use Amazon S3 and create a lifecycle policy that will move the objects to Amazon S3 Glacier after 2 years.

Answer: A,E

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/>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

## QUESTION 116

A company is using AWS Fargate to run a batch job whenever an object is uploaded to an Amazon S3 bucket. The minimum ECS task count is initially set to 1 to save on costs and should only be increased

based on new objects uploaded to the S3 bucket.

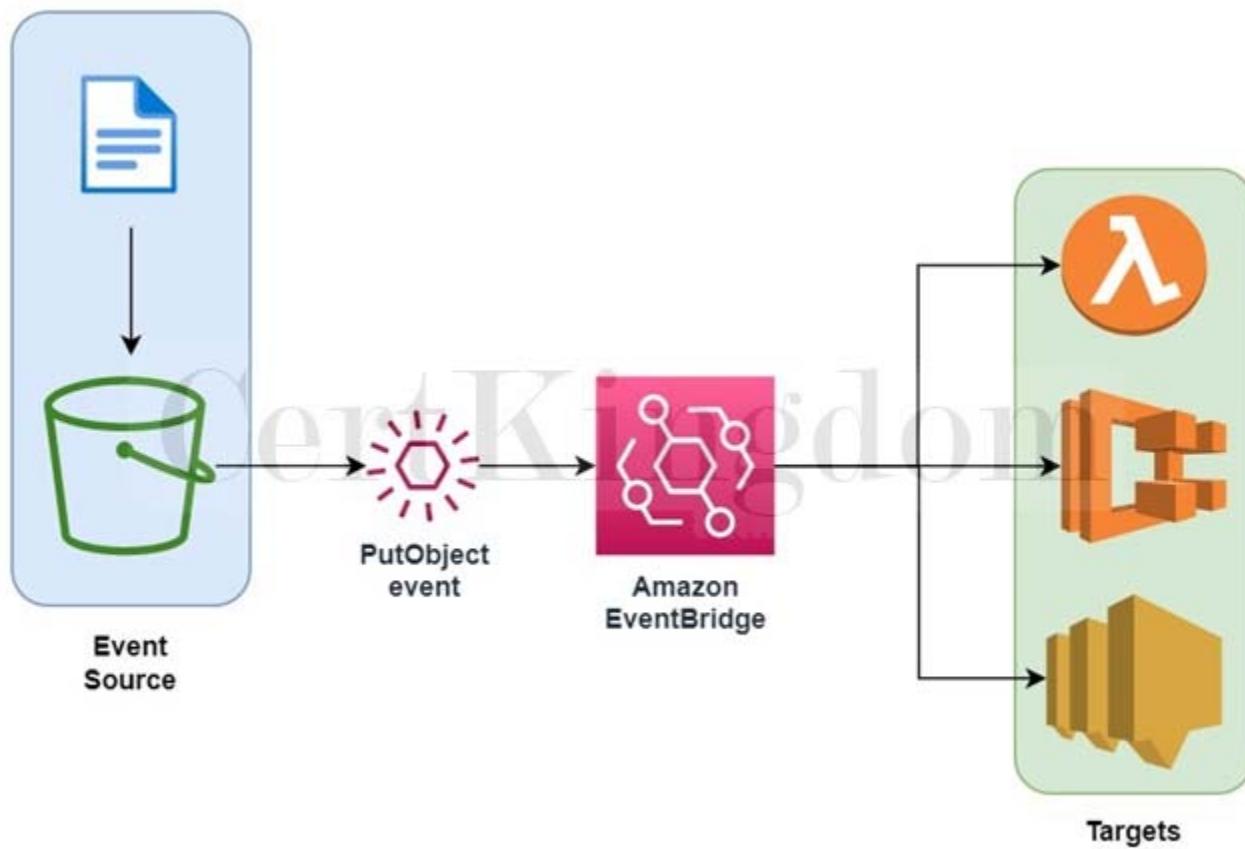
Which is the most suitable option to implement with the LEAST amount of effort?

- A. Set up an alarm in Amazon CloudWatch to monitor S3 object-level operations that are recorded on CloudTrail. Create an Amazon EventBridge rule that triggers the ECS cluster when new CloudTrail events are detected.
- B. Set up an alarm in CloudWatch to monitor S3 object-level operations recorded on CloudTrail. Set two alarm actions to update the ECS task count to scale-out/scale-in depending on the S3 event.
- C. Set up an Amazon EventBridge rule to detect S3 object PUT operations and set the target to a Lambda function that will run the StartTask API command.
- D. Set up an Amazon EventBridge rule to detect S3 object PUT operations and set the target to the ECS cluster to run a new ECS task.

Answer: D

Explanation:

Amazon EventBridge (formerly called CloudWatch Events) is a serverless event bus that makes it easy to connect applications together. It uses data from your own applications, integrated software as a service (SaaS) applications, and AWS services. This simplifies the process of building event-driven architectures by decoupling event producers from event consumers. This allows producers and consumers to be scaled, updated, and deployed independently. Loose coupling improves developer agility in addition to application resiliency.



You can use Amazon EventBridge to run Amazon ECS tasks when certain AWS events occur. You can set up an EventBridge rule that runs an Amazon ECS task whenever a file is uploaded to a certain Amazon S3 bucket using the Amazon S3 PUT operation.

Hence, the correct answer is: Set up an Amazon EventBridge rule to detect S3 object PUT operations and set the target to the ECS cluster to run a new ECS task.

The option that says: Set up an Amazon EventBridge rule to detect S3 object PUT operations and set the target to a Lambda function that will run the StartTask API command is incorrect. 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 tasks directly as targets 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 Amazon CloudWatch to monitor S3 object-level operations that are recorded on CloudTrail. Create an Amazon EventBridge rule that triggers the ECS cluster when new CloudTrail events are detected is incorrect because using CloudTrail and CloudWatch Alarm creates an unnecessary complexity to what you want to achieve. Amazon EventBridge 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 scaleout/scale-in depending on the S3 event is incorrect because you can't directly set CloudWatch Alarms to update the ECS task count.

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>

Check out this Amazon CloudWatch Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudwatch/>

Amazon CloudWatch Overview:

<https://youtu.be/q0DmxfyGkeU>

---

## QUESTION 117

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?

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

Answer: A

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"> <li>- Best for <b>transactional workloads</b></li> <li>- Critical business applications that require sustained IOPS performance</li> <li>- Large database workloads such as MongoDB, Oracle, Microsoft SQL Server and many others...</li> </ul>	<ul style="list-style-type: none"> <li>- Best for <b>large streaming workloads</b> requiring consistent, fast throughput at a low price</li> <li>- Big data, Data warehouses, Log processing</li> <li>- Throughput-oriented storage for large volumes of data that is <i>infrequently accessed</i></li> </ul>
Cost	moderate / high 	low 
Dominant Performance Attribute	IOPS	Throughput (MiB/s)



TutorialsDojo

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.

Volume Type	Solid-State Drives (SSD)		Hard Disk Drives (HDD)	
	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"> <li>• Recommended for most workloads</li> <li>• System boot volumes</li> <li>• Virtual desktops</li> <li>• Low-latency interactive apps</li> <li>• Development and test environments</li> </ul>	<ul style="list-style-type: none"> <li>• Critical business applications that require sustained IOPS performance, or more than 16,000 IOPS or 250 MiB/s of throughput per volume</li> <li>• Large database workloads, such as:           <ul style="list-style-type: none"> <li>▪ MongoDB</li> <li>▪ Cassandra</li> <li>▪ Microsoft SQL Server</li> <li>▪ MySQL</li> <li>▪ PostgreSQL</li> <li>▪ Oracle</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Streaming workloads requiring consistent, fast throughput at a low price</li> <li>• Big data</li> <li>• Data warehouses</li> <li>• Log processing</li> <li>• Cannot be a boot volume</li> </ul>	<ul style="list-style-type: none"> <li>• Throughput-oriented storage for large volumes of data that is infrequently accessed</li> <li>• Scenarios where the lowest storage cost is important</li> <li>• Cannot be a boot volume</li> </ul>
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.

References:

[https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes\\_piops](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_piops)

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

Amazon EBS Overview - SSD vs HDD:

<https://youtu.be/LW7x8wyLFvw>

Check out this Amazon EBS Cheat Sheet:

<https://tutorialsdojo.com/amazon-ebs/>

---

### QUESTION 118

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?

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

Answer: D

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.

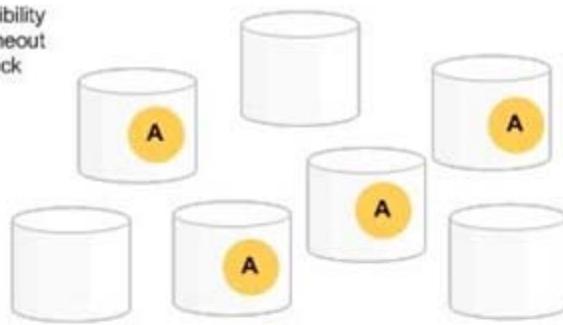
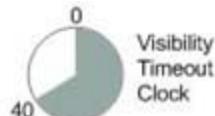
There are three main parts in a distributed messaging system:

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.

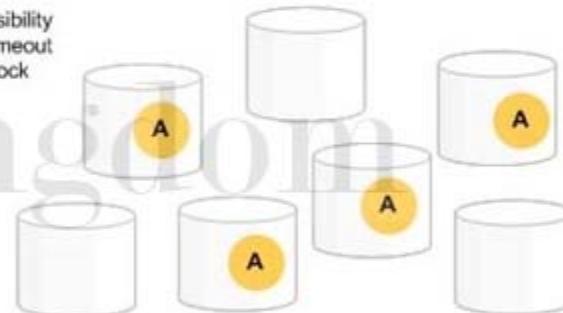
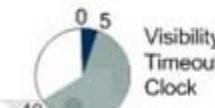
1

Component 1 sends Message A to the queue



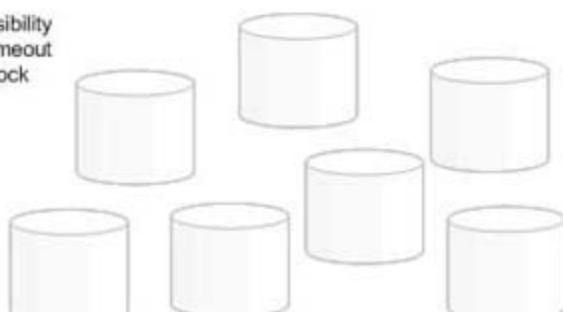
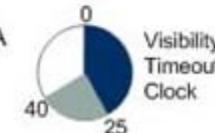
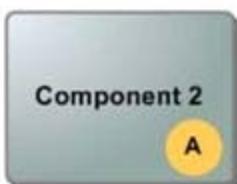
2

Component 2 retrieves Message A from the queue and the visibility timeout period starts



3

Component 2 processes Message A and then deletes it from the queue during the visibility timeout period



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>

Check out this Amazon SQS Cheat Sheet:

<https://tutorialsdojo.com/amazon-sqs/>

## QUESTION 119

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?

- A. 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.
- B. 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.
- 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.
- D. 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.

Answer: A

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 Kernelbased 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 I

A. 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>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

---

## QUESTION 120

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.)

A. AWS Directory Service AD Connector

B. IAM Groups

C. AWS Directory Service Simple AD

D. IAM Roles

E. Lambda

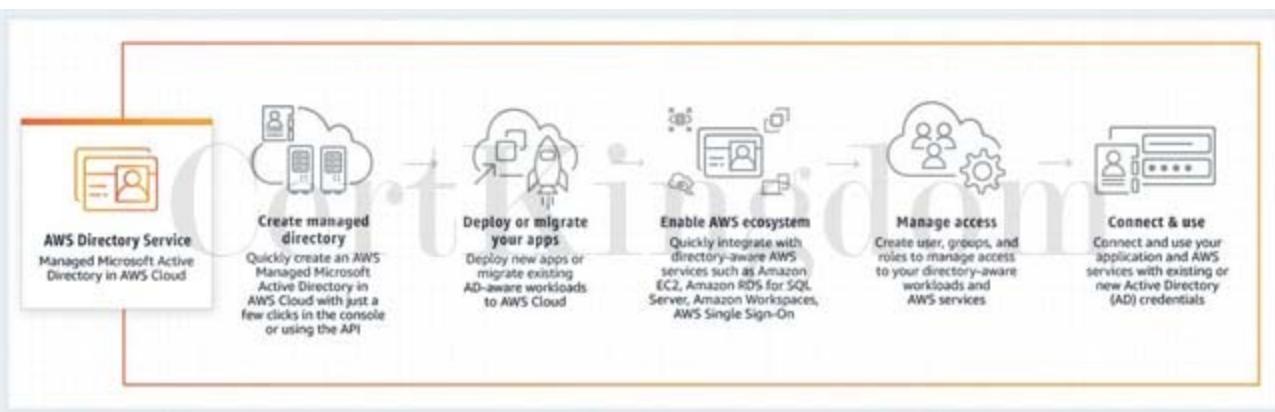
Answer: A,D

## 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 Kerberosbased 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/>

Check out these AWS IAM and Directory Service Cheat Sheets:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

<https://tutorialsdojo.com/aws-directory-service/>

Here is a video tutorial on AWS Directory Service:

<https://youtu.be/XeqotTYBtY>

## QUESTION 121

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?

- A. RDS DB instance running as a Multi-AZ deployment
- B. RDS Read Replica
- C. DynamoDB Read Replica
- D. CloudFront running as a Multi-AZ deployment

Answer: A

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/>

Amazon RDS Overview:

<https://youtu.be/aZmpL18K1UU>

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

## QUESTION 122

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.)

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

C. 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.

D. Consolidate all of the company's accounts using AWS Organizations.

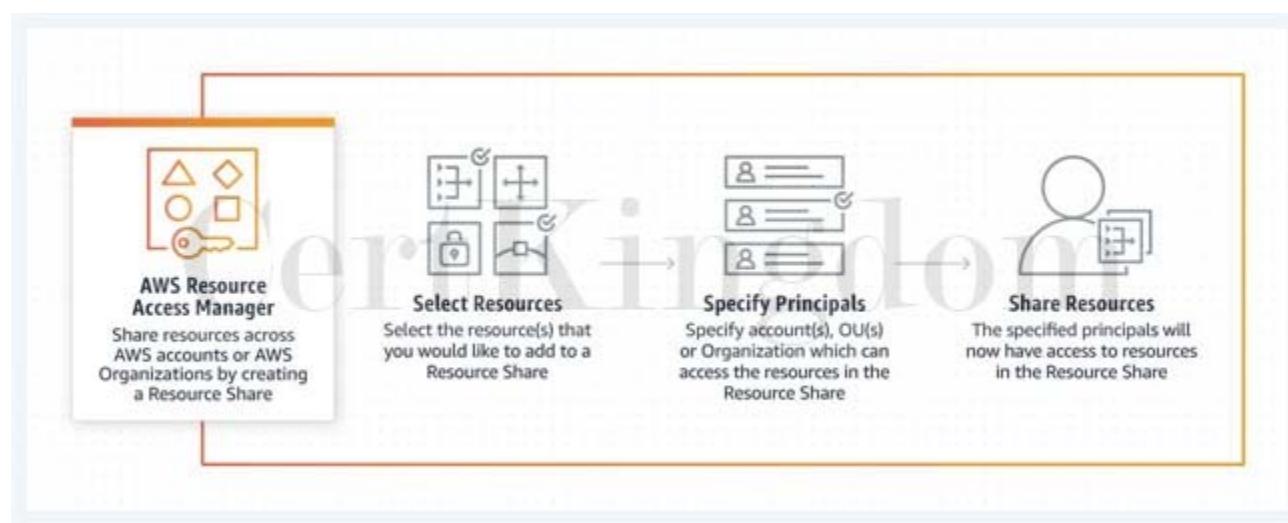
E. Use AWS Control Tower to easily and securely share your resources with your AWS accounts.

Answer: B,D

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. 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 crossaccount 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>

### QUESTION 123

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.

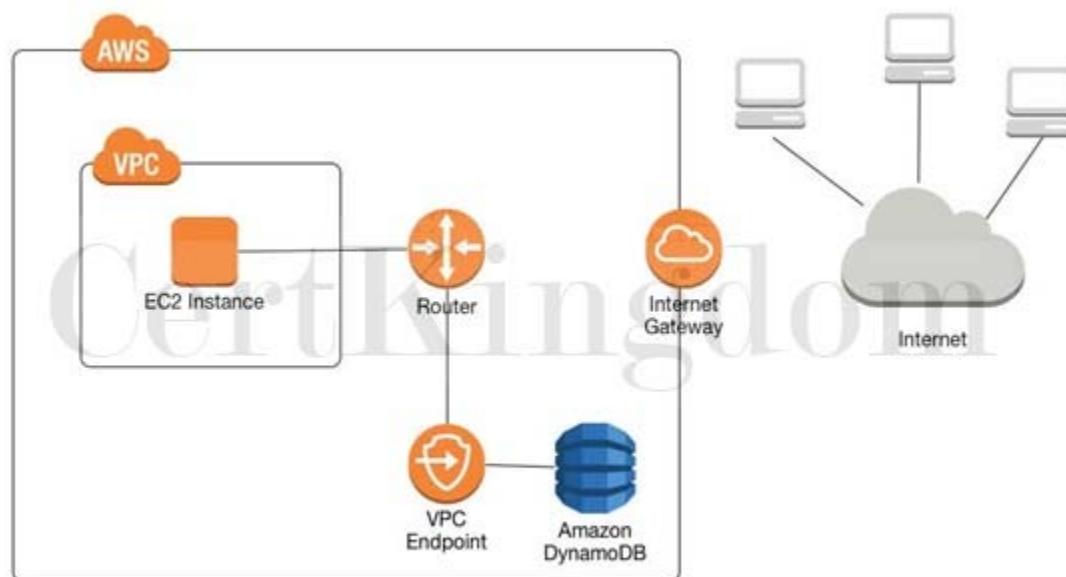
Which of the following can meet the above requirements?

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

Answer: A

#### 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>

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

---

## QUESTION 124

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?

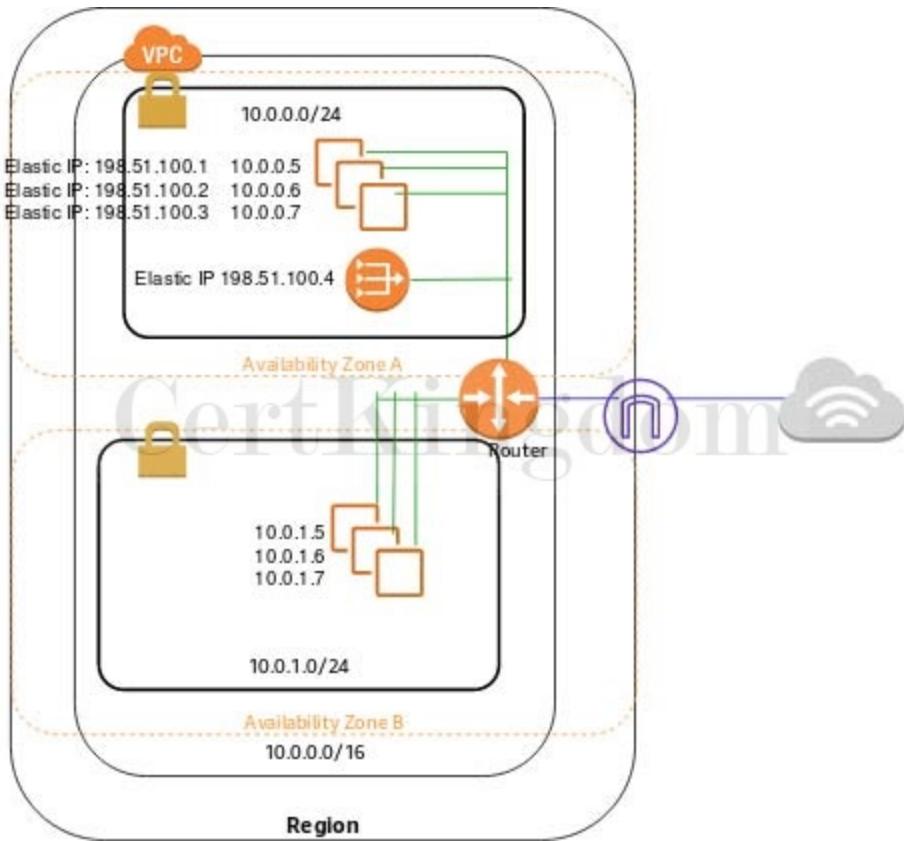
- A. Create two NAT Gateways in each availability zone. Configure the route table in each public subnet to ensure that instances use the NAT Gateway in the same availability zone.
- B. Create a NAT Gateway in each availability zone. Configure the route table in each public subnet to ensure that instances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

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>

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

## QUESTION 125

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?

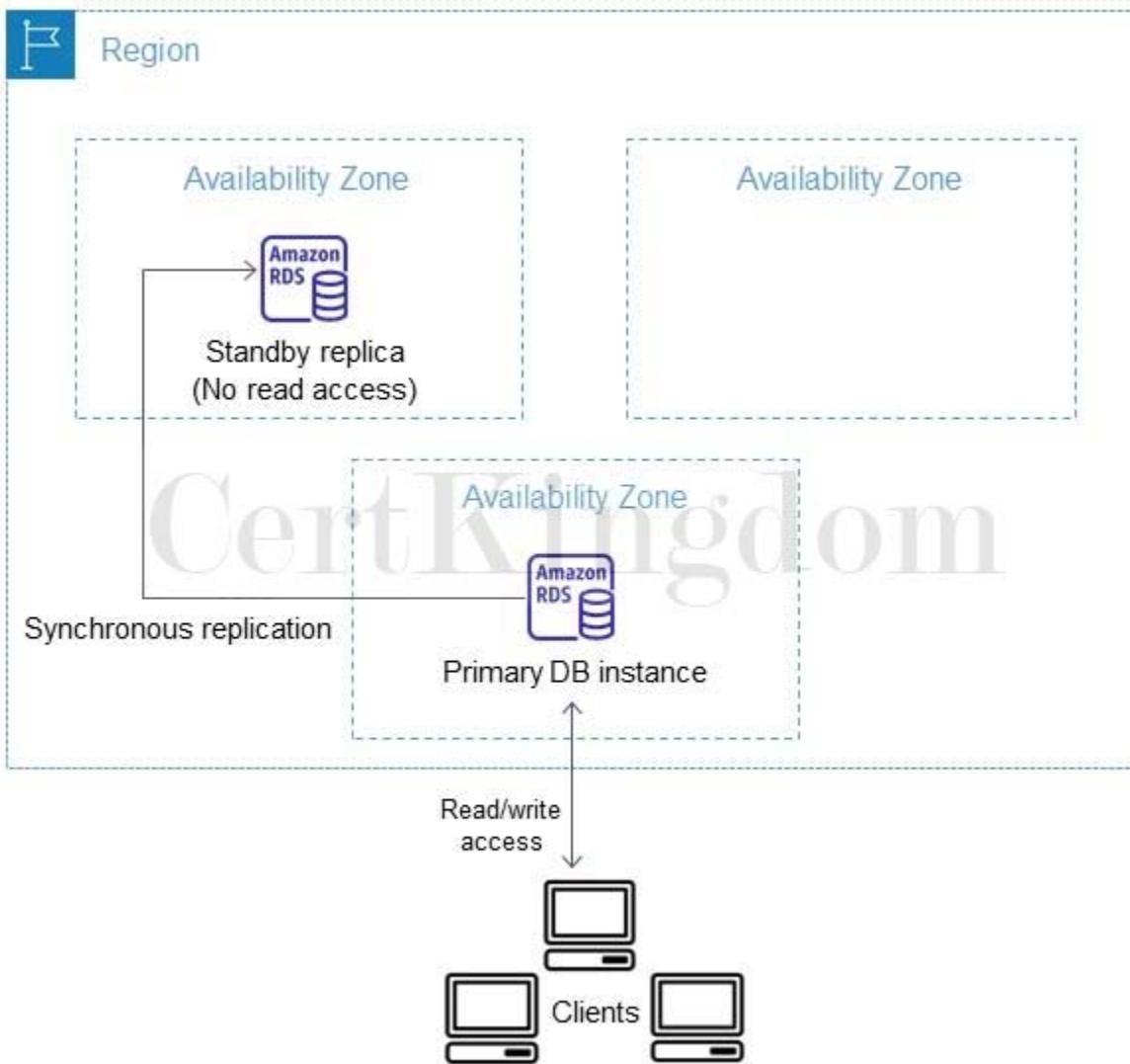
- A. Create an Oracle database in RDS with Multi-AZ deployments.

- B. 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.
- C. Launch an Oracle Real Application Clusters (RAC) in RDS.
- D. Launch an Oracle database instance in RDS with Recovery Manager (RMAN) enabled.

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. 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>

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

---

## QUESTION 126

A media company has an Amazon ECS Cluster, which uses the Fargate launch type, to host its news website. The application data are all stored in Amazon Keyspaces (for Apache Cassandra) with data-at-rest encryption enabled. 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?

A. In the ECS task definition file of the ECS Cluster, store the database credentials to Amazon ECS Anywhere to centrally manage these sensitive data and securely transmit it to only those containers that need access to it. Allocate an IAM Role to the cluster to ensure that the passwords are only accessible by the ECS service tasks. Run the AWS IAM Access Analyzer to verify that the credentials can't be viewed in plaintext.

B. Use the AWS Secrets Manager to store the database credentials and then encrypt them using AWS Certificate Manager (ACM). 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 ACM 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.

C. 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 Amazon Quantum Ledger Database (Amazon QLDB). Create an IAM role to the ECS task definition script that allows access to the Amazon QLDB and then pass the --cli-input-json parameter when calling the ECS register-task-definition action. Reference the task definition JSON file in the Amazon QLDB which contains the database credentials.

D. 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.

Answer: D

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 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 to Amazon ECS Anywhere to centrally manage these sensitive data and securely transmit it to only those containers that need access to it. Allocate an IAM Role to the cluster to ensure that the passwords are only accessible by the ECS service tasks. Run the AWS IAM Access Analyzer to verify that the credentials can't be viewed in plaintext is incorrect. Amazon Elastic Container Service (ECS) Anywhere is just a feature of Amazon ECS that enables you to easily run and manage container workloads on customer-managed infrastructure. This feature is not capable of storing any kind of credentials, let alone centrally manage your sensitive data. The recommended way to secure sensitive data in AWS is either through the use of Secrets Manager or Systems Manager Parameter Store. In addition, the AWS IAM Access Analyzer is primarily used to identify resources in your organization and accounts that are shared with an external entity, as well as to validate your IAM policies. This service can't verify if your database credentials are viewable in plaintext or not.

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 Amazon Quantum Ledger Database (Amazon QLDB). Create an IAM role to the ECS task definition script that allows access to the Amazon QLDB and then pass the --cli-input-json parameter when calling the ECS register-task-definition action. Reference the task definition JSON file in the Amazon QLDB which contains the database credentials is incorrect. Amazon Quantum Ledger Database (QLDB) is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log. This service is not meant to store your sensitive database credentials.

The option that says: Use the AWS Secrets Manager to store the database credentials and then encrypt

them using AWS Certificate Manager (ACM). 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 ACM 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. Although the use of Secrets Manager in securing sensitive data in ECS is valid, Amazon ECS doesn't support resource-based policies. An example of a resource-based policy is the S3 bucket policy. An ECS task assumes an execution role (IAM role) to be able to call other AWS services like AWS Secrets Manager on your behalf. In addition, you cannot encrypt database credentials using the AWS Certificate Manager (ACM) service. You have to use AWS KMS instead.

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/>

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

1

Check out these Amazon ECS and AWS Systems Manager Cheat Sheets:

<https://tutorialsdojo.com/amazon-elastic-container-service-amazon-ecs/>

<https://tutorialsdojo.com/aws-systems-manager/>

---

## QUESTION 127

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.)

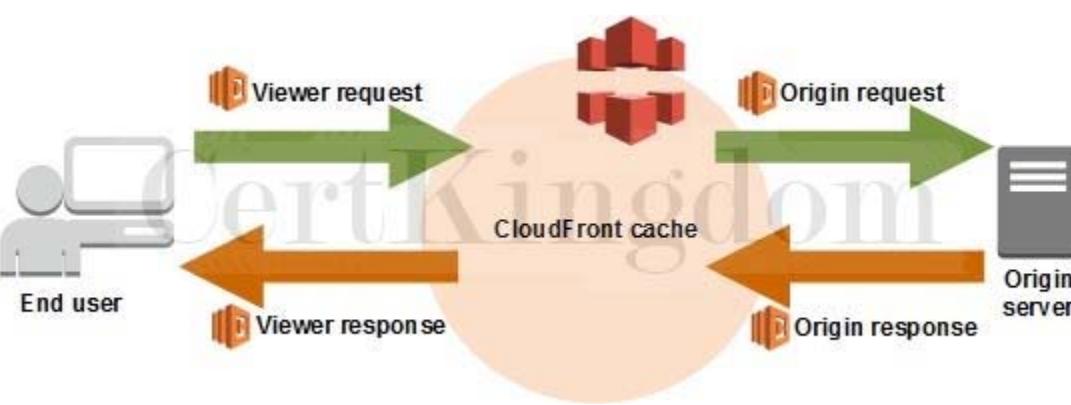
- A. Deploy your application to multiple AWS regions to accommodate your users around the world. Set up a Route 53 record with latency routing policy to route incoming traffic to the region that provides the best latency to the user.
- B. Set up an origin failover by creating an origin group with two 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.
- C. 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.
- D. 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.
- E. 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.

Answer: B,E

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. 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/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.html)

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

Check out these Amazon CloudFront and AWS Lambda Cheat Sheets:

<https://tutorialsdojo.com/amazon-cloudfront/>

<https://tutorialsdojo.com/aws-lambda/>

---

#### QUESTION 128

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?

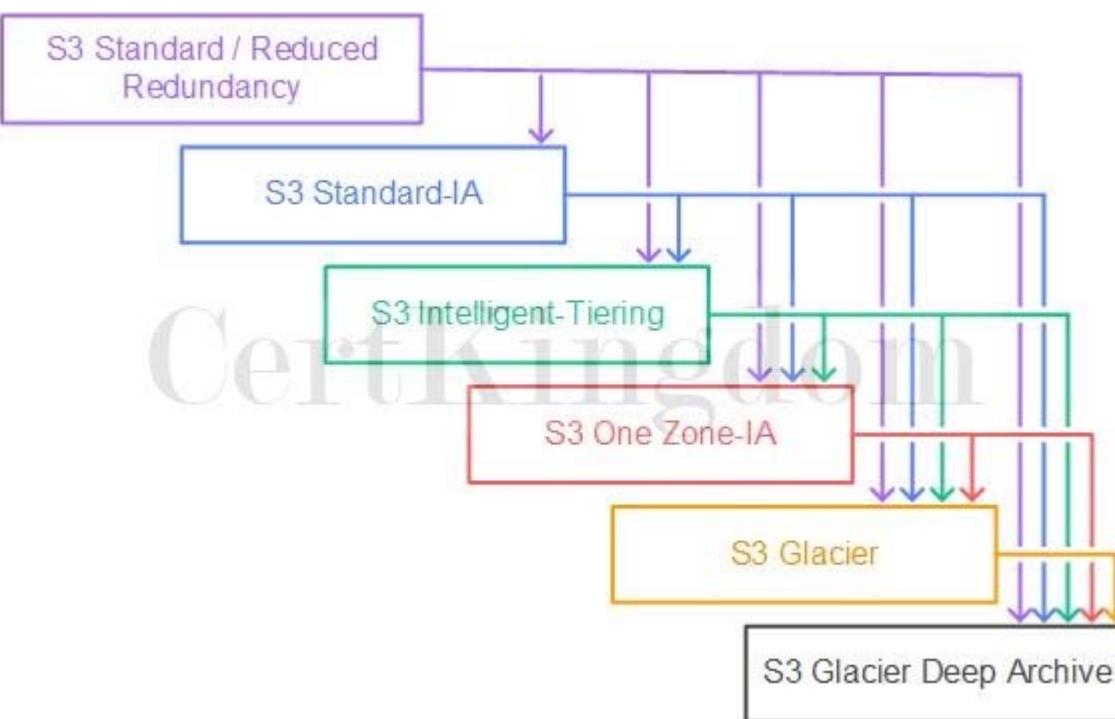
- A. Attach an instance store volume in your existing EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to Amazon S3 Glacier.
- B. Attach an instance store volume in your EC2 instance. Use Amazon S3 to store your backup data and configure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

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/>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

Tutorials Dojo's AWS Storage Services Cheat Sheets:

<https://tutorialsdojo.com/aws-cheat-sheets-storage-services/>

---

## QUESTION 129

A content management system (CMS) is hosted on a fleet of auto-scaled, On-Demand EC2 instances that use Amazon Aurora as its database. Currently, the system stores the file documents that the users upload 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-available POSIX-compliant shared file system?

- A. Create an S3 bucket and use this as the storage for the CMS
- B. Use EFS
- C. Use ElastiCache
- D. Upgrading your existing EBS volumes to Provisioned IOPS SSD Volumes

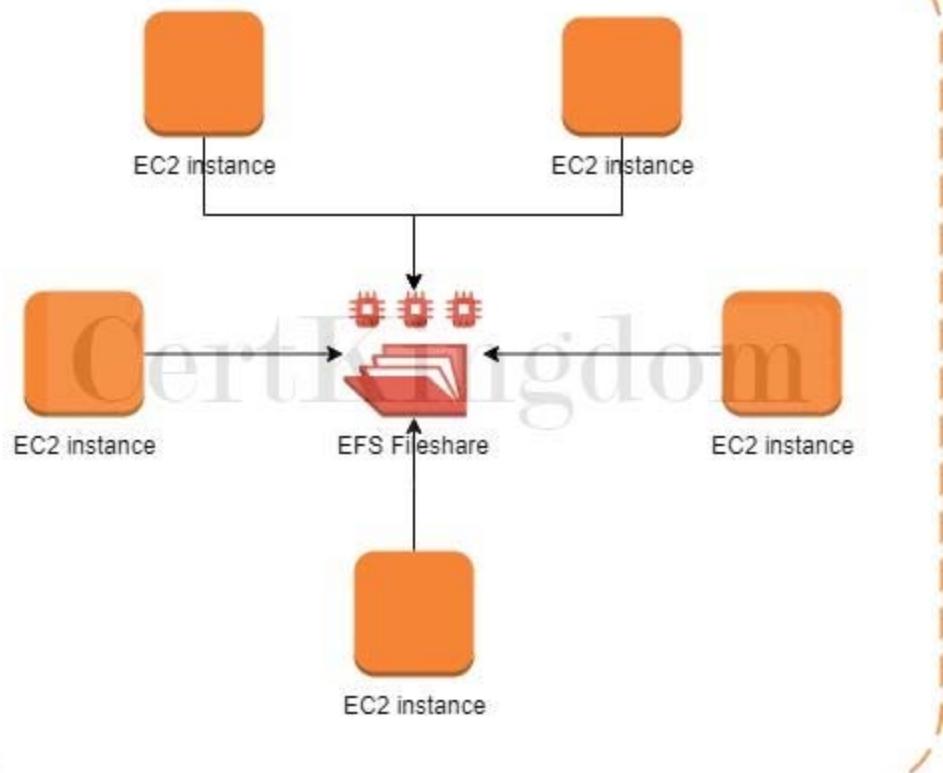
Answer: B

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 store 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 parallel shared access to the file documents.

Although an EBS Volume can be attached to multiple EC2 instances, you can only do so on instances within an availability zone. What we need is high-available storage that can span multiple availability zones. Take note as well that the type of storage needed here is "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 an EBS volume is a storage area network (SAN) storage and not a POSIX-compliant shared file system. 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/>

Check out this Amazon EFS Cheat Sheet:

<https://tutorialsdojo.com/amazon-efs/>

Check out this Amazon S3 vs EBS vs EFS Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3-vs-ebs-vs-efs/>

### QUESTION 130

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?

- A. Use scheduled scaling.
- B. Use target tracking scaling.
- C. Use simple scaling.
- D. Use suspend and resume scaling.

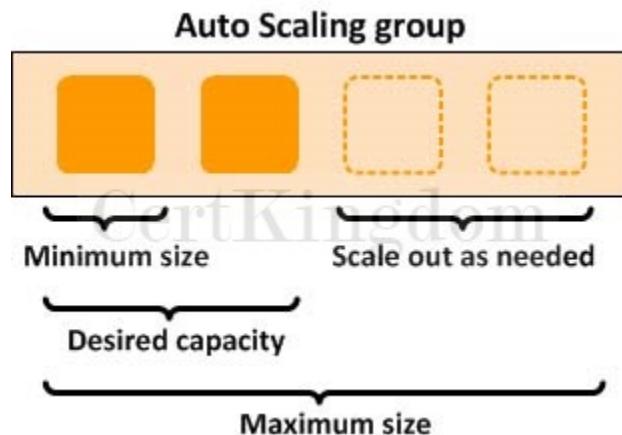
Answer: B

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>

Check out this AWS Auto Scaling Cheat Sheet:

<https://tutorialsdojo.com/aws-auto-scaling/>

## QUESTION 131

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 data containing personally identifiable information (PII) in a manner that meets their compliance standards. They should also be alerted if there are potential policy violations with the privacy of their S3 buckets.

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

- A. Set up and configure Amazon Polly to scan for usage patterns on Amazon S3 data

- B. Set up and configure Amazon Macie to monitor their Amazon S3 data.
- C. Set up and configure Amazon Kendra to monitor malicious activity on their Amazon S3 data
- D. Set up and configure Amazon Fraud Detector to send out alert notifications whenever a security violation is detected on their Amazon S3 data.

Answer: B

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 generates two categories of findings: policy findings and sensitive data findings. A policy finding is a detailed report of a potential policy violation or issue with the security or privacy of an Amazon S3 bucket. Macie generates these findings as part of its ongoing monitoring activities for your Amazon S3 data. A sensitive data finding is a detailed report of sensitive data in an S3 object. Macie generates these findings when it discovers sensitive data in S3 objects that you configure a sensitive data discovery job to analyze.

Hence, the correct answer is: Set up and configure Amazon Macie to monitor their Amazon S3 data. The option that says: Set up and configure Amazon Polly to scan for usage patterns on Amazon S3 data is incorrect because Amazon Polly is simply a service that turns text into lifelike speech, allowing you to create applications that talk, and build entirely new categories of speech-enabled products. Polly can't be used to scan usage patterns on your S3 data.

The option that says: Set up and configure Amazon Kendra to monitor malicious activity on their Amazon S3 data is incorrect. Amazon Kendra is just an enterprise search service that allows developers to add search capabilities to their applications. This enables their end users to discover information stored within the vast amount of content spread across their company, but not monitor malicious activity on their S3 buckets.

The option that says: Set up and configure Amazon Fraud Detector to send out alert notifications whenever a security violation is detected on their Amazon S3 data is incorrect because the Amazon Fraud Detector is only a fully managed service for identifying potentially fraudulent activities and for catching more online fraud faster. It does not check any S3 data containing personally identifiable information (PII), unlike Amazon Macie.

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>

Check out this Amazon Macie Cheat Sheet:

<https://tutorialsdojo.com/amazon-macie/>

AWS Security Services Overview - Secrets Manager, ACM, Macie:

<https://youtu.be/ogVamzF2Dzk>

---

## QUESTION 132

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?

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

Answer: B

Explanation:

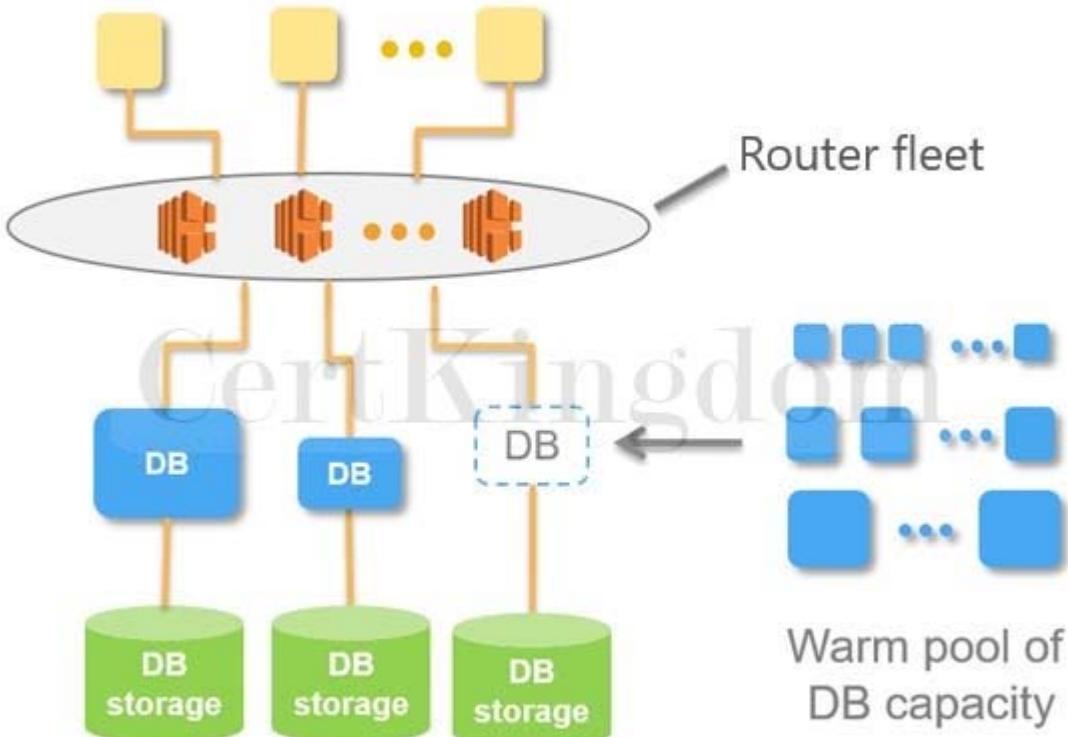
Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora. An Aurora Serverless DB cluster is a DB cluster that automatically starts up, shuts down, and scales up or down its compute capacity based on your application's needs. Aurora Serverless provides a relatively simple, 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.

## Applications



## Aurora Database Storage

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. 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:

## QUESTION 133

A company is using a combination of API Gateway and Lambda for the web services of the online web portal that is being accessed by hundreds of thousands of clients each day. They will be announcing a new revolutionary product and it is expected that the web portal will receive a massive number of visitors all around the globe.

How can you protect the backend systems and applications from traffic spikes?

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

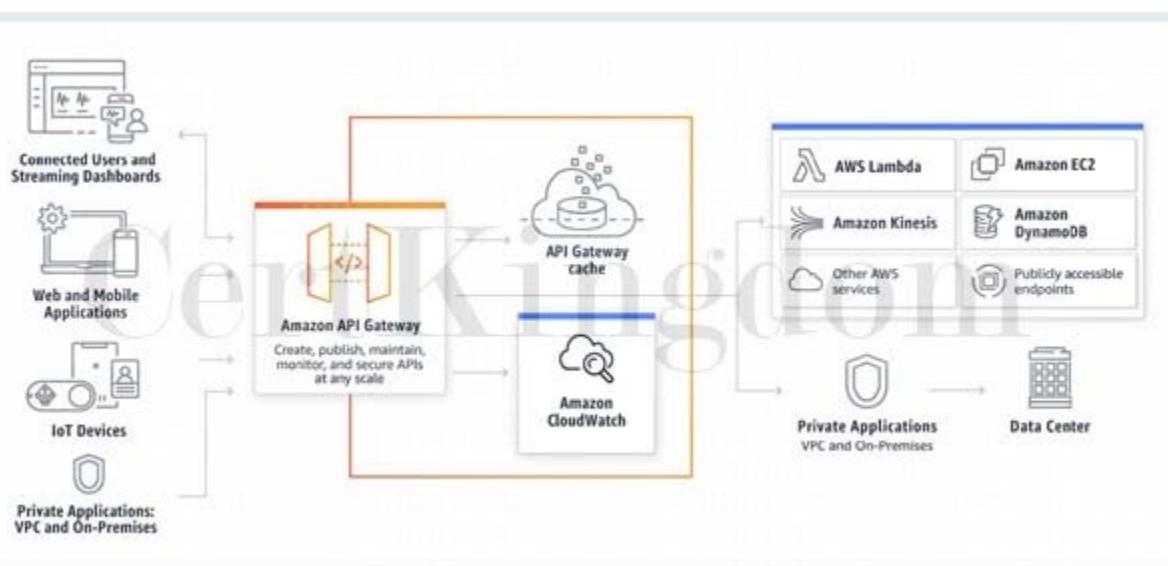
Answer: C

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.



Hence, the correct answer is: Use throttling limits in API Gateway.

The option that says: API Gateway will automatically scale and handle massive traffic spikes so you do not have to do anything is incorrect. 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](https://aws.amazon.com/api-gateway/faqs/#Throttling_and_Caching)

Check out this Amazon API Gateway Cheat Sheet:

<https://tutorialsdojo.com/amazon-api-gateway/>

## QUESTION 134

A company has a cryptocurrency exchange portal that is hosted in an Auto Scaling group of EC2 instances behind an Application Load Balancer and is deployed across multiple AWS regions. The users can be found all around the globe, but the majority are from Japan and Sweden. Because of the compliance requirements in these two locations, you want the Japanese users to connect to the servers in the ap-northeast-1 Asia Pacific (Tokyo) region, while the Swedish users should be connected to the servers in the eu-west-1 EU (Ireland) region.

Which of the following services would allow you to easily fulfill this requirement?

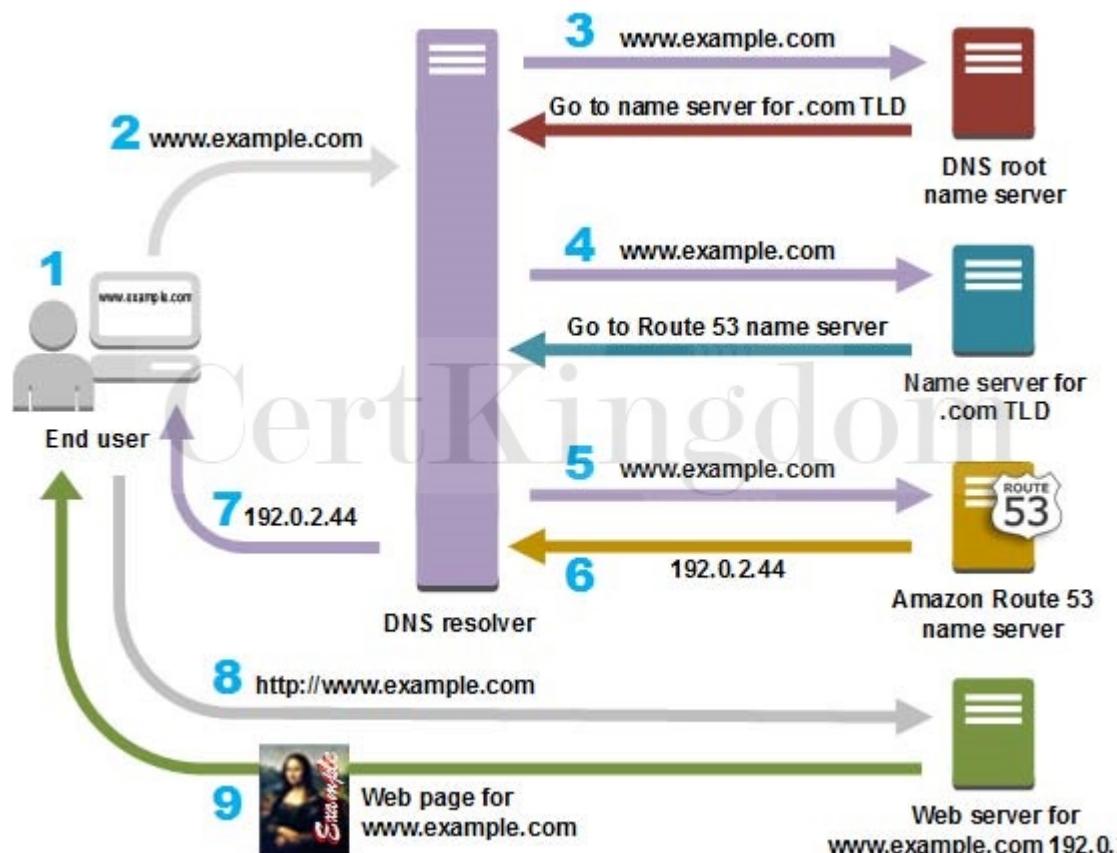
- A. Use Route 53 Geolocation Routing policy.
- B. Use Route 53 Weighted Routing policy.
- C. Set up an Application Load Balancers that will automatically route the traffic to the proper AWS region.
- D. Set up a new CloudFront web distribution with the geo-restriction feature enabled.

Answer: A

Explanation:

Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from. For example, you might want all queries from Europe to be routed to an ELB load balancer in the Frankfurt region.

When you use geolocation routing, you can localize your content and present some or all of your website in the language of your users. You can also use geolocation routing to restrict distribution of content to only the locations in which you have distribution rights. Another possible use is for balancing load across endpoints in a predictable, easy-to-manage way, so that each user location is consistently routed to the same endpoint.



Setting up an Application Load Balancers that will automatically route the traffic to the proper AWS region is incorrect because Elastic Load Balancers distribute traffic among EC2 instances across multiple Availability Zones but not across AWS regions.

Setting up a new CloudFront web distribution with the geo-restriction feature enabled is incorrect

because the CloudFront geo-restriction feature is primarily used to prevent users in specific geographic locations from accessing content that you're distributing through a CloudFront web distribution. It does not let you choose the resources that serve your traffic based on the geographic location of your users, unlike the Geolocation routing policy in Route 53.

Using Route 53 Weighted Routing policy is incorrect because this is not a suitable solution to meet the requirements of this scenario. It just lets you associate multiple resources with a single domain name ([tutorialsdojo.com](https://tutorialsdojo.com)) or subdomain name ([forums.tutorialsdojo.com](https://forums.tutorialsdojo.com)) and choose how much traffic is routed to each resource. You have to use a Geolocation routing policy instead.

References:

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

<https://aws.amazon.com/premiumsupport/knowledge-center/geolocation-routing-policy>

Check out this Amazon Route 53 Cheat Sheet:

<https://tutorialsdojo.com/amazon-route-53/>

Latency Routing vs Geoproximity Routing vs Geolocation Routing:

<https://tutorialsdojo.com/latency-routing-vs-geoproximity-routing-vs-geolocation-routing/>

Comparison of AWS Services Cheat Sheets:

<https://tutorialsdojo.com/comparison-of-aws-services/>

---

### QUESTION 135

A Data Engineer is working for a litigation firm for their case history application. The engineer needs to keep track of all the cases that the firm has handled. The static assets like .jpg, .png, and .pdf files are stored in S3 for cost efficiency and high durability. As these files are critical to the business, the engineer wants to keep track of what's happening in the S3 bucket. The engineer found out that S3 has an event notification whenever a delete or write operation happens within the S3 bucket.

What are the possible Event Notification destinations available for S3 buckets? (Select TWO.)

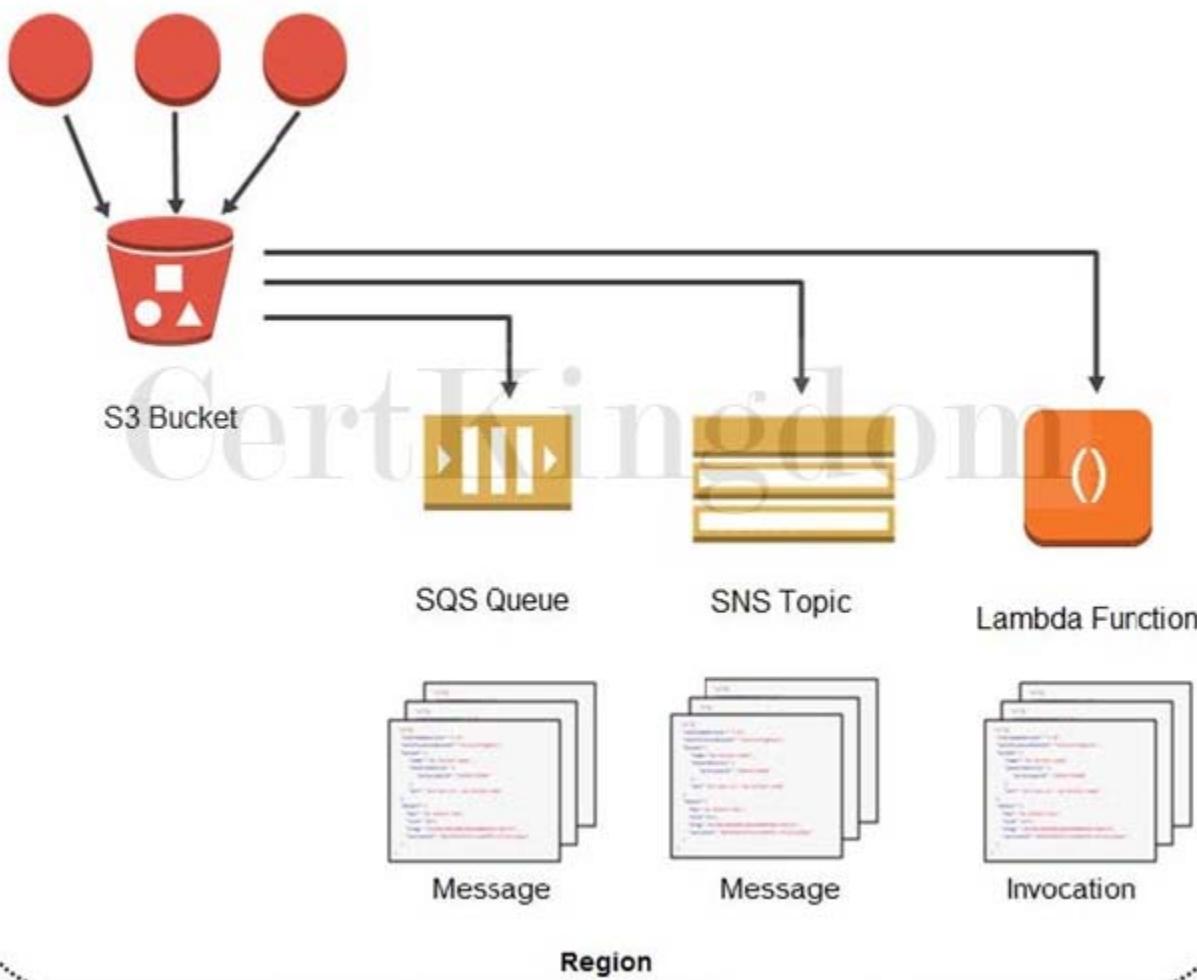
- A. Kinesis
- B. SQS
- C. SES
- D. SWF
- E. Lambda function

Answer: B,E

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 identifying the events you want Amazon S3 to publish, and the destinations where you want Amazon S3 to send the event notifications.

## Incoming Objects



Region

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

Amazon Simple Notification Service (Amazon SNS) topic - A web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients.

Amazon Simple Queue Service (Amazon SQS) queue - Offers reliable and scalable hosted queues for storing messages as they travel between computer.

AWS Lambda - AWS Lambda is a compute service where you can upload your code and the service can run the code on your behalf using the AWS infrastructure. You package up and upload your custom code to AWS Lambda when you create a Lambda function

Kinesis is incorrect because this is used to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information, and not used for event notifications. You have to use SNS, SQS or Lambda.

SES is incorrect because this is mainly used for sending emails designed to help digital marketers and application developers send marketing, notification, and transactional emails, and not for sending event notifications from S3. You have to use SNS, SQS or Lambda.

SWF is incorrect because this is mainly used to build applications that use Amazon's cloud to coordinate work across distributed components and not used as a way to trigger event notifications from S3. You have to use SNS, SQS or Lambda.

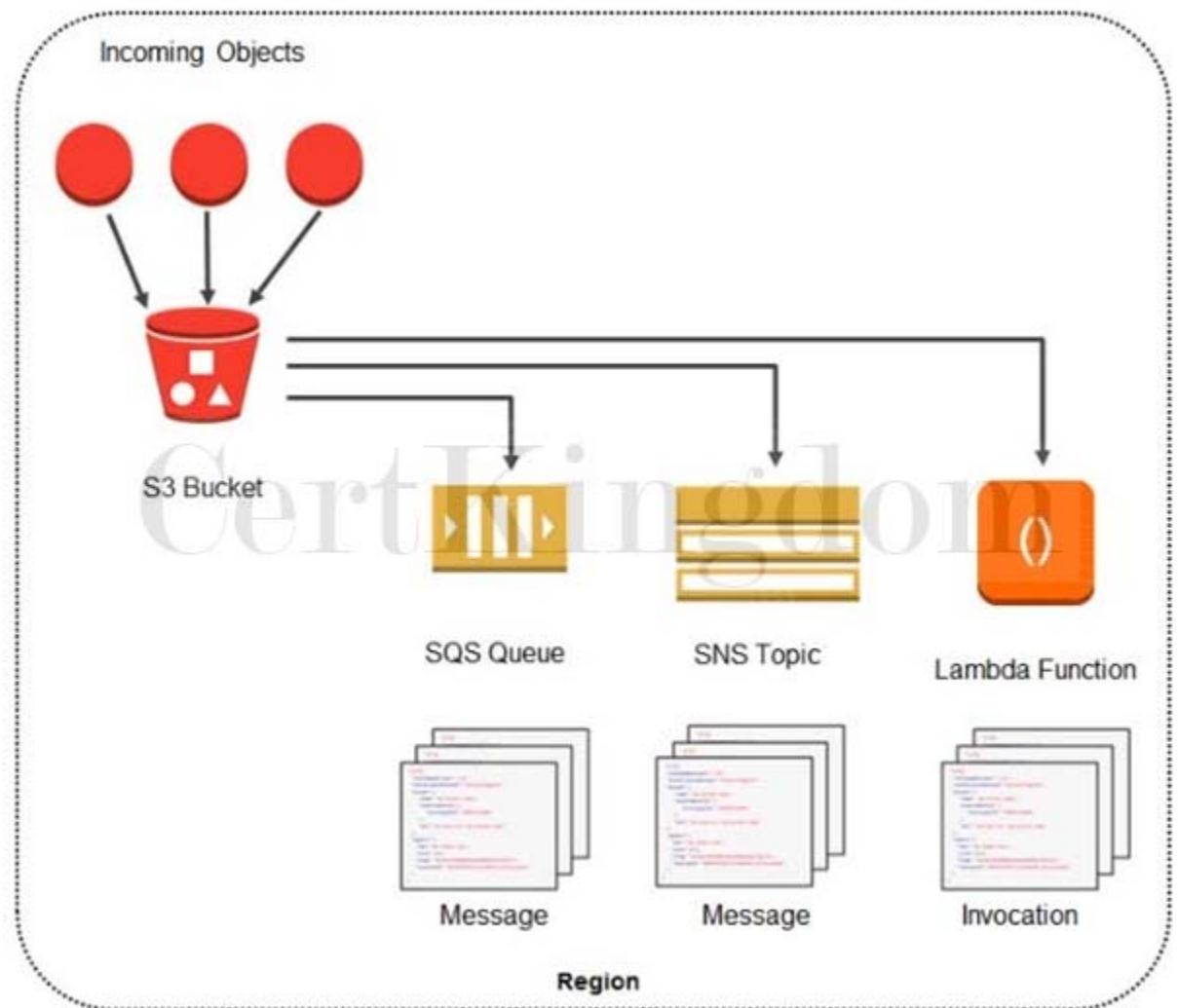
Here's what you need to do in order to start using this new feature with your application:

Create the queue, topic, or Lambda function (which I'll call the target for brevity) if necessary.

Grant S3 permission to publish to the target or invoke the Lambda function. For SNS or SQS, you do this by applying an appropriate policy to the topic or the queue. For Lambda, you must create and supply an IAM role, then associate it with the Lambda function.

Arrange for your application to be invoked in response to activity on the target. As you will see in a moment, you have several options here.

Set the bucket's Notification Configuration to point to the target.



Reference:

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

### QUESTION 136

A company has a requirement to move 80 TB data warehouse to the cloud. It would take 2 months to transfer the data given their current bandwidth allocation.

Which is the most cost-effective service that would allow you to quickly upload their data into AWS?

- A. AWS Direct Connect
- B. Amazon S3 Multipart Upload
- C. AWS Snowball Edge
- D. AWS Snowmobile

Answer: C

Explanation:

AWS Snowball Edge is a type of Snowball device with on-board storage and compute power for select AWS capabilities. Snowball Edge can undertake local processing and edge-computing workloads in addition to transferring data between your local environment and the AWS Cloud.

Each Snowball Edge device can transport data at speeds faster than the internet. This transport is done

by shipping the data in the appliances through a regional carrier. The appliances are rugged shipping containers, complete with E Ink shipping labels. The AWS Snowball Edge device differs from the standard Snowball because it can bring the power of the AWS Cloud to your on-premises location, with local storage and compute functionality.

Snowball Edge devices have three options for device configurations ““ storage optimized, compute optimized, and with GPU.

Hence, the correct answer is: AWS Snowball Edge.

AWS Snowmobile is incorrect because this is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. It is not suitable for transferring a small amount of data, like 80 TB in this scenario. You can transfer up to 100PB per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck. A more cost-effective solution here is to order a Snowball Edge device instead.

AWS Direct Connect is incorrect because it is primarily used to establish a dedicated network connection from your premises network to AWS. This is not suitable for one-time data transfer tasks, like what is depicted in the scenario.

Amazon S3 Multipart Upload is incorrect because this feature simply enables you to upload large objects in multiple parts. It still uses the same Internet connection of the company, which means that the transfer will still take time due to its current bandwidth allocation.

References:

<https://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html>

<https://docs.aws.amazon.com/snowball/latest/ug/device-differences.html>

Check out this AWS Snowball Edge Cheat Sheet:

<https://tutorialsdojo.com/aws-snowball-edge/>

AWS Snow Family Overview:

<https://youtu.be/Ar-51Ip53Q>

---

### QUESTION 137

A Solutions Architect created a new Standard-class S3 bucket to store financial reports that are not frequently accessed but should immediately be available when an auditor requests them. To save costs, the Architect changed the storage class of the S3 bucket from Standard to Infrequent Access storage class.

In Amazon S3 Standard - Infrequent Access storage class, which of the following statements are true? (Select TWO.)

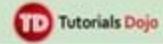
- A. It is designed for data that is accessed less frequently.
- B. Ideal to use for data archiving.
- C. It provides high latency and low throughput performance
- D. It is designed for data that requires rapid access when needed.
- E. It automatically moves data to the most cost-effective access tier without any operational overhead.

Answer: A,D

Explanation:

Amazon S3 Standard - Infrequent Access (Standard - IA) is an Amazon S3 storage class for data that is accessed less frequently, but requires rapid access when needed. Standard - IA offers the high durability, throughput, and low latency of Amazon S3 Standard, with a low per GB storage price and per GB retrieval fee.

	S3 Standard	S3 Standard-Infrequent Access (IA)	S3 One Zone-Infrequent Access (IA)	S3 Intelligent Tiering
Features	General-purpose storage of frequently accessed data	For long-lived, rapid but less frequently accessed data; data is stored redundantly in multiple AZs	For long-lived, rapid but less frequently accessed data; data is stored redundantly in only one AZ of your choice	For long-lived data that have unpredictable access patterns
Durability	99.999999999% (11.9's)	99.999999999% (11.9's)	99.999999999% (11.9's)	99.999999999% (11.9's)
Availability	99.99%	99.9%	99.5%	99.9%
Availability SLA	99.9%	99%	99%	99%
Number of Availability Zones	At least 3	At least 3	Only 1	At least 3
Minimum capacity charge per object	N/A	128KB	128KB	N/A
Minimum storage duration charge	N/A	30 days	30 days	30 days
Inserting data	Directly PUT into S3 Standard	Directly PUT into S3 Standard-IA or set Lifecycle policies to transition objects from the S3 Standard to the S3 Standard-IA storage class.	Directly PUT into S3 One Zone-IA or set Lifecycle policies to transition objects from the S3 Standard to the S3 One Zone-IA storage class.	Directly PUT into S3 Intelligent-Tiering or set Lifecycle policies to transition objects from the S3 Standard to the S3 Intelligent-Tiering storage class.
Retrieval fee	N/A	per GB retrieved	per GB retrieved	N/A
First byte latency	milliseconds	milliseconds	milliseconds	milliseconds
Storage transition	S3 Standard to all other S3 storage types including Glacier	S3 Standard-IA to S3 One Zone-IA or S3 Glacier	S3 One Zone-IA to S3 Glacier	S3 Intelligent to S3 One Zone-IA or S3 Glacier
Use Cases	Cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics.	Ideally suited for long-term file storage, older sync and share storage, and other aging data.	For infrequently-accessed storage, like backup copies, disaster recovery copies, or other easily recreatable data.	Data with unknown or changing access patterns, optimize storage costs automatically, and unpredictable workloads



This combination of low cost and high performance make Standard - IA ideal for long-term storage, backups, and as a data store for disaster recovery. The Standard - IA storage class is set at the object level and can exist in the same bucket as Standard, allowing you to use lifecycle policies to automatically transition objects between storage classes without any application changes.

#### Key Features:

- Same low latency and high throughput performance of Standard
- Designed for durability of 99.999999999% of objects
- Designed for 99.9% availability over a given year
- Backed with the Amazon S3 Service Level Agreement for availability
- Supports SSL encryption of data in transit and at rest
- Lifecycle management for automatic migration of objects

Hence, the correct answers are:

- It is designed for data that is accessed less frequently.
- It is designed for data that requires rapid access when needed.

The option that says: It automatically moves data to the most cost-effective access tier without any operational overhead is incorrect as it actually refers to Amazon S3 - Intelligent Tiering, which is the only cloud storage class that delivers automatic cost savings by moving objects between different access tiers when access patterns change.

The option that says: It provides high latency and low throughput performance is incorrect as it should be "low latency" and "high throughput" instead. S3 automatically scales performance to meet user demands.

The option that says: Ideal to use for data archiving is incorrect because this statement refers to Amazon S3 Glacier. Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup.

#### References:

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

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

## QUESTION 138

Both historical records and frequently accessed data are stored on an on-premises storage system. The amount of current data is growing at an exponential rate. As the storage's capacity is nearing its limit, the company's Solutions Architect has decided to move the historical records to AWS to free up space for the active data.

Which of the following architectures deliver the best solution in terms of cost and operational management?

- A. Use AWS Storage Gateway to move the historical records from on-premises to AWS. Choose Amazon S3 Glacier Deep Archive to be the destination for the data.
- B. Use AWS DataSync to move the historical records from on-premises to AWS. Choose Amazon S3 Glacier Deep Archive to be the destination for the data.
- C. Use AWS Storage Gateway to move the historical records from on-premises to AWS. Choose Amazon S3 Glacier to be the destination for the data. Modify the S3 lifecycle configuration to move the data from the Standard tier to Amazon S3 Glacier Deep Archive after 30 days.
- D. Use AWS DataSync to move the historical records from on-premises to AWS. Choose Amazon S3 Standard to be the destination for the data. Modify the S3 lifecycle configuration to move the data from the Standard tier to Amazon S3 Glacier Deep Archive after 30 days.

Answer: B

Explanation:

AWS DataSync makes it simple and fast to move large amounts of data online between on-premises storage and Amazon S3, Amazon Elastic File System (Amazon EFS), or Amazon FSx for Windows File Server. Manual tasks related to data transfers can slow down migrations and burden IT operations.

DataSync eliminates or automatically handles many of these tasks, including scripting copy jobs, scheduling, and monitoring transfers, validating data, and optimizing network utilization. The DataSync software agent connects to your Network File System (NFS), Server Message Block (SMB) storage, and your self-managed object storage, so you don't have to modify your applications.

DataSync can transfer hundreds of terabytes and millions of files at speeds up to 10 times faster than open-source tools, over the Internet or AWS Direct Connect links. You can use DataSync to migrate active data sets or archives to AWS, transfer data to the cloud for timely analysis and processing, or replicate data to AWS for business continuity. Getting started with DataSync is easy: deploy the DataSync agent, connect it to your file system, select your AWS storage resources, and start moving data between them. You pay only for the data you move.



Since the problem is mainly about moving historical records from on-premises to AWS, using AWS DataSync is a more suitable solution. You can use DataSync to move cold data from expensive on-premises storage systems directly to durable and secure long-term storage, such as Amazon S3 Glacier or Amazon S3 Glacier Deep Archive.

Hence, the correct answer is the option that says: Use AWS DataSync to move the historical records from on-premises to AWS. Choose Amazon S3 Glacier Deep Archive to be the destination for the data.

The following options are both incorrect:

- Use AWS Storage Gateway to move the historical records from on-premises to AWS. Choose Amazon S3 Glacier Deep Archive to be the destination for the data.
- Use AWS Storage Gateway to move the historical records from on-premises to AWS. Choose Amazon S3 Glacier to be the destination for the data. Modify the S3 lifecycle configuration to move the data from the Standard tier to Amazon S3 Glacier Deep Archive after 30 days.

Although you can copy data from on-premises to AWS with Storage Gateway, it is not suitable for transferring large sets of data to AWS. Storage Gateway is mainly used in providing low-latency access to data by caching frequently accessed data on-premises while storing archive data securely and durably in Amazon cloud storage services. Storage Gateway optimizes data transfer to AWS by sending only changed data and compressing data.

The option that says: Use AWS DataSync to move the historical records from on-premises to AWS. Choose Amazon S3 Standard to be the destination for the data. Modify the S3 lifecycle configuration to move the data from the Standard tier to Amazon S3 Glacier Deep Archive after 30 days is incorrect because, with AWS DataSync, you can transfer data from on-premises directly to Amazon S3 Glacier Deep Archive. You don't have to configure the S3 lifecycle policy and wait for 30 days to move the data to Glacier Deep Archive.

References:

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

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

Check out these AWS DataSync and Storage Gateway Cheat Sheets:

<https://tutorialsdojo.com/aws-datasync/>

<https://tutorialsdojo.com/aws-storage-gateway/>

AWS Storage Gateway vs DataSync:

<https://www.youtube.com/watch?v=tmfe1rO-AUs>

---

### QUESTION 139

You have built a web application that checks for new items in an S3 bucket once every hour. If new items exist, a message is added to an SQS queue. You have a fleet of EC2 instances which retrieve messages from the SQS queue, process the file, and finally, send you and the user an email confirmation that the item has been successfully processed. Your officemate uploaded one test file to the S3 bucket and after a couple of hours, you noticed that you and your officemate have 50 emails from your application with the same message.

Which of the following is most likely the root cause why the application has sent you and the user multiple emails?

- A. The sqsSendMessage attribute of the SQS queue is configured to 50.
- B. By default, SQS automatically deletes the messages that were processed by the consumers. It might be possible that your officemate has submitted the request 50 times which is why you received a lot of emails.
- C. There is a bug in the application.
- D. Your application does not issue a delete command to the SQS queue after processing the message, which is why this message went back to the queue and was processed multiple times.

Answer: D

Explanation:

In this scenario, the main culprit is that your application does not issue a delete command to the SQS queue after processing the message, which is why this message went back to the queue and was processed multiple times.

The option that says: The sqsSendMessage attribute of the SQS queue is configured to 50 is incorrect as there is no sqsSendMessage attribute in SQS.

The option that says: There is a bug in the application is a valid answer but since the scenario did not mention that the EC2 instances deleted the processed messages, the most likely cause of the problem is that the application does not issue a delete command to the SQS queue as mentioned above.

The option that says: By default, SQS automatically deletes the messages that were processed by the consumers. It might be possible that your officemate has submitted the request 50 times which is why you received a lot of emails is incorrect as SQS does not automatically delete the messages.

Reference:

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

Check out this Amazon SQS Cheat Sheet:  
<https://tutorialsdojo.com/amazon-sqs/>

## QUESTION 140

A company is running a custom application in an Auto Scaling group of Amazon EC2 instances. Several instances are failing due to insufficient swap space. The Solutions Architect has been instructed to troubleshoot the issue and effectively monitor the available swap space of each EC2 instance. Which of the following options fulfills this requirement?

- A. Create a CloudWatch dashboard and monitor the SwapUsed metric.
- B. Install the CloudWatch agent on each instance and monitor the SwapUtilization metric.
- C. Create a new trail in AWS CloudTrail and configure Amazon CloudWatch Logs to monitor your trail logs.
- D. Enable detailed monitoring on each instance and monitor the SwapUtilization metric.

Answer: B

Explanation:

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health.



The main requirement in the scenario is to monitor the SwapUtilization metric. Take note that you can't use the default metrics of CloudWatch to monitor the SwapUtilization metric. To monitor custom metrics, you must install the CloudWatch agent on the EC2 instance. After installing the CloudWatch agent, you can now collect system metrics and log files of an EC2 instance.

Hence, the correct answer is: Install the CloudWatch agent on each instance and monitor the SwapUtilization metric.

The option that says: Enable detailed monitoring on each instance and monitor the SwapUtilization metric is incorrect because you can't monitor the SwapUtilization metric by just enabling the detailed monitoring option. You must install the CloudWatch agent on the instance.

The option that says: Create a CloudWatch dashboard and monitor the SwapUsed metric is incorrect because you must install the CloudWatch agent first to add the custom metric in the dashboard.

The option that says: Create a new trail in AWS CloudTrail and configure Amazon CloudWatch Logs to monitor your trail logs is incorrect because CloudTrail won't help you monitor custom metrics. CloudTrail is specifically used for monitoring API activities in an AWS account.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html>

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

Check out this Amazon CloudWatch Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudwatch/>

## QUESTION 141

A media company has two VPCs: VPC-1 and VPC-2 with peering connection between each other. VPC-1 only contains private subnets while VPC-2 only contains public subnets. The company uses a single AWS Direct Connect connection and a virtual interface to connect their on-premises network with VPC-1.

Which of the following options increase the fault tolerance of the connection to VPC-1? (Select TWO.)

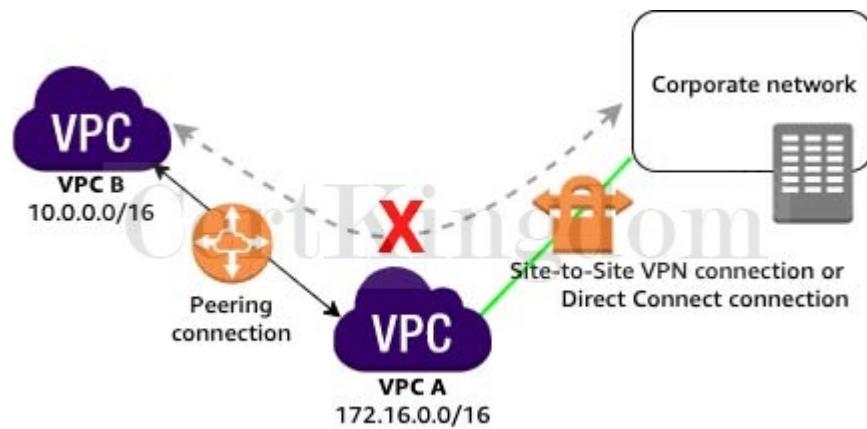
- A. Establish a hardware VPN over the Internet between VPC-1 and the on-premises network.
- B. Establish another AWS Direct Connect connection and private virtual interface in the same AWS region as VPC-1.
- C. Establish a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.
- D. Use the AWS VPN CloudHub to create a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.
- E. Establish a hardware VPN over the Internet between VPC-2 and the on-premises network.

Answer: A,B

Explanation:

In this scenario, you have two VPCs which have peering connections with each other. Note that a VPC peering connection does not support edge to edge routing. This means that if either VPC in a peering relationship has one of the following connections, you cannot extend the peering relationship to that connection:

- A VPN connection or an AWS Direct Connect connection to a corporate network
- An Internet connection through an Internet gateway
- An Internet connection in a private subnet through a NAT device
- A gateway VPC endpoint to an AWS service; for example, an endpoint to Amazon S3.
- (IPv6) A ClassicLink connection. You can enable IPv4 communication between a linked EC2-Classic instance and instances in a VPC on the other side of a VPC peering connection. However, IPv6 is not supported in EC2-Classic, so you cannot extend this connection for IPv6 communication.



For example, if VPC A and VPC B are peered, and VPC A has any of these connections, then instances in VPC B cannot use the connection to access resources on the other side of the connection. Similarly, resources on the other side of a connection cannot use the connection to access VPC B.

Hence, this means that you cannot use VPC-2 to extend the peering relationship that exists between VPC-1 and the on-premises network. For example, traffic from the corporate network can't directly access VPC-1 by using the VPN connection or the AWS Direct Connect connection to VPC-2, which is why the following options are incorrect:

- Use the AWS VPN CloudHub to create a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.

- Establish a hardware VPN over the Internet between VPC-2 and the on-premises network.
- Establish a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.

You can do the following to provide a highly available, fault-tolerant network connection:

- Establish a hardware VPN over the Internet between the VPC and the on-premises network.
- Establish another AWS Direct Connect connection and private virtual interface in the same AWS region.

References:

<https://docs.aws.amazon.com/vpc/latest/peering/invalid-peering-configurations.html#edge-to-edge-vgw>

<https://aws.amazon.com/premiumsupport/knowledge-center/configure-vpn-backup-dx/>

<https://aws.amazon.com/answers/networking/aws-multiple-data-center-ha-network-connectivity/>

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

---

## QUESTION 142

A company has a static corporate website hosted in a standard S3 bucket and a new web domain name that was registered using Route 53. You are instructed by your manager to integrate these two services in order to successfully launch their corporate website.

What are the prerequisites when routing traffic using Amazon Route 53 to a website that is hosted in an Amazon S3 Bucket? (Select TWO.)

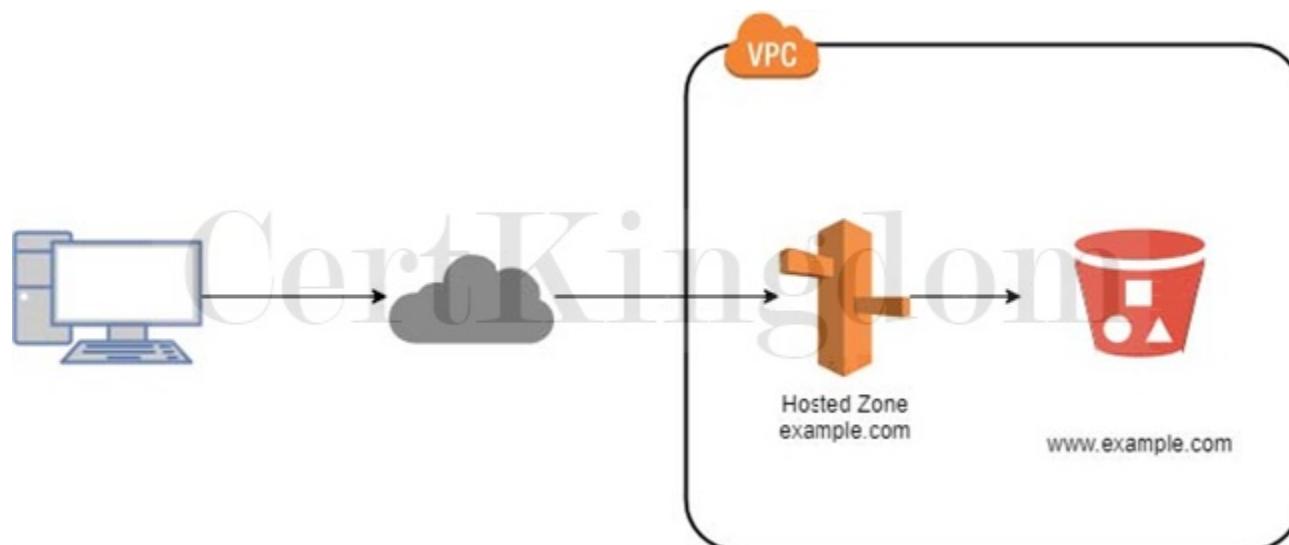
- A. The Cross-Origin Resource Sharing (CORS) option should be enabled in the S3 bucket
- B. The S3 bucket name must be the same as the domain name
- C. The record set must be of type "MX"
- D. A registered domain name
- E. The S3 bucket must be in the same region as the hosted zone

Answer: B,D

Explanation:

Here are the prerequisites for routing traffic to a website that is hosted in an Amazon S3 Bucket:

- An S3 bucket that is configured to host a static website. The bucket must have the same name as your domain or subdomain. For example, if you want to use the subdomain portal.tutorialsdojo.com, the name of the bucket must be portal.tutorialsdojo.com.
- A registered domain name. You can use Route 53 as your domain registrar, or you can use a different registrar.
- Route 53 as the DNS service for the domain. If you register your domain name by using Route 53, we automatically configure Route 53 as the DNS service for the domain.



The option that says: The record set must be of type "MX" is incorrect since an MX record specifies the

mail server responsible for accepting email messages on behalf of a domain name. This is not what is being asked by the question.

The option that says: The S3 bucket must be in the same region as the hosted zone is incorrect. There is no constraint that the S3 bucket must be in the same region as the hosted zone in order for the Route 53 service to route traffic into it.

The option that says: The Cross-Origin Resource Sharing (CORS) option should be enabled in the S3 bucket is incorrect because you only need to enable Cross-Origin Resource Sharing (CORS) when your client web application on one domain interacts with the resources in a different domain.

Reference:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/RoutingToS3Bucket.html>

Amazon Route 53 Overview:

<https://youtu.be/Su308t19ubY>

Check out this Amazon Route 53 Cheat Sheet:

<https://tutorialsdojo.com/amazon-route-53/>

---

### QUESTION 143

A company is running a dashboard application on a Spot EC2 instance inside a private subnet. The dashboard is reachable via a domain name that maps to the private IPv4 address of the instance's network interface. A solutions architect needs to increase network availability by allowing the traffic flow to resume in another instance if the primary instance is terminated.

Which solution accomplishes these requirements?

- A. Set up AWS Transfer for FTPS service in Implicit FTPS mode to automatically disable the source/destination checks on the instance's primary elastic network interface and reassociate it to another instance.
- B. Attach an elastic IP address to the instance's primary network interface and point its IP address to the application's domain name. Automatically move the EIP to a secondary instance if the primary instance becomes unavailable using the AWS Transit Gateway.
- C. Create a secondary elastic network interface and point its private IPv4 address to the application's domain name. Attach the new network interface to the primary instance. If the instance goes down, move the secondary network interface to another instance.
- D. Use the AWS Network Firewall to detach the instance's primary elastic network interface and move it to a new instance upon failure.

Answer: C

Explanation:

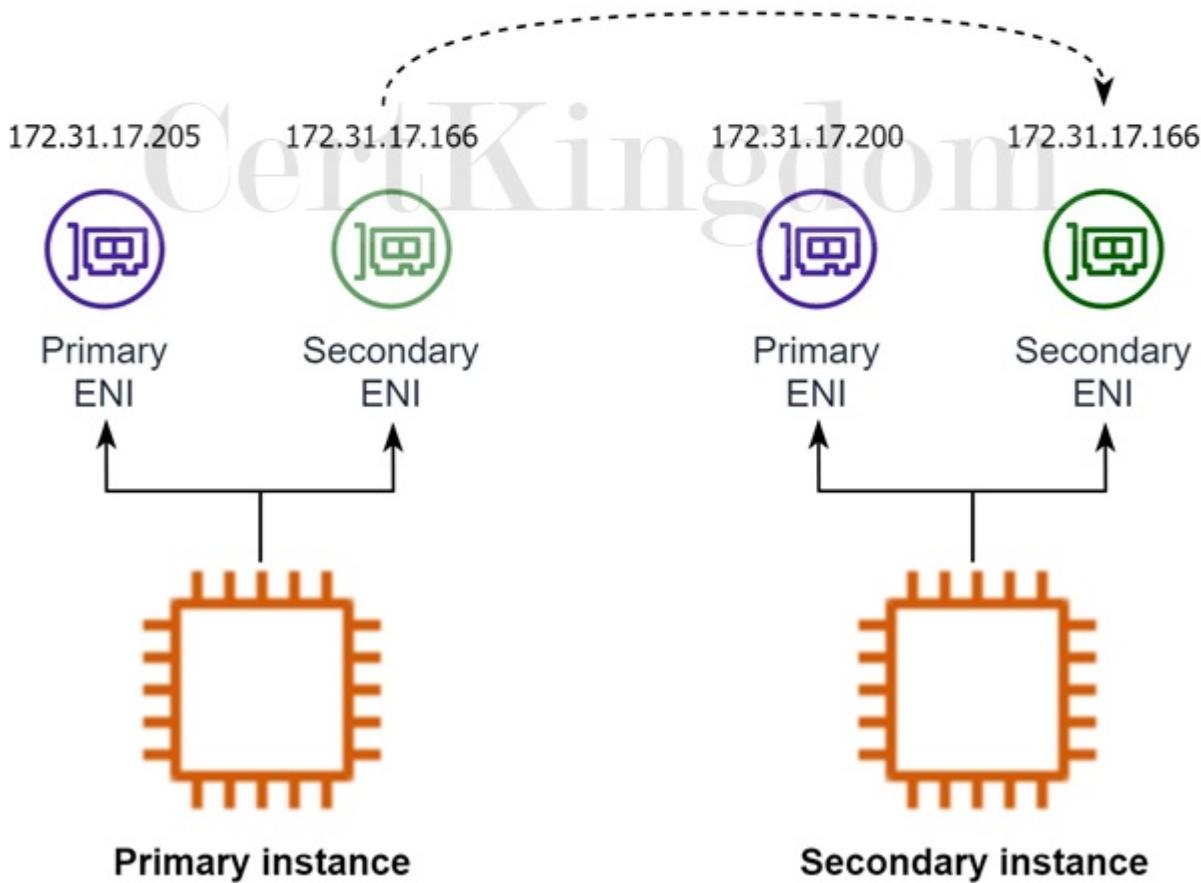
If one of your instances serving a particular function fails, its network interface can be attached to a replacement or hot standby instance pre-configured for the same role in order to rapidly recover the service. For example, you can use a network interface as your primary or secondary network interface to a critical service such as a database instance or a NAT instance. If the instance fails, you (or more likely, the code running on your behalf) can attach the network interface to a hot standby instance.

## DNS record

Record name [Info](#)  
internal .tutorialsdojo.com  
Keep blank to create a record for the root domain.

Value [Info](#)  Alias

172.31.17.205  
172.31.17.166



Because the interface maintains its private IP addresses, Elastic IP addresses, and MAC address, network traffic begins flowing to the standby instance as soon as you attach the network interface to the replacement instance. Users experience a brief loss of connectivity between the time the instance fails and the time that the network interface is attached to the standby instance, but no changes to the route table or your DNS server are required.

Hence, the correct answer is Create a secondary elastic network interface and point its private IPv4 address to the application's domain name. Attach the new network interface to the primary instance. If the instance goes down, move the secondary network interface to another instance.

The option that says: Attach an elastic IP address to the instance's primary network interface and point its IP address to the application's domain name. Automatically move the EIP to a secondary instance if the primary instance becomes unavailable using the AWS Transit Gateway is incorrect. Elastic IPs are not needed in the solution since the application is private. Furthermore, an AWS Transit Gateway is primarily used to connect your Amazon Virtual Private Clouds (VPCs) and on-premises networks through a central hub. This particular networking service cannot be used to automatically move an Elastic IP address to another EC2 instance.

The option that says: Set up AWS Transfer for FTPS service in Implicit FTPS mode to automatically

disable the source/destination checks on the instance's primary elastic network interface and reassociate it to another instance is incorrect. First of all, the AWS Transfer for FTPS service is not capable of automatically disabling the source/destination checks and it only supports Explicit FTPS mode. Disabling the source/destination check only allows the instance to which the ENI is connected to act as a gateway (both a sender and a receiver). It is not possible to make the primary ENI of any EC2 instance detachable. A more appropriate solution would be to use an Elastic IP address which can be reassigned with your secondary instance.

The option that says: Use the AWS Network Firewall to detach the instance's primary elastic network interface and move it to a new instance upon failure is incorrect. It's not possible to detach the primary network interface of an EC2 instance. In addition, the AWS Network Firewall is only used for filtering traffic at the perimeter of your VPC and not for detaching ENIs.

References:

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

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/scenarios-enis.html>

<https://aws.amazon.com/aws-transfer-family/faqs/>

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

---

## QUESTION 144

An organization needs to control the access for several S3 buckets. They plan to use a gateway endpoint to allow access to trusted buckets.

Which of the following could help you achieve this requirement?

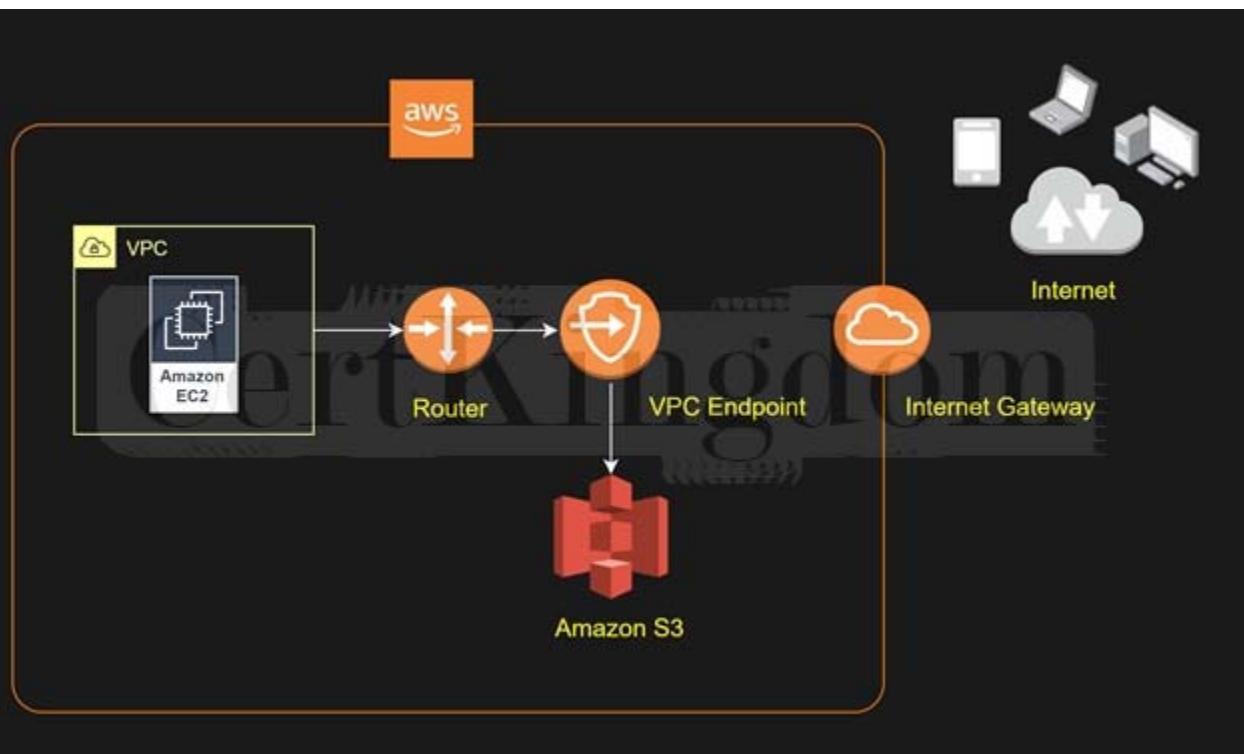
- A. Generate a bucket policy for trusted S3 buckets.
- B. Generate a bucket policy for trusted VPCs.
- C. Generate an endpoint policy for trusted VPCs.
- D. Generate an endpoint policy for trusted S3 buckets.

Answer: D

Explanation:

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, 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.

When you create a VPC endpoint, you can attach an endpoint policy that controls access to the service to which you are connecting. You can modify the endpoint policy attached to your endpoint and add or remove the route tables used by the endpoint. An endpoint policy does not override or replace IAM user policies or service-specific policies (such as S3 bucket policies). It is a separate policy for controlling access from the endpoint to the specified service.



We can use a bucket policy or an endpoint policy to allow the traffic to trusted S3 buckets. The options that have 'trusted S3 buckets' key phrases will be the possible answer in this scenario. It would take you a lot of time to configure a bucket policy for each S3 bucket instead of using a single endpoint policy. Therefore, you should use an endpoint policy to control the traffic to the trusted Amazon S3 buckets. Hence, the correct answer is: Generate an endpoint policy for trusted S3 buckets.

The option that says: Generate a bucket policy for trusted S3 buckets is incorrect. Although this is a valid solution, it takes a lot of time to set up a bucket policy for each and every S3 bucket. This can simply be accomplished by creating an S3 endpoint policy.

The option that says: Generate a bucket policy for trusted VPCs is incorrect because you are generating a policy for trusted VPCs. Remember that the scenario only requires you to allow the traffic for trusted S3 buckets, and not to the VPCs.

The option that says: Generate an endpoint policy for trusted VPCs is incorrect because it only allows access to trusted VPCs, and not to trusted Amazon S3 buckets.

#### References:

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

<https://aws.amazon.com/premiumsupport/knowledge-center/connect-s3-vpc-endpoint/>

#### Amazon VPC Overview:

<https://www.youtube.com/watch?v=oIDHKeN xvQQ>

#### Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

### QUESTION 145

A DevOps Engineer is required to design a cloud architecture in AWS. The Engineer is planning to develop a highly available and fault-tolerant architecture consisting of an Elastic Load Balancer and an Auto Scaling group of EC2 instances deployed across multiple Availability Zones. This will be used by an online accounting application that requires path-based routing, host-based routing, and bi-directional streaming using Remote Procedure Call (gRPC).

Which configuration will satisfy the given requirement?

- Configure an Application Load Balancer in front of the auto-scaling group. Select gRPC as the protocol version.
- Configure a Network Load Balancer in front of the auto-scaling group. Create an AWS Global Accelerator accelerator and set the load balancer as an endpoint.
- Configure a Gateway Load Balancer in front of the auto-scaling group. Ensure that the IP Listener Routing uses the GENEVE protocol on port 6081 to allow gRPC response traffic.

D. Configure a Network Load Balancer in front of the auto-scaling group. Use a UDP listener for routing.

Answer: A

Explanation:

Application Load Balancer operates at the request level (layer 7), routing traffic to targets (EC2 instances, containers, IP addresses, and Lambda functions) based on the content of the request. Ideal for advanced load balancing of HTTP and HTTPS traffic, Application Load Balancer provides advanced request routing targeted at delivery of modern application architectures, including microservices and container-based applications. Application Load Balancer simplifies and improves the security of your application, by ensuring that the latest SSL/TLS ciphers and protocols are used at all times.

The screenshot shows the AWS Application Load Balancer (ALB) rule configuration interface. The 'IF' section of the rule editor is highlighted with a green box, showing options like 'Host header...', 'Path...', 'Http header...', 'Http request method...', 'Query string...', and 'Source IP...'. The 'THEN' section shows a single target group named 'PUNTERYA-PILIPINAS' with a weight of 1 (100%). Group-level stickiness is set to 'Off'. The rule ID is 'HTTP 80: default action'.

If your application is composed of several individual services, an Application Load Balancer can route a request to a service based on the content of the request such as Host field, Path URL, HTTP header, HTTP method, Query string, or Source IP address.

#### IP address type

Only targets with the indicated IP address type can be included in this target group.

- IPv4
- IPv6

#### VPC

Select the VPC that hosts the load balancer. Only VPCs that support the IP address type selected above are available in this list. On the Register targets page, you can register IP addresses from this VPC, or from private IP addresses located outside of this load balancer's VPC (such as a peered VPC, EC2-Classic, or on-premises targets that are reachable over Direct Connect or VPN).

vpc-67ff81e1a  
IPv4: 172.31.0.0/16

#### Protocol version

- HTTP1  
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.
- HTTP2  
Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.
- gRPC  
Send requests to targets using gRPC. Supported when the request protocol is gRPC.

ALBs can also route and load balance gRPC traffic between microservices or between gRPC-enabled clients and services. This will allow customers to seamlessly introduce gRPC traffic management in their architectures without changing any of the underlying infrastructure on their clients or services.

Therefore, the correct answer is: Configure an Application Load Balancer in front of the auto-scaling group. Select gRPC as the protocol version.

The option that says: Configure a Network Load Balancer in front of the auto-scaling group. Use a UDP listener for routing is incorrect. Network Load Balancers do not support gRPC.

The option that says: Configure a Gateway Load Balancer in front of the auto-scaling group. Ensure that the IP Listener Routing uses the GENEVE protocol on port 6081 to allow gRPC response traffic is incorrect. A Gateway Load Balancer operates as a Layer 3 Gateway and a Layer 4 Load Balancing service. Do take note that the gRPC protocol is at Layer 7 of the OSI Model so this service is not appropriate for this scenario.

The option that says: Configure a Network Load Balancer in front of the auto-scaling group. Create an AWS Global Accelerator accelerator and set the load balancer as an endpoint is incorrect. AWS Global Accelerator simply optimizes application performance by routing user traffic to the congestion-free, redundant AWS global network instead of the public internet.

#### References:

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

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

AWS Elastic Load Balancing Overview:

<https://youtu.be/UBI5dw59DO8>

Check out this AWS Elastic Load Balancing (ELB) Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

Application Load Balancer vs Network Load Balancer vs Gateway Load Balancer:

<https://tutorialsdojo.com/application-load-balancer-vs-network-load-balancer-vs-classic-load-balancer/>

---

## QUESTION 146

A company has an on-premises MySQL database that needs to be replicated in Amazon S3 as CSV files. Once data has been fully copied, ongoing changes to the database should be continually streamed into the S3 bucket. The company wants a solution that can be implemented with little management overhead yet still highly secure.

Which ingestion pattern should a solutions architect take?

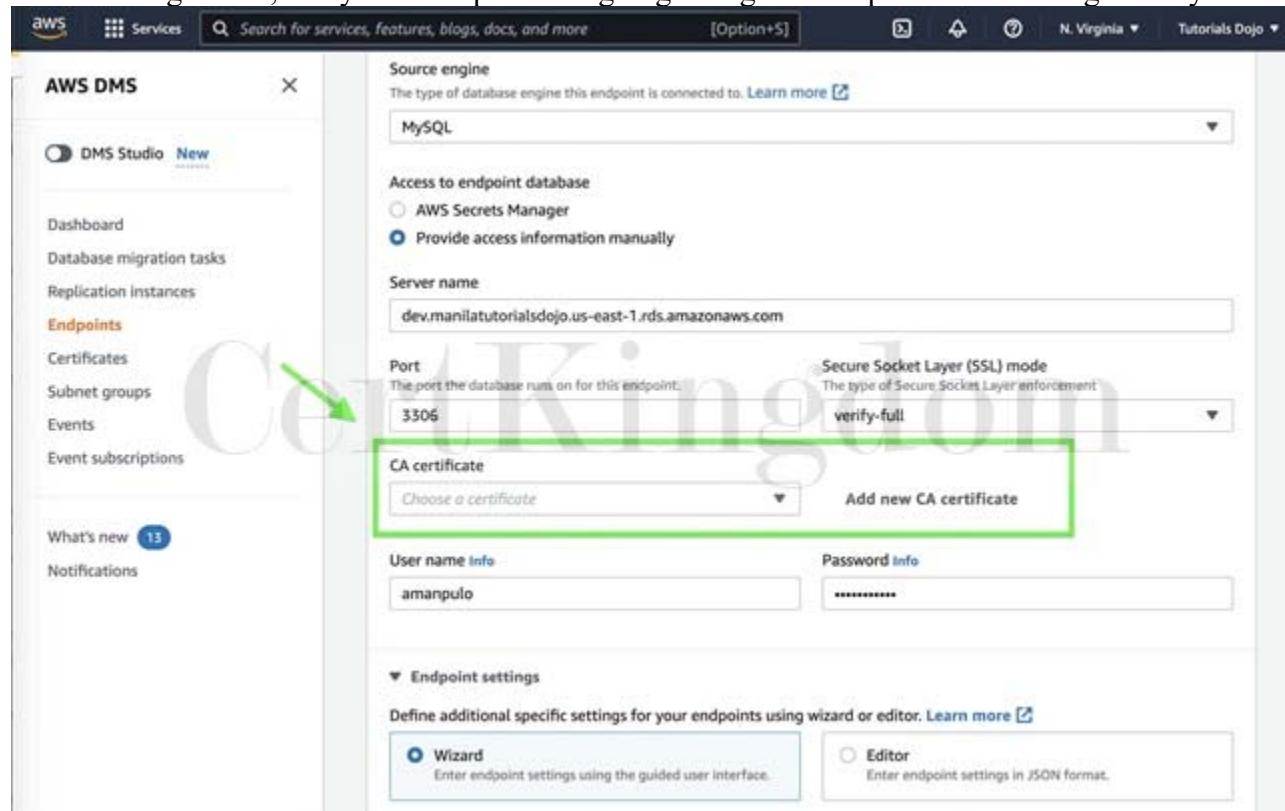
- A. Use AWS Schema Conversion Tool (AWS SCT) to convert MySQL data to CSV files. Set up the AWS Server Migration Service (AWS MGN) to capture ongoing changes from the on-premises MySQL database and send them to Amazon S3.

- B. Set up a full load replication task using AWS Database Migration Service (AWS DMS). Add a new Certificate Authority (CA) certificate and create an AWS DMS endpoint with SSL.
- C. Use an AWS Snowball Edge cluster to migrate data to Amazon S3 and AWS DataSync to capture ongoing changes. Create your own custom AWS KMS envelope encryption key for the associated AWS Snowball Edge job.
- D. Create a full load and change data capture (CDC) replication task using AWS Database Migration Service (AWS DMS). Launch an AWS DMS endpoint with SSL using the AWS Network Firewall service.

Answer: B

Explanation:

AWS Database Migration Service (AWS DMS) is a cloud service that makes it easy to migrate relational databases, data warehouses, NoSQL databases, and other types of data stores. You can use AWS DMS to migrate your data into the AWS Cloud, between on-premises instances (through an AWS Cloud setup), or between combinations of cloud and on-premises setups. With AWS DMS, you can perform one-time migrations, and you can replicate ongoing changes to keep sources and targets in sync.



You can migrate data to Amazon S3 using AWS DMS from any of the supported database sources. When using Amazon S3 as a target in an AWS DMS task, both full load and change data capture (CDC) data is written to comma-separated value (.csv) format by default.

The comma-separated value (.csv) format is the default storage format for Amazon S3 target objects. For more compact storage and faster queries, you can instead use Apache Parquet (.parquet) as the storage format.

You can encrypt connections for source and target endpoints by using Secure Sockets Layer (SSL). To do so, you can use the AWS DMS Management Console or AWS DMS API to assign a certificate to an endpoint. You can also use the AWS DMS console to manage your certificates.

Not all databases use SSL in the same way. Amazon Aurora MySQL-Compatible Edition uses the server name, the endpoint of the primary instance in the cluster, as the endpoint for SSL. An Amazon Redshift endpoint already uses an SSL connection and does not require an SSL connection set up by AWS DMS. Hence, the correct answer is Set up a full load replication task using AWS Database Migration Service (AWS DMS). Add a new Certificate Authority (CA) certificate and create an AWS DMS endpoint with SSL.

The option that says: Create a full load and change data capture (CDC) replication task using AWS

Database Migration Service (AWS DMS). Launch an AWS DMS endpoint with SSL using the AWS Network Firewall service is incorrect because a full load replication task alone won't capture ongoing changes to the database. You still need to implement a change data capture (CDC) replication to copy the recent changes after the migration. Moreover, the AWS Network Firewall service is not capable of creating an AWS DMS endpoint with SSL. The Certificate Authority (CA) certificate can be directly uploaded to the AWS DMS console without the AWS Network Firewall at all.

The option that says: Use an AWS Snowball Edge cluster to migrate data to Amazon S3 and AWS DataSync to capture ongoing changes is incorrect. While this is doable, it's more suited to the migration of large databases which require the use of two or more Snowball Edge appliances. Also, the usage of AWS DataSync for replicating ongoing changes to Amazon S3 requires extra steps that can be simplified with AWS DMS.

The option that says: Use AWS Schema Conversion Tool (AWS SCT) to convert MySQL data to CSV files. Set up the AWS Application Migration Service (AWS MGN) to capture ongoing changes from the on-premises MySQL database and send them to Amazon S3 is incorrect. AWS SCT is not used for data replication, it just eases up the conversion of source databases to a format compatible with the target database when migrating. In addition, using the AWS Application Migration Service (AWS MGN) for this scenario is inappropriate. This service is primarily used for lift-and-shift migrations of applications from physical infrastructure, VMware vSphere, Microsoft Hyper-V, Amazon Elastic Compute Cloud (AmazonEC2), Amazon Virtual Private Cloud (Amazon VPC), and other clouds to AWS.

References:

<https://aws.amazon.com/blogs/big-data/loading-ongoing-data-lake-changes-with-aws-dms-and-aws-glue/>

<https://docs.aws.amazon.com/dms/latest/userguide/Welcome.html>

[https://docs.aws.amazon.com/dms/latest/userguide/CHAP\\_Security.html#CHAP\\_Security.SSL.Limitations](https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Security.html#CHAP_Security.SSL.Limitations)

Check out this AWS Database Migration Service Cheat Sheet:

<https://tutorialsdojo.com/aws-database-migration-service/>

AWS Migration Services Overview:

<https://youtu.be/yqNBkFMnsL8>

---

## QUESTION 147

An insurance company plans to implement a message filtering feature in their web application. To implement this solution, they need to create separate Amazon SQS queues for each type of quote request. The entire message processing should not exceed 24 hours.

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

- A. Create one Amazon SNS topic and configure the Amazon SQS queues to subscribe to the SNS topic. Publish the same messages to all SQS queues. Filter the messages in each queue based on the quote request type.
- B. Create multiple Amazon SNS topics and configure the Amazon SQS queues to subscribe to the SNS topics. Publish the message to the designated SQS queue based on the quote request type.
- C. Create a data stream in Amazon Kinesis Data Streams. Use the Amazon Kinesis Client Library to deliver all the records to the designated SQS queues based on the quote request type.
- D. Create one Amazon SNS topic and configure the Amazon SQS queues to subscribe to the SNS topic. Set the filter policies in the SNS subscriptions to publish the message to the designated SQS queue based on its quote request type.

Answer: D

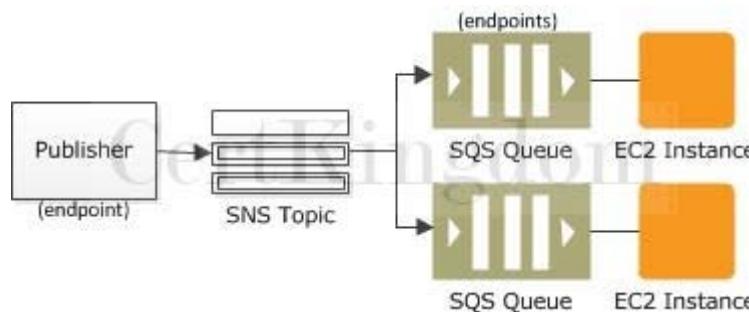
Explanation:

Amazon SNS is a fully managed pub/sub messaging service. With Amazon SNS, you can use topics to simultaneously distribute messages to multiple subscribing endpoints such as Amazon SQS queues, AWS Lambda functions, HTTP endpoints, email addresses, and mobile devices (SMS, Push).

Amazon SQS is a message queue service used by distributed applications to exchange messages through a polling model. It can be used to decouple sending and receiving components without requiring

each component to be concurrently available.

A fanout scenario occurs 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, two or more 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.

By default, an Amazon SNS topic subscriber receives every message published to the topic. You can use Amazon SNS message filtering to assign a filter policy to the topic subscription, and the subscriber will only receive a message that they are interested in. Using Amazon SNS and Amazon SQS together, messages can be delivered to applications that require immediate notification of an event. This method is known as fanout to Amazon SQS queues.

Hence, the correct answer is: Create one Amazon SNS topic and configure the Amazon SQS queues to subscribe to the SNS topic. Set the filter policies in the SNS subscriptions to publish the message to the designated SQS queue based on its quote request type.

The option that says: Create one Amazon SNS topic and configure the Amazon SQS queues to subscribe to the SNS topic. Publish the same messages to all SQS queues. Filter the messages in each queue based on the quote request type is incorrect because this option will distribute the same messages on all SQS queues instead of its designated queue. You need to fan-out the messages to multiple SQS queues using a filter policy in Amazon SNS subscriptions to allow parallel asynchronous processing. By doing so, the entire message processing will not exceed 24 hours.

The option that says: Create multiple Amazon SNS topics and configure the Amazon SQS queues to subscribe to the SNS topics. Publish the message to the designated SQS queue based on the quote request type is incorrect because to implement the solution asked in the scenario, you only need to use one Amazon SNS topic. To publish it to the designated SQS queue, you must set a filter policy that allows you to fanout the messages. If you didn't set a filter policy in Amazon SNS, the subscribers would receive all the messages published to the SNS topic. Thus, using multiple SNS topics is not an appropriate solution for this scenario.

The option that says: Create a data stream in Amazon Kinesis Data Streams. Use the Amazon Kinesis Client Library to deliver all the records to the designated SQS queues based on the quote request type is incorrect because Amazon KDS is not a message filtering service. You should use Amazon SNS and SQS to distribute the topic to the designated queue.

References:

<https://aws.amazon.com/getting-started/hands-on/filter-messages-published-to-topics/>

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

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

Check out these Amazon SNS and SQS Cheat Sheets:

<https://tutorialsdojo.com/amazon-sns/>

<https://tutorialsdojo.com/amazon-sqs/>

Amazon SNS Overview:

<https://youtu.be/ft5R451EUJ8>

## QUESTION 148

A technology company has a suite of container-based web applications and serverless solutions that are hosted in AWS. The Solutions Architect must define a standard infrastructure that will be used across development teams and applications. There are application-specific resources too that change frequently, especially during the early stages of application development. Developers must be able to add supplemental resources to their applications, which are beyond what the architects predefined in the system environments and service templates.

Which of the following should be implemented to satisfy this requirement?

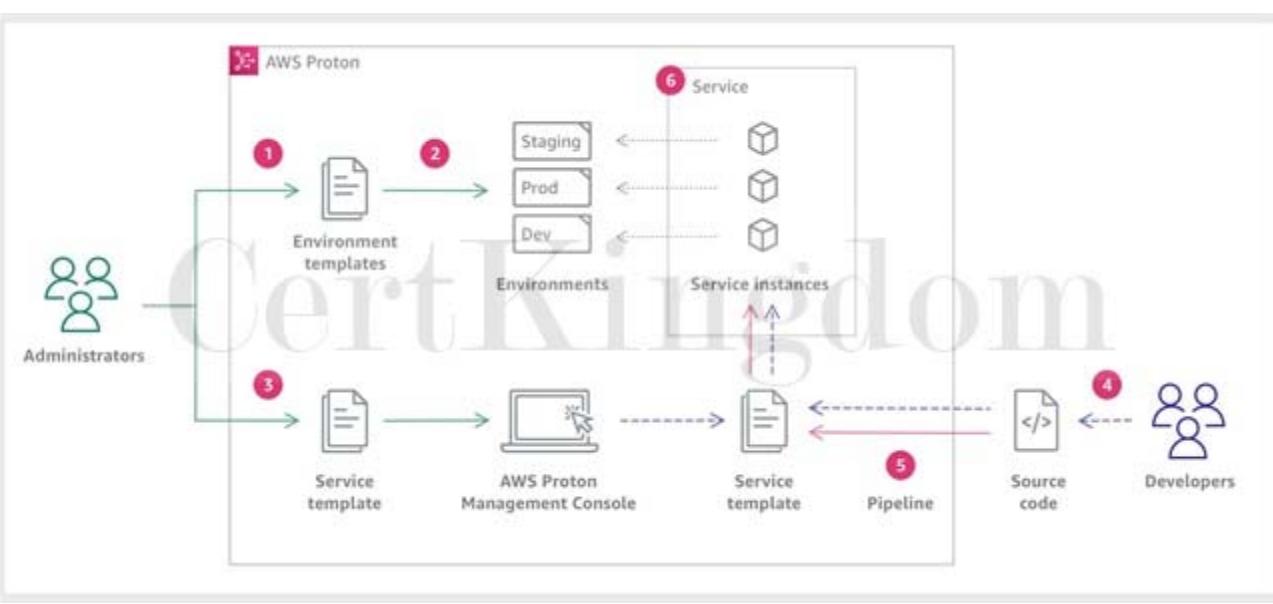
- A. Use the Amazon Elastic Container Service (ECS) Anywhere service for deploying container applications and serverless solutions. Configure Prometheus metrics collection on the ECS cluster and use Amazon Managed Service for Prometheus for monitoring frequently-changing resources
- B. Set up AWS Proton for deploying container applications and serverless solutions. Create components from the AWS Proton console and attach them to their respective service instance.
- C. Set up AWS Control Tower to automate container-based application deployments. Use AWS Config for application-specific resources that change frequently.
- D. Use the Amazon EKS Anywhere service for deploying container applications and serverless solutions. Create a service instance for each application-specific resource.

Answer: B

Explanation:

AWS Proton allows you to deploy any serverless or container-based application with increased efficiency, consistency, and control. You can define infrastructure standards and effective continuous delivery pipelines for your organization. Proton breaks down the infrastructure into environment and service (infrastructure as code' templates).

As a developer, you select a standardized service template that AWS Proton uses to create a service that deploys and manages your application in a service instance. An AWS Proton service is an instantiation of a service template, which normally includes several service instances and a pipeline.



The diagram above displays the high-level overview of a simple AWS Proton workflow.

In AWS Proton administrators define standard infrastructure that is used across development teams and applications. However, development teams might need to include additional resources for their specific use cases, like Amazon Simple Queue Service (Amazon SQS) queues or Amazon DynamoDB tables. These application-specific resources might change frequently, particularly during early application development. Maintaining these frequent changes in administrator-authored templates might be hard to manage and scale" administrators would need to maintain many more templates without real administrator added value. The alternative" letting application developers author templates for their applications" isn't ideal either, because it takes away administrators' ability to standardize the main architecture components, like AWS Fargate tasks. This is where components come in.

With a component, a developer can add supplemental resources to their application, above and beyond what administrators defined in environment and service templates. The developer then attaches the component to a service instance. AWS Proton provisions infrastructure resources defined by the component just like it provisions resources for environments and service instances.

Hence, the correct answer is: Set up AWS Proton for deploying container applications and serverless solutions. Create components from the AWS Proton console and attach them to their respective service instance.

The option that says: Use the Amazon EKS Anywhere service for deploying container applications and serverless solutions. Create a service instance for each application-specific resource is incorrect.

Amazon EKS Anywhere just allows you to manage a Kubernetes cluster on external environments that are supported by AWS. It is better to use AWS Proton with custom Components that can be attached to the different service instances of the company's application suite.

The option that says: Set up AWS Control Tower to automate container-based application deployments. Use AWS Config for application-specific resources that change frequently is incorrect. AWS Control Tower is used to simplify the creation of new accounts with preconfigured constraints. It isn't used to automate application deployments. Moreover, AWS Config is commonly used for monitoring the changes of AWS resources and not the custom resources for serverless or container-based applications in AWS.

A combination of AWS Proton and Components is the most suitable solution for this scenario.

The option that says: Use the Amazon Elastic Container Service (ECS) Anywhere service for deploying container applications and serverless solutions. Configure Prometheus metrics collection on the ECS cluster and use Amazon Managed Service for Prometheus for monitoring frequently-changing resources is incorrect. The Amazon Managed Service for Prometheus is only a Prometheus-compatible monitoring and alerting service that makes it easy to monitor containerized applications and infrastructure at scale.

It is not capable of tracking or maintaining your application-specific resources that change frequently.

References:

[\[https://aws.amazon.com/blogs/architecture/simplifying-multi-account-ci-cd-deployments-using-aws-proto  
n/\]\(https://aws.amazon.com/blogs/architecture/simplifying-multi-account-ci-cd-deployments-using-aws-proton/\)](https://docs.aws.amazon.com/proton/latest/userguide>Welcome.html</a></p></div><div data-bbox=)

---

## QUESTION 149

A company is receiving semi-structured and structured data from different sources every day. The Solutions Architect plans to use big data processing frameworks to analyze vast amounts of data and access it using various business intelligence tools and standard SQL queries.

Which of the following provides the MOST high-performing solution that fulfills this requirement?

- A. Create an Amazon EC2 instance and store the processed data in Amazon EBS.
- B. Use Amazon Kinesis Data Analytics and store the processed data in Amazon DynamoDB.
- C. Create an Amazon EMR cluster and store the processed data in Amazon Redshift.
- D. Use AWS Glue and store the processed data in Amazon S3.

Answer: C

Explanation:

Amazon EMR is a managed cluster platform that simplifies running big data frameworks, such as Apache Hadoop and Apache Spark, on AWS to process and analyze vast amounts of data. By using these frameworks and related open-source projects, such as Apache Hive and Apache Pig, you can process data for analytics purposes and business intelligence workloads. Additionally, you can use Amazon EMR to transform and move large amounts of data into and out of other AWS data stores and databases.

Amazon Redshift is the most widely used cloud data warehouse. It makes it fast, simple and costeffective to analyze all your data using standard SQL and your existing Business Intelligence (BI) tools. It allows you to run complex analytic queries against terabytes to petabytes of structured and semistructured data, using sophisticated query optimization, columnar storage on high-performance storage, and massively parallel query execution.



The key phrases in the scenario are "big data processing frameworks" and "various business intelligence tools and standard SQL queries" to analyze the data. To leverage big data processing frameworks, you need to use Amazon EMR. The cluster will perform data transformations (ETL) and load the processed data into Amazon Redshift for analytic and business intelligence applications.

Hence, the correct answer is: Create an Amazon EMR cluster and store the processed data in Amazon Redshift.

The option that says: Use AWS Glue and store the processed data in Amazon S3 is incorrect because AWS Glue is just a serverless ETL service that crawls your data, builds a data catalog, performs data preparation, data transformation, and data ingestion. It won't allow you to utilize different big data frameworks effectively, unlike Amazon EMR. In addition, the S3 Select feature in Amazon S3 can only run simple SQL queries against a subset of data from a specific S3 object. To perform queries in the S3 bucket, you need to use Amazon Athena.

The option that says: Use Amazon Kinesis Data Analytics and store the processed data in Amazon DynamoDB is incorrect because Amazon DynamoDB doesn't fully support the use of standard SQL and Business Intelligence (BI) tools, unlike Amazon Redshift. It also doesn't allow you to run complex analytic queries against terabytes to petabytes of structured and semi-structured data.

The option that says: Create an Amazon EC2 instance and store the processed data in Amazon EBS is incorrect because a single EBS-backed EC2 instance is quite limited in its computing capability.

Moreover, it also entails an administrative overhead since you have to manually install and maintain the big data frameworks for the EC2 instance yourself. The most suitable solution to leverage big data frameworks is to use EMR clusters.

References:

<https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-what-is-emr.html>

<https://docs.aws.amazon.com/redshift/latest/dg/loading-data-from-emr.html>

Check out this Amazon EMR Cheat Sheet:

<https://tutorialsdojo.com/amazon-emr/>

## QUESTION 150

A company has two On-Demand EC2 instances inside the Virtual Private Cloud in the same Availability Zone but are deployed to different subnets. One EC2 instance is running a database and the other EC2 instance a web application that connects with the database. You need to ensure that these two instances can communicate with each other for the system to work properly.

What are the things you have to check so that these EC2 instances can communicate inside the VPC?  
(Select TWO.)

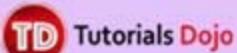
- A. Check if both instances are the same instance class.
- B. Ensure that the EC2 instances are in the same Placement Group.
- C. Check the Network ACL if it allows communication between the two subnets.
- D. Check if all security groups are set to allow the application host to communicate to the database on the right port and protocol.
- E. Check if the default route is set to a NAT instance or Internet Gateway (IGW) for them to communicate.

Answer: C,D

Explanation:

First, the Network ACL should be properly set to allow communication between the two subnets. The security group should also be properly configured so that your web server can communicate with the database server.

Security Group	Network Access Control List
Acts as a firewall for associated Amazon EC2 instances	Acts as a firewall for associated subnets
Controls both inbound and outbound traffic at the instance level	Controls both inbound and outbound traffic at the subnet level
You can secure your VPC instances using only security groups	Network ACLs are an additional layer of defense.
Supports allow rules only	Supports allow rules and deny rules
Stateful (Return traffic is automatically allowed, regardless of any rules)	Stateless (Return traffic must be explicitly allowed by rules)
Evaluates all rules before deciding whether to allow traffic	Evaluates rules in number order when deciding whether to allow traffic, starting with the lowest numbered rule.
Applies only to the instance that is associated to it	Applies to all instances in the subnet it is associated with
Has separate rules for inbound and outbound traffic	Has separate rules for inbound and outbound traffic
A newly created security group denies all inbound traffic by default	A newly created nACL denies all inbound traffic by default
A newly created security group has an outbound rule that allows all outbound traffic by default	A newly created nACL denies all outbound traffic by default
Instances associated with a security group can't talk to each other unless you add rules allowing it	Each subnet in your VPC must be associated with a network ACL. If none is associated, the default nACL is selected.
Security groups are associated with network interfaces	You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time.



Hence, these are the correct answers:

Check if all security groups are set to allow the application host to communicate to the database on the right port and protocol.

Check the Network ACL if it allows communication between the two subnets.

The option that says: Check if both instances are the same instance class is incorrect because the EC2 instances do not need to be of the same class in order to communicate with each other.

The option that says: Check if the default route is set to a NAT instance or Internet Gateway (IGW) for them to communicate is incorrect because an Internet gateway is primarily used to communicate to the Internet.

The option that says: Ensure that the EC2 instances are in the same Placement Group is incorrect

because Placement Group is mainly used to provide low-latency network performance necessary for tightly-coupled node-to-node communication.

Reference:

[http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Subnets.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html)

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

---

## QUESTION 151

A solutions architect is formulating a strategy for a startup that needs to transfer 50 TB of on-premises data to Amazon S3. The startup has a slow network transfer speed between its data center and AWS which causes a bottleneck for data migration.

Which of the following should the solutions architect implement?

- A. Request an Import Job to Amazon S3 using a Snowball device in the AWS Snowball Console.
- B. Integrate AWS Storage Gateway File Gateway with the on-premises data center.
- C. Deploy an AWS Migration Hub Discovery agent in the on-premises data center.
- D. Enable Amazon S3 Transfer Acceleration on the target S3 bucket.

Answer: A

Explanation:

AWS Snowball uses secure, rugged devices so you can bring AWS computing and storage capabilities to your edge environments, and transfer data into and out of AWS. The service delivers you Snowball Edge devices with storage and optional Amazon EC2 and AWS IOT Greengrass compute in shippable, hardened, secure cases. With AWS Snowball, you bring cloud capabilities for machine learning, data analytics, processing, and storage to your edge for migrations, short-term data collection, or even longterm deployments. AWS Snowball devices work with or without the internet, do not require a dedicated IT operator, and are designed to be used in remote environments.

Hence, the correct answer is: Request an Import Job to Amazon S3 using a Snowball device in the AWS Snowball Console.

The option that says: Deploy an AWS Migration Hub Discovery agent in the on-premises data center is incorrect. The AWS Migration Hub service is just a central service that provides a single location to track the progress of application migrations across multiple AWS and partner solutions.

The option that says: Enable Amazon S3 Transfer Acceleration on the target S3 bucket is incorrect because this S3 feature is not suitable for large-scale data migration. Enabling this feature won't always guarantee faster data transfer as it's only beneficial for long-distance transfer to and from your Amazon S3 buckets.

The option that says: Integrate AWS Storage Gateway File Gateway with the on-premises data center is incorrect because this service is mostly used for building hybrid cloud solutions where you still need on-premises access to unlimited cloud storage. Based on the scenario, this service is not the best option because you would still rely on the existing low bandwidth internet connection.

References:

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

<https://aws.amazon.com/blogs/storage/making-it-even-simpler-to-create-and-manage-your-aws-snow-family-jobs/>

Check out this AWS Snowball Cheat Sheet:

<https://tutorialsdojo.com/aws-snowball/>

AWS Snow Family Overview:

<https://www.youtube.com/watch?v=9Ar-51Ip53Q>

---

## QUESTION 152

A large insurance company has an AWS account that contains three VPCs (DEV, UAT and PROD) in the same region. UAT is peered to both PROD and DEV using a VPC peering connection. All VPCs

have non-overlapping CIDR blocks. The company wants to push minor code releases from Dev to Prod to speed up time to market.

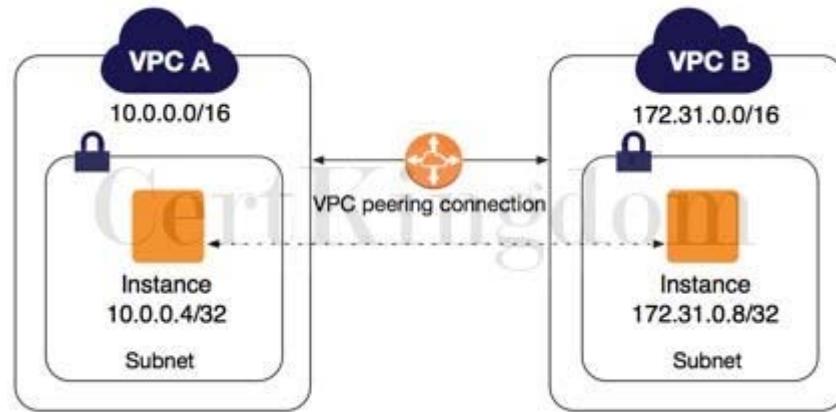
Which of the following options helps the company accomplish this?

- A. Change the DEV and PROD VPCs to have overlapping CIDR blocks to be able to connect them.
- B. Do nothing. Since these two VPCs are already connected via UAT, they already have a connection to each other.
- C. Create a new VPC peering connection between PROD and DEV with the appropriate routes.
- D. Create a new entry to PROD in the DEV route table using the VPC peering connection as the target.

Answer: C

Explanation:

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.



AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

Creating a new entry to PROD in the DEV route table using the VPC peering connection as the target is incorrect because even if you configure the route tables, the two VPCs will still be disconnected until you set up a VPC peering connection between them.

Changing the DEV and PROD VPCs to have overlapping CIDR blocks to be able to connect them is incorrect because you cannot peer two VPCs with overlapping CIDR blocks.

The option that says: Do nothing. Since these two VPCs are already connected via UAT, they already have a connection to each other is incorrect as transitive VPC peering is not allowed hence, even though DEV and PROD are both connected in UAT, these two VPCs do not have a direct connection to each other.

Reference:

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>

Check out these Amazon VPC and VPC Peering Cheat Sheets:

<https://tutorialsdojo.com/amazon-vpc/>

<https://tutorialsdojo.com/vpc-peering/>

Here is a quick introduction to VPC Peering:

<https://youtu.be/i1A1eH8vLtk>

## QUESTION 153

A Solutions Architect is designing a highly available environment for an application. She plans to host the application on EC2 instances within an Auto Scaling Group. One of the conditions requires data stored on root EBS volumes to be preserved if an instance terminates.

What should be done to satisfy the requirement?

- A. Enable the Termination Protection option for all EC2 instances.
- B. Configure ASG to suspend the health check process for each EC2 instance.
- C. Use AWS DataSync to replicate root volume data to Amazon S3.
- D. Set the value of DeleteOnTermination attribute of the EBS volumes to False.

Answer: D

Explanation:

By default, Amazon EBS root device volumes are automatically deleted when the instance terminates. However, by default, any additional EBS volumes that you attach at launch, or any EBS volumes that you attach to an existing instance persist even after the instance terminates. This behavior is controlled by the volume's DeleteOnTermination attribute, which you can modify.

To preserve the root volume when an instance terminates, change the DeleteOnTermination attribute for the root volume to False.

This EBS attribute can be changed through the AWS Console upon launching the instance or through CLI/API command.

Hence, the correct answer is the option that says: Set the value of DeleteOnTermination attribute of the EBS volumes to False.



The option that says: Use AWS DataSync to replicate root volume data to Amazon S3 is incorrect because AWS DataSync does not work with Amazon EBS volumes. DataSync can copy data between Network File System (NFS) shares, Server Message Block (SMB) shares, self-managed object storage, AWS Snowcone, Amazon Simple Storage Service (Amazon S3) buckets, Amazon Elastic File System (Amazon EFS) file systems, and Amazon FSx for Windows File Server file systems.

The option that says: Configure ASG to suspend the health check process for each EC2 instance is incorrect because suspending the health check process will prevent the ASG from replacing unhealthy EC2 instances. This can cause availability issues to the application.

The option that says: Enable the Termination Protection option for all EC2 instances is incorrect.

Termination Protection will just prevent your instance from being accidentally terminated using the Amazon EC2 console.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/deleteontermination-ebs/>

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

Check out this Amazon EBS Cheat Sheet:

<https://tutorialsdojo.com/amazon-ebs/>

## QUESTION 154

A manufacturing company has EC2 instances running in AWS. The EC2 instances are configured with Auto Scaling. There are a lot of requests being lost because of too much load on the servers. The Auto Scaling is launching new EC2 instances to take the load accordingly yet, there are still some requests that are being lost.

Which of the following is the MOST suitable solution that you should implement to avoid losing recently submitted requests?

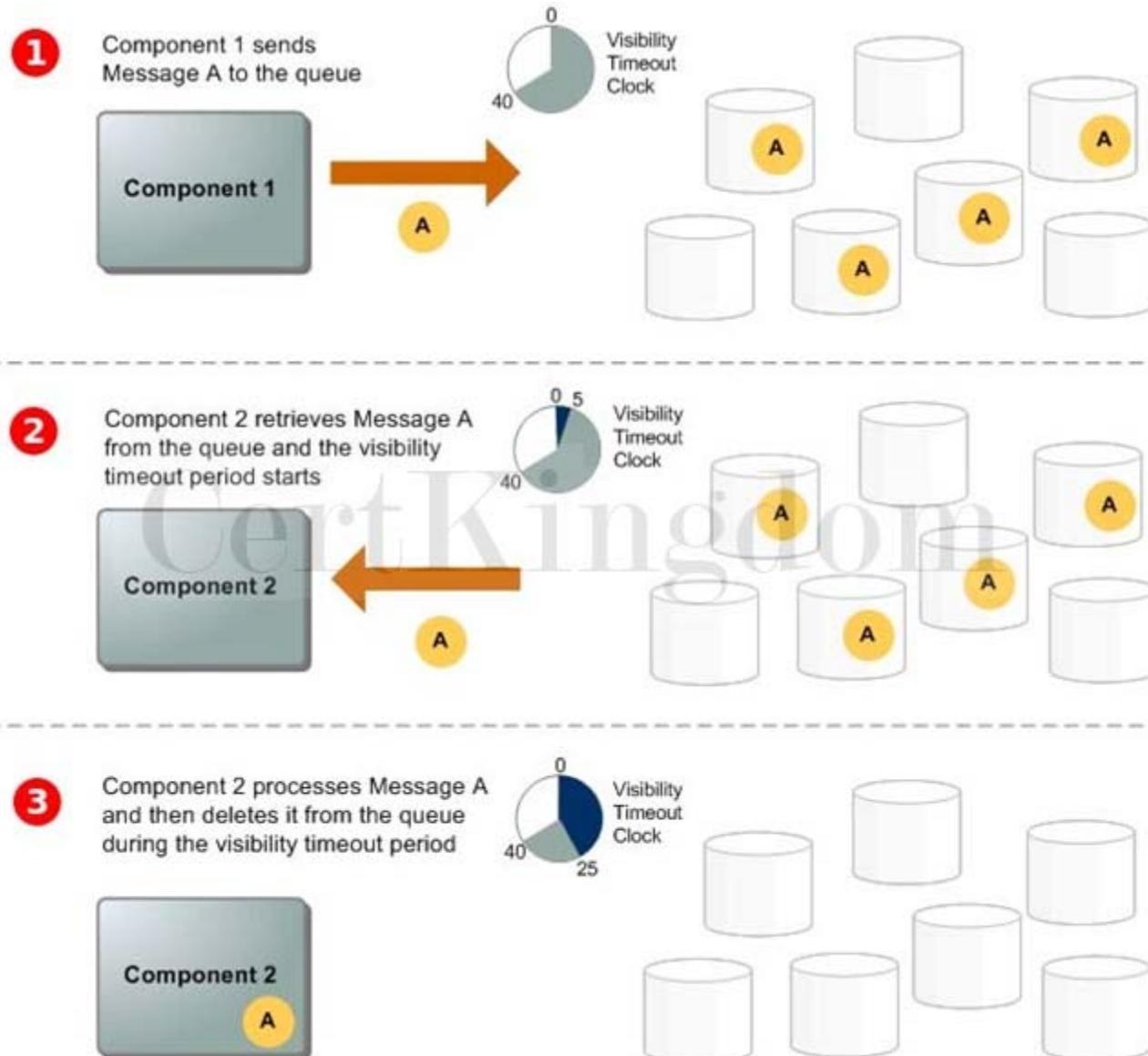
- A. Replace the Auto Scaling group with a cluster placement group to achieve a low-latency network performance necessary for tightly-coupled node-to-node communication.
- B. Set up Amazon Aurora Serverless for on-demand, auto-scaling configuration of your EC2 Instances and also enable Amazon Aurora Parallel Query feature for faster analytical queries over your current data.
- C. Use larger instances for your application with an attached Elastic Fabric Adapter (EFA).

D. Use an Amazon SQS queue to decouple the application components and scale-out the EC2 instances based upon the ApproximateNumberOfMessages metric in Amazon CloudWatch.

Answer: D

Explanation:

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that makes it easy to decouple and scale microservices, distributed systems, and serverless applications. Building applications from individual components that each perform a discrete function improves scalability and reliability, and is best practice design for modern applications. SQS makes it simple and cost-effective to decouple and coordinate the components of a cloud application. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be always available.



The number of messages in your Amazon SQS queue does not solely define the number of instances needed. In fact, the number of instances in the fleet can be driven by multiple factors, including how long it takes to process a message and the acceptable amount of latency (queue delay).

The solution is to use a backlog per instance metric with the target value being the acceptable backlog per instance to maintain. You can calculate these numbers as follows:

**Backlog per instance:** To determine your backlog per instance, start with the Amazon SQS metric ApproximateNumberOfMessages to determine the length of the SQS queue (number of messages available for retrieval from the queue). Divide that number by the fleet's running capacity, which for an Auto Scaling group is the number of instances in the InService state, to get the backlog per instance.

**Acceptable backlog per instance:** To determine your target value, first calculate what your application

can accept in terms of latency. Then, take the acceptable latency value and divide it by the average time that an EC2 instance takes to process a message.

To illustrate with an example, let's say that the current ApproximateNumberOfMessages is 1500 and the fleet's running capacity is 10. If the average processing time is 0.1 seconds for each message and the longest acceptable latency is 10 seconds then the acceptable backlog per instance is  $10 / 0.1$ , which equals 100. This means that 100 is the target value for your target tracking policy. Because the backlog per instance is currently at 150 ( $1500 / 10$ ), your fleet scales out by five instances to maintain proportion to the target value.

Hence, the correct answer is: Use an Amazon SQS queue to decouple the application components and scale-out the EC2 instances based upon the ApproximateNumberOfMessages metric in Amazon CloudWatch.

Replacing the Auto Scaling group with a cluster placement group to achieve a low-latency network performance necessary for tightly-coupled node-to-node communication is incorrect because although it is true that a cluster placement group allows you to achieve a low-latency network performance, you still need to use Auto Scaling for your architecture to add more EC2 instances.

Using larger instances for your application with an attached Elastic Fabric Adapter (EFA) is incorrect because using a larger EC2 instance would not prevent data from being lost in case of a larger spike.

You can take advantage of the durability and elasticity of SQS to keep the messages available for consumption by your instances. Elastic Fabric Adapter (EFA) is simply a network interface for Amazon EC2 instances that enables customers to run applications requiring high levels of inter-node communications at scale on AWS.

Setting up Amazon Aurora Serverless for on-demand, auto-scaling configuration of your EC2 Instances and also enabling Amazon Aurora Parallel Query feature for faster analytical queries over your current data is incorrect because although the Amazon Aurora Parallel Query feature provides faster analytical queries over your current data, Amazon Aurora Serverless is an on-demand, auto-scaling configuration for your database, and NOT for your EC2 instances. This is actually an auto-scaling configuration for your Amazon Aurora database and not for your compute services.

References:

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

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html>

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

Check out this Amazon SQS Cheat Sheet:

<https://tutorialsdojo.com/amazon-sqs/>

---

## QUESTION 155

A company has an e-commerce application that saves the transaction logs to an S3 bucket. You are instructed by the CTO to configure the application to keep the transaction logs for one month for troubleshooting purposes, and then afterward, purge the logs.

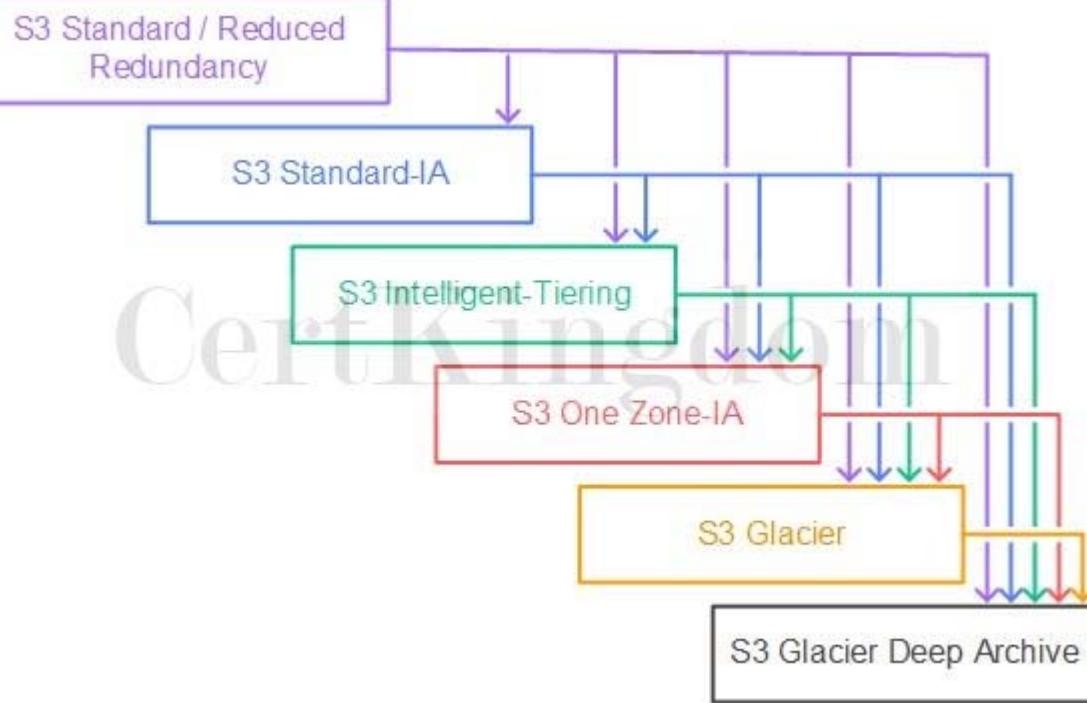
What should you do to accomplish this requirement?

- A. Create a new IAM policy for the Amazon S3 bucket that automatically deletes the logs after a month
- B. Configure the lifecycle configuration rules on the Amazon S3 bucket to purge the transaction logs after a month
- C. Enable CORS on the Amazon S3 bucket which will enable the automatic monthly deletion of data
- D. Add a new bucket policy on the Amazon S3 bucket.

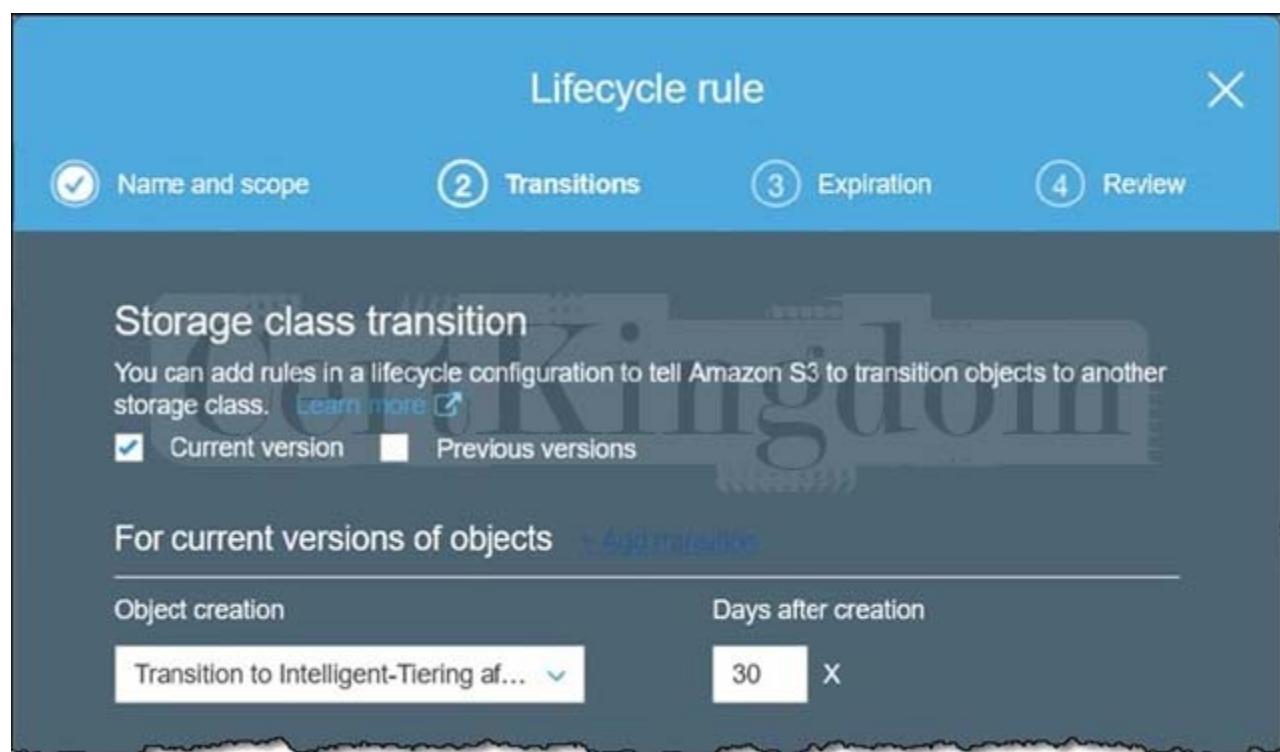
Answer: B

Explanation:

In this scenario, the best way to accomplish the requirement is to simply configure the lifecycle configuration rules on the Amazon S3 bucket to purge the transaction logs after a month.



Lifecycle configuration enables you to specify the lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects.



These actions can be classified as follows:

**Transition actions** “ In which you define when objects transition to another storage class. For example, you may choose to transition objects to the STANDARD\_IA (IA, for infrequent access) storage class 30 days after creation or archive objects to the GLACIER storage class one year after creation.

**Expiration actions** “ In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.

Hence, the correct answer is: Configure the lifecycle configuration rules on the Amazon S3 bucket to purge the transaction logs after a month.

The option that says: Add a new bucket policy on the Amazon S3 bucket is incorrect as it does not provide a solution to any of your needs in this scenario. You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it.

The option that says: Create a new IAM policy for the Amazon S3 bucket that automatically deletes the

logs after a month is incorrect because IAM policies are primarily used to specify what actions are allowed or denied on your S3 buckets. You cannot configure an IAM policy to automatically purge logs for you in any way.

The option that says: Enable CORS on the Amazon S3 bucket which will enable the automatic monthly deletion of data is incorrect. CORS allows client web applications that are loaded in one domain to interact with resources in a different domain.

References:

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

[https://docs.amazonaws.cn/en\\_us/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html](https://docs.amazonaws.cn/en_us/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html)

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

---

## QUESTION 156

An on-premises server is using an SMB network file share to store application data. The application produces around 50 MB of data per day but it only needs to access some of it for daily processes. To save on storage costs, the company plans to copy all the application data to AWS, however, they want to retain the ability to retrieve data with the same low-latency access as the local file share. The company does not have the capacity to develop the needed tool for this operation.

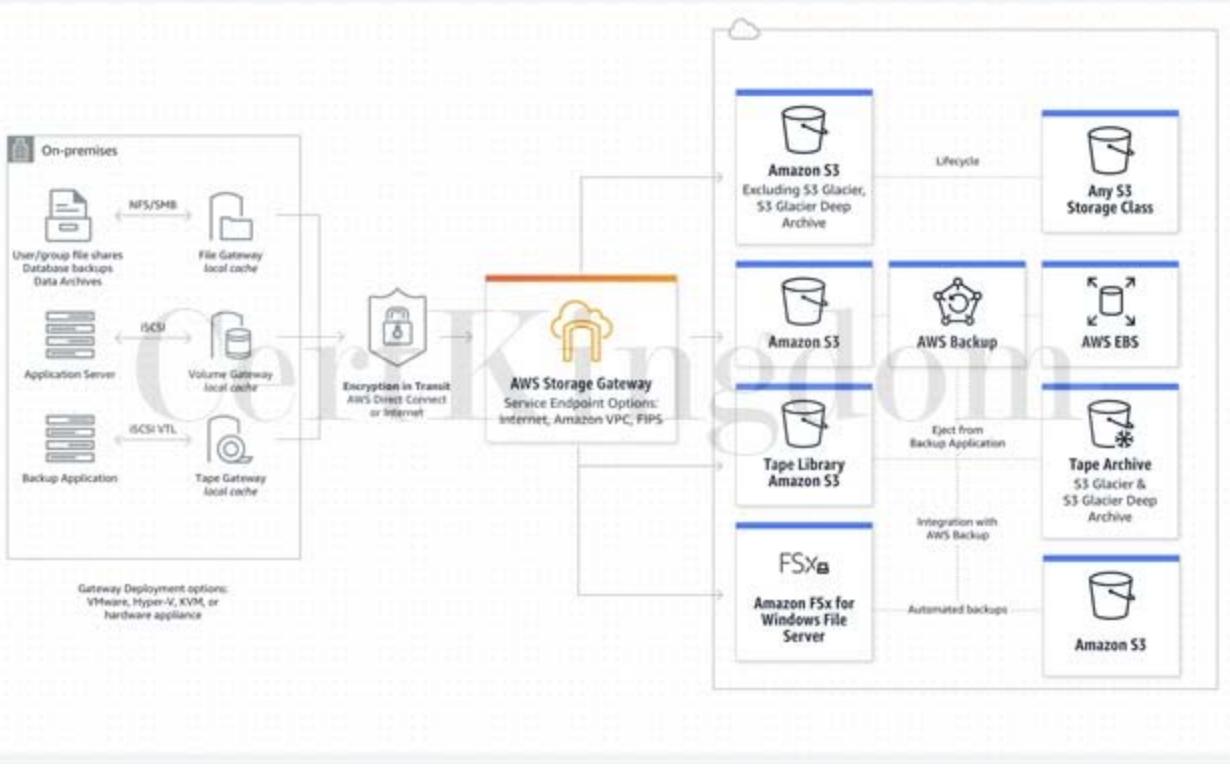
Which AWS service should the company use?

- A. AWS Storage Gateway
- B. AWS Snowball Edge
- C. Amazon FSx for Windows File Server
- D. AWS Virtual Private Network (VPN)

Answer: A

Explanation:

AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases. These include moving backups to the cloud, using on-premises file shares backed by cloud storage, and providing low latency access to data in AWS for on-premises applications.



Specifically for this scenario, you can use Amazon FSx File Gateway to support the SMB file share for the on-premises application. It also meets the requirement for low-latency access. Amazon FSx File Gateway helps accelerate your file-based storage migration to the cloud to enable faster performance, improved data protection, and reduced cost.

Hence, the correct answer is: AWS Storage Gateway.

AWS Virtual Private Network (VPN) is incorrect because this service is mainly used for establishing encryption connections from an on-premises network to AWS.

Amazon FSx for Windows File Server is incorrect. This won't provide low-latency access since all the files are stored on AWS, which means that they will be accessed via the internet. AWS Storage Gateway supports local caching without any development overhead making it suitable for low-latency applications.

AWS Snowball Edge is incorrect. A Snowball edge is a type of Snowball device with on-board storage and compute power that can do local processing in addition to transferring data between your local environment and the AWS Cloud. It's just a data migration tool and not a storage service.

References:

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

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

AWS Storage Gateway Overview:

<https://www.youtube.com/watch?v=pNb7xOBJjHE>

Check out this AWS Storage Gateway Cheat Sheet:

<https://tutorialsdojo.com/aws-storage-gateway/>

## QUESTION 157

A tech company is currently using Auto Scaling for their web application. A new AMI now needs to be used for launching a fleet of EC2 instances.

Which of the following changes needs to be done?

- Create a new target group.
- Create a new launch configuration.
- Do nothing. You can start directly launching EC2 instances in the Auto Scaling group with the same launch configuration.
- Create a new target group and launch configuration.

Answer: B

## Explanation:

A launch configuration is a template that an Auto Scaling group uses to launch EC2 instances. When you create a launch configuration, you specify information for the instances such as the ID of the Amazon Machine Image (AMI), the instance type, a key pair, one or more security groups, and a block device mapping. If you've launched an EC2 instance before, you specified the same information in order to launch the instance.



You can specify your launch configuration with multiple Auto Scaling groups. However, you can only specify one launch configuration for an Auto Scaling group at a time, and you can't modify a launch configuration after you've created it. Therefore, if you want to change the launch configuration for an Auto Scaling group, you must create a launch configuration and then update your Auto Scaling group with the new launch configuration.

For this scenario, you have to create a new launch configuration. Remember that you can't modify a launch configuration after you've created it.

Hence, the correct answer is: Create a new launch configuration.

The option that says: Do nothing. You can start directly launching EC2 instances in the Auto Scaling group with the same launch configuration is incorrect because what you are trying to achieve is change the AMI being used by your fleet of EC2 instances. Therefore, you need to change the launch configuration to update what your instances are using.

The option that says: create a new target group and create a new target group and launch configuration are both incorrect because you only want to change the AMI being used by your instances, and not the instances themselves. Target groups are primarily used in ELBs and not in Auto Scaling. The scenario didn't mention that the architecture has a load balancer. Therefore, you should be updating your launch configuration, not the target group.

References:

<http://docs.aws.amazon.com/autoscaling/latest/userguide/LaunchConfiguration.html>

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

Check out this AWS Auto Scaling Cheat Sheet:

<https://tutorialsdojo.com/aws-auto-scaling/>

## QUESTION 158

A company is storing its financial reports and regulatory documents in an Amazon S3 bucket. To comply with the IT audit, they tasked their Solutions Architect to track all new objects added to the bucket as well as the removed ones. It should also track whether a versioned object is permanently deleted. The Architect must configure Amazon S3 to publish notifications for these events to a queue for postprocessing and to an Amazon SNS topic that will notify the Operations team.

Which of the following is the MOST suitable solution that the Architect should implement?

- A. Create a new Amazon SNS topic and Amazon MQ. Add an S3 event notification configuration on the bucket to publish s3:ObjectAdded:\* and s3:ObjectRemoved:\* event types to SQS and SNS.
- B. Create a new Amazon SNS topic and Amazon SQS queue. Add an S3 event notification configuration on the bucket to publish s3:ObjectCreated:\* and s3:ObjectRemoved:Delete event types to SQS and SNS.
- C. Create a new Amazon SNS topic and Amazon SQS queue. Add an S3 event notification configuration on the bucket to publish s3:ObjectCreated:\* and ObjectRemoved:DeleteMarkerCreated

event types to SQS and SNS.

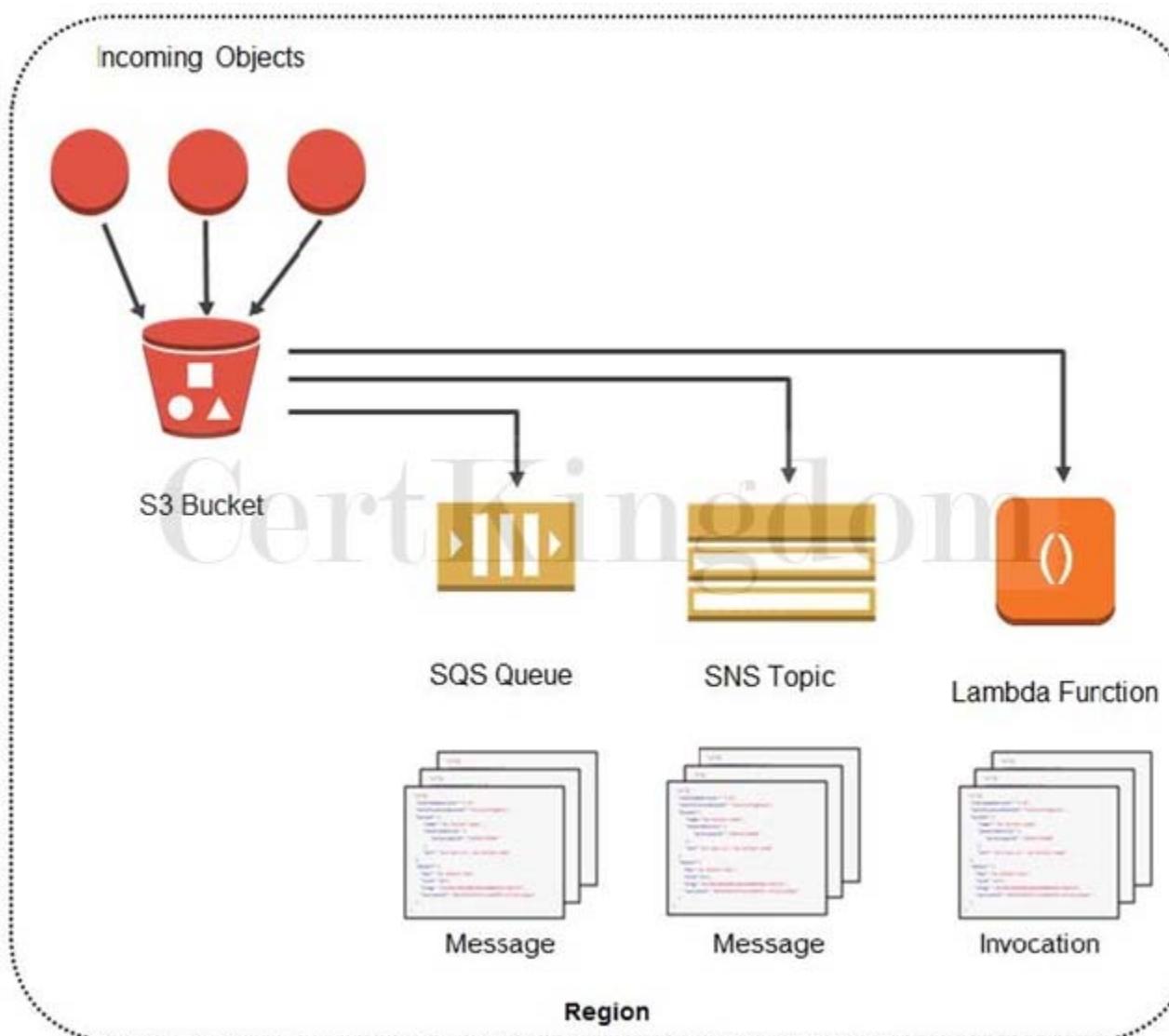
D. Create a new Amazon SNS topic and Amazon MQ. Add an S3 event notification configuration on the bucket to publish s3:ObjectCreated:\* and ObjectRemoved:DeleteMarkerCreated event types to SQS and SNS.

Answer: B

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 provides an API for you to manage this subresource.

Amazon S3 event notifications typically deliver events in seconds but can sometimes take a minute or longer. If two writes are made to a single non-versioned object at the same time, it is possible that only a single event notification will be sent. If you want to ensure that an event notification is sent for every successful write, you can enable versioning on your bucket. With versioning, every successful write will create a new version of your object and will also send an event notification.



Amazon S3 can publish notifications for the following events:

1. New object created events
2. Object removal events
3. Restore object events
4. Reduced Redundancy Storage (RRS) object lost events
5. Replication events

Event types	Description
s3:ObjectCreated:*	Amazon S3 APIs such as PUT, POST, and COPY can create an object. Using these event types, you can enable notification when an object is created using a specific API, or you can use the s3:ObjectCreated:* event type to request notification regardless of the API that was used to create an object.
s3:ObjectCreated:Put	You do not receive event notifications from failed operations.
s3:ObjectCreated:Post	
s3:ObjectCreated:Copy	
s3:ObjectCreated:CompleteMultipartUpload	
s3:ObjectRemoved:*	By using the ObjectRemoved event types, you can enable notification when an object or a batch of objects is removed from a bucket.
s3:ObjectRemoved:Delete	
s3:ObjectRemoved:DeleteMarkerCreated	You can request notification when an object is deleted or a versioned object is permanently deleted by using the s3:ObjectRemoved:Delete event type. Or you can request notification when a delete marker is created for a versioned object by using s3:ObjectRemoved:DeleteMarkerCreated. You can also use a wildcard s3:ObjectRemoved:* to request notification anytime an object is deleted.
s3:ObjectRestore:Post	You do not receive event notifications from automatic deletes from lifecycle policies or from failed operations.
s3:ObjectRestore:Completed	Using restore object event types you can receive notifications for initiation and completion when restoring objects from the S3 Glacier storage class.
s3:ReducedRedundancyLostObject	You use s3:ObjectRestore:Post to request notification of object restoration initiation. You use s3:ObjectRestore:Completed to request notification of restoration completion.
s3:Replication:OperationFailedReplication	You can use this event type to request Amazon S3 to send a notification message when Amazon S3 detects that an object of the RRS storage class is lost.
s3:Replication:OperationMissedThreshold	You receive this notification event when an object that was eligible for replication using Amazon S3 Replication Time Control failed to replicate.
s3:Replication:OperationReplicatedAfterThreshold	You receive this notification event for an object that was eligible for replication using the Amazon S3 Replication Time Control feature replicated after the 15-minute threshold.
s3:Replication:OperationNotTracked	You receive this notification event for an object that was eligible for replication using Amazon S3 Replication Time Control but is no longer tracked by replication metrics.

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

1. Amazon Simple Notification Service (Amazon SNS) topic
2. Amazon Simple Queue Service (Amazon SQS) queue
3. AWS Lambda

If your notification ends up writing to the bucket that triggers the notification, this could cause an execution loop. For example, if the bucket triggers a Lambda function each time an object is uploaded and the function uploads an object to the bucket, then the function indirectly triggers itself. To avoid this, use two buckets, or configure the trigger to only apply to a prefix used for incoming objects.

Hence, the correct answers is: Create a new Amazon SNS topic and Amazon SQS queue. Add an S3 event notification configuration on the bucket to publish s3:ObjectCreated:\* and s3:ObjectRemoved:Delete event types to SQS and SNS.

The option that says: Create a new Amazon SNS topic and Amazon MQ. Add an S3 event notification configuration on the bucket to publish s3:ObjectAdded:\* and s3:ObjectRemoved:\* event types to SQS and SNS is incorrect. There is no s3:ObjectAdded:\* type in Amazon S3. You should add an S3 event notification configuration on the bucket to publish events of the s3:ObjectCreated:\* type instead.

Moreover, Amazon S3 does support Amazon MQ as a destination to publish events.

The option that says: Create a new Amazon SNS topic and Amazon SQS queue. Add an S3 event notification configuration on the bucket to publish s3:ObjectCreated:\* and

ObjectRemoved:DeleteMarkerCreated event types to SQS and SNS is incorrect because the s3:ObjectRemoved:DeleteMarkerCreated type is only triggered when a delete marker is created for a versioned object and not when an object is deleted or a versioned object is permanently deleted.

The option that says: Create a new Amazon SNS topic and Amazon MQ. Add an S3 event notification configuration on the bucket to publish s3:ObjectCreated:\* and ObjectRemoved:DeleteMarkerCreated event types to SQS and SNS is incorrect because Amazon S3 does public event messages to Amazon MQ. You should use an Amazon SQS instead. In addition, the s3:ObjectRemoved:DeleteMarkerCreated type is only triggered when a delete marker is created for a versioned object. Remember that the scenario asked to publish events when an object is deleted or a versioned object is permanently deleted.

References:

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

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

<https://aws.amazon.com/blogs/aws/s3-event-notification/>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

### QUESTION 159

A company has a decoupled application in AWS using EC2, Auto Scaling group, S3, and SQS. The Solutions Architect designed the architecture in such a way that the EC2 instances will consume the message from the SQS queue and will automatically scale up or down based on the number of messages in the queue.

In this scenario, which of the following statements is false about SQS?

- A. Standard queues provide at-least-once delivery, which means that each message is delivered at least once.
- B. Amazon SQS can help you build a distributed application with decoupled components.
- C. FIFO queues provide exactly-once processing.
- D. Standard queues preserve the order of messages.

Answer: D

Explanation:

All of the answers are correct except for the option that says: Standard queues preserve the order of messages. Only FIFO queues can preserve the order of messages and not standard queues.

Reference:

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

Check out this Amazon SQS Cheat Sheet:

<https://tutorialsdojo.com/amazon-sqs/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

---

### QUESTION 160

A global online sports betting company has its popular web application hosted in AWS. They are planning to develop a new online portal for their new business venture and they hired you to implement the cloud architecture for a new online portal that will accept bets globally for world sports. You started to design the system with a relational database that runs on a single EC2 instance, which requires a single EBS volume that can support up to 30,000 IOPS.

In this scenario, which Amazon EBS volume type can you use that will meet the performance requirements of this new online portal?

- A. EBS Cold HDD (sc1)
- B. EBS Throughput Optimized HDD (st1)
- C. EBS Provisioned IOPS SSD (io1)
- D. EBS General Purpose SSD (gp2)

Answer: C

Explanation:

The scenario requires a storage type for a relational database with a high IOPS performance. For these scenarios, SSD volumes are more suitable to use instead of HDD volumes. Remember that the dominant performance attribute of SSD is IOPS while HDD is Throughput.

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.

Since the requirement is 30,000 IOPS, you have to use an EBS type of Provisioned IOPS SSD. This provides sustained performance for mission-critical low-latency workloads. Hence, EBS Provisioned IOPS SSD (io1) is the correct answer.

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"> <li>- Best for <b>transactional workloads</b></li> <li>- Critical business applications that require sustained IOPS performance</li> <li>- Large database workloads such as MongoDB, Oracle, Microsoft SQL Server and many others...</li> </ul>	<ul style="list-style-type: none"> <li>- Best for <b>large streaming workloads</b> requiring consistent, fast throughput at a low price</li> <li>- Big data, Data warehouses, Log processing</li> <li>- Throughput-oriented storage for large volumes of data that is <b>infrequently accessed</b></li> </ul>
Cost	moderate / high 	low 
Dominant Performance Attribute	IOPS	Throughput (MiB/s)



TutorialsDojo

EBS Throughput Optimized HDD (st1) and EBS Cold HDD (sc1) are incorrect because these are HDD volumes which are more suitable for large streaming workloads rather than transactional database workloads.

EBS General Purpose SSD (gp2) is incorrect because although a General Purpose SSD volume can be used for this scenario, it does not provide the high IOPS required by the application, unlike the Provisioned IOPS SSD volume.

Reference:

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

Amazon EBS Overview - SSD vs HDD:

<https://www.youtube.com/watch?v=LW7x8wyLFvw>

Check out this Amazon EBS Cheat Sheet:

<https://tutorialsdojo.com/amazon-ebs/>

## QUESTION 161

A Solutions Architect for a global news company is configuring a fleet of EC2 instances in a subnet that currently is in a VPC with an Internet gateway attached. All of these EC2 instances can be accessed from the Internet. The architect launches another subnet and deploys an EC2 instance in it, however, the architect is not able to access the EC2 instance from the Internet.

What could be the possible reasons for this issue? (Select TWO.)

- A. The Amazon EC2 instance does not have an attached Elastic Fabric Adapter (EFA).
- B. The Amazon EC2 instance does not have a public IP address associated with it.
- C. The route table is not configured properly to send traffic from the EC2 instance to the Internet through the customer gateway (CGW).
- D. The Amazon EC2 instance is not a member of the same Auto Scaling group.
- E. The route table is not configured properly to send traffic from the EC2 instance to the Internet through the Internet gateway.

Answer: B,E

### Explanation:

Your VPC has an implicit router and you use route tables to control where network traffic is directed. Each subnet in your VPC must be associated with a route table, which controls the routing for the subnet (subnet route table). You can explicitly associate a subnet with a particular route table. Otherwise, the subnet is implicitly associated with the main route table.

A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same subnet route table. You can optionally associate a route table with an internet gateway or a virtual private gateway (gateway route table). This enables you to specify routing rules for inbound traffic that enters your VPC through the gateway

Be sure that the subnet route table also has a route entry to the internet gateway. If this entry doesn't exist, the instance is in a private subnet and is inaccessible from the internet.

In cases where your EC2 instance cannot be accessed from the Internet (or vice versa), you usually have to check two things:

- Does it have an EIP or public IP address?

---

### QUESTION 162

A company generates large financial datasets with millions of rows. The Solutions Architect needs to store all the data in a columnar fashion to reduce the number of disk I/O requests and reduce the amount of data needed to load from the disk. The bank has an existing third-party business intelligence application that will connect to the storage service and then generate daily and monthly financial reports for its clients around the globe.

In this scenario, which is the best storage service to use to meet the requirement?

- A. Amazon DynamoDB
- B. Amazon Aurora
- C. Amazon Redshift
- D. Amazon RDS

Answer: C

### Explanation:

Amazon Redshift is a fast, scalable data warehouse that makes it simple and cost-effective to analyze all your data across your data warehouse and data lake. Redshift delivers ten times faster performance than other data warehouses by using machine learning, massively parallel query execution, and columnar storage on high-performance disk.

In this scenario, there is a requirement to have a storage service that will be used by a business intelligence application and where the data must be stored in a columnar fashion. Business Intelligence reporting systems are a type of Online Analytical Processing (OLAP) which Redshift is known to support.

In addition, Redshift also provides columnar storage, unlike the other options.

Hence, the correct answer in this scenario is Amazon Redshift.

### References:

[https://docs.aws.amazon.com/redshift/latest/dg/c\\_columnar\\_storage\\_disk\\_mem\\_mgmnt.html](https://docs.aws.amazon.com/redshift/latest/dg/c_columnar_storage_disk_mem_mgmnt.html)

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

### Amazon Redshift Overview:

<https://youtu.be/jILERNzhHOg>

### Check out this Amazon Redshift Cheat Sheet:

<https://tutorialsdojo.com/amazon-redshift/>

Here is a case study on finding the most suitable analytical tool - Kinesis vs EMR vs Athena vs Redshift:

<https://youtu.be/wEOm6aiN4ww>

---

### QUESTION 163

A company plans to use a durable storage service to store on-premises database backups to the AWS cloud. To move their backup data, they need to use a service that can store and retrieve objects through standard file storage protocols for quick recovery.

Which of the following options will meet this requirement?

- A. Use the AWS Storage Gateway volume gateway to store the backup data and directly access it using Amazon S3 API actions.
- B. Use Amazon EBS volumes to store all the backup data and attach it to an Amazon EC2 instance.
- C. Use AWS Snowball Edge to directly backup the data in Amazon S3 Glacier.
- D. Use the AWS Storage Gateway file gateway to store all the backup data in Amazon S3.

Answer: D

Explanation:

File Gateway presents a file-based interface to Amazon S3, which appears as a network file share. It enables you to store and retrieve Amazon S3 objects through standard file storage protocols. File Gateway allows your existing file-based applications or devices to use secure and durable cloud storage without needing to be modified. With File Gateway, your configured S3 buckets will be available as Network File System (NFS) mount points or Server Message Block (SMB) file shares.

img

src='https://d1.awsstatic.com/cloud-storage/File-Gateway-How-it-Works.6a5ce3c54688864e5b951df9cb8732fc4f2926b4.png'>

To store the backup data from on-premises to a durable cloud storage service, you can use File Gateway to store and retrieve objects through standard file storage protocols (SMB or NFS). File Gateway enables your existing file-based applications, devices, and workflows to use Amazon S3, without modification. File Gateway securely and durably stores both file contents and metadata as objects while providing your on-premises applications low-latency access to cached data.

Hence, the correct answer is: Use the AWS Storage Gateway file gateway to store all the backup data in Amazon S3.

The option that says: Use the AWS Storage Gateway volume gateway to store the backup data and directly access it using Amazon S3 API actions is incorrect. Although this is a possible solution, you cannot directly access the volume gateway using Amazon S3 APIs. You should use File Gateway to access your data in Amazon S3.

The option that says: Use Amazon EBS volumes to store all the backup data and attached it to an Amazon EC2 instance is incorrect. Take note that in the scenario, you are required to store the backup data in a durable storage service. An Amazon EBS volume is not highly durable like Amazon S3. Also, file storage protocols such as NFS or SMB, are not directly supported by EBS.

The option that says: Use AWS Snowball Edge to directly backup the data in Amazon S3 Glacier is incorrect because AWS Snowball Edge cannot store and retrieve objects through standard file storage protocols. Also, Snowball Edge can't directly integrate backups to S3 Glacier.

References:

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

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

Check out this AWS Storage Gateway Cheat Sheet:

<https://tutorialsdojo.com/aws-storage-gateway/>

---

## QUESTION 164

A FinTech startup deployed an application on an Amazon EC2 instance with attached Instance Store volumes and an Elastic IP address. The server is only accessed from 8 AM to 6 PM and can be stopped from 6 PM to 8 AM for cost efficiency using Lambda with the script that automates this based on tags. Which of the following will occur when the EC2 instance is stopped and started? (Select TWO.)

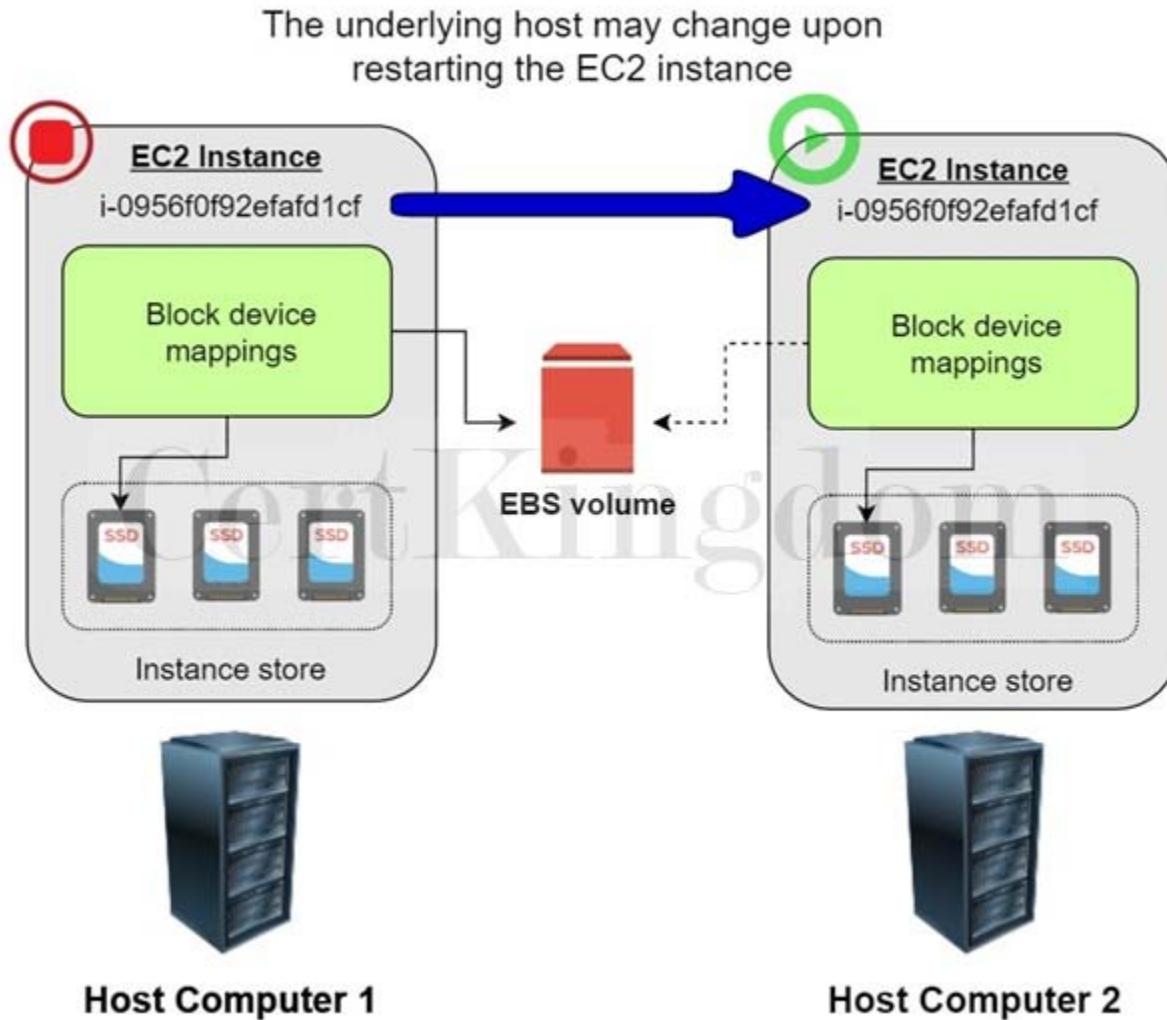
- A. The underlying host for the instance is possibly changed.
- B. The ENI (Elastic Network Interface) is detached.
- C. There will be no changes.
- D. All data on the attached instance-store devices will be lost.
- E. The Elastic IP address is disassociated with the instance.

Answer: A,D

Explanation:

This question did not mention the specific type of EC2 instance, however, it says that it will be stopped and started. Since only EBS-backed instances can be stopped and restarted, it is implied that the instance is EBS-backed. Remember that an instance store-backed instance can only be rebooted or terminated and its data will be erased if the EC2 instance is either stopped or terminated.

If you stopped an EBS-backed EC2 instance, the volume is preserved but the data in any attached instance store volume will be erased. Keep in mind that an EC2 instance has an underlying physical host computer. If the instance is stopped, AWS usually moves the instance to a new host computer. Your instance may stay on the same host computer if there are no problems with the host computer. In addition, its Elastic IP address is disassociated from the instance if it is an EC2-Classic instance. Otherwise, if it is an EC2-VPC instance, the Elastic IP address remains associated.



Take note that an EBS-backed EC2 instance can have attached Instance Store volumes. This is the reason why there is an option that mentions the Instance Store volume, which is placed to test your understanding of this specific storage type. You can launch an EBS-backed EC2 instance and attach several Instance Store volumes but remember that there are some EC2 Instance types that don't support this kind of set up.

## Create Image

X

Instance ID	i-006fcbd48ebf88e5
Image name	TutorialsDojo
Image description	Tutorials-Dojo-Manila
No reboot	<input type="checkbox"/>

### Instance Volumes

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MiB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	srab-0e4c15b8cba3e8ae6	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted
Instance Store 0	/dev/sdb	N/A	N/A	N/A	N/A	N/A	<input type="checkbox"/>	<input type="checkbox"/>
Instance Store 2	/dev/sdc	N/A	N/A	N/A	N/A	N/A	<input type="checkbox"/>	<input type="checkbox"/>
✓ EBS Instance Store 1	/dev/sdd	Search (case-insensit	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input type="checkbox"/>	<input type="checkbox"/>
Instance Store 3			16 GiB					
Instance Store 4								
Instance Store 5								
Instance Store 6								
Instance Store 7								
Instance Store 8								
Instance Store 9								
Instance Store 10								
Instance Store 11								

image, an EBS snapshot will also be created for each of the above volumes.

[Cancel](#) [Create Image](#)

Hence, the correct answers are:

- The underlying host for the instance is possibly changed.
- All data on the attached instance-store devices will be lost.

The option that says: The ENI (Elastic Network Interface) is detached is incorrect because the ENI will stay attached even if you stopped your EC2 instance.

The option that says: The Elastic IP address is disassociated with the instance is incorrect because the EIP will actually remain associated with your instance even after stopping it.

The option that says: There will be no changes is incorrect because there will be a lot of possible changes in your EC2 instance once you stop and start it again. AWS may move the virtualized EC2 instance to another host computer; the instance may get a new public IP address, and the data in your attached instance store volumes will be deleted.

References:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html#storage-for-the-root-device>

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

## QUESTION 165

A large financial firm needs to set up a Linux bastion host to allow access to the Amazon EC2 instances running in their VPC. For security purposes, only the clients connecting from the corporate external public IP address 175.45.11.326.100 should have SSH access to the host.

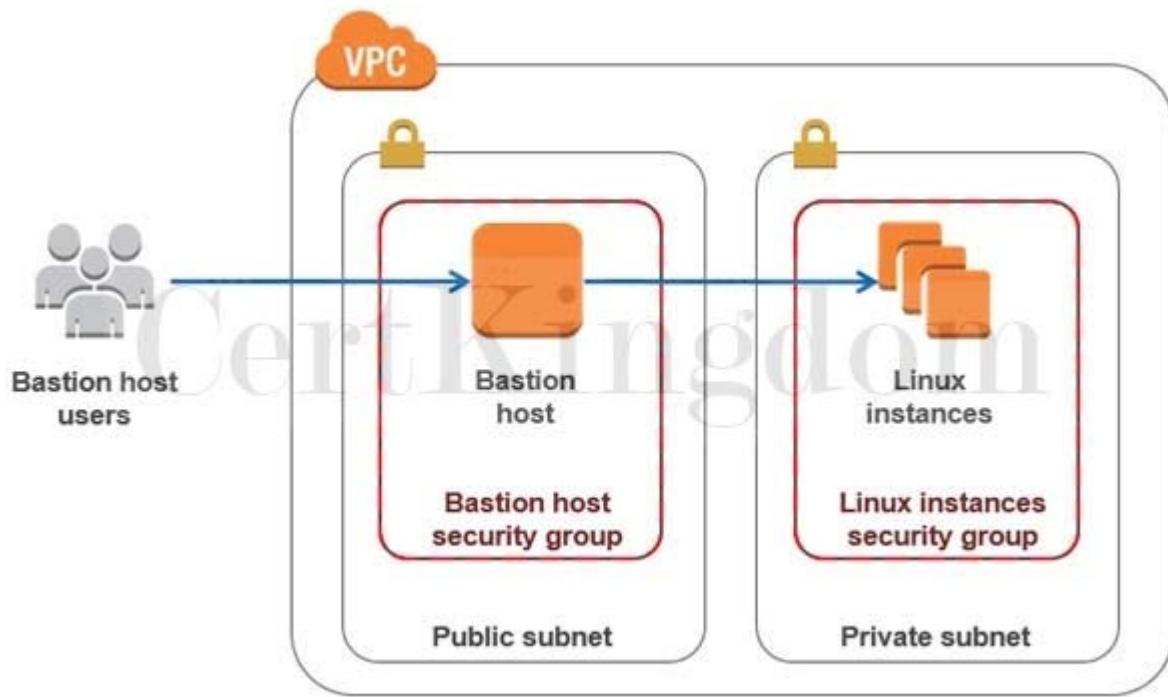
Which is the best option that can meet the customer's requirement?

- Network ACL Inbound Rule: Protocol “ TCP, Port Range-22, Source 175.45.11.326.100/0
- Security Group Inbound Rule: Protocol “ UDP, Port Range “ 22, Source 175.45.11.326.100
- Security Group Inbound Rule: Protocol “ TCP, Port Range “ 22, Source 175.45.11.326.100
- Network ACL Inbound Rule: Protocol “ UDP, Port Range “ 22, Source 175.45.11.326.100

Answer: C

Explanation:

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.



When setting up a bastion host in AWS, you should only allow the individual IP of the client and not the entire network. Therefore, in the Source, the proper CIDR notation should be used. The denotes one IP address and the /0 refers to the entire network.

The option that says: Security Group Inbound Rule: Protocol “ UDP, Port Range “ 22, Source 175.45.11./326.100 is incorrect since the SSH protocol uses TCP and port 22, and not UDP.

The option that says: Network ACL Inbound Rule: Protocol “ UDP, Port Range “ 22, Source 175.45.11./326.100 is incorrect since the SSH protocol uses TCP and port 22, and not UDP. Aside from that, network ACLs act as a firewall for your whole VPC subnet while security groups operate on an instance level. Since you are securing an EC2 instance, you should be using security groups.

The option that says: Network ACL Inbound Rule: Protocol “ TCP, Port Range-22, Source 175.45.11./326.100/0 is incorrect as it allowed the entire network instead of a single IP to gain access to the host.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

## QUESTION 166

A Solutions Architect needs to deploy a mobile application that can collect votes for a popular singing competition. Millions of users from around the world will submit votes using their mobile phones. These votes must be collected and stored in a highly scalable and highly available data store which will be queried for real-time ranking.

Which of the following combination of services should the architect use to meet this requirement?

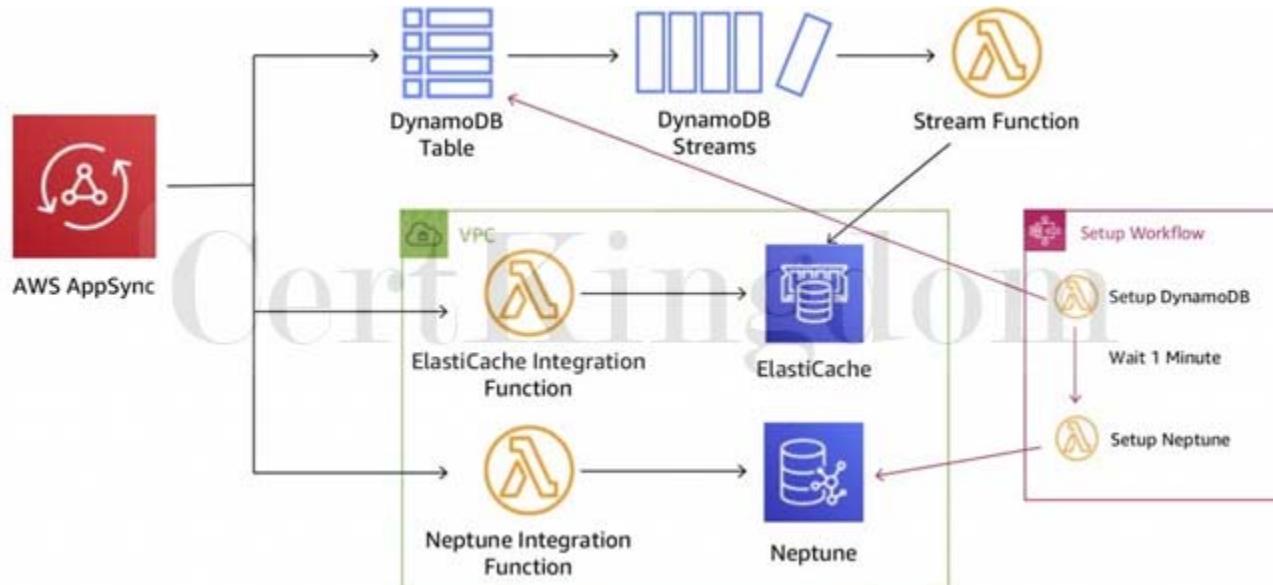
- A. Amazon DynamoDB and AWS AppSync
- B. Amazon Redshift and AWS Mobile Hub
- C. Amazon Relational Database Service (RDS) and Amazon MQ
- D. Amazon Aurora and Amazon Cognito

Answer: A

Explanation:

When the word durability pops out, the first service that should come to your mind is Amazon S3. Since

this service is not available in the answer options, we can look at the other data store available which is Amazon DynamoDB.



DynamoDB is durable, scalable, and highly available data store which can be used for real-time tabulation. You can also use AppSync with DynamoDB to make it easy for you to build collaborative apps that keep shared data updated in real time. You just specify the data for your app with simple code statements and AWS AppSync manages everything needed to keep the app data updated in real time. This will allow your app to access data in Amazon DynamoDB, trigger AWS Lambda functions, or run Amazon Elasticsearch queries and combine data from these services to provide the exact data you need for your app.

Amazon Redshift and AWS Mobile Hub are incorrect as Amazon Redshift is mainly used as a data warehouse and for online analytic processing (OLAP). Although this service can be used for this scenario, DynamoDB is still the top choice given its better durability and scalability.

Amazon Relational Database Service (RDS) and Amazon MQ and Amazon Aurora and Amazon Cognito are possible answers in this scenario, however, DynamoDB is much more suitable for simple mobile apps that do not have complicated data relationships compared with enterprise web applications. It is stated in the scenario that the mobile app will be used from around the world, which is why you need a data storage service which can be supported globally. It would be a management overhead to implement multi-region deployment for your RDS and Aurora database instances compared to using the Global table feature of DynamoDB.

#### References:

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

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

#### Amazon DynamoDB Overview:

<https://www.youtube.com/watch?v=3ZOyUNIeorU>

Check out this Amazon DynamoDB Cheat Sheet:

<https://tutorialsdojo.com/amazon-dynamodb/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

---

#### QUESTION 167

A company plans to set up a cloud infrastructure in AWS. In the planning, it was discussed that you need to deploy two EC2 instances that should continuously run for three years. The CPU utilization of the EC2 instances is also expected to be stable and predictable.

Which is the most cost-efficient Amazon EC2 Pricing type that is most appropriate for this scenario?

- A. Spot instances
- B. On-Demand instances
- C. Reserved Instances

## D. Dedicated Hosts

Answer: C

Explanation:

Reserved Instances provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. In addition, when Reserved Instances are assigned to a specific Availability Zone, they provide a capacity reservation, giving you additional confidence in your ability to launch instances when you need them.

The screenshot shows the 'Purchase Reserved Instances' interface. At the top, there are filters for Platform (Linux/UNIX), Tenancy (Default), Offering Class (Convertible), and Payment Option (Any). Below these, a search bar and a checkbox for 'Only show offerings that reserve capacity' are present. The main table lists three reserved instance offerings for 'c4.large' instances. Each row includes columns for Seller (AWS), Term (36 months), Effective Rate, Upfront Price, Hourly Rate, Payment Option, Offering Class, Quantity Available, and Desired Quantity. Buttons for 'Add to Cart' are provided for each row. At the bottom, a message states 'You currently have no items in your cart.' with 'Cancel' and 'View Cart' buttons.

Seller	Term	Effective Rate	Upfront Price	Hourly Rate	Payment Option	Offering Class	Quantity Available	Desired Quantity	Add to Cart
AWS	36 months	\$0.059	\$1,555.00	\$0.000	All Upfront	convertible	Unlimited	1	Add to Cart
AWS	36 months	\$0.060	\$797.00	\$0.030	Partial Upfront	convertible	Unlimited	1	Add to Cart
AWS	36 months	\$0.070	\$0.00	\$0.070	No Upfront	convertible	Unlimited	1	Add to Cart

For applications that have steady state or predictable usage, Reserved Instances can provide significant savings compared to using On-Demand instances.

Reserved Instances are recommended for:

- Applications with steady state usage
- Applications that may require reserved capacity
- Customers that can commit to using EC2 over a 1 or 3 year term to reduce their total computing costs

References:

<https://aws.amazon.com/ec2/pricing/>

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

Amazon EC2 Overview:

[https://www.youtube.com/watch?v=7VsGIHT\\_jQE](https://www.youtube.com/watch?v=7VsGIHT_jQE)

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

## QUESTION 168

A company needs to collect gigabytes of data per second from websites and social media feeds to gain insights into its product offerings and continuously improve the user experience. To meet this design requirement, an application is deployed on an Auto Scaling group of Spot EC2 instances which processes the data and stores the results to DynamoDB and Redshift. The solution should have a built-in enhanced fan-out feature.

Which fully-managed AWS service can you use to collect and process large streams of data records in real-time with the LEAST amount of administrative overhead?

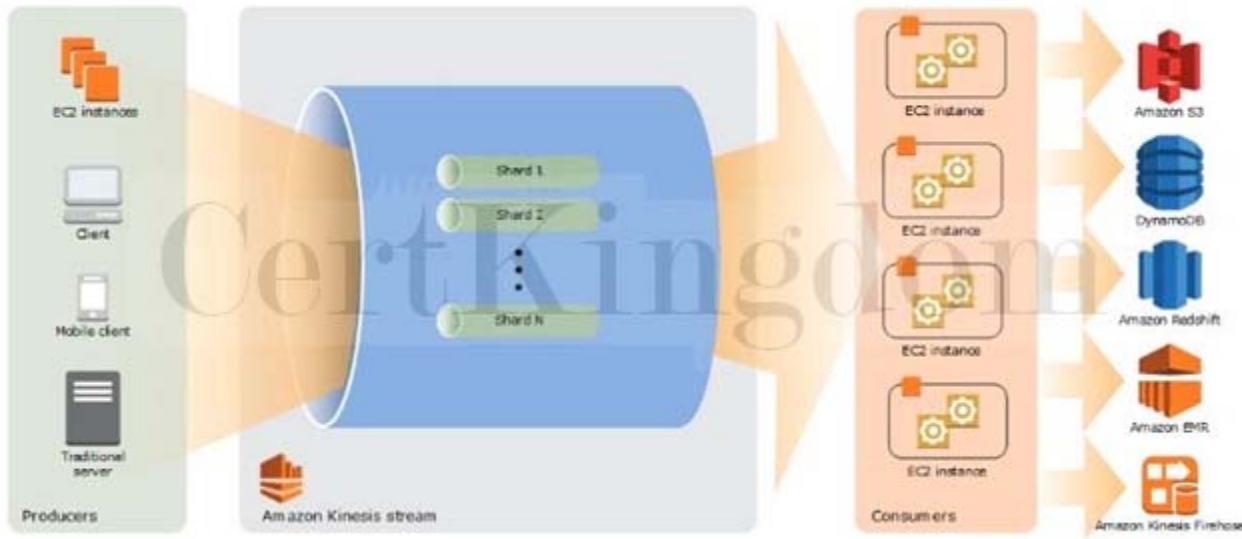
- A. Amazon Kinesis Data Streams
- B. Amazon S3 Access Points
- C. Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- D. AWS Data Exchange

Answer: A

#### Explanation:

Amazon Kinesis Data Streams is used to collect and process large streams of data records in real-time. You can use Kinesis Data Streams for rapid and continuous data intake and aggregation. The type of data used includes IT infrastructure log data, application logs, social media, market data feeds, and web clickstream data. Because the response time for the data intake and processing is in real-time, the processing is typically lightweight.

The following diagram illustrates the high-level architecture of Kinesis Data Streams. The producers continually push data to Kinesis Data Streams, and the consumers process the data in real-time. Consumers (such as a custom application running on Amazon EC2 or an Amazon Kinesis Data Firehose delivery stream) can store their results using an AWS service such as Amazon DynamoDB, Amazon Redshift, or Amazon S3.



Hence, the correct answer is: Amazon Kinesis Data Streams.

Amazon S3 Access Points is incorrect because this is mainly used to manage access of your S3 objects. Amazon S3 access points are named network endpoints that are attached to buckets that you can use to perform S3 object operations, such as uploading and retrieving objects.

AWS Data Exchange is incorrect because this is just a data marketplace service.

Amazon Managed Streaming for Apache Kafka (Amazon MSK) is incorrect. Although you can process streaming data in real-time with Amazon MSK, this service still entails a lot of administrative overhead, unlike Amazon Kinesis. Moreover, it doesn't have a built-in enhanced fan-out feature as required in the scenario.

#### References:

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

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

Check out this Amazon Kinesis Cheat Sheet:

<https://tutorialsdojo.com/amazon-kinesis/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

---

#### QUESTION 169

A Solutions Architect working for a startup is designing a High Performance Computing (HPC) application which is publicly accessible for their customers. The startup founders want to mitigate distributed denial-of-service (DDoS) attacks on their application.

Which of the following options are not suitable to be implemented in this scenario? (Select TWO.)

- A. Use an Amazon CloudFront service for distributing both static and dynamic content.
- B. Add multiple Elastic Fabric Adapters (EFA) to each EC2 instance to increase the network

bandwidth.

C. Use Dedicated EC2 instances to ensure that each instance has the maximum performance possible.

D. Use an Application Load Balancer with Auto Scaling groups for your EC2 instances. Prevent direct Internet traffic to your Amazon RDS database by deploying it to a new private subnet.

E. Use AWS Shield and AWS WAF.

Answer: B,C

Explanation:

Take note that the question asks about the viable mitigation techniques that are NOT suitable to prevent Distributed Denial of Service (DDoS) attack.

A Denial of Service (DoS) attack is an attack that can make your website or application unavailable to end users. To achieve this, attackers use a variety of techniques that consume network or other resources, disrupting access for legitimate end users.

To protect your system from DDoS attack, you can do the following:

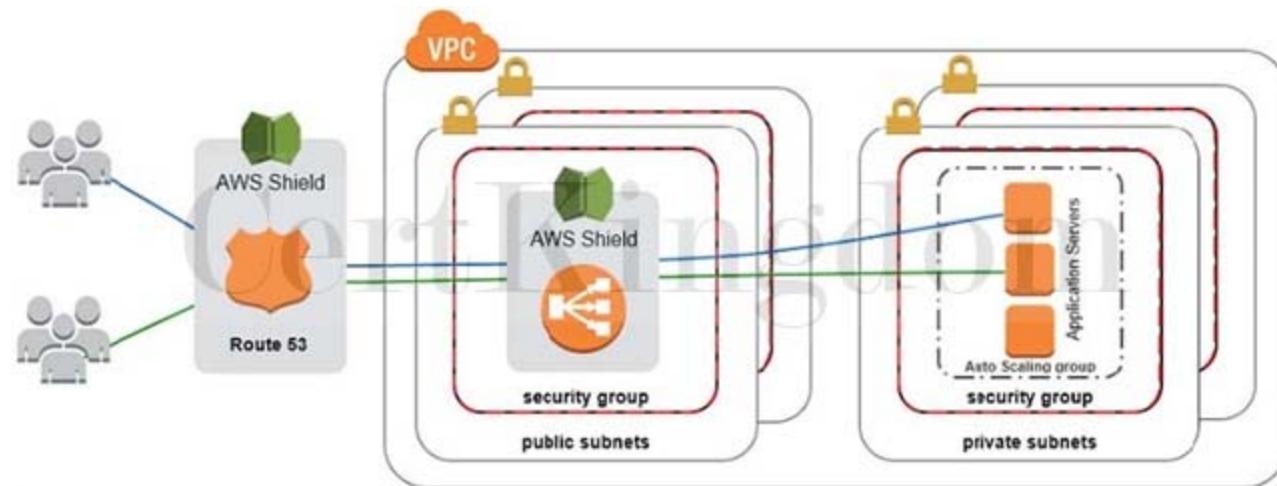
- Use an Amazon CloudFront service for distributing both static and dynamic content.
- Use an Application Load Balancer with Auto Scaling groups for your EC2 instances then restrict direct Internet traffic to your Amazon RDS database by deploying to a private subnet.

- Set up alerts in Amazon CloudWatch to look for high Network In and CPU utilization metrics.

Services that are available within AWS Regions, like Elastic Load Balancing and Amazon Elastic Compute Cloud (EC2), allow you to build Distributed Denial of Service resiliency and scale to handle unexpected volumes of traffic within a given region. Services that are available in AWS edge locations, like Amazon CloudFront, AWS WAF, Amazon Route53, and Amazon API Gateway, allow you to take advantage of a global network of edge locations that can provide your application with greater fault tolerance and increased scale for managing larger volumes of traffic.

In addition, you can also use AWS Shield and AWS WAF to fortify your cloud network. AWS Shield is a managed DDoS protection service that is available in two tiers: Standard and Advanced. AWS Shield Standard applies always-on detection and inline mitigation techniques, such as deterministic packet filtering and priority-based traffic shaping, to minimize application downtime and latency.

AWS WAF is a web application firewall that helps protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. You can use AWS WAF to define customizable web security rules that control which traffic accesses your web applications. If you use AWS Shield Advanced, you can use AWS WAF at no extra cost for those protected resources and can engage the DRT to create WAF rules.



Using Dedicated EC2 instances to ensure that each instance has the maximum performance possible is not a viable mitigation technique because Dedicated EC2 instances are just an instance billing option. Although it may ensure that each instance gives the maximum performance, that by itself is not enough to mitigate a DDoS attack.

Adding multiple Elastic Fabric Adapters (EFA) to each EC2 instance to increase the network bandwidth is also not a viable option as this is mainly done for performance improvement, and not for DDoS attack mitigation. Moreover, you can attach only one EFA per EC2 instance. An Elastic Fabric Adapter (EFA) is

a network device that you can attach to your Amazon EC2 instance to accelerate High-Performance Computing (HPC) and machine learning applications.

The following options are valid mitigation techniques that can be used to prevent DDoS:

- Use an Amazon CloudFront service for distributing both static and dynamic content.
- Use an Application Load Balancer with Auto Scaling groups for your EC2 instances. Prevent direct Internet traffic to your Amazon RDS database by deploying it to a new private subnet.
- Use AWS Shield and AWS WAF.

References:

<https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/>

[https://d0.awsstatic.com/whitepapers/DDoS\\_White\\_Paper\\_June2015.pdf](https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf)

Best practices on DDoS Attack Mitigation:

<https://youtu.be/HnoZS5jj7pk/>

---

## QUESTION 170

A company plans to build a web architecture using On-Demand EC2 instances and a database in AWS. However, due to budget constraints, the company instructed the Solutions Architect to choose a database service in which they no longer need to worry about database management tasks such as hardware or software provisioning, setup, configuration, scaling, and backups.

Which of the following services should the Solutions Architect recommend?

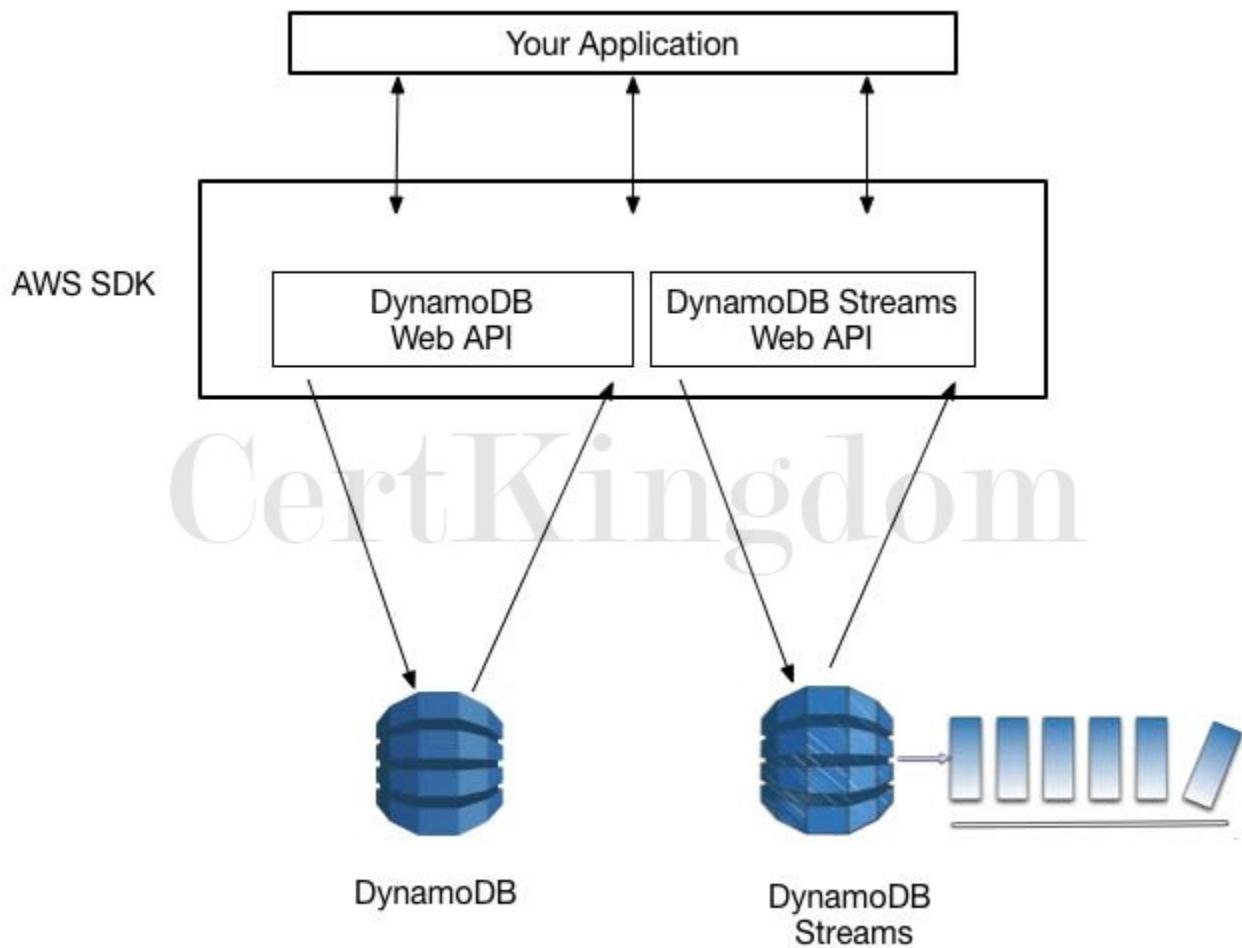
- A. Amazon RDS
- B. Amazon DynamoDB
- C. Amazon Redshift
- D. Amazon ElastiCache

Answer: B

Explanation:

Basically, a database service in which you no longer need to worry about database management tasks such as hardware or software provisioning, setup, and configuration is called a fully managed database. This means that AWS fully manages all of the database management tasks and the underlying host server. The main differentiator here is the keyword "scaling" in the question. In RDS, you still have to manually scale up your resources and create Read Replicas to improve scalability while in DynamoDB, this is automatically done.

Amazon DynamoDB is the best option to use in this scenario. It is a fully managed non-relational database service ““ you simply create a database table, set your target utilization for Auto Scaling, and let the service handle the rest. You no longer need to worry about database management tasks such as hardware or software provisioning, setup, and configuration, software patching, operating a reliable, distributed database cluster, or partitioning data over multiple instances as you scale. DynamoDB also lets you backup and restore all your tables for data archival, helping you meet your corporate and governmental regulatory requirements.



Amazon RDS is incorrect because this is just a "managed" service and not "fully managed". This means that you still have to handle the backups and other administrative tasks such as when the automated OS patching will take place.

Amazon ElastiCache is incorrect. Although ElastiCache is fully managed, it is not a database service but an In-Memory Data Store.

Amazon Redshift is incorrect. Although this is fully managed, it is not a database service but a Data Warehouse.

#### References:

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

<https://aws.amazon.com/products/databases/>

Check out this Amazon DynamoDB Cheat Sheet:

<https://tutorialsdojo.com/amazon-dynamodb/>

---

#### QUESTION 171

A media company recently launched their newly created web application. Many users tried to visit the website, but they are receiving a 503 Service Unavailable Error. The system administrator tracked the EC2 instance status and saw the capacity is reaching its maximum limit and unable to process all the requests. To gain insights from the application's data, they need to launch a real-time analytics service. Which of the following allows you to read records in batches?

- A. Create an Amazon S3 bucket to store the captured data and use Amazon Athena to analyze the data.
- B. Create an Amazon S3 bucket to store the captured data and use Amazon Redshift Spectrum to analyze the data.
- C. Create a Kinesis Data Firehose and use AWS Lambda to read records from the data stream.
- D. Create a Kinesis Data Stream and use AWS Lambda to read records from the data stream.

Answer: D

## Explanation:

Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. KDS can continuously capture gigabytes of data per second from hundreds of thousands of sources. You can use an AWS Lambda function to process records in Amazon KDS. By default, Lambda invokes your function as soon as records are available in the stream. Lambda can process up to 10 batches in each shard simultaneously. If you increase the number of concurrent batches per shard, Lambda still ensures in-order processing at the partition-key level.



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 upscaling capacity for other functions.

Since the media company needs a real-time analytics service, you can use Kinesis Data Streams to gain insights from your data. The data collected is available in milliseconds. Use AWS Lambda to read records in batches and invoke your function to process records from the batch. If the batch that Lambda reads from the stream only has one record in it, Lambda sends only one record to the function.

Hence, the correct answer in this scenario is: Create a Kinesis Data Stream and use AWS Lambda to read records from the data stream.

The option that says: Create a Kinesis Data Firehose and use AWS Lambda to read records from the data stream is incorrect. Although Amazon Kinesis Data Firehose captures and loads data in near realtime, AWS Lambda can't be set as its destination. You can write Lambda functions and integrate it with Kinesis Data Firehose to request additional, customized processing of the data before it is sent downstream. However, this integration is primarily used for stream processing and not the actual consumption of the data stream. You have to use a Kinesis Data Stream in this scenario.

The options that say: Create an Amazon S3 bucket to store the captured data and use Amazon Athena to analyze the data and Create an Amazon S3 bucket to store the captured data and use Amazon Redshift Spectrum to analyze the data are both incorrect. As per the scenario, the company needs a real-time analytics service that can ingest and process data. You need to use Amazon Kinesis to process the data in real-time.

## References:

<https://aws.amazon.com/kinesis/data-streams/>

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

<https://aws.amazon.com/premiumsupport/knowledge-center/error-classic/>

Check out this Amazon Kinesis Cheat Sheet:

<https://tutorialsdojo.com/amazon-kinesis/>

## QUESTION 172

An application needs to retrieve a subset of data from a large CSV file stored in an Amazon S3 bucket by using simple SQL expressions. The queries are made within Amazon S3 and must only return the needed data.

Which of the following actions should be taken?

- A. Perform an S3 Select operation based on the bucket's name.
- B. Perform an S3 Select operation based on the bucket's name and object's metadata.
- C. Perform an S3 Select operation based on the bucket's name and object tags.
- D. Perform an S3 Select operation based on the bucket's name and object's key.

Answer: D

Explanation:

S3 Select enables applications to retrieve only a subset of data from an object by using simple SQL expressions. By using S3 Select to retrieve only the data needed by your application, you can achieve drastic performance increases.

The screenshot shows the AWS S3 console with the 'SQL expression' feature. On the left, there's a sidebar with options like 'Buckets', 'Batch operations', 'Access analyzer for S3', and 'Block public access (account settings)'. The main area has a heading 'SQL expression' with a note about pricing. It features a 'Sample SQL expressions' tab selected, showing a code editor with the following SQL:

```
1 select * from s3object s limit 3
2
3 -- tutorials dojo
4
5
```

Below the code editor are 'Copy' and 'Run SQL' buttons. The 'Result' section displays the output of the query:

Year,Industry\_aggregation\_NZSIOC,Industry\_code\_NZSIOC,Industry\_name\_NZSIOC,Units,Va  
2019,Level 1,99999,All industries,Dollars (millions),H01>Total income,Financial per  
2019,Level 1,99999,All industries,Dollars (millions),H04,"Sales, government funding"

At the bottom right of the result area is a 'Download' button.

Amazon S3 is composed of buckets, object keys, object metadata, object tags, and many other components as shown below:

An Amazon S3 bucket name is globally unique, and the namespace is shared by all AWS accounts.

An Amazon S3 object key refers to the key name, which uniquely identifies the object in the bucket.

An Amazon S3 object metadata is a name-value pair that provides information about the object.

An Amazon S3 object tag is a key-pair value used for object tagging to categorize storage.

You can perform S3 Select to query only the necessary data inside the CSV files based on the bucket's name and the object's key.

The following snippet below shows how it is done using boto3 ( AWS SDK for Python ):

```
client = boto3.client('s3')
```

```
resp = client.select_object_content(  
Bucket='tdojo-bucket', # Bucket Name.  
Key='s3-select/tutorialsdojofile.csv', # Object Key.  
ExpressionType= 'SQL',  
Expression = "select \\"Sample\\" from s3object s where s.\\"tutorialsdojofile\\" in ['A', 'B']"
```

Hence, the correct answer is the option that says: Perform an S3 Select operation based on the bucket's name and object's key.

The option that says: Perform an S3 Select operation based on the bucket's name and object's metadata is incorrect because metadata is not needed when querying subsets of data in an object using S3 Select.

The option that says: Perform an S3 Select operation based on the bucket's name and object tags is incorrect because object tags just provide additional information to your object. This is not needed when querying with S3 Select although this can be useful for S3 Batch Operations. You can categorize objects based on tag values to provide S3 Batch Operations with a list of objects to operate on.

The option that says: Perform an S3 Select operation based on the bucket's name is incorrect because you need both the bucket's name and the object key to successfully perform an S3 Select operation.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-glacier-select-sql-reference-select.html>

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

---

## QUESTION 173

A Solutions Architect is working for a large insurance firm. To maintain compliance with HIPAA laws, all data that is backed up or stored on Amazon S3 needs to be encrypted at rest.

In this scenario, what is the best method of encryption for the data, assuming S3 is being used for storing financial-related data? (Select TWO.)

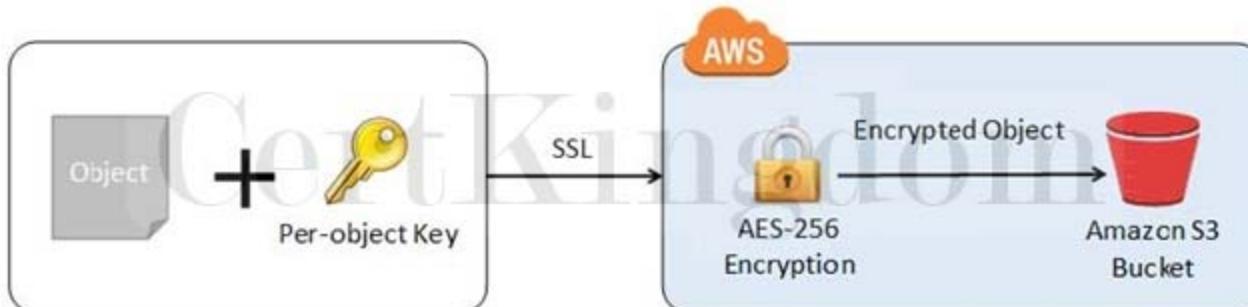
- A. Enable SSE on an S3 bucket to make use of AES-256 encryption
- B. Use AWS Shield to protect your data at rest
- C. Encrypt the data using your own encryption keys then copy the data to Amazon S3 over HTTPS endpoints.
- D. Store the data on EBS volumes with encryption enabled instead of using Amazon S3
- E. Store the data in encrypted EBS snapshots

Answer: A,C

Explanation:

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options for protecting data at rest in Amazon S3. Use Server-Side Encryption “ You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

Use Client-Side Encryption “ You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.



Hence, the following options are the correct answers:

- Enable SSE on an S3 bucket to make use of AES-256 encryption
- Encrypt the data using your own encryption keys then copy the data to Amazon S3 over HTTPS endpoints. This refers to using a Server-Side Encryption with Customer-Provided Keys (SSE-C). Storing the data in encrypted EBS snapshots and storing the data on EBS volumes with encryption enabled instead of using Amazon S3 are both incorrect because all these options are for protecting your data in your EBS volumes. Note that an S3 bucket does not use EBS volumes to store your data.
- Using AWS Shield to protect your data at rest is incorrect because AWS Shield is mainly used to protect your entire VPC against DDoS attacks.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

---

## QUESTION 174

You are automating the creation of EC2 instances in your VPC. Hence, you wrote a python script to trigger the Amazon EC2 API to request 50 EC2 instances in a single Availability Zone. However, you noticed that after 20 successful requests, subsequent requests failed.

What could be a reason for this issue and how would you resolve it?

- A. By default, AWS allows you to provision a maximum of 20 instances per region. Select a different region and retry the failed request.
- B. By default, AWS allows you to provision a maximum of 20 instances per Availability Zone. Select a different Availability Zone and retry the failed request.
- C. There was an issue with the Amazon EC2 API. Just resend the requests and these will be provisioned successfully.
- D. There is a vCPU-based On-Demand Instance limit per region which is why subsequent requests failed. Just submit the limit increase form to AWS and retry the failed requests once approved.

Answer: D

Explanation:

You are limited to running On-Demand Instances per your vCPU-based On-Demand Instance limit, purchasing 20 Reserved Instances, and requesting Spot Instances per your dynamic Spot limit per region. New AWS accounts may start with limits that are lower than the limits described here.



## Calculate vCPU limit

### Calculate number of vCPUs needed

Use this tool to calculate how many vCPUs you need to launch your On-Demand Instances.

Select the instance type and the number of instances you require. The calculator will display the number of vCPUs assigned to the selected instances. Use the New Limit value as a guide for requesting a limit increase.

Instance type	Instance count	vCPU count	Current limit	New limit
t2.medium	12	24 vCPUs	1,920 vCPUs	1,944 vCPUs

**Add instance type**

Limits calculation				
Instance limit name	Current limit	vCPUs needed	New limit	Options
All Standard (A, C, D, H, I, M, R, T, Z) instances	1,920 vCPUs	24 vCPUs	1,944 vCPUs	<a href="#">Request limit increase</a>

**Close**

Tutorials Dojo

If you need more instances, complete the Amazon EC2 limit increase request form with your use case, and your limit increase will be considered. Limit increases are tied to the region they were requested for. Hence, the correct answer is: There is a vCPU-based On-Demand Instance limit per region which is why subsequent requests failed. Just submit the limit increase form to AWS and retry the failed requests once approved.

The option that says: There was an issue with the Amazon EC2 API. Just resend the requests and these will be provisioned successfully is incorrect because you are limited to running On-Demand Instances per your vCPU-based On-Demand Instance limit. There is also a limit of purchasing 20 Reserved Instances, and requesting Spot Instances per your dynamic Spot limit per region hence, there is no problem with the EC2 API.

The option that says: By default, AWS allows you to provision a maximum of 20 instances per region. Select a different region and retry the failed request is incorrect. There is no need to select a different region since this limit can be increased after submitting a request form to AWS.

The option that says: By default, AWS allows you to provision a maximum of 20 instances per Availability Zone. Select a different Availability Zone and retry the failed request is incorrect because the vCPU-based On-Demand Instance limit is set per region and not per Availability Zone. This can be increased after submitting a request form to AWS.

References:

[https://docs.aws.amazon.com/general/latest/gr/aws\\_service\\_limits.html#limits\\_ec2](https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_ec2)

[https://aws.amazon.com/ec2/faqs/#How\\_many\\_instances\\_can\\_I\\_run\\_in\\_Amazon\\_EC2](https://aws.amazon.com/ec2/faqs/#How_many_instances_can_I_run_in_Amazon_EC2)

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

### QUESTION 175

A company has clients all across the globe that access product files stored in several S3 buckets, which are behind each of their own CloudFront web distributions. They currently want to deliver their content to a specific client, and they need to make sure that only that client can access the data. Currently, all of

their clients can access their S3 buckets directly using an S3 URL or through their CloudFront distribution. The Solutions Architect must serve the private content via CloudFront only, to secure the distribution of files.

Which combination of actions should the Architect implement to meet the above requirements? (Select TWO.)

- A. Create a custom CloudFront function to check and ensure that only their clients can access the files.
- B. Enable the Origin Shield feature of the Amazon CloudFront distribution to protect the files from unauthorized access.
- C. Use S3 pre-signed URLs to ensure that only their client can access the files. Remove permission to use Amazon S3 URLs to read the files for anyone else.
- D. Restrict access to files in the origin by creating an origin access identity (OAI) and give it permission to read the files in the bucket.
- E. Require the users to access the private content by using special CloudFront signed URLs or signed cookies.

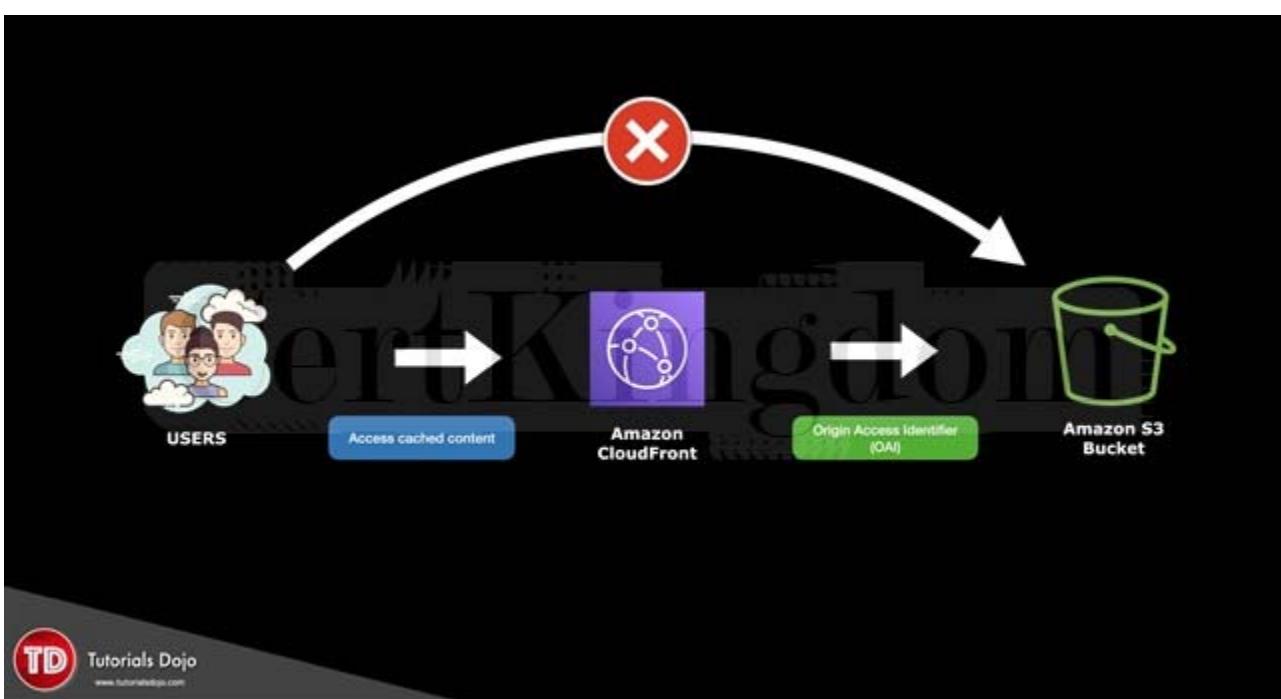
Answer: D,E

Explanation:

Many companies that distribute content over the Internet want to restrict access to documents, business data, media streams, or content that is intended for selected users, for example, users who have paid a fee. To securely serve this private content by using CloudFront, you can do the following:

- Require that your users access your private content by using special CloudFront signed URLs or signed cookies.
- Require that your users access your Amazon S3 content by using CloudFront URLs, not Amazon S3 URLs. Requiring CloudFront URLs isn't necessary, but it is recommended to prevent users from bypassing the restrictions that you specify in signed URLs or signed cookies. You can do this by setting up an origin access identity (OAI) for your Amazon S3 bucket. You can also configure the custom headers for a private HTTP server or an Amazon S3 bucket configured as a website endpoint.

All objects and buckets by default are private. The pre-signed URLs are useful if you want your user/customer to be able to upload a specific object to your bucket, but you don't require them to have AWS security credentials or permissions.



You can generate a pre-signed URL programmatically using the AWS SDK for Java or the AWS SDK for .NET. If you are using Microsoft Visual Studio, you can also use AWS Explorer to generate a pre-signed object URL without writing any code. Anyone who receives a valid pre-signed URL can then programmatically upload an object.

Hence, the correct answers are:

- Restrict access to files in the origin by creating an origin access identity (OAI) and give it permission to read the files in the bucket.
- Require the users to access the private content by using special CloudFront signed URLs or signed cookies.

The option that says: Create a custom CloudFront function to check and ensure that only their clients can access the files is incorrect. CloudFront Functions are just lightweight functions in JavaScript for high-scale, latency-sensitive CDN customizations and not for enforcing security. A CloudFront Function runtime environment offers submillisecond startup times which allows your application to scale immediately to handle millions of requests per second. But again, this can't be used to restrict access to your files.

The option that says: Enable the Origin Shield feature of the Amazon CloudFront distribution to protect the files from unauthorized access is incorrect because this feature is not primarily used for security but for improving your origin's load times, improving origin availability, and reducing your overall operating costs in CloudFront.

The option that says: Use S3 pre-signed URLs to ensure that only their client can access the files.

Remove permission to use Amazon S3 URLs to read the files for anyone else is incorrect. Although this could be a valid solution, it doesn't satisfy the requirement to serve the private content via CloudFront only to secure the distribution of files. A better solution is to set up an origin access identity (OAI) then use Signed URL or Signed Cookies in your CloudFront web distribution.

References:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>

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

Check out this Amazon CloudFront cheat sheet:

<https://tutorialsdojo.com/amazon-cloudfront/>

S3 Pre-signed URLs vs CloudFront Signed URLs vs Origin Access Identity (OAI)

<https://tutorialsdojo.com/s3-pre-signed-urls-vs-cloudfront-signed-urls-vs-origin-access-identity-oai/>

Comparison of AWS Services Cheat Sheets:

<https://tutorialsdojo.com/comparison-of-aws-services/>

---

## QUESTION 176

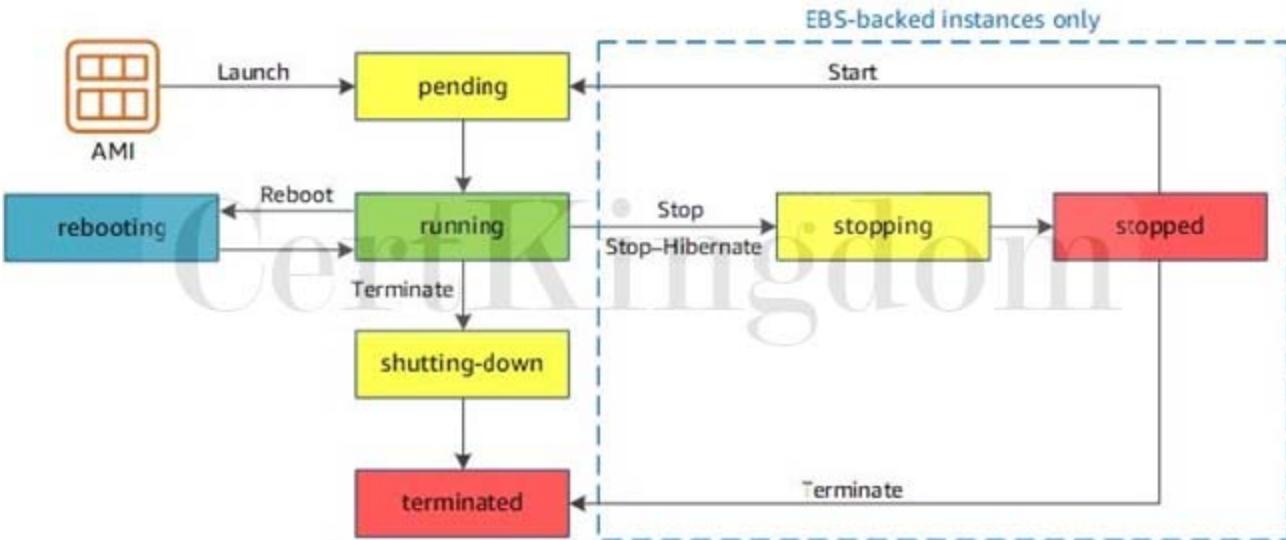
In Amazon EC2, you can manage your instances from the moment you launch them up to their termination. You can flexibly control your computing costs by changing the EC2 instance state. Which of the following statements is true regarding EC2 billing? (Select TWO.)

- A. You will be billed when your On-Demand instance is preparing to hibernate with a stopping state.
- B. You will be billed when your On-Demand instance is in pending state.
- C. You will not be billed for any instance usage while an instance is not in the running state.
- D. You will be billed when your Spot instance is preparing to stop with a stopping state.
- E. You will be billed when your Reserved instance is in terminated state.

Answer: A,E

Explanation:

By working with Amazon EC2 to manage your instances from the moment you launch them through their termination, you ensure that your customers have the best possible experience with the applications or sites that you host on your instances. The following illustration represents the transitions between instance states. Notice that you can't stop and start an instance store-backed instance:



Below are the valid EC2 lifecycle instance states:

**pending** - The instance is preparing to enter the running state. An instance enters the pending state when it launches for the first time, or when it is restarted after being in the stopped state.

**running** - The instance is running and ready for use.

**stopping** - The instance is preparing to be stopped. Take note that you will not be billed if it is preparing to stop however, you will still be billed if it is just preparing to hibernate.

**stopped** - The instance is shut down and cannot be used. The instance can be restarted at any time.

**shutting-down** - The instance is preparing to be terminated.

**terminated** - The instance has been permanently deleted and cannot be restarted. Take note that Reserved Instances that applied to terminated instances are still billed until the end of their term according to their payment option.

The option that says: You will be billed when your On-Demand instance is preparing to hibernate with a stopping state is correct because when the instance state is stopping, you will not be billed if it is preparing to stop however, you will still be billed if it is just preparing to hibernate.

The option that says: You will be billed when your Reserved instance is in terminated state is correct because Reserved Instances that applied to terminated instances are still billed until the end of their term according to their payment option. I actually raised a pull-request to Amazon team about the billing conditions for Reserved Instances, which has been approved and reflected on your official AWS Documentation: <https://github.com/awsdocs/amazon-ec2-user-guide/pull>

The option that says: You will be billed when your On-Demand instance is in pending state is incorrect because you will not be billed if your instance is in pending state.

The option that says: You will be billed when your Spot instance is preparing to stop with a stopping state is incorrect because you will not be billed if your instance is preparing to stop with a stopping state.

The option that says: You will not be billed for any instance usage while an instance is not in the running state is incorrect because the statement is not entirely true. You can still be billed if your instance is preparing to hibernate with a stopping state.

References:

<https://github.com/awsdocs/amazon-ec2-user-guide/pull>

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html>

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

## QUESTION 177

A Solutions Architect is unable to connect to the newly deployed EC2 instance via SSH using a home computer. However, the Architect was able to successfully access other existing instances in the VPC without any issues.

Which of the following should the Architect check and possibly correct to restore connectivity?

- Configure the Security Group of the EC2 instance to permit ingress traffic over port 22 from your IP.
- Configure the Security Group of the EC2 instance to permit ingress traffic over port 3389 from your

IP.  
C. Use Amazon Data Lifecycle Manager.

D. Configure the Network Access Control List of your VPC to permit ingress traffic over port 22 from your IP.

Answer: A

Explanation:

When connecting to your EC2 instance via SSH, you need to ensure that port 22 is allowed on the security group of your EC2 instance.

A security group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group.



Using Amazon Data Lifecycle Manager is incorrect because this is primarily used to manage the lifecycle of your AWS resources and not to allow certain traffic to go through.

Configuring the Network Access Control List of your VPC to permit ingress traffic over port 22 from your IP is incorrect because this is not necessary in this scenario as it was specified that you were able to connect to other EC2 instances. In addition, Network ACL is much suitable to control the traffic that goes in and out of your entire VPC and not just on one EC2 instance.

Configure the Security Group of the EC2 instance to permit ingress traffic over port 3389 from your IP is incorrect because this is relevant to RDP and not SSH.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html>

Check out these AWS Comparison of Services Cheat Sheets:

<https://tutorialsdojo.com/comparison-of-aws-services/>

---

## QUESTION 178

A data analytics company is setting up an innovative checkout-free grocery store. Their Solutions Architect developed a real-time monitoring application that uses smart sensors to collect the items that the customers are getting from the grocery's refrigerators and shelves then automatically deduct it from their accounts. The company wants to analyze the items that are frequently being bought and store the results in S3 for durable storage to determine the purchase behavior of its customers.

What service must be used to easily capture, transform, and load streaming data into Amazon S3, Amazon Elasticsearch Service, and Splunk?

- A. Amazon SQS
- B. Amazon Redshift
- C. Amazon Kinesis Data Firehose
- D. Amazon Kinesis

Answer: C

Explanation:

Amazon Kinesis Data Firehose is the easiest way to load streaming data into data stores and analytics tools. It can capture, transform, and load streaming data into Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk, enabling near real-time analytics with existing business intelligence tools and dashboards you are already using today.

It is a fully managed service that automatically scales to match the throughput of your data and requires no ongoing administration. It can also batch, compress, and encrypt the data before loading it, minimizing the amount of storage used at the destination and increasing security.

In the diagram below, you gather the data from your smart refrigerators and use Kinesis Data firehouse to prepare and load the data. S3 will be used as a method of durably storing the data for analytics and the eventual ingestion of data for output using analytical tools.



You can use Amazon Kinesis Data Firehose in conjunction with Amazon Kinesis Data Streams if you need to implement real-time processing of streaming big data. Kinesis Data Streams provides an ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications. The Amazon Kinesis Client Library (KCL) delivers all records for a given partition key to the same record processor, making it easier to build multiple applications reading from the same Amazon Kinesis data stream (for example, to perform counting, aggregation, and filtering). Amazon Simple Queue Service (Amazon SQS) is different from Amazon Kinesis Data Firehose. SQS offers a reliable, highly scalable hosted queue for storing messages as they travel between computers. Amazon SQS lets you easily move data between distributed application components and helps you build applications in which messages are processed independently (with message-level ack/fail semantics), such as automated workflows. Amazon Kinesis Data Firehose is primarily used to load streaming data into data stores and analytics tools.

Hence, the correct answer is: Amazon Kinesis Data Firehose.

Amazon Kinesis is incorrect because this is the streaming data platform of AWS and has four distinct services under it: Kinesis Data Firehose, Kinesis Data Streams, Kinesis Video Streams, and Amazon Kinesis Data Analytics. For the specific use case just as asked in the scenario, use Kinesis Data Firehose.

Amazon Redshift is incorrect because this is mainly used for data warehousing making it simple and cost-effective to analyze your data across your data warehouse and data lake. It does not meet the requirement of being able to load and stream data into data stores for analytics. You have to use Kinesis Data Firehose instead.

Amazon SQS is incorrect because you can't capture, transform, and load streaming data into Amazon S3, Amazon Elasticsearch Service, and Splunk using this service. You have to use Kinesis Data Firehose instead.

References:

<https://aws.amazon.com/kinesis/data-firehose/>

<https://aws.amazon.com/kinesis/data-streams/faqs/>

## QUESTION 179

A document sharing website is using AWS as its cloud infrastructure. Free users can upload a total of 5 GB data while premium users can upload as much as 5 TB. Their application uploads the user files, which can have a max file size of 1 TB, to an S3 Bucket.

In this scenario, what is the best way for the application to upload the large files in S3?

- A. Use AWS Snowball
- B. Use AWS Import/Export
- C. Use Multipart Upload
- D. Use a single PUT request to upload the large file

Answer: C

Explanation:

The total volume of data and number of objects you can store are unlimited. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 5 terabytes. The largest object that can be uploaded in a single PUT is 5 gigabytes. For objects larger than 100 megabytes, customers should consider using the Multipart Upload capability.

The Multipart upload API enables you to upload large objects in parts. You can use this API to upload new large objects or make a copy of an existing object. Multipart uploading is a three-step process: you initiate the upload, you upload the object parts, and after you have uploaded all the parts, you complete the multipart upload. Upon receiving the complete multipart upload request, Amazon S3 constructs the object from the uploaded parts and you can then access the object just as you would any other object in your bucket.

Using a single PUT request to upload the large file is incorrect because the largest file size you can upload using a single PUT request is 5 GB. Files larger than this will fail to be uploaded.

Using AWS Snowball is incorrect because this is a migration tool that lets you transfer large amounts of data from your on-premises data center to AWS S3 and vice versa. This tool is not suitable for the given scenario. And when you provision Snowball, the device gets transported to you, and not to your customers. Therefore, you bear the responsibility of securing the device.

Using AWS Import/Export is incorrect because Import/Export is similar to AWS Snowball in such a way that it is meant to be used as a migration tool, and not for multiple customer consumption such as in the given scenario.

References:

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

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

---

## QUESTION 180

An investment bank is working with an IT team to handle the launch of the new digital wallet system. The applications will run on multiple EBS-backed EC2 instances which will store the logs, transactions, and billing statements of the user in an S3 bucket. Due to tight security and compliance requirements, the IT team is exploring options on how to safely store sensitive data on the EBS volumes and S3.

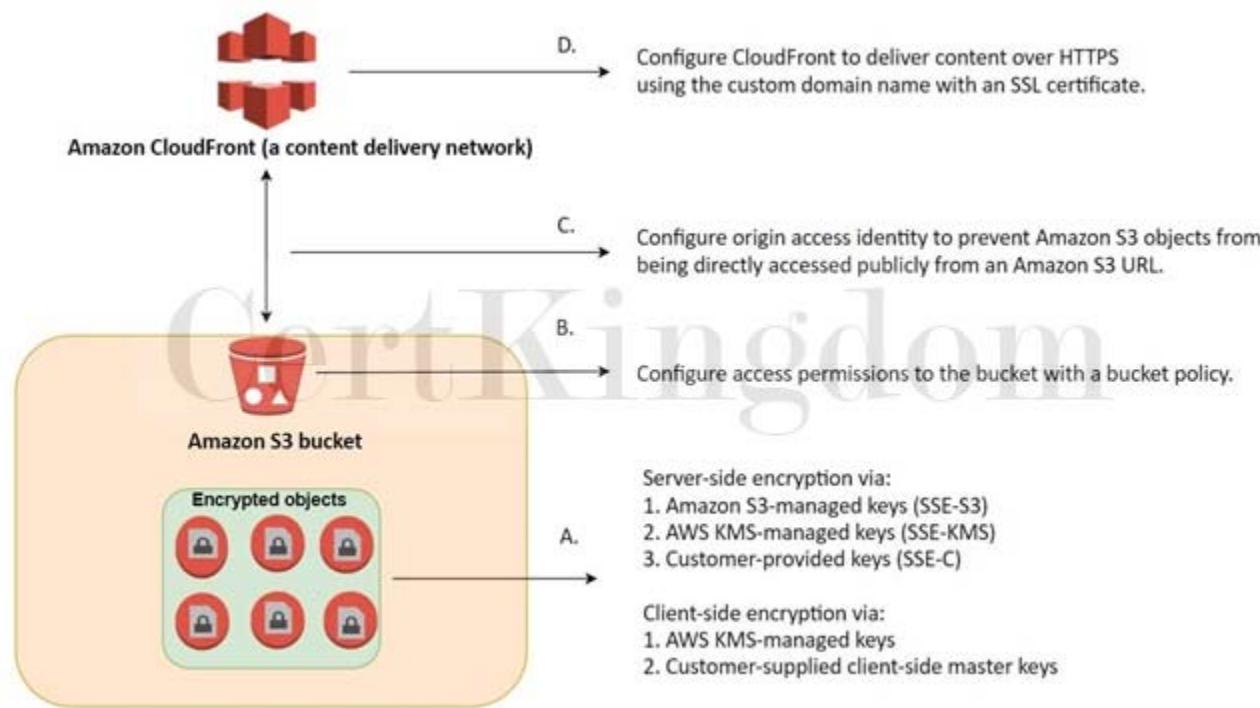
Which of the below options should be carried out when storing sensitive data on AWS? (Select TWO.)

- A. Migrate the EC2 instances from the public to private subnet.
- B. Enable Amazon S3 Server-Side or use Client-Side Encryption
- C. Use AWS Shield and WAF
- D. Create an EBS Snapshot
- E. Enable EBS Encryption

Answer: B,E

Explanation:

Enabling EBS Encryption and enabling Amazon S3 Server-Side or use Client-Side Encryption are correct. Amazon EBS encryption offers a simple encryption solution for your EBS volumes without the need to build, maintain, and secure your own key management infrastructure.



In Amazon S3, data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options to protect data at rest in Amazon S3.

Use Server-Side Encryption ““ You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

Use Client-Side Encryption ““ You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Creating an EBS Snapshot is incorrect because this is a backup solution of EBS. It does not provide security of data inside EBS volumes when executed.

Migrating the EC2 instances from the public to private subnet is incorrect because the data you want to secure are those in EBS volumes and S3 buckets. Moving your EC2 instance to a private subnet involves a different matter of security practice, which does not achieve what you want in this scenario. Using AWS Shield and WAF is incorrect because these protect you from common security threats for your web applications. However, what you are trying to achieve is securing and encrypting your data inside EBS and S3.

References:

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

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

Check out this Amazon EBS Cheat Sheet:

<https://tutorialsdojo.com/amazon-ebs/>

## QUESTION 181

A major TV network has a web application running on eight Amazon T3 EC2 instances. The number of requests that the application processes are consistent and do not experience spikes. To ensure that eight instances are running at all times, the Solutions Architect should create an Auto Scaling group and distribute the load evenly between all instances.

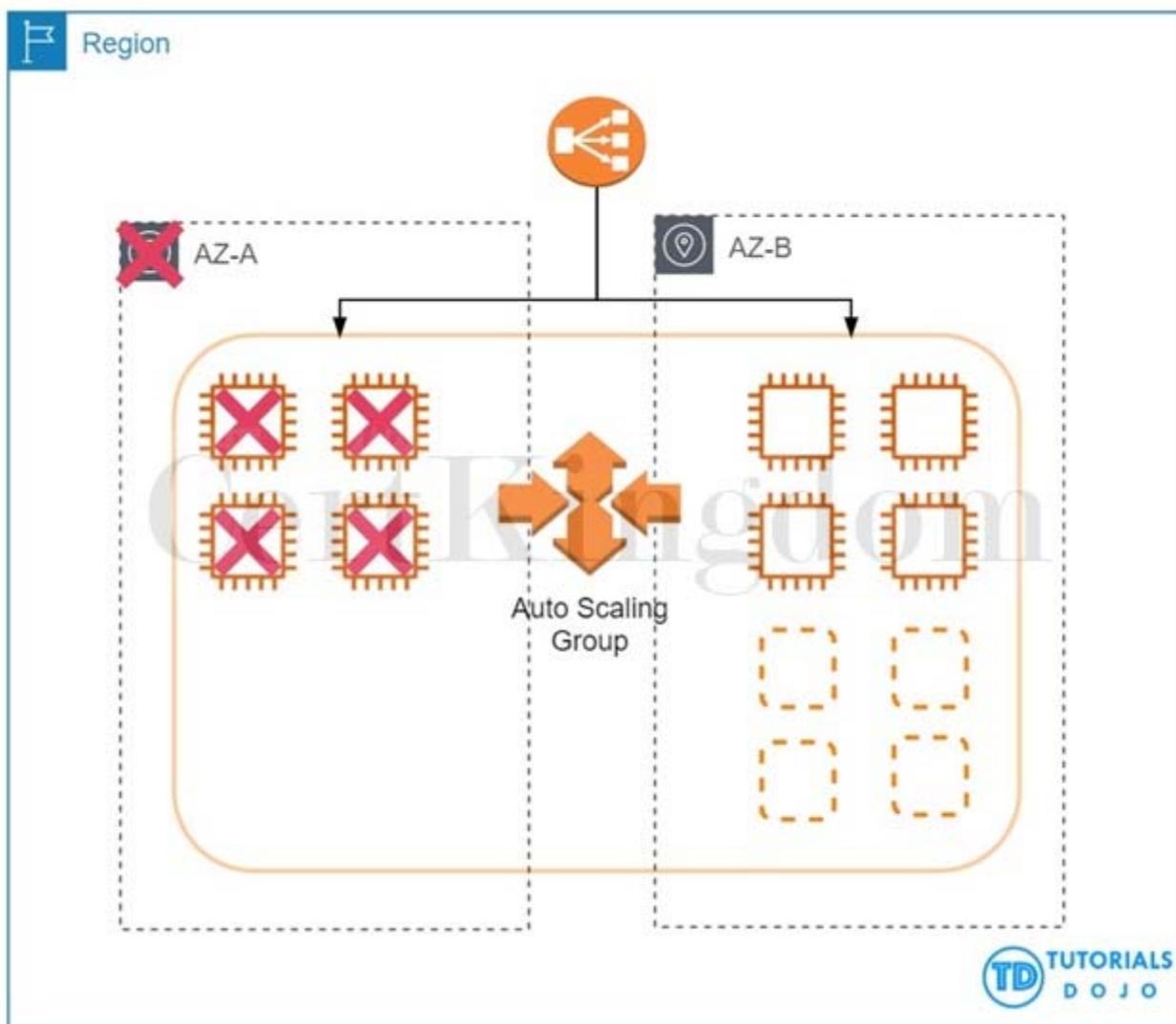
Which of the following options can satisfy the given requirements?

- A. Deploy two EC2 instances with Auto Scaling in four regions behind an Amazon Elastic Load Balancer.
- B. Deploy eight EC2 instances with Auto Scaling in one Availability Zone behind an Amazon Elastic Load Balancer.
- C. Deploy four EC2 instances with Auto Scaling in one region and four in another region behind an Amazon Elastic Load Balancer.
- D. Deploy four EC2 instances with Auto Scaling in one Availability Zone and four in another availability zone in the same region behind an Amazon Elastic Load Balancer.

Answer: D

Explanation:

The best option to take is to deploy four EC2 instances in one Availability Zone and four in another availability zone in the same region behind an Amazon Elastic Load Balancer. In this way, if one availability zone goes down, there is still another available zone that can accommodate traffic.



When the first AZ goes down, the second AZ will only have an initial 4 EC2 instances. This will eventually be scaled up to 8 instances since the solution is using Auto Scaling.

The 110% compute capacity for the 4 servers might cause some degradation of the service, but not a total outage since there are still some instances that handle the requests. Depending on your scale-up configuration in your Auto Scaling group, the additional 4 EC2 instances can be launched in a matter of minutes.

T3 instances also have a Burstable Performance capability to burst or go beyond the current compute capacity of the instance to higher performance as required by your workload. So your 4 servers will be able to manage 110% compute capacity for a short period of time. This is the power of cloud computing

versus our on-premises network architecture. It provides elasticity and unparalleled scalability. Take note that Auto Scaling will launch additional EC2 instances to the remaining Availability Zone/s in the event of an Availability Zone outage in the region. Hence, the correct answer is the option that says: Deploy four EC2 instances with Auto Scaling in one Availability Zone and four in another availability zone in the same region behind an Amazon Elastic Load Balancer.

The option that says: Deploy eight EC2 instances with Auto Scaling in one Availability Zone behind an Amazon Elastic Load Balancer is incorrect because this architecture is not highly available. If that Availability Zone goes down then your web application will be unreachable.

The options that say: Deploy four EC2 instances with Auto Scaling in one region and four in another region behind an Amazon Elastic Load Balancer and Deploy two EC2 instances with Auto Scaling in four regions behind an Amazon Elastic Load Balancer are incorrect because the ELB is designed to only run in one region and not across multiple regions.

References:

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

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

AWS Elastic Load Balancing Overview:

<https://youtu.be/UBl5dw59DO8>

Check out this AWS Elastic Load Balancing (ELB) Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

---

## QUESTION 182

A travel company has a suite of web applications hosted in an Auto Scaling group of On-Demand EC2 instances behind an Application Load Balancer that handles traffic from various web domains such as ilove-manila.com, i-love-boracay.com, i-love-cebu.com and many others. To improve security and lessen the overall cost, you are instructed to secure the system by allowing multiple domains to serve SSL traffic without the need to reauthenticate and reprovision your certificate everytime you add a new domain. This migration from HTTP to HTTPS will help improve their SEO and Google search ranking. Which of the following is the most cost-effective solution to meet the above requirement?

- A. Upload all SSL certificates of the domains in the ALB using the console and bind multiple certificates to the same secure listener on your load balancer. ALB will automatically choose the optimal TLS certificate for each client using Server Name Indication (SNI).
- B. Create a new CloudFront web distribution and configure it to serve HTTPS requests using dedicated IP addresses in order to associate your alternate domain names with a dedicated IP address in each CloudFront edge location.
- C. Add a Subject Alternative Name (SAN) for each additional domain to your certificate.
- D. Use a wildcard certificate to handle multiple sub-domains and different domains.

Answer: A

Explanation:

SNI Custom SSL relies on the SNI extension of the Transport Layer Security protocol, which allows multiple domains to serve SSL traffic over the same IP address by including the hostname which the viewers are trying to connect to.

You can host multiple TLS secured applications, each with its own TLS certificate, behind a single load balancer. In order to use SNI, all you need to do is bind multiple certificates to the same secure listener on your load balancer. ALB will automatically choose the optimal TLS certificate for each client. These features are provided at no additional charge.

To meet the requirements in the scenario, you can upload all SSL certificates of the domains in the ALB using the console and bind multiple certificates to the same secure listener on your load balancer. ALB will automatically choose the optimal TLS certificate for each client using Server Name Indication (SNI). Hence, the correct answer is the option that says: Upload all SSL certificates of the domains in the ALB using the console and bind multiple certificates to the same secure listener on your load balancer. ALB will automatically choose the optimal TLS certificate for each client using Server Name Indication (SNI). Using a wildcard certificate to handle multiple sub-domains and different domains is incorrect because a wildcard certificate can only handle multiple sub-domains but not different domains.

Adding a Subject Alternative Name (SAN) for each additional domain to your certificate is incorrect because although using SAN is correct, you will still have to reauthenticate and reprovision your certificate every time you add a new domain. One of the requirements in the scenario is that you should not have to reauthenticate and reprovision your certificate hence, this solution is incorrect.

The option that says: Create a new CloudFront web distribution and configure it to serve HTTPS requests using dedicated IP addresses in order to associate your alternate domain names with a dedicated IP address in each CloudFront edge location is incorrect because although it is valid to use dedicated IP addresses to meet this requirement, this solution is not cost-effective. Remember that if you configure CloudFront to serve HTTPS requests using dedicated IP addresses, you incur an additional monthly charge. The charge begins when you associate your SSL/TLS certificate with your CloudFront distribution. You can just simply upload the certificates to the ALB and use SNI to handle multiple domains in a cost-effective manner.

#### References:

<https://aws.amazon.com/blogs/aws/new-application-load-balancer-sni/>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-https-dedicated-ip-or-sni.html#cnames-https-dedicated-ip>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html>

Check out this Amazon CloudFront Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudfront/>

SNI Custom SSL vs Dedicated IP Custom SSL:

<https://tutorialsdojo.com/sni-custom-ssl-vs-dedicated-ip-custom-ssl/>

Comparison of AWS Services Cheat Sheets:

<https://tutorialsdojo.com/comparison-of-aws-services/>

## QUESTION 183

A company is setting up a cloud architecture for an international money transfer service to be deployed in AWS which will have thousands of users around the globe. The service should be available 24 to avoid any business disruption and should be resilient enough to handle the outage of an entire AWS region. To meet this requirement, the Solutions Architect has deployed their AWS resources to multiple AWS Regions. He needs to use Route 53 and configure it to set all of the resources to be available all the time as much as possible. When a resource becomes unavailable, Route 53 should detect that it's unhealthy and stop including it when responding to queries.

Which of the following is the most fault-tolerant routing configuration that the Solutions Architect should use in this scenario?

- A. Configure an Active-Active Failover with One Primary and One Secondary Resource.
- B. Configure an Active-Active Failover with Weighted routing policy.
- C. Configure an Active-Passive Failover with Weighted Records.
- D. Configure an Active-Passive Failover with Multiple Primary and Secondary Resources.

Answer: B

Explanation:

You can use Route 53 health checking to configure active-active and active-passive failover configurations. You configure active-active failover using any routing policy (or combination of routing policies) other than failover, and you configure active-passive failover using the failover routing policy.

The screenshot shows the 'Quick create record' interface for Route 53. A new record is being created with the following details:

- Record name:** portal.tutorialsdojo.com
- Routing policy:** Weighted
- Value:** 192.0.2.255
- TTL (seconds):** 300
- Weight:** 200
- Health check - optional:** Choose health check
- Record ID:** US West load balancer

### Active-Active Failover

Use this failover configuration when you want all of your resources to be available the majority of the time. When a resource becomes unavailable, Route 53 can detect that it's unhealthy and stop including it when responding to queries.

In active-active failover, all the records that have the same name, the same type (such as A or AAAA), and the same routing policy (such as weighted or latency) are active unless Route 53 considers them unhealthy. Route 53 can respond to a DNS query using any healthy record.

### Active-Passive Failover

Use an active-passive failover configuration when you want a primary resource or group of resources to be available the majority of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable. When responding to queries, Route 53 includes only the healthy primary resources. If all the primary resources are unhealthy, Route 53 begins to include only the healthy secondary resources in response to DNS queries.

Configuring an Active-Passive Failover with Weighted Records and configuring an Active-Passive Failover with Multiple Primary and Secondary Resources are incorrect because an Active-Passive Failover is mainly used when you want a primary resource or group of resources to be available most of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable. In this scenario, all of your resources should be available all the time as much as possible which is why you have to use an Active-Active Failover instead.

Configuring an Active-Active Failover with One Primary and One Secondary Resource is incorrect because you cannot set up an Active-Active Failover with One Primary and One Secondary Resource. Remember that an Active-Active Failover uses all available resources all the time without a primary nor a secondary resource.

References:

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

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

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

Amazon Route 53 Overview:

<https://www.youtube.com/watch?v=Su308t19ubY>

Check out this Amazon Route 53 Cheat Sheet:

<https://tutorialsdojo.com/amazon-route-53/>

---

## QUESTION 184

A company deployed a high-performance computing (HPC) cluster that spans multiple EC2 instances across multiple Availability Zones and processes various wind simulation models. Currently, the Solutions Architect is experiencing a slowdown in their applications and upon further investigation, it was discovered that it was due to latency issues.

Which is the MOST suitable solution that the Solutions Architect should implement to provide low-latency network performance necessary for tightly-coupled node-to-node communication of the HPC cluster?

- A. Set up a cluster placement group within a single Availability Zone in the same AWS Region.
- B. Set up a spread placement group across multiple Availability Zones in multiple AWS Regions.
- C. Set up AWS Direct Connect connections across multiple Availability Zones for increased bandwidth throughput and more consistent network experience.
- D. Use EC2 Dedicated Instances.

Answer: A

Explanation:

When you launch a new EC2 instance, the EC2 service attempts to place the instance in such a way that all of your instances are spread out across underlying hardware to minimize correlated failures. You can use placement groups to influence the placement of a group of interdependent instances to meet the needs of your workload. Depending on the type of workload, you can create a placement group using one of the following placement strategies:

Cluster ““ packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.

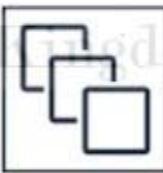
Partition ““ spreads your instances across logical partitions such that groups of instances in one partition do not share the underlying hardware with groups of instances in different partitions. This strategy is typically used by large distributed and replicated workloads, such as Hadoop, Cassandra, and Kafka.

Spread ““ strictly places a small group of instances across distinct underlying hardware to reduce correlated failures.

Cluster placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. They are also recommended when the majority of the network traffic is between the instances in the group. To provide the lowest latency and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking.



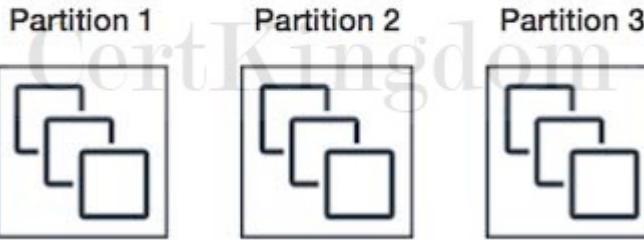
## Availability Zone



Partition placement groups can be used to deploy large distributed and replicated workloads, such as HDFS, HBase, and Cassandra, across distinct racks. When you launch instances into a partition placement group, Amazon EC2 tries to distribute the instances evenly across the number of partitions that you specify. You can also launch instances into a specific partition to have more control over where the instances are placed.



## Availability Zone 1



Spread placement groups are recommended for applications that have a small number of critical instances that should be kept separate from each other. Launching instances in a spread placement group reduces the risk of simultaneous failures that might occur when instances share the same racks. Spread placement groups provide access to distinct racks, and are therefore suitable for mixing instance types or launching instances over time. A spread placement group can span multiple Availability Zones in the same Region. You can have a maximum of seven running instances per Availability Zone per group.



## Availability Zone 1



Hence, the correct answer is: Set up a cluster placement group within a single Availability Zone in the same AWS Region.

The option that says: Set up a spread placement group across multiple Availability Zones in multiple AWS Regions is incorrect because although using a placement group is valid for this particular scenario, you can only set up a placement group in a single AWS Region only. A spread placement group can span multiple Availability Zones in the same Region.

The option that says: Set up AWS Direct Connect connections across multiple Availability Zones for increased bandwidth throughput and more consistent network experience is incorrect because this is primarily used for hybrid architectures. It bypasses the public Internet and establishes a secure, dedicated connection from your on-premises data center into AWS, and not used for having low latency within your AWS network.

The option that says: Use EC2 Dedicated Instances is incorrect because these are EC2 instances that run in a VPC on hardware that is dedicated to a single customer and are physically isolated at the host hardware level from instances that belong to other AWS accounts. It is not used for reducing latency.

References:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

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

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

---

## QUESTION 185

A company is using Amazon VPC that has a CIDR block of 10.31.0.0< that is connected to the onpremises data center. There was a requirement to create a Lambda function that will process massive amounts of cryptocurrency transactions every minute and then store the results to EFS. After setting up the serverless architecture and connecting the Lambda function to the VPC, the Solutions Architect noticed an increase in invocation errors with EC2 error types such as EC2ThrottledException at certain times of the day.

Which of the following are the possible causes of this issue? (Select TWO.)

- A. The attached IAM execution role of your function does not have the necessary permissions to access the resources of your VPC.
- B. Your VPC does not have sufficient subnet ENIs or subnet IPs.
- C. The associated security group of your function does not allow outbound connections.
- D. Your VPC does not have a NAT gateway.
- E. You only specified one subnet in your Lambda function configuration. That single subnet runs out of available IP addresses and there is no other subnet or Availability Zone which can handle the peak load.

Answer: B,E

Explanation:

You can configure a function to connect to a virtual private cloud (VPC) in your account. Use Amazon Virtual Private Cloud (Amazon VPC) to create a private network for resources such as databases, cache instances, or internal services. Connect your function to the VPC to access private resources during execution.

AWS Lambda runs your function code securely within a VPC by default. However, to enable your Lambda function to access resources inside your private VPC, you must provide additional VPC-specific configuration information that includes VPC subnet IDs and security group IDs. AWS Lambda uses this information to set up elastic network interfaces (ENIs) that enable your function to connect securely to other resources within your private VPC.

Lambda functions cannot connect directly to a VPC with dedicated instance tenancy. To connect to resources in a dedicated VPC, peer it to a second VPC with default tenancy.

Your Lambda function automatically scales based on the number of events it processes. If your Lambda function accesses a VPC, you must make sure that your VPC has sufficient ENI capacity to support the scale requirements of your Lambda function. It is also recommended that you specify at least one subnet in each Availability Zone in your Lambda function configuration.

By specifying subnets in each of the Availability Zones, your Lambda function can run in another Availability Zone if one goes down or runs out of IP addresses. If your VPC does not have sufficient ENIs or subnet IPs, your Lambda function will not scale as requests increase, and you will see an increase in invocation errors with EC2 error types like EC2ThrottledException. For asynchronous invocation, if you see an increase in errors without corresponding CloudWatch Logs, invoke the Lambda function synchronously in the console to get the error responses.

Hence, the correct answers for this scenario are:

- You only specified one subnet in your Lambda function configuration. That single subnet runs out of available IP addresses and there is no other subnet or Availability Zone which can handle the peak load.
- Your VPC does not have sufficient subnet ENIs or subnet IPs.

The screenshot shows the AWS Lambda Function Configuration interface with three main sections:

- Execution role**: A dropdown menu titled "Use an existing role" is open, showing the selected role "service-role/tutorialsdojo-lambda-vpc-role-xd5u9vhy". A "View" link is provided to see the role in the IAM console.
- Network**: A dropdown menu titled "No VPC" is open, indicating no VPC is assigned to the function.
- Concurrency**: Shows an unreserved account concurrency limit of 1000. The "Use unreserved account concurrency" option is selected, while "Reserve concurrency" is unselected.

The option that says: Your VPC does not have a NAT gateway is incorrect because an issue in the NAT Gateway is unlikely to cause a request throttling issue or produce an EC2ThrottledException error in Lambda. As per the scenario, the issue is happening only at certain times of the day, which means that the issue is only intermittent and the function works at other times. We can also conclude that an availability issue is not an issue since the application is already using a highly available NAT Gateway and not just a NAT instance.

The option that says: The associated security group of your function does not allow outbound connections is incorrect because if the associated security group does not allow outbound connections then the Lambda function will not work at all in the first place. Remember that as per the scenario, the issue only happens intermittently. In addition, Internet traffic restrictions do not usually produce EC2ThrottledException errors.

The option that says: The attached IAM execution role of your function does not have the necessary permissions to access the resources of your VPC is incorrect because just as what is explained above,

the issue is intermittent and thus, the IAM execution role of the function does have the necessary permissions to access the resources of the VPC since it works at those specific times. In case the issue is indeed caused by a permission problem then an EC2AccessDeniedException the error would most likely be returned and not an EC2ThrottledException error.

References:

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

<https://aws.amazon.com/premiumsupport/knowledge-center/internet-access-lambda-function/>

<https://aws.amazon.com/premiumsupport/knowledge-center/lambda-troubleshoot-invoke-error-502-500/>

Check out this AWS Lambda Cheat Sheet:

<https://tutorialsdojo.com/aws-lambda/>

---

## QUESTION 186

A company has established a dedicated network connection from its on-premises data center to AWS Cloud using AWS Direct Connect (DX). The core network services, such as the Domain Name System (DNS) service and Active Directory services, are all hosted on-premises. The company has new AWS accounts that will also require consistent and dedicated access to these network services.

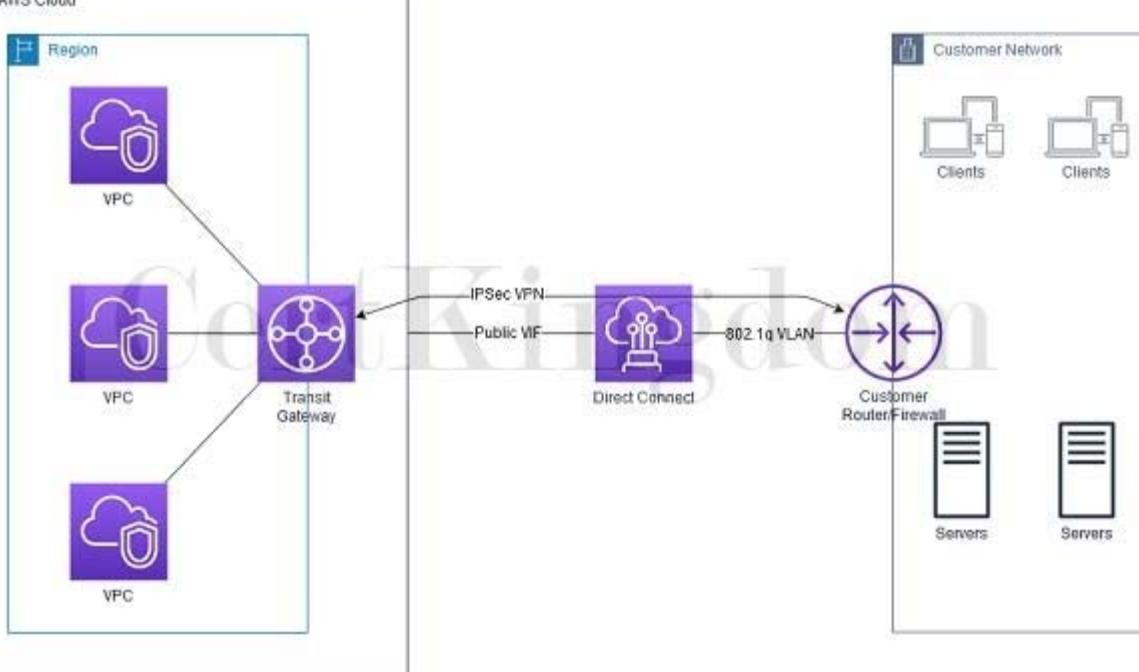
Which of the following can satisfy this requirement with the LEAST amount of operational overhead and in a cost-effective manner?

- A. Set up another Direct Connect connection for each and every new AWS account that will be added.
- B. Create a new Direct Connect gateway and integrate it with the existing Direct Connect connection.  
Set up a Transit Gateway between AWS accounts and associate it with the Direct Connect gateway.
- C. Create a new AWS VPN CloudHub. Set up a Virtual Private Network (VPN) connection for additional AWS accounts.
- D. Set up a new Direct Connect gateway and integrate it with the existing Direct Connect connection.  
Configure a VPC peering connection between AWS accounts and associate it with Direct Connect gateway.

Answer: B

Explanation:

AWS Transit Gateway provides a hub and spoke design for connecting VPCs and on-premises networks. You can attach all your hybrid connectivity (VPN and Direct Connect connections) to a single Transit Gateway consolidating and controlling your organization's entire AWS routing configuration in one place. It also controls how traffic is routed among all the connected spoke networks using route tables. This hub and spoke model simplifies management and reduces operational costs because VPCs only connect to the Transit Gateway to gain access to the connected networks.



By attaching a transit gateway to a Direct Connect gateway using a transit virtual interface, you can manage a single connection for multiple VPCs or VPNs that are in the same AWS Region. You can also advertise prefixes from on-premises to AWS and from AWS to on-premises.

The AWS Transit Gateway and AWS Direct Connect solution simplify the management of connections between an Amazon VPC and your networks over a private connection. It can also minimize network costs, improve bandwidth throughput, and provide a more reliable network experience than Internetbased connections.

Hence, the correct answer is: Create a new Direct Connect gateway and integrate it with the existing Direct Connect connection. Set up a Transit Gateway between AWS accounts and associate it with the Direct Connect gateway.

The option that says: Set up another Direct Connect connection for each and every new AWS account that will be added is incorrect because this solution entails a significant amount of additional cost. Setting up a single DX connection requires a substantial budget and takes a lot of time to establish. It also has high management overhead since you will need to manage all of the Direct Connect connections for all AWS accounts.

The option that says: Create a new AWS VPN CloudHub. Set up a Virtual Private Network (VPN) connection for additional AWS accounts is incorrect because a VPN connection is not capable of providing consistent and dedicated access to the on-premises network services. Take note that a VPN connection traverses the public Internet and doesn't use a dedicated connection.

The option that says: Set up a new Direct Connect gateway and integrate it with the existing Direct Connect connection. Configure a VPC peering connection between AWS accounts and associate it with Direct Connect gateway is incorrect because VPC peering is not supported in a Direct Connect connection. VPC peering does not support transitive peering relationships.

#### References:

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

<https://aws.amazon.com/blogs/networking-and-content-delivery/integrating-sub-1-gbps-hosted-connections-with-aws-transit-gateway/>

Check out this AWS Transit Gateway Cheat Sheet:

<https://tutorialsdojo.com/aws-transit-gateway/>

## QUESTION 187

Due to the large volume of query requests, the database performance of an online reporting application significantly slowed down. The Solutions Architect is trying to convince her client to use Amazon RDS Read Replica for their application instead of setting up a Multi-AZ Deployments configuration.

What are two benefits of using Read Replicas over Multi-AZ that the Architect should point out? (Select TWO.)

- A. Provides synchronous replication and automatic failover in the case of Availability Zone service failures.
- B. It elastically scales out beyond the capacity constraints of a single DB instance for read-heavy database workloads.
- C. Allows both read and write operations on the read replica to complement the primary database.
- D. Provides asynchronous replication and improves the performance of the primary database by taking read-heavy database workloads from it.
- E. It enhances the read performance of your primary database by increasing its IOPS and accelerates its query processing via AWS Global Accelerator.

Answer: B,D

Explanation:

Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This feature makes it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.

You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances.

For the MySQL, MariaDB, PostgreSQL, and Oracle database engines, Amazon RDS creates a second DB instance using a snapshot of the source DB instance. It then uses the engines' native asynchronous replication to update the read replica whenever there is a change to the source DB instance. The read replica operates as a DB instance that allows only read-only connections; applications can connect to a read replica just as they would to any DB instance. Amazon RDS replicates all databases in the source DB instance.

Multi-AZ deployments	Multi-Region deployments	Read replicas
Main purpose is high availability	Main purpose is disaster recovery and local performance	Main purpose is scalability
Non-Aurora: synchronous replication; Aurora: asynchronous replication	Asynchronous replication	Asynchronous replication
Non-Aurora: only the primary instance is active; Aurora: all instances are active	All regions are accessible and can be used for reads	All read replicas are accessible and can be used for rescaling
Non-Aurora: automated backups are taken from standby; Aurora: automated backups are taken from shared storage layer	Automated backups can be taken in each region	No backups configured by default
Always span at least two Availability Zones within a single region	Each region can have a Multi-AZ deployment	Can be within an Availability Zone, Cross-AZ, or Cross-Region
Non-Aurora: database engine version upgrades happen on primary; Aurora: all instances are updated together	Non-Aurora: database engine version upgrade is independent in each region; Aurora: all instances are updated together	Non-Aurora: database engine version upgrade is independent from source instance; Aurora: all instances are updated together
Automatic failover to standby (non-Aurora) or read replica (Aurora) when a problem is detected	Aurora allows promotion of a secondary region to be the master	Can be manually promoted to a standalone database instance (non-Aurora) or to be the primary instance (Aurora)

When you create a read replica for Amazon RDS for MySQL, MariaDB, PostgreSQL, and Oracle, Amazon RDS sets up a secure communications channel using public-key encryption between the source DB instance and the read replica, even when replicating across regions. Amazon RDS establishes any AWS security configurations such as adding security group entries needed to enable the secure channel. You can also create read replicas within a Region or between Regions for your Amazon RDS for MySQL, MariaDB, PostgreSQL, and Oracle database instances encrypted at rest with AWS Key

Management Service (KMS).

Hence, the correct answers are:

- It elastically scales out beyond the capacity constraints of a single DB instance for read-heavy database workloads.
- Provides asynchronous replication and improves the performance of the primary database by taking read-heavy database workloads from it.

The option that says: Allows both read and write operations on the read replica to complement the primary database is incorrect as Read Replicas are primarily used to offload read-only operations from the primary database instance. By default, you can't do a write operation to your Read Replica.

The option that says: Provides synchronous replication and automatic failover in the case of Availability Zone service failures is incorrect as this is a benefit of Multi-AZ and not of a Read Replica. Moreover, Read Replicas provide an asynchronous type of replication and not synchronous replication.

The option that says: It enhances the read performance of your primary database by increasing its IOPS and accelerates its query processing via AWS Global Accelerator is incorrect because Read Replicas do not do anything to upgrade or increase the read throughput on the primary DB instance per se, but it provides a way for your application to fetch data from replicas. In this way, it improves the overall performance of your entire database-tier (and not just the primary DB instance). It doesn't increase the IOPS nor use AWS Global Accelerator to accelerate the compute capacity of your primary database.

AWS Global Accelerator is a networking service, not related to RDS, that direct user traffic to the nearest application endpoint to the client, thus reducing internet latency and jitter. It simply routes the traffic to the closest edge location via Anycast.

References:

<https://aws.amazon.com/rds/details/read-replicas/>

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

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

Additional tutorial - How do I make my RDS MySQL read replica writable?

---

## QUESTION 188

A solutions architect is managing an application that runs on a Windows EC2 instance with an attached Amazon FSx for Windows File Server. To save cost, management has decided to stop the instance during off-hours and restart it only when needed. It has been observed that the application takes several minutes to become fully operational which impacts productivity.

How can the solutions architect speed up the instance's loading time without driving the cost up?

- A. Migrate the application to a Linux-based EC2 instance.
- B. Disable the Instance Metadata Service to reduce the things that need to be loaded at startup.
- C. Enable the hibernation mode on the EC2 instance.
- D. Migrate the application to an EC2 instance with hibernation enabled.

Answer: D

Explanation:

Hibernation provides the convenience of pausing and resuming the instances, saves time by reducing the startup time taken by applications, and saves effort in setting up the environment or applications all over again. Instead of having to rebuild the memory footprint, hibernation allows applications to pick up exactly where they left off.

**Stop - Hibernate behavior Info**

Enable

To enable hibernation, space is allocated on the root volume to store the instance memory (RAM). Make sure that the root volume is large enough to store the RAM contents and accommodate your expected usage, e.g. OS, applications. To use hibernation, the root volume must be an encrypted EBS volume. [Learn more](#)

**Termination protection Info**

Select

**Summary**

Number of instances [Info](#)  
1

Software Image (AMI)  
Amazon Linux 2 Kernel 5.10 AMI... [read more](#)  
ami-0bd6906508e74f692

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
New security group

Storage (volumes)  
1 volume(s) - 8 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier

Cancel **Launch Instance**

While the instance is in hibernation, you pay only for the EBS volumes and Elastic IP Addresses attached to it; there are no other hourly charges (just like any other stopped instance). Therefore, the correct answer is: Migrate the application to an EC2 instance with hibernation enabled. The option that says: Migrate the application to a Linux-based EC2 instance is incorrect. This does not guarantee a faster load time. Moreover, it is a risky thing to do as the application might have dependencies tied to the previous operating system that won't work on a different OS. The option that says: Enable the hibernation mode on the EC2 instance is incorrect. It is not possible to enable or disable hibernation for an instance after it has been launched. The option that says: Disable the instance metadata service to reduce the things that need to be loaded at startup is incorrect. This won't affect the startup load time at all. The Instance Metadata Service is just a service that you can access over the network from within an EC2 instance.

References:

<https://aws.amazon.com/about-aws/whats-new/9/amazon-ec2-hibernation-now-available-on-windows/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enabling-hibernation.html>

<https://aws.amazon.com/blogs/aws/new-hibernate-your-ec2-instances/>

Check out this Amazon EC2 Cheat sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

## QUESTION 189

A new online banking platform has been re-designed to have a microservices architecture in which complex applications are decomposed into smaller, independent services. The new platform is using Docker considering that application containers are optimal for running small, decoupled services. The new solution should remove the need to provision and manage servers, let you specify and pay for resources per application, and improve security through application isolation by design.

Which of the following is the MOST suitable service to use to migrate this new platform to AWS?

- A. Amazon EFS
- B. Amazon EBS
- C. Amazon EKS
- D. AWS Fargate

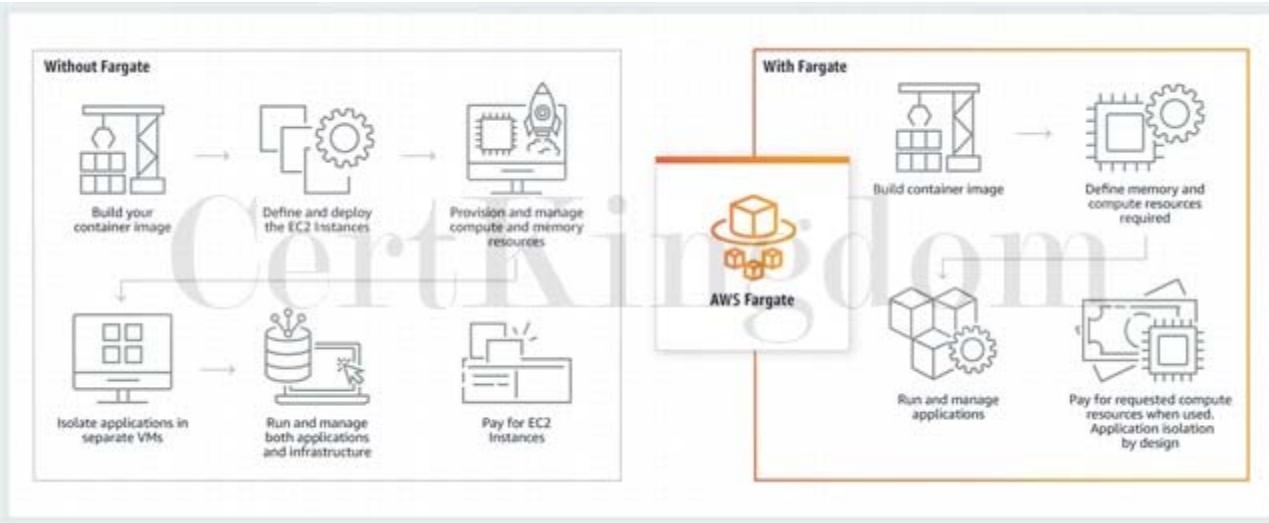
Answer: D

Explanation:

AWS Fargate is a serverless compute engine for containers that works with both Amazon Elastic

Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy for you to focus on building your applications. Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design.

Fargate allocates the right amount of compute, eliminating the need to choose instances and scale cluster capacity. You only pay for the resources required to run your containers, so there is no overprovisioning and paying for additional servers. Fargate runs each task or pod in its own kernel providing the tasks and pods their own isolated compute environment. This enables your application to have workload isolation and improved security by design. This is why customers such as Vanguard, Accenture, Foursquare, and Ancestry have chosen to run their mission critical applications on Fargate.



Hence, the correct answer is: AWS Fargate.

Amazon EKS is incorrect because this is more suitable to run the Kubernetes management infrastructure and not Docker. It does not remove the need to provision and manage servers nor let you specify and pay for resources per application, unlike AWS Fargate.

Amazon EFS is incorrect because this is a file system for Linux-based workloads for use with AWS Cloud services and on-premises resources.

Amazon EBS is incorrect because this is primarily used to provide persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud.

References:

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

[https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ECS\\_GetStarted\\_Fargate.html](https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ECS_GetStarted_Fargate.html)

Check out this Amazon ECS Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-container-service-amazon-ecs/>

## QUESTION 190

A Solutions Architect is managing a company's AWS account of approximately 300 IAM users. They have a new company policy that requires changing the associated permissions of all 100 IAM users that control the access to Amazon S3 buckets.

What will the Solutions Architect do to avoid the time-consuming task of applying the policy to each user?

- A. Create a new IAM group and then add the users that require access to the S3 bucket. Afterward, apply the policy to the IAM group.
- B. Create a new policy and apply it to multiple IAM users using a shell script.
- C. Create a new S3 bucket access policy with unlimited access for each IAM user.
- D. Create a new IAM role and add each user to the IAM role.

Answer: A

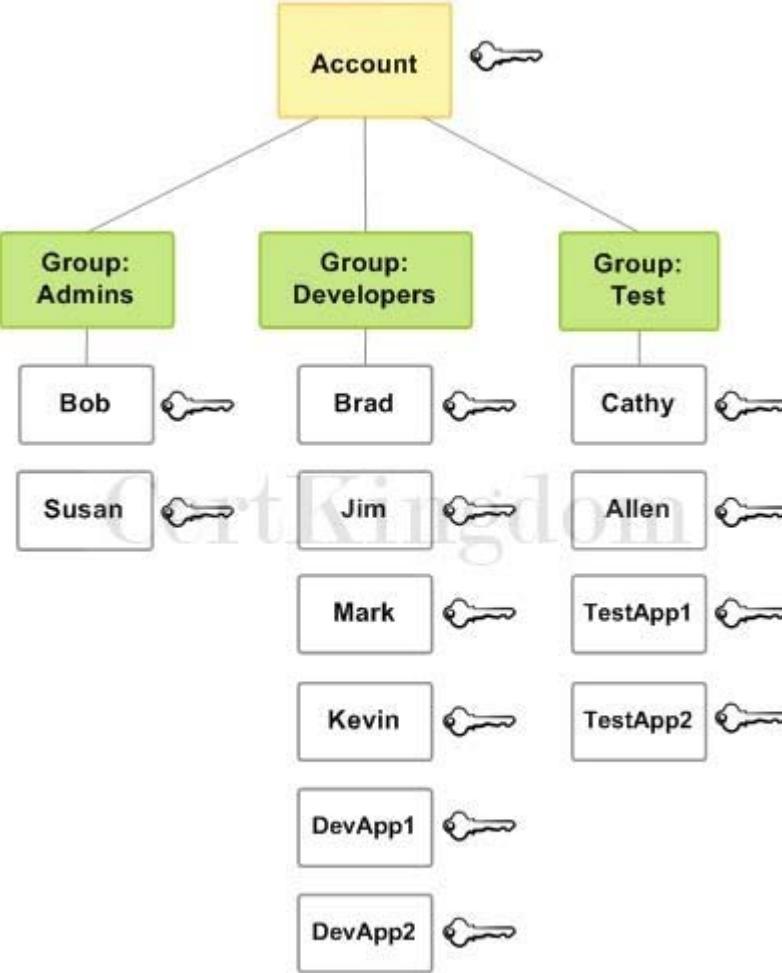
Explanation:

In this scenario, the best option is to group the set of users in an IAM Group and then apply a policy with the required access to the Amazon S3 bucket. This will enable you to easily add, remove, and manage the users instead of manually adding a policy to each and every 100 IAM users.

Creating a new policy and applying it to multiple IAM users using a shell script is incorrect because you need a new IAM Group for this scenario and not assign a policy to each user via a shell script. This method can save you time but afterward, it will be difficult to manage all 100 users that are not contained in an IAM Group.

Creating a new S3 bucket access policy with unlimited access for each IAM user is incorrect because you need a new IAM Group and the method is also time-consuming.

Creating a new IAM role and adding each user to the IAM role is incorrect because you need to use an IAM Group and not an IAM role.



#### Reference:

[http://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_groups.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html)

#### AWS Identity Services Overview:

<https://www.youtube.com/watch?v=AIdUw0i8rr0>

#### Check out this AWS IAM Cheat Sheet:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

#### Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

---

### QUESTION 191

A company deployed several EC2 instances in a private subnet. The Solutions Architect needs to ensure the security of all EC2 instances. Upon checking the existing Inbound Rules of the Network ACL, she saw this configuration:

[Summary](#)[Inbound Rules](#)[Outbound Rules](#)[Subnet Associations](#)[Tags](#)

Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

[Edit](#)

View: All rules

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
101	Custom TCP Rule	TCP (6)	4000	110.238.109.37/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

tutorialsdojo.com

If a computer with an IP address of 110.238.109.37 sends a request to the VPC, what will happen?

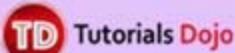
- A. It will be allowed.
- B. Initially, it will be allowed and then after a while, the connection will be denied.
- C. Initially, it will be denied and then after a while, the connection will be allowed.
- D. It will be denied.

Answer: A

Explanation:

Rules are evaluated starting with the lowest numbered rule. As soon as a rule matches traffic, it's applied immediately regardless of any higher-numbered rule that may contradict it.

Security Group	Network Access Control List
Acts as a firewall for associated Amazon EC2 instances	Acts as a firewall for associated subnets
Controls both inbound and outbound traffic at the instance level	Controls both inbound and outbound traffic at the subnet level
You can secure your VPC instances using only security groups	Network ACLs are an additional layer of defense.
Supports allow rules only	Supports allow rules and deny rules
Stateful (Return traffic is automatically allowed, regardless of any rules)	Stateless (Return traffic must be explicitly allowed by rules)
Evaluates all rules before deciding whether to allow traffic	Evaluates rules in number order when deciding whether to allow traffic, starting with the lowest numbered rule.
Applies only to the instance that is associated to it	Applies to all instances in the subnet it is associated with
Has separate rules for inbound and outbound traffic	Has separate rules for inbound and outbound traffic
A newly created security group denies all inbound traffic by default	A newly created nACL denies all inbound traffic by default
A newly created security group has an outbound rule that allows all outbound traffic by default	A newly created nACL denies all outbound traffic by default
Instances associated with a security group can't talk to each other unless you add rules allowing it	Each subnet in your VPC must be associated with a network ACL. If none is associated, the default nACL is selected.
Security groups are associated with network interfaces	You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time.



We have 3 rules here:

1. Rule 100 permits all traffic from any source.
2. Rule 101 denies all traffic coming from 110.238.109.37
3. The Default Rule (\*) denies all traffic from any source.

The Rule 100 will first be evaluated. If there is a match then it will allow the request. Otherwise, it will then go to Rule 101 to repeat the same process until it goes to the default rule. In this case, when there is a request from 110.238.109.37, it will go through Rule 100 first. As Rule 100 says it will permit all traffic from any source, it will allow this request and will not further evaluate Rule 101 (which denies 110.238.109.37) nor the default rule.

Reference:

[http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_ACLs.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html)

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

## QUESTION 192

A large financial firm in the country has an AWS environment that contains several Reserved EC2 instances hosting a web application that has been decommissioned last week. To save costs, you need

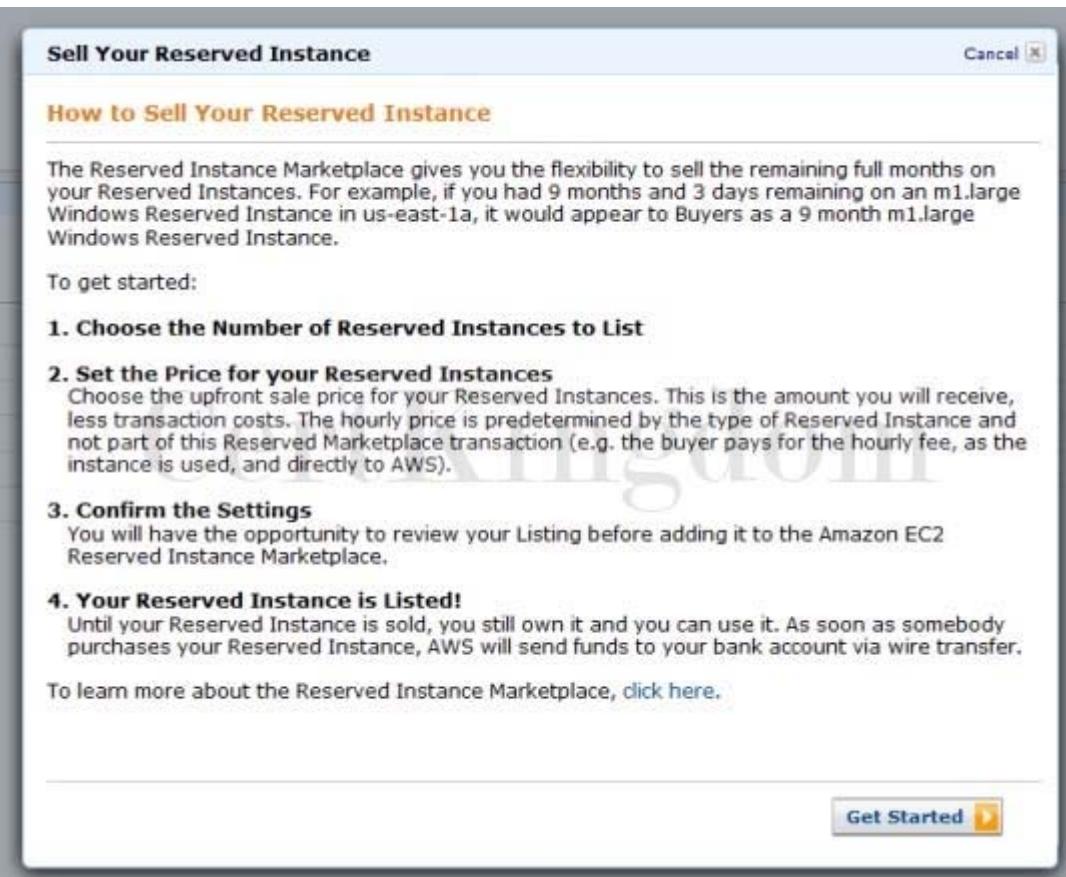
to stop incurring charges for the Reserved instances as soon as possible.  
What cost-effective steps will you take in this circumstance? (Select TWO.)

- A. Go to the AWS Reserved Instance Marketplace and sell the Reserved instances.
- B. Terminate the Reserved instances as soon as possible to avoid getting billed at the on-demand price when it expires.
- C. Go to the Amazon.com online shopping website and sell the Reserved instances.
- D. Contact AWS to cancel your AWS subscription.
- E. Stop the Reserved instances as soon as possible.

Answer: A,B

Explanation:

The Reserved Instance Marketplace is a platform that supports the sale of third-party and AWS customers' unused Standard Reserved Instances, which vary in terms of lengths and pricing options. For example, you may want to sell Reserved Instances after moving instances to a new AWS region, changing to a new instance type, ending projects before the term expiration, when your business needs change, or if you have unneeded capacity.



Hence, the correct answers are:

- Go to the AWS Reserved Instance Marketplace and sell the Reserved instances.
- Terminate the Reserved instances as soon as possible to avoid getting billed at the on-demand price when it expires.

Stopping the Reserved instances as soon as possible is incorrect because a stopped instance can still be restarted. Take note that when a Reserved Instance expires, any instances that were covered by the Reserved Instance are billed at the on-demand price which costs significantly higher. Since the application is already decommissioned, there is no point of keeping the unused instances. It is also possible that there are associated Elastic IP addresses, which will incur charges if they are associated with stopped instances.

Contacting AWS to cancel your AWS subscription is incorrect as you don't need to close down your AWS account.

Going to the Amazon.com online shopping website and selling the Reserved instances is incorrect as

you have to use AWS Reserved Instance Marketplace to sell your instances.

References:

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

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

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

---

## QUESTION 193

A large telecommunications company needs to run analytics against all combined log files from the Application Load Balancer as part of the regulatory requirements.

Which AWS services can be used together to collect logs and then easily perform log analysis?

- A. Amazon S3 for storing ELB log files and Amazon EMR for analyzing the log files.
- B. Amazon DynamoDB for storing and EC2 for analyzing the logs.
- C. Amazon S3 for storing the ELB log files and an EC2 instance for analyzing the log files using a custom-built application.
- D. Amazon EC2 with EBS volumes for storing and analyzing the log files.

Answer: A

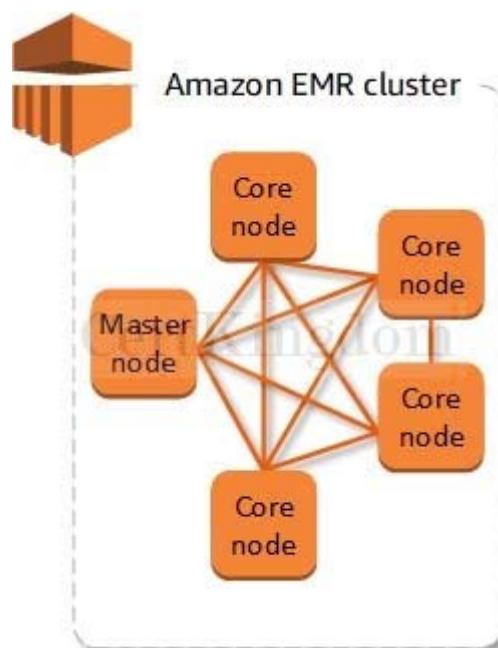
Explanation:

In this scenario, it is best to use a combination of Amazon S3 and Amazon EMR: Amazon S3 for storing ELB log files and Amazon EMR for analyzing the log files. Access logging in the ELB is stored in Amazon S3 which means that the following are valid options:

- Amazon S3 for storing the ELB log files and an EC2 instance for analyzing the log files using a custom-built application.
- Amazon S3 for storing ELB log files and Amazon EMR for analyzing the log files.

However, log analysis can be automatically provided by Amazon EMR, which is more economical than building a custom-built log analysis application and hosting it in EC2. Hence, the option that says: Amazon S3 for storing ELB log files and Amazon EMR for analyzing the log files is the best answer between the two.

Access logging is an optional feature of Elastic Load Balancing that is disabled by default. After you enable access logging for your load balancer, Elastic Load Balancing captures the logs and stores them in the Amazon S3 bucket that you specify as compressed files. You can disable access logging at any time.



Amazon EMR provides a managed Hadoop framework that makes it easy, fast, and cost-effective to

process vast amounts of data across dynamically scalable Amazon EC2 instances. It securely and reliably handles a broad set of big data use cases, including log analysis, web indexing, data transformations (ETL), machine learning, financial analysis, scientific simulation, and bioinformatics. You can also run other popular distributed frameworks such as Apache Spark, HBase, Presto, and Flink in Amazon EMR, and interact with data in other AWS data stores such as Amazon S3 and Amazon DynamoDB.

The option that says: Amazon DynamoDB for storing and EC2 for analyzing the logs is incorrect because DynamoDB is a noSQL database solution of AWS. It would be inefficient to store logs in DynamoDB while using EC2 to analyze them.

The option that says: Amazon EC2 with EBS volumes for storing and analyzing the log files is incorrect because using EC2 with EBS would be costly, and EBS might not provide the most durable storage for your logs, unlike S3.

The option that says: Amazon S3 for storing the ELB log files and an EC2 instance for analyzing the log files using a custom-built application is incorrect because using EC2 to analyze logs would be inefficient and expensive since you will have to program the analyzer yourself.

References:

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

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html>

Check out this Amazon EMR Cheat Sheet:

<https://tutorialsdojo.com/amazon-emr/>

Check out this AWS Elastic Load Balancing (ELB) Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

---

## QUESTION 194

A large electronics company is using Amazon Simple Storage Service to store important documents. For reporting purposes, they want to track and log every request access to their S3 buckets including the requester, bucket name, request time, request action, referrer, turnaround time, and error code information. The solution should also provide more visibility into the object-level operations of the bucket. Which is the best solution among the following options that can satisfy the requirement?

- A. Enable Amazon S3 Event Notifications for PUT and POST.
- B. Enable AWS CloudTrail to audit all Amazon S3 bucket access.
- C. Enable the Requester Pays option to track access via AWS Billing.
- D. Enable server access logging for all required Amazon S3 buckets.

Answer: D

Explanation:

Amazon S3 is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon S3. CloudTrail captures a subset of API calls for Amazon S3 as events, including calls from the Amazon S3 console and code calls to the Amazon S3 APIs.

AWS CloudTrail logs provide a record of actions taken by a user, role, or an AWS service in Amazon S3, while Amazon S3 server access logs provide detailed records for the requests that are made to an S3 bucket.

## Edit server access logging

**Server access logging**

Log requests for access to your bucket. [Learn more](#)

Server access logging

Disable

Enable

**⚠️** By enabling server access logging, S3 console will automatically update your bucket access control list (ACL) to include access to the S3 log delivery group.

Target bucket

s3://manila-s3-bucket/AWSLogs/

Format: s3://bucket/prefix

Browse S3

Cancel **Save changes**

For this scenario, you can use CloudTrail and the Server Access Logging feature of Amazon S3. However, it is mentioned in the scenario that they need detailed information about every access request sent to the S3 bucket including the referrer and turn-around time information. These two records are not available in CloudTrail.

Hence, the correct answer is: Enable server access logging for all required Amazon S3 buckets.

The option that says: Enable AWS CloudTrail to audit all Amazon S3 bucket access is incorrect because enabling AWS CloudTrail alone won't give detailed logging information for object-level access.

The option that says: Enabling the Requester Pays option to track access via AWS Billing is incorrect because this action refers to AWS billing and not for logging.

The option that says: Enabling Amazon S3 Event Notifications for PUT and POST is incorrect because we are looking for a logging solution and not an event notification.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/cloudtrail-logging.html#cloudtrail-logging-vs-server-logs>

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

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

### QUESTION 195

A data analytics company has been building its new generation big data and analytics platform on their AWS cloud infrastructure. They need a storage service that provides the scale and performance that their big data applications require such as high throughput to compute nodes coupled with read-afterwrite consistency and low-latency file operations. In addition, their data needs to be stored redundantly across multiple AZs and allows concurrent connections from multiple EC2 instances hosted on multiple AZs.

Which of the following AWS storage services will you use to meet this requirement?

- A. EFS
- B. Glacier
- C. S3

## D. EBS

Answer: A

Explanation:

In this question, you should take note of the two keywords/phrases: "file operation" and "allows concurrent connections from multiple EC2 instances". There are various AWS storage options that you can choose but whenever these criteria show up, always consider using EFS instead of using EBS Volumes which is mainly used as a "block" storage and can only have one connection to one EC2 instance at a time. Amazon EFS provides the scale and performance required for big data applications that require high throughput to compute nodes coupled with read-after-write consistency and low-latency file operations.

Amazon EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud. With a few clicks in the AWS Management Console, you can create file systems that are accessible to Amazon EC2 instances via a file system interface (using standard operating system file I/O APIs) and supports full file system access semantics (such as strong consistency and file locking).

Amazon EFS file systems can automatically scale from gigabytes to petabytes of data without needing to provision storage. Tens, hundreds, or even thousands of Amazon EC2 instances can access an Amazon EFS file system at the same time, and Amazon EFS provides consistent performance to each Amazon EC2 instance. Amazon EFS is designed to be highly durable and highly available.

EBS is incorrect because it does not allow concurrent connections from multiple EC2 instances hosted on multiple AZs and it does not store data redundantly across multiple AZs by default, unlike EFS.

S3 is incorrect because although it can handle concurrent connections from multiple EC2 instances, it does not have the ability to provide low-latency file operations, which is required in this scenario.

Glacier is incorrect because this is an archiving storage solution and is not applicable in this scenario.

References:

<https://docs.aws.amazon.com/efs/latest/ug/performance.html>

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

Check out this Amazon EFS Cheat Sheet:

<https://tutorialsdojo.com/amazon-efs/>

Check out this Amazon S3 vs EBS vs EFS Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3-vs-ebs-vs-efs/>

Here's a short video tutorial on Amazon EFS:

<https://youtu.be/AvgAozsfCrY>

---

## QUESTION 196

A company has a web application hosted in AWS cloud where the application logs are sent to Amazon CloudWatch. Lately, the web application has recently been encountering some errors which can be resolved simply by restarting the instance.

What will you do to automatically restart the EC2 instances whenever the same application error occurs?

A. First, look at the existing CloudWatch logs for keywords related to the application error to create a custom metric. Then, create a CloudWatch alarm for that custom metric which invokes an action to restart the EC2 instance.

B. First, look at the existing Flow logs for keywords related to the application error to create a custom metric. Then, create a CloudWatch alarm for that custom metric which invokes an action to restart the EC2 instance.

C. First, look at the existing Flow logs for keywords related to the application error to create a custom metric. Then, create a CloudWatch alarm for that custom metric which calls a Lambda function that invokes an action to restart the EC2 instance.

D. First, look at the existing CloudWatch logs for keywords related to the application error to create a custom metric. Then, create an alarm in Amazon SNS for that custom metric which invokes an action to restart the EC2 instance.

Answer: A

## Explanation:

In this scenario, you can look at the existing CloudWatch logs for keywords related to the application error to create a custom metric. Then, create a CloudWatch alarm for that custom metric which invokes an action to restart the EC2 instance.

### Notification

#### Alarm state trigger

Define the alarm state that will trigger this action.

[Remove](#)

In alarm

The metric or expression is outside of the defined threshold.

OK

The metric or expression is within the defined threshold.

Insufficient data

The alarm has just started or not enough data is available.

#### Select an SNS topic

Define the SNS (Simple Notification Service) topic that will receive the notification.

- Select an existing SNS topic
- Create new topic
- Use topic ARN

#### Create a new topic...

The topic name must be unique.

Default\_CloudWatch\_Alarms\_Topic

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (\_).

#### Email endpoints that will receive the notification...

Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

portal@tutorialsdojo.com

user1@example.com, user2@example.com

[Create topic](#)

[Add notification](#)

You can create alarms that automatically stop, terminate, reboot, or recover your EC2 instances using Amazon CloudWatch alarm actions. You can use the stop or terminate actions to help you save money when you no longer need an instance to be running. You can use the reboot and recover actions to automatically reboot those instances or recover them onto new hardware if a system impairment occurs. Hence, the correct answer is: First, look at the existing CloudWatch logs for keywords related to the application error to create a custom metric. Then, create a CloudWatch alarm for that custom metric which invokes an action to restart the EC2 instance.

The option that says: First, look at the existing CloudWatch logs for keywords related to the application error to create a custom metric. Then, create an alarm in Amazon SNS for that custom metric which invokes an action to restart the EC2 instance is incorrect because you can't create an alarm in Amazon SNS.

The following options are incorrect because Flow Logs are used in VPC and not on specific EC2 instance:

- First, look at the existing Flow logs for keywords related to the application error to create a custom metric. Then, create a CloudWatch alarm for that custom metric which invokes an action to restart the EC2 instance.

First, look at the existing Flow logs for keywords related to the application error to create a custom metric. Then, create a CloudWatch alarm for that custom metric which calls a Lambda function that

invokes an action to restart the EC2 instance.

Reference:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html>

Check out this Amazon CloudWatch Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudwatch/>

---

## QUESTION 197

A company is using an On-Demand EC2 instance to host a legacy web application that uses an Amazon Instance Store-Backed AMI. The web application should be decommissioned as soon as possible and hence, you need to terminate the EC2 instance.

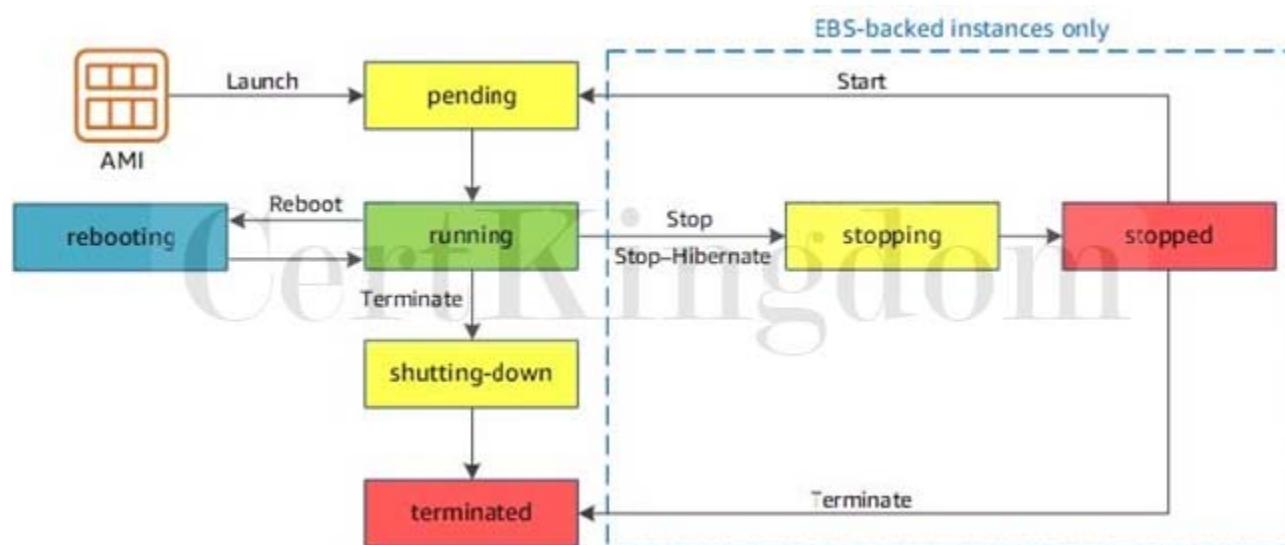
When the instance is terminated, what happens to the data on the root volume?

- A. Data is unavailable until the instance is restarted.
- B. Data is automatically saved as an EBS snapshot.
- C. Data is automatically saved as an EBS volume.
- D. Data is automatically deleted.

Answer: D

Explanation:

AMIs are categorized as either backed by Amazon EBS or backed by instance store. The former means that the root device for an instance launched from the AMI is an Amazon EBS volume created from an Amazon EBS snapshot. The latter means that the root device for an instance launched from the AMI is an instance store volume created from a template stored in Amazon S3.



The data on instance store volumes persist only during the life of the instance which means that if the instance is terminated, the data will be automatically deleted.

Hence, the correct answer is: Data is automatically deleted.

Reference:

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

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

---

## QUESTION 198

A company plans to deploy an application in an Amazon EC2 instance. The application will perform the following tasks:

- Read large datasets from an Amazon S3 bucket.
- Execute multi-stage analysis on the datasets.
- Save the results to Amazon RDS.

During multi-stage analysis, the application will store a large number of temporary files in the instance storage. As the Solutions Architect, you need to recommend the fastest storage option with high I/O performance for the temporary files.

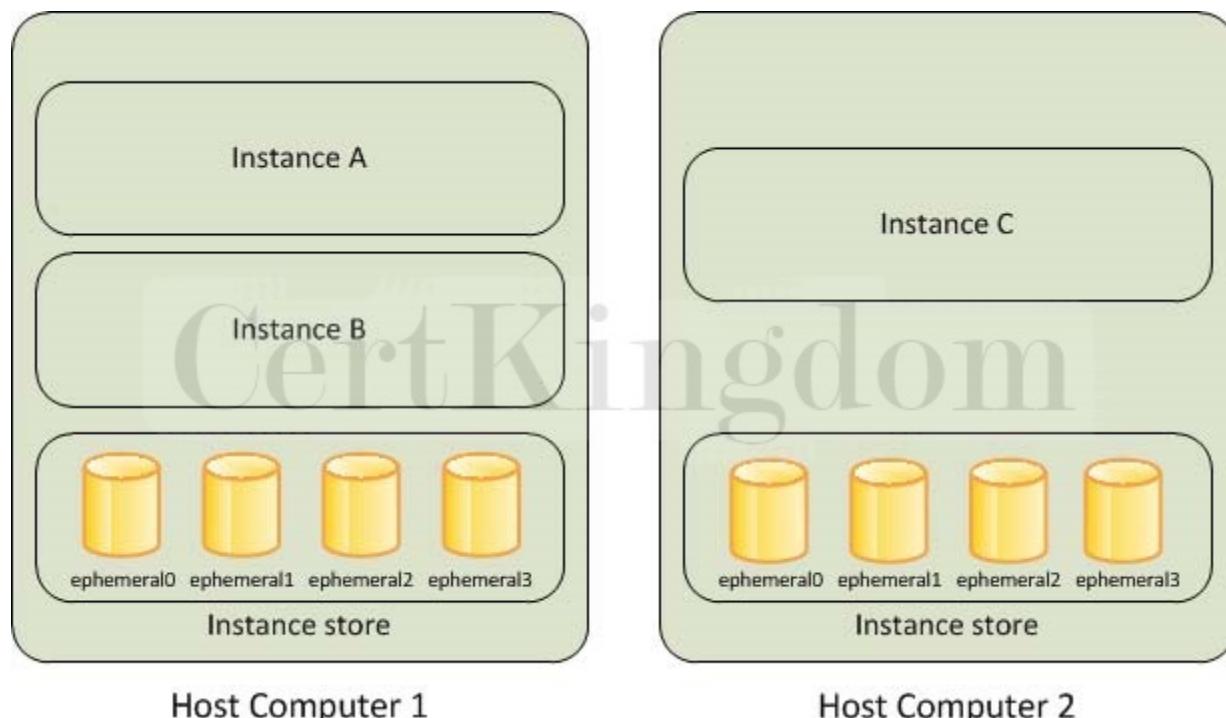
Which of the following options fulfills this requirement?

- A. Attach multiple Provisioned IOPS SSD volumes in the instance.
- B. Configure RAID 0 in multiple instance store volumes.
- C. Enable Transfer Acceleration in Amazon S3.
- D. Configure RAID 1 in multiple instance store volumes.

Answer: B

Explanation:

Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) Cloud. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.



RAID 0 configuration enables you to improve your storage volumes' performance by distributing the I/O across the volumes in a stripe. Therefore, if you add a storage volume, you get the straight addition of throughput and IOPS. This configuration can be implemented on both EBS or instance store volumes. Since the main requirement in the scenario is storage performance, you need to use an instance store volume. It uses NVMe or SATA-based SSD to deliver high random I/O performance. This type of storage is a good option when you need storage with very low latency, and you don't need the data to persist when the instance terminates.

Hence, the correct answer is: Configure RAID 0 in multiple instance store volumes.

The option that says: Enable Transfer Acceleration in Amazon S3 is incorrect because S3 Transfer Acceleration is mainly used to speed up the transfer of gigabytes or terabytes of data between clients and an S3 bucket.

The option that says: Configure RAID 1 in multiple instance volumes is incorrect because RAID 1 configuration is used for data mirroring. You need to configure RAID 0 to improve the performance of your storage volumes.

The option that says: Attach multiple Provisioned IOPS SSD volumes in the instance is incorrect because persistent storage is not needed in the scenario. Also, instance store volumes have greater I/O performance than EBS volumes.

## References:

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

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html>

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

---

### QUESTION 199

A company has stored 200 TB of backup files in Amazon S3. The files are in a vendor-proprietary format. The Solutions Architect needs to use the vendor's proprietary file conversion software to retrieve the files from their Amazon S3 bucket, transform the files to an industry-standard format, and re-upload the files back to Amazon S3. The solution must minimize the data transfer costs.

Which of the following options can satisfy the given requirement?

A. Deploy the EC2 instance in a different Region. Install the conversion software on the instance.

Perform data transformation and re-upload it to Amazon S3.

B. Install the file conversion software in Amazon S3. Use S3 Batch Operations to perform data transformation.

C. Deploy the EC2 instance in the same Region as Amazon S3. Install the file conversion software on the instance. Perform data transformation and re-upload it to Amazon S3.

D. Export the data using AWS Snowball Edge device. Install the file conversion software on the device. Transform the data and re-upload it to Amazon S3.

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.



You pay for all bandwidth into and out of Amazon S3, except for the following:

- Data transferred in from the Internet.
- Data transferred out to an Amazon EC2 instance, when the instance is in the same AWS Region as the S3 bucket (including to a different account in the same AWS region).
- Data transferred out to Amazon CloudFront.

To minimize the data transfer charges, you need to deploy the EC2 instance in the same Region as Amazon S3. Take note that there is no data transfer cost between S3 and EC2 in the same AWS

Region. Install the conversion software on the instance to perform data transformation and re-upload the data to Amazon S3.

Hence, the correct answer is: Deploy the EC2 instance in the same Region as Amazon S3. Install the file conversion software on the instance. Perform data transformation and re-upload it to Amazon S3.

The option that says: Install the file conversion software in Amazon S3. Use S3 Batch Operations to perform data transformation is incorrect because it is not possible to install the software in Amazon S3. The S3 Batch Operations just runs multiple S3 operations in a single request. It can't be integrated with your conversion software.

The option that says: Export the data using AWS Snowball Edge device. Install the file conversion software on the device. Transform the data and re-upload it to Amazon S3 is incorrect. Although this is possible, it is not mentioned in the scenario that the company has an on-premises data center. Thus, there's no need for Snowball.

The option that says: Deploy the EC2 instance in a different Region. Install the file conversion software on the instance. Perform data transformation and re-upload it to Amazon S3 is incorrect because this approach wouldn't minimize the data transfer costs. You should deploy the instance in the same Region as Amazon S3.

References:

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

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonS3.html>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

---

## QUESTION 200

A Solutions Architect is designing a setup for a database that will run on Amazon RDS for MySQL. He needs to ensure that the database can automatically failover to an RDS instance to continue operating in the event of failure. The architecture should also be as highly available as possible.

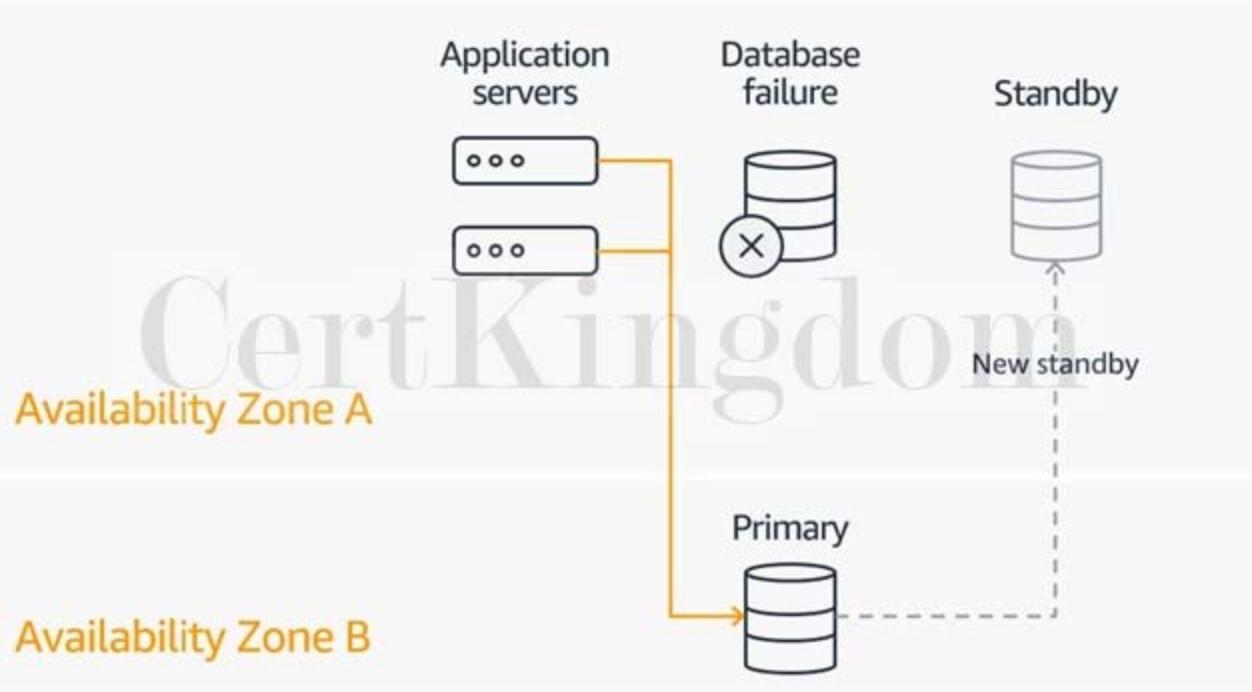
Which among the following actions should the Solutions Architect do?

- A. Create five cross-region read replicas in each region. In the event of an Availability Zone outage, promote any replica to become the primary instance.
- B. Create a read replica in the same region where the DB instance resides. In addition, create a read replica in a different region to survive a region's failure. In the event of an Availability Zone outage, promote any replica to become the primary instance.
- C. Create a standby replica in another availability zone by enabling Multi-AZ deployment.
- D. Create five read replicas across different availability zones. In the event of an Availability Zone outage, promote any replica to become the primary instance.

Answer: C

Explanation:

You can run an Amazon RDS DB instance in several AZs with Multi-AZ deployment. Amazon automatically provisions and maintains a secondary standby DB instance in a different AZ. Your primary DB instance is synchronously replicated across AZs to the secondary instance to provide data redundancy, failover support, eliminate I/O freezes, and minimize latency spikes during systems backup.



As described in the scenario, the architecture must meet two requirements:

The database should automatically failover to an RDS instance in case of failures.

The architecture should be as highly available as possible.

Hence, the correct answer is: Create a standby replica in another availability zone by enabling Multi-AZ deployment because it meets both of the requirements.

The option that says: Create a read replica in the same region where the DB instance resides. In addition, create a read replica in a different region to survive a region's failure. In the event of an Availability Zone outage, promote any replica to become the primary instance is incorrect. Although this architecture provides higher availability since it can survive a region failure, it still does not meet the first requirement since the process is not automated. The architecture should also support automatic failover to an RDS instance in case of failures.

Both the following options are incorrect:

- Create five read replicas across different availability zones. In the event of an Availability Zone outage, promote any replica to become the primary instance
- Create five cross-region read replicas in each region. In the event of an Availability Zone outage, promote any replica to become the primary instance

Although it is possible to achieve high availability with these architectures by promoting a read replica into the primary instance in an event of failure, it does not support automatic failover to an RDS instance which is also a requirement in the problem.

References:

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

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

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

## QUESTION 201

A company has a two-tier environment in its on-premises data center which is composed of an application tier and database tier. You are instructed to migrate their environment to the AWS cloud, and to design the subnets in their VPC with the following requirements:

1. There is an application load balancer that would distribute the incoming traffic among the servers in the application tier.
  2. The application tier and the database tier must not be accessible from the public Internet. The application tier should only accept traffic coming from the load balancer.
  3. The database tier contains very sensitive data. It must not share the same subnet with other AWS resources and its custom route table with other instances in the environment.
  4. The environment must be highly available and scalable to handle a surge of incoming traffic over the Internet.
- How many subnets should you create to meet the above requirements?

- A. 4
- B. 6
- C. 3
- D. 2

Answer: B

Explanation:

The given scenario indicated 4 requirements that should be met in order to successfully migrate their two-tier environment from their on-premises data center to AWS Cloud. The first requirement means that you have to use an application load balancer (ALB) to distribute the incoming traffic to your application servers.

The second requirement specifies that both your application and database tier should not be accessible from the public Internet. This means that you could create a single private subnet for both of your application and database tier. However, the third requirement mentioned that the database tier should not share the same subnet with other AWS resources to protect its sensitive data. This means that you should provision one private subnet for your application tier and another private subnet for your database tier.

The last requirement alludes to the need for using at least two Availability Zones to achieve high availability. This means that you have to distribute your application servers to two AZs as well as your database which can be set up with a master-slave configuration to properly replicate the data between two zones.

If you have more than one private subnet in the same Availability Zone that contains instances that need to be registered with the load balancer, you only need to create one public subnet. You need only one public subnet per Availability Zone; you can add the private instances in all the private subnets that reside in that particular Availability Zone.

mg

src='https://i.udemycdn.com/redactor/raw9-11-15\_05-21-05-c823048b82f65f434901a13b2ecdbfce.p

ng'>

Since you have a public internet-facing load balancer that has a group of backend Amazon EC2 instances that are deployed in a private subnet, you must create the corresponding public subnets in the same Availability Zones. This new public subnet is on top of the private subnet that is used by your private EC2 instances. Lastly, you should associate these public subnets to the Internet-facing load balancer to complete the setup.

To summarize, we need to have one private subnet for the application tier and another one for the database tier. We then need to create another public subnet in the same Availability Zone where the private EC2 instances are hosted, in order to properly connect the public Internet-facing load balancer to your instances. This means that we have to use a total of 3 subnets consisting of 2 private subnets and 1 public subnet.

To meet the requirement of high availability, we have to deploy the stack to two Availability Zones. This means that you have to double the number of subnets you are using. Take note as well that you must create the corresponding public subnet in the same Availability Zone of your private EC2 servers in order for it to properly communicate with the load balancer. Hence, the correct answer is 6 subnets.

References:

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Scenario2.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html)

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

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

---

## QUESTION 202

A company needs to implement a solution that will process real-time streaming data of its users across the globe. This will enable them to track and analyze globally-distributed user activity on their website and mobile applications, including clickstream analysis. The solution should process the data in close geographical proximity to their users and respond to user requests at low latencies.

Which of the following is the most suitable solution for this scenario?

- A. Use a CloudFront web distribution and Route 53 with a Geoproximity routing policy in order to process the data in close geographical proximity to users and respond to user requests at low latencies.

Process real-time streaming data using Kinesis and durably store the results to an Amazon S3 bucket.

- B. Use a CloudFront web distribution and Route 53 with a latency-based routing policy, in order to process the data in close geographical proximity to users and respond to user requests at low latencies.

Process real-time streaming data using Kinesis and durably store the results to an Amazon S3 bucket.

C. Integrate CloudFront with Lambda@Edge in order to process the data in close geographical proximity to users and respond to user requests at low latencies. Process real-time streaming data using Amazon Athena and durably store the results to an Amazon S3 bucket.

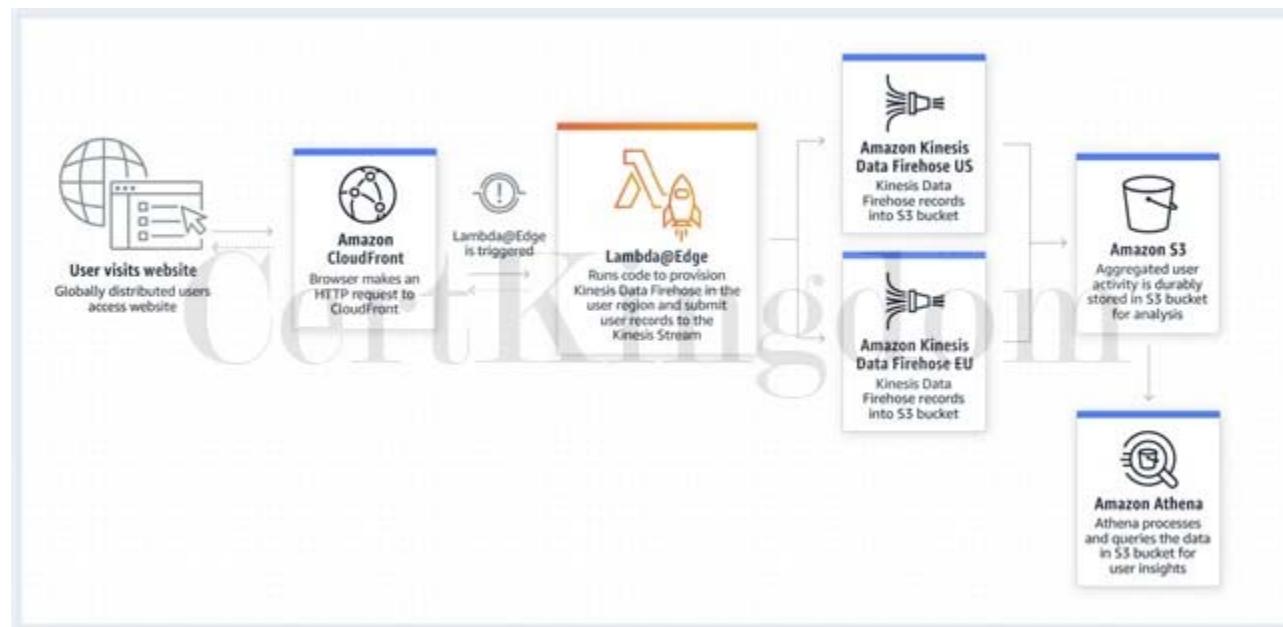
D. Integrate CloudFront with Lambda@Edge in order to process the data in close geographical proximity to users and respond to user requests at low latencies. Process real-time streaming data using Kinesis and durably store the results to an Amazon S3 bucket.

Answer: D

Explanation:

Lambda@Edge is a feature of Amazon CloudFront that lets you run code closer to users of your application, which improves performance and reduces latency. With Lambda@Edge, you don't have to provision or manage infrastructure in multiple locations around the world. You pay only for the compute time you consume - there is no charge when your code is not running.

With Lambda@Edge, you can enrich your web applications by making them globally distributed and improving their performance " " all with zero server administration. Lambda@Edge runs your code in response to events generated by the Amazon CloudFront content delivery network (CDN). Just upload your code to AWS Lambda, which takes care of everything required to run and scale your code with high availability at an AWS location closest to your end user.



By using Lambda@Edge and Kinesis together, you can process real-time streaming data so that you can track and analyze globally-distributed user activity on your website and mobile applications, including clickstream analysis. Hence, the correct answer in this scenario is the option that says:

Integrate CloudFront with Lambda@Edge in order to process the data in close geographical proximity to users and respond to user requests at low latencies. Process real-time streaming data using Kinesis and durably store the results to an Amazon S3 bucket.

The options that say: Use a CloudFront web distribution and Route 53 with a latency-based routing policy, in order to process the data in close geographical proximity to users and respond to user requests at low latencies. Process real-time streaming data using Kinesis and durably store the results to an Amazon S3 bucket and Use a CloudFront web distribution and Route 53 with a Geoproximity routing policy in order to process the data in close geographical proximity to users and respond to user requests at low latencies. Process real-time streaming data using Kinesis and durably store the results to an Amazon S3 bucket are both incorrect because you can only route traffic using Route 53 since it does not have any computing capability. This solution would not be able to process and return the data in close geographical proximity to your users since it is not using Lambda@Edge.

The option that says: Integrate CloudFront with Lambda@Edge in order to process the data in close geographical proximity to users and respond to user requests at low latencies. Process real-time streaming data using Amazon Athena and durably store the results to an Amazon S3 bucket is incorrect because although using Lambda@Edge is correct, Amazon Athena is just an interactive query service that enables you to easily analyze data in Amazon S3 using standard SQL. Kinesis should be used to process the streaming data in real-time.

## References:

<https://aws.amazon.com/lambda/edge/>

<https://aws.amazon.com/blogs/networking-and-content-delivery/global-data-ingestion-with-amazon-cloud-front-and-lambdaedge/>

## QUESTION 203

A large multinational investment bank has a web application that requires a minimum of 4 EC2 instances to run to ensure that it can cater to its users across the globe. You are instructed to ensure fault tolerance of this system.

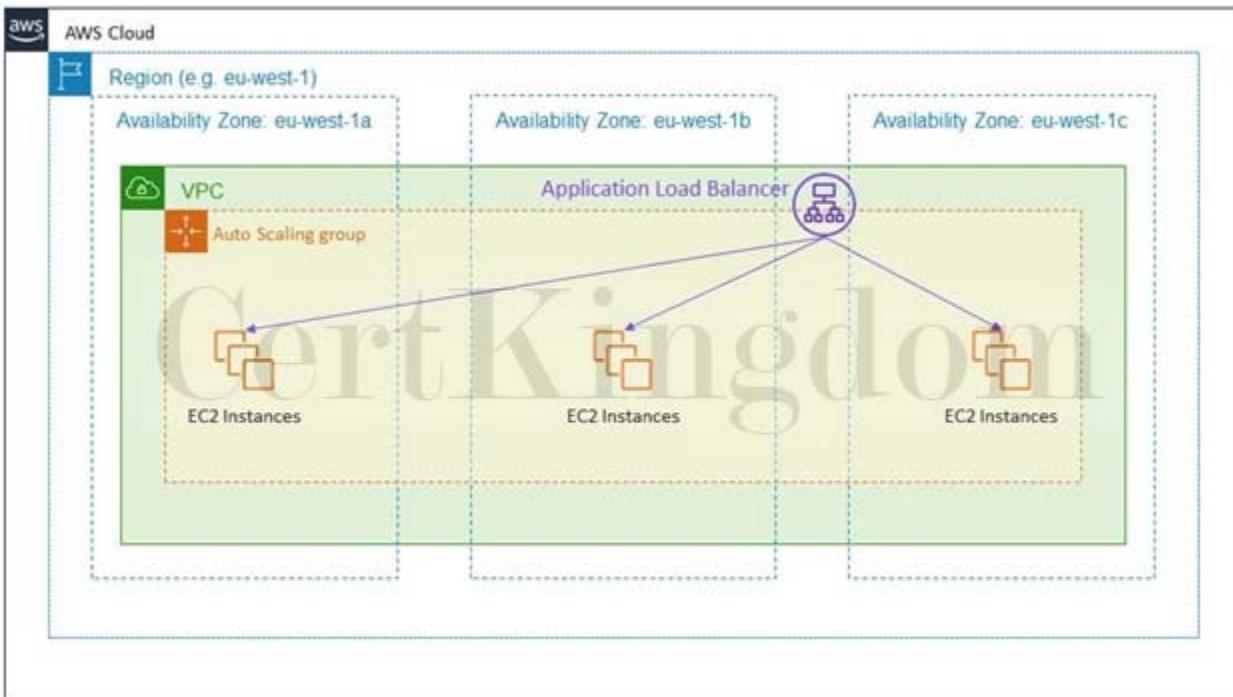
Which of the following is the best option?

- A. Deploy an Auto Scaling group with 4 instances in one Availability Zone behind an Application Load Balancer.
- B. Deploy an Auto Scaling group with 2 instances in each of 3 Availability Zones behind an Application Load Balancer.
- C. Deploy an Auto Scaling group with 2 instances in each of 2 Availability Zones behind an Application Load Balancer.
- D. Deploy an Auto Scaling group with 1 instance in each of 4 Availability Zones behind an Application load Balancer.

Answer: B

Explanation:

Fault Tolerance is the ability of a system to remain in operation even if some of the components used to build the system fail. In AWS, this means that in the event of server fault or system failures, the number of running EC2 instances should not fall below the minimum number of instances required by the system for it to work properly. So if the application requires a minimum of 4 instances, there should be at least 4 instances running in case there is an outage in one of the Availability Zones or if there are server issues.



One of the differences between Fault Tolerance and High Availability is that the former refers to the minimum number of running instances. For example, you have a system that requires a minimum of 4 running instances and currently has 6 running instances deployed in two Availability Zones. There was a component failure in one of the Availability Zones which knocks out 3 instances. In this case, the system can still be regarded as Highly Available since there are still instances running that can accommodate the requests. However, it is not Fault-Tolerant since the required minimum of four instances has not been met.

Hence, the correct answer is: Deploy an Auto Scaling group with 2 instances in each of 3 Availability Zones behind an Application Load Balancer.

The option that says: Deploy an Auto Scaling group with 2 instances in each of 2 Availability Zones behind an Application Load Balancer is incorrect because if one Availability Zone went out, there will only be 2 running instances available out of the required 4 minimum instances. Although the Auto Scaling group can spin up another 2 instances, the fault tolerance of

the web application has already been compromised.

The option that says: Deploy an Auto Scaling group with 4 instances in one Availability Zone behind an Application Load Balancer is incorrect because if the Availability Zone went out, there will be no running instance available to accommodate the request.

The option that says: Deploy an Auto Scaling group with 1 instance in each of 4 Availability Zones behind an Application Load Balancer is incorrect because if one Availability Zone went out, there will only be 3 instances available to accommodate the request.

References:

[https://media.amazonwebservices.com/AWS\\_Building\\_Fault\\_Tolerant\\_Applications.pdf](https://media.amazonwebservices.com/AWS_Building_Fault_Tolerant_Applications.pdf)

<https://d1.awsstatic.com/whitepapers/aws-building-fault-tolerant-applications.pdf>

AWS Overview Cheat Sheets:

<https://tutorialsdojo.com/aws-cheat-sheets-overview/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

---

## QUESTION 204

A technology company is building a new cryptocurrency trading platform that allows the buying and selling of Bitcoin, Ethereum, Ripple, Tether, and many others. You were hired as a Cloud Engineer to build the required infrastructure needed for this new trading platform. On your first week at work, you started to create CloudFormation YAML scripts that define all of the needed AWS resources for the application. Your manager was shocked that you haven't created the EC2 instances, S3 buckets, and other AWS resources straight away. He does not understand the text-based scripts that you have done and has asked for your clarification.

In this scenario, what are the benefits of using the Amazon CloudFormation service that you should tell your manager to clarify his concerns? (Select TWO.)

- A. Allows you to model your entire infrastructure in a text file
- B. Provides highly durable and scalable data storage
- C. Using CloudFormation itself is free, including the AWS resources that have been created.
- D. A storage location for the code of your application
- E. Enables modeling, provisioning, and version-controlling of your entire AWS infrastructure

Answer: A,E

Explanation:

AWS CloudFormation provides a common language for you to describe and provision all the infrastructure resources in your cloud environment. CloudFormation allows you to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. This file serves as the single source of truth for your cloud environment. AWS CloudFormation is available at no additional charge, and you pay only for the AWS resources needed to run your applications.



Hence, the correct answers are:

- Enables modeling, provisioning, and version-controlling of your entire AWS infrastructure

- Allows you to model your entire infrastructure in a text file

The option that says: Provides highly durable and scalable data storage is incorrect because CloudFormation is not a data storage service.

The option that says: A storage location for the code of your application is incorrect because CloudFormation is not used to store your application code. You have to use CodeCommit as a code repository and not CloudFormation.

The option that says: Using CloudFormation itself is free, including the AWS resources that have been created is incorrect because although the use of CloudFormation service is free, you have to pay the AWS resources that you created.

References:

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

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

Check out this AWS CloudFormation Cheat Sheet:

<https://tutorialsdojo.com/aws-cloudformation/>

---

## QUESTION 205

A popular augmented reality (AR) mobile game is heavily using a RESTful API which is hosted in AWS.

The API uses Amazon API Gateway and a DynamoDB table with a preconfigured read and write capacity. Based on your systems monitoring, the DynamoDB table begins to throttle requests during high peak loads which causes the slow performance of the game.

Which of the following can you do to improve the performance of your app?

- A. Create an SQS queue in front of the DynamoDB table.
- B. Use DynamoDB Auto Scaling
- C. Add the DynamoDB table to an Auto Scaling Group.
- D. Integrate an Application Load Balancer with your DynamoDB table.

Answer: B

Explanation:

DynamoDB auto scaling uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read and write capacity to handle sudden increases in traffic, without throttling. When the workload decreases, Application Auto Scaling decreases the throughput so that you don't pay for unused provisioned capacity.

Using DynamoDB Auto Scaling is the best answer. DynamoDB Auto Scaling uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf.

Integrating an Application Load Balancer with your DynamoDB table is incorrect because an Application Load Balancer is not suitable to be used with DynamoDB and in addition, this will not increase the throughput of your DynamoDB table.

Adding the DynamoDB table to an Auto Scaling Group is incorrect because you usually put EC2 instances on an Auto Scaling Group, and not a DynamoDB table.

Creating an SQS queue in front of the DynamoDB table is incorrect because this is not a design principle for high throughput DynamoDB table. Using SQS is for handling queuing and polling the request. This will not increase the throughput of DynamoDB which is required in this situation.

Reference:

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

Check out this Amazon DynamoDB Cheat Sheet:

<https://tutorialsdojo.com/amazon-dynamodb/>

Amazon DynamoDB Overview:

<https://www.youtube.com/watch?v=3ZOyUNIeorU>

---

## QUESTION 206

A company has a web application hosted in an On-Demand EC2 instance. You are creating a shell script that needs the instance's public and private IP addresses.

What is the best way to get the instance's associated IP addresses which your shell script can use?

- A. By using a Curl or Get Command to get the latest user data information from <http://.254.169.254/latest/user-data/>

- B. By using IAM.
- C. By using a Curl or Get Command to get the latest metadata information from <http://.254.169.254/latest/meta-data/>
- D. By using a CloudWatch metric.

Answer: C

Explanation:

Instance metadata is data about your EC2 instance that you can use to configure or manage the running instance. Because your instance metadata is available from your running instance, you do not need to use the Amazon EC2 console or the AWS CLI. This can be helpful when you're writing scripts to run from your instance. For example, you can access the local IP address of your instance from instance metadata to manage a connection to an external application.

```
[ec2-user@ip-10-0-1-172 ~]$ curl http://169.254.169.254/latest/meta-data  
ami-id  
ami-launch-index  
ami-manifest-path  
block-device-mapping/  
events/  
hostname  
iam/  
identity-credentials/  
instance-action  
instance-id  
instance-type  
local-hostname  
local-ipv4  
mac  
metrics/  
network/  
placement/  
profile  
public-hostname  
public-ipv4  
public-keys/  
reservation-id  
security-groups  
services/[ec2-user@ip-10-0-1-172 ~]$ █
```

To view the private IPv4 address, public IPv4 address, and all other categories of instance metadata from within a running instance, use the following URL:

<http://.254.169.254/latest/meta-data/>

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

---

## QUESTION 207

A company recently migrated their applications to AWS. The Solutions Architect must ensure that the applications are highly available and safe from common web security vulnerabilities.

Which is the most suitable AWS service to use to mitigate Distributed Denial of Service (DDoS) attacks from hitting your back-end EC2 instances?

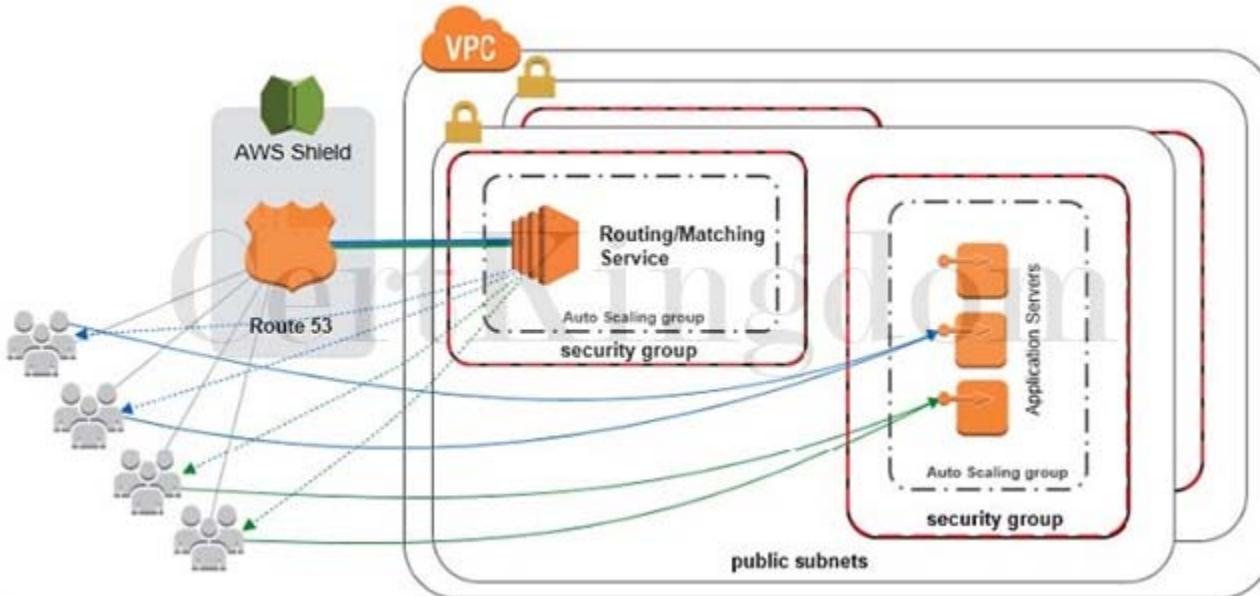
- A. AWS Shield
- B. AWS Firewall Manager
- C. AWS WAF
- D. Amazon GuardDuty

Answer: A

Explanation:

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield - Standard and Advanced.

All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications. When you use AWS Shield Standard with Amazon CloudFront and Amazon Route 53, you receive comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks.



AWS WAF is incorrect because this is a web application firewall service that helps protect your web apps from common exploits that could affect app availability, compromise security, or consume excessive resources. Although this can help you against DDoS attacks, AWS WAF alone is not enough to fully protect your VPC. You still need to use AWS Shield in this scenario.

AWS Firewall Manager is incorrect because this just simplifies your AWS WAF administration and maintenance tasks across multiple accounts and resources.

Amazon GuardDuty is incorrect because this is just an intelligent threat detection service to protect your AWS accounts and workloads. Using this alone will not fully protect your AWS resources against DDoS attacks.

References:

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-which-to-choose.html>

<https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/>

Check out this AWS Shield Cheat Sheet:

<https://tutorialsdojo.com/aws-shield/>

AWS Security Services Overview - WAF, Shield, CloudHSM, KMS:

<https://www.youtube.com/watch?v=-1S-RdeAmMo>

## QUESTION 208

An Auto Scaling group (ASG) of Linux EC2 instances has an Amazon FSx for OpenZFS file system with basic monitoring enabled in CloudWatch. The Solutions Architect noticed that the legacy web application hosted in the ASG takes a long time to load. After checking the instances, the Architect noticed that the ASG is not launching more instances as it should be, even though the servers already have high memory usage.

Which of the following options should the Architect implement to solve this issue?

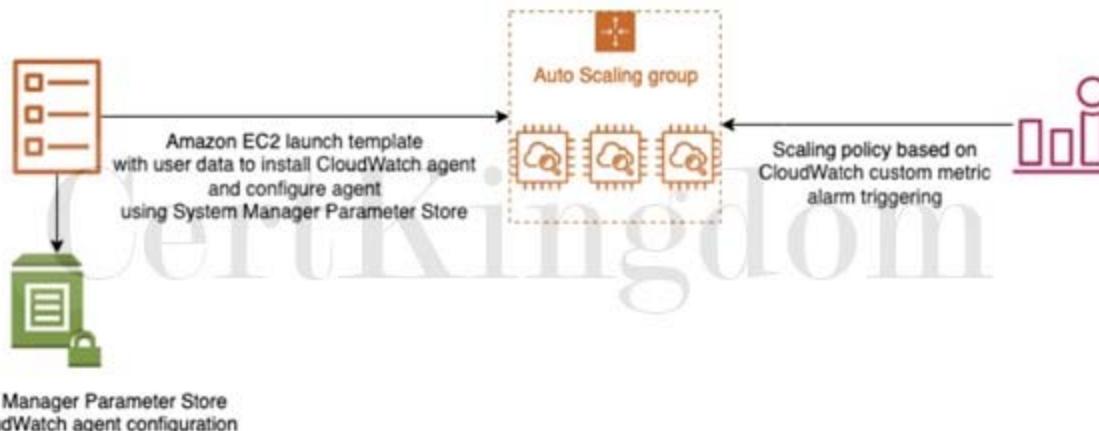
- A. Implement an AI solution that leverages Amazon Comprehend to track the near-real-time memory usage of each and every EC2 instance? Use Amazon SageMaker to automatically trigger the Auto Scaling event if there is high memory usage.
- B. Install the CloudWatch unified agent to the EC2 instances. Set up a custom parameter in AWS Systems Manager Parameter Store with the CloudWatch agent configuration to create an aggregated

metric on memory usage percentage. Scale the Auto Scaling group based on the aggregated metric.  
C. Set up Amazon Rekognition to automatically identify and recognize the cause of the high memory usage. Use the AWS Well-Architected Tool to automatically trigger the scale-out event in the ASG based on the overall memory usage.  
D. Enable detailed monitoring on the Amazon EC2 instances of the Auto Scaling group. Use Amazon Forecast to automatically scale out the Auto Scaling group based on the aggregated memory usage of Amazon EC2 instances.

Answer: B

Explanation:

Amazon CloudWatch agent enables you to collect both system metrics and log files from Amazon EC2 instances and on-premises servers. The agent supports both Windows Server and Linux and allows you to select the metrics to be collected, including sub-resource metrics such as per-CPU core.



The premise of the scenario is that the EC2 servers have high memory usage, but since this specific metric is not tracked by the Auto Scaling group by default, the scaling out activity is not being triggered.

Remember that by default, CloudWatch doesn't monitor memory usage but only the CPU utilization, Network utilization, Disk performance, and Disk Reads/Writes.

This is the reason why you have to install a CloudWatch agent in your EC2 instances to collect and monitor the custom metric (memory usage), which will be used by your Auto Scaling Group as a trigger for scaling activities.

The AWS Systems Manager Parameter Store is one of the capabilities of AWS Systems Manager. It provides secure, hierarchical storage for configuration data management and secrets management. You can store data such as passwords, database strings, Amazon Machine Image (AMI) IDs, and license codes as parameter values. You can store values as plain text or encrypted data. You can reference

Systems Manager parameters in your scripts, commands, SSM documents, and configuration and automation workflows by using the unique name that you specified when you created the parameter.

Hence, the correct answer is: Install the CloudWatch unified agent to the EC2 instances. Set up a custom parameter in AWS Systems Manager Parameter Store with the CloudWatch agent configuration to create an aggregated metric on memory usage percentage. Scale the Auto Scaling group based on the aggregated metric

The option that says: Implement an AI solution that leverages Amazon Comprehend to track the nearreal-time memory usage of each and every EC2 instance? Use Amazon SageMaker to automatically trigger the Auto Scaling event if there is high memory usage is incorrect because Amazon Comprehend cannot track near-real-time memory usage in Amazon EC2. This is just a natural-language processing (NLP) service that uses machine learning to uncover valuable insights and connections in text. Also, the use of an Amazon SageMaker in this scenario is not warranted since there is no machine learning requirement involved.

The option that says: Enable detailed monitoring on the Amazon EC2 instances of the Auto Scaling group. Use Amazon Forecast to automatically scale out the Auto Scaling group based on the aggregated memory usage of Amazon EC2 instances is incorrect because detailed monitoring does not provide metrics for memory usage. CloudWatch does not monitor memory usage in its default set of EC2 metrics and detailed monitoring just provides a higher frequency of metrics (1-minute frequency). Amazon Forecast is a time-series forecasting service based on machine learning (ML) and built for business metrics analysis “” not for scaling out an Auto Scaling group based on an aggregated metric.

The option that says: Set up Amazon Rekognition to automatically identify and recognize the cause of the high memory usage. Use the AWS Well-Architected Tool to automatically trigger the scale-out event in the ASG based on the overall memory usage is incorrect because Amazon Rekognition is simply an image recognition service that detects objects, scenes,

and faces; extracts text; recognizes celebrities; and identifies inappropriate content in images. It can't be used to track the high memory usage of your Amazon EC2 instances. The AWS Well-Architected Tool, on the other hand, is designed to help you review the state of your applications and workloads. It merely provides a central place for architectural best practices in AWS and nothing more.

#### References:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html>  
<https://aws.amazon.com/blogs/mt/create-amazon-ec2-auto-scaling-policy-memory-utilization-metric-linux/>  
<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-parameter-store.html>

Check out these Amazon EC2 and CloudWatch Cheat Sheets:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>  
<https://tutorialsdojo.com/amazon-cloudwatch/>

---

### QUESTION 209

A company plans to develop a custom messaging service that will also be used to train their AI for an automatic response feature which they plan to implement in the future. Based on their research and tests, the service can receive up to thousands of messages a day, and all of these data are to be sent to Amazon EMR for further processing. It is crucial that none of the messages are lost, no duplicates are produced, and that they are processed in EMR in the same order as their arrival. Which of the following options can satisfy the given requirement?

- A. Create an Amazon Kinesis Data Stream to collect the messages.
- B. Set up a default Amazon SQS queue to handle the messages.
- C. Create a pipeline using AWS Data Pipeline to handle the messages.
- D. Set up an Amazon SNS Topic to handle the messages.

Answer: A

#### Explanation:

Two important requirements that the chosen AWS service should fulfill is that data should not go missing, is durable, and streams data in the sequence of arrival. Kinesis can do the job just fine because of its architecture. A Kinesis data stream is a set of shards that has a sequence of data records, and each data record has a sequence number that is assigned by Kinesis Data Streams. Kinesis can also easily handle the high volume of messages being sent to the service.



Amazon Kinesis Data Streams enables real-time processing of streaming big data. It provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications. The Amazon Kinesis Client Library (KCL) delivers all records for a given partition key to the same record processor, making it easier to build multiple applications reading from the same Amazon Kinesis data stream (for example, to perform counting, aggregation, and filtering).

Setting up a default Amazon SQS queue to handle the messages is incorrect because although SQS is a valid messaging service, it is not suitable for scenarios where you need to process the data based on the order they were received. Take note that a default queue in SQS is just a standard queue and not a FIFO (First-In-First-Out) queue. In addition, SQS does not guarantee that no duplicates will be sent.

Setting up an Amazon SNS Topic to handle the messages is incorrect because SNS is a pub-sub messaging service in AWS. SNS might not be capable of handling such a large volume of messages being received and sent at a time. It does not also guarantee that the data will be transmitted in the same order they were received.

Creating a pipeline using AWS Data Pipeline to handle the messages is incorrect because this is primarily used as a cloud-based data workflow service that helps you process and move data between different AWS services and on-premises data sources. It is not suitable for collecting data from distributed sources such as users, IoT devices, or clickstreams.

References:

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

For additional information, read the When should I use Amazon Kinesis Data Streams, and when should I use Amazon SQS? section of the Kinesis Data Stream FAQ:

<https://aws.amazon.com/kinesis/data-streams/faqs/>

Check out this Amazon Kinesis Cheat Sheet:

<https://tutorialsdojo.com/amazon-kinesis/>

---

## QUESTION 210

A company has a High Performance Computing (HPC) cluster that is composed of EC2 Instances with Provisioned IOPS volume to process transaction-intensive, low-latency workloads. The Solutions Architect must maintain high IOPS while keeping the latency down by setting the optimal queue length for the volume. The size of each volume is 10 GiB.

Which of the following is the MOST suitable configuration that the Architect should set up?

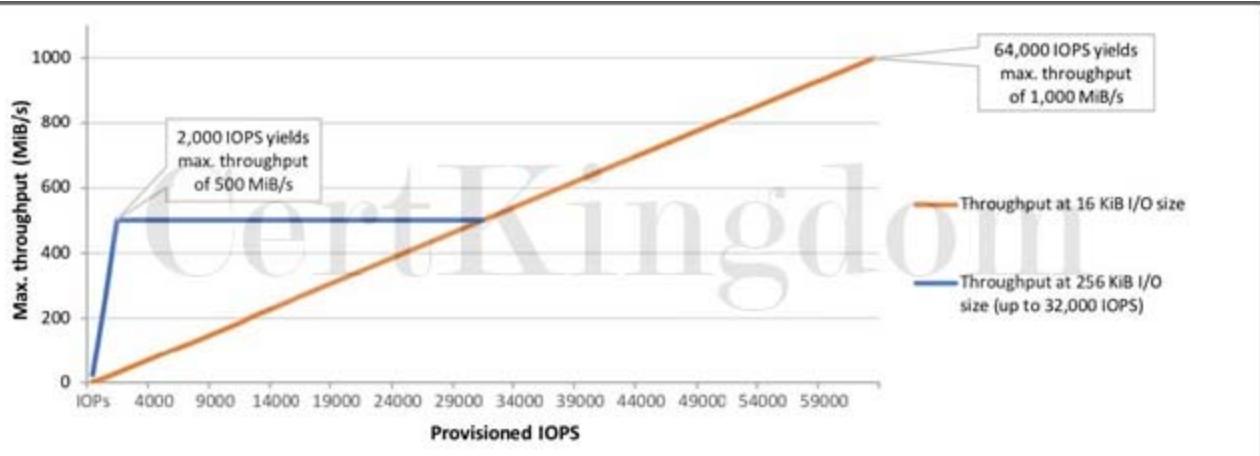
- A. Set the IOPS to 500 then maintain a low queue length.
- B. Set the IOPS to 400 then maintain a low queue length.
- C. Set the IOPS to 600 then maintain a high queue length.
- D. Set the IOPS to 800 then maintain a low queue length.

Answer: A

Explanation:

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. An io1 volume can range in size from 4 GiB to 16 TiB. You can provision from 100 IOPS up to 64,000 IOPS per volume on Nitro system instance families and up to 32,000 on other instance families. The maximum ratio of provisioned IOPS to requested volume size (in GiB) is 50:1.

For example, a 100 GiB volume can be provisioned with up to 5,000 IOPS. On a supported instance type, any volume 1,280 GiB in size or greater allows provisioning up to the 64,000 IOPS maximum ( $50 \times 1,280 \text{ GiB} = 64,000$ ).



An io1 volume provisioned with up to 32,000 IOPS supports a maximum I/O size of 256 KiB and yields as much as 500 MiB/s of throughput. With the I/O size at the maximum, peak throughput is reached at 2,000 IOPS. A volume provisioned with more than 32,000 IOPS (up to the cap of 64,000 IOPS) supports a maximum I/O size of 16 KiB and yields as much as 1,000 MiB/s of throughput.

The volume queue length is the number of pending I/O requests for a device. Latency is the true end-to-end client time of an I/O operation, in other words, the time elapsed between sending an I/O to EBS and receiving an acknowledgement from EBS that the I/O read or write is complete. Queue length must be correctly calibrated with I/O size and latency to avoid creating bottlenecks either on the guest operating system or on the network link to EBS.

Optimal queue length varies for each workload, depending on your particular application's sensitivity to IOPS and latency. If your workload is not delivering enough I/O requests to fully use the performance available to your EBS volume then your volume might not deliver the IOPS or throughput that you have provisioned.

Transaction-intensive applications are sensitive to increased I/O latency and are well-suited for SSD-backed io1 and gp2 volumes. You can maintain high IOPS while keeping latency down by maintaining a low queue length and a high number of IOPS available to the volume. Consistently driving more IOPS to a volume than it has available can cause increased I/O latency.

Throughput-intensive applications are less sensitive to increased I/O latency, and are well-suited for HDD-backed st1 and sc1 volumes. You can maintain high throughput to HDD-backed volumes by maintaining a high queue length when performing large, sequential I/O.

Therefore, for instance, a 10 GiB volume can be provisioned with up to 500 IOPS. Any volume 640 GiB in size or greater allows provisioning up to a maximum of 32,000 IOPS ( $50 \text{ GiB} / 640 \text{ GiB} = 32,000$ ). Hence, the correct answer is to set the IOPS to 500 then maintain a low queue length.

Setting the IOPS to 400 then maintaining a low queue length is incorrect because although a value of 400 is an acceptable value, it is not the maximum value for the IOPS. You will not fully utilize the available IOPS that the volume can offer if you just set it to 400.

The options that say: Set the IOPS to 600 then maintain a high queue length and Set the IOPS to 800 then maintain a low queue length are both incorrect because the maximum IOPS for the 10 GiB volume is only 500. Therefore, any value greater than the maximum amount, such as 600 or 800, is wrong.

Moreover, you should keep the latency down by maintaining a low queue length, and not higher.

#### References:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>

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

#### Amazon EBS Overview - SSD vs HDD:

<https://www.youtube.com/watch?v=LW7x8wyLFvw&t=8s>

#### Check out this Amazon EBS Cheat Sheet:

<https://tutorialsdojo.com/amazon-ebs/>

## QUESTION 211

A company launched an EC2 instance in the newly created VPC. They noticed that the generated instance does not have an associated DNS hostname.

Which of the following options could be a valid reason for this issue?

- A. The security group of the EC2 instance needs to be modified.

- B. Amazon Route53 is not enabled.
- C. The newly created VPC has an invalid CIDR block.
- D. The DNS resolution and DNS hostname of the VPC configuration should be enabled.

Answer: D

Explanation:

When you launch an EC2 instance into a default VPC, AWS provides it with public and private DNS hostnames that correspond to the public IPv4 and private IPv4 addresses for the instance.

VPC ID	State	VPC CIDR	DHCP options set	Route table
vpc-3902905c	available	172.31.0.0/16	dopt-fa2f3498	rtb-554ed530
vpc-d0bf29b4	available	10.10.0.0/16	dopt-fa2f3498	rtb-100d4174

**| PrivateSDN**

Logs Tags

VPC ID: vpc-d0bf29b4 | PrivateSDN  
State: available  
CIDR: 10.10.0.0/16  
DHCP options set: dopt-fa2f3498  
Route table: rtb-100d4174

Network ACL: acl-70c55c14  
Tenancy: Default  
**DNS resolution: yes**  
**DNS hostnames: yes**

However, when you launch an instance into a non-default VPC, AWS provides the instance with a private DNS hostname only. New instances will only be provided with public DNS hostname depending on these two DNS attributes: the DNS resolution and DNS hostnames, that you have specified for your VPC, and if your instance has a public IPv4 address. In this case, the new EC2 instance does not automatically get a DNS hostname because the DNS resolution and DNS hostnames attributes are disabled in the newly created VPC. Hence, the correct answer is: The DNS resolution and DNS hostname of the VPC configuration should be enabled.

The option that says: The newly created VPC has an invalid CIDR block is incorrect since it's very unlikely that a VPC has an invalid CIDR block because of AWS validation schemes.

The option that says: Amazon Route 53 is not enabled is incorrect since Route 53 does not need to be enabled. Route 53 is the DNS service of AWS, but the VPC is the one that enables assigning of instance hostnames.

The option that says: The security group of the EC2 instance needs to be modified is incorrect since security groups are just firewalls for your instances. They filter traffic based on a set of security group rules.

References:

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-dns.html>

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

Amazon VPC Overview:

<https://www.youtube.com/watch?v=oIDHKeNxvQQ>

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

## QUESTION 212

A company is looking to store their confidential financial files in AWS which are accessed every week.

The Architect was instructed to set up the storage system which uses envelope encryption and automates key rotation. It should also provide an audit trail that shows who used the encryption key and by whom for security purposes.

Which combination of actions should the Architect implement to satisfy the requirement in the most costeffective way? (Select TWO.)

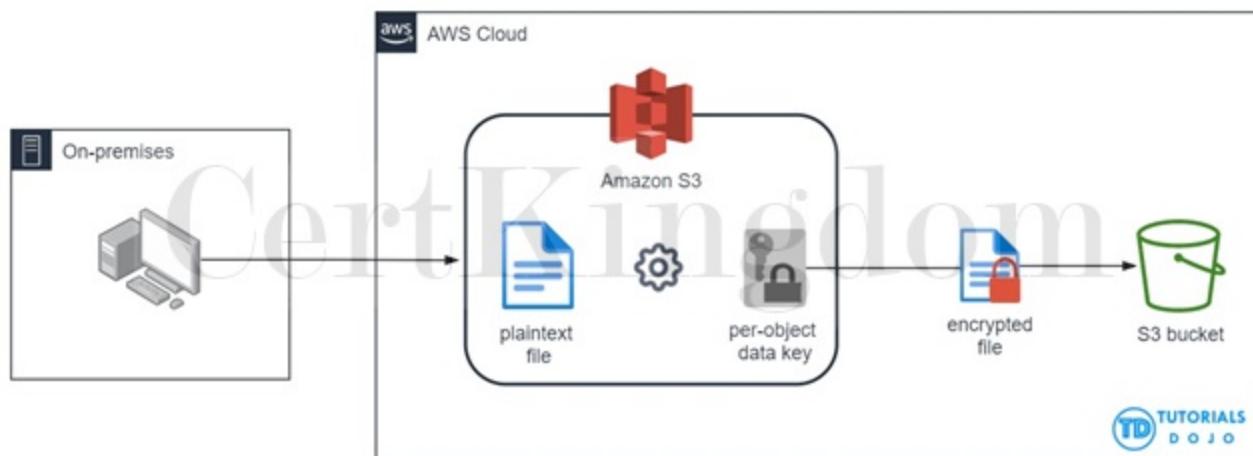
- A. Configure Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3).

- B. Configure Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS).
- C. Use Amazon S3 Glacier Deep Archive to store the data.
- D. Configure Server-Side Encryption with Customer-Provided Keys (SSE-C).
- E. Use Amazon S3 to store the data.
- F. Amazon Certificate Manager

Answer: B,E

Explanation:

Server-side encryption is the encryption of data at its destination by the application or service that receives it. AWS Key Management Service (AWS KMS) is a service that combines secure, highly available hardware and software to provide a key management system scaled for the cloud. Amazon S3 uses AWS KMS customer master keys (CMKs) to encrypt your Amazon S3 objects. SSE-KMS encrypts only the object data. Any object metadata is not encrypted. If you use customer-managed CMKs, you use AWS KMS via the AWS Management Console or AWS KMS APIs to centrally create encryption keys, define the policies that control how keys can be used, and audit key usage to prove that they are being used correctly. You can use these keys to protect your data in Amazon S3 buckets.



A customer master key (CMK) is a logical representation of a master key. The CMK includes metadata, such as the key ID, creation date, description, and key state. The CMK also contains the key material used to encrypt and decrypt data. You can use a CMK to encrypt and decrypt up to 4 KB (4096 bytes) of data. Typically, you use CMKs to generate, encrypt, and decrypt the data keys that you use outside of AWS KMS to encrypt your data. This strategy is known as envelope encryption.

You have three mutually exclusive options depending on how you choose to manage the encryption keys:

Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) “ Each object is encrypted with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

Use Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS) “ Similar to SSE-S3, but with some additional benefits and charges for using this service. There are separate permissions for the use of a CMK that provides added protection against unauthorized access of your objects in Amazon S3. SSE-KMS also provides you with an audit trail that shows when your CMK was used and by whom. Additionally, you can create and manage customer-managed CMKs or use AWS managed CMKs that are unique to you, your service, and your Region.

Use Server-Side Encryption with Customer-Provided Keys (SSE-C) “ You manage the encryption keys and Amazon S3 manages the encryption, as it writes to disks, and decryption when you access your objects.

In the scenario, the company needs to store financial files in AWS which are accessed every week and the solution should use envelope encryption. This requirement can be fulfilled by using an Amazon S3 configured with Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS). Hence, using Amazon S3 to store the data and configuring Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS) are the correct answers.

Using Amazon S3 Glacier Deep Archive to store the data is incorrect. Although this provides the most cost-effective storage solution, it is not the appropriate service to use if the files being stored are frequently accessed every week.

Configuring Server-Side Encryption with Customer-Provided Keys (SSE-C) and configuring Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) are both incorrect. Although you can configure automatic key

rotation, these two do not provide you with an audit trail that shows when your CMK was used and by whom, unlike Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS).

#### References:

- <https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>
  - <https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html>
  - <https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html>
- Check out this Amazon S3 Cheat Sheet:  
<https://tutorialsdojo.com/amazon-s3/>
- 

### QUESTION 213

A company deployed an online enrollment system database on a prestigious university, which is hosted in RDS. The Solutions Architect is required to monitor the database metrics in Amazon CloudWatch to ensure the availability of the enrollment system.

What are the enhanced monitoring metrics that Amazon CloudWatch gathers from Amazon RDS DB instances which provide more accurate information? (Select TWO.)

- A. OS processes
- B. Database Connections
- C. Freeable Memory
- D. CPU Utilization
- E. RDS child processes.

Answer: A,E

#### 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.

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. 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.

## Enhanced monitoring (9)

Manage graphs

Monitoring ▾

5 minutes ▾

2/13/2018

17

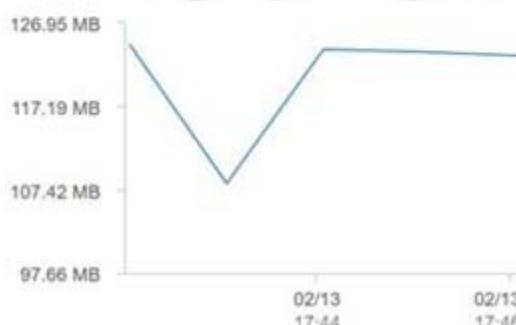
: 34

Go

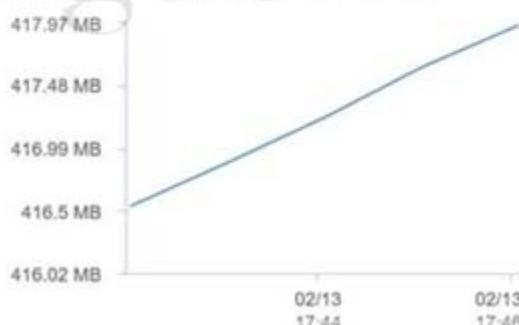


< 1 2 > ⚙️ ⌂

### Free Memory



### Active Memory



In RDS, the Enhanced Monitoring metrics shown in the Process List view are organized as follows: RDS child processes ““ Shows a summary of the RDS processes that support the DB instance, for example aurora for Amazon Aurora DB clusters and mysqld for MySQL DB instances. Process threads appear nested beneath the parent process. Process threads show CPU utilization only as other metrics are the same for all threads for the process. The console displays a maximum of 100 processes and threads. The results are a combination of the top CPU consuming and memory consuming processes and threads. If there are more than 50 processes and more than 50 threads, the console displays the top 50 consumers in each category. This display helps you identify which processes are having the greatest impact on performance.

RDS processes ““ Shows a summary of the resources used by the RDS management agent, diagnostics monitoring processes, and other AWS processes that are required to support RDS DB instances.

OS processes ““ Shows a summary of the kernel and system processes, which generally have minimal impact on performance.

CPU Utilization, Database Connections, and Freeable Memory are incorrect because these are just the regular items provided by Amazon RDS Metrics in CloudWatch. Remember that the scenario is asking for the Enhanced Monitoring metrics.

### References:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/rds-metricscollected.html>

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_Monitoring.OS.html#USER\\_Monitoring.OS.CloudWatchLogs](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Monitoring.OS.html#USER_Monitoring.OS.CloudWatchLogs)

Check out this Amazon CloudWatch Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudwatch/>

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

## QUESTION 214

A company has a set of Linux servers running on multiple On-Demand EC2 Instances. The Audit team wants to collect and process the application log files generated from these servers for their report.

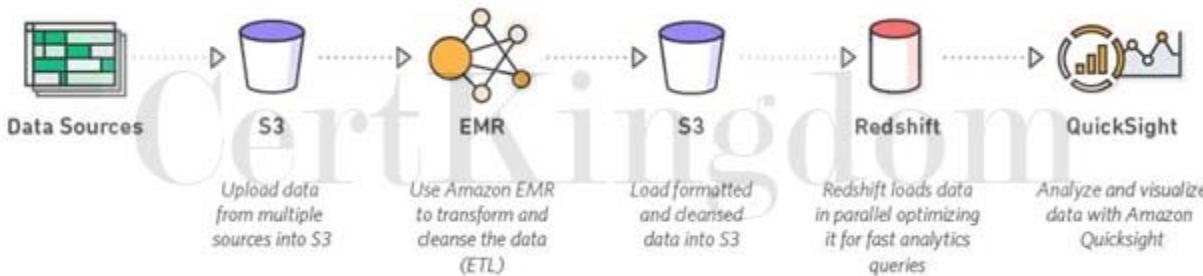
Which of the following services is best to use in this case?

- A. A single On-Demand Amazon EC2 instance for both storing and processing the log files
- B. Amazon S3 Glacier Deep Archive for storing the application log files and AWS ParallelCluster for processing the log files.
- C. Amazon S3 Glacier for storing the application log files and Spot EC2 Instances for processing them.
- D. Amazon S3 for storing the application log files and Amazon Elastic MapReduce for processing the log files.

Answer: D

Explanation:

Amazon EMR is a managed cluster platform that simplifies running big data frameworks, such as Apache Hadoop and Apache Spark, on AWS to process and analyze vast amounts of data. By using these frameworks and related open-source projects such as Apache Hive and Apache Pig, you can process data for analytics purposes and business intelligence workloads. Additionally, you can use Amazon EMR to transform and move large amounts of data into and out of other AWS data stores and databases such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB.



Hence, the correct answer is: Amazon S3 for storing the application log files and Amazon Elastic MapReduce for processing the log files.

The option that says: Amazon S3 Glacier for storing the application log files and Spot EC2 Instances for processing them is incorrect as Amazon S3 Glacier is used for data archive only.

The option that says: A single On-Demand Amazon EC2 instance for both storing and processing the logfiles is incorrect as an EC2 instance is not a recommended storage service. In addition, Amazon EC2 does not have a built-in data processing engine to process large amounts of data.

The option that says: Amazon S3 Glacier Deep Archive for storing the application log files and AWS ParallelCluster for processing the log files is incorrect because the long retrieval time of Amazon S3 Glacier Deep Archive makes this option unsuitable. Moreover, AWS ParallelCluster is just 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. ParallelCluster uses a simple text file to model and provision all the resources needed for your HPC applications in an automated and secure manner.

References:

<http://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-what-is-emr.html>

<https://aws.amazon.com/hpc/parallelcluster/>

Check out this Amazon EMR Cheat Sheet:

<https://tutorialsdojo.com/amazon-emr/>

## QUESTION 215

An online trading platform with thousands of clients across the globe is hosted in AWS. To reduce latency, you have to direct user traffic to the nearest application endpoint to the client. The traffic should be routed to the closest edge location via an Anycast static IP address. AWS Shield should also be integrated into the solution for DDoS protection.

Which of the following is the MOST suitable service that the Solutions Architect should use to satisfy the above requirements?

- A. AWS WAF
- B. AWS Global Accelerator
- C. AWS PrivateLink
- D. Amazon CloudFront

Answer: B

Explanation:

AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers or Amazon EC2 instances.

AWS Global Accelerator uses the AWS global network to optimize the path from your users to your applications, improving the performance of your TCP and UDP traffic. AWS Global Accelerator continually monitors the health of your application endpoints and will detect an unhealthy endpoint and redirect traffic to healthy endpoints in less than 1 minute.



Many applications, such as gaming, media, mobile applications, and financial applications, need very low latency for a great user experience. To improve the user experience, AWS Global Accelerator directs user traffic to the nearest application endpoint to the client, thus reducing internet latency and jitter. It routes the traffic to the closest edge location via Anycast, then by routing it to the closest regional endpoint over the AWS global network. AWS Global Accelerator quickly reacts to changes in network performance to improve your users' application performance.

AWS Global Accelerator and Amazon CloudFront are separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable content (such as images and videos) and dynamic content (such as API acceleration and dynamic site delivery). Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. Both services integrate with AWS Shield for DDoS protection.

Hence, the correct answer is AWS Global Accelerator.

Amazon CloudFront is incorrect because although this service uses edge locations, it doesn't have the capability to route the traffic to the closest edge location via an Anycast static IP address.

AWS WAF is incorrect because this service is just a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources.

AWS PrivateLink is incorrect because this service simply provides private connectivity between VPCs, AWS services, and on-premises applications, securely on the Amazon network. It doesn't route traffic to the closest edge location via an Anycast static IP address.

#### References:

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

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

Check out this AWS Global Accelerator Cheat Sheet:

<https://tutorialsdojo.com/aws-global-accelerator/>

## QUESTION 216

An application is using a RESTful API hosted in AWS which uses Amazon API Gateway and AWS Lambda. There is a requirement to trace and analyze user requests as they travel through your Amazon API Gateway APIs to the underlying services.

Which of the following is the most suitable service to use to meet this requirement?

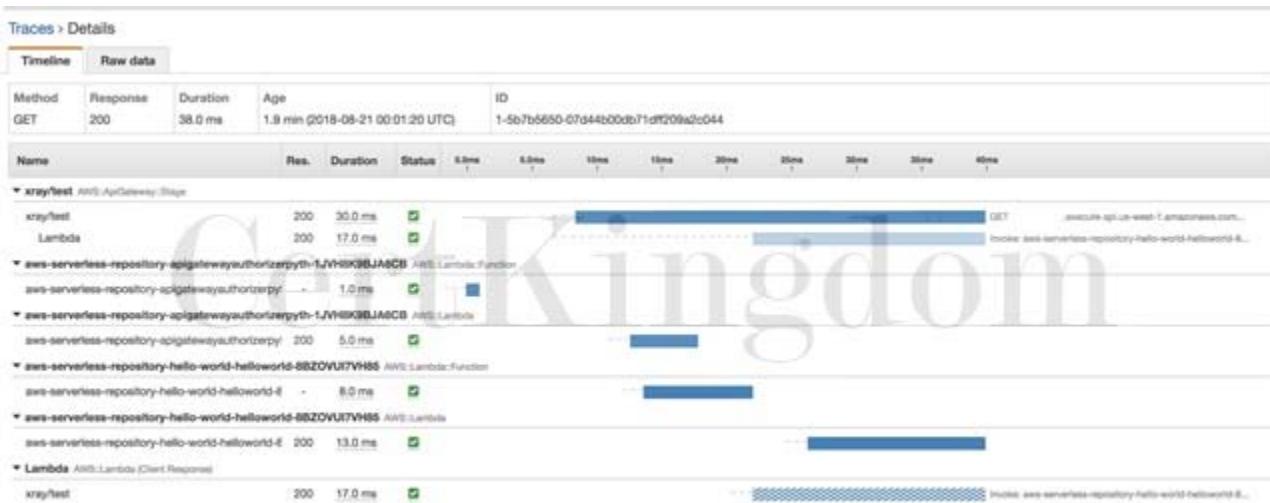
- A. CloudWatch
- B. CloudTrail
- C. VPC Flow Logs
- D. AWS X-Ray

Answer: D

## Explanation:

You can use AWS X-Ray to trace and analyze user requests as they travel through your Amazon API Gateway APIs to the underlying services. API Gateway supports AWS X-Ray tracing for all API Gateway endpoint types: regional, edge-optimized, and private. You can use AWS X-Ray with Amazon API Gateway in all regions where X-Ray is available. X-Ray gives you an end-to-end view of an entire request, so you can analyze latencies in your APIs and their backend services. You can use an X-Ray service map to view the latency of an entire request and that of the downstream services that are integrated with X-Ray. And you can configure sampling rules to tell X-Ray which requests to record, at what sampling rates, according to criteria that you specify. If you call an API Gateway API from a service that's already being traced, API Gateway passes the trace through, even if X-Ray tracing is not enabled on the API.

You can enable X-Ray for an API stage by using the API Gateway management console, or by using the API Gateway API or CLI.



VPC Flow Logs is incorrect because this is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your entire VPC. Although it can capture some details about the incoming user requests, it is still better to use AWS X-Ray as it provides a better way to debug and analyze your microservices applications with request tracing so you can find the root cause of your issues and performance.

CloudWatch is incorrect because this is a monitoring and management service. It does not have the capability to trace and analyze user requests as they travel through your Amazon API Gateway APIs.

CloudTrail is incorrect because this is primarily used for IT audits and API logging of all of your AWS resources. It does not have the capability to trace and analyze user requests as they travel through your Amazon API Gateway APIs, unlike AWS X-Ray.

Reference:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-xray.html>

Check out this AWS X-Ray Cheat Sheet:

<https://tutorialsdojo.com/aws-x-ray/>

Instrumenting your Application with AWS X-Ray:

<https://tutorialsdojo.com/instrumenting-your-application-with-aws-x-ray/>

## QUESTION 217

A financial firm is designing an application architecture for its online trading platform that must have high availability and fault tolerance. Their Solutions Architect configured the application to use an Amazon S3 bucket located in the us-east-1 region to store large amounts of intraday financial data. The stored financial data in the bucket must not be affected even if there is an outage in one of the Availability Zones or if there's a regional service failure.

What should the Architect do to avoid any costly service disruptions and ensure data durability?

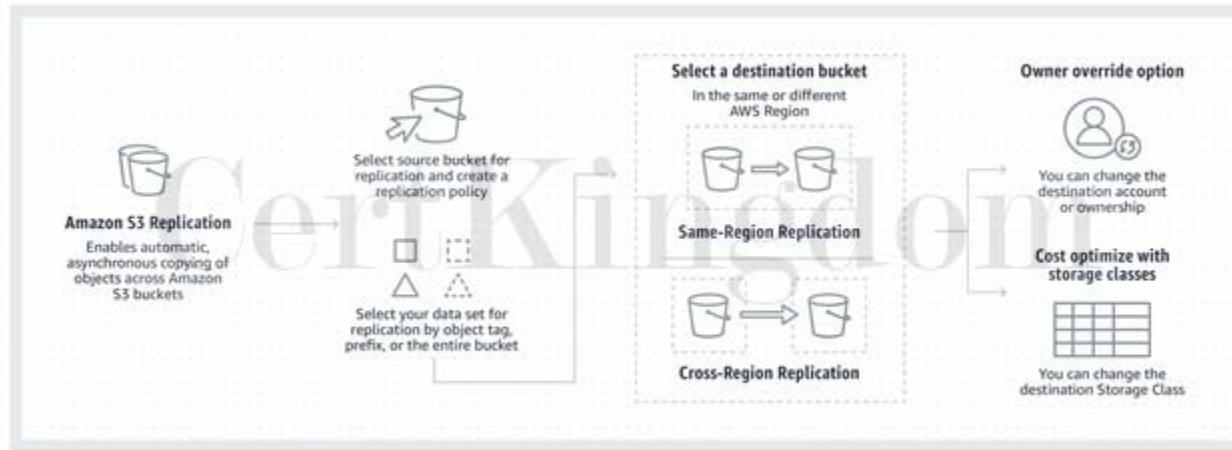
- A. Copy the S3 bucket to an EBS-backed EC2 instance.
- B. Create a Lifecycle Policy to regularly backup the S3 bucket to Amazon Glacier.
- C. Enable Cross-Region Replication.
- D. Create a new S3 bucket in another region and configure Cross-Account Access to the bucket located in us-east-1.

Answer: C

#### Explanation:

In this scenario, you need to enable Cross-Region Replication to ensure that your S3 bucket would not be affected even if there is an outage in one of the Availability Zones or a regional service failure in us-east-

- When you upload your data in S3, your objects are redundantly stored on multiple devices across multiple facilities within the region only, where you created the bucket. Thus, if there is an outage on the entire region, your S3 bucket will be unavailable if you do not enable Cross-Region Replication, which should make your data available to another region.



Note that an Availability Zone (AZ) is more related with Amazon EC2 instances rather than Amazon S3 so if there is any outage in the AZ, the S3 bucket is usually not affected but only the EC2 instances deployed on that zone.

Hence, the correct answer is: Enable Cross-Region Replication.

The option that says: Copy the S3 bucket to an EBS-backed EC2 instance is incorrect because EBS is not as durable as Amazon S3. Moreover, if the Availability Zone where the volume is hosted goes down then the data will also be inaccessible.

The option that says: Create a Lifecycle Policy to regularly backup the S3 bucket to Amazon Glacier is incorrect because Glacier is primarily used for data archival. You also need to replicate your data to another region for better durability.

The option that says: Create a new S3 bucket in another region and configure Cross-Account Access to the bucket located in us-east-1 is incorrect because Cross-Account Access in Amazon S3 is primarily used if you want to grant access to your objects to another AWS account, and not just to another AWS Region. For example, Account MANILA can grant another AWS account (Account CEBU) permission to access its resources such as buckets and objects. S3 Cross-Account Access does not replicate data from one region to another. A better solution is to enable Cross-Region Replication (CRR) instead.

References:

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

<https://aws.amazon.com/s3/features/replication/>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

## QUESTION 218

A Solutions Architect is designing the cloud architecture for the enterprise application suite of the company. Both the web and application tiers need to access the Internet to fetch data from public APIs.

However, these servers should be inaccessible from the Internet.

Which of the following steps should the Architect implement to meet the above requirements?

- Deploy the web and application tier instances to a private subnet and then allocate an Elastic IP address to each EC2 instance.
- Deploy a NAT gateway in the public subnet and add a route to it from the private subnet where the web and application tiers are hosted.
- Deploy a NAT gateway in the private subnet and add a route to it from the public subnet where the web and application tiers are hosted.

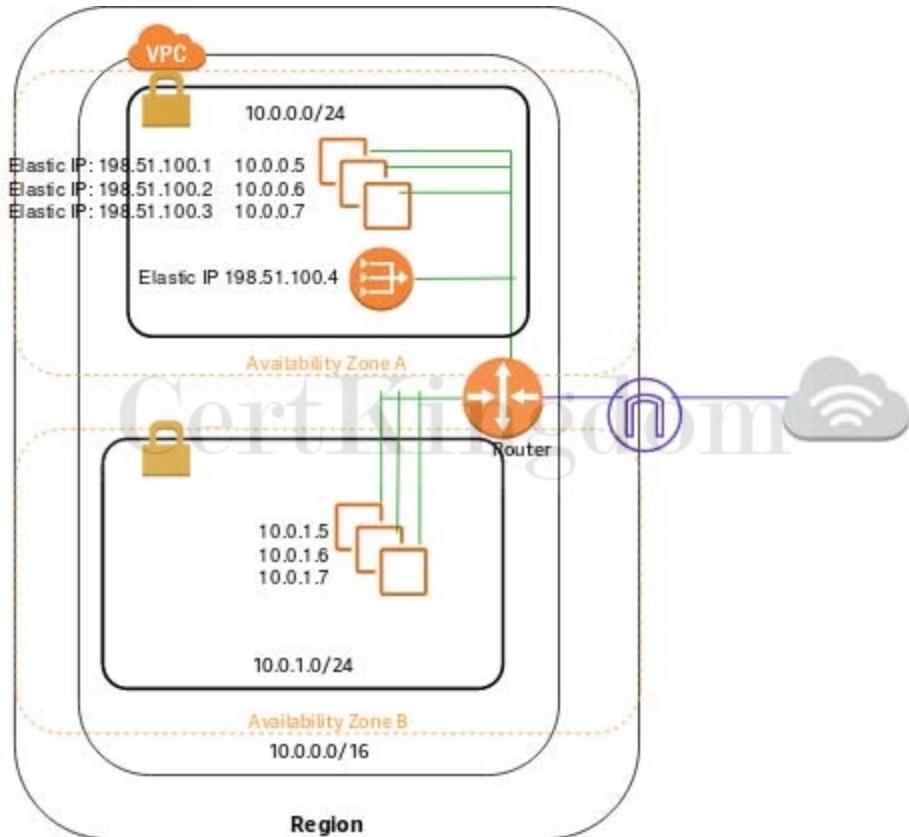
D. Deploy the web and application tier instances to a public subnet and then allocate an Elastic IP address to each EC2 instance.

Answer: B

Explanation:

You can use a network address translation (NAT) gateway 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. You are charged for creating and using a NAT gateway in your account.

NAT gateway hourly usage and data processing rates apply. Amazon EC2 charges for data transfer also apply. NAT gateways are not supported for IPv6 traffic; use an egress-only internet gateway instead.



To create a NAT gateway, you must specify the public subnet in which the NAT gateway should reside. You must also specify an Elastic IP address to associate with the NAT gateway when you create it. The Elastic IP address cannot be changed once you associate it with the NAT Gateway.

After you've created a NAT gateway, you must update the route table associated with one or more of your private subnets to point Internet-bound traffic to the NAT gateway. This enables instances in your private subnets to communicate with the internet. Each NAT gateway is created in a specific Availability Zone and implemented with redundancy in that zone. You have a limit on the number of NAT gateways you can create in an Availability Zone.

Hence, the correct answer is to deploy a NAT gateway in the public subnet and add a route to it from the private subnet where the web and application tiers are hosted.

Deploying the web and application tier instances to a private subnet and then allocating an Elastic IP address to each EC2 instance is incorrect because an Elastic IP address is just a static, public IPv4 address. In this scenario, you have to use a NAT Gateway instead.

Deploying a NAT gateway in the private subnet and adding a route to it from the public subnet where the web and application tiers are hosted is incorrect because you have to deploy a NAT gateway in the public subnet instead and not on a private one.

Deploying the web and application tier instances to a public subnet and then allocating an Elastic IP address to each EC2 instance is incorrect because having an EIP address is irrelevant as it is only a static, public IPv4 address. Moreover, you should deploy the web and application tier in the private subnet instead of a public subnet to make it inaccessible from the Internet and then just add a NAT Gateway to allow outbound Internet connection.

Reference:

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

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

---

## QUESTION 219

A tech startup has recently received a Series A round of funding to continue building their mobile forex trading application. You are hired to set up their cloud architecture in AWS and to implement a highly available, fault tolerant system. For their database, they are using DynamoDB and for authentication, they have chosen to use Cognito. Since the mobile application contains confidential financial transactions, there is a requirement to add a second authentication method that doesn't rely solely on user name and password.

How can you implement this in AWS?

- A. Add multi-factor authentication (MFA) to a user pool in Cognito to protect the identity of your users.
- B. Add a new IAM policy to a user pool in Cognito.
- C. Develop a custom application that integrates with Cognito that implements a second layer of authentication.
- D. Integrate Cognito with Amazon SNS Mobile Push to allow additional authentication via SMS.

Answer: A

Explanation:

You can add multi-factor authentication (MFA) to a user pool to protect the identity of your users. MFA adds a second authentication method that doesn't rely solely on user name and password. You can choose to use SMS text messages, or time-based one-time (TOTP) passwords as second factors in signing in your users. You can also use adaptive authentication with its risk-based model to predict when you might need another authentication factor. It's part of the user pool advanced security features, which also include protections against compromised credentials.

Reference:

<https://docs.aws.amazon.com/cognito/latest/developerguide/managing-security.html>

---

## QUESTION 220

There are a few, easily reproducible but confidential files that your client wants to store in AWS without worrying about storage capacity. For the first month, all of these files will be accessed frequently but after that, they will rarely be accessed at all. The old files will only be accessed by developers so there is no set retrieval time requirement. However, the files under a specific tdojo-finance prefix in the S3 bucket will be used for post-processing that requires millisecond retrieval time.

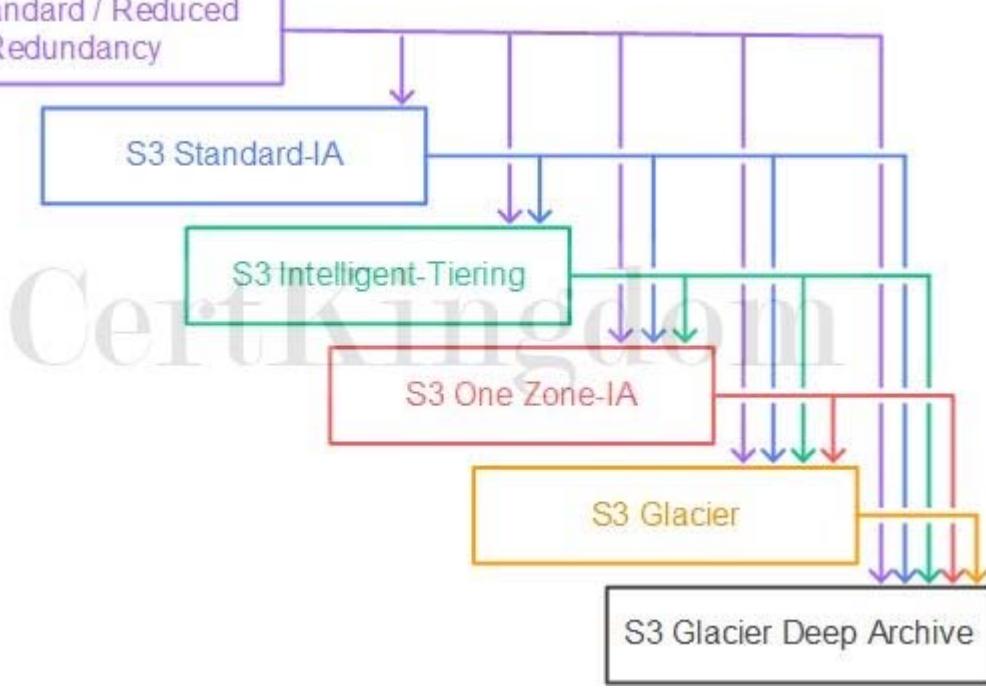
Given these conditions, which of the following options would be the most cost-effective solution for your client's storage needs?

- A. Store the files in S3 then after a month, change the storage class of the tdojo-finance prefix to S3-IA while the remaining go to Glacier using lifecycle policy.
- B. Store the files in S3 then after a month, change the storage class of the tdojo-finance prefix to One Zone-IA while the remaining go to Glacier using lifecycle policy.
- C. Store the files in S3 then after a month, change the storage class of the bucket to Intelligent-Tiering using lifecycle policy.
- D. Store the files in S3 then after a month, change the storage class of the bucket to S3-IA using lifecycle policy.

Answer: B

Explanation:

Initially, the files will be accessed frequently, and S3 is a durable and highly available storage solution for that. After a month has passed, the files won't be accessed frequently anymore, so it is a good idea to use lifecycle policies to move them to a storage class that would have a lower cost for storing them.



Since the files are easily reproducible and some of them are needed to be retrieved quickly based on a specific prefix filter (tdoj-finance), S3-One Zone IA would be a good choice for storing them. The other files that do not contain such prefix would then be moved to Glacier for low-cost archival. This setup would also be the most cost-effective for the client. Hence, the correct answer is: Store the files in S3 then after a month, change the storage class of the tdojo-finance prefix to One Zone-IA while the remaining go to Glacier using lifecycle policy.

## Lifecycle rule



1 Name and scope

2 Transitions

3 Expiration

4 Review

Enter a rule name

Tutorials Dojo S3 Lifecycle

Add filter to limit scope to prefix/tags

Type to add prefix/tag filter

[Cancel](#) [Next](#)

The option that says: Storing the files in S3 then after a month, changing the storage class of the bucket to S3-IA using lifecycle policy is incorrect. Although it is valid to move the files to S3-IA, this solution still costs more compared with using a combination of S3-One Zone IA and Glacier.

The option that says: Storing the files in S3 then after a month, changing the storage class of the bucket to Intelligent-Tiering using lifecycle policy is incorrect. While S3 Intelligent-Tiering can automatically move data between two access tiers (frequent access and infrequent access) when access patterns change, it is more suitable for scenarios where you don't know the access patterns of your data. It may take some time for S3 Intelligent-Tiering to analyze the access patterns before it moves the data to a cheaper storage class like S3-IA which means you may still end up paying more in the beginning. In addition, you already know the access patterns of the files which means you can directly change the storage class immediately and save cost right away.

The option that says: Storing the files in S3 then after a month, changing the storage class of the tdojofinance prefix to S3-IA while the remaining go to Glacier using lifecycle policy is incorrect. Even though S3-IA costs less than the S3 Standard storage class, it is still more expensive than S3-One Zone IA.

Remember that the files are easily reproducible so you can safely move the data to S3-One Zone IA and in case there is an outage, you can simply generate the missing data again.

References:

<https://aws.amazon.com/blogs/compute/amazon-s3-adds-prefix-and-suffix-filters-for-lambda-function-triggering>

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

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

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

## QUESTION 221

A Fortune 500 company which has numerous offices and customers around the globe has hired you as their Principal Architect. You have staff and customers that upload gigabytes to terabytes of data to a centralized S3 bucket from the regional data centers, across continents, all over the world on a regular basis. At the end of the financial year, there are thousands of data being uploaded to the central S3 bucket which is in ap-southeast-2 (Sydney) region and a lot of employees are starting to complain about the slow upload times. You were instructed by the CTO to resolve this issue as soon as possible to avoid any delays in processing their global end of financial year (EOFY) reports.

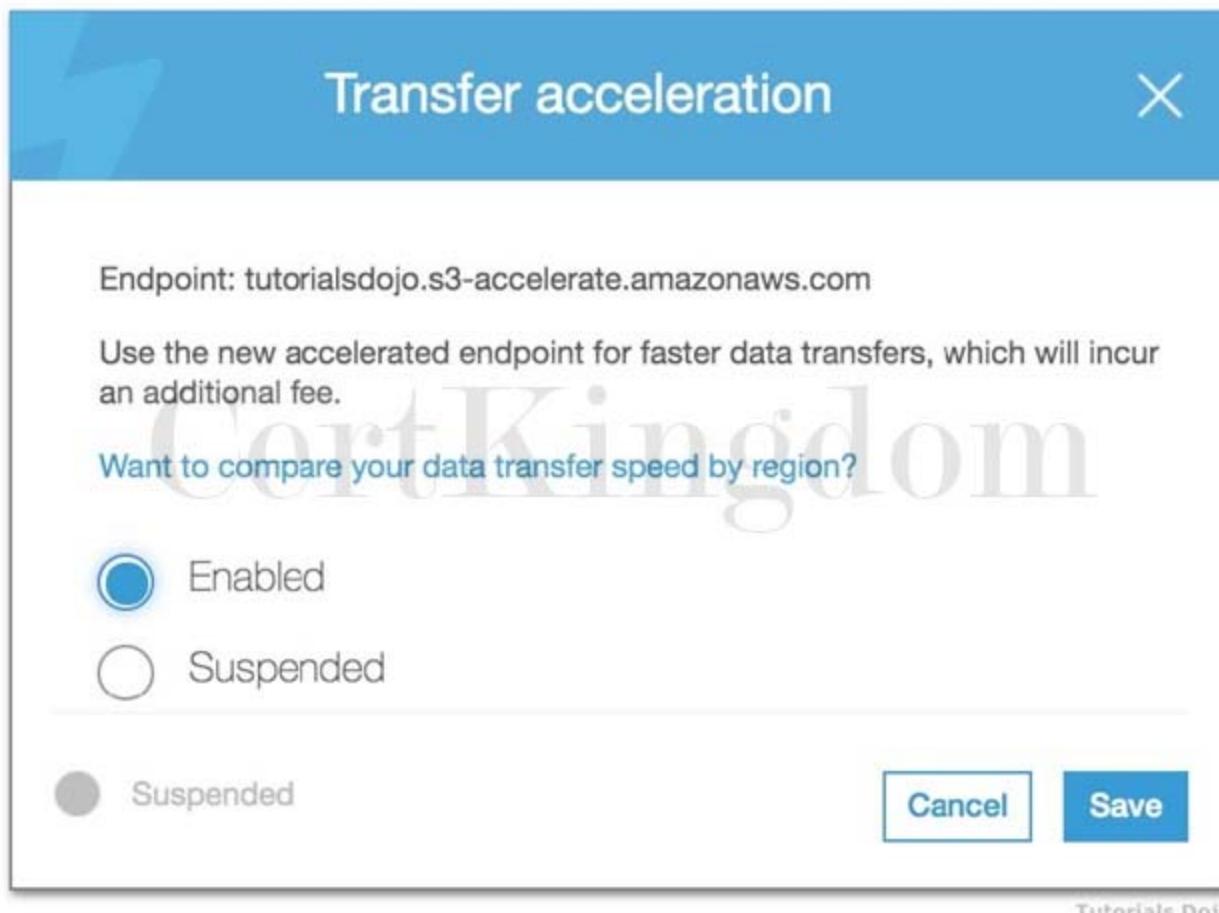
Which feature in Amazon S3 enables fast, easy, and secure transfer of your files over long distances between your client and your Amazon S3 bucket?

- A. AWS Global Accelerator
- B. Transfer Acceleration
- C. Cross-Region Replication
- D. Multipart Upload

Answer: B

Explanation:

Amazon S3 Transfer Acceleration enables fast, easy, and secure transfer of files over long distances between your client and your Amazon S3 bucket. Transfer Acceleration leverages Amazon CloudFront's globally distributed AWS Edge Locations. As data arrives at an AWS Edge Location, data is routed to your Amazon S3 bucket over an optimized network path.



Amazon S3 Transfer Acceleration can speed up content transfers to and from Amazon S3 by as much as 50-500% for long-distance transfer of larger objects. Customers who have either web or mobile applications with widespread users or applications hosted far away from their S3 bucket can experience long and variable upload and download speeds over the Internet. S3 Transfer Acceleration (S3TA) reduces the variability in Internet routing, congestion and speeds that can affect transfers, and logically shortens the distance to S3 for remote applications. S3TA improves transfer performance by routing traffic through Amazon CloudFront's globally distributed Edge Locations and over AWS backbone networks, and by using network protocol optimizations.

Hence, Transfer Acceleration is the correct answer. AWS Global Accelerator is incorrect because this service is primarily used to optimize the path from your users to your applications which improves the performance of your TCP and UDP traffic. Using Amazon S3 Transfer Acceleration is a more suitable service for this scenario.

Cross-Region Replication is incorrect because this simply enables you to automatically copy S3 objects from one bucket to another bucket that is placed in a different AWS Region or within the same Region.

Multipart Upload is incorrect because this feature simply allows you to upload a single object as a set of parts. You can upload these object parts independently and in any order. If transmission of any part fails, you can retransmit that part without affecting other parts. After all parts of your object are uploaded, Amazon S3 assembles these parts and creates the object. In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation.

References:

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

<https://aws.amazon.com/s3/transfer-acceleration/>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

---

## QUESTION 222

A financial company instructed you to automate the recurring tasks in your department such as patch management, infrastructure selection, and data synchronization to improve their current processes. You need to have a service which can coordinate multiple AWS services into serverless workflows.

Which of the following is the most cost-effective service to use in this scenario?

- A. AWS Step Functions
- B. AWS Batch
- C. AWS Lambda
- D. SWF

Answer: A

Explanation:

AWS Step Functions provides serverless orchestration for modern applications. Orchestration centrally manages a workflow by breaking it into multiple steps, adding flow logic, and tracking the inputs and outputs between the steps. As your applications execute, Step Functions maintains application state, tracking exactly which workflow step your application is in, and stores an event log of data that is passed between application components. That means that if networks fail or components hang, your application can pick up right where it left off.

Application development is faster and more intuitive with Step Functions, because you can define and manage the workflow of your application independently from its business logic. Making changes to one does not affect the other. You can easily update and modify workflows in one place, without having to struggle with managing, monitoring and maintaining multiple point-to-point integrations. Step Functions frees your functions and containers from excess code, so your applications are faster to write, more resilient, and easier to maintain.

SWF is incorrect because this is a fully-managed state tracker and task coordinator service. It does not provide serverless orchestration to multiple AWS resources.

AWS Lambda is incorrect because although Lambda is used for serverless computing, it does not provide a direct way to coordinate multiple AWS services into serverless workflows.

AWS Batch is incorrect because this is primarily used to efficiently run hundreds of thousands of batch computing jobs in AWS.

Reference:

<https://aws.amazon.com/step-functions/features/>

Check out this AWS Step Functions Cheat Sheet:

<https://tutorialsdojo.com/aws-step-functions/>

Amazon Simple Workflow (SWF) vs AWS Step Functions vs Amazon SQS:

<https://tutorialsdojo.com/amazon-simple-workflow-swf-vs-aws-step-functions-vs-amazon-sqs/>

Comparison of AWS Services Cheat Sheets:

<https://tutorialsdojo.com/comparison-of-aws-services/>

---

## QUESTION 223

A newly hired Solutions Architect is checking all of the security groups and network access control list rules of the company's AWS resources. For security purposes, the MS SQL connection via port 1433 of the database tier should be secured. Below is the security group configuration of their Microsoft SQL Server database:

The screenshot shows the 'Edit inbound rules' dialog box. It contains two rules:

- RDP:** Protocol TCP, Port Range 3389, Source Custom (125.84.117.80/32), Description RDP Connection.
- MS SQL:** Protocol TCP, Port Range 1433, Source Anywhere (0.0.0.0/0, ::/0), Description MS SQL Connection.

Below the rules, a note states: "Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created."

At the bottom right are 'Cancel' and 'Save' buttons, with 'Tutorialspoint' and 'Tutorialspoint Static' links below them.

The application tier hosted in an Auto Scaling group of EC2 instances is the only identified resource that needs to connect to the database. The Architect should ensure that the architecture complies with the best practice of granting least privilege. Which of the following changes should be made to the security group configuration?

- A. For the MS SQL rule, change the Source to the EC2 instance IDs of the underlying instances of the Auto Scaling group.
- B. For the MS SQL rule, change the Source to the static AnyCast IP address attached to the application tier.
- C. For the MS SQL rule, change the Source to the Network ACL ID attached to the application tier.
- D. For the MS SQL rule, change the Source to the security group ID attached to the application tier.

Answer: D

Explanation:

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC can be assigned to a different set of security groups.

If you launch an instance using the Amazon EC2 API or a command line tool and you don't specify a security group, the instance is automatically assigned to the default security group for the VPC. If you launch an instance using the Amazon EC2 console, you have an option to create a new security group for the instance.

Inbound			
Source	Protocol	Port Range	Description
0.0.0.0/0	TCP	80	Allow inbound HTTP access from all IPv4 addresses
::/0	TCP	80	Allow inbound HTTP access from all IPv6 addresses
0.0.0.0/0	TCP	443	Allow inbound HTTPS access from all IPv4 addresses
::/0	TCP	443	Allow inbound HTTPS access from all IPv6 addresses
Your network's public IPv4 address range	TCP	22	Allow inbound SSH access to Linux instances from IPv4 IP addresses in your network (over the internet gateway)
Your network's public IPv4 address range	TCP	3389	Allow inbound RDP access to Windows instances from IPv4 IP addresses in your network (over the internet gateway)

Outbound			
Destination	Protocol	Port Range	Description
The ID of the security group for your Microsoft SQL Server database servers	TCP	1433	Allow outbound Microsoft SQL Server access to instances in the specified security group
The ID of the security group for your MySQL database servers	TCP	3306	Allow outbound MySQL access to instances in the specified security group

For each security group, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic. This section describes the basic things that you need to know about security groups for your VPC and their rules.

Amazon security groups and network ACLs don't filter traffic to or from link-local addresses (169.254.0.0) or AWS reserved

IPv4 addresses (these are the first four IPv4 addresses of the subnet, including the Amazon DNS server address for the VPC). Similarly, flow logs do not capture IP traffic to or from these addresses.

In the scenario, the security group configuration allows any server (0.0.0.0/0) from anywhere to establish an MS SQL connection to the database via the 1433 port. The most suitable solution here is to change the Source field to the security group ID attached to the application tier.

Hence, the correct answer is the option that says: For the MS SQL rule, change the Source to the security group ID attached to the application tier.

The option that says: For the MS SQL rule, change the Source to the EC2 instance IDs of the underlying instances of the Auto Scaling group is incorrect because using the EC2 instance IDs of the underlying instances of the Auto Scaling group as the source can cause intermittent issues. New instances will be added and old instances will be removed from the Auto Scaling group over time, which means that you have to manually update the security group setting once again. A better solution is to use the security group ID of the Auto Scaling group of EC2 instances.

The option that says: For the MS SQL rule, change the Source to the static AnyCast IP address attached to the application tier is incorrect because a static AnyCast IP address is primarily used for AWS Global Accelerator and not for security group configurations.

The option that says: For the MS SQL rule, change the Source to the Network ACL ID attached to the application tier is incorrect because you have to use the security group ID instead of the Network ACL ID of the application tier. Take note that the Network ACL covers the entire subnet which means that other applications that use the same subnet will also be affected.

References:

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_SecurityGroups.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html)

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Security.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html)

---

## QUESTION 224

A tech company currently has an on-premises infrastructure. They are currently running low on storage and want to have the ability to extend their storage using the AWS cloud.

Which AWS service can help them achieve this requirement?

- A. Amazon Elastic Block Storage
- B. Amazon EC2
- C. Amazon SQS
- D. Amazon Storage Gateway

Answer: D

Explanation:

AWS Storage Gateway connects an on-premises software appliance with cloud-based storage to provide seamless integration with data security features between your on-premises IT environment and the AWS storage infrastructure. You can use the service to store data in the AWS Cloud for scalable and cost-effective storage that helps maintain data security. Amazon EC2 is incorrect since this is a compute service, not a storage service. Amazon Elastic Block Storage is incorrect since EBS is primarily used as a storage of your EC2 instances.

Amazon SQS is incorrect since this is a message queuing service, and does not extend your on-premises storage capacity.

Reference:

<http://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html>

AWS Storage Gateway Overview:

<https://youtu.be/pNb7xOBJjHE>

Check out this AWS Storage Gateway Cheat Sheet:

<https://tutorialsdojo.com/aws-storage-gateway/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

---

## QUESTION 225

A company launched a global news website that is deployed to AWS and is using MySQL RDS. The website has millions of viewers from all over the world which means that the website has read-heavy database workloads. All database transactions must be ACID compliant to ensure data integrity.

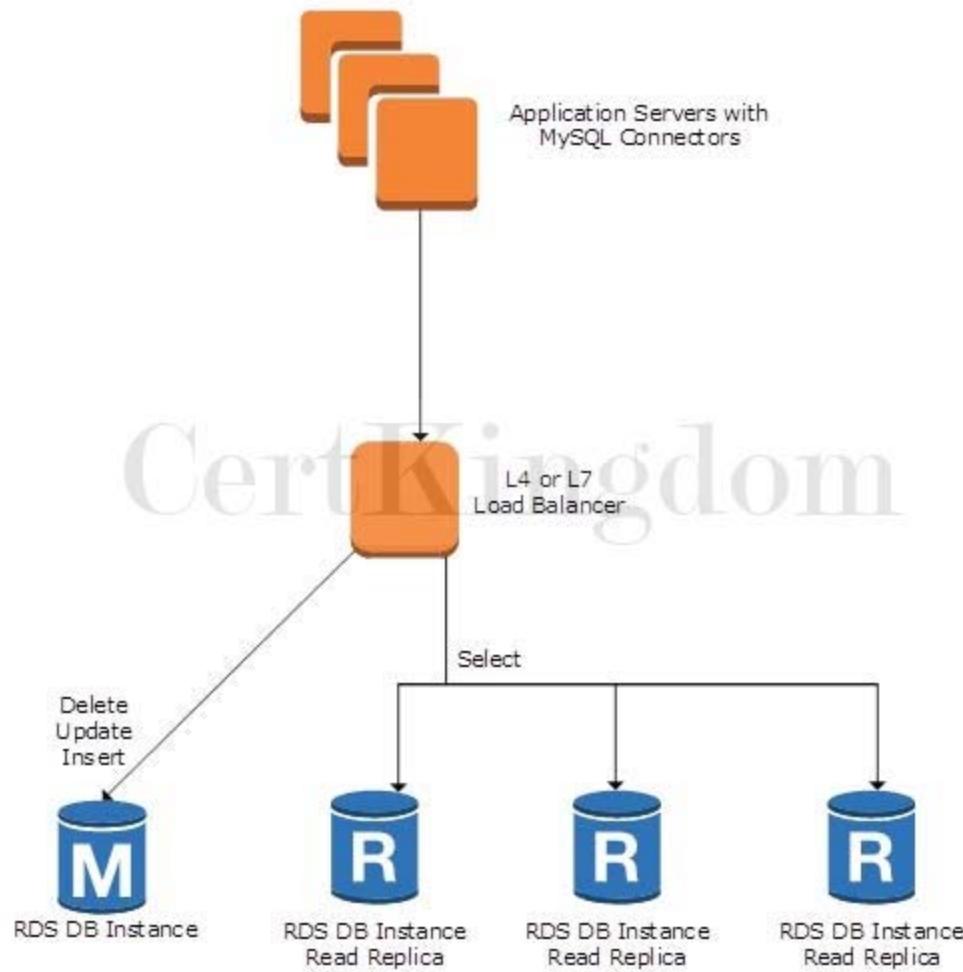
In this scenario, which of the following is the best option to use to increase the read throughput on the MySQL database?

- A. Enable Amazon RDS Standby Replicas
- B. Use SQS to queue up the requests
- C. Enable Amazon RDS Read Replicas
- D. Enable Multi-AZ deployments

Answer: C

Explanation:

Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This feature makes it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read replicas are available in Amazon RDS for MySQL, MariaDB, Oracle, and PostgreSQL as well as Amazon Aurora.



Enabling Multi-AZ deployments is incorrect because the Multi-AZ deployments feature is mainly used to achieve high availability and failover support for your database.

Enabling Amazon RDS Standby Replicas is incorrect because a Standby replica is used in Multi-AZ deployments and hence, it is not a solution to reduce read-heavy database workloads.

Using SQS to queue up the requests is incorrect. Although an SQS queue can effectively manage the requests, it won't be able to entirely improve the read-throughput of the database by itself.

References:

<https://aws.amazon.com/rds/details/read-replicas/>

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_ReadRepl.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html)

Amazon RDS Overview:

<https://www.youtube.com/watch?v=aZmpL18K1UU>

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

## QUESTION 226

A company is using an Auto Scaling group which is configured to launch new t2.micro EC2 instances when there is a significant load increase in the application. To cope with the demand, you now need to replace those instances with a larger t2.2xlarge instance type.

How would you implement this change?

- A. Create another Auto Scaling Group and attach the new instance type.
- B. Change the instance type of each EC2 instance manually.
- C. Just change the instance type to t2.2xlarge in the current launch configuration
- D. Create a new launch configuration with the new instance type and update the Auto Scaling Group.

Answer: D

Explanation:

You can only specify one launch configuration for an Auto Scaling group at a time, and you can't modify a launch configuration after you've created it. Therefore, if you want to change the launch configuration for an Auto Scaling group, you must create a launch configuration and then update your Auto Scaling group with the new launch configuration.

The screenshot shows the AWS Create Launch Configuration wizard. The top navigation bar includes 'Services', 'Resource Groups', 'Tutorials Dojo', 'N. Virginia', and 'Support'. Below the navigation is a progress bar with steps: 1. Choose AMI, 2. Choose Instance Type (which is highlighted in orange), 3. Configure details, 4. Add Storage, 5. Configure Security Group, and 6. Review. The main section is titled 'Create Launch Configuration' with a sub-instruction: 'Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.' Below this is a filter section with 'Filter by: All instance types' and 'Current generation'. A table lists various instance types:

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate
General purpose	t2.small	1	2	EBS only	-	Low to Moderate
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
General purpose	t2.large	2	8	EBS only	-	Low to Moderate

Hence, the correct answer is: Create a new launch configuration with the new instance type and update the Auto Scaling Group.

The option that says: Just change the instance type to t2.2xlarge in the current launch configuration is incorrect because you can't change your launch configuration once it is created. You have to create a new one instead.

The option that says: Create another Auto Scaling Group and attach the new instance type is incorrect because you can't directly attach or declare the new instance type to your Auto Scaling group. You have to create a new launch configuration first, with a new instance type, then attach it to your existing Auto Scaling group.

The option that says: Change the instance type of each EC2 instance manually is incorrect because you can't directly change the instance type of your EC2 instance. This should be done by creating a brand new launch configuration then attaching it to your existing Auto Scaling group.

References:

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

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-asg.html>

Check out this AWS Auto Scaling Cheat Sheet:

<https://tutorialsdojo.com/aws-auto-scaling/>

---

## QUESTION 227

A customer is transitioning their ActiveMQ messaging broker service onto the AWS cloud in which they require an alternative asynchronous service that supports NMS and MQTT messaging protocol. The customer does not have the time and resources needed to recreate their messaging service in the cloud.

The service has to be highly available and should require almost no management overhead.

Which of the following is the most suitable service to use to meet the above requirement?

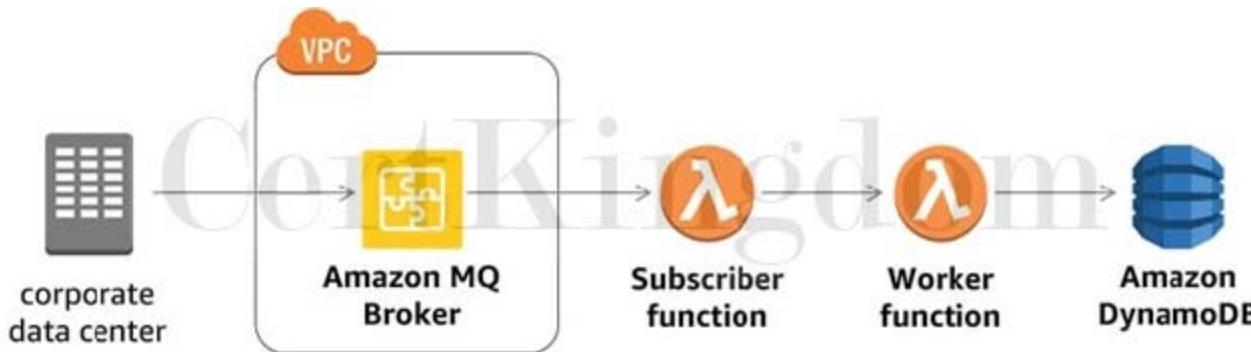
- A. Amazon SWF
- B. Amazon SNS
- C. Amazon MQ
- D. AWS Step Functions

Answer: C

Explanation:

Amazon MQ is a managed message broker service for Apache ActiveMQ that makes it easy to set up and operate message brokers in the cloud. Connecting your current applications to Amazon MQ is easy because it uses industry-standard APIs and protocols for messaging, including JMS, NMS, AMQP, STOMP, MQTT, and WebSocket. Using standards means that in most cases, there's no need to rewrite any messaging code when you migrate to AWS.

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.



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.

Hence, Amazon MQ is the correct answer.

Amazon SNS is incorrect because this is more suitable as a pub/sub messaging service instead of a message broker service. Amazon SQS is incorrect. Although this is a fully managed message queuing service, it does not support an extensive list of industry-standard messaging APIs and protocols, unlike Amazon MQ. Moreover, using Amazon SQS requires you to do additional changes in the messaging code of applications to make it compatible.

AWS Step Functions is incorrect because this is a serverless function orchestrator and not a messaging service, unlike Amazon MQ, Amazon SQS, and Amazon SNS.

References:

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

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

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

Check out this Amazon MQ Cheat Sheet:  
<https://tutorialsdojo.com/amazon-mq/>

## QUESTION 228

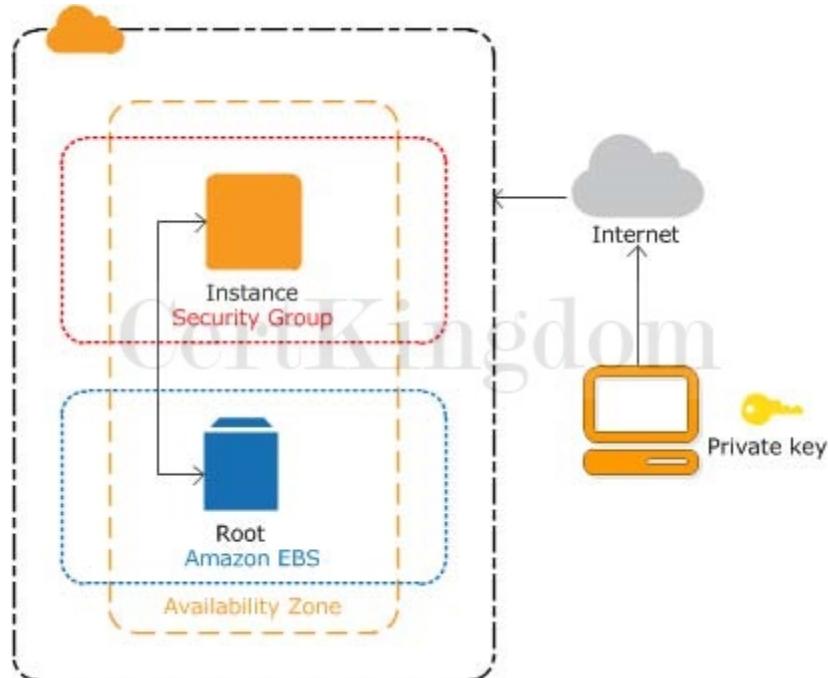
A technical lead of the Cloud Infrastructure team was consulted by a software developer regarding the required AWS resources of the web application that he is building. The developer knows that an Instance Store only provides ephemeral storage where the data is automatically deleted when the instance is terminated. To ensure that the data of the web application persists, the app should be launched in an EC2 instance that has a durable, block-level storage volume attached. The developer knows that they need to use an EBS volume, but they are not sure what type they need to use. In this scenario, which of the following is true about Amazon EBS volume types and their respective usage? (Select TWO.)

- A. Magnetic volumes provide the lowest cost per gigabyte of all EBS volume types and are ideal for workloads where data is accessed infrequently, and applications where the lowest storage cost is important.
- B. Spot volumes provide the lowest cost per gigabyte of all EBS volume types and are ideal for workloads where data is accessed infrequently, and applications where the lowest storage cost is important.
- C. Single root I/O virtualization (SR-IOV) volumes are suitable for a broad range of workloads, including small to medium-sized databases, development and test environments, and boot volumes.
- D. Provisioned IOPS volumes offer storage with consistent and low-latency performance, and are designed for I/O intensive applications such as large relational or NoSQL databases.
- E. General Purpose SSD (gp3) volumes with multi-attach enabled offer consistent and low-latency performance, and are designed for applications requiring multi-az resiliency.

Answer: A,D

Explanation:

Amazon EBS provides three volume types to best meet the needs of your workloads: General Purpose (SSD), Provisioned IOPS (SSD), and Magnetic.



General Purpose (SSD) is the new, SSD-backed, general purpose EBS volume type that is recommended as the default choice for customers. General Purpose (SSD) volumes are suitable for a broad range of workloads, including small to medium sized databases, development, and test environments, and boot volumes.

Provisioned IOPS (SSD) volumes offer storage with consistent and low-latency performance and are designed for I/O intensive applications such as large relational or NoSQL databases. Magnetic volumes provide the lowest cost per gigabyte of all EBS volume types.

Magnetic volumes are ideal for workloads where data are accessed infrequently, and applications where the lowest storage cost is important. Take note that this is a Previous Generation Volume. The latest low-cost magnetic storage types are Cold HDD (sc1) and Throughput Optimized HDD (st1) volumes.

Hence, the correct answers are:

- Provisioned IOPS volumes offer storage with consistent and low-latency performance, and are designed for I/O intensive applications such as large relational or NoSQL databases.
- Magnetic volumes provide the lowest cost per gigabyte of all EBS volume types and are ideal for workloads where data is accessed infrequently, and applications where the lowest storage cost is important.

The option that says: Spot volumes provide the lowest cost per gigabyte of all EBS volume types and are ideal for workloads where data is accessed infrequently, and applications where the lowest storage cost is important is incorrect because there is no EBS type called a "Spot volume" however, there is an Instance purchasing option for Spot Instances.

The option that says: General Purpose SSD (gp3) volumes with multi-attach enabled offer consistent and low-latency performance, and are designed for applications requiring multi-az resiliency is incorrect because the multi-attach feature can only be enabled on EBS Provisioned IOPS io2 or io1 volumes. In addition, multi-attach won't offer multi-az resiliency because this feature only allows an EBS volume to be attached on multiple instances within an availability zone.

The option that says: Single root I/O virtualization (SR-IOV) volumes are suitable for a broad range of workloads, including small to medium-sized databases, development and test environments, and boot volumes is incorrect because SR-IOV is related with Enhanced Networking on Linux and not in EBS.

References:

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

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

Check out this Amazon EBS Cheat Sheet:

<https://tutorialsdojo.com/amazon-ebs/>

---

## QUESTION 229

A real-time data analytics application is using AWS Lambda to process data and store results in JSON format to an S3 bucket. To speed up the existing workflow, you have to use a service where you can run sophisticated Big Data analytics on your data without moving them into a separate analytics system.

Which of the following group of services can you use to meet this requirement?

- A. S3 Select, Amazon Athena, Amazon Redshift Spectrum
- B. S3 Select, Amazon Neptune, DynamoDB DAX
- C. Amazon Glue, Glacier Select, Amazon Redshift
- D. Amazon X-Ray, Amazon Neptune, DynamoDB

Answer: A

Explanation:

Amazon S3 allows you to run sophisticated Big Data analytics on your data without moving the data into a separate analytics system. In AWS, there is a suite of tools that make analyzing and processing large amounts of data in the cloud faster, including ways to optimize and integrate existing workflows with Amazon S3:

### 1. S3 Select

Amazon S3 Select is designed to help analyze and process data within an object in Amazon S3 buckets, faster and cheaper. It works by providing the ability to retrieve a subset of data from an object in Amazon S3 using simple SQL expressions. Your applications no longer have to use compute resources to scan and filter the data from an object, potentially increasing query performance by up to 400%, and reducing query costs as much as 80%. You simply change your application to use SELECT instead of GET to take advantage of S3 Select.

### 2. Amazon Athena

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL expressions. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries you run. Athena is easy to use. Simply point to your data in Amazon S3, define the schema, and start querying using standard SQL expressions. Most results are delivered within seconds. With Athena, there's no need for complex ETL jobs to prepare your data for analysis. This makes it easy for anyone with SQL skills to quickly analyze large-scale datasets.

### 3. Amazon Redshift Spectrum

Amazon Redshift also includes Redshift Spectrum, allowing you to directly run SQL queries against exabytes of unstructured data in Amazon S3. No loading or transformation is required, and you can use open data formats, including Avro, CSV, Grok, ORC, Parquet, RCFFile, RegexSerDe, SequenceFile, TextFile, and TSV. Redshift Spectrum automatically scales query compute capacity based on the data being retrieved, so queries against Amazon S3 run fast, regardless of data

set size.

Reference:

[https://aws.amazon.com/s3/features/#Query\\_in\\_Place](https://aws.amazon.com/s3/features/#Query_in_Place)

Amazon Redshift Overview:

<https://youtu.be/jLERNzhHOg>

Check out these AWS Cheat Sheets:

<https://tutorialsdojo.com/amazon-s3/>

<https://tutorialsdojo.com/amazon-athena/>

<https://tutorialsdojo.com/amazon-redshift/>

---

### QUESTION 230

A company is building an internal application that processes loans, accruals, and interest rates for their clients. They require a storage service that is able to handle future increases in storage capacity of up to 16 TB and can provide the lowest-latency access to their data. The web application will be hosted in a single m5ad.24xlarge Reserved EC2 instance that will process and store data to the storage service.

Which of the following storage services would you recommend?

- A. EBS
- B. Storage Gateway
- C. S3
- D. EFS

Answer: A

Explanation:

Amazon Web Services (AWS) offers cloud storage services to support a wide range of storage workloads such as Amazon S3, EFS and EBS. Amazon EFS is a file storage service for use with Amazon EC2. Amazon EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently-accessible storage for up to thousands of Amazon EC2 instances. Amazon S3 is an object storage service. Amazon S3 makes data available through an Internet API that can be accessed anywhere. Amazon EBS is a block-level storage service for use with Amazon EC2. Amazon EBS can deliver performance for workloads that require the lowest-latency access to data from a single EC2 instance. You can also increase EBS storage for up to 16TB or add new volumes for additional storage.

In this scenario, the company is looking for a storage service which can provide the lowest-latency access to their data which will be fetched by a single m5ad.24xlarge Reserved EC2 instance. This type of workloads can be supported better by using either EFS or EBS but in this case, the latter is the most suitable storage service. As mentioned above, EBS provides the lowest-latency access to the data for your EC2 instance since the volume is directly attached to the instance. In addition, the scenario does not require concurrently-accessible storage since they only have one instance.

Hence, the correct answer is EBS.

Storage Need	Solution	AWS Services
Temporary storage	Consider using local instance store volumes for needs such as scratch disks, buffers, queues, and caches.	<a href="#">Amazon Local Instance Store</a>
Multi-instance storage	Amazon EBS volumes can only be attached to one EC2 instance at a time. If you need multiple EC2 instances accessing volume data at the same time, consider using Amazon EFS as a file system.	<a href="#">Amazon EFS</a>
Highly durable storage	If you need very highly durable storage, use S3 or Amazon EFS. Amazon S3 Standard storage is designed for 99.99999999 percent (11 nines) annual durability per object. You can even decide to take a snapshot of the EBS volumes. Such a snapshot then gets saved in Amazon S3, thus providing you the durability of Amazon S3. For more information on EBS durability, see the <a href="#">Durability and Availability</a> section. EFS is designed for high durability and high availability, with data stored in multiple Availability Zones within an AWS Region.	<a href="#">Amazon S3</a> <a href="#">Amazon EFS</a>
Static data or web content	If your data doesn't change that often, Amazon S3 might represent a more cost-effective and scalable solution for storing this fixed information. Also, web content served out of Amazon EBS requires a web server running on Amazon EC2; in contrast, you can deliver web content directly out of Amazon S3 or from multiple EC2 instances using Amazon EFS.	<a href="#">Amazon S3</a> <a href="#">Amazon EFS</a>

Storage Gateway is incorrect since this is primarily used to extend your on-premises storage to your AWS Cloud.

S3 is incorrect because although this is also highly available and highly scalable, it still does not provide the lowest-latency access to the data, unlike EBS. Remember that S3 does not reside within your VPC by default, which means the data will traverse the public Internet that may result to higher latency. You can set up a VPC Endpoint for S3 yet still, its latency is greater than that of EBS.

EFS is incorrect because the scenario does not require concurrently-accessible storage since the internal application is only hosted in one instance. Although EFS can provide low latency data access to the EC2 instance as compared with S3, the storage service that can provide the lowest latency access is still EBS.

References:

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

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

Check out this Amazon EBS Cheat Sheet:

<https://tutorialsdojo.com/amazon-ebs/>

## QUESTION 231

A Solutions Architect is designing a monitoring application which generates audit logs of all operational activities of the company's cloud infrastructure. Their IT Security and Compliance team mandates that the application retain the logs for 5 years before the data can be deleted.

How can the Architect meet the above requirement?

- A. Store the audit logs in an EBS volume and then take EBS snapshots every month.
- B. Store the audit logs in an EFS volume and use Network File System version 4 (NFSv4) file-locking mechanism.
- C. Store the audit logs in an Amazon S3 bucket and enable Multi-Factor Authentication Delete (MFA Delete) on the S3 bucket.
- D. Store the audit logs in a Glacier vault and use the Vault Lock feature.

Answer: D

## Explanation:

An Amazon S3 Glacier (Glacier) vault can have one resource-based vault access policy and one Vault Lock policy attached to it. A Vault Lock policy is a vault access policy that you can lock. Using a Vault Lock policy can help you enforce regulatory and compliance requirements. Amazon S3 Glacier provides a set of API operations for you to manage the Vault Lock policies.

## Vault Lock policy for BusinessCritical

The Vault Lock policy for the vault is shown below. [Click here](#) to learn about writing a Vault Lock policy.

Add a permission

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Deny",  
      "Principal": {  
        "AWS": ""  
      },  
      "Action": "glacier:DeleteArchive",  
      "Resource": "arn:aws:glacier:us-east-1:  
      /vaults/BusinessCritical",  
      "Condition": {  
        "NumericLessThanEquals": {  
          "glacier:ArchiveAgeInDays": "365"  
        }  
      }  
    }  
  ]  
}
```

[Cancel](#) [Initiate Vault Lock](#)

As an example of a Vault Lock policy, suppose that you are required to retain archives for one year before you can delete them. To implement this requirement, you can create a Vault Lock policy that denies users permissions to delete an archive until the archive has existed for one year. You can test this policy before locking it down. After you lock the policy, the policy becomes immutable. For more information about the locking process, see Amazon S3 Glacier Vault Lock. If you want to manage other user permissions that can be changed, you can use the vault access policy

Amazon S3 Glacier supports the following archive operations: Upload, Download, and Delete. Archives are immutable and cannot be modified. Hence, the correct answer is to store the audit logs in a Glacier vault and use the Vault Lock feature.

Storing the audit logs in an EBS volume and then taking EBS snapshots every month is incorrect because this is not a suitable and secure solution. Anyone who has access to the EBS Volume can simply delete and modify the audit logs. Snapshots can be deleted too.

Storing the audit logs in an Amazon S3 bucket and enabling Multi-Factor Authentication Delete (MFA Delete) on the S3 bucket is incorrect because this would still not meet the requirement. If someone has access to the S3 bucket and also has the proper MFA privileges then the audit logs can be edited.

Storing the audit logs in an EFS volume and using Network File System version 4 (NFSv4) file-locking mechanism is incorrect because the data integrity of the audit logs can still be compromised if it is stored in an EFS volume with Network File System version 4 (NFSv4) file-locking mechanism and hence, not suitable as storage for the files. Although it will provide some sort of security, the file lock can still be overridden and the audit logs might be edited by someone else.

### References:

<https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-lock.html>

<https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-lock-policy.html>

<https://aws.amazon.com/blogs/aws/glacier-vault-lock/>

Amazon S3 and S3 Glacier Overview:

<https://www.youtube.com/watch?v=1ymyeN2tki4>

Check out this Amazon S3 Glacier Cheat Sheet:

<https://tutorialsdojo.com/amazon-glacier/>

## QUESTION 232

A data analytics company, which uses machine learning to collect and analyze consumer data, is using Redshift cluster as their data warehouse. You are instructed to implement a disaster recovery plan for their systems to ensure business continuity even in the event of an AWS region outage.

Which of the following is the best approach to meet this requirement?

- A. Do nothing because Amazon Redshift is a highly available, fully-managed data warehouse which can withstand an outage of an entire AWS region.
- B. Enable Cross-Region Snapshots Copy in your Amazon Redshift Cluster.
- C. Create a scheduled job that will automatically take the snapshot of your Redshift Cluster and store it to an S3 bucket.
- Restore the snapshot in case of an AWS region outage.
- D. Use Automated snapshots of your Redshift Cluster.

Answer: B

Explanation:

You can configure Amazon Redshift to copy snapshots for a cluster to another region. To configure cross-region snapshot copy, you need to enable this copy feature for each cluster and configure where to copy snapshots and how long to keep copied automated snapshots in the destination region. When cross-region copy is enabled for a cluster, all new manual and automatic snapshots are copied to the specified region.

The screenshot shows the 'Table restore' tab of the Amazon Redshift console. At the top, there are buttons for 'Restore table' and 'Copy restore request'. Below is a table with columns: Table, Database, Schema, and Status. There are two entries:

Table	Database	Schema	Status
new_table	dev	public	PENDING
test_no_proxy	dev	public	SUCCEEDED

The option that says: Create a scheduled job that will automatically take the snapshot of your Redshift Cluster and store it to an S3 bucket. Restore the snapshot in case of an AWS region outage is incorrect because although this option is possible, this entails a lot of manual work and hence, not the best option.

You should configure cross-region snapshot copy instead. The option that says: Do nothing because Amazon Redshift is a highly available, fully-managed data warehouse which can withstand an outage of an entire AWS region is incorrect because although Amazon Redshift is a fully-managed data warehouse, you will still need to configure cross-region snapshot copy to ensure that your data is properly replicated to another region.

Using Automated snapshots of your Redshift Cluster is incorrect because using automated snapshots is not enough and will not be available in case the entire AWS region is down.

Reference:

<https://docs.aws.amazon.com/redshift/latest/mgmt/managing-snapshots-console.html>

Amazon Redshift Overview:

<https://youtu.be/jILERNzhHOg>

Check out this Amazon Redshift Cheat Sheet:

<https://tutorialsdojo.com/amazon-redshift/>

### QUESTION 233

A company launched an online platform that allows people to easily buy, sell, spend, and manage their cryptocurrency. To meet the strict IT audit requirements, each of the API calls on all of the AWS resources should be properly captured and recorded. You used CloudTrail in the VPC to help you in the compliance, operational auditing, and risk auditing of your AWS account. In this scenario, where does CloudTrail store all of the logs that it creates?

- A. Amazon S3
- B. A RDS instance
- C. DynamoDB
- D. Amazon Redshift

Answer: A

Explanation:

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 events in the CloudTrail console by going to Event history.



Event history allows you to view, search, and download the past 90 days of supported activity in your AWS account. In addition, you can create a CloudTrail trail to further archive, analyze, and respond to changes in your AWS resources. A trail is a configuration that enables the delivery of events to an Amazon S3 bucket that you specify. You can also deliver and analyze events in a trail with Amazon CloudWatch Logs and Amazon CloudWatch Events. You can create a trail with the CloudTrail console, the AWS CLI, or the CloudTrail API.

The rest of the answers are incorrect. DynamoDB and an RDS instance are for database; Amazon Redshift is used for data warehouse that scales horizontally and allows you to store terabytes and petabytes of data.

References:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/how-cloudtrail-works.html>

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

Check out this AWS CloudTrail Cheat Sheet:

<https://tutorialsdojo.com/aws-cloudtrail/>

## QUESTION 234

A company has a global news website hosted in a fleet of EC2 Instances. Lately, the load on the website has increased which resulted in slower response time for the site visitors. This issue impacts the revenue of the company as some readers tend to

leave the site if it does not load after 10 seconds.

Which of the below services in AWS can be used to solve this problem? (Select TWO.)

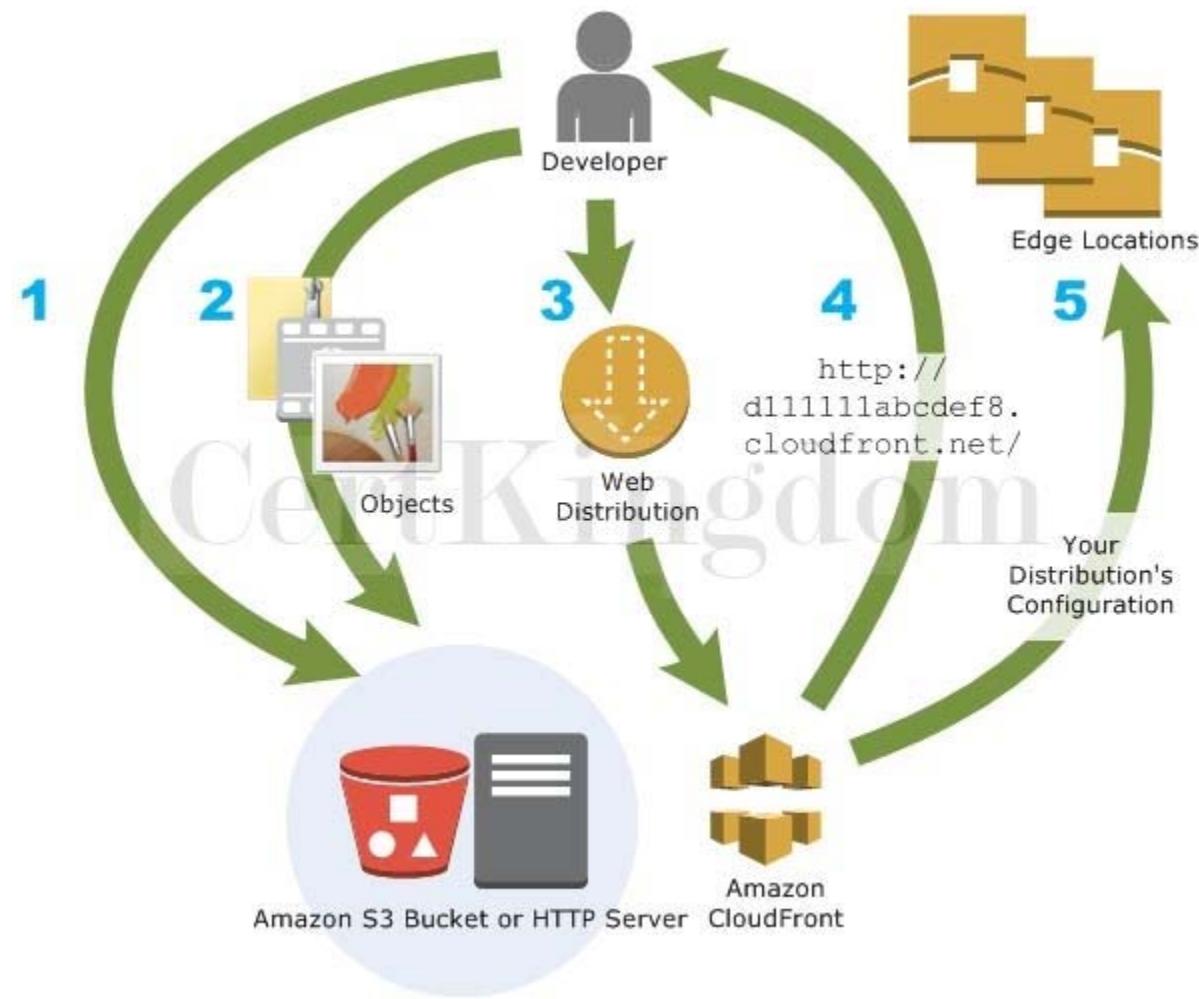
- A. Use Amazon ElastiCache for the website's in-memory data store or cache.
- B. For better read throughput, use AWS Storage Gateway to distribute the content across multiple regions.
- C. Use Amazon CloudFront with website as the custom origin.
- D. Deploy the website to all regions in different VPCs for faster processing.

Answer: A,C

Explanation:

The global news website has a problem with latency considering that there are a lot of readers of the site from all parts of the globe. In this scenario, you can use a content delivery network (CDN) which is a geographically distributed group of servers that work together to provide fast delivery of Internet content.

And since this is a news website, most of its data are read-only, which can be cached to improve the read throughput and avoid repetitive requests from the server.



In AWS, Amazon CloudFront is the global content delivery network (CDN) service that you can use and for web caching, Amazon ElastiCache is the suitable service.

Hence, the correct answers are:

- Use Amazon CloudFront with website as the custom origin.
- Use Amazon ElastiCache for the website's in-memory data store or cache.

The option that says: For better read throughput, use AWS Storage Gateway to distribute the content across multiple regions is incorrect as AWS Storage Gateway is used for storage.

Deploying the website to all regions in different VPCs for faster processing is incorrect as this would be costly and totally unnecessary considering that you can use Amazon CloudFront and ElastiCache to improve the performance of the website.

References:

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

<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

## QUESTION 235

A company plans to migrate a NoSQL database to an EC2 instance. The database is configured to replicate the data automatically to keep multiple copies of data for redundancy. The Solutions Architect needs to launch an instance that has a high IOPS and sequential read/write access.

Which of the following options fulfills the requirement if I/O throughput is the highest priority?

- A. Use Compute optimized instance with instance store volume.
- B. Use Storage optimized instances with instance store volume.
- C. Use Memory optimized instances with EBS volume.
- D. Use General purpose instances with EBS volume.

Answer: B

Explanation:

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications. Each instance type includes one or more instance sizes, allowing you to scale your resources to the requirements of your target workload.

<b>C: Compute Optimized Instances</b>	<b>Cost-effective high performance at a low price per compute ratio</b>
<b>D: Storage Optimized Instances</b>	High disk throughput
<b>G: Accelerated Computing Instances</b>	Graphics-intensive GPU instances
<b>H: Storage Optimized Instances</b>	HDD-based local storage for high disk throughput
<b>I: Storage Optimized Instances</b>	High storage instances, low latency, high random I/O performance, high sequential read throughput, and high IOPS
<b>M: General Purpose Instances</b>	Fixed performance
<b>P: Accelerated Computing Instances</b>	General purpose GPU instances
<b>F: Accelerated Computing Instances</b>	Reconfigurable FPGA instances
<b>R: Memory Optimized Instances</b>	Memory-intensive applications
<b>T: General Purpose Instances</b>	Burstable performance instances
<b>X: Memory Optimized Instances</b>	Large-scale, enterprise-class, in-memory applications, and high-performance databases

A storage optimized instance is designed for workloads that require high, sequential read and write access to very large data sets on local storage. They are optimized to deliver tens of thousands of lowlatency, random I/O operations per second (IOPS) to applications. Some instance types can drive more I/O throughput than what you can provision for a single EBS

volume. You can join multiple volumes together in a RAID 0 configuration to use the available bandwidth for these instances.

Based on the given scenario, the NoSQL database will be migrated to an EC2 instance. The suitable instance type for NoSQL database is I3 and I3en instances. Also, the primary data storage for I3 and I3en instances is non-volatile memory express (NVMe) SSD instance store volumes. Since the data is replicated automatically, there will be no problem using an instance store volume.

Hence, the correct answer is: Use Storage optimized instances with instance store volume.

The option that says: Use Compute optimized instances with instance store volume is incorrect because this type of instance is ideal for compute-bound applications that benefit from high-performance processors. It is not suitable for a NoSQL database.

The option that says: Use General purpose instances with EBS volume is incorrect because this instance only provides a balance of computing, memory, and networking resources. Take note that the requirement in the scenario is high sequential read and write access. Therefore, you must use a storage optimized instance.

The option that says: Use Memory optimized instances with EBS volume is incorrect. Although this type of instance is suitable for a NoSQL database, it is not designed for workloads that require high, sequential read and write access to very large data sets on local storage.

References:

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

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

Amazon EC2 Overview:

[https://www.youtube.com/watch?v=7VsGIHT\\_jQE](https://www.youtube.com/watch?v=7VsGIHT_jQE)

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

---

## QUESTION 236

A company recently launched an e-commerce application that is running in eu-east-2 region, which strictly requires six EC2 instances running at all times. In that region, there are 3 Availability Zones (AZ) that you can use - eu-east-2a, eu-east-2b, and eu-east-2c.

Which of the following deployments provide 100% fault tolerance if any single AZ in the region becomes unavailable? (Select TWO.)

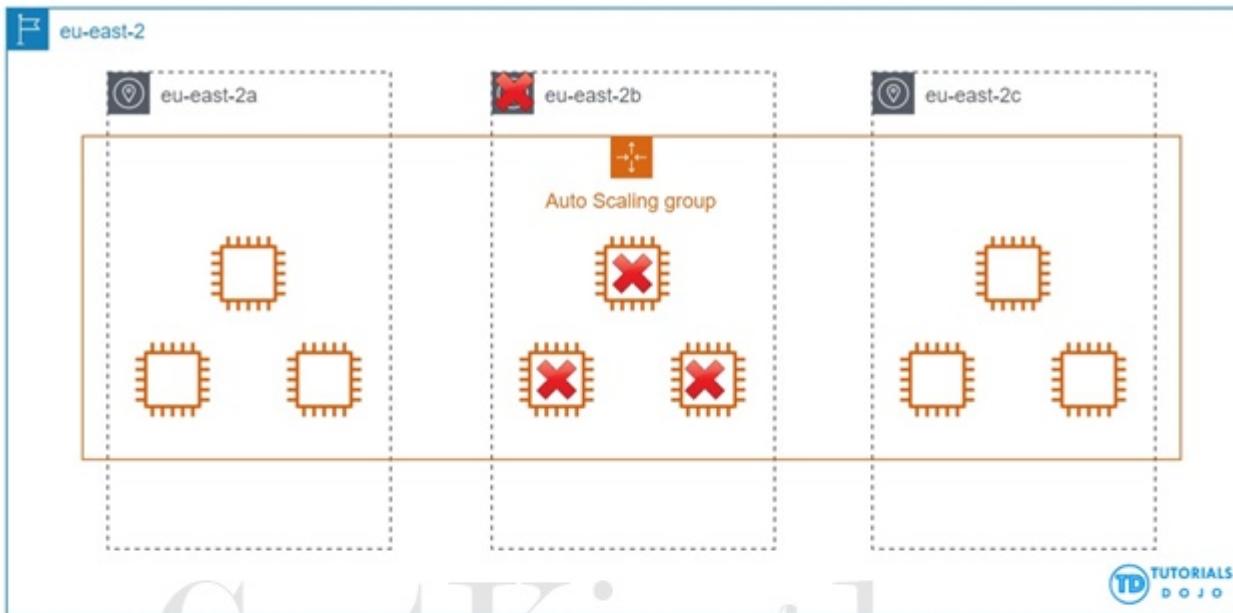
- A. eu-east-2a with four EC2 instances, eu-east-2b with two EC2 instances, and eu-east-2c with two EC2 instances
- B. eu-east-2a with six EC2 instances, eu-east-2b with six EC2 instances, and eu-east-2c with no EC2 instances
- C. eu-east-2a with two EC2 instances, eu-east-2b with four EC2 instances, and eu-east-2c with two EC2 instances
- D. eu-east-2a with three EC2 instances, eu-east-2b with three EC2 instances, and eu-east-2c with three EC2 instances
- E. eu-east-2a with two EC2 instances, eu-east-2b with two EC2 instances, and eu-east-2c with two EC2 instances

Answer: B,D

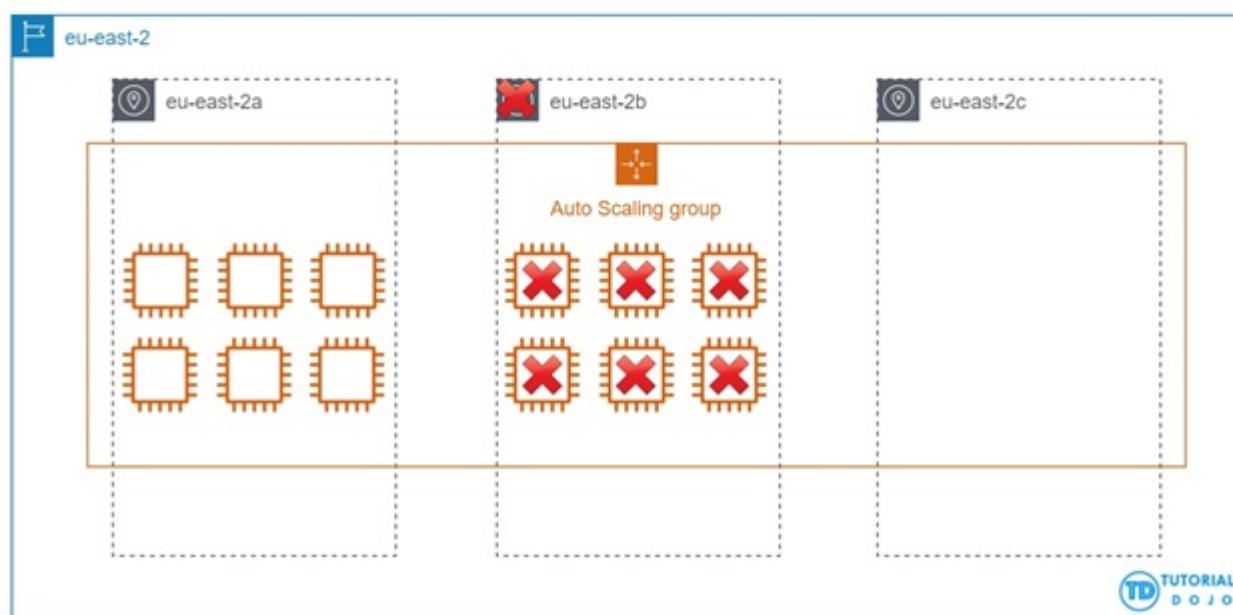
Explanation:

Fault Tolerance is the ability of a system to remain in operation even if some of the components used to build the system fail. In AWS, this means that in the event of server fault or system failures, the number of running EC2 instances should not fall below the minimum number of instances required by the system for it to work properly. So if the application requires a minimum of 6 instances, there should be at least 6 instances running in case there is an outage in one of the Availability Zones or if there are server issues.

## Case 1



## Case 2



In this scenario, you have to simulate a situation where one Availability Zone became unavailable for each option and check whether it still has 6 running instances.

Hence, the correct answers are: eu-east-2a with six EC2 instances, eu-east-2b with six EC2 instances, and eu-east-2c with no EC2 instances and eu-east-2a with three EC2 instances, eu-east-2b with three EC2 instances, and eu-east-2c with three EC2 instances because even if one of the availability zones were to go down, there would still be 6 active instances.

Reference:

[https://media.amazonwebservices.com/AWS\\_Building\\_Fault\\_Tolerant\\_Applications.pdf](https://media.amazonwebservices.com/AWS_Building_Fault_Tolerant_Applications.pdf)

## QUESTION 237

An automotive company is working on an autonomous vehicle development and deployment project using AWS. The solution requires High Performance Computing (HPC) in order to collect, store and manage massive amounts of data as well as to support deep learning frameworks. The Linux EC2 instances that will be used should have a lower latency and higher throughput than the TCP transport traditionally used in cloud-based HPC systems. It should also enhance the performance of inter-instance communication and must include an OS-bypass functionality to allow the HPC to communicate directly with the network interface hardware to provide low-latency, reliable transport functionality.

Which of the following is the MOST suitable solution that you should implement to achieve the above requirements?

- A. Attach a Private Virtual Interface (VIF) on each Amazon EC2 instance to accelerate High Performance Computing (HPC).
- B. Attach an Elastic Network Adapter (ENA) on each Amazon EC2 instance to accelerate High Performance Computing (HPC).
- C. Attach an Elastic Network Interface (ENI) on each Amazon EC2 instance to accelerate High Performance Computing (HPC).
- D. Attach an Elastic Fabric Adapter (EFA) on each Amazon EC2 instance to accelerate High Performance Computing (HPC).

Answer: D

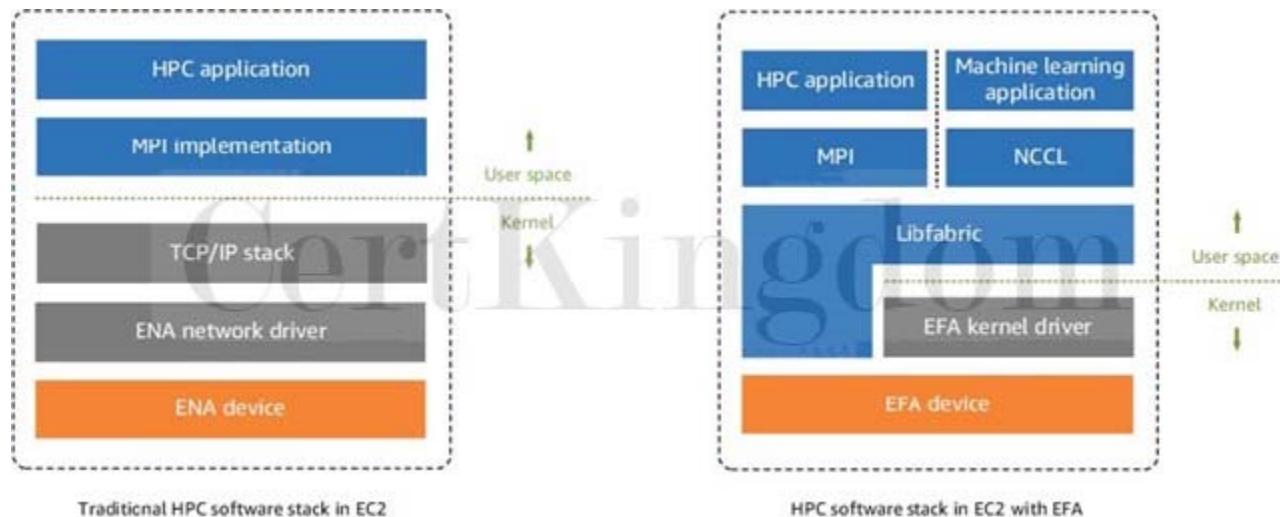
Explanation:

An Elastic Fabric Adapter (EFA) is a network device that you can attach to your Amazon EC2 instance to accelerate High Performance Computing (HPC) and machine learning applications. EFA enables you to achieve the application performance of an on-premises HPC cluster, with the scalability, flexibility, and elasticity provided by the AWS Cloud.

EFA provides lower and more consistent latency and higher throughput than the TCP transport traditionally used in cloud-based HPC systems. It enhances the performance of inter-instance communication that is critical for scaling HPC and machine learning applications. It is optimized to work

on the existing AWS network infrastructure and it can scale depending on application requirements.

EFA integrates with Libfabric 1.9.0 and it supports Open MPI 4.0.2 and Intel MPI 2019 Update 6 for HPC applications, and Nvidia Collective Communications Library (NCCL) for machine learning applications.



The OS-bypass capabilities of EFAs are not supported on Windows instances. If you attach an EFA to a Windows instance, the instance functions as an Elastic Network Adapter, without the added EFA capabilities.

Elastic Network Adapters (ENAs) provide traditional IP networking features that are required to support VPC networking. EFAs provide all of the same traditional IP networking features as ENAs, and they also support OS-bypass capabilities. OS-bypass enables HPC and machine learning applications to bypass the operating system kernel and to communicate directly with the EFA device.

Hence, the correct answer is to attach an Elastic Fabric Adapter (EFA) on each Amazon EC2 instance to accelerate High Performance Computing (HPC).

Attaching an Elastic Network Adapter (ENA) on each Amazon EC2 instance to accelerate High Performance Computing (HPC) is incorrect because Elastic Network Adapter (ENA) doesn't have OSbypass capabilities, unlike EFA.

Attaching an Elastic Network Interface (ENI) on each Amazon EC2 instance to accelerate High Performance Computing (HPC) is incorrect because an Elastic Network Interface (ENI) is simply a logical networking component in a VPC that represents a virtual network card. It doesn't have OS-bypass capabilities that allow the HPC to communicate directly with the network interface hardware to provide low-latency, reliable transport functionality.

Attaching a Private Virtual Interface (VIF) on each Amazon EC2 instance to accelerate High Performance Computing (HPC) is incorrect because Private Virtual Interface just allows you to connect to your VPC resources on your private IP address or endpoint.

References:

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

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking-ena>

Check out this Elastic Fabric Adapter (EFA) Cheat Sheet:

<https://tutorialsdojo.com/elastic-fabric-adapter-efa/>

---

## QUESTION 238

A company has hundreds of VPCs with multiple VPN connections to their data centers spanning 5 AWS Regions. As the number of its workloads grows, the company must be able to scale its networks across multiple accounts and VPCs to keep up. A Solutions Architect is tasked to interconnect all of the company's on-premises networks, VPNs, and VPCs into a single gateway, which includes support for inter-region peering across multiple AWS regions.

Which of the following is the BEST solution that the architect should set up to support the required interconnectivity?

- A. Enable inter-region VPC peering that allows peering relationships to be established between multiple VPCs across different AWS regions. Set up a networking configuration that ensures that the traffic will always stay on the global AWS backbone and never traverse the public Internet.
- B. Set up an AWS VPN CloudHub for inter-region VPC access and a Direct Connect gateway for the VPN connections to the on-premises data centers. Create a virtual private gateway in each VPC, then create a private virtual interface for each AWS Direct Connect connection to the Direct Connect gateway.
- C. Set up an AWS Direct Connect Gateway to achieve inter-region VPC access to all of the AWS resources and on-premises data centers. Set up a link aggregation group (LAG) to aggregate multiple connections at a single AWS Direct Connect endpoint in order to treat them as a single, managed connection. Launch a virtual private gateway in each VPC and then create a public virtual interface for each AWS Direct Connect connection to the Direct Connect Gateway.
- D. Set up an AWS Transit Gateway in each region to interconnect all networks within it. Then, route traffic between the transit gateways through a peering connection.

Answer: D

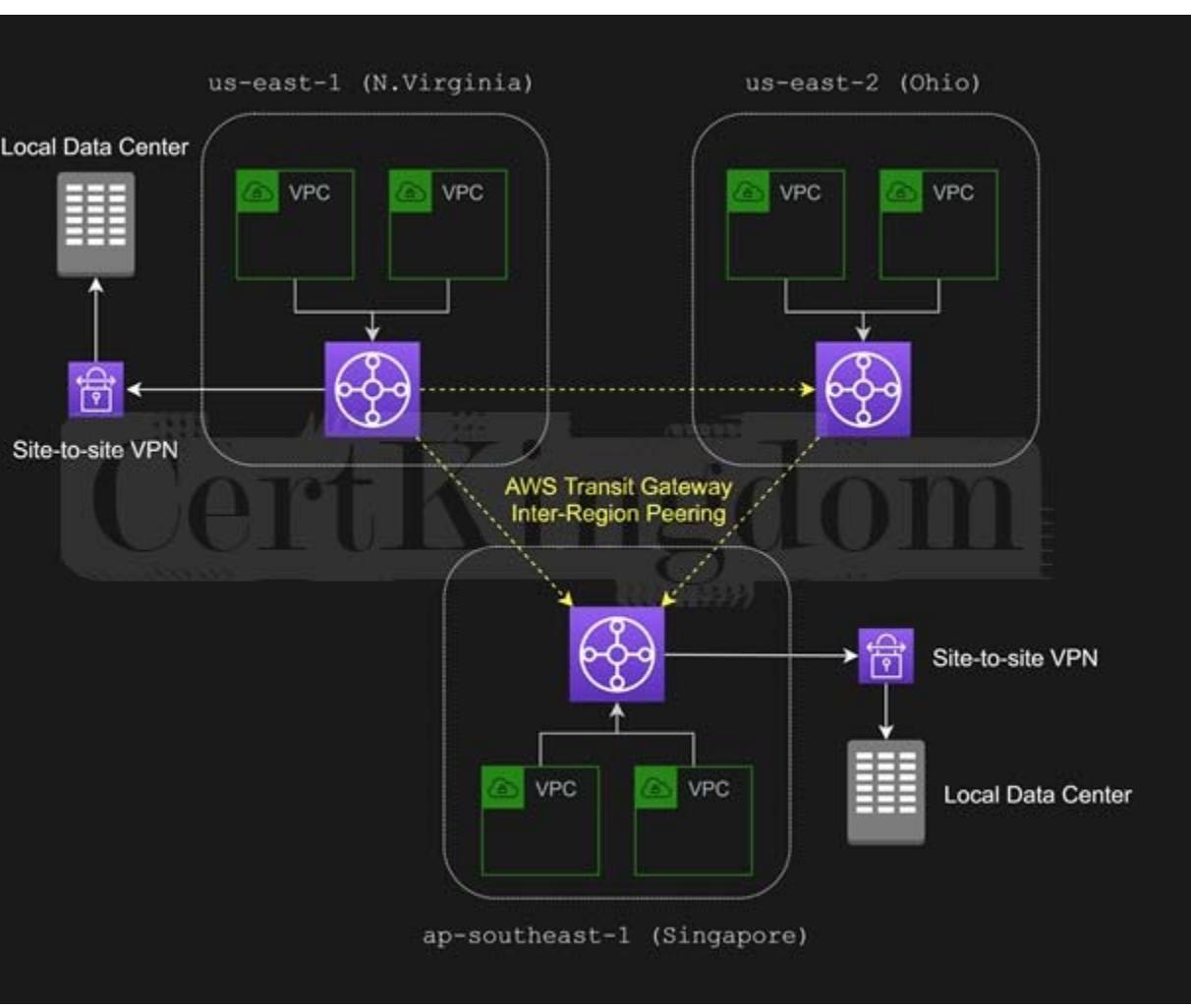
### Explanation:

AWS Transit Gateway is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. As you grow the number of workloads running on AWS, you need to be able to scale your networks across multiple accounts and Amazon VPCs to keep up with the growth.

Today, you can connect pairs of Amazon VPCs using peering. However, managing point-to-point connectivity across many Amazon VPCs without the ability to centrally manage the connectivity policies can be operationally costly and cumbersome. For on-premises connectivity, you need to attach your AWS VPN to each individual Amazon VPC. This solution can be time-consuming to build and hard to manage when the number of VPCs grows into the hundreds.

With AWS Transit Gateway, you only have to create and manage a single connection from the central gateway to each Amazon VPC, on-premises data center, or remote office across your network. Transit Gateway acts as a hub that controls how traffic is routed among all the connected networks which act like spokes. This hub and spoke model significantly simplifies management and reduces operational costs because each network only has to connect to the Transit Gateway and not to every other network.

Any new VPC is simply connected to the Transit Gateway and is then automatically available to every other network that is connected to the Transit Gateway. This ease of connectivity makes it easy to scale your network as you grow.



It acts as a Regional virtual router for traffic flowing between your virtual private clouds (VPC) and VPNconnections. A transit gateway scales elastically based on the volume of network traffic. Routing through a transit gateway operates at layer 3, where the packets are sent to a specific next-hop attachment,based on their destination IP addresses.

A transit gateway attachment is both a source and a destination of packets. You can attach the following resources to your transit gateway:

- One or more VPCs
- One or more VPN connections
- One or more AWS Direct Connect gateways
- One or more transit gateway peering connections

If you attach a transit gateway peering connection, the transit gateway must be in a different Region.

Hence, the correct answer is: Set up an AWS Transit Gateway in each region to interconnect all networks within it. Then, route traffic between the transit gateways through a peering connection.

The option that says: Set up an AWS Direct Connect Gateway to achieve inter-region VPC access to all of the AWS resources and on-premises data centers. Set up a link aggregation group (LAG) to aggregate multiple connections at a single AWS Direct Connect endpoint in order to treat them as a single, managed connection. Launch a virtual private gateway in each VPC and then create a public virtual interface for each AWS Direct Connect connection to the Direct Connect Gateway is incorrect.

You can only create a private virtual interface to a Direct Connect gateway and not a public virtual interface. Using a link aggregation group (LAG) is also irrelevant in this scenario because it is just a logical interface that uses the Link Aggregation Control Protocol (LACP) to aggregate multiple connections at a single AWS Direct Connect endpoint, allowing you to treat them as a single, managed connection.

The option that says: Enable inter-region VPC peering which allows peering relationships to be established between VPCs across different AWS regions. This will ensure that the traffic will always stay on the global AWS backbone and will never traverse the public Internet is incorrect. This would require a lot of manual set up and management overhead to successfully build a functional, error-free inter-region VPC network compared with just using a Transit Gateway. Although the Inter-Region VPC Peering provides a cost-effective way to share resources between regions or replicate data for geographic redundancy, its connections are not dedicated and highly available. Moreover, it doesn't support the company's on-premises data centers in multiple AWS Regions.

The option that says: Set up an AWS VPN CloudHub for inter-region VPC access and a Direct Connect gateway for the

VPN connections to the on-premises data centers. Create a virtual private gateway in each VPC, then create a private virtual interface for each AWS Direct Connect connection to the Direct Connect gateway is incorrect. This option doesn't meet the requirement of interconnecting all of the company's on-premises networks, VPNs, and VPCs into a single gateway, which includes support for inter-region peering across multiple AWS regions. As its name implies, the AWS VPN CloudHub is only for VPNs and not for VPCs. It is also not capable of managing hundreds of VPCs with multiple VPN connections to their data centers that span multiple AWS Regions.

#### References:

<https://aws.amazon.com/transit-gateway/>

<https://docs.aws.amazon.com/vpc/latest/tgw/how-transit-gateways-work.html>

<https://aws.amazon.com/blogs/networking-and-content-delivery/building-a-global-network-using-aws-transit-gateway-inter-region-peering/>

Check out this AWS Transit Gateway Cheat Sheet:

<https://tutorialsdojo.com/aws-transit-gateway/>

### QUESTION 239

A company has a distributed application in AWS that periodically processes large volumes of data across multiple instances. The Solutions Architect designed the application to recover gracefully from any instance failures. He is then required to launch the application in the most cost-effective way.

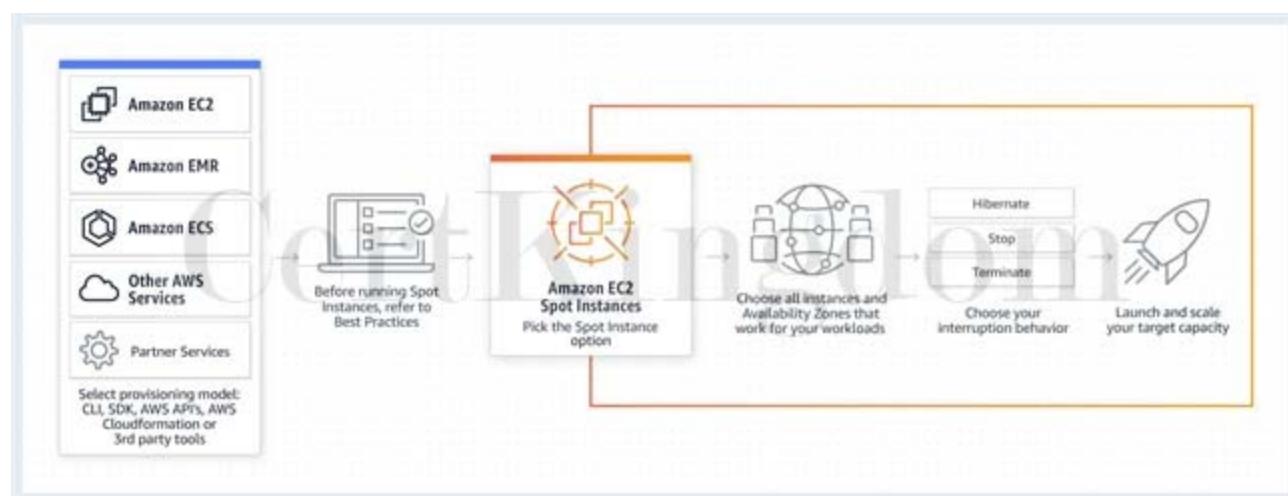
Which type of EC2 instance will meet this requirement?

- A. Dedicated instances
- B. On-Demand instances
- C. Spot Instances
- D. Reserved instances

Answer: C

#### Explanation:

You require an EC2 instance that is the most cost-effective among other types. In addition, the application it will host is designed to gracefully recover in case of instance failures.



In terms of cost-effectiveness, Spot and Reserved instances are the top options. And since the application can gracefully recover from instance failures, the Spot instance is the best option for this case as it is the cheapest type of EC2 instance. Remember that when you use Spot Instances, there will be interruptions. Amazon EC2 can interrupt your Spot Instance when the Spot price exceeds your maximum price, when the demand for Spot Instances rises, or when the supply of Spot Instances decreases.

Hence, the correct answer is: Spot Instances.

Reserved instances is incorrect. Although you can also use reserved instances to save costs, it entails a commitment of 1-year or 3-year terms of usage. Since your processes only run periodically, you won't be able to maximize the discounted price of using reserved instances.

Dedicated instances and On-Demand instances are also incorrect because Dedicated and on-demand instances are not a cost-effective solution to use for your application.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/how-spot-instances-work.html>

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

Here is an in-depth look at Spot Instances:

<https://youtu.be/PKvss-RgSjI>

## QUESTION 240

A company needs to integrate the Lightweight Directory Access Protocol (LDAP) directory service from the on-premises data center to the AWS VPC using IAM. The identity store which is currently being used is not compatible with SAML. Which of the following provides the most valid approach to implement the integration?

- A. Use IAM roles to rotate the IAM credentials whenever LDAP credentials are updated.
- B. Develop an on-premises custom identity broker application and use STS to issue short-lived AWS credentials.
- C. Use an IAM policy that references the LDAP identifiers and AWS credentials.
- D. Use AWS Single Sign-On (SSO) service to enable single sign-on between AWS and your LDAP.

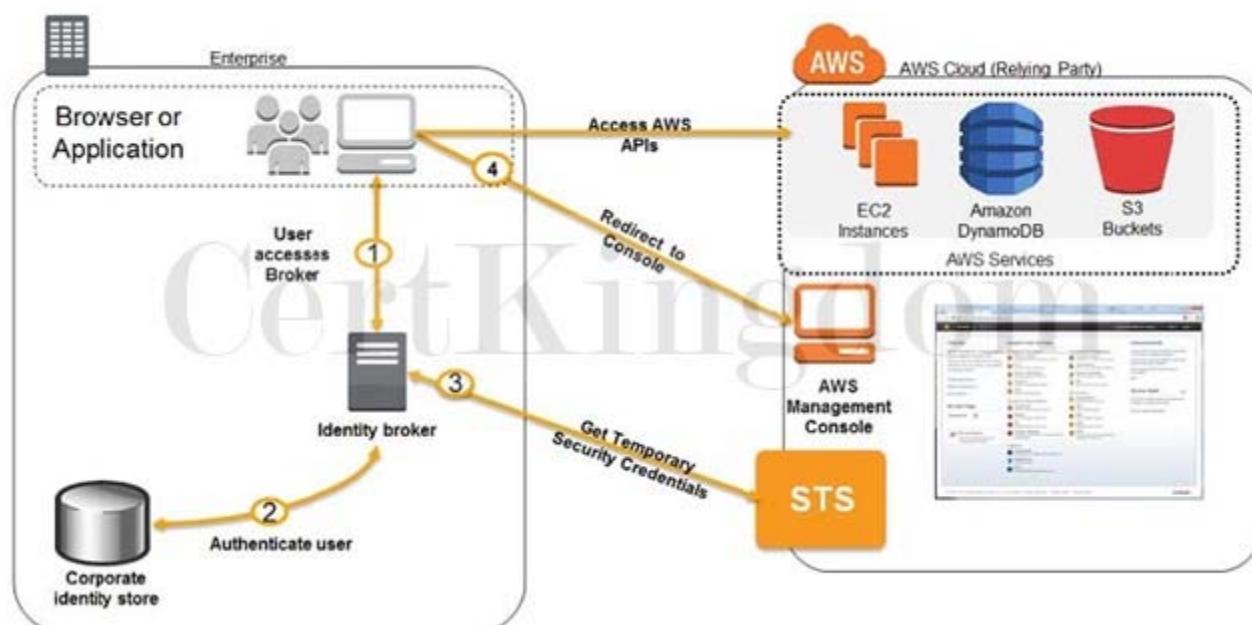
Answer: B

Explanation:

If your identity store is not compatible with SAML 2.0 then you can build a custom identity broker application to perform a similar function. The broker application authenticates users, requests temporary credentials for users from AWS, and then provides them to the user to access AWS resources.

The application verifies that employees are signed into the existing corporate network's identity and authentication system, which might use LDAP, Active Directory, or another system. The identity broker application then obtains temporary security credentials for the employees.

To get temporary security credentials, the identity broker application calls either AssumeRole or GetFederationToken to obtain temporary security credentials, depending on how you want to manage the policies for users and when the temporary credentials should expire. The call returns temporary security credentials consisting of an AWS access key ID, a secret access key, and a session token. The identity broker application makes these temporary security credentials available to the internal company application. The app can then use the temporary credentials to make calls to AWS directly. The app caches the credentials until they expire, and then requests a new set of temporary credentials.



Using an IAM policy that references the LDAP identifiers and AWS credentials is incorrect because using an IAM policy is not enough to integrate your LDAP service to IAM. You need to use SAML, STS, or a custom identity broker.

Using AWS Single Sign-On (SSO) service to enable single sign-on between AWS and your LDAP is incorrect because the scenario did not require SSO and in addition, the identity store that you are using is not SAML-

compatible.

Using IAM roles to rotate the IAM credentials whenever LDAP credentials are updated is incorrect because manually rotating the IAM credentials is not an optimal solution to integrate your on-premises and VPC network. You need to use SAML, STS, or a custom identity broker.

References:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_common-scenarios\\_federated-users.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html)

<https://aws.amazon.com/blogs/aws/aws-identity-and-access-management-now-with-identity-federation/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

---

## QUESTION 241

A Solutions Architect is working for a large global media company with multiple office locations all around the world. The Architect is instructed to build a system to distribute training videos to all employees.

Using CloudFront, what method would be used to serve content that is stored in S3, but not publicly accessible from S3 directly?

- A. Create an S3 bucket policy that lists the CloudFront distribution ID as the principal and the target bucket as the Amazon Resource Name (ARN).
- B. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
- C. Create a web ACL in AWS WAF to block any public S3 access and attach it to the Amazon CloudFront distribution.
- D. Create an Identity and Access Management (IAM) user for CloudFront and grant access to the objects in your S3 bucket to that IAM user.

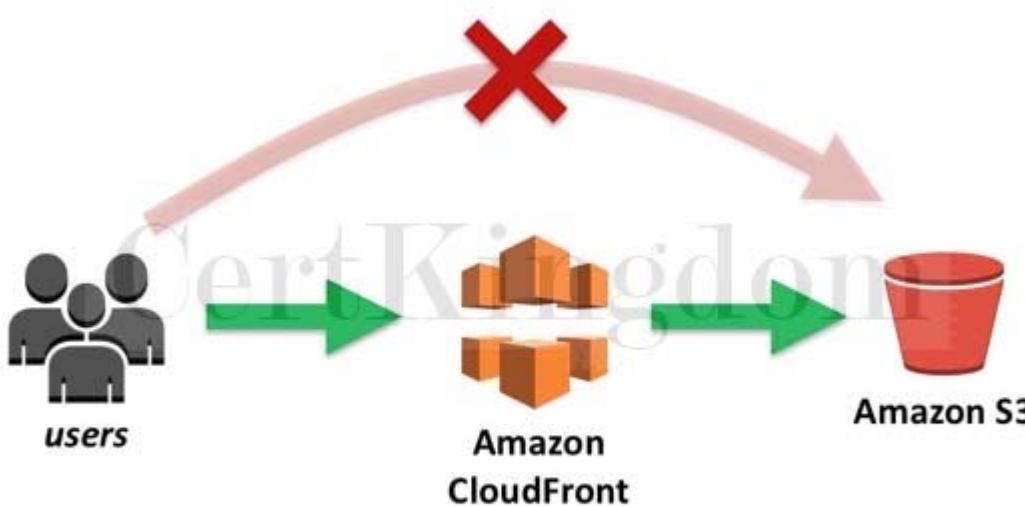
Answer: B

Explanation:

When you create or update a distribution in CloudFront, you can add an origin access identity (OAI) and automatically update the bucket policy to give the origin access identity permission to access your bucket. Alternatively, you can choose to manually change the bucket policy or change ACLs, which control permissions on individual objects in your bucket.

You can update the Amazon S3 bucket policy using either the AWS Management Console or the Amazon S3 API:

- Grant the CloudFront origin access identity the applicable permissions on the bucket.



- Deny access to anyone that you don't want to have access using Amazon S3 URLs.

Hence, the correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.

The option that says: Create an Identity and Access Management (IAM) user for CloudFront and grant access to the objects in your S3 bucket to that IAM user is incorrect because you cannot directly create an IAM User for a specific Amazon

CloudFront distribution. You have to use an origin access identity (OAI) instead.  
The option that says: Create an S3 bucket policy that lists the CloudFront distribution ID as the principal and the target bucket as the Amazon Resource Name (ARN) is incorrect because setting up an Amazon S3 bucket policy won't suffice. You have to first create an OAI in CloudFront and use that OAI as an authorized user in your Amazon S3 bucket.  
The option that says: Create a web ACL in AWS WAF to block any public S3 access and attach it to the Amazon CloudFront distribution is incorrect because AWS WAF is primarily used to protect your applications from common web vulnerabilities and not for ensuring exclusive access to CloudFront.

Reference:

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

Check out this Amazon CloudFront Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudfront/>

S3 Pre-signed URLs vs CloudFront Signed URLs vs Origin Access Identity (OAI)

<https://tutorialsdojo.com/s3-pre-signed-urls-vs-cloudfront-signed-urls-vs-origin-access-identity-oai/>

Comparison of AWS Services Cheat Sheets:

<https://tutorialsdojo.com/comparison-of-aws-services/>

---

## QUESTION 242

There is a new compliance rule in your company that audits every Windows and Linux EC2 instances each month to view any performance issues. They have more than a hundred EC2 instances running in production, and each must have a logging function that collects various system details regarding that instance. The SysOps team will periodically review these logs and analyze their contents using AWS Analytics tools, and the result will need to be retained in an S3 bucket.

In this scenario, what is the most efficient way to collect and analyze logs from the instances with minimal effort?

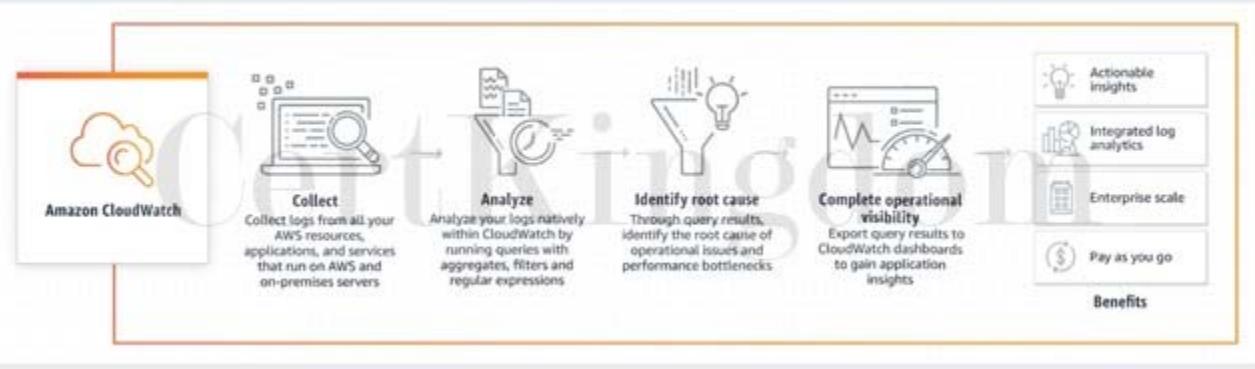
- A. Install AWS SDK in each instance and create a custom daemon script that would collect and push data to CloudWatch Logs periodically. Enable CloudWatch detailed monitoring and use CloudWatch Logs Insights to analyze the log data of all instances.
- B. Install the unified CloudWatch Logs agent in each instance which will automatically collect and push data to CloudWatch Logs. Analyze the log data with CloudWatch Logs Insights.
- C. Install AWS Inspector Agent in each instance which will collect and push data to CloudWatch Logs periodically. Set up a CloudWatch dashboard to properly analyze the log data of all instances.
- D. Install the AWS Systems Manager Agent (SSM Agent) in each instance which will automatically collect and push data to CloudWatch Logs. Analyze the log data with CloudWatch Logs Insights.

Answer: B

Explanation:

To collect logs from your Amazon EC2 instances and on-premises servers into CloudWatch Logs, AWS offers both a new unified CloudWatch agent, and an older CloudWatch Logs agent. It is recommended to use the unified CloudWatch agent which has the following advantages:

- You can collect both logs and advanced metrics with the installation and configuration of just one agent.
- The unified agent enables the collection of logs from servers running Windows Server.
- If you are using the agent to collect CloudWatch metrics, the unified agent also enables the collection of additional system metrics, for in-guest visibility.
- The unified agent provides better performance.



CloudWatch Logs Insights enables you to interactively search and analyze your log data in Amazon CloudWatch Logs. You can perform queries to help you quickly and effectively respond to operational issues. If an issue occurs, you can use CloudWatch Logs Insights to identify potential causes and validate deployed fixes.

CloudWatch Logs Insights includes a purpose-built query language with a few simple but powerful commands. CloudWatch Logs Insights provides sample queries, command descriptions, query autocomplete, and log field discovery to help you get started quickly. Sample queries are included for several types of AWS service logs.

The option that says: Install AWS SDK in each instance and create a custom daemon script that would collect and push data to CloudWatch Logs periodically. Enable CloudWatch detailed monitoring and use CloudWatch Logs Insights to analyze the log data of all instances is incorrect. Although this is a valid solution, this entails a lot of effort to implement as you have to allocate time to install the AWS SDK to each instance and develop a custom monitoring solution. Remember that the question is specifically looking for a solution that can be implemented with minimal effort. In addition, it is unnecessary and not cost-efficient to enable detailed monitoring in CloudWatch in order to meet the requirements of this scenario since this can be done using CloudWatch Logs.

The option that says: Install the AWS Systems Manager Agent (SSM Agent) in each instance which will automatically collect and push data to CloudWatch Logs. Analyze the log data with CloudWatch Logs

Insights is incorrect. Although this is also a valid solution, it is more efficient to use CloudWatch agent than an SSM agent. Manually connecting to an instance to view log files and troubleshoot an issue with SSM Agent is time-consuming hence, for more efficient instance monitoring, you can use the CloudWatch Agent instead to send the log data to Amazon CloudWatch Logs.

The option that says: Install AWS Inspector Agent in each instance which will collect and push data to CloudWatch Logs periodically. Set up a CloudWatch dashboard to properly analyze the log data of all instances is incorrect because AWS Inspector is simply a security assessments service which only helps you in checking for unintended network accessibility of your EC2 instances and for vulnerabilities on those EC2 instances. Furthermore, setting up an Amazon CloudWatch dashboard is not suitable since it's primarily used for scenarios where you have to monitor your resources in a single view, even those resources that are spread across different AWS Regions. It is better to use CloudWatch Logs Insights instead since it enables you to interactively search and analyze your log data.

#### References:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html>

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

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AnalyzingLogData.html>

#### Amazon CloudWatch Overview:

<https://www.youtube.com/watch?v=q0DmxfyGkeU>

Check out this Amazon CloudWatch Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudwatch/>

CloudWatch Agent vs SSM Agent vs Custom Daemon Scripts:

<https://tutorialsdojo.com/cloudwatch-agent-vs-ssm-agent-vs-custom-daemon-scripts/>

## QUESTION 243

A startup plans to develop a multiplayer game that uses UDP as the protocol for communication between clients and game servers. The data of the users will be stored in a key-value store. As the Solutions Architect, you need to implement a solution that will distribute the traffic across a number of servers.

Which of the following could help you achieve this requirement?

- A. Distribute the traffic using Application Load Balancer and store the data in Amazon DynamoDB.
- B. Distribute the traffic using Application Load Balancer and store the data in Amazon RDS.

- C. Distribute the traffic using Network Load Balancer and store the data in Amazon Aurora.  
 D. Distribute the traffic using Network Load Balancer and store the data in Amazon DynamoDB.

Answer: D

Explanation:

A Network Load Balancer functions at the fourth layer of the Open Systems Interconnection (OSI) model. It can handle millions of requests per second. After the load balancer receives a connection request, it selects a target from the target group for the default rule. For UDP traffic, the load balancer selects a target using a flow hash algorithm based on the protocol, source IP address, source port, destination IP address, and destination port. A UDP flow has the same source and destination, so it is consistently routed to a single target throughout its lifetime. Different UDP flows have different source IP addresses and ports, so they can be routed to different targets.

Feature	APPLICATION LOAD BALANCER	NETWORK LOAD BALANCER	CLASSIC LOAD BALANCER
Protocols	HTTP, HTTPS	TCP, UDP, TLS	TCP, SSL/TLS, HTTP, HTTPS
Platforms	VPC	VPC	EC2-Classic, VPC
Health checks	✓	✓	✓
CloudWatch metrics	✓	✓	✓
Logging	✓	✓	✓
Zonal fail-over	✓	✓	✓
Connection draining (deregistration delay)	✓		✓
Load Balancing to multiple ports on the same instance	✓	✓	
IP addresses as targets	✓	✓ (TCP, TLS)	
Load balancer deletion protection	✓	✓	
Configurable idle connection timeout	✓		✓
Cross-zone load balancing	✓	✓	✓
Sticky sessions	✓	✓	✓
Static IP		✓	
Elastic IP address		✓	
Preserve Source IP address		✓	
Resource-based IAM Permissions	✓	✓	✓
Tag-based IAM permissions	✓	✓	
Slow start	✓		
WebSockets	✓	✓	
PrivateLink Support		✓ (TCP, TLS)	
Source IP address CIDR-based routing	✓		

Tutorials Dojo

In this scenario, a startup plans to create a multiplayer game that uses UDP as the protocol for communications. Since UDP is a Layer 4 traffic, we can limit the option that uses Network Load Balancer. The data of the users will be stored in a key-value store. This means that we should select Amazon DynamoDB since it supports both document and key-value store models.

Hence, the correct answer is: Distribute the traffic using Network Load Balancer and store the data in Amazon DynamoDB. The option that says: Distribute the traffic using Application Load Balancer and store the data in Amazon DynamoDB is incorrect because UDP is not supported in Application Load Balancer. Remember that UDP is a Layer 4 traffic. Therefore, you should use a Network Load Balancer.

The option that says: Distribute the traffic using Network Load Balancer and store the data in Amazon Aurora is incorrect because Amazon Aurora is a relational database service. Instead of Aurora, you should use Amazon DynamoDB.

The option that says: Distribute the traffic using Application Load Balancer and store the data in Amazon RDS is incorrect because Application Load Balancer only supports application traffic (Layer 7). Also, Amazon RDS is not suitable as a key-value store. You should use DynamoDB since it supports both document and key-value store models.

#### References:

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

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html>

Check out this AWS Elastic Load Balancing Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

---

### QUESTION 244

A web application is hosted in an Auto Scaling group of EC2 instances deployed across multiple Availability Zones behind an Application Load Balancer. You need to implement an SSL solution for your system to improve its security which is why you requested an SSL/TLS certificate from a third-party certificate authority (CA).

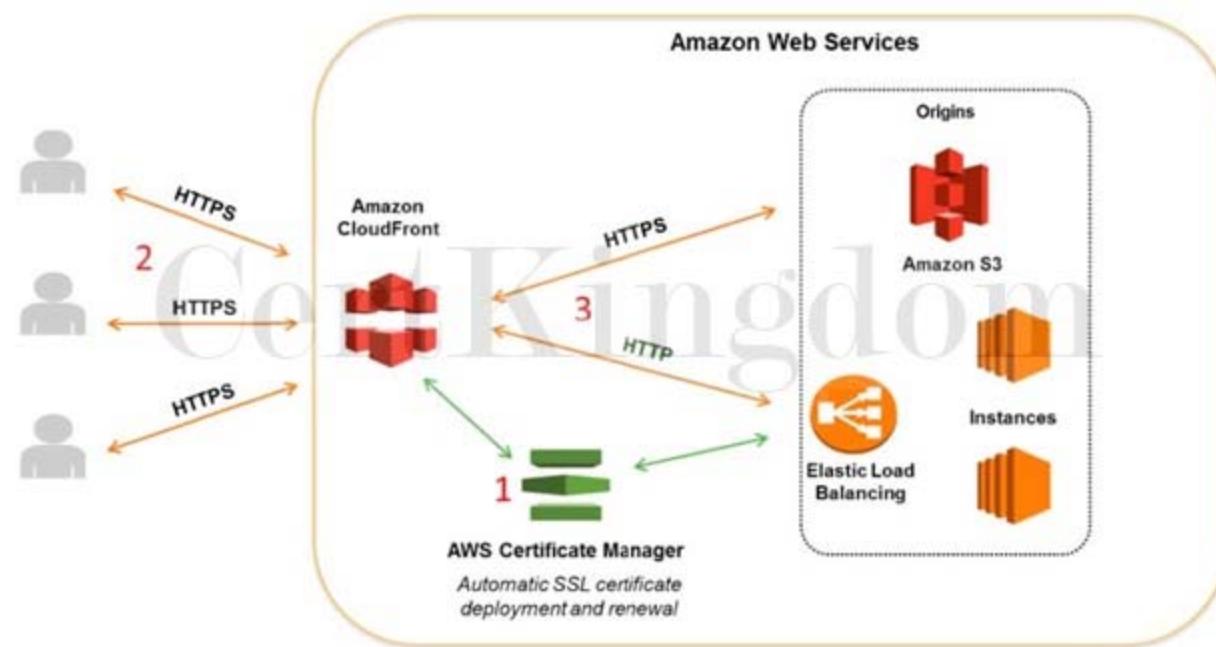
Where can you safely import the SSL/TLS certificate of your application? (Select TWO.)

- A. AWS Certificate Manager
- B. CloudFront
- C. A private S3 bucket with versioning enabled
- D. IAM certificate store
- E. An S3 bucket configured with server-side encryption with customer-provided encryption keys (SSEC)

Answer: A,D

#### Explanation:

If you got your certificate from a third-party CA, import the certificate into ACM or upload it to the IAM certificate store. Hence, AWS Certificate Manager and IAM certificate store are the correct answers.



ACM lets you import third-party certificates from the ACM console, as well as programmatically. If ACM is not available in

your region, use AWS CLI to upload your third-party certificate to the IAM certificate store. A private S3 bucket with versioning enabled and an S3 bucket configured with server-side encryption with customer-provided encryption keys (SSE-C) are both incorrect as S3 is not a suitable service to store the SSL certificate. CloudFront is incorrect. Although you can upload certificates to CloudFront, it doesn't mean that you can import SSL certificates on it. You would not be able to export the certificate that you have loaded in CloudFront nor assign them to your EC2 or ELB instances as it would be tied to a single CloudFront distribution.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-procedures.html#cnames-and-https-uploading-certificates>

Check out this Amazon CloudFront Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudfront/>

AWS Security Services Overview - Secrets Manager, ACM, Macie:

<https://www.youtube.com/watch?v=ogVamzF2Dzk>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

---

## QUESTION 245

A company has a web-based order processing system that is currently using a standard queue in Amazon SQS. The IT Manager noticed that there are a lot of cases where an order was processed twice. This issue has caused a lot of trouble in processing and made the customers very unhappy. The manager has asked you to ensure that this issue will not recur. What can you do to prevent this from happening again in the future? (Select TWO.)

- A. Use an Amazon SQS FIFO Queue instead.
- B. Change the message size in SQS.
- C. Replace Amazon SQS and instead, use Amazon Simple Workflow service.
- D. Alter the visibility timeout of SQS.
- E. Alter the retention period in Amazon SQS.

Answer: A,C

Explanation:

Amazon SQS FIFO (First-In-First-Out) Queues have all the capabilities of the standard queue with additional capabilities designed to enhance messaging between applications when the order of operations and events is critical, or where duplicates can't be tolerated, for example:

- Ensure that user-entered commands are executed in the right order.
- Display the correct product price by sending price modifications in the right order.
- Prevent a student from enrolling in a course before registering for an account.

## Standard Queue

## FIFO Queue



### Unlimited Throughput

Supports a nearly unlimited number of transactions per second (TPS) per API action.

### At-Least-Once Delivery

A message is delivered at least once.  
Occasionally more than one copy of a message is delivered.

### Best-Effort Ordering

Occasionally, messages might be delivered in an order different from which they were sent.

### High Throughput

By default, FIFO queues support up to 3,000 messages per second (TPS), per API action through batching

### Exactly-Once Processing

A message is delivered once and remains available until a consumer processes and deletes it.  
Duplicates are not introduced into the queue.

### First-In-First-Out Delivery

The order in which messages are sent and received is strictly preserved.

Tutorials Dojo

Amazon SWF provides useful guarantees around task assignments. It ensures that a task is never duplicated and is assigned only once. Thus, even though you may have multiple workers for a particular activity type (or a number of instances of a decider), Amazon SWF will give a specific task to only one worker (or one decider instance). Additionally, Amazon SWF keeps at most one decision task outstanding at a time for a workflow execution. Thus, you can run multiple decider instances without worrying about two instances operating on the same execution simultaneously. These facilities enable you to coordinate your workflow without worrying about duplicate, lost, or conflicting tasks.

The main issue in this scenario is that the order management system produces duplicate orders at times.

Since the company is using SQS, there is a possibility that a message can have a duplicate in case an EC2 instance failed to delete the already processed message. To prevent this issue from happening, you have to use Amazon Simple Workflow service instead of SQS.

Therefore, the correct answers are:

- Replace Amazon SQS and instead, use Amazon Simple Workflow service.
- Use an Amazon SQS FIFO Queue instead.

Altering the retention period in Amazon SQS is incorrect because the retention period simply specifies if the Amazon SQS should delete the messages that have been in a queue for a certain period of time.

Altering the visibility timeout of SQS is incorrect because for standard queues, the visibility timeout isn't a guarantee against receiving a message twice. To avoid duplicate SQS messages, it is better to design your applications to be idempotent (they should not be affected adversely when processing the same message more than once).

Changing the message size in SQS is incorrect because this is not related at all in this scenario.

References:

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

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

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

Check out this Amazon SWF Cheat Sheet:

<https://tutorialsdojo.com/amazon-simple-workflow-amazon-swf/>

## QUESTION 246

A company plans to reduce the amount of data that Amazon S3 transfers to the servers in order to lower the operating costs as well as lower the latency of retrieving the data. To accomplish this, you need to use simple structured query language (SQL) statements to filter the contents of Amazon S3 objects and retrieve just the subset of data that you need. Which of the following services will help you accomplish this requirement?

- A. S3 Select
- B. AWS Step Functions
- C. Redshift Spectrum
- D. RDS

Answer: A

Explanation:

With Amazon S3 Select, you can use simple structured query language (SQL) statements to filter the contents of Amazon S3 objects and retrieve just the subset of data that you need. By using Amazon S3Select to filter this data, you can reduce the amount of data that Amazon S3 transfers, which reduces the cost and latency to retrieve this data.

### SQL expression

S3 Select pricing is based on the size of the input, the output, and the data transferred.  
Each query will cost 0.002 USD per GB scanned, plus 0.0007 USD per GB returned.



The screenshot shows the AWS Lambda SQL editor interface. At the top, there are three tabs: "SQL editor" (disabled), "Sample SQL expressions" (selected), and "Learn more". Below the tabs, a code editor displays the following SQL query:

```
1 Select * from s3object s where s."Country (Name)" like '%United States%'
```

At the bottom right of the editor are two buttons: "Copy" and "Run SQL".

### Result

Location	City	State/Region	Country	Latitude	Longitude
OCH	A L Mangham Jr. Regional	United States	United States	31.6	-94.65
AYE	AAF Heliport	United States	United States	19.833333	-72.5
ARA	Acadiana Regional	United States	United States	80.133333	32.583333
MFV	Accomack County	United States	United States	13.633333	39.133333
ADK	Adak Island Ns	United States	United States	51.878056	-176.646111
TT	Adams Field Airport	United States	United States	34.729444	-92.224444

Amazon S3 Select works on objects stored in CSV, JSON, or Apache Parquet format. It also works with objects that are compressed with GZIP or BZIP2 (for CSV and JSON objects only), and server-side encrypted objects. You can specify the format of the results as either CSV or JSON, and you can determine how the records in the result are delimited.

RDS is incorrect. Although RDS is an SQL database where you can perform SQL operations, it is still not valid because you want to apply SQL transactions on S3 itself, and not on the database, which RDScan do.

Redshift Spectrum is incorrect. Although Amazon Redshift Spectrum provides a similar in-query functionality like S3 Select, this service is more suitable for querying your data from the Redshift external tables hosted in S3. The Redshift queries are run on your cluster resources against local disk. Redshift Spectrum queries run using per-query scale-out resources against data in S3 which can entail additional costs compared with S3 Select.

AWS Step Functions is incorrect because this only lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/selecting-content-from-objects.html>

<https://docs.aws.amazon.com/redshift/latest/dg/c-using-spectrum.html>

Check out these AWS Cheat Sheets:

<https://tutorialsdojo.com/amazon-s3/>

<https://tutorialsdojo.com/amazon-athena/>

<https://tutorialsdojo.com/amazon-redshift/>

---

## QUESTION 247

A new company policy requires IAM users to change their passwords' minimum length to 12 characters.

After a random inspection, you found out that there are still employees who do not follow the policy.

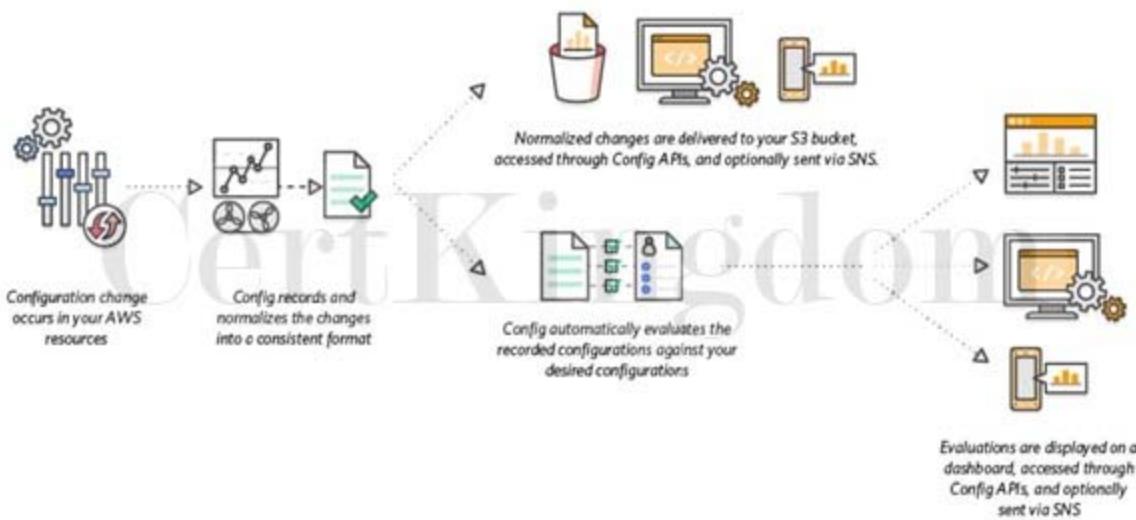
How can you automatically check and evaluate whether the current password policy for an account complies with the company password policy?

- A. Configure AWS Config to trigger an evaluation that will check the compliance for a user's password periodically.
- B. Create a rule in the Amazon CloudWatch event. Build an event pattern to match events on IAM. Set the event name to ChangePassword' in the event pattern. Configure SNS to send notifications to you whenever a user has made changes to his password.
- C. Create a Scheduled Lambda Function that will run a custom script to check compliance against changes made to the passwords periodically.
- D. Create a CloudTrail trail. Filter the result by setting the attribute to Event Name' and lookup value to ChangePassword' . This easily gives you the list of users who have made changes to their passwords.

Answer: A

Explanation:

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.



In the scenario given, we can utilize AWS Config to check for compliance on the password policy by configuring the Config rule to check the IAM\_PASSWORD\_POLICY on an account. Additionally, because Config integrates with AWS Organizations, we can improve the set up to aggregate compliance information across accounts to a central dashboard. Hence, the correct answer is: Configure AWS Config to trigger an evaluation that will check the compliance for a user's password periodically.

Create a CloudTrail trail. Filter the result by setting the attribute to Event Name' and lookup value to ChangePassword'. This easily gives you the list of users who have made changes to their passwords is incorrect because this setup will just give you the name of the users who have made changes to their respective passwords. It will not give you the ability to check whether their passwords have met the required minimum length.

Create a Scheduled Lambda function that will run a custom script to check compliance against changes made to the passwords periodically is a valid solution but still incorrect. AWS Config is already integrated with AWS Lambda. You don't have to create and manage your own Lambda function. You just have to define a Config rule where you will check compliance, and Lambda will process the evaluation.

Moreover, you can't directly create a scheduled function by using Lambda itself. You have to create a rule in AWS CloudWatch Events to run the Lambda functions on the schedule that you define.

Create a rule in the Amazon CloudWatch event. Build an event pattern to match events on IAM. Set the event name to ChangePassword' in the event pattern. Configure SNS to send notifications to you whenever a user has made changes to his password is incorrect because this setup will just alert you whenever a user changes his password. Sure, you'll have information about who made changes, but that is not enough to check whether it complies with the required minimum password length. This can be easily done in AWS Config.

#### References:

<https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html>

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

Check out this AWS Config Cheat Sheet:

<https://tutorialsdojo.com/aws-config/>

---

## QUESTION 248

A startup launched a new FTP server using an On-Demand EC2 instance in a newly created VPC with default settings. The server should not be accessible publicly but only through the IP address 175.45.11./326.100 and nowhere else. Which of the following is the most suitable way to implement this requirement?

- A. Create a new Network ACL inbound rule in the subnet of the EC2 instance with the following details:
- B. Protocol: TCP
- C. Port Range: 20 - 21
- D. Source: 175.45.11./326.100/0
- E. Allow/Deny: ALLOW
- F. Create a new inbound rule in the security group of the EC2 instance with the following details:
- G. Protocol: TCP
- H. Port Range: 20 - 21

I. Source: 175.45.11./326.100

J. Create a new Network ACL inbound rule in the subnet of the EC2 instance with the following details:

K. Protocol: UDP

L. Port Range: 20 - 21

M. Source: 175.45.11./326.100/0

N. Allow/Deny: ALLOW

O. Create a new inbound rule in the security group of the EC2 instance with the following details:

P. Protocol: UDP

Q. Port Range: 20 - 21

R. Source: 175.45.11./326.100

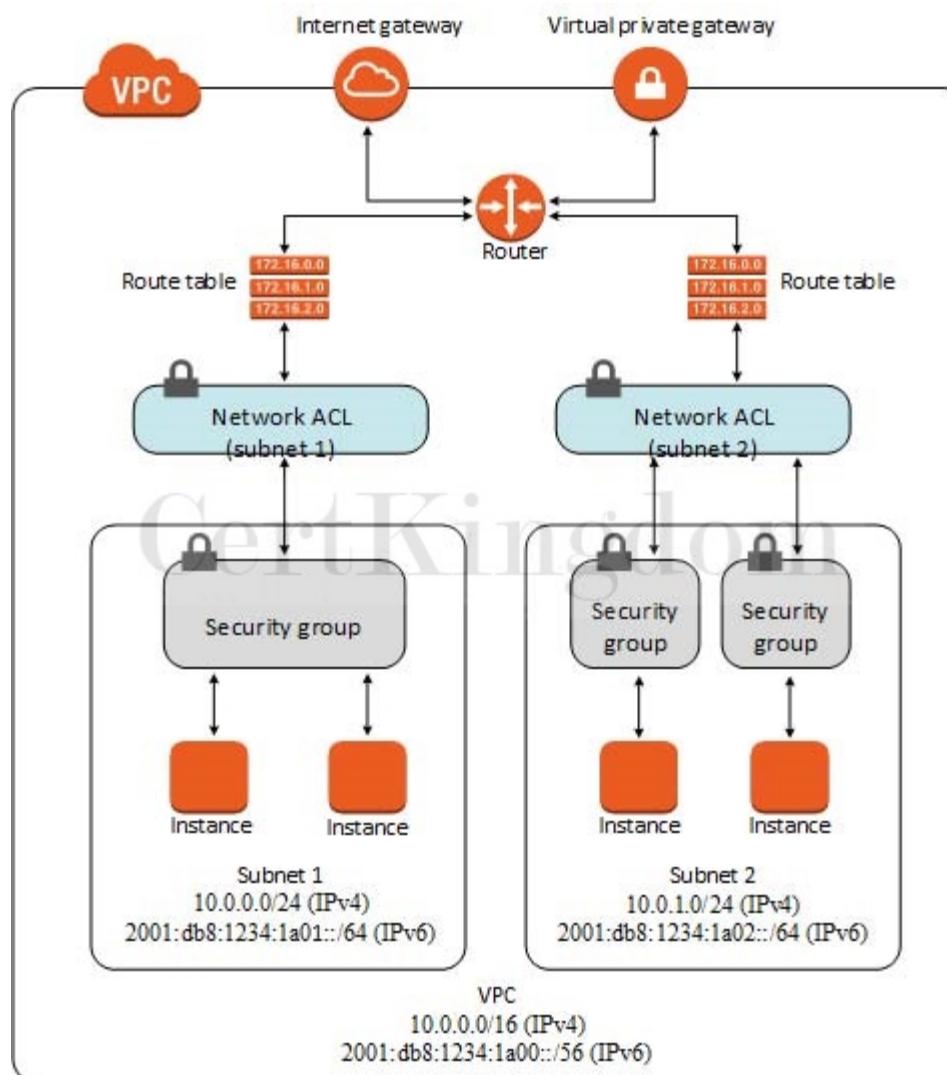
Answer: I

Explanation:

The FTP protocol uses TCP via ports 20 and 21. This should be configured in your security groups or in your Network ACL inbound rules. As required by the scenario, you should only allow the individual IP of the client and not the entire network. Therefore, in the Source, the proper CIDR notation should be used.

The denotes one IP address and the /0 refers to the entire network.

It is stated in the scenario that you launched the EC2 instances in a newly created VPC with default settings. Your VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic. Hence, you actually don't need to explicitly add inbound rules to your Network ACL to allow inbound traffic, if your VPC has a default setting.



The below option is incorrect:

Create a new inbound rule in the security group of the EC2 instance with the following details:

Protocol: UDP

Port Range: 20 - 21

Source: 175.45.11./326.100

Although the configuration of the Security Group is valid, the provided Protocol is incorrect. Take note that FTP uses TCP and not UDP.

The below option is also incorrect:

Create a new Network ACL inbound rule in the subnet of the EC2 instance with the following details:

Protocol: TCP

Port Range: 20 - 21

Source: 175.45.11./326.100/0

Allow/Deny: ALLOW

Although setting up an inbound Network ACL is valid, the source is invalid since it must be an IPv4 or IPv6 CIDR block. In the provided IP address, the /0 refers to the entire network and not a specific IP address. In addition, it is stated in the scenario that the newly created VPC has default settings and by default, the Network ACL allows all traffic. This means that there is actually no need to configure your Network ACL.

Likewise, the below option is also incorrect:

Create a new Network ACL inbound rule in the subnet of the EC2 instance with the following details:

Protocol: UDP

Port Range: 20 - 21

Source: 175.45.11./326.100/0

Allow/Deny: ALLOW

Just like in the above, the source is also invalid. Take note that FTP uses TCP and not UDP, which is one of the reasons why this option is wrong. In addition, it is stated in the scenario that the newly created VPC has default settings and by default, the Network ACL allows all traffic. This means that there is actually no need to configure your Network ACL.

References:

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_SecurityGroups.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html)

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

---

## QUESTION 249

A web application requires a minimum of six Amazon Elastic Compute Cloud (EC2) instances running at all times. You are tasked to deploy the application to three availability zones in the EU Ireland region (euwest- 1a, eu-west-1b, and eu-west-1c). It is required that the system is fault-tolerant up to the loss of one Availability Zone.

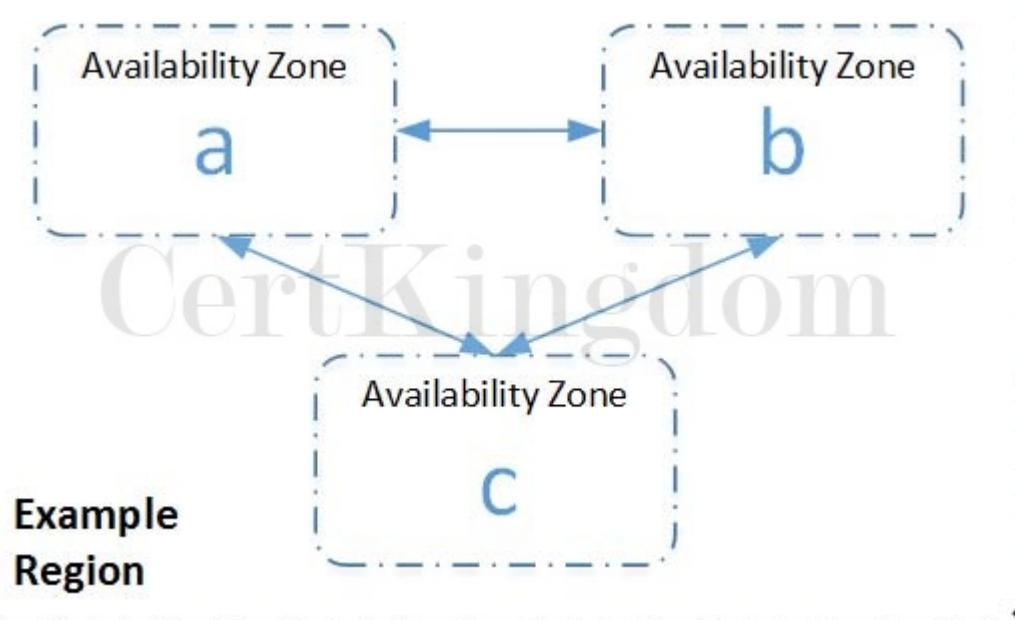
Which of the following setup is the most cost-effective solution which also maintains the fault-tolerance of your system?

- A. 6 instances in eu-west-1a, 6 instances in eu-west-1b, and no instances in eu-west-1c
- B. 2 instances in eu-west-1a, 2 instances in eu-west-1b, and 2 instances in eu-west-1c
- C. 6 instances in eu-west-1a, 6 instances in eu-west-1b, and 6 instances in eu-west-1c
- D. 3 instances in eu-west-1a, 3 instances in eu-west-1b, and 3 instances in eu-west-1c

Answer: D

Explanation:

Basically, fault-tolerance is the ability of a system to remain in operation even in the event that some of its components fail, without any service degradation. In AWS, it can also refer to the minimum number of running EC2 instances or resources which should be running at all times in order for the system to properly operate and serve its consumers. Take note that this is quite different from the concept of High Availability, which is just concerned with having at least one running instance or resource in case of failure.



In this scenario, 3 instances in eu-west-1a, 3 instances in eu-west-1b, and 3 instances in eu-west-1c is the correct answer because even if there was an outage in one of the Availability Zones, the system still satisfies the requirement of having a minimum of 6 running instances. It is also the most cost-effective solution among other options.

The option that says: 6 instances in eu-west-1a, 6 instances in eu-west-1b, and 6 instances in euwest- 1c is incorrect because although this solution provides the maximum fault-tolerance for the system, it entails a significant cost to maintain a total of 18 instances across 3 AZs.

The option that says: 2 instances in eu-west-1a, 2 instances in eu-west-1b, and 2 instances in euwest- 1c is incorrect because if one Availability Zone goes down, there will only be 4 running instances available. Although this is the most cost-effective solution, it does not provide fault-tolerance.

The option that says: 6 instances in eu-west-1a, 6 instances in eu-west-1b, and no instances in euwest- 1c is incorrect because although it provides fault-tolerance, it is not the most cost-effective solution as compared with the options above. This solution has 12 running instances, unlike the correct answer which only has 9 instances.

References:

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

[https://media.amazonaws.com/AWS\\_Building\\_Fault\\_Tolerant\\_Applications.pdf](https://media.amazonaws.com/AWS_Building_Fault_Tolerant_Applications.pdf)

## QUESTION 250

An organization plans to use an AWS Direct Connect connection to establish a dedicated connection between its on-premises network and AWS. The organization needs to launch a fully managed solution that will automate and accelerate the replication of data to and from various AWS storage services.

Which of the following solutions would you recommend?

- A. Use an AWS Storage Gateway tape gateway to store data on virtual tape cartridges and asynchronously copy your backups to AWS.
- B. Use an AWS DataSync agent to rapidly move the data over a service endpoint.
- C. Use an AWS DataSync agent to rapidly move the data over the Internet.
- D. Use an AWS Storage Gateway file gateway to store and retrieve files directly using the SMB file system protocol.

Answer: B

Explanation:

AWS DataSync allows you to copy large datasets with millions of files, without having to build custom solutions with open source tools or license and manage expensive commercial network acceleration software. You can use DataSync to migrate active data to AWS, transfer data to the cloud for analysis and processing, archive data to free up on-premises storage capacity, or replicate data to AWS for business continuity.

AWS DataSync simplifies, automates, and accelerates copying large amounts of data to and from AWS storage services

over the internet or AWS Direct Connect. DataSync can copy data between Network File System (NFS), Server Message Block (SMB) file servers, self-managed object storage, or AWS Snowcone, and Amazon Simple Storage Service (Amazon S3) buckets, Amazon EFS file systems, and Amazon FSx for Windows File Server file systems.



You deploy an AWS DataSync agent to your on-premises hypervisor or in Amazon EC2. To copy data to or from an on-premises file server, you download the agent virtual machine image from the AWS Console and deploy to your on-premises VMware ESXi, Linux Kernel-based Virtual Machine (KVM), or Microsoft Hyper-V hypervisor. To copy data to or from an in-cloud file server, you create an Amazon EC2 instance using a DataSync agent AMI. In both cases the agent must be deployed so that it can access your file server using the NFS, SMB protocol, or the Amazon S3 API. To set up transfers between your AWS Snowcone device and AWS storage, use the DataSync agent AMI that comes pre-installed on your device.

Since the scenario plans to use AWS Direct Connect for private connectivity between on-premises and AWS, you can use DataSync to automate and accelerate online data transfers to AWS storage services.

The AWS DataSync agent will be deployed in your on-premises network to accelerate data transfer to AWS. To connect programmatically to an AWS service, you will need to use an AWS Direct Connect service endpoint.

Hence, the correct answer is: Use an AWS DataSync agent to rapidly move the data over a service endpoint.

The option that says: Use AWS DataSync agent to rapidly move the data over the Internet is incorrect because the organization will be using an AWS Direct Connect connection for private connectivity. This means that the connection will not pass through the public Internet.

The options that say: Use AWS Storage Gateway tape gateway to store data on virtual tape cartridges and asynchronously copy your backups to AWS and Use AWS Storage Gateway file gateway to store and retrieve files directly using the SMB file system protocol are both incorrect because, in the scenario, you need to accelerate the replication of data, and not establish a hybrid cloud storage architecture. AWS Storage Gateway only supports a few AWS storage services as a target based on the type of gateway that you launched. AWS DataSync is more suitable in automating and accelerating online data transfers to a variety of AWS storage services.

#### References:

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

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

<https://docs.aws.amazon.com/general/latest/gr/dc.html>

#### AWS DataSync Overview:

[https://www.youtube.com/watch?v=uQDVZfj\\_VEA](https://www.youtube.com/watch?v=uQDVZfj_VEA)

Check out this AWS DataSync Cheat Sheet:

<https://tutorialsdojo.com/aws-datasync/>

## QUESTION 251

A leading IT consulting company has an application which processes a large stream of financial data by an Amazon ECS Cluster then stores the result to a DynamoDB table. You have to design a solution to detect new entries in the DynamoDB table then automatically trigger a Lambda function to run some tests to verify the processed data.

What solution can be easily implemented to alert the Lambda function of new entries while requiring minimal configuration change to your architecture?

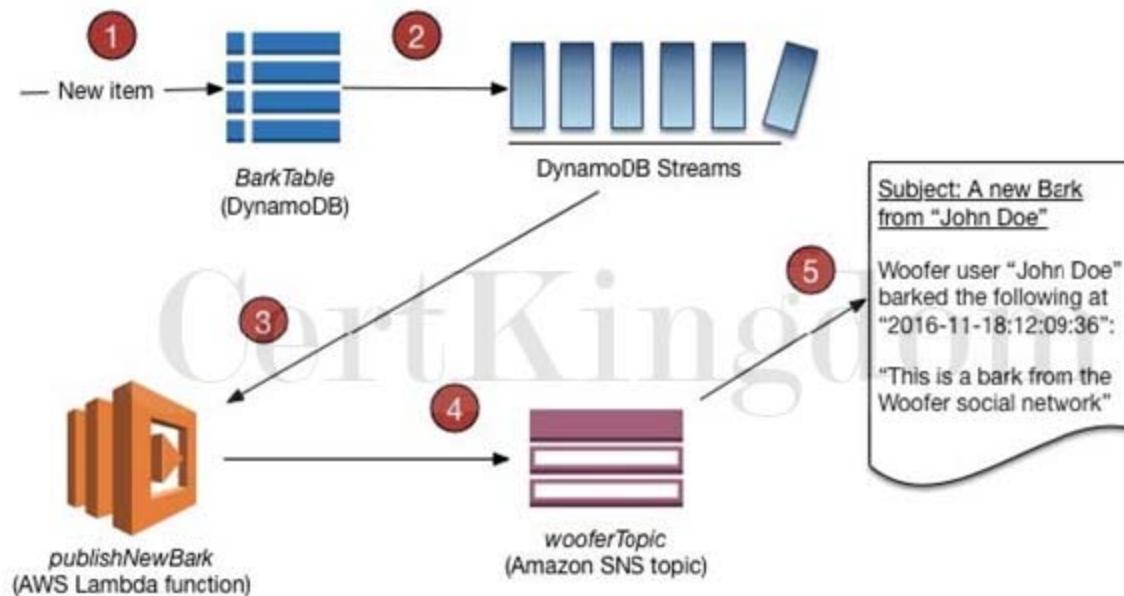
- A. Invoke the Lambda functions using SNS each time that the ECS Cluster successfully processed financial data.
- B. Enable DynamoDB Streams to capture table activity and automatically trigger the Lambda function.
- C. Use Systems Manager Automation to detect new entries in the DynamoDB table then automatically invoke the Lambda function for processing.
- D. Use CloudWatch Alarms to trigger the Lambda function whenever a new entry is created in the DynamoDB table.

Answer: B

Explanation:

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.



You can create a Lambda function which can perform a specific action that you specify, such as sending a notification or initiating a workflow. For instance, you can set up a Lambda function to simply copy each stream record to persistent storage, such as EFS or S3, to create a permanent audit trail of write activity in your table.

Suppose you have a mobile gaming app that writes to a `TutorialsDojoCourses` table. Whenever the `TopCourse` attribute of the `TutorialsDojoScores` table is updated, a corresponding stream record is written to the table's stream. This event could then trigger a Lambda function that posts a congratulatory message on a social media network. (The function would simply ignore any stream records that are not updates to `TutorialsDojoCourses` or that do not modify the `TopCourse` attribute.) Hence, enabling DynamoDB Streams to capture table activity and automatically trigger the Lambda function is the correct answer because the requirement can be met with minimal configuration change using DynamoDB streams which can automatically trigger Lambda functions whenever there is a new entry.

Using CloudWatch Alarms to trigger the Lambda function whenever a new entry is created in the DynamoDB table is incorrect because CloudWatch Alarms only monitor service metrics, not changes in DynamoDB table data.

Invoking the Lambda functions using SNS each time that the ECS Cluster successfully processed financial data is incorrect because you don't need to create an SNS topic just to invoke Lambda functions. You can enable DynamoDB streams instead to meet the requirement with less configuration.

Using Systems Manager Automation to detect new entries in the DynamoDB table then automatically invoking the Lambda function for processing is incorrect because the Systems Manager Automation service is primarily used to simplify common maintenance and deployment tasks of Amazon EC2 instances and other AWS resources. It does not have the capability to detect new entries in a DynamoDB table.

References:

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

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

Check out this Amazon DynamoDB cheat sheet:

<https://tutorialsdojo.com/amazon-dynamodb/>

---

## QUESTION 252

A media company needs to configure an Amazon S3 bucket to serve static assets for the public-facing web application. Which methods ensure that all of the objects uploaded to the S3 bucket can be read publicly all over the Internet? (Select TWO.)

- A. Create an IAM role to set the objects inside the S3 bucket to public read.
- B. Configure the S3 bucket policy to set all objects to public read.
- C. Configure the cross-origin resource sharing (CORS) of the S3 bucket to allow objects to be publicly accessible from all domains.
- D. Do nothing. Amazon S3 objects are already public by default.
- E. Grant public read access to the object when uploading it using the S3 Console.

Answer: B,E

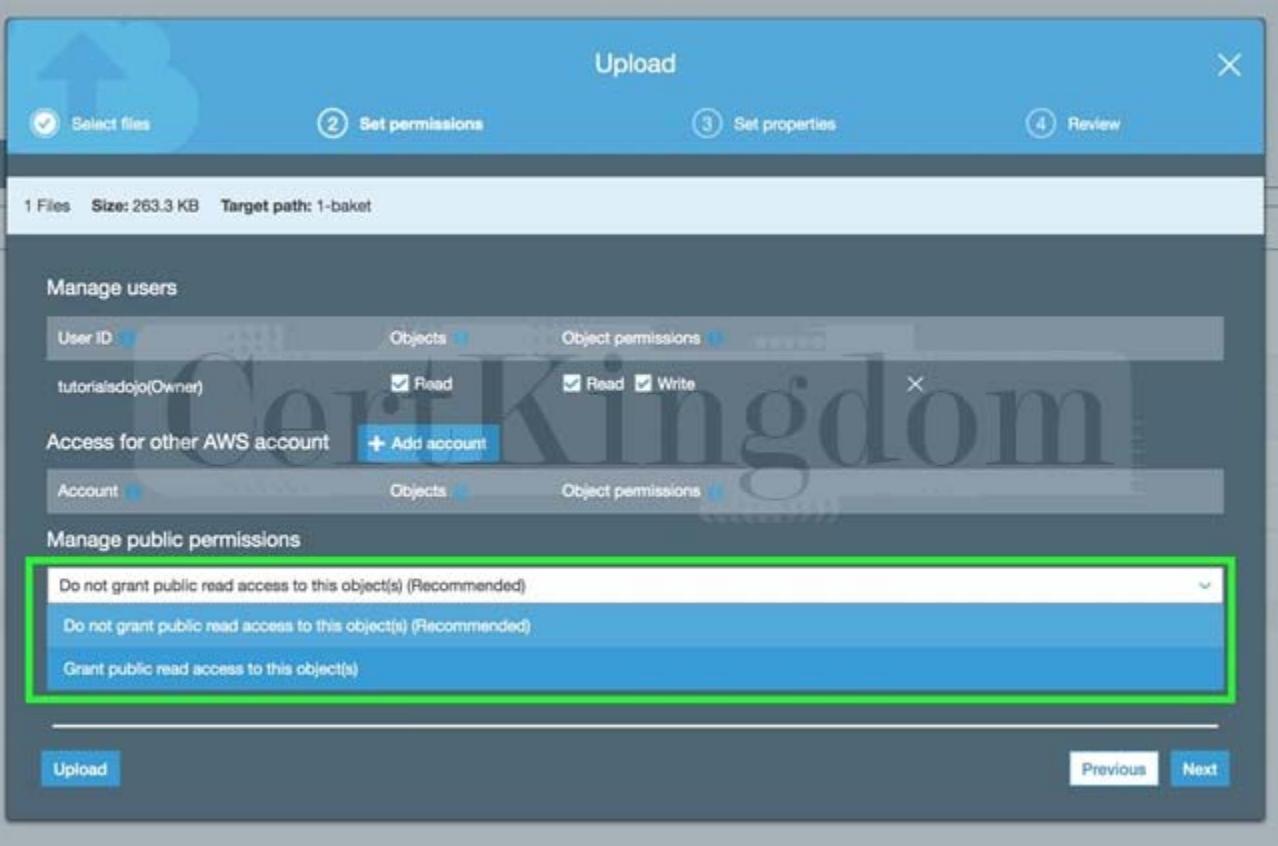
Explanation:

By default, all Amazon S3 resources such as buckets, objects, and related subresources are private which means that only the AWS account holder (resource owner) that created it has access to the resource. The resource owner can optionally grant access permissions to others by writing an access policy. In S3, you also set the permissions of the object during upload to make it public.

Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as resourcebased policies.

For example, bucket policies and access control lists (ACLs) are resource-based policies. You can also attach access policies to users in your account. These are called user policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources.

You can also manage the public permissions of your objects during upload. Under Manage public permissions, you can grant read access to your objects to the general public (everyone in the world), for all of the files that you're uploading. Granting public read access is applicable to a small subset of use cases such as when buckets are used for websites.



Hence, the correct answers are:

- Grant public read access to the object when uploading it using the S3 Console.
- Configure the S3 bucket policy to set all objects to public read.

The option that says: Configure the cross-origin resource sharing (CORS) of the S3 bucket to allow objects to be publicly accessible from all domains is incorrect. CORS will only allow objects from one domain (travel.cebu.com) to be loaded and accessible to a different domain (palawan.com). It won't necessarily expose objects for public access all over the internet.

The option that says: Creating an IAM role to set the objects inside the S3 bucket to public read is incorrect. You can create an IAM role and attach it to an EC2 instance in order to retrieve objects from the S3 bucket or add new ones. An IAM Role, in itself, cannot directly make the S3 objects public or change the permissions of each individual object.

The option that says: Do nothing. Amazon S3 objects are already public by default is incorrect because, by default, all the S3 resources are private, so only the AWS account that created the resources can access them.

References:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html>

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

## QUESTION 253

To save costs, your manager instructed you to analyze and review the setup of your AWS cloud infrastructure. You should also provide an estimate of how much your company will pay for all of the AWS resources that they are using. In this scenario, which of the following will incur costs? (Select TWO.)

- A. A stopped On-Demand EC2 Instance
- B. EBS Volumes attached to stopped EC2 Instances
- C. Using an Amazon VPC
- D. Public Data Set
- E. A running EC2 Instance

Answer: B,E

Explanation:

Billing commences when Amazon EC2 initiates the boot sequence of an AMI instance. Billing ends when the instance

terminates, which could occur through a web services command, by running "shutdown -h", or through instance failure. When you stop an instance, AWS shuts it down but doesn't charge hourly usage for a stopped instance or data transfer fees. However, AWS does charge for the storage of any Amazon EBS volumes. Hence, a running EC2 Instance and EBS Volumes attached to stopped EC2 Instances are the right answers and conversely, a stopped On-Demand EC2 Instance is incorrect as there is no charge for a stopped EC2 instance that you have shut down. Using Amazon VPC is incorrect because there are no additional charges for creating and using the VPC itself. Usage charges for other Amazon Web Services, including Amazon EC2, still apply at published rates for those resources, including data transfer charges.

Public Data Set is incorrect due to the fact that Amazon stores the data sets at no charge to the community and, as with all AWS services, you pay only for the compute and storage you use for your own applications.

#### References:

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

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

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

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

---

### QUESTION 254

A company has an OLTP (Online Transactional Processing) application that is hosted in an Amazon ECS cluster using the Fargate launch type. It has an Amazon RDS database that stores data of its production website. The Data Analytics team needs to run queries against the database to track and audit all user transactions. These query operations against the production database must not impact application performance in any way.

Which of the following is the MOST suitable and cost-effective solution that you should implement?

- A. Set up a new Amazon Redshift database cluster. Migrate the product database into Redshift and allow the Data Analytics team to fetch data from it.
- B. Set up a new Amazon RDS Read Replica of the production database. Direct the Data Analytics team to query the production data from the replica.
- C. Set up a Multi-AZ deployments configuration of your production database in RDS. Direct the Data Analytics team to query the production data from the standby instance.
- D. Upgrade the instance type of the RDS database to a large instance.

Answer: B

#### Explanation:

Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances.

This feature makes it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.

You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read replicas are available in Amazon RDS for MySQL, MariaDB, Oracle and PostgreSQL, as well as Amazon Aurora.

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

You can reduce the load on your source DB instance by routing read queries from your applications to the read replica.

These replicas allow you to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.

Because read replicas can be promoted to master status, they are useful as part of a sharding implementation. To shard your database, add a read replica and promote it to master status, then, from each of the resulting DB Instances, delete the data that belongs to the other shard.

Hence, the correct answer is: Set up a new Amazon RDS Read Replica of the production database.

Direct the Data Analytics team to query the production data from the replica. The option that says: Set up a new Amazon Redshift database cluster. Migrate the product database into Redshift and allow the Data Analytics team to fetch data from it is incorrect because Redshift is primarily used for OLAP (Online Analytical Processing) applications and not for OLTP.

The option that says: Set up a Multi-AZ deployments configuration of your production database in RDS.

Direct the Data Analytics team to query the production data from the standby instance is incorrect because you can't directly connect to the standby instance. This is only used in the event of a database failover when your primary instance encountered an outage.

The option that says: Upgrade the instance type of the RDS database to a large instance is incorrect because this entails a significant amount of cost. Moreover, the production database could still be affected by the queries done by the Data Analytics team. A better solution for this scenario is to use a Read Replica instead.

References:

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

<https://aws.amazon.com/rds/details/read-replicas/>

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

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

---

## QUESTION 255

A company decided to change its third-party data analytics tool to a cheaper solution. They sent a full data export on a CSV file which contains all of their analytics information. You then save the CSV file to an S3 bucket for storage. Your manager asked you to do some validation on the provided data export.

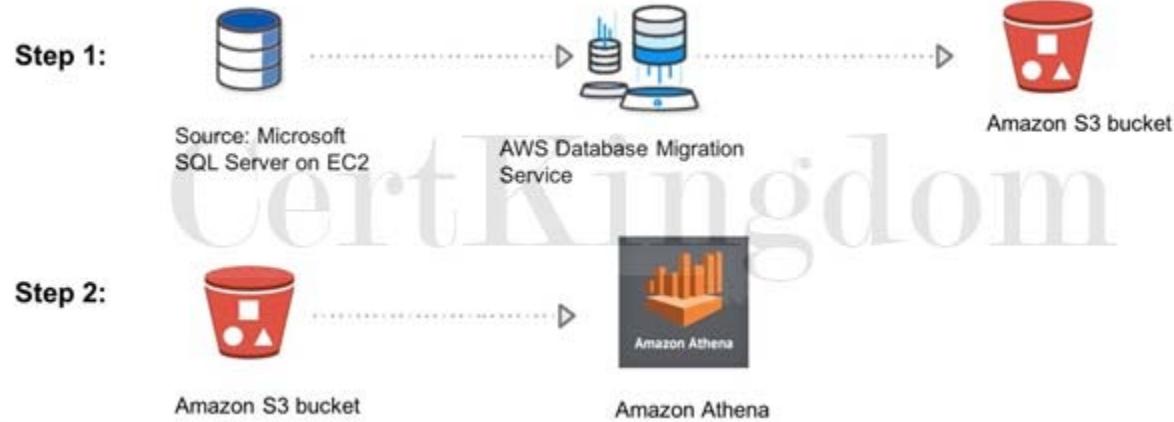
In this scenario, what is the most cost-effective and easiest way to analyze export data using standard SQL?

- A. Use a migration tool to load the CSV export file from S3 to a database that is designed for online analytic processing (OLAP) such as AWS RedShift. Run some queries once the data has been loaded to complete your validation.
- B. To be able to run SQL queries, use AWS Athena to analyze the export data file in S3.
- C. Use mysqldump client utility to load the CSV export file from S3 to a MySQL RDS instance. Run some SQL queries once the data has been loaded to complete your validation.
- D. Create a migration tool to load the CSV export file from S3 to a DynamoDB instance. Once the data has been loaded, run queries using DynamoDB.

Answer: B

Explanation:

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



Athena is serverless, so there is no infrastructure to set up or manage, and you pay only for the queries you run. Athena scales automatically “executing queries in parallel” so results are fast, even with large datasets and complex queries. Athena helps you analyze unstructured, semi-structured, and structured data stored in Amazon S3.

Examples include CSV, JSON, or columnar data formats such as Apache Parquet and Apache ORC.

You can use Athena to run ad-hoc queries using ANSI SQL, without the need to aggregate or load the data into Athena. Hence, the correct answer is: To be able to run SQL queries, use Amazon Athena to analyze the export data file in S3.

The rest of the options are all incorrect because it is not necessary to set up a database to be able to analyze the CSV export file. You can use a cost-effective option (AWS Athena), which is a serverless that enables you to pay only for the queries you run.

Reference:

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

Check out this Amazon Athena Cheat Sheet:

<https://tutorialsdojo.com/amazon-athena/>

## QUESTION 256

The company you are working for has a set of AWS resources hosted in ap-northeast-1 region. You have been asked by your IT Manager to create an AWS CLI shell script that will call an AWS service which could create duplicate resources in another region in the event that ap-northeast-1 region fails.

The duplicated resources should also contain the VPC Peering configuration and other networking components from the primary stack.

Which of the following AWS services could help fulfill this task?

- A. Amazon SQS
- B. Amazon SNS
- C. AWS CloudFormation
- D. AWS Elastic Beanstalk

Answer: C

Explanation:

AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS.

The screenshot shows the AWS CloudFormation template editor. The template is named 'template1' and is set to JSON format. The code defines parameters for VPC ID, Subnets, and AZs, and specifies resources for VPC, AutoScaling, and ElasticLoadBalancer.

```
1+ {
2     "AWS::TemplateFormatVersion": "2010-09-09",
3     "Description": "AWS CloudFormation Sample Template VPC_AutoScaling_and_ElasticLoadBalancer: Create a load balanced, Auto Scaled sample website",
4     "Parameters": {
5         "VpcId": {
6             "Type": "AWS::EC2::VPC::Id",
7             "Description": "VpcId of your existing Virtual Private Cloud (VPC)",
8             "ConstraintDescription": "must be the VPC Id of an existing Virtual Private Cloud."
9         },
10        "Subnets": {
11            "Type": "List<AWS::EC2::Subnet::Id>",
12            "Description": "The list of SubnetIds in your Virtual Private Cloud (VPC)",
13            "ConstraintDescription": "must be a list of an existing subnets in the selected Virtual Private Cloud."
14        },
15        "AZs": {
16            "Type": "List<String>",
17            ...
18        }
19    },
20    "Resources": {
21        "VPC": {
22            "Type": "AWS::VPC::VPC",
23            "Properties": {
24                "CidrBlock": "10.0.0.0/16",
25                "EnableDnsSupport": true,
26                "EnableDnsHostnames": true,
27                "InstanceTenancy": "default"
28            }
29        },
30        "AutoScalingGroup": {
31            "Type": "AWS::AutoScaling::AutoScalingGroup",
32            "Properties": {
33                "DesiredCapacity": 3,
34                "HealthCheckGracePeriod": 300,
35                "HealthCheckType": "ELB",
36                "LaunchConfigurationName": "MyLaunchConfig",
37                "MaxSize": 3,
38                "MinSize": 3,
39                "VPCZoneIdentifier": "subnet-00000000,subnet-00000001"
40            }
41        },
42        "ElasticLoadBalancer": {
43            "Type": "AWS::ElasticLoadBalancing::LoadBalancer",
44            "Properties": {
45                "Listeners": [
46                    {
47                        "Protocol": "HTTP",
48                        "Port": 80
49                    }
50                ],
51                "Subnets": "subnet-00000000,subnet-00000001",
52                "SecurityGroups": "sg-00000000"
53            }
54        }
55    }
56}
```

You can create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you. With this, you can deploy an exact copy of your AWS architecture, along with all of the AWS resources which are hosted in one region to another.

Hence, the correct answer is AWS CloudFormation.

AWS Elastic Beanstalk is incorrect. Elastic Beanstalk is a high-level service that simplifies the creation of application resources such as an EC2 instance with preconfigured proxy servers (Nginx or Apache), a load balancer, an auto-scaling group, and so on. Elastic Beanstalk environments have limited resources;

for example, Elastic Beanstalk does not create a VPC for you. CloudFormation on the other hand is more of a low-level service that you can use to model the entirety of your AWS environment. In fact, Elastic Beanstalk uses CloudFormation under the hood to create resources.

Amazon SQS and Amazon SNS are both incorrect because SNS and SQS are just messaging services.

References:

[<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-cli-creating-stack.html>](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide>Welcome.html</a></p></div><div data-bbox=)

Check out this AWS CloudFormation Cheat Sheet:

<https://tutorialsdojo.com/aws-cloudformation/>

AWS CloudFormation - Templates, Stacks, Change Sets:

<https://youtu.be/Xpuprxg7aY>

## QUESTION 257

A company plans to design a highly available architecture in AWS. They have two target groups with three EC2 instances each, which are added to an Application Load Balancer. In the security group of the EC2 instance, you have verified that port 80 for HTTP is allowed. However, the instances are still showing out of service from the load balancer.

What could be the root cause of this issue?

- A. The wrong instance type was used for the EC2 instance.
- B. The health check configuration is not properly defined.
- C. The wrong subnet was used in your VPC
- D. The instances are using the wrong AMI.

Answer: B

Explanation:

Since the security group is properly configured, the issue may be caused by a wrong health check configuration in the Target Group.

## Edit health check

X

Protocol	<input type="radio"/> i	HTTP
Path	<input type="radio"/> i	/healthcheck

### Advanced health check settings

Port	<input type="radio"/> i	traffic port
	<input type="radio"/>	override
Healthy threshold	i	2
Unhealthy threshold	i	2
Timeout	i	6 seconds
Interval	i	30 seconds
Success codes	i	200-399

Cancel

Save

Your Application Load Balancer periodically sends requests to its registered targets to test their status. These tests are called health checks. Each load balancer node routes requests only to the healthy targets in the enabled Availability Zones for the load balancer. Each load balancer node checks the health of each target, using the health check settings for the target group with which the target is registered. After your target is registered, it must pass one health check to be considered healthy. After each health check is completed, the load balancer node closes the connection that was established for the health check.

Reference:

<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html>

AWS Elastic Load Balancing Overview:

<https://www.youtube.com/watch?v=UB15dw59DO8>

Check out this AWS Elastic Load Balancing (ELB) Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

ELB Health Checks vs Route 53 Health Checks For Target Health Monitoring:

<https://tutorialsdojo.com/elb-health-checks-vs-route-53-health-checks-for-target-health-monitoring/>

### QUESTION 258

A company has a web application hosted on a fleet of EC2 instances located in two Availability Zones that are all placed behind an Application Load Balancer. As a Solutions Architect, you have to add a health check configuration to ensure your application is highly-available.

Which health checks will you implement?

- A. HTTP or HTTPS health check
- B. FTP health check
- C. TCP health check
- D. ICMP health check

Answer: A

Explanation:

A load balancer takes requests from clients and distributes them across the EC2 instances that are registered with the load

balancer. You can create a load balancer that listens to both the HTTP (80) and HTTPS (443) ports. If you specify that the HTTPS listener sends requests to the instances on port 80, the load balancer terminates the requests, and communication from the load balancer to the instances is not encrypted. If the HTTPS listener sends requests to the instances on port 443, communication from the load balancer to the instances is encrypted.

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTP	80	HTTP	80
HTTPS (Secure HTTP)	443	HTTPS (Secure HTTP)	443
<b>Add</b>			

If your load balancer uses an encrypted connection to communicate with the instances, you can optionally enable authentication of the instances. This ensures that the load balancer communicates with an instance only if its public key matches the key that you specified to the load balancer for this purpose.

The type of ELB that is mentioned in this scenario is an Application Elastic Load Balancer. This is used if you want a flexible feature set for your web applications with HTTP and HTTPS traffic. Conversely, it only allows 2 types of health check: HTTP and HTTPS.

Hence, the correct answer is: HTTP or HTTPS health check.

ICMP health check and FTP health check are incorrect as these are not supported.

TCP health check is incorrect. A TCP health check is only offered in Network Load Balancers and Classic Load Balancers.

References:

<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html>

Check out this AWS Elastic Load Balancing (ELB) Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

EC2 Instance Health Check vs ELB Health Check vs Auto Scaling and Custom Health Check:

<https://tutorialsdojo.com/ec2-instance-health-check-vs-elb-health-check-vs-auto-scaling-and-custom-health-check/>

Comparison of AWS Services Cheat Sheets:

<https://tutorialsdojo.com/comparison-of-aws-services/>

---

## QUESTION 259

A company has an application hosted in an Amazon ECS Cluster behind an Application Load Balancer.

The Solutions Architect is building a sophisticated web filtering solution that allows or blocks web requests based on the country that the requests originate from. However, the solution should still allow specific IP addresses from that country.

Which combination of steps should the Architect implement to satisfy this requirement? (Select TWO.)

- A. Place a Transit Gateway in front of the VPC where the application is hosted and set up Network ACLs that block requests that originate from a specific country.
- B. Using AWS WAF, create a web ACL with a rule that explicitly allows requests from approved IP addresses declared in an IP Set.
- C. In the Application Load Balancer, create a listener rule that explicitly allows requests from approved IP addresses.
- D. Set up a geo match condition in the Application Load Balancer that blocks requests from a specific country.
- E. Add another rule in the AWS WAF web ACL with a geo match condition that blocks requests that originate from a specific country.

Answer: B,E

Explanation:

If you want to allow or block web requests based on the country that the requests originate from, create one or more geo match conditions. A geo match condition lists countries that your requests originate from. Later in the process, when you create a web ACL, you specify whether to allow or block requests from those countries.

You can use geo match conditions with other AWS WAF Classic conditions or rules to build sophisticated filtering. For example, if you want to block certain countries but still allow specific IP addresses from that country, you could create a rule

containing a geo match condition and an IP match condition. Configure the rule to block requests that originate from that country and do not match the approved IP addresses. As another example, if you want to prioritize resources for users in a particular country, you could include a geo match condition in two different rate-based rules. Set a higher rate limit for users in the preferred country and set a lower rate limit for all other users.

The screenshot shows the AWS WAF 'Create web ACL' interface. On the left, a sidebar lists steps: Step 1 (Describe web ACL and associate it to AWS resources), Step 2 (Add rules and rule groups, which is selected and highlighted in blue), Step 3 (Set rule priority), Step 4 (Configure metrics), and Step 5 (Review and create web ACL). The main content area is titled 'Add rules and rule groups'. It contains a section for 'Rules' with a table:

Name	Capacity	Action
Allowed_IP_Phippines	1	Allow
Block_Requests_from_the_Phippines	1	Block

Below the table, a note states: 'Web ACL rule capacity units used. The total capacity units used by the web ACL can't exceed 1500.' A status bar indicates '3/1500 WCU's'. At the bottom, there are 'Default web ACL action for requests that don't match any rules' settings, where 'Allow' is selected. Navigation buttons at the bottom right include 'Cancel', 'Previous', and 'Next'.

If you are using the CloudFront geo restriction feature to block a country from accessing your content, any request from that country is blocked and is not forwarded to AWS WAF Classic. So if you want to allow or block requests based on geography plus other AWS WAF Classic conditions, you should not use the CloudFront geo restriction feature. Instead, you should use an AWS WAF Classic geo match condition.

Hence, the correct answers are:

- Using AWS WAF, create a web ACL with a rule that explicitly allows requests from approved IP addresses declared in an IP Set.
- Add another rule in the AWS WAF web ACL with a geo match condition that blocks requests that originate from a specific country.

The option that says: In the Application Load Balancer, create a listener rule that explicitly allows requests from approved IP addresses is incorrect because a listener rule just checks for connection requests using the protocol and port that you configure. It only determines how the load balancer routes the requests to its registered targets.

The option that says: Set up a geo match condition in the Application Load Balancer that block requests that originate from a specific country is incorrect because you can't configure a geo match condition in an Application Load Balancer. You have to use AWS WAF instead.

The option that says: Place a Transit Gateway in front of the VPC where the application is hosted and set up Network ACLs that block requests that originate from a specific country is incorrect because AWS Transit Gateway is simply a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. Using this type of gateway is not warranted in this scenario. Moreover, Network ACLs are not suitable for blocking requests from a specific country. You have to use AWS WAF instead.

References:

<https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-geo-conditions.html>

<https://docs.aws.amazon.com/waf/latest/developerguide/how-aws-waf-works.html>

Check out this AWS WAF Cheat Sheet:

<https://tutorialsdojo.com/aws-waf/>

AWS Security Services Overview - WAF, Shield, CloudHSM, KMS:

<https://www.youtube.com/watch?v=-1S-RdeAmMo>

---

## QUESTION 260

A company has a web application hosted in their on-premises infrastructure that they want to migrate to AWS cloud. Your manager has instructed you to ensure that there is no downtime while the migration process is on-going. In order to achieve this, your team decided to divert 50% of the traffic to the new application in AWS and the other 50% to the application hosted in their on-premises infrastructure. Once the migration is over and the application works with no issues, a full diversion to AWS will be implemented. The company's VPC is connected to its on-premises network via an AWS Direct Connect connection.

Which of the following are the possible solutions that you can implement to satisfy the above requirement? (Select TWO.)

- A. Use a Network Load balancer with Weighted Target Groups to divert the traffic between the on-premises and AWS-hosted application. Divert 50% of the traffic to the new application in AWS and the other 50% to the application hosted in their on-premises infrastructure.
- B. Use an Application Elastic Load balancer with Weighted Target Groups to divert and proportion the traffic between the on-premises and AWS-hosted application. Divert 50% of the traffic to the new application in AWS and the other 50% to the application hosted in their on-premises infrastructure.
- C. Use Route 53 with Weighted routing policy to divert the traffic between the on-premises and AWS-hosted application. Divert 50% of the traffic to the new application in AWS and the other 50% to the application hosted in their on-premises infrastructure.
- D. Use AWS Global Accelerator to divert and proportion the HTTP and HTTPS traffic between the on-premises and AWS-hosted application. Ensure that the on-premises network has an AnyCast static IP address and is connected to your VPC via a Direct Connect Gateway.
- E. Use Route 53 with Failover routing policy to divert and proportion the traffic between the on-premises and AWS-hosted application. Divert 50% of the traffic to the new application in AWS and the other 50% to the application hosted in their on-premises infrastructure.

Answer: B,C

Explanation:

Application Load Balancers support Weighted Target Groups routing. With this feature, you will be able to do weighted routing of the traffic forwarded by a rule to multiple target groups. This enables various use cases like blue-green, canary and hybrid deployments without the need for multiple load balancers.

It even enables zero-downtime migration between on-premises and cloud or between different compute types like EC2 and Lambda.

The screenshot shows the AWS Application Load Balancer (ALB) configuration interface. At the top, there are tabs for 'Rules' and other navigation options. The main area displays a rule titled 'last' under the 'arn:aws:lambda' target. The rule is set to 'IF (all match)' and has a condition 'Requests otherwise not routed'. The 'THEN' section contains three actions under 'Forward to...': 'blue' with a weight of 50%, 'green' with a weight of 50%, and 'Select a target group' with a weight of 0%. There is also an option for 'Group-level stickiness'. A large watermark for 'CertKingdom' is overlaid across the entire interface.

To divert 50% of the traffic to the new application in AWS and the other 50% to the application, you can also use Route 53 with Weighted routing policy. This will divert the traffic between the on-premises and AWS-hosted application accordingly. Weighted routing lets you associate multiple resources with a single domain name ([tutorialsdojo.com](http://tutorialsdojo.com)) or subdomain name ([portal.tutorialsdojo.com](http://portal.tutorialsdojo.com)) and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load balancing and testing new versions of software.

You can set a specific percentage of how much traffic will be allocated to the resource by specifying the weights. For example, if you want to send a tiny portion of your traffic to one resource and the rest to another resource, you might specify weights of 1 and 255. The resource with a weight of 1 gets 1th of the traffic ( $1+255$ ), and the other resource gets 255ths ( $255+255$ ).

You can gradually change the balance by changing the weights. If you want to stop sending traffic to a resource, you can change the weight for that record to 0.

When you create a target group in your Application Load Balancer, you specify its target type. This determines the type of target you specify when registering with this target group. You can select the following target types:

1. instance - The targets are specified by instance ID.
2. ip - The targets are IP addresses.
3. Lambda - The target is a Lambda function.

## Step 5: Register Targets

Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

### ip-target-1 (target group)

Specify one or more IP addresses to register as targets

Network	Port	Availability Zone	IP (allowed ranges)	Port
Other private IP address	80	all		80
10.1.200.1	80	all	private network resource	X
10.0.100.2	80	us-east-1b	private network resource	X
10.0.100.1	80	us-east-1a	private network resource	X

When the target type is ip, you can specify IP addresses from one of the following CIDR blocks:

- 10.0.0.0 (RFC 1918)
- 100.64.0.0 (RFC 6598)
- 172.16.0.0 (RFC 1918)
- 192.168.0.0 (RFC 1918)
- The subnets of the VPC for the target group

These supported CIDR blocks enable you to register the following with a target group: ClassicLink instances, instances in a VPC that is peered to the load balancer VPC, AWS resources that are addressable by IP address and port (for example, databases), and on-premises resources linked to AWS through AWS Direct Connect or a VPN connection.

Take note that you can not specify publicly routable IP addresses. If you specify targets using an instance ID, traffic is routed to instances using the primary private IP address specified in the primary network interface for the instance. If you specify targets using IP addresses, you can route traffic to an instance using any private IP address from one or more network interfaces. This enables multiple applications on an instance to use the same port. Each network interface can have its own security group.

Hence, the correct answers are the following options:

- Use an Application Elastic Load balancer with Weighted Target Groups to divert and proportion the traffic between the on-premises and AWS-hosted application. Divert 50% of the traffic to the new application in AWS and the other 50% to the application hosted in their on-premises infrastructure.
- Use Route 53 with Weighted routing policy to divert the traffic between the on-premises and AWShosted application. Divert 50% of the traffic to the new application in AWS and the other 50% to the application hosted in their on-premises infrastructure.

The option that says: Use a Network Load balancer with Weighted Target Groups to divert the traffic between the on-premises and AWS-hosted application. Divert 50% of the traffic to the new application in AWS and the other 50% to the application hosted in their on-premises infrastructure is incorrect because a Network Load balancer doesn't have Weighted Target Groups to divert the traffic between the onpremises and AWS-hosted application.

The option that says: Use Route 53 with Failover routing policy to divert and proportion the traffic between the on-premises and AWS-hosted application. Divert 50% of the traffic to the new application in AWS and the other 50% to the application hosted in their on-premises infrastructure is incorrect because you cannot divert and proportion the traffic between the on-premises and AWS-hosted application using Route 53 with Failover routing policy. This is primarily used if you want to configure active-passive failover to your application architecture.

The option that says: Use AWS Global Accelerator to divert and proportion the HTTP and HTTPS traffic between the on-premises and AWS-hosted application. Ensure that the on-premises network has an AnyCast static IP address and is connected to your VPC via a Direct Connect Gateway is incorrect because although you can control the proportion of traffic directed to each endpoint using AWS Global Accelerator by assigning weights across the endpoints, it is still wrong to use a

Direct Connect Gateway and an AnyCast IP address since these are not required at all. You can only associate static IP addresses provided by AWS Global Accelerator to regional AWS resources or endpoints, such as Network Load Balancers, Application Load Balancers, EC2 Instances, and Elastic IP addresses. Take note that a Direct Connect Gateway, per se, doesn't establish a connection from your on-premises network to your Amazon VPCs. It simply enables you to use your AWS Direct Connect connection to connect to two or more VPCs that are located in different AWS Regions.

References:

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

<https://aws.amazon.com/blogs/aws/new-application-load-balancer-simplifies-deployment-with-weighted-target-groups/>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html>

Check out this Amazon Route 53 Cheat Sheet:

<https://tutorialsdojo.com/amazon-route-53/>

---

### QUESTION 261

An application is hosted in an On-Demand EC2 instance and is using Amazon SDK to communicate to other AWS services such as S3, DynamoDB, and many others. As part of the upcoming IT audit, you need to ensure that all API calls to your AWS resources are logged and durably stored.

Which is the most suitable service that you should use to meet this requirement?

- A. AWS X-Ray
- B. Amazon CloudWatch
- C. Amazon API Gateway
- D. AWS CloudTrail

Answer: D

Explanation:

AWS CloudTrail increases visibility into your user and resource activity by recording AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred.

Amazon CloudWatch is incorrect because this is primarily used for systems monitoring based on the server metrics. It does not have the capability to track API calls to your AWS resources.

AWS X-Ray is incorrect because this is usually used to debug and analyze your microservices applications with request tracing so you can find the root cause of issues and performance. Unlike CloudTrail, it does not record the API calls that were made to your AWS resources.

Amazon API Gateway is incorrect because this is not used for logging each and every API call to your AWS resources. It is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale.

Reference:

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

Check out this AWS CloudTrail Cheat Sheet:

<https://tutorialsdojo.com/aws-cloudtrail/>

---

### QUESTION 262

A Solutions Architect is working for a multinational telecommunications company. The IT Manager wants to consolidate their log streams including the access, application, and security logs in one single system.

Once consolidated, the company will analyze these logs in real-time based on heuristics. There will be some time in the future where the company will need to validate heuristics, which requires going back to data samples extracted from the last 12 hours.

What is the best approach to meet this requirement?

- A. First, configure Amazon Cloud Trail to receive custom logs and then use EMR to apply heuristics on the logs.
- B. First, send all the log events to Amazon SQS then set up an Auto Scaling group of EC2 servers to consume the logs and finally, apply the heuristics.
- C. First, set up an Auto Scaling group of EC2 servers then store the logs on Amazon S3 then finally, use EMR to apply

heuristics on the logs.

D. First, send all of the log events to Amazon Kinesis then afterwards, develop a client process to apply heuristics on the logs.

Answer: D

Explanation:

In this scenario, you need a service that can collect, process, and analyze data in real-time hence, the right service to use here is Amazon Kinesis.

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. Amazon Kinesis offers key capabilities to costeffectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of your application.



With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications. Amazon Kinesis enables you to process and analyze data as it arrives and respond instantly instead of having to wait until all your data is collected before the processing can begin.

All other options are incorrect since these services do not have real-time processing capability, unlike Amazon Kinesis.

Reference:

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

Check out this Amazon Kinesis Cheat Sheet:

<https://tutorialsdojo.com/amazon-kinesis/>

---

## QUESTION 263

A leading media company has recently adopted a hybrid cloud architecture which requires them to migrate their application servers and databases in AWS. One of their applications requires a heterogeneous database migration in which you need to transform your on-premises Oracle database to PostgreSQL in AWS. This entails a schema and code transformation before the proper data migration starts.

Which of the following options is the most suitable approach to migrate the database in AWS?

- A. First, use the AWS Schema Conversion Tool to convert the source schema and application code to match that of the target database, and then use the AWS Database Migration Service to migrate data from the source database to the target database.
- B. Configure a Launch Template that automatically converts the source schema and code to match that of the target database. Then, use the AWS Database Migration Service to migrate data from the source database to the target database.
- C. Use Amazon Neptune to convert the source schema and code to match that of the target database in RDS. Use the AWS Batch to effectively migrate the data from the source database to the target database in a batch process.
- D. Heterogeneous database migration is not supported in AWS. You have to transform your database first to PostgreSQL and then migrate it to RDS.

Answer: A

Explanation:

AWS Database Migration Service helps you migrate databases to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. The AWS Database Migration Service can migrate your data to and from most widely used commercial and open-source databases.

AWS Database Migration Service can migrate your data to and from most of the widely used commercial and open source

databases. It supports homogeneous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different database platforms, such as Oracle to Amazon Aurora.

Migrations can be from on-premises databases to Amazon RDS or Amazon EC2, databases running on EC2 to RDS, or vice versa, as well as from one RDS database to another RDS database. It can also move data between SQL, NoSQL, and text based targets.

In heterogeneous database migrations the source and target databases engines are different, like in the case of Oracle to Amazon Aurora, Oracle to PostgreSQL, or Microsoft SQL Server to MySQL migrations.

In this case, the schema structure, data types, and database code of source and target databases can be quite different, requiring a schema and code transformation before the data migration starts. That makes heterogeneous migrations a two step process. First use the AWS Schema Conversion Tool to convert the source schema and code to match that of the target database, and then use the AWS Database Migration Service to migrate data from the source database to the target database. All the required data type conversions will automatically be done by the AWS Database Migration Service during the migration. The source database can be located in your own premises outside of AWS, running on an Amazon EC2 instance, or it can be an Amazon RDS database. The target can be a database in Amazon EC2 or Amazon RDS.

The option that says: Configure a Launch Template that automatically converts the source schema and code to match that of the target database. Then, use the AWS Database Migration Service to migrate data from the source database to the target database is incorrect because Launch templates are primarily used in EC2 to enable you to store launch parameters so that you do not have to specify them every time you launch an instance.

The option that says: Use Amazon Neptune to convert the source schema and code to match that of the target database in RDS. Use the AWS Batch to effectively migrate the data from the source database to the target database in a batch process is incorrect because Amazon Neptune is a fully-managed graph database service and not a suitable service to use to convert the source schema. AWS Batch is not a database migration service and hence, it is not suitable to be used in this scenario. You should use the AWS Schema Conversion Tool and AWS Database Migration Service instead.

The option that says: Heterogeneous database migration is not supported in AWS. You have to transform your database first to PostgreSQL and then migrate it to RDS is incorrect because heterogeneous database migration is supported in AWS using the Database Migration Service.

References:

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

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

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

Check out this AWS Database Migration Service Cheat Sheet:

<https://tutorialsdojo.com/aws-database-migration-service/>

AWS Migration Services Overview:

<https://www.youtube.com/watch?v=yqNBkFMnsL8>

---

## QUESTION 264

A company has a running m5ad.large EC2 instance with a default attached 75 GB SSD instance-store backed volume. You shut it down and then start the instance. You noticed that the data which you have saved earlier on the attached volume is no longer available.

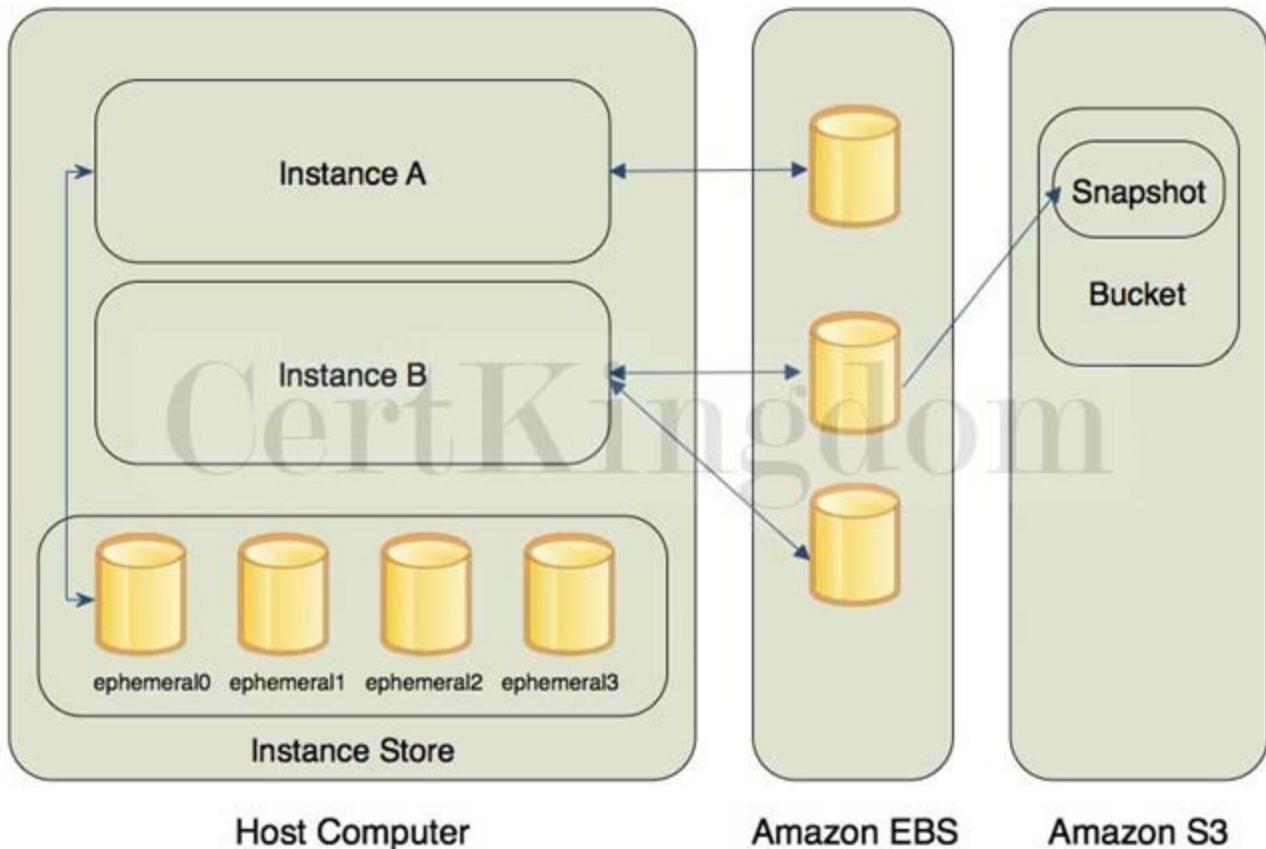
What might be the cause of this?

- A. The instance was hit by a virus that wipes out all data.
- B. The EC2 instance was using EBS backed root volumes, which are ephemeral and only live for the life of the instance.
- C. The EC2 instance was using instance store volumes, which are ephemeral and only live for the life of the instance.
- D. The volume of the instance was not big enough to handle all of the processing data.

Answer: C

Explanation:

An instance store provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers.



An instance store consists of one or more instance store volumes exposed as block devices. The size of an instance store as well as the number of devices available varies by instance type. While an instance store is dedicated to a particular instance, the disk subsystem is shared among instances on a host computer.

The data in an instance store persists only during the lifetime of its associated instance. If an instance reboots (intentionally or unintentionally), data in the instance store persists. However, data in the instance store is lost under the following circumstances:

- The underlying disk drive fails
- The instance stops
- The instance terminates

Reference:

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

Amazon EC2 Overview:

[https://www.youtube.com/watch?v=7VsGIHT\\_jQE](https://www.youtube.com/watch?v=7VsGIHT_jQE)

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

## QUESTION 265

A data analytics startup is collecting clickstream data and stores them in an S3 bucket. You need to launch an AWS Lambda function to trigger the ETL jobs to run as soon as new data becomes available in Amazon S3.

Which of the following services can you use as an extract, transform, and load (ETL) service in this scenario?

- A. S3 Select
- B. AWS Step Functions
- C. AWS Glue
- D. Redshift Spectrum

Answer: C

Explanation:

AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. You can create and run an ETL job with a few clicks in the AWS Management Console. You simply point AWS Glue to your data stored on AWS, and AWS Glue discovers your data and stores the associated metadata

(e.g. table definition and schema) in the AWS Glue Data Catalog. Once cataloged, your data is immediately searchable, queryable, and available for ETL. AWS Glue generates the code to execute your data transformations and data loading processes.



Reference:

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

Check out this AWS Glue Cheat Sheet:

<https://tutorialsdojo.com/aws-glue/>

## QUESTION 266

A company is planning to launch a High Performance Computing (HPC) cluster in AWS that does Computational Fluid Dynamics (CFD) simulations. The solution should scale-out their simulation jobs to experiment with more tunable parameters for faster and more accurate results. The cluster is composed of Windows servers hosted on t3a.medium EC2 instances. As the Solutions Architect, you should ensure that the architecture provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies.

Which is the MOST suitable and cost-effective solution that the Architect should implement to achieve the above requirements?

- A. Enable Enhanced Networking with Intel 82599 Virtual Function (VF) interface on the Windows EC2 Instances.
- B. Enable Enhanced Networking with Elastic Fabric Adapter (EFA) on the Windows EC2 Instances.
- C. Enable Enhanced Networking with Elastic Network Adapter (ENA) on the Windows EC2 Instances.
- D. Use AWS ParallelCluster to deploy and manage the HPC cluster to provide higher bandwidth, higher packet per second (PPS) performance, and lower inter-instance latencies.

Answer: C

Explanation:

Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types. SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies. There is no additional charge for using enhanced networking.

```

Administrator: Windows PowerShell (x86)
PS C:\Users\Administrator> aws ec2 modify-instance-attribute --instance-id i-0227930417944257a --ena-support

```

Amazon EC2 provides enhanced networking capabilities through the Elastic Network Adapter (ENA). It supports network speeds of up to 100 Gbps for supported instance types. Elastic Network Adapters (ENAs) provide traditional IP networking features that are required to support VPC networking.

An Elastic Fabric Adapter (EFA) is simply an Elastic Network Adapter (ENA) with added capabilities. It provides all of the functionality of an ENA, with additional OS-bypass functionality. OS-bypass is an access model that allows HPC and machine learning applications to communicate directly with the network interface hardware to provide low-latency, reliable transport functionality.

The OS-bypass capabilities of EFAs are not supported on Windows instances. If you attach an EFA to a Windows instance, the instance functions as an Elastic Network Adapter, without the added EFA capabilities.

Hence, the correct answer is to enable Enhanced Networking with Elastic Network Adapter (ENA) on the Windows EC2 Instances.

Enabling Enhanced Networking with Elastic Fabric Adapter (EFA) on the Windows EC2 Instances is incorrect because the OS-bypass capabilities of the Elastic Fabric Adapter (EFA) are not supported on Windows instances. Although you can attach EFA to your Windows instances, this will just act as a regular Elastic Network Adapter, without the added EFA capabilities. Moreover, it doesn't support the t3a.medium instance type that is being used in the HPC cluster.

Enabling Enhanced Networking with Intel 82599 Virtual Function (VF) interface on the Windows EC2 Instances is incorrect because although you can attach an Intel 82599 Virtual Function (VF) interface on your Windows EC2 Instances to improve its networking capabilities, it doesn't support the t3a.medium instance type that is being used in the HPC cluster.

Using AWS ParallelCluster to deploy and manage the HPC cluster to provide higher bandwidth, higher packet per second (PPS) performance, and lower inter-instance latencies is incorrect because an AWS ParallelCluster is just 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. It does not provide higher bandwidth, higher packet per second (PPS) performance, and lower inter-instance latencies, unlike ENA or EFA.

#### References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html>

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

## QUESTION 267

An online shopping platform is hosted on an Auto Scaling group of On-Demand EC2 instances with a default Auto Scaling termination policy and no instance protection configured. The system is deployed across three Availability Zones in the US West region (us-west-1) with an Application Load Balancer in front to provide high availability and fault tolerance for the shopping platform. The us-west-1a, uswest-1b, and us-west-1c Availability Zones have 10, 8 and 7 running instances respectively. Due to the low number of incoming traffic, the scale-in operation has been triggered.

Which of the following will the Auto Scaling group do to determine which instance to terminate first in this scenario? (Select THREE.)

- A. Select the instance that is farthest to the next billing hour.
- B. Choose the Availability Zone with the least number of instances, which is the us-west-1c Availability Zone in this scenario.
- C. Select the instances with the oldest launch configuration.
- D. Select the instances with the most recent launch configuration.
- E. Choose the Availability Zone with the most number of instances, which is the us-west-1a Availability Zone in this scenario.
- F. Select the instance that is closest to the next billing hour.

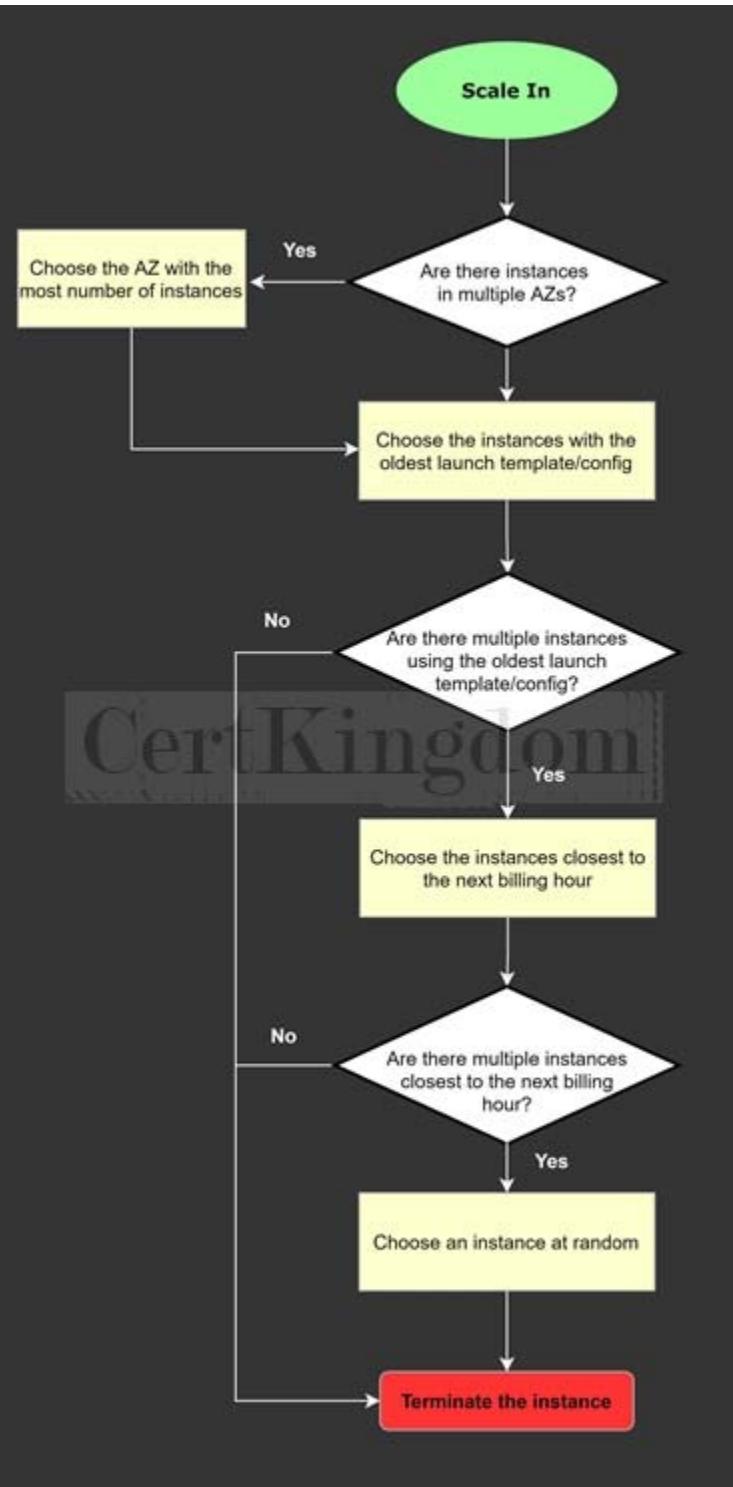
Answer: C,E,F

## 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:



## Reference:

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

n-policy

Check out this AWS Auto Scaling Cheat Sheet:

<https://tutorialsdojo.com/aws-auto-scaling/>

---

## QUESTION 268

In a startup company you are working for, you are asked to design a web application that requires a NoSQL database that has no limit on the storage size for a given table. The startup is still new in the market and it has very limited human resources who can take care of the database infrastructure.

Which is the most suitable service that you can implement that provides a fully managed, scalable and highly available NoSQL service?

- A. SimpleDB
- B. Amazon Aurora
- C. Amazon Neptune
- D. DynamoDB

Answer: D

Explanation:

The term "fully managed" means that Amazon will manage the underlying infrastructure of the service hence, you don't need an additional human resource to support or maintain the service. Therefore, Amazon DynamoDB is the right answer. Remember that Amazon RDS is a managed service but not "fully managed" as you still have the option to maintain and configure the underlying server of the database.

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed cloud database and supports both document and key-value store models. Its flexible data model, reliable performance, and automatic scaling of throughput capacity make it a great fit for mobile, web, gaming, ad tech, IoT, and many other applications.

Amazon Neptune is incorrect because this is primarily used as a graph database.

Amazon Aurora is incorrect because this is a relational database and not a NoSQL database.

SimpleDB is incorrect. Although SimpleDB is also a highly available and scalable NoSQL database, it has a limit on the request capacity or storage size for a given table, unlike DynamoDB.

Reference:

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

Check out this Amazon DynamoDB Cheat Sheet:

<https://tutorialsdojo.com/amazon-dynamodb/>

Amazon DynamoDB Overview:

<https://www.youtube.com/watch?v=3ZOyUNIeorU>

---

## QUESTION 269

A web application is hosted on an EC2 instance that processes sensitive financial information which is launched in a private subnet. All of the data are stored in an Amazon S3 bucket. Financial information is accessed by users over the Internet. The security team of the company is concerned that the Internet connectivity to Amazon S3 is a security risk.

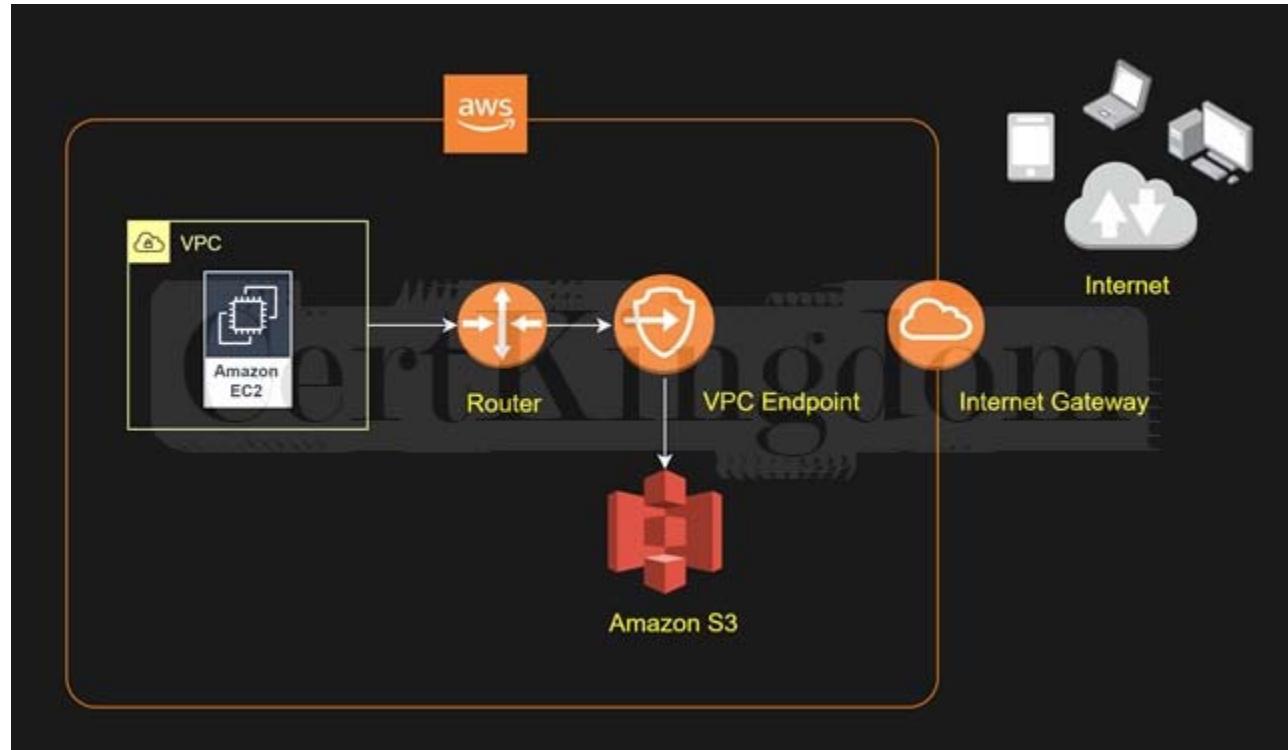
In this scenario, what will you do to resolve this security vulnerability in the most cost-effective manner?

- A. Change the web architecture to access the financial data in S3 through an interface VPC endpoint, which is powered by AWS PrivateLink.
- B. Change the web architecture to access the financial data in your S3 bucket through a VPN connection.
- C. Change the web architecture to access the financial data hosted in your S3 bucket by creating a custom VPC endpoint service.
- D. Change the web architecture to access the financial data through a Gateway VPC Endpoint.

Answer: D

Explanation:

Take note that your VPC lives within a larger AWS network and the services, such as S3, DynamoDB, RDS, and many others, are located outside of your VPC, but still within the AWS network. By default, the connection that your VPC uses to connect to your S3 bucket or any other service traverses the public Internet via your Internet Gateway. A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, 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.



There are two types of VPC endpoints: interface endpoints and gateway endpoints. You have to create the type of VPC endpoint required by the supported service.

An interface endpoint is an elastic network interface with a private IP address that serves as an entry point for traffic destined to a supported service. A gateway endpoint is a gateway that is a target for a specified route in your route table, used for traffic destined to a supported AWS service.

Gateway endpoints for Amazon S3	Interface endpoints for Amazon S3
In both cases, your network traffic remains on the AWS network.	
Use Amazon S3 public IP addresses	Use private IP addresses from your VPC to access Amazon S3
Does not allow access from on premises	Allow access from on premises
Does not allow access from another AWS Region	Allow access from a VPC in another AWS Region using VPC peering or AWS Transit Gateway
Not billed	Billed

Hence, the correct answer is: Change the web architecture to access the financial data through a Gateway VPC Endpoint. The option that says: Changing the web architecture to access the financial data in your S3 bucket through a VPN connection is incorrect because a VPN connection still goes through the public Internet.

You have to use a VPC Endpoint in this scenario and not VPN, to privately connect your VPC to supported AWS services such as S3.

The option that says: Changing the web architecture to access the financial data hosted in your S3 bucket by creating a custom VPC endpoint service is incorrect because a "VPC endpoint service" is quite different from a "VPC endpoint". With the VPC endpoint service, you are the service provider where you can create your own application in your VPC and configure it as an AWS PrivateLink-powered service (referred to as an endpoint service). Other AWS principals can create a connection from their VPC to your endpoint service using an interface VPC endpoint.

The option that says: Changing the web architecture to access the financial data in S3 through an interface VPC endpoint, which is powered by AWS PrivateLink is incorrect. Although you can use an Interface VPC Endpoint to satisfy the requirement, this type entails an associated cost, unlike a Gateway VPC Endpoint. Remember that you won't get billed if you use a Gateway VPC endpoint for your Amazon S3 bucket, unlike an Interface VPC endpoint that is billed for hourly usage

and data processing charges.

Take note that the scenario explicitly asks for the most cost-effective solution.

References:

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html>

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

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

---

## QUESTION 270

An e-commerce application is using a fanout messaging pattern for its order management system. For every order, it sends an Amazon SNS message to an SNS topic, and the message is replicated and pushed to multiple Amazon SQS queues for parallel asynchronous processing. A Spot EC2 instance retrieves the message from each SQS queue and processes the message. There was an incident that while an EC2 instance is currently processing a message, the instance was abruptly terminated, and the processing was not completed in time.

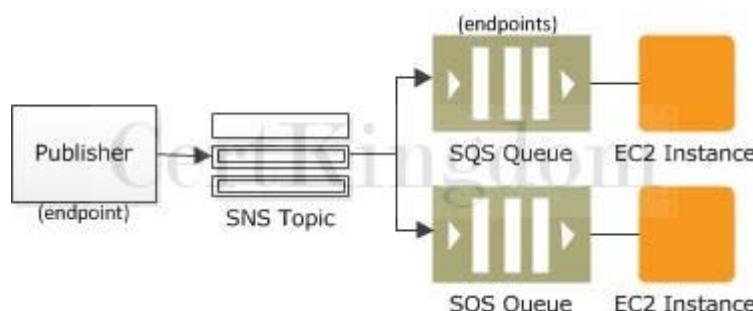
In this scenario, what happens to the SQS message?

- A. The message is deleted and becomes duplicated in the SQS when the EC2 instance comes online.
- B. When the message visibility timeout expires, the message becomes available for processing by other EC2 instances
- C. The message will automatically be assigned to the same EC2 instance when it comes back online within or after the visibility timeout.
- D. The message will be sent to a Dead Letter Queue in AWS DataSync.

Answer: B

Explanation:

A "fanout" pattern is when an Amazon SNS message is sent to a topic and then replicated and pushed to multiple Amazon SQS queues, HTTP endpoints, or email addresses. This allows for parallel asynchronous processing. For example, you could develop an application that sends an Amazon SNS message to a topic whenever an order is placed for a product. Then, the Amazon SQS queues that are subscribed to that topic would receive identical notifications for the new order. The Amazon EC2 server instance attached to one of the queues could handle the processing or fulfillment of the order, while the other server instance could be attached to a data warehouse for analysis of all orders received.



When a consumer receives and processes a message from a queue, the message remains in the queue. Amazon SQS doesn't automatically delete the message. Because Amazon SQS is a distributed system, there's no guarantee that the consumer actually receives the message (for example, due to a connectivity issue, or due to an issue in the consumer application). Thus, the consumer must delete the message from the queue after receiving and processing it.

Immediately after the message is received, it remains in the queue. To prevent other consumers from processing the message again, Amazon SQS sets a visibility timeout, a period of time during which Amazon SQS prevents other consumers from receiving and processing the message. The default visibility timeout for a message is 30 seconds. The maximum is 12 hours. The option that says: The message will automatically be assigned to the same EC2 instance when it comes back online within or after the visibility timeout is incorrect because the message will not be automatically assigned to the same EC2 instance once it is abruptly terminated. When the message visibility timeout expires, the message becomes available for processing by other EC2 instances.

The option that says: The message is deleted and becomes duplicated in the SQS when the EC2 instance comes online is incorrect because the message will not be deleted and won't be duplicated in the SQS queue when the EC2 instance comes online.

The option that says: The message will be sent to a Dead Letter Queue in AWS DataSync is incorrect because although the

message could be programmatically sent to a Dead Letter Queue (DLQ), it won't be handled by AWS DataSync but by Amazon SQS instead. AWS DataSync is primarily used to simplify your migration with AWS. It makes it simple and fast to move large amounts of data online between onpremises storage and Amazon S3 or Amazon Elastic File System (Amazon EFS).

References:

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

<https://docs.aws.amazon.com/sns/latest/dg/sns-common-scenarios.html>

Check out this Amazon SQS Cheat Sheet:

<https://tutorialsdojo.com/amazon-sqs/>

---

## QUESTION 271

An investment bank has a distributed batch processing application which is hosted in an Auto Scaling group of Spot EC2 instances with an SQS queue. You configured your components to use client-side buffering so that the calls made from the client will be buffered first and then sent as a batch request to SQS. What is a period of time during which the SQS queue prevents other consuming components from receiving and processing a message?

- A. Processing Timeout
- B. Visibility Timeout
- C. Receiving Timeout
- D. Component Timeout

Answer: B

Explanation:

The visibility timeout is a period of time during which Amazon SQS prevents other consuming components from receiving and processing a message.

When a consumer receives and processes a message from a queue, the message remains in the queue. Amazon SQS doesn't automatically delete the message. Because Amazon SQS is a distributed system, there's no guarantee that the consumer actually receives the message (for example, due to a connectivity issue, or due to an issue in the consumer application).

Thus, the consumer must delete the message from the queue after receiving and processing it.

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

References:

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

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

Check out this Amazon SQS Cheat Sheet:

<https://tutorialsdojo.com/amazon-sqs/>

---

## QUESTION 272

A Solutions Architect needs to ensure that all of the AWS resources in Amazon VPC don't go beyond their respective service limits. The Architect should prepare a system that provides real-time guidance in provisioning resources that adheres to the AWS best practices.

Which of the following is the MOST appropriate service to use to satisfy this task?

- A. Amazon Inspector
- B. AWS Trusted Advisor
- C. AWS Cost Explorer
- D. AWS Budgets

Answer: B

Explanation:

AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. It inspects your AWS environment and makes recommendations for saving money, improving system performance and reliability, or closing security gaps.

Whether establishing new workflows, developing applications, or as part of ongoing improvement, take advantage of the recommendations provided by Trusted Advisor on a regular basis to help keep your solutions provisioned optimally.



Trusted Advisor includes an ever-expanding list of checks in the following five categories:

- Cost Optimization – recommendations that can potentially save you money by highlighting unused resources and opportunities to reduce your bill.

Security – identification of security settings that could make your AWS solution less secure.

Fault Tolerance – recommendations that help increase the resiliency of your AWS solution by highlighting redundancy shortfalls, current service limits, and over-utilized resources.

Performance – recommendations that can help to improve the speed and responsiveness of your applications.

Service Limits – recommendations that will tell you when service usage is more than 80% of the service limit.

Hence, the correct answer in this scenario is AWS Trusted Advisor.

AWS Cost Explorer is incorrect because this is just a tool that enables you to view and analyze your costs and usage. You can explore your usage and costs using the main graph, the Cost Explorer cost and usage reports, or the Cost Explorer RI reports. It has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time.

AWS Budgets is incorrect because it simply gives you the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. You can also use AWS Budgets to set reservation utilization or coverage targets and receive alerts when your utilization drops below the threshold you define.

Amazon Inspector is incorrect because it is just an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices.

References:

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/>

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/faqs/>

Check out this AWS Trusted Advisor Cheat Sheet:

<https://tutorialsdojo.com/aws-trusted-advisor/>

## QUESTION 273

A client is hosting their company website on a cluster of web servers that are behind a public-facing load balancer. The client also uses Amazon Route 53 to manage their public DNS.

How should the client configure the DNS zone apex record to point to the load balancer?

- A. Create a CNAME record pointing to the load balancer DNS name.

- B. Create an A record aliased to the load balancer DNS name.

C. Create an alias for CNAME record to the load balancer DNS name.

D. Create an A record pointing to the IP address of the load balancer.

Answer: B

Explanation:

Route 53's DNS implementation connects user requests to infrastructure running inside (and outside) of Amazon Web Services (AWS). For example, if you have multiple web servers running on EC2 instances behind an Elastic Load Balancing load balancer, Route 53 will route all traffic addressed to your website (e.g. www.tutorialsdojo.com) to the load balancer DNS name (e.g. elbtutorialsdojo123.elb.amazonaws.com).



Additionally, Route 53 supports the alias resource record set, which lets you map your zone apex (e.g. tutorialsdojo.com) DNS name to your load balancer DNS name. IP addresses associated with Elastic Load Balancing can change at any time due to scaling or software updates. Route 53 responds to each request for an Alias resource record set with one IP address for the load balancer.

Creating an A record pointing to the IP address of the load balancer is incorrect. You should be using an Alias record pointing to the DNS name of the load balancer since the IP address of the load balancer can change at any time.

Creating a CNAME record pointing to the load balancer DNS name and creating an alias for CNAME record to the load balancer DNS name are incorrect because CNAME records cannot be created for your zone apex. You should create an alias record at the top node of a DNS namespace which is also known as the zone apex. For example, if you register the DNS name tutorialsdojo.com, the zone apex is tutorialsdojo.com. You can't create a CNAME record directly for tutorialsdojo.com, but you can create an alias record for tutorialsdojo.com that routes traffic to www.tutorialsdojo.com.

References:

<http://docs.aws.amazon.com/govcloud-us/latest/UserGuide/setting-up-route53-zoneapex-elb.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-nonalias.html>

Check out this Amazon Route 53 Cheat Sheet:

<https://tutorialsdojo.com/amazon-route-53/>

## QUESTION 274

An organization plans to run an application in a dedicated physical server that doesn't use virtualization.

The application data will be stored in a storage solution that uses an NFS protocol. To prevent data loss, you need to use a durable cloud storage service to store a copy of your data.

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

A. Use an AWS Storage Gateway hardware appliance for your compute resources. Configure Volume Gateway to store the application data and backup data.

B. Use an AWS Storage Gateway hardware appliance for your compute resources. Configure File Gateway to store the application data and create an Amazon S3 bucket to store a backup of your data.

C. Use an AWS Storage Gateway hardware appliance for your compute resources. Configure Volume Gateway to store the

application data and create an Amazon S3 bucket to store a backup of your data.

D. Use AWS Storage Gateway with a gateway VM appliance for your compute resources. Configure File Gateway to store the application data and backup data.

Answer: B

Explanation:

AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage by linking it to S3. Storage Gateway provides 3 types of storage solutions for your on-premises applications: file, volume, and tape gateways. The AWS Storage Gateway Hardware Appliance is a physical, standalone, validated server configuration for on-premises deployments.



The AWS Storage Gateway Hardware Appliance is a physical hardware appliance with the Storage Gateway software preinstalled on a validated server configuration. The hardware appliance is a high-performance 1U server that you can deploy in your data center, or on-premises inside your corporate firewall. When you buy and activate your hardware appliance, the activation process associates your hardware appliance with your AWS account. After activation, your hardware appliance appears in the console as a gateway on the Hardware page. You can configure your hardware appliance as a file gateway, tape gateway, or volume gateway type. The procedure that you use to deploy and activate these gateway types on a hardware appliance is the same as on a virtual platform.

Since the company needs to run a dedicated physical appliance, you can use an AWS Storage Gateway Hardware Appliance. It comes pre-loaded with Storage Gateway software, and provides all the required resources to create a file gateway. A file gateway can be configured to store and retrieve objects in Amazon S3 using the protocols NFS and SMB.

Hence, the correct answer in this scenario is: Use an AWS Storage Gateway hardware appliance for your compute resources. Configure File Gateway to store the application data and create an Amazon S3 bucket to store a backup of your data.

The option that says: Use AWS Storage Gateway with a gateway VM appliance for your compute resources. Configure File Gateway to store the application data and backup data is incorrect because as per the scenario, the company needs to use an on-premises hardware appliance and not just a Virtual Machine (VM).

The options that say: Use an AWS Storage Gateway hardware appliance for your compute resources.

Configure Volume Gateway to store the application data and backup data and Use an AWS Storage Gateway hardware appliance for your compute resources. Configure Volume Gateway to store the application data and create an Amazon S3 bucket to store a backup of your data are both incorrect. As per the scenario, the requirement is a file system that uses an NFS protocol and not iSCSI devices.

Among the AWS Storage Gateway storage solutions, only file gateway can store and retrieve objects in Amazon S3 using the protocols NFS and SMB.

References:

<https://docs.aws.amazon.com/storagegateway/latest/userguide/hardware-appliance.html>

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

AWS Storage Gateway Overview:

<https://www.youtube.com/watch?v=pNb7xOBJjHE>

Check out this AWS Storage Gateway Cheat Sheet:

<https://tutorialsdojo.com/aws-storage-gateway/>

## QUESTION 275

A Solutions Architect joined a large tech company with an existing Amazon VPC. When reviewing the Auto Scaling events, the Architect noticed that their web application is scaling up and down multiple times within the hour.

What design change could the Architect make to optimize cost while preserving elasticity?

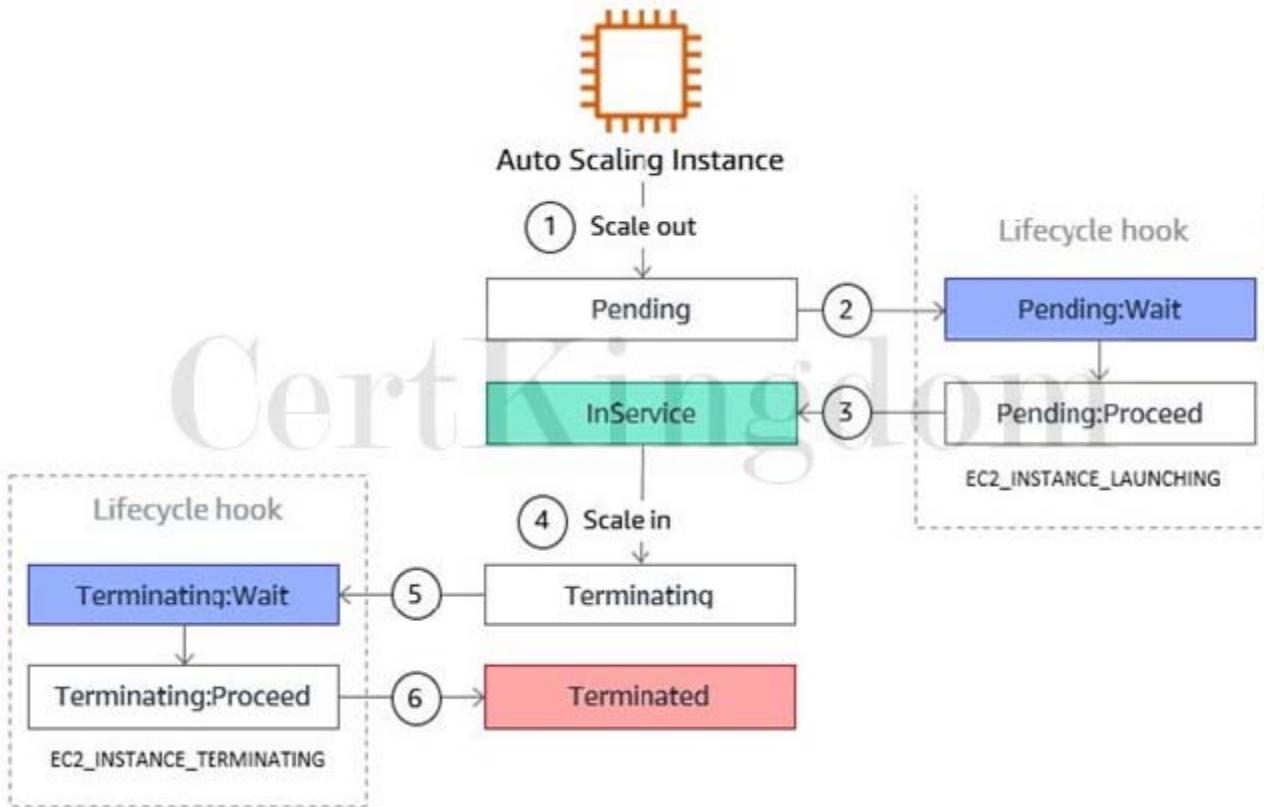
- A. Increase the instance type in the launch configuration

- B. Add provisioned IOPS to the instances
- C. Change the cooldown period of the Auto Scaling group and set the CloudWatch metric to a higher threshold
- D. Increase the base number of Auto Scaling instances for the Auto Scaling group

Answer: C

Explanation:

Since the application is scaling up and down multiple times within the hour, the issue lies on the cooldown period of the Auto Scaling group.



The cooldown period is a configurable setting for your Auto Scaling group that helps to ensure that it doesn't launch or terminate additional instances before the previous scaling activity takes effect. After the Auto Scaling group dynamically scales using a simple scaling policy, it waits for the cooldown period to complete before resuming scaling activities. When you manually scale your Auto Scaling group, the default is not to wait for the cooldown period, but you can override the default and honor the cooldown period. If an instance becomes unhealthy, the Auto Scaling group does not wait for the cooldown period to complete before replacing the unhealthy instance.

Reference:

<http://docs.aws.amazon.com/autoscaling/latest/userguide/as-scale-based-on-demand.html>

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

## QUESTION 276

A company troubleshoots the operational issues of their cloud architecture by logging the AWS API call history of all AWS resources. The Solutions Architect must implement a solution to quickly identify the most recent changes made to resources in their environment, including creation, modification, and deletion of AWS resources. One of the requirements is that the generated log files should be encrypted to avoid any security issues.

Which of the following is the most suitable approach to implement the encryption?

- A. Use CloudTrail and configure the destination Amazon Glacier archive to use Server-Side Encryption (SSE).
- B. Use CloudTrail and configure the destination S3 bucket to use Server-Side Encryption (SSE).
- C. Use CloudTrail and configure the destination S3 bucket to use Server Side Encryption (SSE) with AES-128 encryption algorithm.
- D. Use CloudTrail with its default settings

Answer: D

Explanation:

By default, CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encrypt your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about log file delivery and validation, you can set up Amazon SNS notifications.



Using CloudTrail and configuring the destination Amazon Glacier archive to use Server-Side Encryption (SSE) is incorrect because CloudTrail stores the log files to S3 and not in Glacier. Take note that by default, CloudTrail event log files are already encrypted using Amazon S3 server-side encryption (SSE).

Using CloudTrail and configuring the destination S3 bucket to use Server-Side Encryption (SSE) is incorrect because CloudTrail event log files are already encrypted using the Amazon S3 server-side encryption (SSE) which is why you do not have to do this anymore.

Use CloudTrail and configure the destination S3 bucket to use Server Side Encryption (SSE) with AES-128 encryption algorithm is incorrect because Cloudtrail event log files are already encrypted using the Amazon S3 server-side encryption (SSE) by default. Additionally, SSE-S3 only uses the AES-256 encryption algorithm and not the AES-128.

References:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/how-cloudtrail-works.html>

<https://aws.amazon.com/blogs/aws/category/cloud-trail/>

Check out this AWS CloudTrail Cheat Sheet:

<https://tutorialsdojo.com/aws-cloudtrail/>

## QUESTION 277

A health organization is using a large Dedicated EC2 instance with multiple EBS volumes to host its health records web application. The EBS volumes must be encrypted due to the confidentiality of the data that they are handling and also to comply with the HIPAA (Health Insurance Portability and Accountability Act) standard.

In EBS encryption, what service does AWS use to secure the volume's data at rest? (Select TWO.)

- A. By using the SSL certificates provided by the AWS Certificate Manager (ACM).
- B. By using S3 Server-Side Encryption.
- C. By using a password stored in CloudHSM.
- D. By using your own keys in AWS Key Management Service (KMS).
- E. By using S3 Client-Side Encryption.
- F. By using Amazon-managed keys in AWS Key Management Service (KMS).

Answer: D,F

Explanation:

Amazon EBS encryption offers seamless encryption of EBS data volumes, boot volumes, and snapshots, eliminating the need to build and maintain a secure key management infrastructure. EBS encryption enables data at rest security by encrypting your data using Amazon-managed keys, or keys you create and manage using the AWS Key Management Service (KMS). The encryption occurs on the servers that host EC2 instances, providing encryption of data as it moves between EC2 instances and EBS storage.

Hence, the correct answers are: using your own keys in AWS Key Management Service (KMS) and using Amazon-managed keys in AWS Key Management Service (KMS).

Using S3 Server-Side Encryption and using S3 Client-Side Encryption are both incorrect as these relate only to S3.

Using a password stored in CloudHSM is incorrect as you only store keys in CloudHSM and not passwords.

Using the SSL certificates provided by the AWS Certificate Manager (ACM) is incorrect as ACM only provides SSL certificates and not data encryption of EBS Volumes.

Reference:

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

Check out this Amazon EBS Cheat Sheet:

<https://tutorialsdojo.com/amazon-ebs/>

---

## QUESTION 278

A data analytics company keeps a massive volume of data that they store in their on-premises data center. To scale their storage systems, they are looking for cloud-backed storage volumes that they can mount using Internet Small Computer System Interface (iSCSI) devices from their on-premises application servers. They have an on-site data analytics application that frequently accesses the latest data subsets locally while the older data are rarely accessed. You are required to minimize the need to scale the on-premises storage infrastructure while still providing their web application with low-latency access to the data.

Which type of AWS Storage Gateway service will you use to meet the above requirements?

- A. Volume Gateway in cached mode
- B. Volume Gateway in stored mode
- C. Tape Gateway
- D. File Gateway

Answer: A

Explanation:

In this scenario, the technology company is looking for a storage service that will enable their analytics application to frequently access the latest data subsets and not the entire data set (as it was mentioned that the old data are rarely being used). This requirement can be fulfilled by setting up a Cached Volume Gateway in AWS Storage Gateway.

By using cached volumes, you can use Amazon S3 as your primary data storage, while retaining frequently accessed data locally in your storage gateway. Cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low-latency access to frequently accessed data. You can create storage volumes up to

32 TiB in size and afterward, attach these volumes as iSCSI devices to your on-premises application servers. When you write to these volumes, your gateway stores the data in Amazon S3. It retains the recently read data in your on-premises storage gateway's cache and uploads buffer storage.

Cached volumes can range from 1 GiB to 32 TiB in size and must be rounded to the nearest GiB. Each gateway configured for cached volumes can support up to 32 volumes for a total maximum storage volume of 1,024 TiB (1 PiB).

In the cached volumes solution, AWS Storage Gateway stores all your on-premises application data in a storage volume in Amazon S3. Hence, the correct answer is: Volume Gateway in cached mode.

Volume Gateway in stored mode is incorrect because the requirement is to provide low latency access to the frequently accessed data subsets locally. Stored Volumes are used if you need low-latency access to your entire dataset.

Tape Gateway is incorrect because this is just a cost-effective, durable, long-term offsite alternative for data archiving, which is not needed in this scenario.

File Gateway is incorrect because the scenario requires you to mount volumes as iSCSI devices. File Gateway is used to store and retrieve Amazon S3 objects through NFS and SMB protocols.

References:

<https://docs.aws.amazon.com/storagegateway/latest/userguide/StorageGatewayConcepts.html#volumegateway-concepts>

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

AWS Storage Gateway Overview:

<https://www.youtube.com/watch?v=pNb7xOBJjHE>

Check out this AWS Storage Gateway Cheat Sheet:

<https://tutorialsdojo.com/aws-storage-gateway/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

---

## QUESTION 279

A company has several microservices that send messages to an Amazon SQS queue and a backend application that poll the queue to process the messages. The company also has a Service Level Agreement (SLA) which defines the acceptable amount of time that can elapse from the point when the messages are received until a response is sent. The backend operations are I/O-intensive as the number of messages is constantly growing, causing the company to miss its SL.

A. The Solutions

Architect must implement a new architecture that improves the application's processing time and load management. Which of the following is the MOST effective solution that can satisfy the given requirement?

- A. Create an AMI of the backend application's EC2 instance. Use the image to set up an Auto Scaling group and configure a target tracking scaling policy based on the ApproximateAgeOfOldestMessage metric.
- B. Create an AMI of the backend application's EC2 instance. Use the image to set up an Auto Scaling group and configure a target tracking scaling policy based on the CPUUtilization metric with a target value of 80%.
- C. Create an AMI of the backend application's EC2 instance and replace it with a larger instance size.
- D. Create an AMI of the backend application's EC2 instance and launch it to a cluster placement group.

Answer: A

Explanation:

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message-oriented middleware and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.



The `ApproximateAgeOfOldestMessage` metric is useful when applications have time-sensitive messages and you need to ensure that messages are processed within a specific time period. You can use this metric to set Amazon CloudWatch alarms that issue alerts when messages remain in the queue for extended periods of time. You can also use alerts to take action, such as increasing the number of consumers to process messages more quickly.

With a target tracking scaling policy, you can scale (increase or decrease capacity) a resource based on a target value for a specific CloudWatch metric. To create a custom metric for this policy, you need to use AWS CLI or AWS SDKs. Take note that you need to create an AMI from the instance first before you can create an Auto Scaling group to scale the instances based on the `ApproximateAgeOfOldestMessage` metric.

Hence, the correct answer is: Create an AMI of the backend application's EC2 instance. Use the image to set up an Auto Scaling Group and configure a target tracking scaling policy based on the `ApproximateAgeOfOldestMessage` metric.

The option that says: Create an AMI of the backend application's EC2 instance. Use the image to set up an Auto Scaling Group and configure a target tracking scaling policy based on the `CPUUtilization` metric with a target value of 80% is incorrect. Although this will improve the backend processing, the scaling policy based on the `CPUUtilization` metric is not meant for time-sensitive messages where you need to ensure that the messages are processed within a specific time period. It will only trigger the scale-out activities based on the CPU Utilization of the current instances, and not based on the age of the message, which is a crucial factor in meeting the SL

A. To satisfy the requirement in the scenario, you should use the `ApproximateAgeOfOldestMessage` metric.

The option that says: Create an AMI of the backend application's EC2 instance and replace it with a larger instance size is incorrect because replacing the instance with a large size won't be enough to dynamically handle workloads at any level. You need to implement an Auto Scaling group to automatically adjust the capacity of your computing resources.

The option that says: Create an AMI of the backend application's EC2 instance and launch it to a cluster placement group is incorrect because a cluster placement group is just a logical grouping of EC2 instances. Instead of launching the instance in a placement group, you must set up an Auto Scaling group for your EC2 instances and configure a target tracking scaling policy based on the `ApproximateAgeOfOldestMessage` metric.

#### References:

<https://aws.amazon.com/about-aws/whats-new/08/new-amazon-cloudwatch-metric-for-amazon-sqs-monitors-the-age-of-the-oldest-message/>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-available-cloud-watch-metrics.html>

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

Check out this Amazon SQS Cheat Sheet:

<https://tutorialsdojo.com/amazon-sqs/>

## QUESTION 280

An operations team has an application running on EC2 instances inside two custom VPCs. The VPCs are located in the Ohio and N. Virginia Region respectively. The team wants to transfer data between the instances without traversing the public internet.

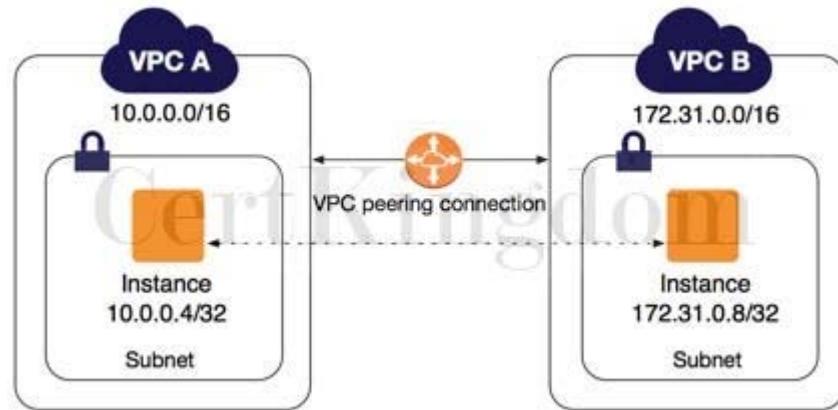
Which combination of steps will achieve this? (Select TWO.)

- A. Launch a NAT Gateway in the public subnet of each VPC.
- B. Create an Egress-only Internet Gateway.
- C. Deploy a VPC endpoint on each region to enable a private connection.
- D. Set up a VPC peering connection between the VPCs.
- E. Re-configure the route table's target and destination of the instances' subnet.

Answer: D,E

Explanation:

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).



Inter-Region VPC Peering provides a simple and cost-effective way to share resources between regions or replicate data for geographic redundancy. Built on the same horizontally scaled, redundant, and highly available technology that powers VPC today, Inter-Region VPC Peering encrypts inter-region traffic with no single point of failure or bandwidth bottleneck. Traffic using Inter-Region VPC Peering always stays on the global AWS backbone and never traverses the public internet, thereby reducing threat vectors, such as common exploits and DDoS attacks.

Hence, the correct answers are:

- Set up a VPC peering connection between the VPCs.
- Re-configure the route table's target and destination of the instances' subnet.

The option that says: Create an Egress only Internet Gateway is incorrect because this will just enable outbound IPv6 communication from instances in a VPC to the internet. Take note that the scenario requires private communication to be enabled between VPCs from two different regions.

The option that says: Launch a NAT Gateway in the public subnet of each VPC is incorrect because NAT Gateways are used to allow instances in private subnets to access the public internet. Note that the requirement is to make sure that communication between instances will not traverse the internet.

The option that says: Deploy a VPC endpoint on each region to enable private connection is incorrect. VPC endpoints are region-specific only and do not support inter-region communication.

References:

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

<https://aws.amazon.com/about-aws/whats-new/7/announcing-support-for-inter-region-vpc-peering/>

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

## QUESTION 281

A startup launched a fleet of on-demand EC2 instances to host a massively multiplayer online roleplaying game (MMORPG). The EC2 instances are configured with Auto Scaling and AWS Systems

Manager.  
What can be used to configure the EC2 instances without having to establish an RDP or SSH connection to each instance?

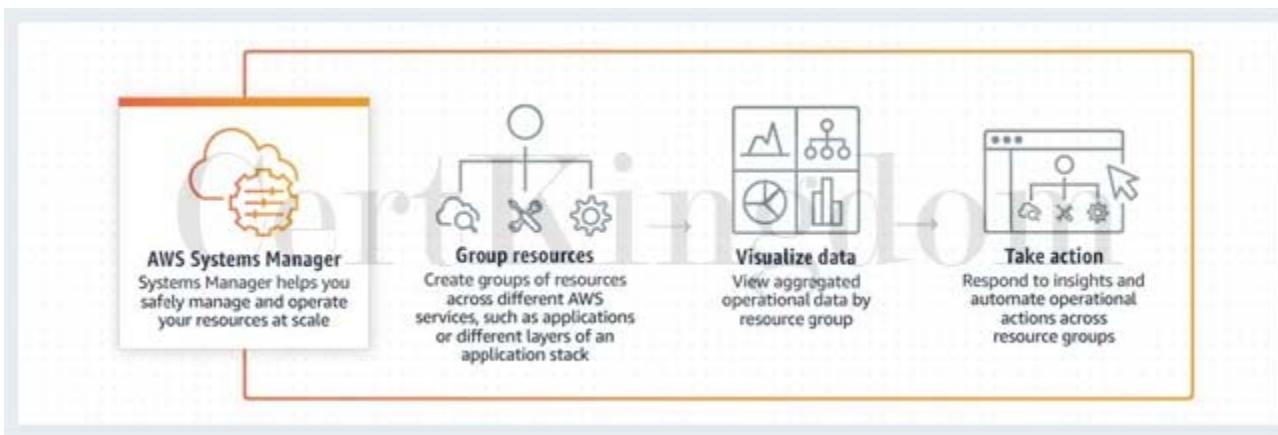
- A. AWS CodePipeline
- B. Run Command
- C. EC2Config
- D. AWS Config

Answer: B

Explanation:

You can use Run Command from the console to configure instances without having to login to each instance.

AWS Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances.



A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the AWS console, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the AWS SDKs. Run Command is offered at no additional cost.

Hence, the correct answer is: Run Command.

Reference:

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

AWS Systems Manager Overview:

<https://www.youtube.com/watch?v=KVFKyMAHxqY>

Check out this AWS Systems Manager Cheat Sheet:

<https://tutorialsdojo.com/aws-systems-manager/>

## QUESTION 282

A loan processing application is hosted in a single On-Demand EC2 instance in your VPC. To improve the scalability of your application, you have to use Auto Scaling to automatically add new EC2 instances to handle a surge of incoming requests.

Which of the following items should be done in order to add an existing EC2 instance to an Auto Scaling group? (Select TWO.)

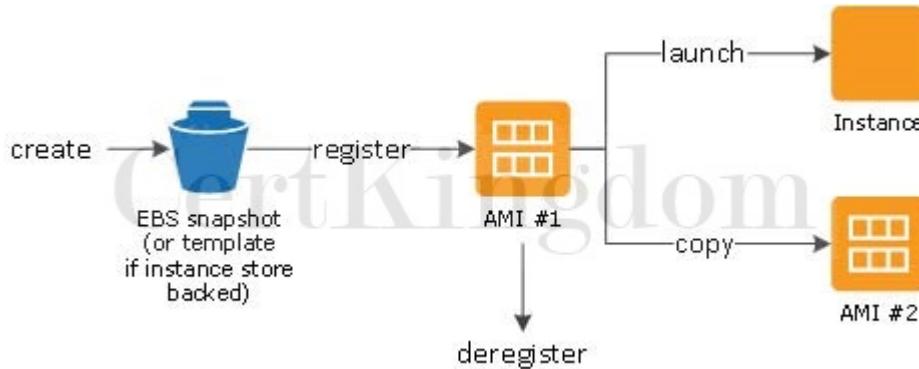
- A. You must stop the instance first.
- B. You have to ensure that the instance is launched in one of the Availability Zones defined in your Auto Scaling group.
- C. You have to ensure that the AMI used to launch the instance no longer exists.
- D. You have to ensure that the AMI used to launch the instance still exists.

E. You have to ensure that the instance is in a different Availability Zone as the Auto Scaling group.

Answer: B,D

Explanation:

Amazon EC2 Auto Scaling provides you with an option to enable automatic scaling for one or more EC2 instances by attaching them to your existing Auto Scaling group. After the instances are attached, they become a part of the Auto Scaling group.



The instance that you want to attach must meet the following criteria:

- The instance is in the running state.
- The AMI used to launch the instance must still exist.
- The instance is not a member of another Auto Scaling group.
- The instance is launched into one of the Availability Zones defined in your Auto Scaling group.
- If the Auto Scaling group has an attached load balancer, the instance and the load balancer must both be in EC2-Classic or the same VPC. If the Auto Scaling group has an attached target group, the instance and the load balancer must both be in the same VPC.

Based on the above criteria, the following are the correct answers among the given options:

- You have to ensure that the AMI used to launch the instance still exists.
- You have to ensure that the instance is launched in one of the Availability Zones defined in your Auto Scaling group.

The option that says: You must stop the instance first is incorrect because you can directly add a running EC2 instance to an Auto Scaling group without stopping it.

The option that says: You have to ensure that the AMI used to launch the instance no longer exists is incorrect because it should be the other way around. The AMI used to launch the instance should still exist.

The option that says: You have to ensure that the instance is in a different Availability Zone as the Auto Scaling group is incorrect because the instance should be launched in one of the Availability Zones defined in your Auto Scaling group.

References:

<http://docs.aws.amazon.com/autoscaling/latest/userguide/attach-instance-asg.html>

[https://docs.aws.amazon.com/autoscaling/ec2/userguide/scaling\\_plan.html](https://docs.aws.amazon.com/autoscaling/ec2/userguide/scaling_plan.html)

Check out this AWS Auto Scaling Cheat Sheet:

<https://tutorialsdojo.com/aws-auto-scaling/>

## QUESTION 283

A company needs to use Amazon S3 to store irreproducible financial documents. For their quarterly reporting, the files are required to be retrieved after a period of 3 months. There will be some occasions when a surprise audit will be held, which requires access to the archived data that they need to present immediately.

What will you do to satisfy this requirement in a cost-effective way?

- A. Use Amazon Glacier Deep Archive
- B. Use Amazon S3 Standard - Infrequent Access
- C. Use Amazon S3 -Intelligent Tiering

## D. Use Amazon S3 Standard

Answer: B

Explanation:

In this scenario, the requirement is to have a storage option that is cost-effective and has the ability to access or retrieve the archived data immediately. The cost-effective options are Amazon Glacier Deep Archive and Amazon S3 Standard- Infrequent Access (Standard - IA). However, the former option is not designed for rapid retrieval of data which is required for the surprise audit.

Hence, using Amazon Glacier Deep Archive is incorrect and the best answer is to use Amazon S3 Standard - Infrequent Access.

## Amazon S3 Storage Classes



CertKingdom					
S3 Standard	S3 Intelligent-Tiering	S3 Standard-IA	S3 One Zone-IA	S3 Glacier	S3 Deep Archive
Frequently Accessed Data (Hot)					Archived Data (Cold)
Active, frequently-accessed data	Data with changing access patterns	Infrequently-accessed data	Re-creatable, less accessed data	Data archiving	Cheapest storage class for long-term retention of data
Milliseconds access ≥ 3 AZs	30 days min. storage duration charge	30 days min. storage duration charge	30 days min. storage duration charge	90 days min. storage duration charge	180 days min. storage duration charge
Tutorials Dojo	Milliseconds access ≥ 3 AZs	Milliseconds access ≥ 3 AZs	Milliseconds access 1 AZ	Retrievable within minutes or hours ≥ 3 AZs	Retrievable within hours ≥ 3 AZs

Using Amazon S3 Standard is incorrect because the standard storage class is not cost-efficient in this scenario. It costs more than Glacier Deep Archive and S3 Standard - Infrequent Access.

Using Amazon S3 -Intelligent Tiering is incorrect because the Intelligent Tiering storage class entails an additional fee for monitoring and automation of each object in your S3 bucket vs. the Standard storage class and S3 Standard - Infrequent Access.

Amazon S3 Standard - Infrequent Access is an Amazon S3 storage class for data that is accessed less frequently but requires rapid access when needed. Standard - IA offers the high durability, throughput, and low latency of Amazon S3 Standard, with a low per GB storage price and per GB retrieval fee. This combination of low cost and high performance makes Standard - IA ideal for long-term storage, backups, and as a data store for disaster recovery. The Standard - IA storage class is set at the object level and can exist in the same bucket as Standard, allowing you to use lifecycle policies to automatically transition objects between storage classes without any application changes.

References:

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

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

## QUESTION 284

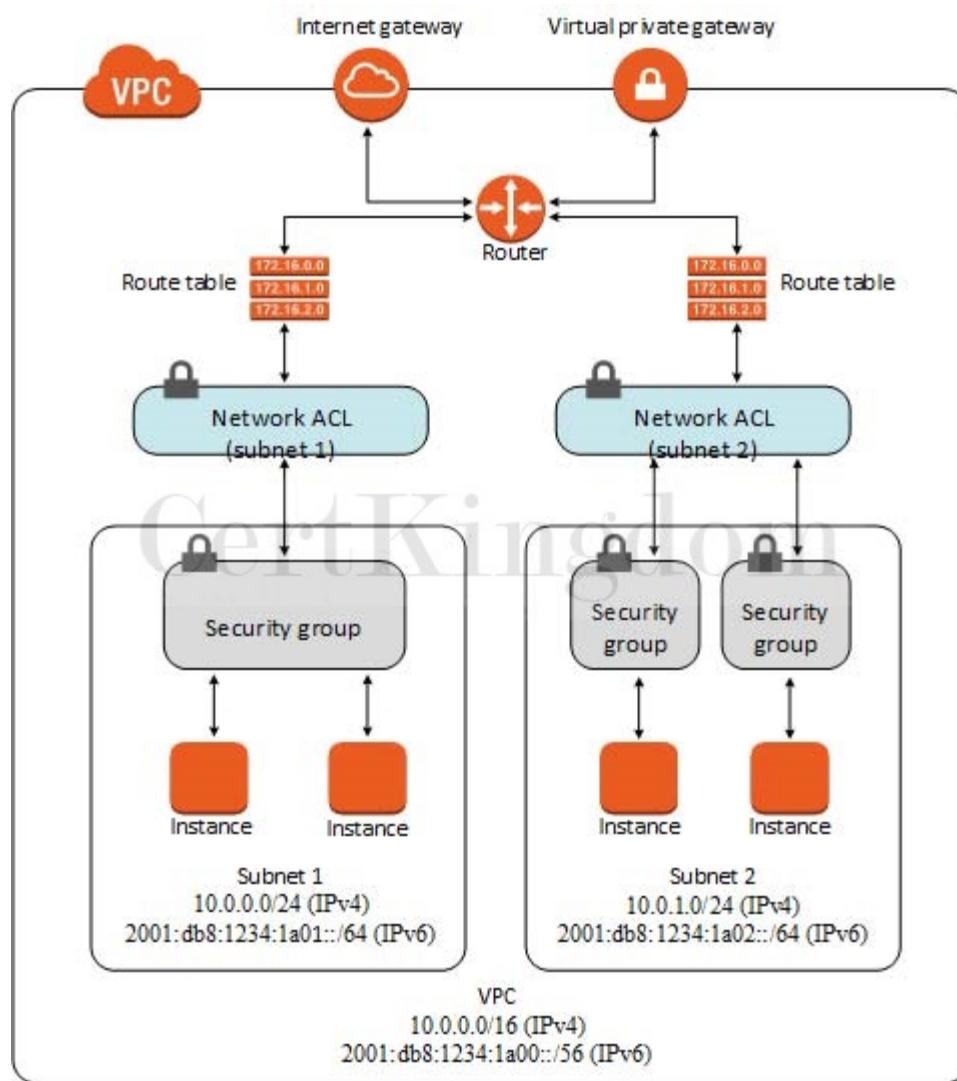
A top IT Consultancy has a VPC with two On-Demand EC2 instances with Elastic IP addresses. You were notified that the EC2 instances are currently under SSH brute force attacks over the Internet. The IT Security team has identified the IP addresses where these attacks originated. You have to immediately implement a temporary fix to stop these attacks while the team is setting up AWS WAF, GuardDuty, and AWS Shield Advanced to permanently fix the security vulnerability. Which of the following provides the quickest way to stop the attacks to the instances?

- A. Place the EC2 instances into private subnets
- B. Assign a static Anycast IP address to each EC2 instance
- C. Block the IP addresses in the Network Access Control List
- D. Remove the Internet Gateway from the VPC

Answer: C

Explanation:

A network access control list (ACL) 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. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.



The following are the basic things that you need to know about network ACLs:

- Your VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic.

- You can create a custom network ACL and associate it with a subnet. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
- Each subnet in your VPC must be associated with a network ACL. If you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL.
- You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time. When you associate a network ACL with a subnet, the previous association is removed.
- A network ACL contains a numbered list of rules that we evaluate in order, starting with the lowest numbered rule, to determine whether traffic is allowed in or out of any subnet associated with the network ACL. The highest number that you can use for a rule is 32766. We recommend that you start by creating rules in increments (for example, increments of 10 or 100) so that you can insert new rules where you need to later on.
- A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
- Network ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).

The scenario clearly states that it requires the quickest way to fix the security vulnerability. In this situation, you can manually block the offending IP addresses using Network ACLs since the IT Security team already identified the list of offending IP addresses. Alternatively, you can set up a bastion host, however, this option entails additional time to properly set up as you have to configure the security configurations of your bastion host.

Hence, blocking the IP addresses in the Network Access Control List is the best answer since it can quickly resolve the issue by blocking the IP addresses using Network ACL.

Placing the EC2 instances into private subnets is incorrect because if you deploy the EC2 instance in the private subnet without public or EIP address, it would not be accessible over the Internet, even to you.

Removing the Internet Gateway from the VPC is incorrect because doing this will also make your EC2 instance inaccessible to you as it will cut down the connection to the Internet.

Assigning a static Anycast IP address to each EC2 instance is incorrect because a static Anycast IP address is primarily used by AWS Global Accelerator to enable organizations to seamlessly route traffic to multiple regions and improve availability and performance for their end-users.

References:

[https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_ACLs.html](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html)

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Security.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html)

Security Group vs NACL:

<https://tutorialsdojo.com/security-group-vs-nacl/>

## QUESTION 285

A company has both on-premises data center as well as AWS cloud infrastructure. They store their graphics, audios, videos, and other multimedia assets primarily in their on-premises storage server and use an S3 Standard storage class bucket as a backup. Their data is heavily used for only a week (7 days) but after that period, it will only be infrequently used by their customers. The Solutions Architect is instructed to save storage costs in AWS yet maintain the ability to fetch a subset of their media assets in a matter of minutes for a surprise annual data audit, which will be conducted on their cloud storage. Which of the following are valid options that the Solutions Architect can implement to meet the above requirement? (Select TWO.)

- Set a lifecycle policy in the bucket to transition the data to S3 - One Zone-Infrequent Access storage class after one week (7 days).
- Set a lifecycle policy in the bucket to transition the data to Glacier after one week (7 days).
- Set a lifecycle policy in the bucket to transition to S3 - Standard IA after 30 days
- Set a lifecycle policy in the bucket to transition the data to S3 Glacier Deep Archive storage class after one week (7 days).
- Set a lifecycle policy in the bucket to transition the data to S3 - Standard IA storage class after one week (7 days).

Answer: B,C

Explanation:

You can add rules in a lifecycle configuration to tell Amazon S3 to transition objects to another Amazon S3 storage class. For example: When you know that objects are infrequently accessed, you might transition them to the STANDARD\_IA storage class. Or transition your data to the GLACIER storage class in case you want to archive objects that you don't need to access in real time.

In a lifecycle configuration, you can define rules to transition objects from one storage class to another to save on storage costs. When you don't know the access patterns of your objects or your access patterns are changing over time, you can transition the objects to the INTELLIGENT\_TIERING storage class for automatic cost savings.

The lifecycle storage class transitions have a constraint when you want to transition from the STANDARD storage classes to either STANDARD\_IA or ONEZONE\_I

A. The following constraints apply:

- For larger objects, there is a cost benefit for transitioning to STANDARD\_IA or ONEZONE\_I

A. Amazon

S3 does not transition objects that are smaller than 128 KB to the STANDARD\_IA or ONEZONE\_IA storage classes because it's not cost effective.

- Objects must be stored at least 30 days in the current storage class before you can transition them to STANDARD\_IA or ONEZONE\_I

A. For example, you cannot create a lifecycle rule to transition objects to the STANDARD\_IA storage class one day after you create them. Amazon S3 doesn't transition objects within the first 30 days because newer objects are often accessed more frequently or deleted sooner than is suitable for STANDARD\_IA or ONEZONE\_IA storage.

- If you are transitioning noncurrent objects (in versioned buckets), you can transition only objects that are at least 30 days noncurrent to STANDARD\_IA or ONEZONE\_IA storage.

## Lifecycle rule



1 Name and scope

2 Transitions

3 Expiration

4 Review

Enter a rule name

Tutorials Dojo S3 Lifecycle

Add filter to limit scope to prefix/tags

Type to add prefix/tag filter

Cancel

Since there is a time constraint in transitioning objects in S3, you can only change the storage class of your objects from S3 Standard storage class to STANDARD\_IA or ONEZONE\_IA storage after 30 days. This limitation does not apply on INTELLIGENT\_TIERING, GLACIER, and DEEP\_ARCHIVE storage class.

In addition, the requirement says that the media assets should be fetched in a matter of minutes for a surprise annual data audit. This means that the retrieval will only happen once a year. You can use expedited retrievals in Glacier which will allow you to quickly access your data (within 1-5 minutes) when occasional urgent requests for a subset of archives are required.

In this scenario, you can set a lifecycle policy in the bucket to transition to S3 - Standard IA after 30 days or alternatively, you can directly transition your data to Glacier after one week (7 days).

Hence, the following are the correct answers:

- Set a lifecycle policy in the bucket to transition the data from Standard storage class to Glacier after one week (7 days).
- Set a lifecycle policy in the bucket to transition to S3 - Standard IA after 30 days.

Setting a lifecycle policy in the bucket to transition the data to S3 - Standard IA storage class after one week (7 days) and setting a lifecycle policy in the bucket to transition the data to S3 - One Zone-Infrequent Access storage class after one week (7 days) are both incorrect because there is a constraint in S3 that objects must be stored at least 30 days in the current storage class before you can transition them to STANDARD\_IA or ONEZONE\_I

A. You cannot create a lifecycle rule to transition objects to either STANDARD\_IA or ONEZONE\_IA storage class 7 days after you create them because you can only do this after the 30-day period has elapsed. Hence, these options are incorrect.

Setting a lifecycle policy in the bucket to transition the data to S3 Glacier Deep Archive storage class after one week (7 days) is incorrect because although DEEP\_ARCHIVE storage class provides the most cost-effective storage option, it does not have the ability to do expedited retrievals, unlike Glacier. In the event that the surprise annual data audit happens, it may take several hours before you can retrieve your

data.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/restoring-objects.html>

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

---

## QUESTION 286

A company is running a batch job on an EC2 instance inside a private subnet. The instance gathers input data from an S3 bucket in the same region through a NAT Gateway. The company is looking for a solution that will reduce costs without imposing risks on redundancy or availability.

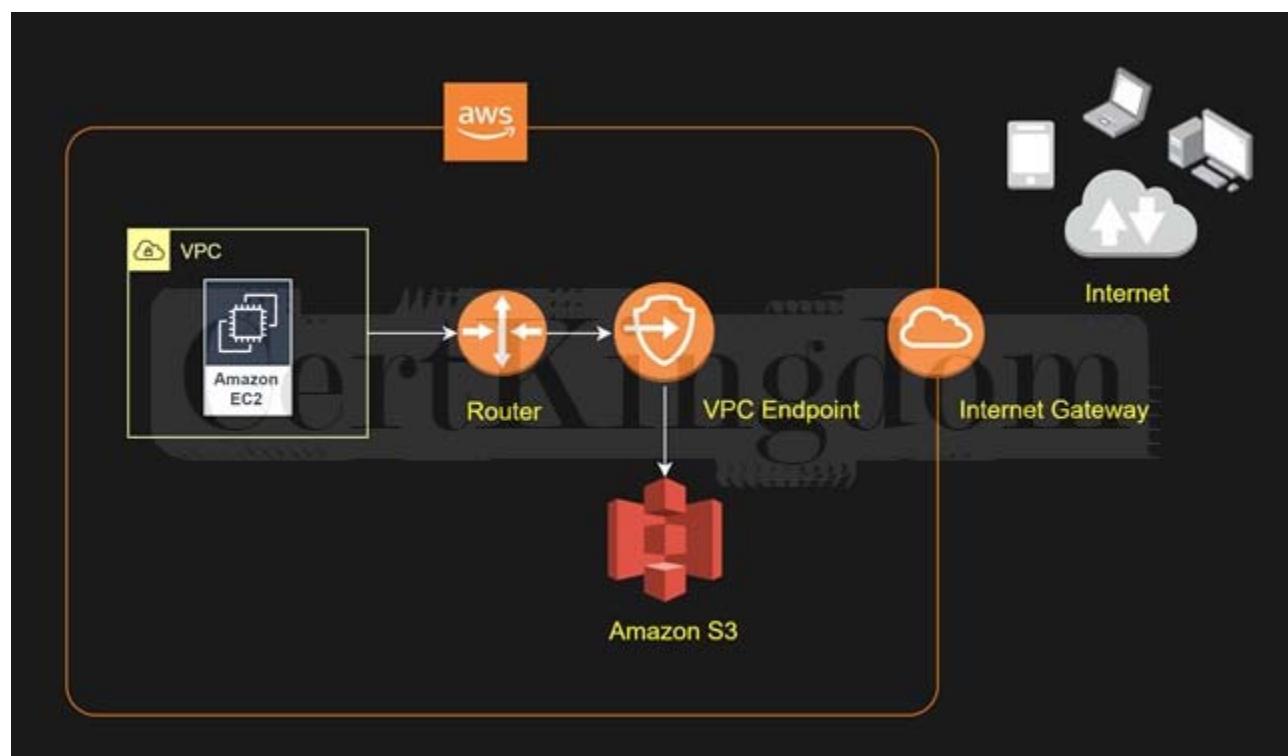
Which solution will accomplish this?

- A. Re-assign the NAT Gateway to a lower EC2 instance type.
- B. Remove the NAT Gateway and use a Gateway VPC endpoint to access the S3 bucket from the instance.
- C. Deploy a Transit Gateway to peer connection between the instance and the S3 bucket.
- D. Replace the NAT Gateway with a NAT instance hosted on a burstable instance type.

Answer: B

Explanation:

A gateway endpoint is a gateway that you specify in your route table to access Amazon S3 from your VPC over the AWS network. Interface endpoints extend the functionality of gateway endpoints by using private IP addresses to route requests to Amazon S3 from within your VPC, on-premises, or from a different AWS Region. Interface endpoints are compatible with gateway endpoints. If you have an existing gateway endpoint in the VPC, you can use both types of endpoints in the same VPC.



There is no additional charge for using gateway endpoints. However, standard charges for data transfer and resource usage still apply.

Hence, the correct answer is: Remove the NAT Gateway and use a Gateway VPC endpoint to access the S3 bucket from the instance.

The option that says: Replace the NAT Gateway with a NAT instance hosted on burstable instance type is incorrect. This solution may possibly reduce costs, but the availability and redundancy will be

compromised.

The option that says: Deploy a Transit Gateway to peer connection between the instance and the S3 bucket is incorrect. Transit Gateway is a service that is specifically used for connecting multiple VPCs through a central hub.

The option that says: Re-assign the NAT Gateway to a lower EC2 instance type is incorrect. NAT Gateways are fully managed resources. You cannot access nor modify the underlying instance that hosts it.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html>

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

Amazon VPC Overview:

<https://youtu.be/oIDHKeNvxQQ>

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

## QUESTION 287

A company has multiple AWS Site-to-Site VPN connections placed between their VPCs and their remote network. During peak hours, many employees are experiencing slow connectivity issues, which limits their productivity. The company has asked a solutions architect to scale the throughput of the VPN connections.

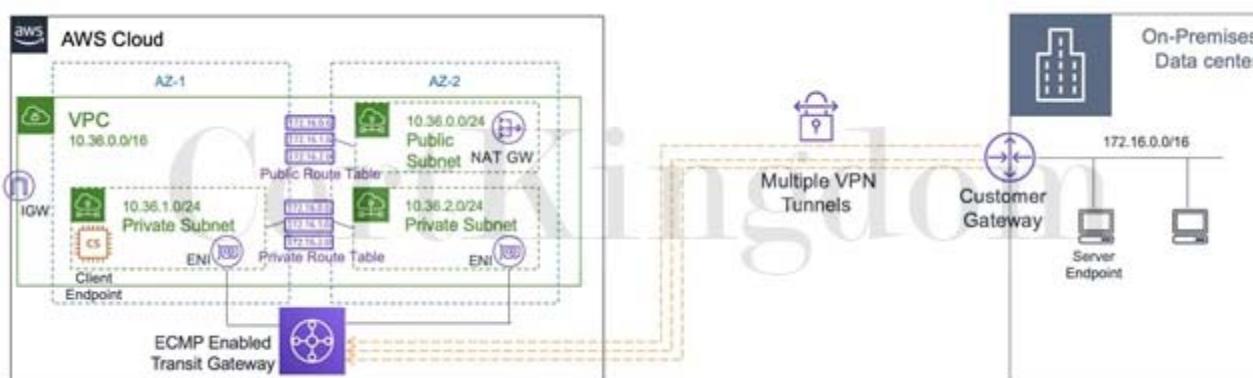
Which solution should the architect carry out?

- A. Modify the VPN configuration by increasing the number of tunnels to scale the throughput.
- B. Associate the VPCs to an Equal Cost Multipath Routing (ECMR)-enabled transit gateway and attach additional VPN tunnels.
- C. Re-route some of the VPN connections to a secondary customer gateway device on the remote network's end.
- D. Add more virtual private gateways to a VPC and enable Equal Cost Multipath Routing (ECMR) to get higher VPN bandwidth.

Answer: B

Explanation:

With AWS Transit Gateway, you can simplify the connectivity between multiple VPCs and also connect to any VPC attached to AWS Transit Gateway with a single VPN connection.



AWS Transit Gateway also enables you to scale the IPsec VPN throughput with equal-cost multi-path (ECMP) routing support over multiple VPN tunnels. A single VPN tunnel still has a maximum throughput of 1.25 Gbps. If you establish multiple VPN tunnels to an ECMP-enabled transit gateway, it can scale beyond the default limit of 1.25 Gbps.

Hence, the correct answer is: Associate the VPCs to an Equal Cost Multipath Routing (ECMR)-enabled transit gateway and attach additional VPN tunnels.

The option that says: Add more virtual private gateways to a VPC and enable Equal Cost Multipath Routing (ECMR) to get higher VPN bandwidth is incorrect because a VPC can only have a single virtual

private gateway attached to it one at a time. Also, there is no option to enable ECMR in a virtual private gateway.

The option that says: Modify the VPN configuration by increasing the number of tunnels to scale the throughput is incorrect. The maximum tunnel for a VPN connection is two. You cannot increase this beyond its limit.

The option that says: Re-route some of the VPN connections to a secondary customer gateway device on the remote network's end is incorrect. This would only increase connection redundancy and won't increase throughput. For example, connections can failover to the secondary customer gateway device in case the primary customer gateway device becomes unavailable.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/transit-gateway-ecmp-multiple-tunnels/>  
<https://aws.amazon.com/blogs/networking-and-content-delivery/scaling-vpn-throughput-using-aws-transit-gateway/>

Check out this AWS Transit Gateway Cheat Sheet:

<https://tutorialsdojo.com/aws-transit-gateway/>

---

## QUESTION 288

A company has a web-based ticketing service that utilizes Amazon SQS and a fleet of EC2 instances. The EC2 instances that consume messages from the SQS queue are configured to poll the queue as often as possible to keep end-to-end throughput as high as possible. The Solutions Architect noticed that polling the queue in tight loops is using unnecessary CPU cycles, resulting in increased operational costs due to empty responses.

In this scenario, what should the Solutions Architect do to make the system more cost-effective?

- A. Configure Amazon SQS to use long polling by setting the ReceiveMessageWaitTimeSeconds to a number greater than zero.
- B. Configure Amazon SQS to use long polling by setting the ReceiveMessageWaitTimeSeconds to zero.
- C. Configure Amazon SQS to use short polling by setting the ReceiveMessageWaitTimeSeconds to a number greater than zero.
- D. Configure Amazon SQS to use short polling by setting the ReceiveMessageWaitTimeSeconds to zero.

Answer: A

Explanation:

In this scenario, the application is deployed in a fleet of EC2 instances that are polling messages from a single SQS queue. Amazon SQS uses short polling by default, querying only a subset of the servers (based on a weighted random distribution) to determine whether any messages are available for inclusion in the response. Short polling works for scenarios that require higher throughput. However, you can also configure the queue to use Long polling instead, to reduce cost.

The ReceiveMessageWaitTimeSeconds is the queue attribute that determines whether you are using Short or Long polling. By default, its value is zero which means it is using Short polling. If it is set to a value greater than zero, then it is Long polling.

Hence, configuring Amazon SQS to use long polling by setting the ReceiveMessageWaitTimeSeconds to a number greater than zero is the correct answer.

Quick facts about SQS Long Polling:

- Long polling helps reduce your cost of using Amazon SQS by reducing the number of empty responses when there are no messages available to return in reply to a ReceiveMessage request sent to an Amazon SQS queue and eliminating false empty responses when messages are available in the queue but aren't included in the response.
- Long polling reduces the number of empty responses by allowing Amazon SQS to wait until a message is available in the queue before sending a response. Unless the connection times out, the response to the ReceiveMessage request contains at least one of the available messages, up to the maximum number of messages specified in the ReceiveMessage action.

- Long polling eliminates false empty responses by querying all (rather than a limited number) of the servers. Long polling returns messages as soon any message becomes available.

Reference:

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

Check out this Amazon SQS Cheat Sheet:

<https://tutorialsdojo.com/amazon-sqs/>

## QUESTION 289

A company plans to implement a hybrid architecture. They need to create a dedicated connection from their Amazon Virtual Private Cloud (VPC) to their on-premises network. The connection must provide high bandwidth throughput and a more consistent network experience than Internet-based solutions.

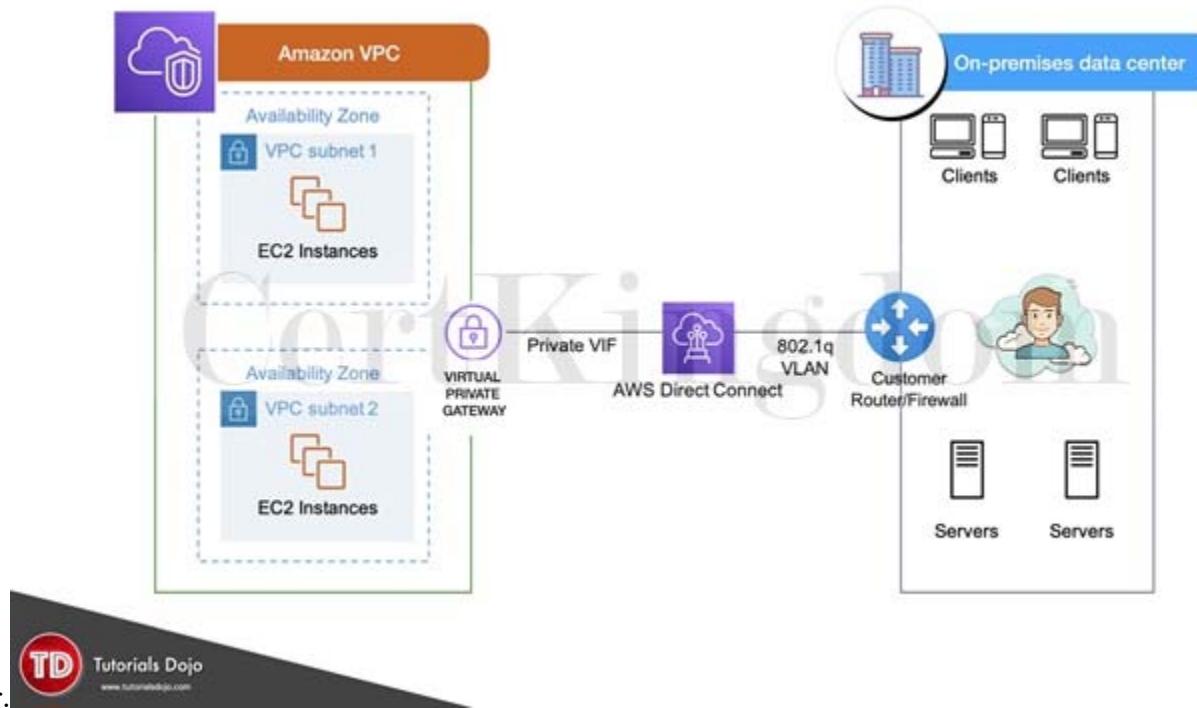
Which of the following can be used to create a private connection between the VPC and the company's on-premises network?

- A. AWS Direct Connect
- B. AWS Site-to-Site VPN
- C. Transit VPC
- D. Transit Gateway with equal-cost multipath routing (ECMP)

Answer: A

Explanation:

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct



With this connection, you can create virtual interfaces directly to public AWS services (for example, to Amazon S3) or to Amazon VPC, bypassing internet service providers in your network path. An AWS Direct Connect location provides access to AWS in the region with which it is associated. You can use a single connection in a public Region or AWS GovCloud (US) to access public AWS services in all other public Regions.

Hence, the correct answer is: AWS Direct Connect.

The option that says: Transit VPC is incorrect because this in itself is not enough to integrate your on-premises network to your VPC. You have to either use a VPN or a Direct Connect connection. A transit VPC is primarily used to connect multiple VPCs and remote networks in order to create a global network.

transit center and not for establishing a dedicated connection to your on-premises network. The option that says: Transit Gateway with equal-cost multipath routing (ECMP) is incorrect because a transit gateway is commonly used to connect multiple VPCs and on-premises networks through a central hub. Just like transit VPC, a transit gateway is not capable of establishing a direct and dedicated connection to your on-premises network.

The option that says: AWS Site-to-Site VPN is incorrect because this type of connection traverses the public Internet. Moreover, it doesn't provide a high bandwidth throughput and a more consistent network experience than Internet-based solutions.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/connect-vpc/>

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html>

Check out this AWS Direct Connect Cheat Sheet:

<https://tutorialsdojo.com/aws-direct-connect/>

S3 Transfer Acceleration vs Direct Connect vs VPN vs Snowball vs Snowmobile:

<https://tutorialsdojo.com/s3-transfer-acceleration-vs-direct-connect-vs-vpn-vs-snowball-vs-snowmobile/>

Comparison of AWS Services Cheat Sheets:

<https://tutorialsdojo.com/comparison-of-aws-services/>

---

## QUESTION 290

A local bank has an in-house application that handles sensitive financial data in a private subnet. After the data is processed by the EC2 worker instances, they will be delivered to S3 for ingestion by other services.

How should you design this solution so that the data does not pass through the public Internet?

- A. Configure a VPC Endpoint along with a corresponding route entry that directs the data to S3.
- B. Create an Internet gateway in the public subnet with a corresponding route entry that directs the data to S3.
- C. Provision a NAT gateway in the private subnet with a corresponding route entry that directs the data to S3.
- D. Configure a Transit gateway along with a corresponding route entry that directs the data to S3.

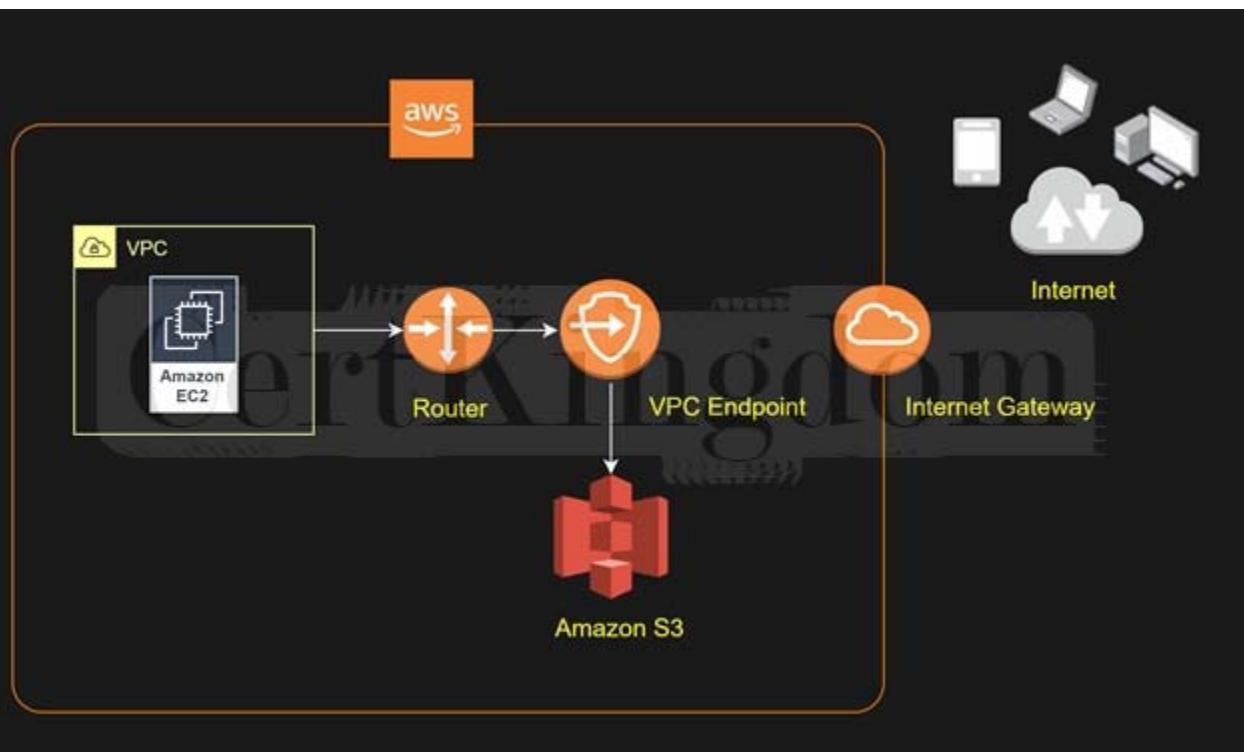
Answer: A

Explanation:

The important concept that you have to understand in this scenario is that your VPC and your S3 bucket are located within the larger AWS network. However, the traffic coming from your VPC to your S3 bucket is traversing the public Internet by default. To better protect your data in transit, you can set up a VPC endpoint so the incoming traffic from your VPC will not pass through the public Internet, but instead through the private AWS network.

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an Internet gateway, NAT device, 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 services does not leave the Amazon network.

Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.



Hence, the correct answer is: Configure a VPC Endpoint along with a corresponding route entry that directs the data to S3.

The option that says: Create an Internet gateway in the public subnet with a corresponding route entry that directs the data to S3 is incorrect because the Internet gateway is used for instances in the public subnet to have accessibility to the Internet.

The option that says: Configure a Transit gateway along with a corresponding route entry that directs the data to S3 is incorrect because the Transit Gateway is used for interconnecting VPCs and on-premises networks through a central hub. Since Amazon S3 is outside of VPC, you still won't be able to connect to it privately.

The option that says: Provision a NAT gateway in the private subnet with a corresponding route entry that directs the data to S3 is incorrect because NAT Gateway allows instances in the private subnet to gain access to the Internet, but not vice versa.

References:

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

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

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

## QUESTION 291

An application is hosted on an EC2 instance with multiple EBS Volumes attached and uses Amazon Neptune as its database. To improve data security, you encrypted all of the EBS volumes attached to the instance to protect the confidential data stored in the volumes.

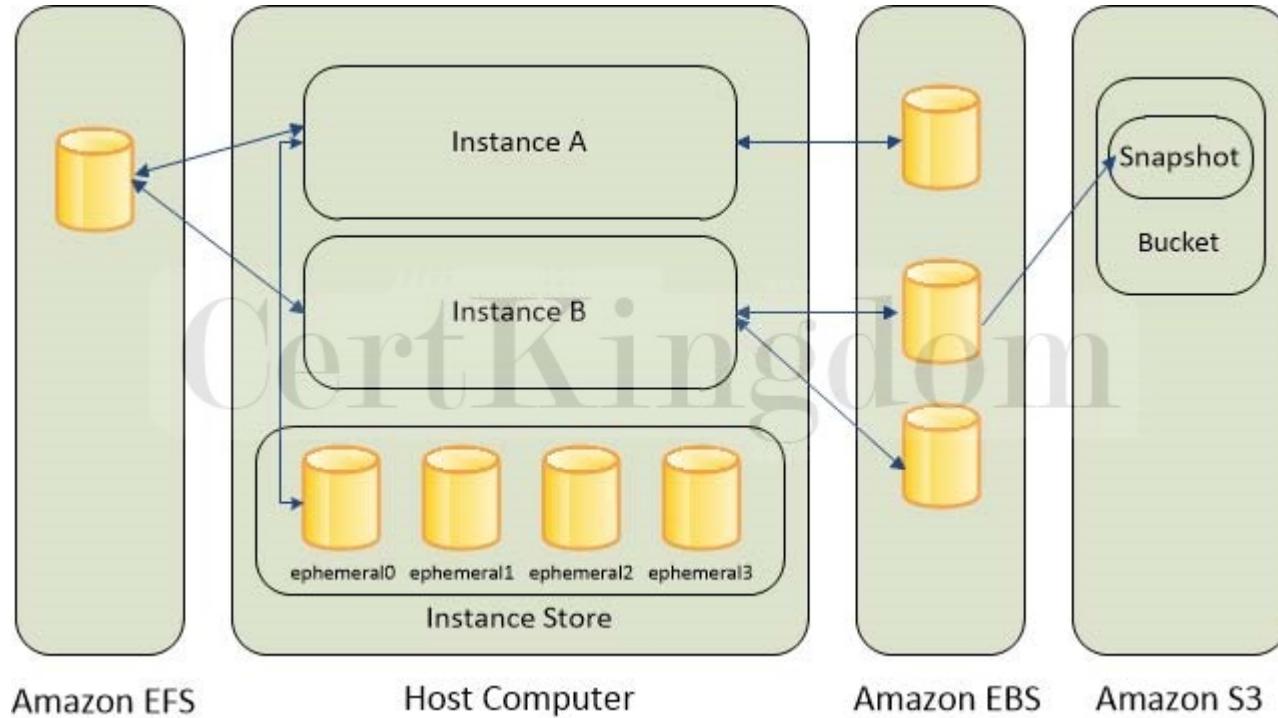
Which of the following statements are true about encrypted Amazon Elastic Block Store volumes?  
(Select TWO.)

- A. All data moving between the volume and the instance are encrypted.
- B. Only the data in the volume is encrypted and not all the data moving between the volume and the instance.
- C. Snapshots are automatically encrypted.
- D. The volumes created from the encrypted snapshot are not encrypted.
- E. Snapshots are not automatically encrypted.

Answer: A,C

Explanation:

Amazon Elastic Block Store (Amazon EBS) provides block level storage volumes for use with EC2 instances. EBS volumes are highly available and reliable storage volumes that can be attached to any running instance that is in the same Availability Zone. EBS volumes that are attached to an EC2 instance are exposed as storage volumes that persist independently from the life of the instance.



#### Amazon EFS

#### Host Computer

#### Amazon EBS

#### Amazon S3

When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted:

- Data at rest inside the volume
- All data moving between the volume and the instance
- All snapshots created from the volume
- All volumes created from those snapshots

Encryption operations occur on the servers that host EC2 instances, ensuring the security of both data-at-rest and data-in-transit between an instance and its attached EBS storage. You can encrypt both the boot and data volumes of an EC2 instance.

References:

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

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

Check out this Amazon EBS Cheat Sheet:

<https://tutorialsdojo.com/amazon-ebs/>

---

### QUESTION 292

A leading e-commerce company is in need of a storage solution that can be simultaneously accessed by 1000 Linux servers in multiple availability zones. The servers are hosted in EC2 instances that use a hierarchical directory structure via the NFSv4 protocol. The service should be able to handle the rapidly changing data at scale while still maintaining high performance. It should also be highly durable and highly available whenever the servers will pull data from it, with little need for management.

As the Solutions Architect, which of the following services is the most cost-effective choice that you should use to meet the above requirement?

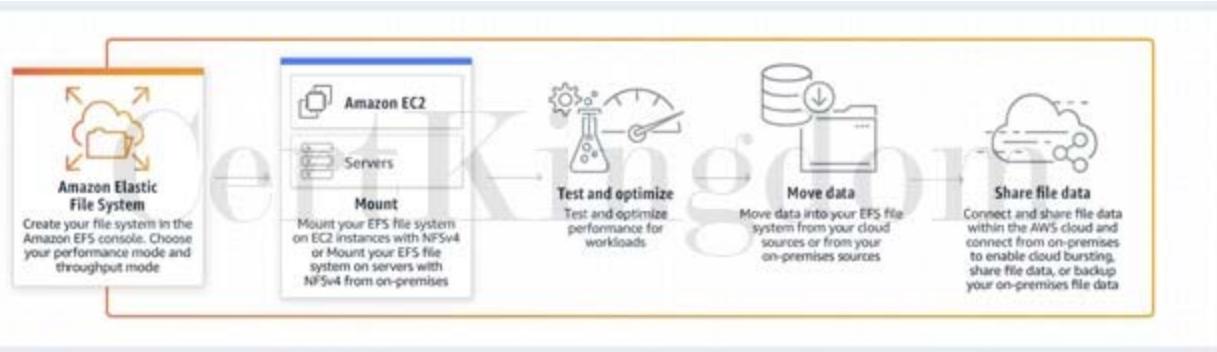
- A. EFS
- B. Storage Gateway
- C. S3
- D. EBS

Answer: A

## Explanation:

Amazon Web Services (AWS) offers cloud storage services to support a wide range of storage workloads such as EFS, S3 and EBS. You have to understand when you should use Amazon EFS, Amazon S3 and Amazon Elastic Block Store (EBS) based on the specific workloads. In this scenario, the keywords are rapidly changing data and 1000 Linux servers.

Amazon EFS is a file storage service for use with Amazon EC2. Amazon EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently-accessible storage for up to thousands of Amazon EC2 instances. EFS provides the same level of high availability and high scalability like S3 however, this service is more suitable for scenarios where it is required to have a POSIX-compatible file system or if you are storing rapidly changing data.



Data that must be updated very frequently might be better served by storage solutions that take into account read and write latencies, such as Amazon EBS volumes, Amazon RDS, Amazon DynamoDB, Amazon EFS, or relational databases running on Amazon EC2.

Amazon EBS is a block-level storage service for use with Amazon EC2. Amazon EBS can deliver performance for workloads that require the lowest-latency access to data from a single EC2 instance. Amazon S3 is an object storage service. Amazon S3 makes data available through an Internet API that can be accessed anywhere.

In this scenario, EFS is the best answer. As stated above, Amazon EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently-accessible storage for up to thousands of Amazon EC2 instances. EFS provides the performance, durability, high availability, and storage capacity needed by the 1000 Linux servers in the scenario.

S3 is incorrect because although this provides the same level of high availability and high scalability like EFS, this service is not suitable for storing data which are rapidly changing, just as mentioned in the above explanation. It is still more effective to use EFS as it offers strong consistency and file locking which the S3 service lacks.

EBS is incorrect because an EBS Volume cannot be shared by multiple instances.

Storage Gateway is incorrect because this is primarily used to extend the storage of your on-premises data center to your AWS Cloud.

## References:

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

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

<https://d1.awsstatic.com/whitepapers/AWS%20Storage%20Services%20Whitepaper-v9.pdf#page=9>

Check out this Amazon EFS Cheat Sheet:

<https://tutorialsdojo.com/amazon-efs/>

## QUESTION 293

A healthcare company stores sensitive patient health records in their on-premises storage systems. These records must be kept indefinitely and protected from any type of modifications once they are stored. Compliance regulations mandate that the records must have granular access control and each data access must be audited at all levels. Currently, there are millions of obsolete records that are not accessed by their web application, and their on-premises storage is quickly running out of space. The Solutions Architect must design a solution to immediately move existing records to AWS and support the ever-growing number of new health records.

Which of the following is the most suitable solution that the Solutions Architect should implement to meet the above requirements?

- A. Set up AWS DataSync to move the existing health records from the on-premises network to the AWS Cloud. Launch a new Amazon S3 bucket to store existing and new records. Enable AWS CloudTrail with Data Events and Amazon S3 Object Lock in the bucket.
- B. Set up AWS Storage Gateway to move the existing health records from the on-premises network to the AWS Cloud. Launch an Amazon EBS-backed EC2 instance to store both the existing and new records. Enable Amazon S3 server access logging and S3 Object Lock in the bucket.
- C. Set up AWS DataSync to move the existing health records from the on-premises network to the AWS Cloud. Launch a new Amazon S3 bucket to store existing and new records. Enable AWS CloudTrail with Management Events and Amazon S3 Object Lock in the bucket.
- D. Set up AWS Storage Gateway to move the existing health records from the on-premises network to the AWS Cloud. Launch a new Amazon S3 bucket to store existing and new records. Enable AWS CloudTrail with Management Events and Amazon S3 Object Lock in the bucket.

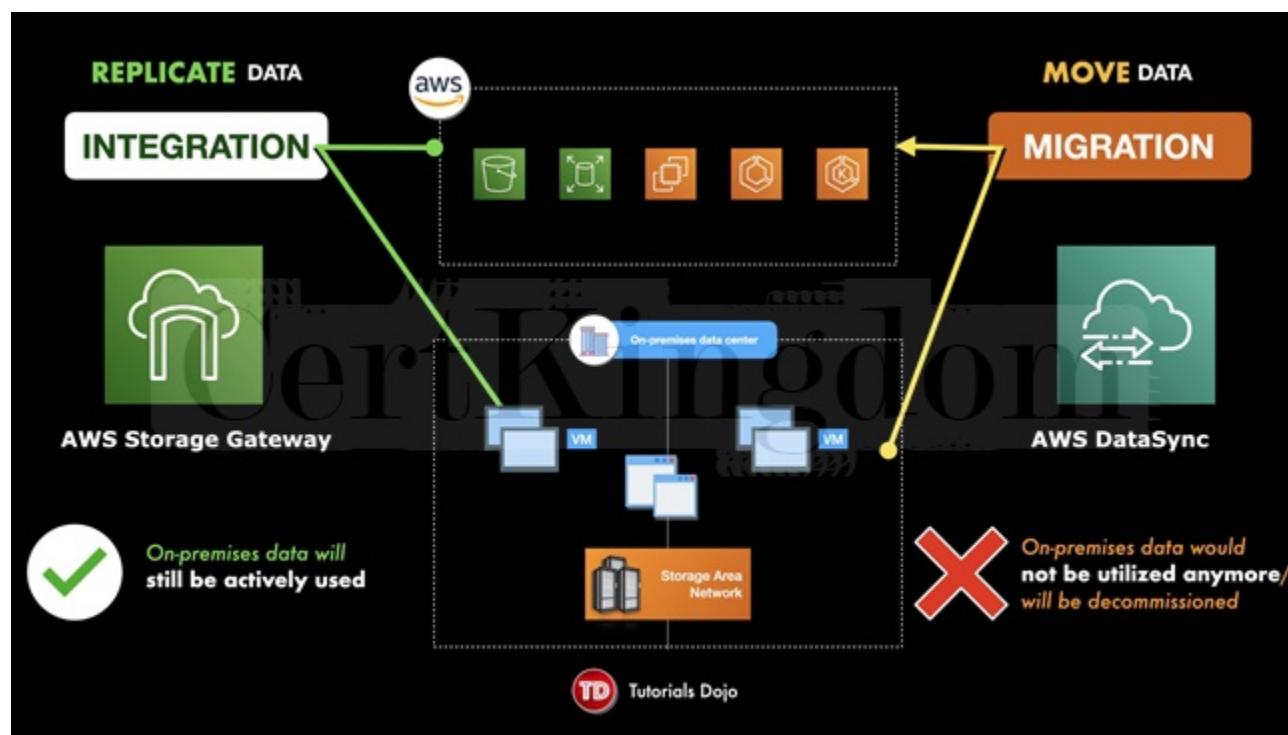
Answer: A

Explanation:

AWS Storage Gateway is a set of hybrid cloud services that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to integrate AWS Cloud storage with existing on-site workloads so they can simplify storage management and reduce costs for key hybrid cloud storage use cases. These include moving backups to the cloud, using on-premises file shares backed by cloud storage, and providing low latency access to data in AWS for on-premises applications.

AWS DataSync is an online data transfer service that simplifies, automates, and accelerates moving data between on-premises storage systems and AWS Storage services, as well as between AWS Storage services. You can use DataSync to migrate active datasets to AWS, archive data to free up on-premises storage capacity, replicate data to AWS for business continuity, or transfer data to the cloud for analysis and processing.

Both AWS Storage Gateway and AWS DataSync can send data from your on-premises data center to AWS and vice versa. However, AWS Storage Gateway is more suitable to be used in integrating your storage services by replicating your data while AWS DataSync is better for workloads that require you to move or migrate your data.



You can also use a combination of DataSync and File Gateway to minimize your on-premises infrastructure while seamlessly connecting on-premises applications to your cloud storage. AWS

DataSync enables you to automate and accelerate online data transfers to AWS storage services. File Gateway is a fully managed solution that will automate and accelerate the replication of data between the on-premises storage systems and AWS storage services.

AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

There are two types of events that you configure your CloudTrail for:

- Management Events
- Data Events

Management Events provide visibility into management operations that are performed on resources in your AWS account. These are also known as control plane operations. Management events can also include non-API events that occur in your account.

Data Events, on the other hand, provide visibility into the resource operations performed on or within a resource. These are also known as data plane operations. It allows granular control of data event logging with advanced event selectors. You can currently log data events on different resource types such as Amazon S3 object-level API activity (e.g. GetObject, DeleteObject, and PutObject API operations), AWS Lambda function execution activity (the Invoke API), DynamoDB Item actions, and many more.

The screenshot shows the AWS S3 console under the 'Server access logging' tab. On the left, there's a sidebar with links like 'Buckets', 'Access Points', 'Object Lambda Access Points', 'Batch Operations', 'Access analyzer for S3', 'Block Public Access settings for this account', 'Storage Lens', 'Dashboards', 'AWS Organizations settings', 'Feature spotlight', and 'AWS Marketplace for S3'. The main area has a heading 'Server access logging' with a sub-section 'AWS CloudTrail data events (1)'. This section contains a table with one row: 'Name' (TutorialsDojo-Davao) and 'Access' (Read, Write). A green box highlights this table. Below it is another section 'Event notifications (0)' with a 'Create event notification' button.

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

Log properties	AWS CloudTrail	Amazon S3 server logs
Can be forwarded to other systems (CloudWatch Logs, CloudWatch Events)	Yes	
Deliver logs to more than one destination (for example, send the same logs to two different buckets)	Yes	
Turn on logs for a subset of objects (prefix)	Yes	
Cross-account log delivery (target and source bucket owned by different accounts)	Yes	
Integrity validation of log file using digital signature/hashing	Yes	
Default/choice of encryption for log files	Yes	
Object operations (using Amazon S3 APIs)	Yes	Yes
Bucket operations (using Amazon S3 APIs)	Yes	Yes
Searchable UI for logs	Yes	
Fields for Object Lock parameters, Amazon S3 Select properties for log records	Yes	
Fields for Object Size, Total Time, Turn-Around Time, and HTTP Referer for log records		Yes
Lifecycle transitions, expirations, restores		Yes
Logging of keys in a batch delete operation		Yes
Authentication failures <sup>1</sup>		Yes
Accounts where logs get delivered	Bucket owner <sup>2</sup> , and requester	Bucket owner only

You can record the actions that are taken by users, roles, or AWS services on Amazon S3 resources and maintain log records for auditing and compliance purposes. To do this, you can use server access logging, AWS CloudTrail logging, or a combination of both. AWS recommends that you use AWS CloudTrail for logging bucket and object-level actions for your Amazon S3 resources.

Hence, the correct answer is: Set up AWS DataSync to move the existing health records from the on-premises network to the AWS Cloud. Launch a new Amazon S3 bucket to store existing and new records. Enable AWS CloudTrail with Data Events and Amazon S3 Object Lock in the bucket.

The option that says: Set up AWS Storage Gateway to move the existing health records from the on-premises network to the AWS Cloud. Launch a new Amazon S3 bucket to store existing and new records. Enable AWS CloudTrail with Management Events and Amazon S3 Object Lock in the bucket is incorrect. The requirement explicitly says that the Solutions Architect must immediately move the existing records to AWS and not integrate or replicate the data. Using AWS DataSync is a more suitable service to use here since the primary objective is to migrate or move data. You also have to use Data Events here and not Management Events in CloudTrail, to properly track all the data access and changes to your objects.

The option that says: Set up AWS Storage Gateway to move the existing health records from the on-premises network to the AWS Cloud. Launch an Amazon EBS-backed EC2 instance to store both the existing and new records. Enable Amazon S3 server access logging and S3 Object Lock in the bucket is incorrect. Just as mentioned in the previous option, using AWS Storage Gateway is not a recommended service to use in this situation since the objective is to move the obsolete data. Moreover, using Amazon EBS to store health records is not a scalable solution compared with Amazon S3. Enabling server access logging can help audit the stored objects. However, it is better to use CloudTrail as it provides more granular access control and tracking.

The option that says: Set up AWS DataSync to move the existing health records from the on-premises network to the AWS Cloud. Launch a new Amazon S3 bucket to store existing and new records. Enable AWS CloudTrail with Management Events and Amazon S3 Object Lock in the bucket is incorrect.

Although it is right to use AWS DataSync to move the health records, you still have to configure Data Events in AWS CloudTrail and not Management Events. This type of event only provides visibility into management operations that are performed on resources in your AWS account and not the data events that are happening in the individual objects in Amazon S3.

References:

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

<https://aws.amazon.com/about-aws/whats-new/0/aws-cloudtrail-provides-more-granular-control-of-data-event-logging/>

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

Check out this AWS DataSync Cheat Sheet:

<https://tutorialsdojo.com/aws-datasync/>

AWS Storage Gateway vs DataSync:

<https://www.youtube.com/watch?v=tmfe1rO-AUs>

## QUESTION 294

A startup needs to use a shared file system for its .NET web application running on an Amazon EC2 Windows instance. The file system must provide a high level of throughput and IOPS that can also be integrated with Microsoft Active Directory.

Which is the MOST suitable service that you should use to achieve this requirement?

- A. AWS Storage Gateway - File Gateway
- B. Amazon Elastic File System
- C. Amazon EBS Provisioned IOPS SSD volumes
- D. Amazon FSx for Windows File Server

Answer: D

Explanation:

Amazon FSx for Windows File Server provides fully managed, highly reliable, and scalable file storage 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 supports the use of Microsoft's Distributed File System (DFS) Namespaces to scale-out performance across multiple file systems in the same namespace up to tens of Gbps and millions of IOPS.



The key phrases in this scenario are "file system" and "Active Directory integration." You need to implement a solution that will meet these requirements. Among the options given, the possible answers are FSx Windows File Server and File Gateway. But you need to consider that the question also states that you need to provide a high level of throughput and IOPS. Amazon FSx Windows File Server can scale-out storage to hundreds of petabytes of data with tens of GB/s of throughput performance and millions of IOPS.

Hence, the correct answer is: Amazon FSx for Windows File Server.

Amazon EBS Provisioned IOPS SSD volumes is incorrect because this is just a block storage volume and not a full-fledged file system. Amazon EBS is primarily used as persistent block storage for EC2 instances.

Amazon Elastic File System is incorrect because it is stated in the scenario that the startup uses an Amazon EC2 Windows instance. Remember that Amazon EFS can only handle Linux workloads.

AWS Storage Gateway - File Gateway is incorrect. Although it can be used as a shared file system for Windows and can also be integrated with Microsoft Active Directory, Amazon FSx still has a higher level of throughput and IOPS compared with AWS Storage Gateway. Amazon FSX is capable of providing hundreds of thousands (or even millions) of IOPS.

References:

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

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

Check out this Amazon FSx Cheat Sheet:  
<https://tutorialsdojo.com/amazon-fsx/>

---

### QUESTION 295

A company needs secure access to its Amazon RDS for MySQL database that is used by multiple applications. Each IAM user must use a short-lived authentication token to connect to the database. Which of the following is the most suitable solution in this scenario?

- A. Use AWS Secrets Manager to generate and store short-lived authentication tokens.
- B. Use an MFA token to access and connect to a database.
- C. Use AWS SSO to access the RDS database.
- D. Use IAM DB Authentication and create database accounts using the AWS-provided AWSAuthenticationPlugin plugin in MySQL.

Answer: D

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.

An authentication token is a string of characters that you use instead of a password. After you generate an authentication token, it's valid for 15 minutes before it expires. If you try to connect using an expired token, the connection request is denied.

## Database options

DB cluster identifier [Info](#)

tutorialsdojo

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

Database name [Info](#)

tutorialsdojo

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

Since the scenario asks you to create a short-lived authentication token to access an Amazon RDS database, you can use an IAM database authentication when connecting to a database instance. Authentication is handled by AWSAuthenticationPlugin—an AWS-provided plugin that works seamlessly with IAM to authenticate your IAM users.

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, the correct answer is the option that says: Use IAM DB Authentication and create database accounts using the AWS-provided AWSAuthenticationPlugin plugin in MySQL.

The options that say: Use AWS SSO to access the RDS database is incorrect because AWS SSO just enables you to centrally manage SSO access and user permissions for all of your AWS accounts managed through AWS Organizations.

The option that says: Use AWS Secrets Manager to generate and store short-lived authentication tokens is incorrect because AWS Secrets Manager is not a suitable service to create an authentication token to

access an Amazon RDS database. It's primarily used to store passwords, secrets, and other sensitive credentials. It can't generate a short-lived token either. You have to use IAM DB Authentication instead. The option that says: Use an MFA token to access and connect to a database is incorrect because you can't use an MFA token to connect to your database. You have to set up IAM DB Authentication instead.

References:

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

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

Check out this AWS IAM Cheat Sheet:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

---

## QUESTION 296

A company has a UAT and production EC2 instances running on AWS. They want to ensure that employees who are responsible for the UAT instances don't have the access to work on the production instances to minimize security risks.

Which of the following would be the best way to achieve this?

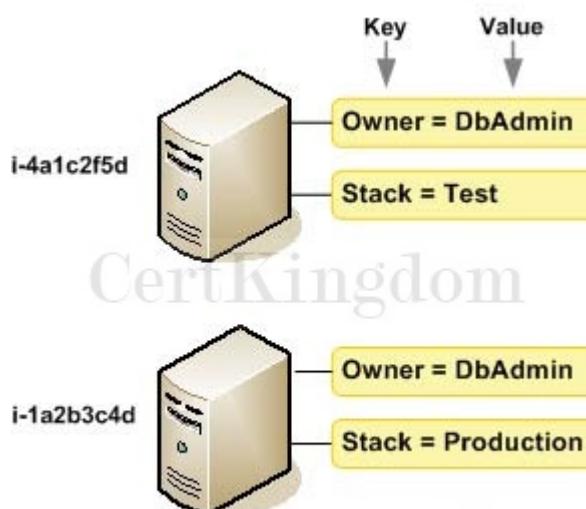
- A. Define the tags on the UAT and production servers and add a condition to the IAM policy which allows access to specific tags.
- B. Provide permissions to the users via the AWS Resource Access Manager (RAM) service to only access EC2 instances that are used for production or development.
- C. Launch the UAT and production EC2 instances in separate VPC's connected by VPC peering.
- D. Launch the UAT and production instances in different Availability Zones and use Multi Factor Authentication.

Answer: A

Explanation:

For this scenario, the best way to achieve the required solution is to use a combination of Tags and IAM policies. You can define the tags on the UAT and production EC2 instances and add a condition to the IAM policy which allows access to specific tags.

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type "" you can quickly identify a specific resource based on the tags you've assigned to it.



By default, IAM users don't have permission to create or modify Amazon EC2 resources, or perform tasks using the Amazon EC2 API. (This means that they also can't do so using the Amazon EC2 console or CLI.) To allow IAM users to create or modify resources and perform tasks, you must create IAM

policies that grant IAM users permission to use the specific resources and API actions they'll need, and then attach those policies to the IAM users or groups that require those permissions.

Hence, the correct answer is: Define the tags on the UAT and production servers and add a condition to the IAM policy which allows access to specific tags.

The option that says: Launch the UAT and production EC2 instances in separate VPC's connected by VPC peering is incorrect because these are just network changes to your cloud architecture and don't have any effect on the security permissions of your users to access your EC2 instances.

The option that says: Provide permissions to the users via the AWS Resource Access Manager (RAM) service to only access EC2 instances that are used for production or development is incorrect because the AWS Resource Access Manager (RAM) is primarily used to securely share your resources across AWS accounts or within your Organization and not on a single AWS account. You also have to set up a custom IAM Policy in order for this to work.

The option that says: Launch the UAT and production instances in different Availability Zones and use Multi Factor Authentication is incorrect because placing the EC2 instances to different AZs will only improve the availability of the systems but won't have any significance in terms of security. You have to set up an IAM Policy that allows access to EC2 instances based on their tags. In addition, a Multi-Factor Authentication is not a suitable security feature to be implemented for this scenario.

References:

[http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using\\_Tags.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html)

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-policies-for-amazon-ec2.html>

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

---

## QUESTION 297

A company plans to migrate a MySQL database from an on-premises data center to the AWS Cloud. This database will be used by a legacy batch application that has steady-state workloads in the morning but has its peak load at night for the end-of-day processing. You need to choose an EBS volume that can handle a maximum of 450 GB of data and can also be used as the system boot volume for your EC2 instance.

Which of the following is the most cost-effective storage type to use in this scenario?

- A. Amazon EBS Cold HDD (sc1)
- B. Amazon EBS Provisioned IOPS SSD (io1)
- C. Amazon EBS General Purpose SSD (gp2)
- D. Amazon EBS Throughput Optimized HDD (st1)

Answer: C

Explanation:

In this scenario, a legacy batch application which has steady-state workloads requires a relational MySQL database. The EBS volume that you should use has to handle a maximum of 450 GB of data and can also be used as the system boot volume for your EC2 instance. Since HDD volumes cannot be used as a bootable volume, we can narrow down our options by selecting SSD volumes. In addition, SSD volumes are more suitable for transactional database workloads, as shown in the table below:

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"> <li>- Best for <b>transactional workloads</b></li> <li>- Critical business applications that require sustained IOPS performance</li> <li>- Large database workloads such as MongoDB, Oracle, Microsoft SQL Server and many others...</li> </ul>	<ul style="list-style-type: none"> <li>- Best for <b>large streaming workloads</b> requiring consistent, fast throughput at a low price</li> <li>- Big data, Data warehouses, Log processing</li> <li>- Throughput-oriented storage for large volumes of data that is <b>infrequently accessed</b></li> </ul>
Cost	moderate / high 	low 
Dominant Performance Attribute	IOPS	Throughput (MiB/s)



TutorialsDojo

General Purpose SSD (gp2) volumes offer cost-effective storage that is ideal for a broad range of workloads. These volumes deliver single-digit millisecond latencies and the ability to burst to 3,000 IOPS for extended periods of time. AWS designs gp2 volumes to deliver the provisioned performance 99% of the time. A gp2 volume can range in size from 1 GiB to 16 TiB.

Amazon EBS Provisioned IOPS SSD (io1) is incorrect because this is not the most cost-effective EBS type and is primarily used for critical business applications that require sustained IOPS performance.

Amazon EBS Throughput Optimized HDD (st1) is incorrect because this is primarily used for frequently accessed, throughput-intensive workloads. Although it is a low-cost HDD volume, it cannot be used as a system boot volume.

Amazon EBS Cold HDD (sc1) is incorrect. Although Amazon EBS Cold HDD provides lower cost HDD volume compared to General Purpose SSD, it cannot be used as a system boot volume.

Reference:

[https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes\\_gp2](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_gp2)

Amazon EBS Overview - SSD vs HDD:

<https://www.youtube.com/watch?v=LW7x8wyLFvw>

Check out this Amazon EBS Cheat Sheet:

<https://tutorialsdojo.com/amazon-ebs/>

## QUESTION 298

A financial company wants to store their data in Amazon S3 but at the same time, they want to store their frequently accessed data locally on their on-premises server. This is due to the fact that they do not have the option to extend their on-premises storage, which is why they are looking for a durable and scalable storage service to use in AWS.

What is the best solution for this scenario?

- A. Use Amazon Glacier.
- B. Use the Amazon Storage Gateway - Cached Volumes.
- C. Use a fleet of EC2 instances with EBS volumes to store the commonly used data.

D. Use both Elasticache and S3 for frequently accessed data.

Answer: B

Explanation:

By using Cached volumes, you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally in your on-premises network. Cached volumes offer substantial cost savings on primary storage and minimize the need to scale your storage on-premises. You also retain low-latency access to your frequently accessed data. This is the best solution for this scenario.

Using a fleet of EC2 instances with EBS volumes to store the commonly used data is incorrect because an EC2 instance is not a storage service and it does not provide the required durability and scalability.

Using both Elasticache and S3 for frequently accessed data is incorrect as this is not efficient. Moreover, the question explicitly said that the frequently accessed data should be stored locally on their on-premises server and not on AWS.

Using Amazon Glacier is incorrect as this is mainly used for data archiving.

Reference:

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

Check out this AWS Storage Gateway Cheat Sheet:

<https://tutorialsdojo.com/aws-storage-gateway/>

---

### QUESTION 299

A company plans to use Route 53 instead of an ELB to load balance the incoming request to the web application. The system is deployed to two EC2 instances to which the traffic needs to be distributed. You want to set a specific percentage of traffic to go to each instance.

Which routing policy would you use?

- A. Weighted
- B. Geolocation
- C. Failover
- D. Latency

Answer: A

Explanation:

Weighted routing lets you associate multiple resources with a single domain name (tutorialsdojo.com) or subdomain name (portal.tutorialsdojo.com) and choose how much traffic is routed to each resource. This can be useful for a variety of purposes including load balancing and testing new versions of software.

You can set a specific percentage of how much traffic will be allocated to the resource by specifying the weights.

## ▼ Record 1

[Delete](#)

Routing policy <a href="#">Info</a> Weighted	Record name <a href="#">Info</a> portal.tutorialsdojo.com	Alias <input checked="" type="checkbox"/>
Record type <a href="#">Info</a> A – Routes traffic to an IPv4 address and so...		TTL (seconds) <a href="#">Info</a> 300  1m    1h    1d Recommended values: 60 to 172800 (two days)
Value <a href="#">Info</a> 192.0.2.255 Enter multiple values on separate lines.		
Weight 200	Health check - optional <a href="#">Info</a> Choose health check	Record ID <a href="#">Info</a> US West load balancer
The weight can be a number between 0 and 255. If you specify 0, Route 53 stops responding to DNS queries using this record.		

For example, if you want to send a tiny portion of your traffic to one resource and the rest to another resource, you might specify weights of 1 and 255. The resource with a weight of 1 gets 1th of the traffic (1+255), and the other resource gets 255ths (255+255).

You can gradually change the balance by changing the weights. If you want to stop sending traffic to a resource, you can change the weight for that record to 0.

Hence, the correct answer is Weighted.

Latency is incorrect because you cannot set a specific percentage of traffic for the 2 EC2 instances with this routing policy. Latency routing policy is primarily used when you have resources in multiple AWS Regions and if you need to automatically route traffic to a specific AWS Region that provides the best latency with less round-trip time.

Failover is incorrect because this type is commonly used if you want to set up an active-passive failover configuration for your web application.

Geolocation is incorrect because this is more suitable for routing traffic based on the location of your users, and not for distributing a specific percentage of traffic to two AWS resources.

Reference:

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

Amazon Route 53 Overview:

<https://youtu.be/Su308t19ubY>

Check out this Amazon Route 53 Cheat Sheet:

<https://tutorialsdojo.com/amazon-route-53/>

## QUESTION 300

A financial analytics application that collects, processes and analyzes stock data in real-time is using Kinesis Data Streams. The producers continually push data to Kinesis Data Streams while the consumers process the data in real time. In Amazon Kinesis, where can the consumers store their results? (Select TWO.)

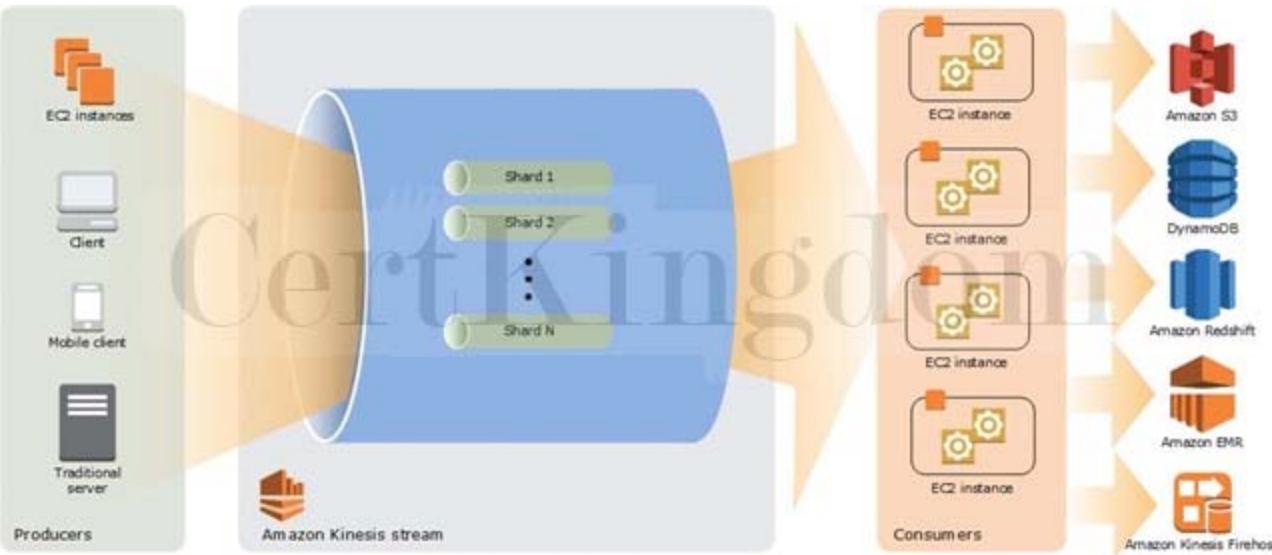
- A. Amazon Athena
- B. Glacier Select
- C. Amazon Redshift
- D. AWS Glue
- E. Amazon S3

Answer: C,E

Explanation:

In Amazon Kinesis, the producers continually push data to Kinesis Data Streams and the consumers process the data in real time. Consumers (such as a custom application running on Amazon EC2, or an Amazon Kinesis Data Firehose delivery stream) can store their results using an AWS service such as Amazon DynamoDB, Amazon Redshift, or Amazon S3.

Hence, Amazon S3 and Amazon Redshift are the correct answers. The following diagram illustrates the high-level architecture of Kinesis Data Streams:



Glacier Select is incorrect because this is not a storage service. It is primarily used to run queries directly on data stored in Amazon Glacier, retrieving only the data you need out of your archives to use for analytics.

AWS Glue is incorrect because this is not a storage service. It is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics.

Amazon Athena is incorrect because this is just an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. It is not a storage service where you can store the results processed by the consumers.

Reference:

<http://docs.aws.amazon.com/streams/latest/dev/key-concepts.html>

Amazon Redshift Overview:

<https://youtu.be/jILERNzhHOg>

Check out this Amazon Kinesis Cheat Sheet:

<https://tutorialsdojo.com/amazon-kinesis/>

## QUESTION 301

A Solutions Architect is working for a fast-growing startup that just started operations during the past 3 months. They currently have an on-premises Active Directory and 10 computers. To save costs in procuring physical workstations, they decided to deploy virtual desktops for their new employees in a virtual private cloud in AWS. The new cloud infrastructure should leverage the existing security controls in AWS but can still communicate with their on-premises network.

Which set of AWS services will the Architect use to meet these requirements?

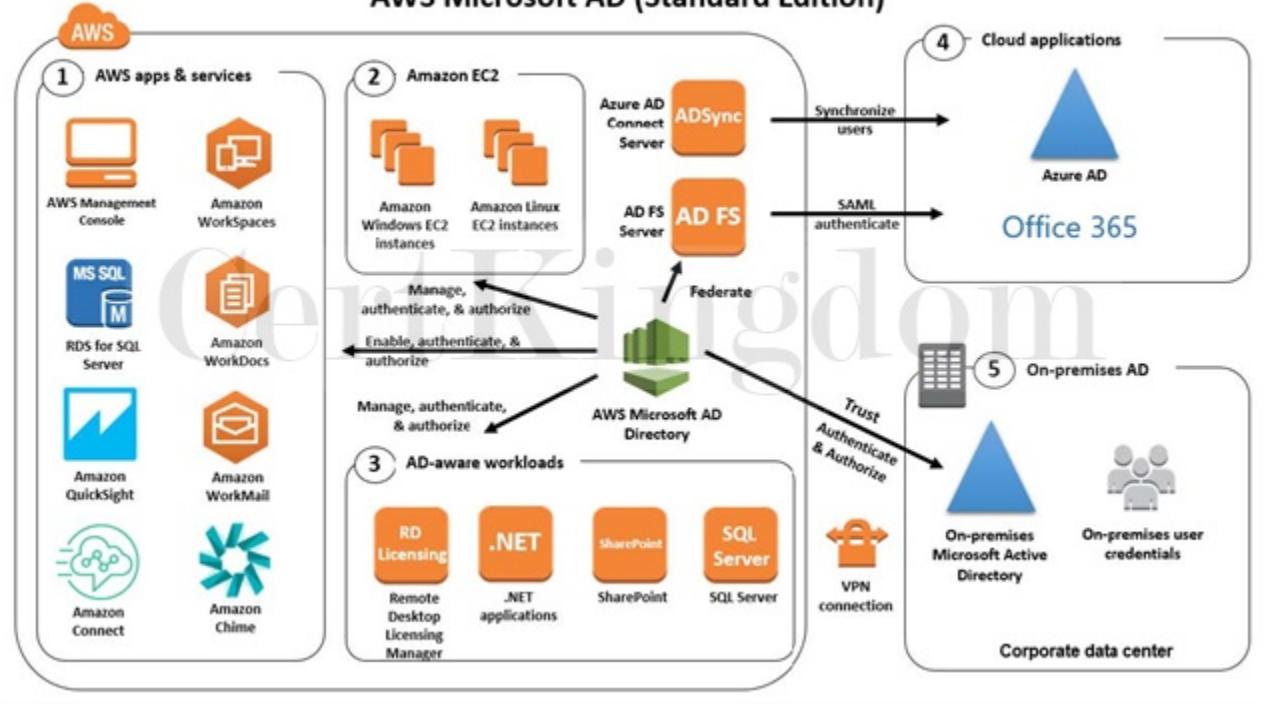
- A. AWS Directory Services, VPN connection, and Amazon S3
- B. AWS Directory Services, VPN connection, and Amazon Workspaces
- C. AWS Directory Services, VPN connection, and ClassicLink
- D. AWS Directory Services, VPN connection, and AWS Identity and Access Management

Answer: B

Explanation:

For this scenario, the best answer is: AWS Directory Services, VPN connection, and Amazon Workspaces.

## Some Ways You Can Use AWS Microsoft AD (Standard Edition)



First, you need a VPN connection to connect the VPC and your on-premises network. Second, you need AWS Directory Services to integrate with your on-premises Active Directory and lastly, you need to use Amazon Workspaces to create the needed virtual desktops in your VPC.

References:

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

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html>

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

AWS Identity Services Overview:

<https://www.youtube.com/watch?v=AIdUw0i8rr0>

Check out these cheat sheets on AWS Directory Service, Amazon VPC, and Amazon WorkSpaces:

<https://tutorialsdojo.com/aws-directory-service/>

<https://tutorialsdojo.com/amazon-vpc/>

### QUESTION 302

An application is hosted in an Auto Scaling group of EC2 instances. To improve the monitoring process, you have to configure the current capacity to increase or decrease based on a set of scaling adjustments. This should be done by specifying the scaling metrics and threshold values for the CloudWatch alarms that trigger the scaling process.

Which of the following is the most suitable type of scaling policy that you should use?

- A. Target tracking scaling
- B. Scheduled Scaling
- C. Simple scaling
- D. Step scaling

Answer: D

Explanation:

With step scaling, you choose scaling metrics and threshold values for the CloudWatch alarms that trigger the scaling process as well as define how your scalable target should be scaled when a threshold is in breach for a specified number of evaluation periods. Step scaling policies increase or decrease the current capacity of a scalable target based on a set of scaling adjustments, known as step adjustments. The adjustments vary based on the size of the alarm breach. After a scaling activity is started, the policy continues to respond to additional alarms, even while a scaling activity is in progress. Therefore, all

alarms that are breached are evaluated by Application Auto Scaling as it receives the alarm messages. When you configure dynamic scaling, you must define how to scale in response to changing demand. For example, you have a web application that currently runs on two instances and you want the CPU utilization of the Auto Scaling group to stay at around 50 percent when the load on the application changes. This gives you extra capacity to handle traffic spikes without maintaining an excessive amount of idle resources. You can configure your Auto Scaling group to scale automatically to meet this need. The policy type determines how the scaling action is performed.

The screenshot shows the configuration for a step scaling policy named 'Increase Group Size'. It is triggered by an alarm named 'SystemBusy' when CPUUtilization breaches the threshold of 50 for 60 seconds. The policy adds instances in four steps: 1 instance at 50 CPUUtilization <= 60, 2 instances at 60 CPUUtilization <= 70, 4 instances at 70 CPUUtilization <= 80, and 8 instances at 80 CPUUtilization < infinity. A note indicates that 300 seconds are needed to warm up after each step. There is also a link to 'Create a simple scaling policy'.

Amazon EC2 Auto Scaling supports the following types of scaling policies:

Target tracking scaling - Increase or decrease the current capacity of the group based on a target value for a specific metric. This is similar to the way that your thermostat maintains the temperature of your home ““ you select a temperature and the thermostat does the rest.

Step scaling - Increase or decrease the current capacity of the group based on a set of scaling adjustments, known as step adjustments, that vary based on the size of the alarm breach.

Simple scaling - Increase or decrease the current capacity of the group based on a single scaling adjustment.

If you are scaling based on a utilization metric that increases or decreases proportionally to the number of instances in an Auto Scaling group, then it is recommended that you use target tracking scaling policies. Otherwise, it is better to use step scaling policies instead.

Hence, the correct answer in this scenario is Step Scaling.

Target tracking scaling is incorrect because the target tracking scaling policy increases or decreases the current capacity of the group based on a target value for a specific metric, instead of a set of scaling adjustments.

Simple scaling is incorrect because the simple scaling policy increases or decreases the current capacity of the group based on a single scaling adjustment, instead of a set of scaling adjustments.

Scheduled Scaling is incorrect because the scheduled scaling policy is based on a schedule that allows you to set your own scaling schedule for predictable load changes. This is not considered as one of the types of dynamic scaling.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-on-demand.html>

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

## QUESTION 303

A company has an On-Demand EC2 instance with an attached EBS volume. There is a scheduled job that creates a snapshot of this EBS volume every midnight at 12 AM when the instance is not used. One

night, there has been a production incident where you need to perform a change on both the instance and on the EBS volume at the same time when the snapshot is currently taking place. Which of the following scenario is true when it comes to the usage of an EBS volume while the snapshot is in progress?

- A. The EBS volume cannot be used until the snapshot completes.
- B. The EBS volume can be used in read-only mode while the snapshot is in progress.
- C. The EBS volume can be used while the snapshot is in progress.
- D. The EBS volume cannot be detached or attached to an EC2 instance until the snapshot completes

Answer: C

Explanation:

Snapshots occur asynchronously; the point-in-time snapshot is created immediately, but the status of the snapshot is pending until the snapshot is complete (when all of the modified blocks have been transferred to Amazon S3), which can take several hours for large initial snapshots or subsequent snapshots where many blocks have changed.

Snapshots > Create Snapshot

## Create Snapshot

Select resource type  Volume  Instance

Instance ID\*  C i

Description  i

Exclude root volume

Volume ID	Volume Type	Encryption
vol-11111111	Root	Encrypted
vol-22222222	EBS	Not Encrypted
vol-33333333	EBS	Not Encrypted
vol-44444444	EBS	Not Encrypted

Copy tags from volume

Key (127 characters maximum) Value (255 characters maximum)

This resource currently has no tags  
Choose the Add tag button or click to add a Name tag

Add Tag 50 remaining (Up to 50 tags maximum)

\* Required Cancel Create Snapshot

While it is completing, an in-progress snapshot is not affected by ongoing reads and writes to the volume hence, you can still use the EBS volume normally.

When you create an EBS volume based on a snapshot, the new volume begins as an exact replica of the original volume that was used to create the snapshot. The replicated volume loads data lazily in the background so that you can begin using it immediately. If you access data that hasn't been loaded yet, the volume immediately downloads the requested data from Amazon S3, and then continues loading the rest of the volume's data in the background.

References:

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

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

Check out this Amazon EBS Cheat Sheet:  
<https://tutorialsdojo.com/amazon-ebs/>

---

## QUESTION 304

A company has 10 TB of infrequently accessed financial data files that would need to be stored in AWS. These data would be accessed infrequently during specific weeks when they are retrieved for auditing purposes. The retrieval time is not strict as long as it does not exceed 24 hours.

Which of the following would be a secure, durable, and cost-effective solution for this scenario?

- A. Upload the data to S3 and set a lifecycle policy to transition data to Glacier after 0 days.
- B. Upload the data to Amazon FSx for Windows File Server using the Server Message Block (SMB) protocol.
- C. Upload the data to S3 then use a lifecycle policy to transfer data to S3 One Zone-IA.
- D. Upload the data to S3 then use a lifecycle policy to transfer data to S3-IA.

Answer: A

Explanation:

Glacier is a cost-effective archival solution for large amounts of data. Bulk retrievals are S3 Glacier's lowest-cost retrieval option, enabling you to retrieve large amounts, even petabytes, of data inexpensively in a day. Bulk retrievals typically complete within 5 “ 12 hours. You can specify an absolute or relative time period (including 0 days) after which the specified Amazon S3 objects should be transitioned to Amazon Glacier.

Hence, the correct answer is the option that says: Upload the data to S3 and set a lifecycle policy to transition data to Glacier after 0 days.

Glacier has a management console that you can use to create and delete vaults. However, you cannot directly upload archives to Glacier by using the management console. To upload data such as photos, videos, and other documents, you must either use the AWS CLI or write code to make requests by using either the REST API directly or by using the AWS SDKs.

Take note that uploading data to the S3 Console and setting its storage class of "Glacier" is a different story as the proper way to upload data to Glacier is still via its API or CLI. In this way, you can set up your vaults and configure your retrieval options. If you uploaded your data using the S3 console then it will be managed via S3 even though it is internally using a Glacier storage class.

Uploading the data to S3 then using a lifecycle policy to transfer data to S3-IA is incorrect because using Glacier would be a more cost-effective solution than using S3-IA.

A. Since the required retrieval period

should not exceed more than a day, Glacier would be the best choice.

Uploading the data to Amazon FSx for Windows File Server using the Server Message Block (SMB) protocol is incorrect because this option costs more than Amazon Glacier, which is more suitable for storing infrequently accessed data. Amazon FSx for Windows File Server provides fully managed, highly reliable, and scalable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol.

Uploading the data to S3 then using a lifecycle policy to transfer data to S3 One Zone-IA is incorrect because with S3 One Zone-IA, the data will only be stored in a single availability zone and thus, this storage solution is not durable. It also costs more compared to Glacier.

References:

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

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

<https://docs.aws.amazon.com/amazonglacier/latest/dev/uploading-an-archive.html>

Amazon S3 and S3 Glacier Overview:

<https://www.youtube.com/watch?v=1ymyeN2tki4>

Check out this Amazon S3 Glacier Cheat Sheet:

<https://tutorialsdojo.com/amazon-glacier/>

---

## QUESTION 305

A news company is planning to use a Hardware Security Module (CloudHSM) in AWS for secure key storage of their web applications. You have launched the CloudHSM cluster but after just a few hours, a support staff mistakenly attempted to log in as the administrator three times using an invalid password in the Hardware Security Module. This has caused the HSM to be zeroized, which means that the encryption keys on it have been wiped. Unfortunately, you did not have a copy of the keys stored anywhere else.

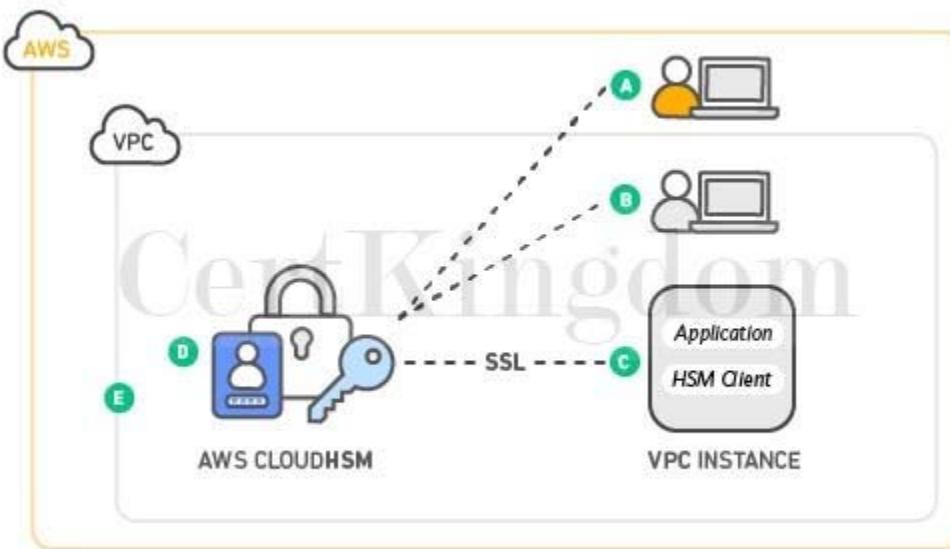
How can you obtain a new copy of the keys that you have stored on Hardware Security Module?

- A. Restore a snapshot of the Hardware Security Module.
- B. Use the Amazon CLI to get a copy of the keys.
- C. The keys are lost permanently if you did not have a copy.
- D. Contact AWS Support and they will provide you a copy of the keys.

Answer: C

Explanation:

Attempting to log in as the administrator more than twice with the wrong password zeroizes your HSM appliance. When an HSM is zeroized, all keys, certificates, and other data on the HSM is destroyed. You can use your cluster's security group to prevent an unauthenticated user from zeroizing your HSM.



Amazon does not have access to your keys nor to the credentials of your Hardware Security Module (HSM) and therefore has no way to recover your keys if you lose your credentials. Amazon strongly recommends that you use two or more HSMs in separate Availability Zones in any production CloudHSM Cluster to avoid loss of cryptographic keys.

Refer to the CloudHSM FAQs for reference:

Q: Could I lose my keys if a single HSM instance fails?

---

## QUESTION 306

A company needs to set up a cost-effective architecture for a log processing application that has frequently accessed, throughput-intensive workloads with large, sequential I/O operations. The application should be hosted in an already existing On-Demand EC2 instance in the VPC. You have to attach a new EBS volume that will be used by the application.

Which of the following is the most suitable EBS volume type that you should use in this scenario?

- A. EBS Cold HDD (sc1)
- B. EBS Provisioned IOPS SSD (io1)
- C. EBS General Purpose SSD (gp2)
- D. EBS Throughput Optimized HDD (st1)

Answer: D

Explanation:

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"><li>- Best for <b>transactional workloads</b></li><li>- Critical business applications that require sustained IOPS performance</li><li>- Large database workloads such as MongoDB, Oracle, Microsoft SQL Server and many others...</li></ul>	<ul style="list-style-type: none"><li>- Best for <i>large streaming workloads</i> requiring consistent, fast throughput at a low price</li><li>- Big data, Data warehouses, Log processing</li><li>- Throughput-oriented storage for large volumes of data that is <i>infrequently accessed</i></li></ul>
Cost	moderate / high 	low 
Dominant Performance Attribute	IOPS	Throughput (MiB/s)



Since the scenario has workloads with large, sequential I/O operations, we can narrow down our options by selecting HDD volumes, instead of SDD volumes which are more suitable for small, random I/O operations.

Throughput Optimized HDD (st1) volumes provide low-cost magnetic storage that defines performance in terms of throughput rather than IOPS. This volume type is a good fit for large, sequential workloads such as Amazon EMR, ETL, data warehouses, and log processing. Bootable st1 volumes are not supported.

Throughput Optimized HDD (st1) volumes, though similar to Cold HDD (sc1) volumes, are designed to support frequently accessed data.

EBS Provisioned IOPS SSD (io1) is incorrect because Amazon EBS Provisioned IOPS SSD is not the most cost-effective EBS type and is primarily used for critical business applications that require sustained IOPS performance.

EBS General Purpose SSD (gp2) is incorrect. Although an Amazon EBS General Purpose SSD volume balances price and performance for a wide variety of workloads, it is not suitable for frequently accessed, throughput-intensive workloads. Throughput Optimized HDD is a more suitable option to use than General Purpose SSD.

EBS Cold HDD (sc1) is incorrect. Although this provides lower cost HDD volume compared to General Purpose SSD, it is much suitable for less frequently accessed workloads.

Reference:

[https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes\\_st1](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_st1)

Amazon EBS Overview - SSD vs HDD:

<https://www.youtube.com/watch?v=LW7x8wyLFvw&t=8s>

Check out this Amazon EBS Cheat Sheet:

<https://tutorialsdojo.com/amazon-ebs/>

---

## QUESTION 307

A business plans to deploy an application on EC2 instances within an Amazon VPC and is considering adopting a Network Load Balancer to distribute incoming traffic among the instances. A solutions architect needs to suggest a solution that will enable the security team to inspect traffic entering and exiting their VPC.

Which approach satisfies the requirements?

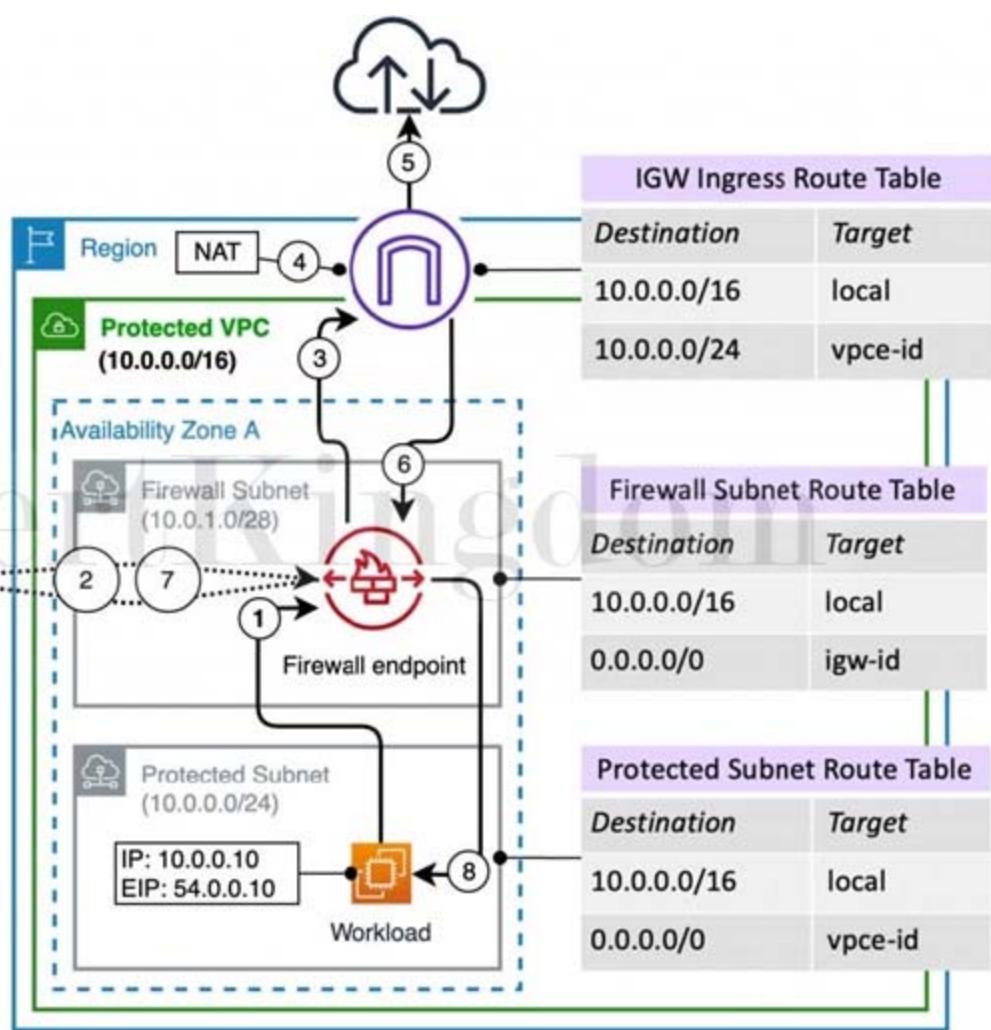
- A. Create a firewall at the subnet level using the Amazon Detective service. Inspect the ingress and egress traffic using the VPC Reachability Analyzer.
- B. Use the Network Access Analyzer service on the application's VPC for inspecting ingress and egress traffic. Create a new Network Access Scope to filter and analyze all incoming and outgoing requests.
- C. Create a firewall using the AWS Network Firewall service at the VPC level then add custom rule groups for inspecting ingress and egress traffic. Update the necessary VPC route tables.
- D. Enable Traffic Mirroring on the Network Load Balancer and forward traffic to the instances. Create a traffic mirror filter to inspect the ingress and egress of data that traverses your Amazon VPC.

Answer: C

Explanation:

AWS Network Firewall is a stateful, managed, network firewall, and intrusion detection and prevention service for your virtual private cloud (VPC). With Network Firewall, you can filter traffic at the perimeter of your VPC. This includes traffic going to and coming from an internet gateway, NAT gateway, or over VPN or AWS Direct Connect. Network Firewall uses Suricata – an open-source intrusion prevention system (IPS) for stateful inspection.

The diagram below shows an AWS Network firewall deployed in a single availability zone and traffic flow for a workload in a public subnet:



You can use Network Firewall to monitor and protect your Amazon VPC traffic in a number of ways, including the following:

- Pass traffic through only from known AWS service domains or IP address endpoints, such as Amazon S3.
- Use custom lists of known bad domains to limit the types of domain names that your applications can access.
- Perform deep packet inspection on traffic entering or leaving your VPC.
- Use stateful protocol detection to filter protocols like HTTPS, independent of the port used.

Therefore, the correct answer is: Create a firewall using the AWS Network Firewall service at the VPC level then add custom rule groups for inspecting ingress and egress traffic. Update the necessary VPC route tables.

The option that says: Use the Network Access Analyzer service on the application's VPC for inspecting ingress and egress traffic. Create a new Network Access Scope to filter and analyze all incoming and outgoing requests is incorrect. Network Access Analyzer is a feature of VPC that reports on unintended access to your AWS resources based on the security and compliance that you set. This service is not capable of performing deep packet inspection on traffic entering or leaving your VPC, unlike AWS Network Firewall.

The option that says: Create a firewall at the subnet level using the Amazon Detective service. Inspect the ingress and egress traffic using the VPC Reachability Analyzer is incorrect because a firewall must be created at the VPC level and not at the subnet level. Moreover, Amazon Detective can't be used to create a firewall. This service just automatically collects log data from your AWS resources to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities in your AWS account. For this scenario, you have to use the AWS Network Firewall instead.

The option that says: Enable Traffic Mirroring on the Network Load Balancer and forward traffic to the instances. Create a traffic mirror filter to inspect the ingress and egress of data that traverses your Amazon VPC is incorrect as this alone accomplishes nothing. It would make more sense if you redirect the traffic to an EC2 instance where an Intrusion Detection System (IDS) is running. Remember that Traffic Mirroring is simply an Amazon VPC feature that you can use to copy network traffic from an

elastic network interface. Traffic mirror filters can't inspect the actual packet of the incoming and outgoing traffic.

#### References:

<https://aws.amazon.com/blogs/networking-and-content-delivery/deployment-models-for-aws-network-firewall/>  
<https://docs.aws.amazon.com/network-firewall/latest/developerguide/what-is-aws-network-firewall.html>

---

### QUESTION 308

A company has an application hosted in an Auto Scaling group of Amazon EC2 instances across multiple Availability Zones behind an Application Load Balancer. There are several occasions where some instances are automatically terminated after failing the HTTPS health checks in the ALB and then purges all the ephemeral logs stored in the instance. A Solutions Architect must implement a solution that collects all of the application and server logs effectively. She should be able to perform a root cause analysis based on the logs, even if the Auto Scaling group immediately terminated the instance.

What is the EASIEST way for the Architect to automate the log collection from the Amazon EC2 instances?

A. Add a lifecycle hook to your Auto Scaling group to move instances in the Terminating state to the Terminating:Wait state to delay the termination of the unhealthy Amazon EC2 instances. Configure a CloudWatch Events rule for the EC2 Instance Terminate Successful Auto Scaling Event with an associated Lambda function. Set up the AWS Systems Manager Run Command service to run a script that collects and uploads the application logs from the instance to a CloudWatch Logs group. Resume the instance termination once all the logs are sent.

B. Add a lifecycle hook to your Auto Scaling group to move instances in the Terminating state to the Terminating:Wait state to delay the termination of the unhealthy Amazon EC2 instances. Set up AWS Step Functions to collect the application logs and send them to a CloudWatch Log group. Configure the solution to resume the instance termination as soon as all the logs were successfully sent to CloudWatch Logs.

C. Add a lifecycle hook to your Auto Scaling group to move instances in the Terminating state to the Terminating:Wait state to delay the termination of unhealthy Amazon EC2 instances. Configure a CloudWatch Events rule for the EC2 Instance-terminate Lifecycle Action Auto Scaling Event with an associated Lambda function. Trigger the CloudWatch agent to push the application logs and then resume the instance termination once all the logs are sent to CloudWatch Logs.

D. Add a lifecycle hook to your Auto Scaling group to move instances in the Terminating state to the Pending:Wait state to delay the termination of the unhealthy Amazon EC2 instances. Configure a CloudWatch Events rule for the EC2 Instance-terminate Lifecycle Action Auto Scaling Event with an associated Lambda function. Set up an AWS Systems Manager Automation script that collects and uploads the application logs from the instance to a CloudWatch Logs group. Configure the solution to only resume the instance termination once all the logs were successfully sent.

Answer: C

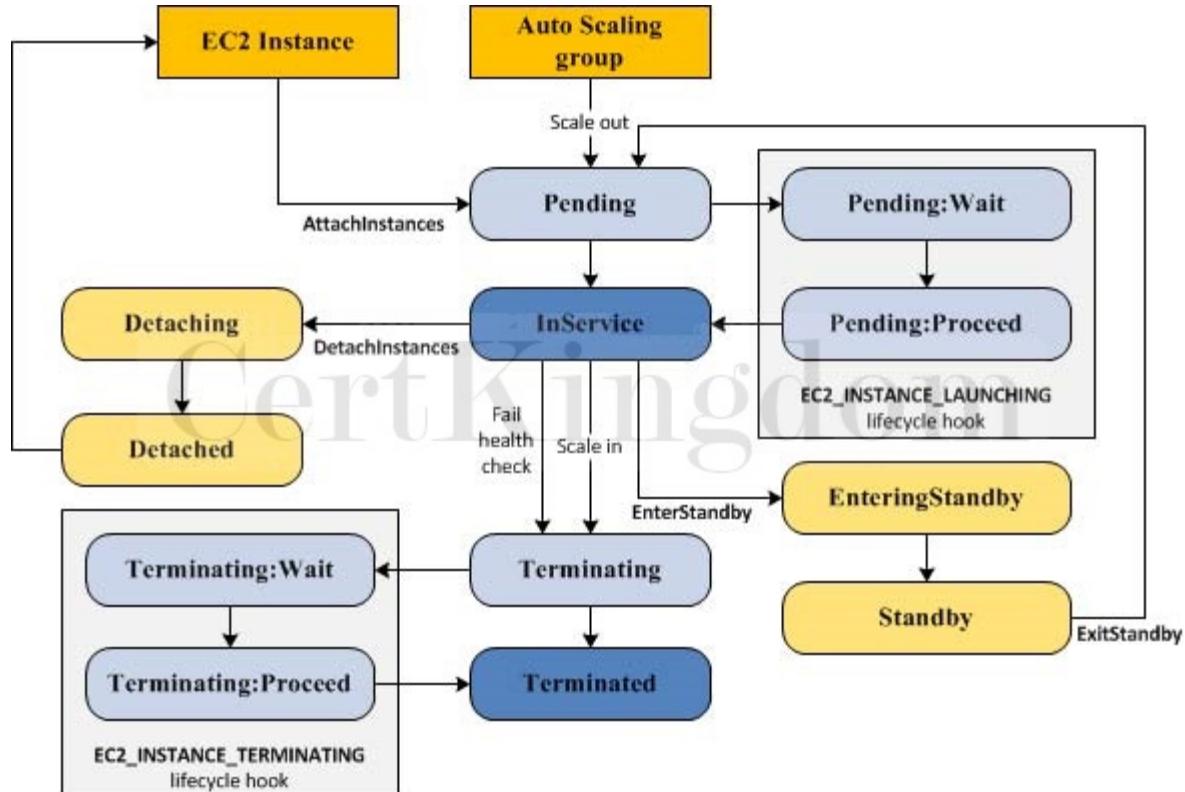
#### Explanation:

The EC2 instances in an Auto Scaling group have a path, or lifecycle, that differs from that of other EC2 instances. The lifecycle starts when the Auto Scaling group launches an instance and puts it into service. The lifecycle ends when you terminate the instance, or the Auto Scaling group takes the instance out of service and terminates it.

You can add a lifecycle hook to your Auto Scaling group so that you can perform custom actions when instances launch or terminate.

When Amazon EC2 Auto Scaling responds to a scale out event, it launches one or more instances. These instances start in the Pending state. If you added an autoscaling:EC2\_INSTANCE\_LAUNCHING lifecycle hook to your Auto Scaling group, the instances move from the Pending state to the Pending:Wait state. After you complete the lifecycle action, the instances enter the Pending:Proceed state. When the instances are fully configured, they are attached to the Auto Scaling group and they enter the InService state.

When Amazon EC2 Auto Scaling responds to a scale in event, it terminates one or more instances. These instances are detached from the Auto Scaling group and enter the Terminating state. If you added an autoscaling:EC2\_INSTANCE\_TERMINATING lifecycle hook to your Auto Scaling group, the instances move from the Terminating state to the Terminating:Wait state. After you complete the lifecycle action, the instances enter the Terminating:Proceed state. When the instances are fully terminated, they enter the Terminated state.



Using CloudWatch agent is the most suitable tool to use to collect the logs. The unified CloudWatch agent enables you to do the following:

- Collect more system-level metrics from Amazon EC2 instances across operating systems. The metrics can include in-guest metrics, in addition to the metrics for EC2 instances. The additional metrics that can be collected are listed in Metrics Collected by the CloudWatch Agent.
- Collect system-level metrics from on-premises servers. These can include servers in a hybrid environment as well as servers not managed by AWS.
- Retrieve custom metrics from your applications or services using the StatsD and collectd protocols. StatsD is supported on both Linux servers and servers running Windows Server. collectd is supported only on Linux servers.
- Collect logs from Amazon EC2 instances and on-premises servers, running either Linux or Windows Server.



- CloudWatch
- Dashboards
- Alarms
- ALARM 2
- INSUFFICIENT 2
- OK 6
- Billing
- Logs
- Log groups
- Insights
- Metrics
- Events
- Rules
- Event Buses
- ServiceLens NEW
- Service Map
- Traces
- Synthetics NEW
- Canaries
- Thresholds
- Contributor Insights NEW
- Settings NEW

## Favorites

[Add a dashboard](#)

## Step 1: Create rule

Create rules to invoke Targets based on Events happening in your AWS environment.

## Event Source

Build or customize an Event Pattern or set a Schedule to invoke Targets.

 Event Pattern [?](#)  Schedule [?](#)

Build event pattern to match events by service

Service Name

Auto Scaling

Event Type

Instance Launch and Terminate

 Any instance event Specific instance event(s)

- EC2 Instance Launch Successful
- EC2 Instance Launch Unsuccessful
- EC2 Instance Terminate Successful
- EC2 Instance Terminate Unsuccessful
- EC2 Instance-launch Lifecycle Action
- EC2 Instance-terminate Lifecycle Action

## Event Pattern Preview

[Copy to clipboard](#) [Edit](#)

```
{  
  "source": [  
    "aws.autoscaling"  
  ],  
  "detail-type": [  
    "EC2 Instance Launch Successful",  
    "EC2 Instance Terminate Successful",  
    "EC2 Instance Launch Unsuccessful",  
    "EC2 Instance Terminate Unsuccessful",  
    "EC2 Instance-launch Lifecycle Action",  
    "EC2 Instance-terminate Lifecycle Action"  
  ]  
}
```

TutorialDojo

TutorialDojo

You can store and view the metrics that you collect with the CloudWatch agent in CloudWatch just as you can with any other CloudWatch metrics. The default namespace for metrics collected by the CloudWatch agent is CWAgent, although you can specify a different namespace when you configure the agent.

Hence, the correct answer is: Add a lifecycle hook to your Auto Scaling group to move instances in the Terminating state to the Terminating:Wait state to delay the termination of unhealthy Amazon EC2 instances. Configure a CloudWatch Events rule for the EC2 Instance-terminate Lifecycle Action Auto Scaling Event with an associated Lambda function. Trigger the CloudWatch agent to push the application logs and then resume the instance termination once all the logs are sent to CloudWatch Logs.

The option that says: Add a lifecycle hook to your Auto Scaling group to move instances in the Terminating state to the Pending:Wait state to delay the termination of the unhealthy Amazon EC2 instances. Configure a CloudWatch Events rule for the EC2 Instance-terminate Lifecycle Action Auto Scaling Event with an associated Lambda function. Set up an AWS Systems Manager Automation script that collects and uploads the application logs from the instance to a CloudWatch Logs group. Configure the solution to only resume the instance termination once all the logs were successfully sent is incorrect because the Pending:Wait state refers to the scale-out action in Amazon EC2 Auto Scaling and not for scale-in or for terminating the instances.

The option that says: Add a lifecycle hook to your Auto Scaling group to move instances in the Terminating state to the Terminating:Wait state to delay the termination of the unhealthy Amazon EC2 instances. Set up AWS Step Functions to collect the application logs and send them to a CloudWatch Log group. Configure the solution to resume the instance termination as soon as all the logs were successfully sent to CloudWatch Logs is incorrect because using AWS Step Functions is inappropriate in collecting the logs from your EC2 instances. You should use a CloudWatch agent instead.

The option that says: Add a lifecycle hook to your Auto Scaling group to move instances in the Terminating state to the Terminating:Wait state to delay the termination of the unhealthy Amazon EC2 instances. Configure a CloudWatch Events rule for the EC2 Instance Terminate Successful Auto Scaling

Event with an associated Lambda function. Set up the AWS Systems Manager Run Command service to run a script that collects and uploads the application logs from the instance to a CloudWatch Logs group. Resume the instance termination once all the logs are sent is incorrect because although this solution could work, it entails a lot of effort to write a custom script that the AWS Systems Manager Run Command will run. Remember that the scenario asks for a solution that you can implement with the least amount of effort. This solution can be simplified by automatically uploading the logs using a CloudWatch Agent. You have to use the EC2 Instance-terminate Lifecycle Action event instead.

References:

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

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/cloud-watch-events.html#terminate-successful>

<https://aws.amazon.com/premiumsupport/knowledge-center/auto-scaling-delay-termination/>

Check out this AWS Auto Scaling Cheat Sheet:

<https://tutorialsdojo.com/aws-auto-scaling/>

## QUESTION 309

A Solutions Architect is trying to enable Cross-Region Replication to an S3 bucket but this option is disabled. Which of the following options is a valid reason for this?

- A. The Cross-Region Replication feature is only available for Amazon S3 - Infrequent Access.
- B. The Cross-Region Replication feature is only available for Amazon S3 - One Zone-IA
- C. This is a premium feature which is only for AWS Enterprise accounts.
- D. In order to use the Cross-Region Replication feature in S3, you need to first enable versioning on the bucket.

Answer: D

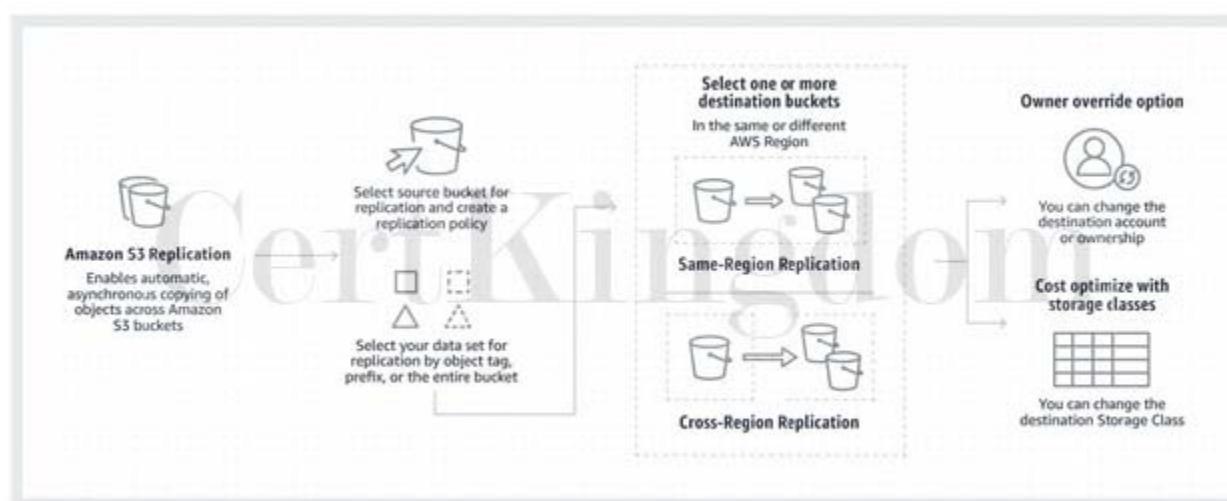
Explanation:

To enable the cross-region replication feature in S3, the following items should be met:

The source and destination buckets must have versioning enabled.

The source and destination buckets must be in different AWS Regions.

Amazon S3 must have permissions to replicate objects from that source bucket to the destination bucket on your behalf.



The options that say: The Cross-Region Replication feature is only available for Amazon S3 - One Zone-IA and The Cross-Region Replication feature is only available for Amazon S3 - Infrequent Access are incorrect as this feature is available to all types of S3 classes.

The option that says: This is a premium feature which is only for AWS Enterprise accounts is incorrect as this CRR feature is available to all Support Plans.

References:

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

<https://aws.amazon.com/blogs/aws/new-cross-region-replication-for-amazon-s3/>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

---

## QUESTION 310

A global news network created a CloudFront distribution for their web application. However, you noticed that the application's origin server is being hit for each request instead of the AWS Edge locations, which serve the cached objects. The issue occurs even for the commonly requested objects.

What could be a possible cause of this issue?

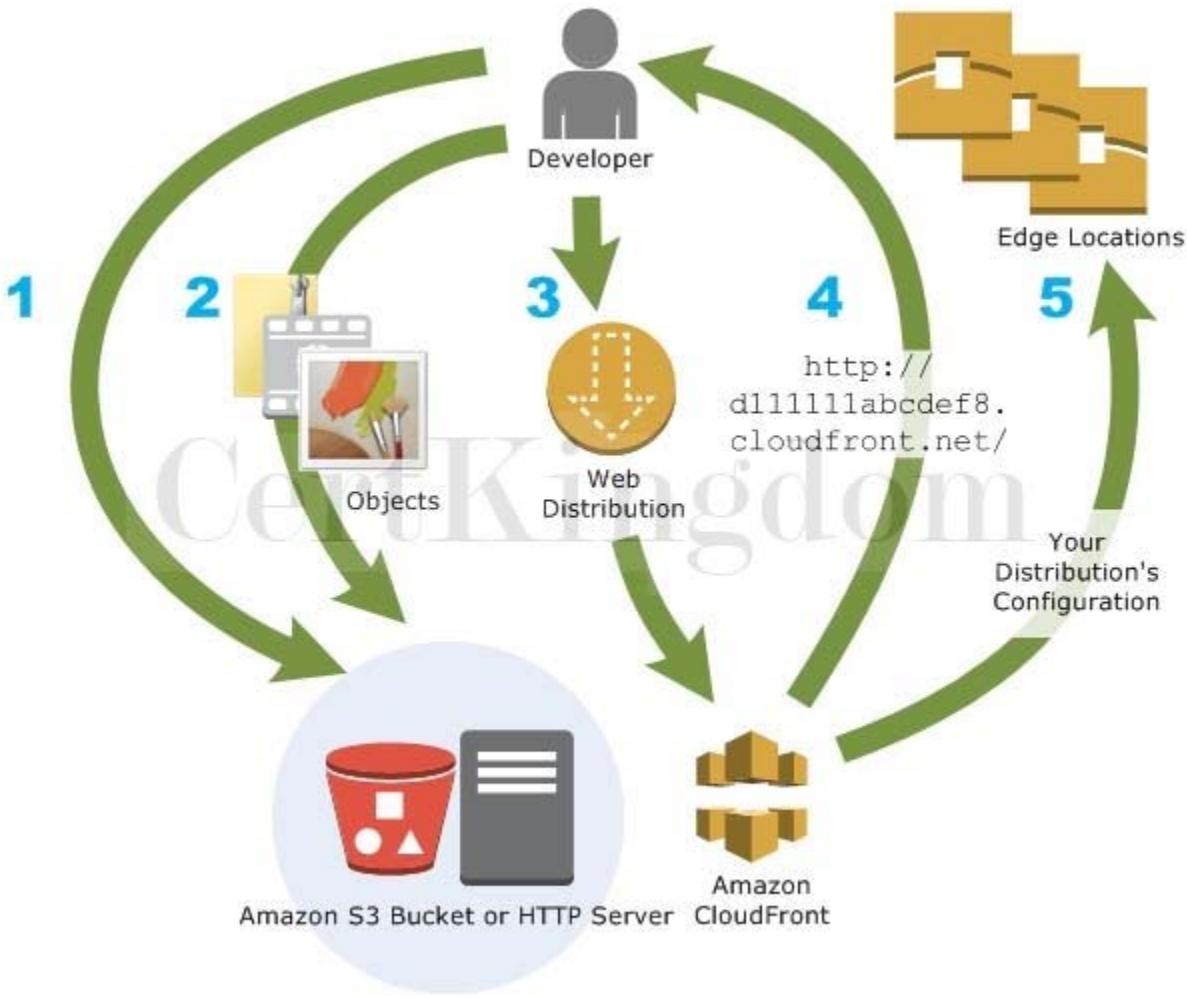
- A. The Cache-Control max-age directive is set to zero.
- B. The file sizes of the cached objects are too large for CloudFront to handle.
- C. An object is only cached by Cloudfront once a successful request has been made hence, the objects were not requested before, which is why the request is still directed to the origin server.
- D. There are two primary origins configured in your Amazon CloudFront Origin Group.

Answer: A

Explanation:

You can control how long your objects stay in a CloudFront cache before CloudFront forwards another request to your origin. Reducing the duration allows you to serve dynamic content. Increasing the duration means your users get better performance because your objects are more likely to be served directly from the edge cache. A longer duration also reduces the load on your origin.

Typically, CloudFront serves an object from an edge location until the cache duration that you specified passes “” that is, until the object expires. After it expires, the next time the edge location gets a user request for the object, CloudFront forwards the request to the origin server to verify that the cache contains the latest version of the object.



The Cache-Control and Expires headers control how long objects stay in the cache. The Cache-Control max-age directive lets you specify how long (in seconds) you want an object to remain in the cache before CloudFront gets the object again from the origin server. The minimum expiration time CloudFront supports is 0 seconds for web distributions and 3600 seconds for RTMP distributions.

In this scenario, the main culprit is that the Cache-Control max-age directive is set to a low value, which is why the request is always directed to your origin server.

Hence, the correct answer is: The Cache-Control max-age directive is set to zero.

The option that says: An object is only cached by CloudFront once a successful request has been made hence, the objects were not requested before, which is why the request is still directed to the origin server is incorrect because the issue also occurs even for the commonly requested objects. This means that these objects were successfully requested before but due to a zero Cache-Control max-age directive value, it causes this issue in CloudFront.

The option that says: The file sizes of the cached objects are too large for CloudFront to handle is incorrect because this is not related to the issue in caching.

The option that says: There are two primary origins configured in your Amazon CloudFront Origin Group is incorrect because you cannot set two origins in CloudFront in the first place. An origin group includes two origins which are the primary origin and the second origin that will be used for the actual failover. It also includes the failover criteria that you need to specify. In this scenario, the issue is more on the cache hit ratio and not about origin failovers.

Reference:

<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html>

Check out this Amazon CloudFront Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudfront/>

## QUESTION 311

An application is loading hundreds of JSON documents into an Amazon S3 bucket every hour which is registered in AWS Lake Formation as a data catalog. The Data Analytics team uses Amazon Athena to run analyses on these data, but due to the volume, most queries take a long time to complete.

What change should be made to improve the query performance while ensuring data security?

- A. Convert the JSON documents into CSV format. Provide fine-grained named resource access control to specific databases or tables in AWS Lake Formation.
- B. Transform the JSON data into Apache Parquet format. Ensure that the user has an `lakeformation:GetDataAccess` IAM permission for underlying data access control.
- C. Apply minification on the data and implement the Lake Formation tag-based access control (LFTBAC) authorization strategy to ensure security.
- D. Compress the data into GZIP format before storing it in the S3 bucket. Apply an IAM policy with `aws:SourceArn` and `aws:SourceAccount` global condition context keys in Lake Formation that prevents cross-service confused deputy problems and other security issues.

Answer: B

Explanation:

Amazon Athena supports a wide variety of data formats like CSV, TSV, JSON, or Textfiles and also supports open-source columnar formats such as Apache ORC and Apache Parquet. Athena also supports compressed data in Snappy, Zlib, LZO, and GZIP formats. By compressing, partitioning, and using columnar formats you can improve performance and reduce your costs.

Parquet and ORC file formats both support predicate pushdown (also called predicate filtering). Parquet and ORC both have blocks of data that represent column values. Each block holds statistics for the block, such as max/min values. When a query is being executed, these statistics determine whether the block should be read or skipped.

Athena charges you by the amount of data scanned per query. You can save on costs and get better performance if you partition the data, compress data, or convert it to columnar formats such as Apache Parquet.

Dataset	Size on Amazon S3	Query Run time	Data Scanned	Cost
Data stored as CSV files	1 TB	236 seconds	1.15 TB	\$5.75
Data stored in Apache Parquet format*	130 GB	6.78 seconds	2.51 GB	\$0.01
Savings / Speedup	87% less with Parquet	34x faster	99% less data scanned	99.7% savings

Apache Parquet is an open-source columnar storage format that is 2x faster to unload and takes up 6x less storage in Amazon S3 as compared to other text formats. One can COPY Apache Parquet and Apache ORC file formats from Amazon S3 to your Amazon Redshift cluster. Using AWS Glue, one can configure and run a job to transform CSV data to Parquet. Parquet is a columnar format that is well suited for AWS analytics services like Amazon Athena and Amazon Redshift Spectrum.

When an integrated AWS service requests access to data in an Amazon S3 location that is accesscontrolled by AWS Lake Formation, Lake Formation supplies temporary credentials to access the data.

To enable Lake Formation to control access to underlying data at an Amazon S3 location, you register that location with Lake Formation.

To enable Lake Formation principals to read and write underlying data with access controlled by Lake Formation permissions:

- The Amazon S3 locations that contain the data must be registered with Lake Formation.
- Principals who create Data Catalog tables that point to underlying data locations must have data location permissions.
- Principals who read and write underlying data must have Lake Formation data access permissions on the Data Catalog tables that point to the underlying data locations.
- Principals who read and write underlying data must have the `lakeformation:GetDataAccess` IAM permission.

Thus, the correct answer is: Transform the JSON data into Apache Parquet format. Ensure that the user has an `lakeformation:GetDataAccess` IAM permission for underlying data access control.

The option that says: Convert the JSON documents into CSV format. Provide fine-grained named resource access control to specific databases or tables in AWS Lake Formation is incorrect because Athena queries performed against row-based formats like CSV are slower than columnar file formats like

## Apache Parquet.

The option that says: Apply minification on the data and implement the Lake Formation tag-based access control (LF-TBAC) authorization strategy using IAM Tags to ensure security is incorrect. Although minifying the JSON file might reduce its overall file size, there won't be a significant difference in terms of querying performance. LF-TBAC is a type of an attribute-based access control (ABAC) that defines permissions based on certain attributes, such as tags in AWS. LF-TBAC uses LF-Tags to grant Lake Formation permissions and not regular IAM Tags.

The option that says: Compress the data into GZIP format before storing in the S3 bucket. Apply an IAM policy with aws:SourceArn and aws:SourceAccount global condition context keys in Lake Formation that prevents cross-service confused deputy problems and other security issues. is incorrect. Compressing the files prior to storing them in Amazon S3 will only save storage costs. As for query performance, it won't have much improvement. In addition, using an IAM Policy to prevent cross-service confused deputy issues is not warranted in this scenario. Having an lakeformation:GetDataAccess IAM permission for underlying data access control should suffice.

## References:

<https://aws.amazon.com/blogs/big-data/top-10-performance-tuning-tips-for-amazon-athena/>

<https://docs.aws.amazon.com/lake-formation/latest/dg/access-control-underlying-data.html>

<https://docs.aws.amazon.com/lake-formation/latest/dg/TBAC-overview.html>

Check out this Amazon Athena Cheat Sheet:

<https://tutorialsdojo.com/amazon-athena/>

---

## QUESTION 312

A Solutions Architect needs to launch a web application that will be served globally using Amazon CloudFront. The application is hosted in an Amazon EC2 instance which will be configured as the origin server to process and serve dynamic content to its customers.

Which of the following options provides high availability for the application?

- A. Use Lambda@Edge to improve the performance of your web application and ensure high availability. Set the Lambda@Edge functions to be part of an origin group.
- B. Provision two EC2 instances deployed in different Availability Zones and configure them to be part of an origin group.
- C. Launch an Auto Scaling group of EC2 instances and configure it to be part of an origin group.
- D. Use Amazon S3 to serve the dynamic content of your web application and configure the S3 bucket to be part of an origin group.

Answer: B

## Explanation:

An origin is a location where content is stored, and from which CloudFront gets content to serve to viewers. Amazon CloudFront is a service that speeds up the distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

Figure 1 : Origin failover on cache miss.



You can also set up CloudFront with origin failover for scenarios that require high availability. An origin group may contain two origins: a primary and a secondary. If the primary origin is unavailable or returns specific HTTP response status codes that indicate a failure, CloudFront automatically switches to the secondary origin. To set up origin failover, you must have a distribution with at least two origins.

The scenario uses an EC2 instance as an origin. Take note that we can also use an EC2 instance or a custom origin in configuring CloudFront. To achieve high availability in an EC2 instance, we need to deploy the instances in two or more Availability Zones. You also need to configure the instances to be part of the origin group to ensure that the application is highly available.

Hence, the correct answer is: Provision two EC2 instances deployed in different Availability Zones and configure them to be part of an origin group.

The option that says: Use Amazon S3 to serve the dynamic content of your web application and configure the S3 bucket to be part of an origin group is incorrect because Amazon S3 can only serve static content. If you need to host dynamic content, you have to use an Amazon EC2 instance instead.

The option that says: Launch an Auto Scaling group of EC2 instances and configure it to be part of an origin group is incorrect because you must have at least two origins to set up an origin failover in CloudFront. In addition, you can't directly use a single Auto Scaling group as an origin.

The option that says: Use Lambda@Edge to improve the performance of your web application and ensure high availability. Set the Lambda@Edge functions to be part of an origin group is incorrect because Lambda@Edge is primarily used for serverless edge computing. You can't set Lambda@Edge functions as part of your origin group in CloudFront.

#### References:

[https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high\\_availability\\_origin\\_failover.html](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.html)

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/introduction.html>

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

Check out this Amazon CloudFront Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudfront/>

### QUESTION 313

A mobile application stores pictures in Amazon Simple Storage Service (S3) and allows application sign in using an OpenID Connect-compatible identity provider.

Which AWS Security Token Service approach to temporary access should you use for this scenario?

- A. AWS Identity and Access Management roles
- B. SAML-based Identity Federation
- C. Cross-Account Access
- D. Web Identity Federation

Answer: D

Explanation:

With web identity federation, you don't need to create custom sign-in code or manage your own user identities. Instead, users of your app can sign in using a well-known identity provider (IdP) such as Login with Amazon, Facebook, Google, or any other OpenID Connect (OIDC)-compatible IdP, receive an authentication token, and then exchange that token for temporary security credentials in AWS that map to an IAM role with permissions to use the resources in your AWS account. Using an IdP helps you keep your AWS account secure because you don't have to embed and distribute long-term security credentials with your application.

Reference:

[http://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_providers\\_oidc.html](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html)

Check out this AWS IAM Cheat Sheet:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

---

### QUESTION 314

A web application, which is hosted in your on-premises data center and uses a MySQL database, must be migrated to AWS Cloud. You need to ensure that the network traffic to and from your RDS database instance is encrypted using SSL. For improved security, you have to use the profile credentials specific to your EC2 instance to access your database, instead of a password.

Which of the following should you do to meet the above requirement?

- A. Launch a new RDS database instance with the Backtrack feature enabled.
- B. Set up an RDS database and enable the IAM DB Authentication.
- C. Launch the mysql client using the --ssl-ca parameter when connecting to the database.
- D. Configure your RDS database to enable encryption.

Answer: B

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.

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, setting up an RDS database and enable the IAM DB Authentication is the correct answer based on the above reference.

Launching a new RDS database instance with the Backtrack feature enabled is incorrect because the Backtrack feature simply "rewinds" the DB cluster to the time you specify. Backtracking is not a replacement for backing up your DB cluster so that you can restore it to a point in time. However, you can easily undo mistakes using the backtrack feature if you mistakenly perform a destructive action, such as a DELETE without a WHERE clause.

Configuring your RDS database to enable encryption is incorrect because this encryption feature in RDS is mainly for securing your Amazon RDS DB instances and snapshots at rest. The data that is encrypted at rest includes the underlying storage for DB instances, its automated backups, Read Replicas, and snapshots.

Launching the mysql client using the --ssl-ca parameter when connecting to the database is incorrect because even though using the --ssl-ca parameter can provide SSL connection to your database, you still need to use IAM database connection to use the profile credentials specific to your EC2 instance to access your database instead of a password.

Reference:

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

Check out this Amazon RDS cheat sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

### QUESTION 315

A computer animation film studio has a web application running on an Amazon EC2 instance. It uploads 5 GB video objects to an Amazon S3 bucket. Video uploads are taking longer than expected, which impacts the performance of your application.

Which method will help improve the performance of the application?

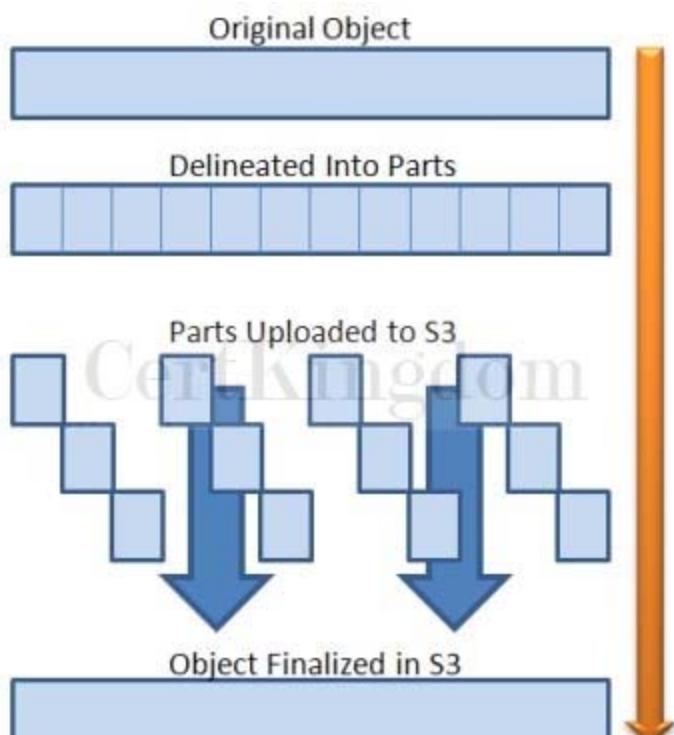
- A. Enable Enhanced Networking with the Elastic Network Adapter (ENA) on your EC2 Instances.
- B. Use Amazon S3 Multipart Upload API.
- C. Leverage on Amazon CloudFront and use HTTP POST method to reduce latency.
- D. Use Amazon Elastic Block Store Provisioned IOPS and an Amazon EBS-optimized instance.

Answer: B

Explanation:

The main issue is the slow upload time of the video objects to Amazon S3. To address this issue, you can use Multipart upload in S3 to improve the throughput. It allows you to upload parts of your object in parallel thus, decreasing the time it takes to upload big objects. Each part is a contiguous portion of the object's data.

You can upload these object parts independently and in any order. If transmission of any part fails, you can retransmit that part without affecting other parts. After all parts of your object are uploaded, Amazon S3 assembles these parts and creates the object. In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation.



Using multipart upload provides the following advantages:

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

Quick recovery from any network issues - Smaller part size minimizes the impact of restarting a failed upload due to a network error.

Pause and resume object uploads - You can upload object parts over time. Once you initiate a multipart upload, there is no expiry; you must explicitly complete or abort the multipart upload.

Begin an upload before you know the final object size - You can upload an object as you are creating it. Enabling Enhanced Networking with the Elastic Network Adapter (ENA) on your EC2 Instances is incorrect. Even though this will improve network performance, the issue will still persist since the problem lies in the upload time of the object to Amazon S3. You should use the Multipart upload feature instead. Leveraging on Amazon CloudFront and using HTTP POST method to reduce latency is incorrect because CloudFront is a CDN service and is not used to expedite the upload process of objects to Amazon S3. Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

Using Amazon Elastic Block Store Provisioned IOPS and an Amazon EBS-optimized instance is incorrect. Although the use of Amazon Elastic Block Store Provisioned IOPS will speed up the I/O performance of the EC2 instance, the root cause is still not resolved since the primary problem here is the slow video upload to Amazon S3. There is no network contention in the EC2 instance.

References:

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

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

---

## QUESTION 316

A software development company has hundreds of Amazon EC2 instances with multiple Application Load Balancers (ALBs) across multiple AWS Regions. The public applications hosted in their EC2 instances are accessed on their on-premises network. The company needs to reduce the number of IP addresses that it needs to regularly whitelist on the corporate firewall device.

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

- A. Use AWS Global Accelerator and create an endpoint group for each AWS Region. Associate the Application Load Balancer from each region to the corresponding endpoint group.
- B. Create a new Lambda function that tracks the changes in the IP addresses of all ALBs across multiple AWS Regions. Schedule the function to run and update the corporate firewall every hour using Amazon CloudWatch Events.
- C. Use AWS Global Accelerator and create multiple endpoints for all the available AWS Regions. Associate all the private IP addresses of the EC2 instances to the corresponding endpoints.
- D. Launch a Network Load Balancer with an associated Elastic IP address. Set the ALBs in multiple Regions as targets.

Answer: A

Explanation:

AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers, or Amazon EC2 instances.

When the application usage grows, the number of IP addresses and endpoints that you need to manage also increase. AWS Global Accelerator allows you to scale your network up or down. AWS Global Accelerator lets you associate regional resources, such as load balancers and EC2 instances, to two static IP addresses. You only whitelist these addresses once in your client applications, firewalls, and DNS records.

The screenshot shows the AWS Global Accelerator 'Create accelerator' wizard at Step 3: Add endpoint groups. The main title is 'Add endpoint groups'. A note states: 'An accelerator includes one or more listeners that direct traffic to one or more endpoint groups. An endpoint group includes endpoints, such as load balancers.' Below this, under 'Listener: 80 TCP', it says: 'Each listener can have multiple endpoint groups. Each endpoint group can only include endpoints that are in one Region. You aren't required to add an endpoint group, but until you do, traffic to this listener won't reach any endpoints.' There are two 'Region Info' dropdowns: 'us-east-1' and 'us-east-2'. Next to each is a 'Traffic dial Info' input field set to '100'. To the right of each input is a 'Remove' button. Below the first row is a note: 'A number from 0 to 100.' Underneath the rows are 'Configure health checks' buttons and an 'Add endpoint group' button.

With AWS Global Accelerator, you can add or remove endpoints in the AWS Regions, run blue/green deployment, and A/B test without needing to update the IP addresses in your client applications. This is particularly useful for IoT, retail, media, automotive, and healthcare use cases in which client applications cannot be updated frequently.

If you have multiple resources in multiple regions, you can use AWS Global Accelerator to reduce the number of IP addresses. By creating an endpoint group, you can add all of your EC2 instances from a single region in that group. You can add additional endpoint groups for instances in other regions. After it, you can then associate the appropriate ALB endpoints to each of your endpoint groups. The created accelerator would have two static IP addresses that you can use to create a security rule in your firewall device. Instead of regularly adding the Amazon EC2 IP addresses in your firewall, you can use the static IP addresses of AWS Global Accelerator to automate the process and eliminate this repetitive task.

Hence, the correct answer is: Use AWS Global Accelerator and create an endpoint group for each AWS Region. Associate the Application Load Balancer from each region to the corresponding endpoint group. The option that says: Use AWS Global Accelerator and create multiple endpoints for all the available AWS Regions. Associate all the private IP addresses of the EC2 instances to the corresponding endpoints is incorrect. It is better to create one endpoint group instead of multiple endpoints. Moreover, you have to associate the ALBs in AWS Global Accelerator and not the underlying EC2 instances.

The option that says: Create a new Lambda function that tracks the changes in the IP addresses of all ALBs across multiple AWS Regions. Schedule the function to run and update the corporate firewall every hour using Amazon CloudWatch Events is incorrect because this approach entails a lot of administrative overhead and takes a significant amount of time to implement. Using a custom Lambda function is actually not necessary since you can simply use AWS Global Accelerator to achieve this requirement.

The option that says: Launch a Network Load Balancer with an associated Elastic IP address. Set the ALBs in multiple Regions as targets is incorrect. Although you can allocate an Elastic IP address to your ELB, it is not suitable to route traffic to your ALBs across multiple Regions. You have to use AWS Global Accelerator instead.

#### References:

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups.html>

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

<https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works.html>

Check out this AWS Global Accelerator Cheat Sheet:

<https://tutorialsdojo.com/aws-global-accelerator/>

## QUESTION 317

A game company has a requirement of load balancing the incoming TCP traffic at the transport level (Layer 4) to their containerized gaming servers hosted in AWS Fargate. To maintain performance, it

should handle millions of requests per second sent by gamers around the globe while maintaining ultralow latencies.

Which of the following must be implemented in the current architecture to satisfy the new requirement?

- A. Launch a new Application Load Balancer.
- B. Create a new record in Amazon Route 53 with Weighted Routing policy to load balance the incoming traffic.
- C. Launch a new microservice in AWS Fargate that acts as a load balancer since using an ALB or NLB with Fargate is not possible.
- D. Launch a new Network Load Balancer.

Answer: D

Explanation:

Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones. Elastic Load Balancing offers three types of load balancers that all feature the high availability, automatic scaling, and robust security necessary to make your applications fault-tolerant. They are: Application Load Balancer, Network Load Balancer, and Classic Load Balancer

Network Load Balancer is best suited for load balancing of TCP traffic where extreme performance is required. Operating at the connection level (Layer 4), Network Load Balancer routes traffic to targets within Amazon Virtual Private Cloud (Amazon VPC) and is capable of handling millions of requests per second while maintaining ultra-low latencies. Network Load Balancer is also optimized to handle sudden and volatile traffic patterns.



Hence, the correct answer is to launch a new Network Load Balancer.

The option that says: Launch a new Application Load Balancer is incorrect because it cannot handle TCP or Layer 4 connections, only Layer 7 (HTTP and HTTPS).

The option that says: Create a new record in Amazon Route 53 with Weighted Routing policy to load balance the incoming traffic is incorrect because although Route 53 can act as a load balancer by assigning each record a relative weight that corresponds to how much traffic you want to send to each resource, it is still not capable of handling millions of requests per second while maintaining ultra-low latencies. You have to use a Network Load Balancer instead.

The option that says: Launch a new microservice in AWS Fargate that acts as a load balancer since using an ALB or NLB with Fargate is not possible is incorrect because you can place an ALB and NLB in front of your AWS Fargate cluster.

References:

<https://aws.amazon.com/elasticloadbalancing/features/#compare>

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/load-balancer-types.html>

<https://aws.amazon.com/getting-started/projects/build-modern-app-fargate-lambda-dynamodb-python/module-two/>

Check out this AWS Elastic Load Balancing (ELB) Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

## QUESTION 318

A company plans to launch an application that tracks the GPS coordinates of delivery trucks in the country. The coordinates are transmitted from each delivery truck every five seconds. You need to design an architecture that will enable real-time processing of these coordinates from multiple consumers. The aggregated data will be analyzed in a separate reporting application.

Which AWS service should you use for this scenario?

- A. AWS Data Pipeline
- B. Amazon Simple Queue Service
- C. Amazon AppStream
- D. Amazon Kinesis

Answer: D

Explanation:

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. It offers key capabilities to cost-effectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of your application.



With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications. Amazon Kinesis enables you to process and analyze data as it arrives and responds instantly instead of having to wait until all your data are collected before the processing can begin.

Reference:

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

Check out this Amazon Kinesis Cheat Sheet:

<https://tutorialsdojo.com/amazon-kinesis/>

## QUESTION 319

A company is looking for a way to analyze the calls between customers and service agents. Each conversation is transcribed, JSON-formatted, and saved to an Amazon S3 bucket. The company's solutions architect is tasked to design a solution for extracting and visualizing sentiments from the transcribed files.

Which solution meets the requirements while minimizing the amount of operational overhead?

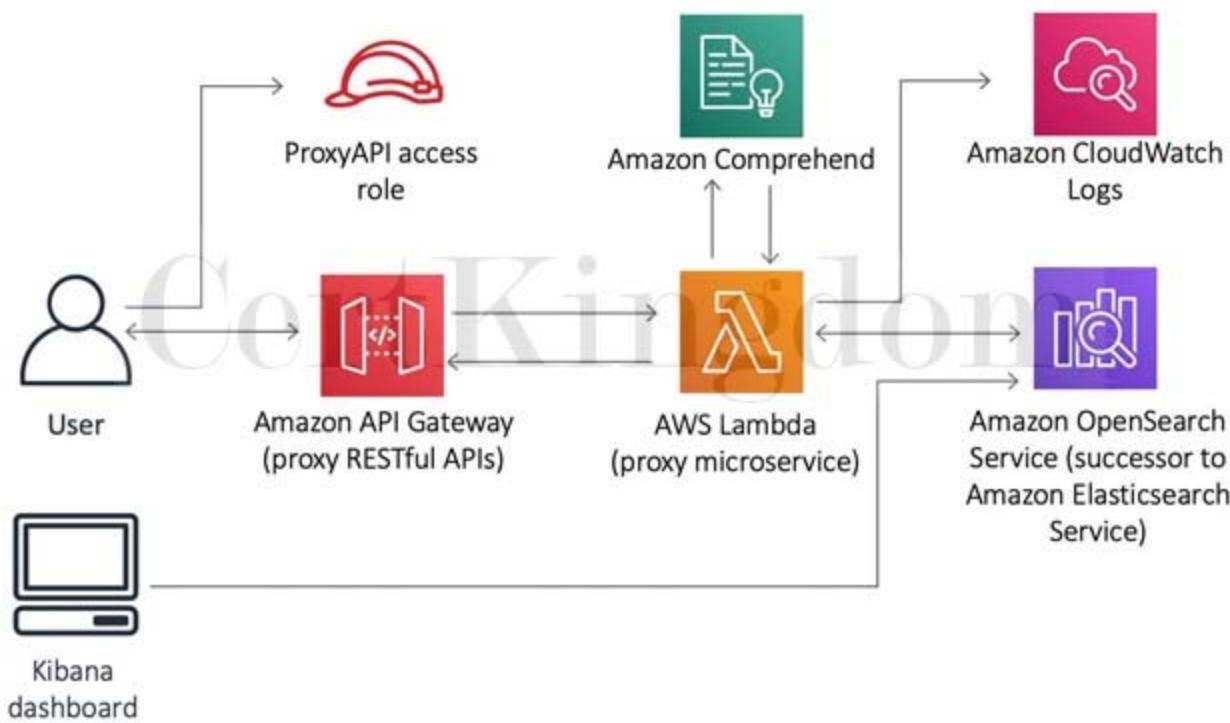
- A. Create an Amazon Comprehend analysis job. Index the sentiment along with the transcript to an Amazon OpenSearch cluster. Visualize the results using Amazon Managed Grafana.
- B. Create an Amazon Comprehend analysis job. Index the sentiment along with the transcript to an Amazon OpenSearch cluster. Visualize the results using the OpenSearch Dashboard.
- C. Train a custom Natural Language Processing (NLP) model using Amazon SageMaker. Index the sentiment along with the transcript to an Amazon OpenSearch cluster. Visualize the results using the OpenSearch Dashboard.

D. Analyze the JSON files with Amazon Textract. Index the sentiment along with the transcript to an Amazon OpenSearch cluster. Visualize the results using Amazon Managed Grafana.

Answer: B

Explanation:

Amazon Comprehend uses machine learning to help you uncover the insights and relationships in your unstructured data. The service identifies the language of the text; extracts key phrases, places, people, brands, or events; understands how positive or negative the text is; analyzes text using tokenization and parts of speech, and automatically organizes a collection of text files by topic. You can also use AutoML capabilities in Amazon Comprehend to build a custom set of entities or text classification models that are tailored uniquely to your organization's needs.



In this scenario, you can build the application with the help of Amazon Comprehend. You could expose the application through a RESTful endpoint, have it invoke a Lambda function that will call Amazon Comprehend for sentiment analysis, and index data into an Amazon OpenSearch cluster.

Hence, the correct answer is: Create an Amazon Comprehend analysis job. Index the sentiment along with the transcript to an Amazon OpenSearch cluster. Visualize the results using the OpenSearch Dashboard.

The option that says: Analyze the JSON files with Amazon Textract. Index the sentiment along with the transcript to an Amazon OpenSearch cluster. Visualize the results using Amazon Managed Grafana is incorrect. Amazon Textract is just an AI service used to extract text data from scanned documents in PNG, JPEG, TIFF, PDF formats and is not capable of running sentiment analysis. Furthermore, Grafana is more suited for the visualization of time-series data such as system metrics (CPU load, disk storage, memory utilization, temperature, etc). While there are hacks you can use to visualize non-time series like the one in the scenario, they come with additional overhead on your part. The built-in OpenSearch dashboard is enough to do the job.

The option that says: Create an Amazon Comprehend analysis job. Index the sentiment along with the transcript to an Amazon OpenSearch cluster. Visualize the results using Amazon Managed Grafana is incorrect. The Amazon OpenSearch dashboard is a more suitable service to use than Grafana since the sentiment data is already processed by an Amazon OpenSearch cluster. This solution needs a separate AWS data source configuration in the Grafana workspace console to integrate and read the sentiment data, which entails an additional operational overhead.

The option that says: Train a custom Natural Language Processing (NLP) model using Amazon SageMaker. Index the sentiment along with the transcript to an Amazon OpenSearch cluster. Visualize the results using the Amazon QuickSight Dashboard is incorrect. Although this may be a viable option, training your own ML model rather than using the readily available Amazon Comprehend service requires more time and effort. The same is true in using the Amazon QuickSight dashboard instead of the OpenSearch Dashboard. It takes a lot of steps to properly integrate Amazon QuickSight and an OpenSearch cluster which might cause delays in the project implementation.

References:

<https://aws.amazon.com/solutions/implementations/text-analysis-with-amazon-opensearch-service-and-a-mazon-comprehend/>

<https://docs.aws.amazon.com/opensearch-service/latest/developerguide/walkthrough.html#walkthroughanalysis>

Check out this Amazon Comprehend Cheat Sheet:

<https://tutorialsdojo.com/amazon-comprehend/>

---

## QUESTION 320

In a tech company that you are working for, there is a requirement to allow one IAM user to modify the configuration of one of your Elastic Load Balancers (ELB) which is used in a specific project. Each developer in your company has an individual IAM user and they usually move from one project to another.

Which of the following would be the best way to allow this access?

- A. Provide the user temporary access to the root account for 8 hours only. Afterwards, change the password once the activity is completed.
- B. Create a new IAM Role which will be assumed by the IAM user. Attach a policy allowing access to modify the ELB and once it is done, remove the IAM role from the user.
- C. Open up the port that ELB uses in a security group and then give the user access to that security group via a policy.
- D. Create a new IAM user that has access to modify the ELB. Delete that user when the work is completed.

Answer: B

Explanation:

In this scenario, the best option is to use IAM Role to provide access. You can create a new IAM Role then associate it to the IAM user. Attach a policy allowing access to modify the ELB and once it is done, remove the IAM role to the user.

An IAM role is similar to a user in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have standard longterm credentials (password or access keys) associated with it. Instead, if a user assumes a role, temporary security credentials are created dynamically and provided to the user.

You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. For example, you might want to grant users in your AWS account access to resources they don't usually have, or grant users in one AWS account access to resources in another account. Or you might want to allow a mobile app to use AWS resources, but not want to embed AWS keys within the app (where they can be difficult to rotate and where users can potentially extract them). Sometimes you want to give AWS access to users who already have identities defined outside of AWS, such as in your corporate directory. Or, you might want to grant access to your account to third parties so that they can perform an audit on your resources.

Reference:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_create\\_for-user.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user.html)

Check out this AWS IAM Cheat Sheet:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

## QUESTION 321

A Solutions Architect is working for a weather station in Asia with a weather monitoring system that needs to be migrated to AWS. Since the monitoring system requires a low network latency and high network throughput, the Architect decided to launch the EC2 instances to a new cluster placement group. The system was working fine for a couple of weeks, however, when they try to add new instances to the placement group that already has running EC2 instances, they receive an 'insufficient capacity error'.

How will the Architect fix this issue?

- A. Create another Placement Group and launch the new instances in the new group.
- B. Verify all running instances are of the same size and type and then try the launch again.
- C. Stop and restart the instances in the Placement Group and then try the launch again.
- D. Submit a capacity increase request to AWS as you are initially limited to only 12 instances per Placement Group.

Answer: C

Explanation:

A cluster placement group is a logical grouping of instances within a single Availability Zone. A cluster placement group can span peered VPCs in the same Region. Instances in the same cluster placement group enjoy a higher per-flow throughput limit for TCP/IP traffic and are placed in the same highbisection bandwidth segment of the network.



It is recommended that you launch the number of instances that you need in the placement group in a single launch request and that you use the same instance type for all instances in the placement group. If you try to add more instances to the placement group later, or if you try to launch more than one instance type in the placement group, you increase your chances of getting an insufficient capacity error. If you stop an instance in a placement group and then start it again, it still runs in the placement group. However, the start fails if there isn't enough capacity for the instance.

If you receive a capacity error when launching an instance in a placement group that already has running instances, stop and start all of the instances in the placement group, and try the launch again. Restarting the instances may migrate them to hardware that has capacity for all the requested instances.

Stop and restart the instances in the Placement group and then try the launch again can resolve this issue. If the instances are stopped and restarted, AWS may move the instances to a hardware that has the capacity for all the requested instances.

Hence, the correct answer is: Stop and restart the instances in the Placement Group and then try the launch again.

The option that says: Create another Placement Group and launch the new instances in the new group is incorrect because to benefit from the enhanced networking, all the instances should be in the same Placement Group. Launching the new ones in a new Placement Group will not work in this case.

The option that says: Verify all running instances are of the same size and type and then try the launch again is incorrect because the capacity error is not related to the instance size.

The option that says: Submit a capacity increase request to AWS as you are initially limited to only 12 instances per Placement Group is incorrect because there is no such limit on the number of instances in a Placement Group.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html#placement-groups-cluster>

[http://docs.amazonaws.cn/en\\_us/AWSEC2/latest/UserGuide/troubleshooting-launch.html#troubleshooting-launch-capacity](http://docs.amazonaws.cn/en_us/AWSEC2/latest/UserGuide/troubleshooting-launch.html#troubleshooting-launch-capacity)

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

## QUESTION 322

A Solutions Architect needs to create a publicly accessible EC2 instance by using an Elastic IP (EIP) address and generate a report on how much it will cost to use that EIP.

Which of the following statements is correct regarding the pricing of EIP?

- A. There is no cost if the instance is running and it has only one associated EIP.
- B. There is no cost if the instance is running and it has at least two associated EIP.
- C. There is no cost if the instance is terminated and it has only one associated EIP.
- D. There is no cost if the instance is stopped and it has only one associated EIP.

Answer: A

Explanation:

An Elastic IP address doesn't incur charges as long as the following conditions are true:

- The Elastic IP address is associated with an Amazon EC2 instance.
- The instance associated with the Elastic IP address is running.
- The instance has only one Elastic IP address attached to it.

Elastic IP addresses (1/1)					
Actions		Allocate Elastic IP address			
<input checked="" type="checkbox"/>	Name	Allocated IPv4 add...	Type	Allocation ID	Associated instance ID
<input checked="" type="checkbox"/>	tdojo-EIP	58.25.150.101	Public IP	eipalloc-0343302404655a6d3	i-09cb6b7d738780915

If you've stopped or terminated an EC2 instance with an associated Elastic IP address and you don't need that Elastic IP address anymore, consider disassociating or releasing the Elastic IP address.

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/elastic-ip-charges/>

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

## QUESTION 323

An intelligence agency is currently hosting a learning and training portal in AWS. Your manager instructed you to launch a large EC2 instance with an attached EBS Volume and enable Enhanced Networking. What are the valid case scenarios in using Enhanced Networking? (Select TWO.)

- A. When you need a dedicated connection to your on-premises data center
- B. When you need high latency networking
- C. When you need a low packet-per-second performance
- D. When you need a higher packet per second (PPS) performance
- E. When you need a consistently lower inter-instance latencies

Answer: D,E

Explanation:

Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types. SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies. There is no additional charge for using enhanced networking.

```
% aws ec2 describe-instances  
--instance-id i-07a94b1806d6cd309 \  
--query "Reservations[].Instances[].EnaSupport"
```



The option that says: When you need a low packet-per-second performance is incorrect because you want to increase packet-per-second performance, and not lower it when you enable enhanced networking.

The option that says: When you need high latency networking is incorrect because higher latencies mean slower network, which is the opposite of what you want to happen when you enable enhanced networking.

The option that says: When you need a dedicated connection to your on-premises data center is incorrect because enabling enhanced networking does not provide a dedicated connection to your on-premises data center. Use AWS Direct Connect or enable VPN tunneling instead for this purpose.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html>

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

## QUESTION 324

A company plans to use a cloud storage service to temporarily store its log files. The number of files to be stored is still unknown, but it only needs to be kept for 12 hours.

Which of the following is the most cost-effective storage class to use in this scenario?

- A. Amazon S3 Standard-IA

- B. Amazon S3 Standard
- C. Amazon S3 Glacier Deep Archive
- D. Amazon S3 One Zone-IA

Answer: B

Explanation:

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Amazon S3 also offers a range of storage classes for the objects that you store. You choose a class depending on your use case scenario and performance access requirements. All of these storage classes offer high durability.

Storage class	Designed for	Availability Zones	Min storage duration
<input checked="" type="radio"/> Standard	Frequently accessed data (more than once a month) with milliseconds access	≥ 3	-
<input type="radio"/> Intelligent-Tiering	Data with changing or unknown access patterns	≥ 3	-
<input type="radio"/> Standard-IA	Infrequently accessed data (once a month) with milliseconds access	≥ 3	30 days
<input type="radio"/> One Zone-IA	Recreatable, infrequently accessed data (once a month) stored in a single Availability Zone with milliseconds access	1	30 days
<input type="radio"/> Glacier Instant Retrieval	Long-lived archive data accessed once a quarter with instant retrieval in milliseconds	≥ 3	90 days
<input type="radio"/> Glacier Flexible Retrieval (formerly Glacier)	Long-lived archive data accessed once a year with retrieval of minutes to hours	≥ 3	90 days
<input type="radio"/> Glacier Deep Archive	Long-lived archive data accessed less than once a year with retrieval of hours	≥ 3	180 days
<input type="radio"/> Reduced redundancy	Noncritical, frequently accessed data with milliseconds access (not recommended as S3 Standard is more cost effective)	≥ 3	-

The scenario requires you to select a cost-effective service that does not have a minimum storage duration since the data will only last for 12 hours. Among the options given, only Amazon S3 Standard has the feature of no minimum storage duration. It is also the most cost-effective storage service because you will only be charged for the last 12 hours, unlike in other storage classes where you will still be charged based on its respective storage duration (e.g. 30 days, 90 days, 180 days). S3 Intelligent-Tiering also has no minimum storage duration and this is designed for data with changing or unknown access patterns.

S3 Standard-IA is designed for long-lived but infrequently accessed data that is retained for months or years. Data that is deleted from S3 Standard-IA within 30 days will still be charged for a full 30 days. S3 Glacier Deep Archive is designed for long-lived but rarely accessed data that is retained for 7-10 years or more. Objects that are archived to S3 Glacier Deep Archive have a minimum of 180 days of storage, and objects deleted before 180 days incur a pro-rated charge equal to the storage charge for the remaining days.

Hence, the correct answer is: Amazon S3 Standard.

Amazon S3 Standard-IA is incorrect because this storage class has a minimum storage duration of at least 30 days. Remember that the scenario requires the data to be kept for 12 hours only.

Amazon S3 One Zone-IA is incorrect. Just like S3 Standard-IA, this storage class has a minimum storage duration of at least 30 days.

Amazon S3 Glacier Deep Archive is incorrect. Although it is the most cost-effective storage class among all other options, it has a minimum storage duration of at least 180 days which is only suitable for backup and data archival. If you store your data in Glacier Deep Archive for only 12 hours, you will still be charged for the full 180 days.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html>

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

S3 Standard vs S3 Standard-IA vs S3 One Zone-IA Cheat Sheet:

<https://tutorialsdojo.com/s3-standard-vs-s3-standard-ia-vs-s3-one-zone-ia/>

---

## QUESTION 325

An online stock trading system is hosted in AWS and uses an Auto Scaling group of EC2 instances, an RDS database, and an Amazon ElastiCache for Redis. You need to improve the data security of your inmemory data store by requiring the user to enter a password before they are granted permission to execute Redis commands.

Which of the following should you do to meet the above requirement?

- A. Authenticate the users using Redis AUTH by creating a new Redis Cluster with both the --transitencryption-enabled and --auth-token parameters enabled.
- B. Enable the in-transit encryption for Redis replication groups.
- C. None of the above.
- D. Create a new Redis replication group and set the AtRestEncryptionEnabled parameter to true.
- E. Do nothing. This feature is already enabled by default.

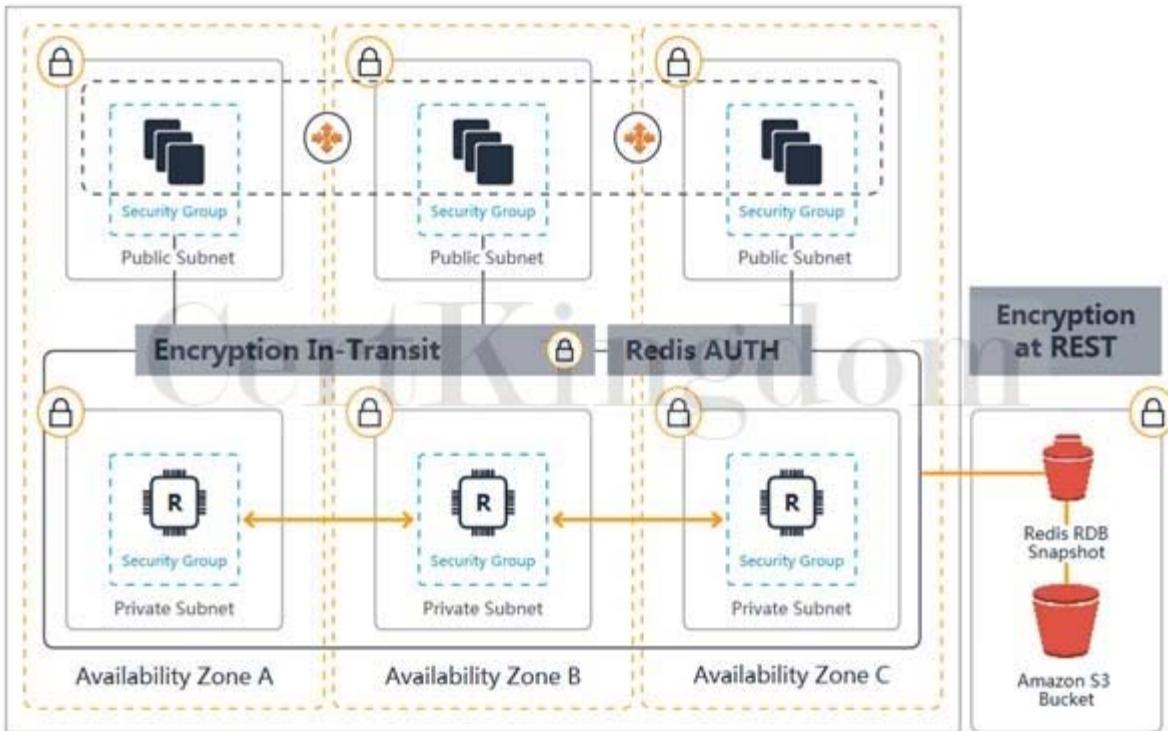
Answer: A

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 to 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.



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. Creating a new Redis replication group and setting the AtRestEncryptionEnabled parameter to true 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.

The option that says: Do nothing. This feature is already enabled by default is incorrect because the Redis AUTH option is disabled by default.

References:

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

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

Check out this Amazon ElastiCache Cheat Sheet:

<https://tutorialsdojo.com/amazon-elasticache/>

Redis Append-Only Files vs Redis Replication:

<https://tutorialsdojo.com/redis-append-only-files-vs-redis-replication/>

Comparison of AWS Services Cheat Sheets:

<https://tutorialsdojo.com/comparison-of-aws-services/>

## QUESTION 326

A company created a VPC with a single subnet then launched an On-Demand EC2 instance in that subnet. You have attached an Internet gateway (IGW) to the VPC and verified that the EC2 instance has a public IP. The main route table of the VPC is as shown below:

	TutorialsDojo	rtb-46b1813b	0 Subnets	Yes	vpc-b0968fc8
		rtb-43b15626	0 Subnets	Yes	vpc-f2bf5897   Default VPC

rtb-46b1813b

Summary	Routes	Subnet Associations	Route Propagation	Tags
Edit	View: All rules			
Destination	Target	Status	Propagated	
10.0.0.0/27	local	Active	No	

However, the instance still cannot be reached from the Internet when you tried to connect to it from your computer. Which of the following should be made to the route table to fix this issue?

- A. Add this new entry to the route table: 0.0.0.0 -> Your Internet Gateway
- B. Add this new entry to the route table: 0.0.0.0/0 -> Your Internet Gateway
- C. Add the following entry to the route table: 10.0.0.0 -> Your Internet Gateway
- D. Modify the above route table: 10.0.0.0 -> Your Internet Gateway

Answer: B

Explanation:

Apparently, the route table does not have an entry for the Internet Gateway. This is why you cannot connect to the EC2 instance. To fix this, you have to add a route with a destination of 0.0.0.0/0 for IPv4 traffic or ::/0 for IPv6 traffic, and then a target of the Internet gateway ID (igw-xxxxxxxx).

	TutorialsDojo	rtb-46b1813b	0 Subnets	Yes	vpc-b0968fc8
		rtb-43b15626	0 Subnets	Yes	vpc-f2bf5897   Default VPC

rtb-46b1813b | TutorialsDojo

Summary	Routes	Subnet Associations	Route Propagation	Tags
Edit	View: All rules			
Destination	Target	Status	Propagated	
10.0.0.0/27	local	Active	No	
0.0.0.0/0	igw-b51618cc	Active	No	

Reference:

[http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Route\\_Tables.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html)

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

## QUESTION 327

A multinational corporate and investment bank is regularly processing steady workloads of accruals, loan interests, and other critical financial calculations every night from 10 PM to 3 AM on their on-premises data center for their corporate clients. Once the process is done, the results are then uploaded to the Oracle General Ledger which means that the processing should not be delayed or interrupted. The CTO has decided to move its IT infrastructure to AWS to save costs. The company needs to reserve compute capacity in a specific Availability Zone to properly run their workloads.

As the Senior Solutions Architect, how can you implement a cost-effective architecture in AWS for their financial system?

- A. Use Regional Reserved Instances to reserve capacity on a specific Availability Zone and lower down the operating cost through its billing discounts.
- B. Use Dedicated Hosts which provide a physical host that is fully dedicated to running your instances, and bring your existing per-socket, per-core, or per-VM software licenses to reduce costs.
- C. Use On-Demand Capacity Reservations, which provide compute capacity that is always available on the specified recurring schedule.
- D. Use On-Demand EC2 instances which allows you to pay for the instances that you launch and use by the second. Reserve compute capacity in a specific Availability Zone to avoid any interruption.

Answer: C

Explanation:

On-Demand Capacity Reservations enable you to reserve compute capacity for your Amazon EC2 instances in a specific Availability Zone for any duration. This gives you the ability to create and manage Capacity Reservations independently from the billing discounts offered by Savings Plans or Regional Reserved Instances.

By creating Capacity Reservations, you ensure that you always have access to EC2 capacity when you need it, for as long as you need it. You can create Capacity Reservations at any time, without entering into a one-year or three-year term commitment, and the capacity is available immediately. Billing starts as soon as the capacity is provisioned and the Capacity Reservation enters the active state. When you no longer need it, cancel the Capacity Reservation to stop incurring charges.

	Capacity Reservations	Zonal Reserved Instances	Regional Reserved Instances	Savings Plans
Term	No commitment required. Can be created and canceled as needed.	Requires a fixed one-year or three-year commitment		
Capacity benefit	Capacity reserved in a specific Availability Zone.		No capacity reserved.	
Billing discount	No billing discount. †	Provides a billing discount.		
Instance Limits	Your On-Demand instance limits per Region apply.	Default is 20 per Availability Zone. You can request a limit increase.	Default is 20 per Region. You can request a limit increase.	No limit.

When you create a Capacity Reservation, you specify:

- The Availability Zone in which to reserve the capacity
- The number of instances for which to reserve capacity
- The instance attributes, including the instance type, tenancy, and platform/OS

Capacity Reservations can only be used by instances that match their attributes. By default, they are automatically used by running instances that match the attributes. If you don't have any running instances that match the attributes of the Capacity Reservation, it remains unused until you launch an instance with matching attributes.

In addition, you can use Savings Plans and Regional Reserved Instances with your Capacity Reservations to benefit from billing discounts. AWS automatically applies your discount when the attributes of a Capacity Reservation match the attributes of a Savings Plan or Regional Reserved Instance.

Hence, the correct answer is to use On-Demand Capacity Reservations, which provide compute

capacity that is always available on the specified recurring schedule. Using On-Demand EC2 instances which allows you to pay for the instances that you launch and use by the second. Reserve compute capacity in a specific Availability Zone to avoid any interruption is incorrect because although an On-Demand instance is stable and suitable for processing critical data, it costs more than any other option. Moreover, the critical financial calculations are only done every night from 10 PM to 3 AM only and not 24. This means that your compute capacity will not be utilized for a total of 19 hours every single day. On-Demand instances cannot reserve compute capacity at all. So this option is incorrect.

Using Regional Reserved Instances to reserve capacity on a specific Availability Zone and lower down the operating cost through its billing discounts is incorrect because this feature is available in Zonal Reserved Instances only and not on Regional Reserved Instances.

Using Dedicated Hosts which provide a physical host that is fully dedicated to running your instances, and bringing your existing per-socket, per-core, or per-VM software licenses to reduce costs is incorrect because the use of a fully dedicated physical host is not warranted in this scenario. Moreover, this will be underutilized since you only run the process for 5 hours (from 10 PM to 3 AM only), wasting 19 hours of compute capacity every single day.

References:

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

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

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

---

## QUESTION 328

A company deployed a web application to an EC2 instance that adds a variety of photo effects to a picture uploaded by the users. The application will put the generated photos to an S3 bucket by sending PUT requests to the S3 API.

What is the best option for this scenario considering that you need to have API credentials to be able to send a request to the S3 API?

- A. Encrypt the API credentials and store in any directory of the EC2 instance.
- B. Store your API credentials in Amazon Glacier.
- C. Create a role in IAM. Afterwards, assign this role to a new EC2 instance.
- D. Store the API credentials in the root web application directory of the EC2 instance.

Answer: C

Explanation:

The best option is to create a role in IAM. Afterward, assign this role to a new EC2 instance. Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances.

**1**

## IAM Role

**2**

## Permissions

**Trust**  
 Who can assume this role



What you can do after assuming a role

Defined by the role trust policy

Defined by IAM permissions policies

You can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance, especially those that AWS creates on your behalf such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.

In this scenario, you have to use IAM roles so that your applications can securely make API requests from your instances without requiring you to manage the security credentials that the applications use. Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles.

Hence, the correct answer is: Create a role in IAM. Afterwards, assign this role to a new EC2 instance. The option that says: Encrypt the API credentials and storing in any directory of the EC2 instance and Store the API credentials in the root web application directory of the EC2 instance are incorrect. Though you can store and use the API credentials in the EC2 instance, it will be difficult to manage just as mentioned above. You have to use IAM Roles.

The option that says: Store your API credentials in Amazon S3 Glacier is incorrect as Amazon S3 Glacier is used for data archives and not for managing API credentials.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

### QUESTION 329

A Solutions Architect is managing a three-tier web application that processes credit card payments and online transactions. Static web pages are used on the front-end tier while the application tier contains a single Amazon EC2 instance that handles long-running processes. The data is stored in a MySQL database. The Solutions Architect is instructed to decouple the tiers to create a highly available application.

Which of the following options can satisfy the given requirement?

- A. Move all the static assets and web pages to Amazon S3. Re-host the application to Amazon Elastic Container Service (Amazon ECS) containers and enable Service Auto Scaling. Migrate the database to Amazon RDS with Multi-AZ deployments configuration.
- B. Move all the static assets, web pages, and the backend application to a larger instance. Use Auto Scaling in Amazon EC2 instance. Migrate the database to Amazon Aurora.
- C. Move all the static assets and web pages to Amazon CloudFront. Use Auto Scaling in Amazon EC2 instance. Migrate the database to Amazon RDS with Multi-AZ deployments configuration.
- D. Move all the static assets to Amazon S3. Set concurrency limit in AWS Lambda to move the application to a serverless architecture. Migrate the database to Amazon DynamoDB.

Answer: A

## Explanation:

Amazon Elastic Container Service (ECS) is a highly scalable, high performance container management service that supports Docker containers and allows you to easily run applications on a managed cluster of Amazon EC2 instances. Amazon ECS makes it easy to use containers as a building block for your applications by eliminating the need for you to install, operate, and scale your own cluster management infrastructure. Amazon ECS lets you schedule long-running applications, services, and batch processes using Docker containers. Amazon ECS maintains application availability and allows you to scale your containers up or down to meet your application's capacity requirements.



The requirement in the scenario is to decouple the services to achieve a highly available architecture. To accomplish this requirement, you must move the existing set up to each AWS services. For static assets, you should use Amazon S3. You can use Amazon ECS for your web application and then migrate the database to Amazon RDS with Multi-AZ deployment. Decoupling your app with application integration services allows them to remain interoperable, but if one service has a failure or spike in workload, it won't affect the rest of them.

Hence, the correct answer is: Move all the static assets and web pages to Amazon S3. Re-host the application to Amazon Elastic Container Service (Amazon ECS) containers and enable Service Auto Scaling. Migrate the database to Amazon RDS with Multi-AZ deployments configuration.

The option that says: Move all the static assets to Amazon S3. Set concurrency limit in AWS Lambda to move the application to a serverless architecture. Migrate the database to Amazon DynamoDB is incorrect because Lambda functions can't process long-running processes. Take note that a Lambda function has a maximum processing time of 15 minutes.

The option that says: Move all the static assets, web pages, and the backend application to a larger instance. Use Auto Scaling in Amazon EC2 instance. Migrate the database to Amazon Aurora is incorrect because static assets are more suitable and cost-effective to be stored in S3 instead of storing them in an EC2 instance.

The option that says: Move all the static assets and web pages to Amazon CloudFront. Use Auto Scaling in Amazon EC2 instance. Migrate the database to Amazon RDS with Multi-AZ deployments configuration is incorrect because you can't store data in Amazon CloudFront. Technically, you only store cache data in CloudFront, but you can't host applications or web pages using this service. You have to use Amazon S3 to host the static web pages and use CloudFront as the CDN.

## References:

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-auto-scaling.html>

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

Check out this Amazon ECS Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-container-service-amazon-ecs/>

## QUESTION 330

A company has an application architecture that stores both the access key ID and the secret access key in a plain text file on a custom Amazon Machine Image (AMI). The EC2 instances, which are created by using this AMI, are using the stored access keys to connect to a DynamoDB table.

What should the Solutions Architect do to make the current architecture more secure?

- A. Do nothing. The architecture is already secure because the access keys are already in the Amazon Machine Image.
- B. Put the access keys in Amazon Glacier instead.
- C. Put the access keys in an Amazon S3 bucket instead.
- D. Remove the stored access keys in the AMI. Create a new IAM role with permissions to access the DynamoDB table and assign it to the EC2 instances.

Answer: D

Explanation:

You should use an IAM role to manage temporary credentials for applications that run on an EC2 instance. When you use an IAM role, you don't have to distribute long-term credentials (such as a user name and password or access keys) to an EC2 instance.

Instead, the role supplies temporary permissions that applications can use when they make calls to other AWS resources. When you launch an EC2 instance, you specify an IAM role to associate with the instance. Applications that run on the instance can then use the role-supplied temporary credentials to sign API requests.

Hence, the best option here is to remove the stored access keys first in the AMI. Then, create a new IAM role with permissions to access the DynamoDB table and assign it to the EC2 instances.

Putting the access keys in Amazon Glacier or in an Amazon S3 bucket are incorrect because S3 and Glacier are mainly used as a storage option. It is better to use an IAM role instead of storing access keys in these storage services.

The option that says: Do nothing. The architecture is already secure because the access keys are already in the Amazon Machine Image is incorrect because you can make the architecture more secure by using IAM.

Reference:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_use\\_switch-role-ec2.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html)

Check out this AWS Identity & Access Management (IAM) Cheat Sheet:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

---

## QUESTION 331

A multinational company has been building its new data analytics platform with high-performance computing workloads (HPC) which requires a scalable, POSIX-compliant storage service. The data need to be stored redundantly across multiple AZs and allows concurrent connections from thousands of EC2 instances hosted on multiple Availability Zones.

Which of the following AWS storage service is the most suitable one to use in this scenario?

- A. Amazon ElastiCache
- B. Amazon S3
- C. Amazon Elastic File System
- D. Amazon EBS Volumes

Answer: C

Explanation:

In this question, you should take note of this phrase, "allows concurrent connections from multiple EC2 instances". There are various AWS storage options that you can choose but whenever these criteria show up, always consider using EFS instead of using EBS Volumes which is mainly used as a "block" storage and can only have one connection to one EC2 instance at a time.

Amazon EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud. With a few clicks in the AWS Management Console, you can create file systems that are accessible to Amazon EC2 instances via a file system interface (using standard operating system file I/O APIs) and supports full file system access semantics (such as strong consistency and file locking).

Amazon EFS file systems can automatically scale from gigabytes to petabytes of data without needing to provision storage. Tens, hundreds, or even thousands of Amazon EC2 instances can access an Amazon

EFS file system at the same time, and Amazon EFS provides consistent performance to each Amazon EC2 instance. Amazon EFS is designed to be highly durable and highly available.

References:

<https://docs.aws.amazon.com/efs/latest/ug/performance.html>

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

Check out this Amazon EFS Cheat Sheet:

<https://tutorialsdojo.com/amazon-efs/>

Here's a short video tutorial on Amazon EFS:

<https://youtu.be/AvgAozsfCrY>

## QUESTION 332

A software development company needs to connect its on-premises infrastructure to the AWS cloud.

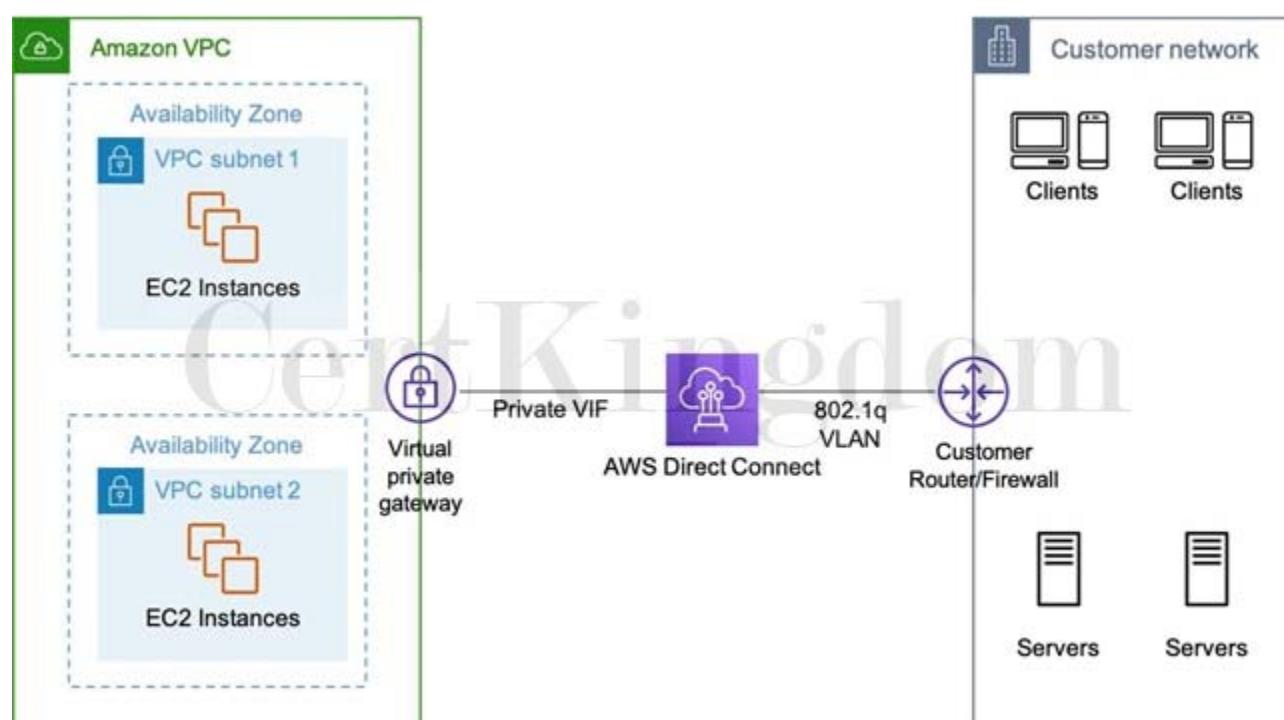
Which of the following AWS services can you use to accomplish this? (Select TWO.)

- A. NAT Gateway
- B. Amazon Connect
- C. VPC Peering
- D. AWS Direct Connect
- E. IPsec VPN connection

Answer: D,E

Explanation:

You can connect your VPC to remote networks by using a VPN connection which can be IPsec VPN connection, AWS VPN CloudHub, or a third party software VPN appliance. A VPC VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet.



AWS Direct Connect is a network service that provides an alternative to using the Internet to connect customer's on-premises sites to AWS. AWS Direct Connect does not involve the Internet; instead, it uses dedicated, private network connections between your intranet and Amazon VPC.

Hence, IPsec VPN connection and AWS Direct Connect are the correct answers.

Amazon Connect is incorrect because this is not a VPN connectivity option. It is actually a self-service, cloud-based contact center service in AWS that makes it easy for any business to deliver better customer service at a lower cost. Amazon Connect is based on the same contact center technology used by Amazon customer service associates around the world to power millions of customer conversations.

VPC Peering is incorrect because this is a networking connection between two VPCs only, which enables you to route traffic between them privately. This can't be used to connect your on-premises network to your VPC.

NAT Gateway is incorrect because you only use a network address translation (NAT) gateway 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. This is not used to connect to your on-premises network.

References:

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html>

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

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

---

## QUESTION 333

An online shopping platform has been deployed to AWS using Elastic Beanstalk. They simply uploaded their Node.js application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring. Since the entire deployment process is automated, the DevOps team is not sure where to get the application log files of their shopping platform.

In Elastic Beanstalk, where does it store the application files and server log files?

- A. Application files are stored in S3. The server log files can be optionally stored in CloudTrail or in CloudWatch Logs.
- B. Application files are stored in S3. The server log files can only be stored in the attached EBS volumes of the EC2 instances, which were launched by AWS Elastic Beanstalk.
- C. Application files are stored in S3. The server log files can also optionally be stored in S3 or in CloudWatch Logs.
- D. Application files are stored in S3. The server log files can be stored directly in Glacier or in CloudWatch Logs.

Answer: C

Explanation:

AWS Elastic Beanstalk stores your application files and optionally, server log files in Amazon S3. If you are using the AWS Management Console, the AWS Toolkit for Visual Studio, or AWS Toolkit for Eclipse, an Amazon S3 bucket will be created in your account and the files you upload will be automatically copied from your local client to Amazon S3. Optionally, you may configure Elastic Beanstalk to copy your server log files every hour to Amazon S3. You do this by editing the environment configuration settings. Thus, the correct answer is the option that says: Application files are stored in S3. The server log files can also optionally be stored in S3 or in CloudWatch Logs.

With CloudWatch Logs, you can monitor and archive your Elastic Beanstalk application, system, and custom log files from Amazon EC2 instances of your environments. You can also configure alarms that make it easier for you to react to specific log stream events that your metric filters extract. The CloudWatch Logs agent installed on each Amazon EC2 instance in your environment publishes metric data points to the CloudWatch service for each log group you configure. Each log group applies its own filter patterns to determine what log stream events to send to CloudWatch as data points. Log streams that belong to the same log group share the same retention, monitoring, and access control settings. You can configure Elastic Beanstalk to automatically stream logs to the CloudWatch service.

The option that says: Application files are stored in S3. The server log files can only be stored in the attached EBS volumes of the EC2 instances, which were launched by AWS Elastic Beanstalk is incorrect because the server log files can also be stored in either S3 or CloudWatch Logs, and not only on the EBS volumes of the EC2 instances which are launched by AWS Elastic Beanstalk.

The option that says: Application files are stored in S3. The server log files can be stored directly in Glacier or in CloudWatch Logs is incorrect because the server log files can optionally be stored in either S3 or CloudWatch Logs, but not directly to Glacier. You can create a lifecycle policy to the S3 bucket to

store the server logs and archive it in Glacier, but there is no direct way of storing the server logs to Glacier using Elastic Beanstalk unless you do it programmatically.

The option that says: Application files are stored in S3. The server log files can be optionally stored in CloudTrail or in CloudWatch Logs is incorrect because the server log files can optionally be stored in either S3 or CloudWatch Logs, but not directly to CloudTrail as this service is primarily used for auditing API calls.

Reference:

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

AWS Elastic Beanstalk Overview:

<https://www.youtube.com/watch?v=rx7e7Fej1Oo>

Check out this AWS Elastic Beanstalk Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-beanstalk/>

---

### QUESTION 334

A global medical research company has a molecular imaging system that provides each client with frequently updated images of what is happening inside the human body at the molecular and cellular levels. The system is hosted in AWS and the images are hosted in an S3 bucket behind a CloudFront web distribution. When a fresh batch of images is uploaded to S3, it is required to keep the previous ones in order to prevent them from being overwritten.

Which of the following is the most suitable solution to solve this issue?

- A. Use versioned objects
- B. Invalidate the files in your CloudFront web distribution
- C. Add Cache-Control no-cache, no-store, or private directives in the S3 bucket
- D. Add a separate cache behavior path for the content and configure a custom object caching with a Minimum TTL of 0

Answer: A

Explanation:

To control the versions of files that are served from your distribution, you can either invalidate files or give them versioned file names. If you want to update your files frequently, AWS recommends that you primarily use file versioning for the following reasons:

- Versioning enables you to control which file a request returns even when the user has a version cached either locally or behind a corporate caching proxy. If you invalidate the file, the user might continue to see the old version until it expires from those caches.
- CloudFront access logs include the names of your files, so versioning makes it easier to analyze the results of file changes.
- Versioning provides a way to serve different versions of files to different users.
- Versioning simplifies rolling forward and back between file revisions.
- Versioning is less expensive. You still have to pay for CloudFront to transfer new versions of your files to edge locations, but you don't have to pay for invalidating files.

Invalidating the files in your CloudFront web distribution is incorrect because even though using invalidation will solve this issue, this solution is more expensive as compared to using versioned objects.

Adding a separate cache behavior path for the content and configuring a custom object caching with a Minimum TTL of 0 is incorrect because this alone is not enough to solve the problem. A cache behavior is primarily used to configure a variety of CloudFront functionality for a given URL path pattern for files on your website. Although this solution may work, it is still better to use versioned objects where you can control which image will be returned by the system even when the user has another version cached either locally or behind a corporate caching proxy.

Adding Cache-Control no-cache, no-store, or private directives in the S3 bucket is incorrect because although it is right to configure your origin to add the Cache-Control or Expires header field, you should do this to your objects and not on the entire S3 bucket.

References:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/UpdatingExistingObjects.html>

<https://aws.amazon.com/premiumsupport/knowledge-center/prevent-cloudfront-from-caching-files/>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Invalidation.html#PayingForInvalidation>

Check out this Amazon CloudFront Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudfront/>

## QUESTION 335

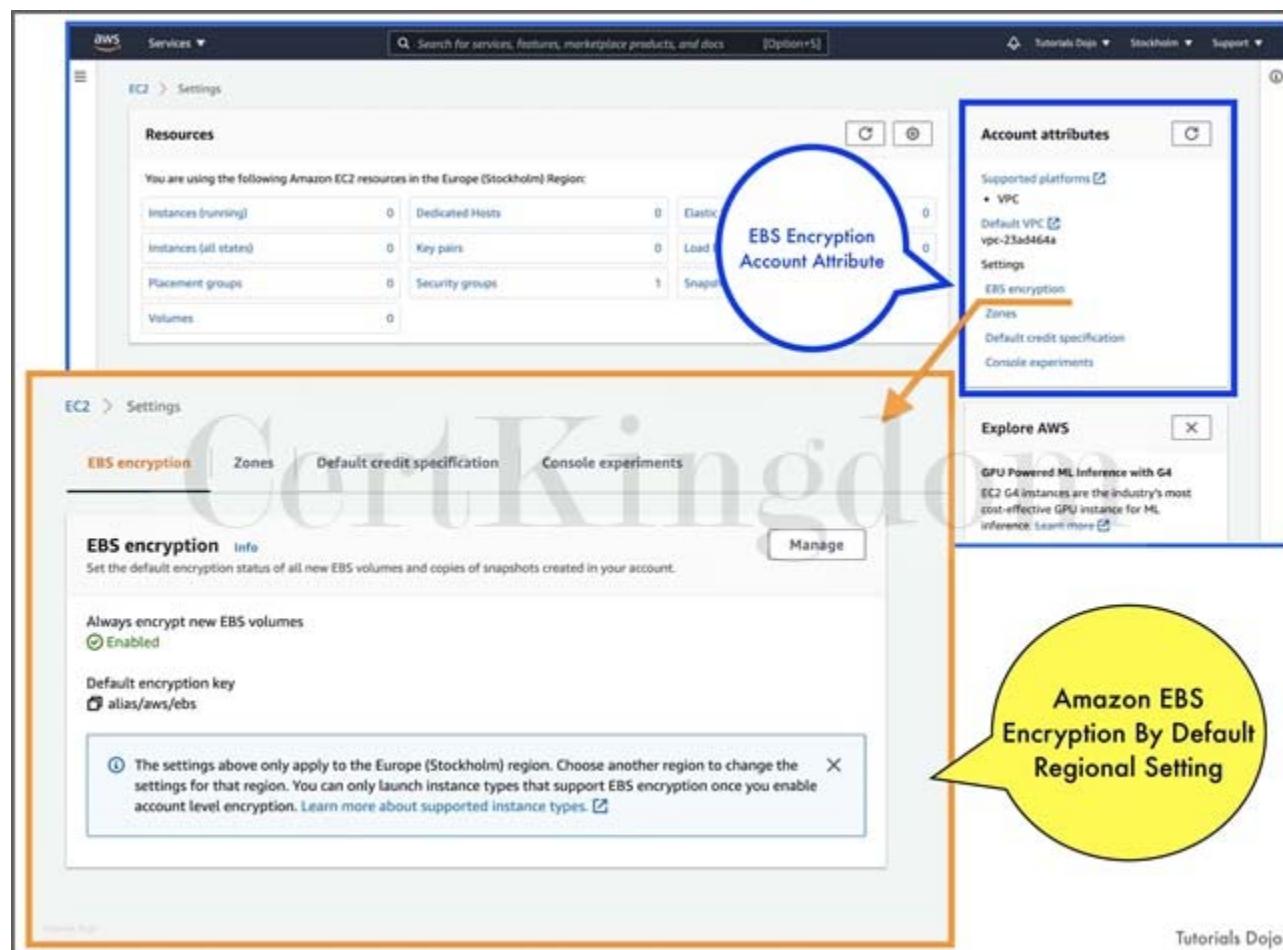
A company has several unencrypted EBS snapshots in their VPC. The Solutions Architect must ensure that all of the new EBS volumes restored from the unencrypted snapshots are automatically encrypted. What should be done to accomplish this requirement?

- A. Launch new EBS volumes and specify the symmetric customer master key (CMK) for encryption.
- B. Enable the EBS Encryption By Default feature for the AWS Region.
- C. Enable the EBS Encryption By Default feature for specific EBS volumes.
- D. Launch new EBS volumes and encrypt them using an asymmetric customer master key (CMK).

Answer: B

Explanation:

You can configure your AWS account to enforce the encryption of the new EBS volumes and snapshot copies that you create. For example, Amazon EBS encrypts the EBS volumes created when you launch an instance and the snapshots that you copy from an unencrypted snapshot.



Encryption by default has no effect on existing EBS volumes or snapshots. The following are important considerations in EBS encryption:

- Encryption by default is a Region-specific setting. If you enable it for a Region, you cannot disable it for individual volumes or snapshots in that Region.
- When you enable encryption by default, you can launch an instance only if the instance type supports EBS encryption.
- Amazon EBS does not support asymmetric CMKs.

When migrating servers using AWS Server Migration Service (SMS), do not turn on encryption by

default. If encryption by default is already on and you are experiencing delta replication failures, turn off encryption by default. Instead, enable AMI encryption when you create the replication job.

You cannot change the CMK that is associated with an existing snapshot or encrypted volume. However, you can associate a different CMK during a snapshot copy operation so that the resulting copied snapshot is encrypted by the new CMK.

Although there is no direct way to encrypt an existing unencrypted volume or snapshot, you can encrypt them by creating either a volume or a snapshot. If you enabled encryption by default, Amazon EBS encrypts the resulting new volume or snapshot using your default key for EBS encryption. Even if you have not enabled encryption by default, you can enable encryption when you create an individual volume or snapshot. Whether you enable encryption by default or in individual creation operations, you can override the default key for EBS encryption and use symmetric customer-managed CMK.

Hence, the correct answer is: Enable the EBS Encryption By Default feature for the AWS Region.

The option that says: Launch new EBS volumes and encrypt them using an asymmetric customer master key (CMK) is incorrect because Amazon EBS does not support asymmetric CMKs. To encrypt an EBS snapshot, you need to use symmetric CMK.

The option that says: Launch new EBS volumes and specify the symmetric customer master key (CMK) for encryption is incorrect. Although this solution will enable data encryption, this process is manual and can potentially cause some unencrypted EBS volumes to be launched. A better solution is to enable the EBS Encryption By Default feature. It is stated in the scenario that all of the new EBS volumes restored from the unencrypted snapshots must be automatically encrypted.

The option that says: Enable the EBS Encryption By Default feature for specific EBS volumes is incorrect because the Encryption By Default feature is a Region-specific setting and thus, you can't enable it to selected EBS volumes only.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#encryption-by-default>

<https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html>

Check out this Amazon EBS Cheat Sheet:

<https://tutorialsdojo.com/amazon-ebs/>

Comparison of Amazon S3 vs Amazon EBS vs Amazon EFS:

<https://tutorialsdojo.com/amazon-s3-vs-ebs-vs-efs/>

---

## QUESTION 336

A startup is building a microservices architecture in which the software is composed of small independent services that communicate over well-defined APIs. In building large-scale systems, fine-grained decoupling of microservices is a recommended practice to implement. The decoupled services should scale horizontally from each other to improve scalability.

What is the difference between Horizontal scaling and Vertical scaling?

A. Vertical scaling means running the same software on a fully serverless architecture using Lambda. Horizontal scaling means adding more servers to the existing pool and it doesn't run into limitations of individual servers.

B. Horizontal scaling means running the same software on smaller containers such as Docker and Kubernetes using ECS or EKS. Vertical scaling is adding more servers to the existing pool and doesn't run into limitations of individual servers.

C. Horizontal scaling means running the same software on bigger machines which is limited by the capacity of individual servers. Vertical scaling is adding more servers to the existing pool and doesn't run into limitations of individual servers.

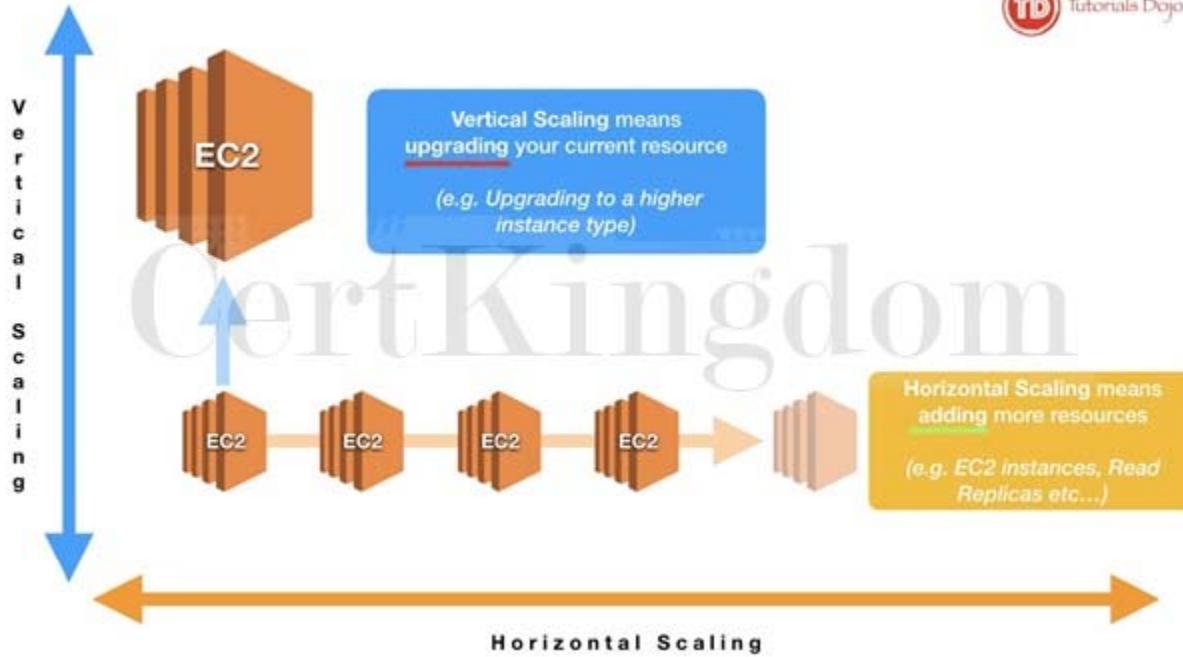
D. Vertical scaling means running the same software on bigger machines which is limited by the capacity of the individual server. Horizontal scaling is adding more servers to the existing pool and doesn't run into limitations of individual servers.

Answer: D

Explanation:

Vertical scaling means running the same software on bigger machines which is limited by the capacity of

the individual server. Horizontal scaling is adding more servers to the existing pool and doesn't run into limitations of individual servers.



Fine-grained decoupling of microservices is a best practice for building large-scale systems. It's a prerequisite for performance optimization since it allows choosing the appropriate and optimal technologies for a specific service. Each service can be implemented with the appropriate programming languages and frameworks, leverage the optimal data persistence solution, and be fine-tuned with the best performing service configurations.

Properly decoupled services can be scaled horizontally and independently from each other. Vertical scaling, which is running the same software on bigger machines, is limited by the capacity of individual servers and can incur downtime during the scaling process. Horizontal scaling, which is adding more servers to the existing pool, is highly dynamic and doesn't run into limitations of individual servers. The scaling process can be completely automated.

Furthermore, the resiliency of the application can be improved because failing components can be easily and automatically replaced. Hence, the correct answer is the option that says: Vertical scaling means running the same software on bigger machines which is limited by the capacity of the individual server. Horizontal scaling is adding more servers to the existing pool and doesn't run into limitations of individual servers.

The option that says: Vertical scaling means running the same software on a fully serverless architecture using Lambda. Horizontal scaling means adding more servers to the existing pool and it doesn't run into limitations of individual servers is incorrect because Vertical scaling is not about running the same software on a fully serverless architecture. AWS Lambda is not required for scaling.

The option that says: Horizontal scaling means running the same software on bigger machines which is limited by the capacity of individual servers. Vertical scaling is adding more servers to the existing pool and doesn't run into limitations of individual servers is incorrect because the definitions for the two concepts were switched. Vertical scaling means running the same software on bigger machines which is limited by the capacity of the individual server. Horizontal scaling is adding more servers to the existing pool and doesn't run into limitations of individual servers.

The option that says: Horizontal scaling means running the same software on smaller containers such as Docker and Kubernetes using ECS or EKS. Vertical scaling is adding more servers to the existing pool and doesn't run into limitations of individual servers is incorrect because Horizontal scaling is not related to using ECS or EKS containers on a smaller instance.

Reference:

<https://docs.aws.amazon.com/aws-technical-content/latest/microservices-on-aws/microservices-on-aws.pdf#page=8>

### QUESTION 337

A tech company is running two production web servers hosted on Reserved EC2 instances with EBS-backed root volumes. These instances have a consistent CPU load of 90%. Traffic is being distributed to these instances by an Elastic Load Balancer. In addition, they also have Multi-AZ RDS MySQL databases for their production, test, and development environments.

What recommendation would you make to reduce cost in this AWS environment without affecting availability and performance of mission-critical systems? Choose the best answer.

- A. Consider using On-demand instances instead of Reserved EC2 instances
- B. Consider removing the Elastic Load Balancer
- C. Consider not using a Multi-AZ RDS deployment for the development and test database
- D. Consider using Spot instances instead of reserved EC2 instances

Answer: C

Explanation:

One thing that you should notice here is that the company is using Multi-AZ databases in all of their environments, including their development and test environment. This is costly and unnecessary as these two environments are not critical. It is better to use Multi-AZ for production environments to reduce costs, which is why the option that says: Consider not using a Multi-AZ RDS deployment for the development and test database is the correct answer.

The option that says: Consider using On-demand instances instead of Reserved EC2 instances is incorrect because selecting Reserved instances is cheaper than On-demand instances for long term usage due to the discounts offered when purchasing reserved instances.

The option that says: Consider using Spot instances instead of reserved EC2 instances is incorrect because the web servers are running in a production environment. Never use Spot instances for production level web servers unless you are sure that they are not that critical in your system. This is because your spot instances can be terminated once the maximum price goes over the maximum amount that you specified.

The option that says: Consider removing the Elastic Load Balancer is incorrect because the Elastic Load Balancer is crucial in maintaining the elasticity and reliability of your system.

References:

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

<https://aws.amazon.com/pricing/cost-optimization/>

Amazon RDS Overview:

<https://www.youtube.com/watch?v=aZmpL18K1UU>

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

---

### QUESTION 338

A Solutions Architect is implementing a new High-Performance Computing (HPC) system in AWS that involves orchestrating several Amazon Elastic Container Service (Amazon ECS) tasks with an EC2 launch type that is part of an Amazon ECS cluster. The system will be frequently accessed by users around the globe and it is expected that there would be hundreds of ECS tasks running most of the time. The Architect must ensure that its storage system is optimized for high-frequency read and write operations. The output data of each ECS task is around 10 MB but the obsolete data will eventually be archived and deleted so the total storage size won't exceed 10 TB.

Which of the following is the MOST suitable solution that the Architect should recommend?

- A. Set up an SMB file share by creating an Amazon FSx File Gateway in Storage Gateway. Set the file share as the container mount point in the ECS task definition of the Amazon ECS cluster.
- B. Launch an Amazon Elastic File System (Amazon EFS) file system with Bursting Throughput mode

and set the performance mode to General Purpose. Configure the EFS file system as the container mount point in the ECS task definition of the Amazon ECS cluster.

- C. Launch an Amazon DynamoDB table with Amazon DynamoDB Accelerator (DAX) and DynamoDB Streams enabled. Configure the table to be accessible by all Amazon ECS cluster instances. Set the DynamoDB table as the container mount point in the ECS task definition of the Amazon ECS cluster.
- D. Launch an Amazon Elastic File System (Amazon EFS) with Provisioned Throughput mode and set the performance mode to Max I/O. Configure the EFS file system as the container mount point in the ECS task definition of the Amazon ECS cluster.

Answer: D

Explanation:

Amazon Elastic File System (Amazon EFS) provides simple, scalable file storage for use with your Amazon ECS tasks. With Amazon EFS, storage capacity is elastic, growing and shrinking automatically as you add and remove files. Your applications can have the storage they need when they need it.

You can use Amazon EFS file systems with Amazon ECS to access file system data across your fleet of Amazon ECS tasks. That way, your tasks have access to the same persistent storage, no matter the infrastructure or container instance on which they land. When you reference your Amazon EFS file system and container mount point in your Amazon ECS task definition, Amazon ECS takes care of mounting the file system in your container.

The screenshot shows the 'File system settings' page for creating a new EFS file system. The 'General' section includes a 'Name - optional' field with 'Tutorials-Dojo-Binondo', a 'Availability and Durability' section with 'Regional' selected (stores data redundantly across multiple AZs), and sections for 'Automatic backups' and 'Lifecycle management'. The 'Performance Mode' section is highlighted with a yellow border, showing 'General Purpose' and 'Max I/O' options, with 'Max I/O' selected. The 'Throughput Mode' section is highlighted with a blue border, showing 'Bursting' and 'Provisioned' options, with 'Provisioned' selected. Below these are fields for 'Provisioned Throughput (MiB/s)' (10) and 'Maximum Read Throughput (MiB/s)' (30). The 'Encryption' section at the bottom is also visible.

To support a wide variety of cloud storage workloads, Amazon EFS offers two performance modes:

- General Purpose mode
- Max I/O mode.

You choose a file system's performance mode when you create it, and it cannot be changed. The two performance modes have no additional costs, so your Amazon EFS file system is billed and metered the same, regardless of your performance mode.

There are two throughput modes to choose from for your file system:

- Bursting Throughput
- Provisioned Throughput

With Bursting Throughput mode, a file system's throughput scales as the amount of data stored in the EFS Standard or One Zone storage class grows. File-based workloads are typically spiky, driving high levels of throughput for short periods of time, and low levels of throughput the rest of the time. To accommodate this, Amazon EFS is designed to burst to high throughput levels for periods of time. Provisioned Throughput mode is available for applications with high throughput to storage (MiB/s per TiB) ratios, or with requirements greater than those allowed by the Bursting Throughput mode. For example, say you're using Amazon EFS for development tools, web serving, or content management applications where the amount of data in your file system is low relative to throughput demands. Your file system can now get the high levels of throughput your applications require without having to pad your file system.

In the scenario, the file system will be frequently accessed by users around the globe so it is expected that there would be hundreds of ECS tasks running most of the time. The Architect must ensure that its storage system is optimized for high-frequency read and write operations.

Hence, the correct answer is: Launch an Amazon Elastic File System (Amazon EFS) with Provisioned Throughput mode and set the performance mode to Max I/O. Configure the EFS file system as the container mount point in the ECS task definition of the Amazon ECS cluster.

The option that says: Set up an SMB file share by creating an Amazon FSx File Gateway in Storage Gateway. Set the file share as the container mount point in the ECS task definition of the Amazon ECS cluster is incorrect. Although you can use an Amazon FSx for Windows File Server in this situation, it is not appropriate to use this since the application is not connected to an on-premises data center. Take note that the AWS Storage Gateway service is primarily used to integrate your existing on-premises storage to AWS.

The option that says: Launch an Amazon Elastic File System (Amazon EFS) file system with Bursting Throughput mode and set the performance mode to General Purpose. Configure the EFS file system as the container mount point in the ECS task definition of the Amazon ECS cluster is incorrect because using Bursting Throughput mode won't be able to sustain the constant demand of the global application. Remember that the application will be frequently accessed by users around the world and there are hundreds of ECS tasks running most of the time.

The option that says: Launch an Amazon DynamoDB table with Amazon DynamoDB Accelerator (DAX) and DynamoDB Streams enabled. Configure the table to be accessible by all Amazon ECS cluster instances. Set the DynamoDB table as the container mount point in the ECS task definition of the Amazon ECS cluster is incorrect because you cannot directly set a DynamoDB table as a container mount point. In the first place, DynamoDB is a database and not a file system which means that it can't be "mounted" to a server.

#### References:

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/tutorial-efs-volumes.html>

<https://docs.aws.amazon.com/efs/latest/ug/performance.html>

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/tutorial-wfsx-volumes.html>

Check out this Amazon EFS Cheat Sheet:

<https://tutorialsdojo.com/amazon-efs/>

---

## QUESTION 339

A company plans to implement a network monitoring system in AWS. The Solutions Architect launched an EC2 instance to host the monitoring system and used CloudWatch to monitor, store, and access the log files of the instance.

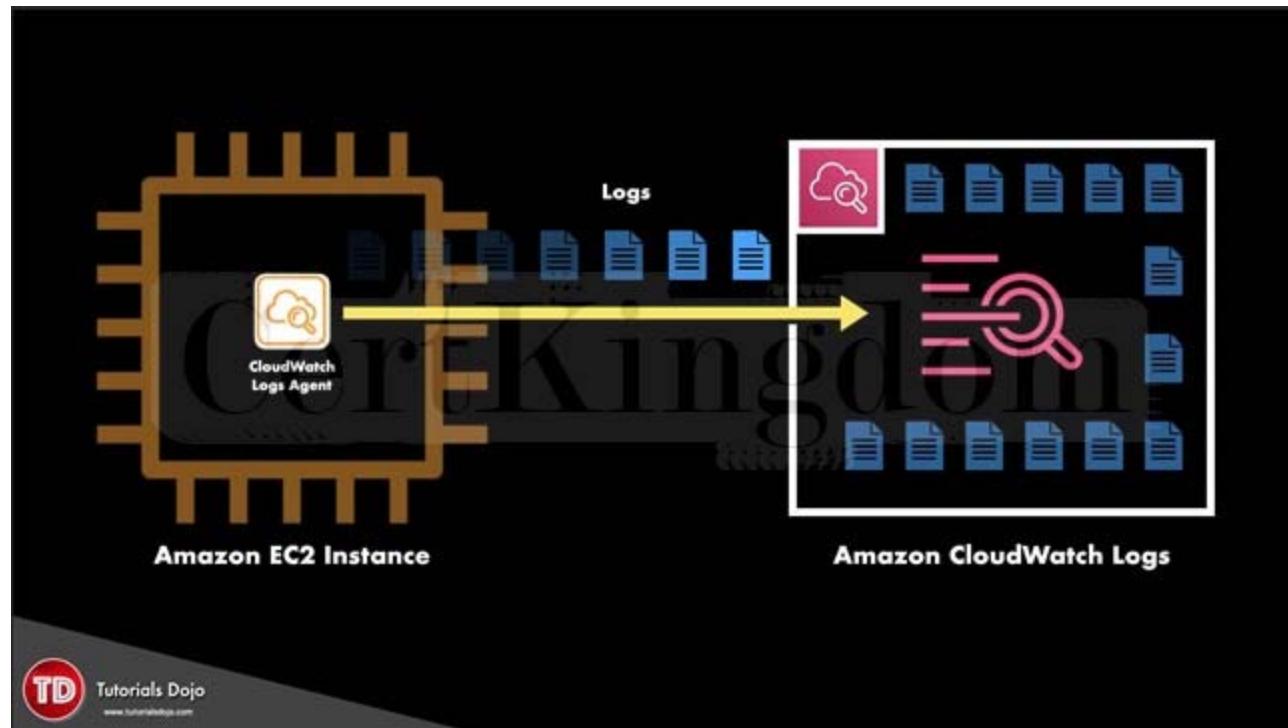
Which of the following provides an automated way to send log data to CloudWatch Logs from the Amazon EC2 instance?

- A. AWS Transfer for SFTP
- B. CloudTrail with log file validation
- C. CloudTrail Processing Library
- D. CloudWatch Logs agent

Answer: D

## Explanation:

CloudWatch Logs enables you to centralize the logs from all of your systems, applications, and AWS services that you use, in a single, highly scalable service. You can then easily view them, search them for specific error codes or patterns, filter them based on specific fields, or archive them securely for future analysis. CloudWatch Logs enables you to see all of your logs, regardless of their source, as a single and consistent flow of events ordered by time, and you can query them and sort them based on other dimensions, group them by specific fields, create custom computations with a powerful query language, and visualize log data in dashboards.



The CloudWatch Logs agent is comprised of the following components:

- A plug-in to the AWS CLI that pushes log data to CloudWatch Logs.
- A script (daemon) that initiates the process to push data to CloudWatch Logs.
- A cron job that ensures that the daemon is always running.

CloudWatch Logs agent provides an automated way to send log data to CloudWatch Logs from Amazon instances hence, CloudWatch Logs agent is the correct answer. CloudTrail with log file validation is incorrect as this is mainly used for tracking the API calls of your AWS resources and not for sending EC2 logs to CloudWatch.

AWS Transfer for SFTP is incorrect as this is only a fully managed SFTP service for Amazon S3 used for tracking the traffic coming into the VPC and not for EC2 instance monitoring. This service enables you to easily move your file transfer workloads that use the Secure Shell File Transfer Protocol (SFTP) to AWS without needing to modify your applications or manage any SFTP servers. This can't be used to send log data from your EC2 instance to Amazon CloudWatch.

CloudTrail Processing Library is incorrect because this is just a Java library that provides an easy way to process AWS CloudTrail logs. It cannot send your log data to CloudWatch Logs.

References:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html>

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AgentReference.html>

Check out this Amazon CloudWatch Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudwatch/>

## QUESTION 340

A company has an application that uses multiple EC2 instances located in various AWS regions such as US East (Ohio), US West (N. California), and EU (Ireland). The manager instructed the Solutions Architect to set up a latency-based routing to route incoming traffic for [www.tutorialsdojo.com](http://www.tutorialsdojo.com) to all the EC2 instances across all AWS regions.

Which of the following options can satisfy the given requirement?

- A. Use Route 53 to distribute the load to the multiple EC2 instances across all AWS Regions.
- B. Use a Network Load Balancer to distribute the load to the multiple EC2 instances across all AWS Regions.

C. Use AWS DataSync to distribute the load to the multiple EC2 instances across all AWS Regions.

D. Use an Application Load Balancer to distribute the load to the multiple EC2 instances across all AWS Regions.

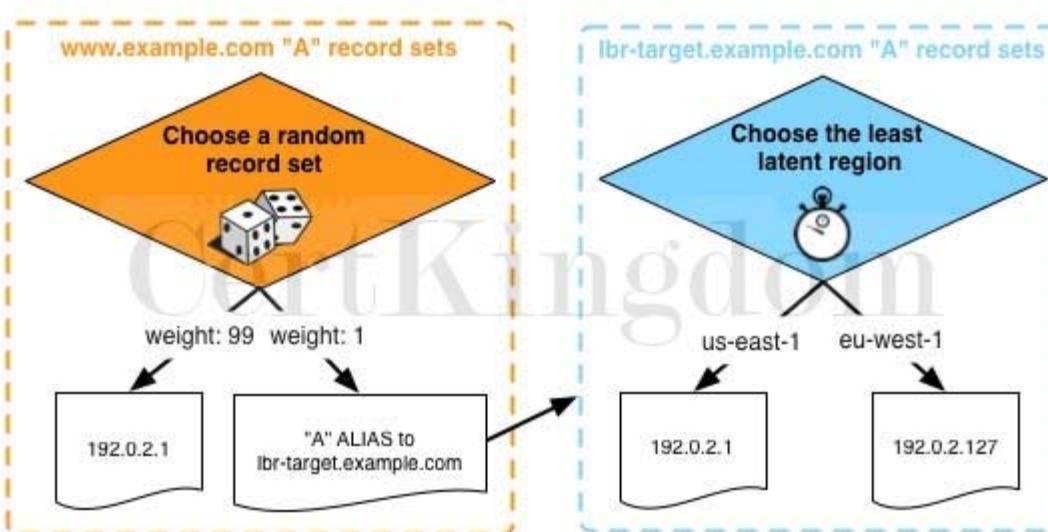
Answer: A

Explanation:

If your application is hosted in multiple AWS Regions, you can improve performance for your users by serving their requests from the AWS Region that provides the lowest latency.

You can create latency records for your resources in multiple AWS Regions by using latency-based routing. In the event that Route 53 receives a DNS query for your domain or subdomain such as [astutorialsdojo.com](http://astutorialsdojo.com) or [portal.tutorialsdojo.com](http://portal.tutorialsdojo.com), it determines which AWS Regions you've created latency records for, determines which region gives the user the lowest latency and then selects a latency record for that region. Route 53 responds with the value from the selected record which can be the IP address for a web server or the CNAME of your elastic load balancer.

Hence, using Route 53 to distribute the load to the multiple EC2 instances across all AWS Regions is the correct answer.



Using a Network Load Balancer to distribute the load to the multiple EC2 instances across all AWS Regions and using an Application Load Balancer to distribute the load to the multiple EC2 instances across all AWS Regions are both incorrect because load balancers distribute traffic only within their respective regions and not to other AWS regions by default. Although Network Load Balancers support connections from clients to IP-based targets in peered VPCs across different AWS Regions, the scenario didn't mention that the VPCs are peered with each other. It is best to use Route 53 instead to balance the incoming load to two or more AWS regions more effectively.

Using AWS DataSync to distribute the load to the multiple EC2 instances across all AWS Regions is incorrect because the AWS DataSync service simply provides a fast way to move large amounts of data online between on-premises storage and Amazon S3 or Amazon Elastic File System (Amazon EFS).

References:

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

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/TutorialAddingLBRRegion.html>

Check out this Amazon Route 53 Cheat Sheet:

<https://tutorialsdojo.com/amazon-route-53/>

## QUESTION 341

A startup is building IoT devices and monitoring applications. They are using IoT sensors to monitor the traffic in real-time by using an Amazon Kinesis Stream that is configured with default settings. It then sends the data to an Amazon S3 bucket every 3 days. When you checked the data in S3 on the 3rd day, only the data for the last day is present and no data is present from 2 days ago.

Which of the following is the MOST likely cause of this issue?

A. Someone has manually deleted the record in Amazon S3.

B. The access of the Kinesis stream to the S3 bucket is insufficient.

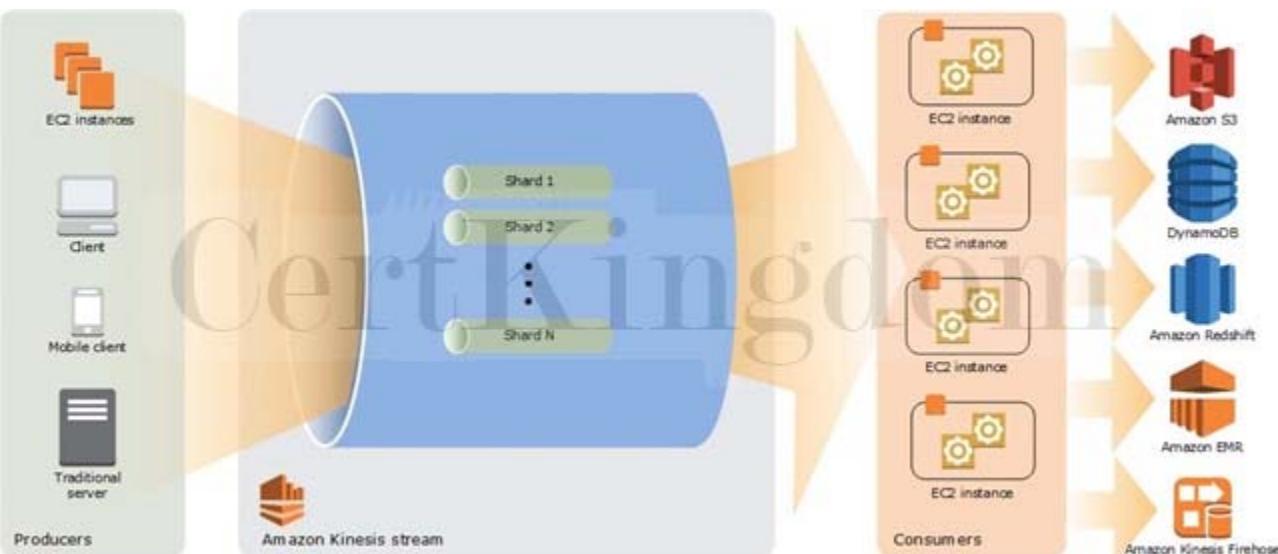
C. By default, data records in Kinesis are only accessible for 24 hours from the time they are added to a stream.

D. Amazon S3 bucket has encountered a data loss.

Answer: C

Explanation:

By default, records of a stream in Amazon Kinesis are accessible for up to 24 hours from the time they are added to the stream. You can raise this limit to up to 7 days by enabling extended data retention.



Hence, the correct answer is: By default, data records in Kinesis are only accessible for 24 hours from the time they are added to a stream.

The option that says: Amazon S3 bucket has encountered a data loss is incorrect because Amazon S3 rarely experiences data loss. Amazon has an SLA for S3 that it commits to its customers. Amazon S3 Standard, S3 Standard-IA, S3 One Zone-IA, and S3 Glacier are all designed to provide 99.999999999% durability of objects over a given year. This durability level corresponds to an average annual expected loss of 0.000000001% of objects. Hence, Amazon S3 bucket data loss is highly unlikely.

The option that says: Someone has manually deleted the record in Amazon S3 is incorrect because if someone has deleted the data, this should have been visible in CloudTrail. Also, deleting that much data manually shouldn't have occurred in the first place if you have put in the appropriate security measures.

The option that says: The access of the Kinesis stream to the S3 bucket is insufficient is incorrect because having insufficient access is highly unlikely since you are able to access the bucket and view the contents of the previous day's data collected by Kinesis.

Reference:

<https://aws.amazon.com/kinesis/data-streams/faqs/>

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

Check out this Amazon Kinesis Cheat Sheet:

<https://tutorialsdojo.com/amazon-kinesis/>

## QUESTION 342

A game development company operates several virtual reality (VR) and augmented reality (AR) games which use various RESTful web APIs hosted on their on-premises data center. Due to the unprecedented growth of their company, they decided to migrate their system to AWS Cloud to scale out their resources as well to minimize costs.

Which of the following should you recommend as the most cost-effective and scalable solution to meet the above requirement?

- A. Use AWS Lambda and Amazon API Gateway.
- B. Use a Spot Fleet of Amazon EC2 instances, each with an Elastic Fabric Adapter (EFA) for more consistent latency and higher network throughput. Set up an Application Load Balancer to distribute traffic to the instances.
- C. Host the APIs in a static S3 web hosting bucket behind a CloudFront web distribution.
- D. Set up a micro-service architecture with ECS, ECR, and Fargate.

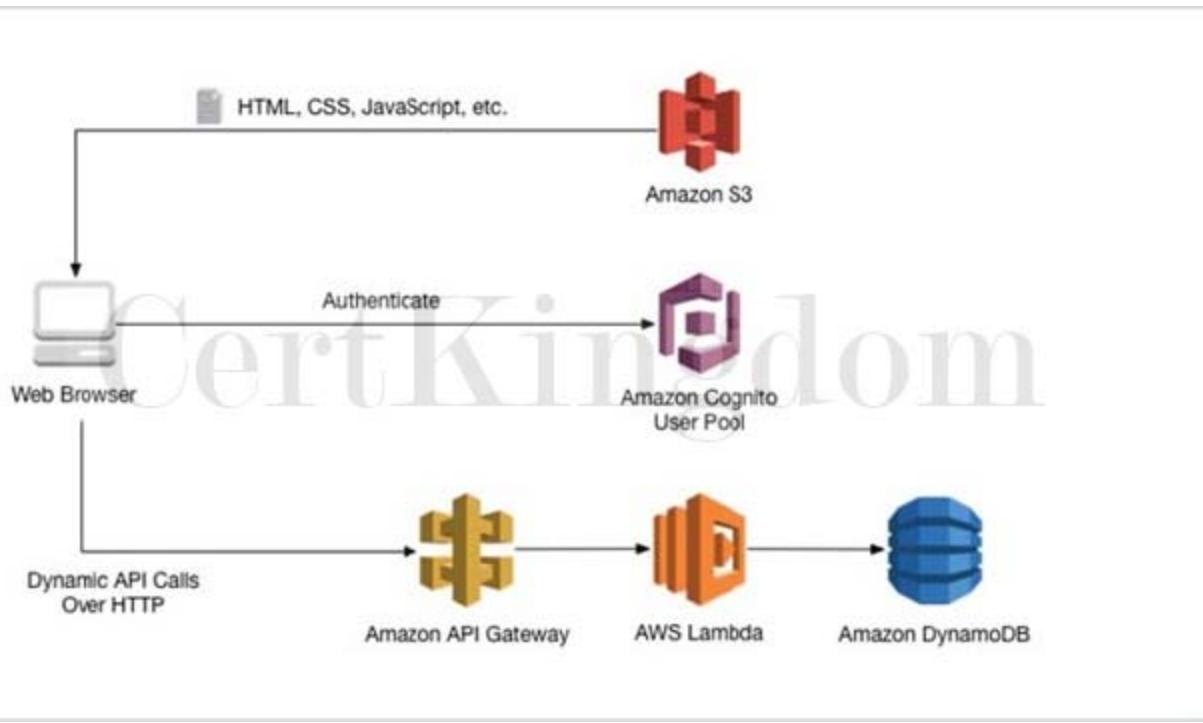
Answer: A

#### Explanation:

With AWS Lambda, you pay only for what you use. You are charged based on the number of requests for your functions and the duration, the time it takes for your code to execute.

Lambda counts a request each time it starts executing in response to an event notification or invoke call, including test invokes from the console. You are charged for the total number of requests across all your functions.

Duration is calculated from the time your code begins executing until it returns or otherwise terminates, rounded up to the nearest 1ms. The price depends on the amount of memory you allocate to your function. The Lambda free tier includes 1M free requests per month and over 400,000 GB-seconds of compute time per month.



The best possible answer here is to use a combination of AWS Lambda and Amazon API Gateway because this solution is both scalable and cost-effective. You will only be charged when you use your Lambda function, unlike having an EC2 instance that always runs even though you don't use it.

Hence, the correct answer is: Use AWS Lambda and Amazon API Gateway.

Setting up a micro-service architecture with ECS, ECR, and Fargate is incorrect because ECS is mainly used to host Docker applications, and in addition, using ECS, ECR, and Fargate alone is not scalable and not recommended for this type of scenario.

Hosting the APIs in a static S3 web hosting bucket behind a CloudFront web distribution is not a suitable option as there is no compute capability for S3 and you can only use it as a static website. Although this solution is scalable since uses CloudFront, the use of S3 to host the web APIs or the dynamic website is still incorrect.

The option that says: Use a Spot Fleet of Amazon EC2 instances, each with an Elastic Fabric Adapter (EFA) for more consistent latency and higher network throughput. Set up an Application Load Balancer to distribute traffic to the instances is incorrect. EC2 alone, without Auto Scaling, is not scalable. Even though you use Spot EC2 instance, it is still more expensive compared to Lambda because you will be charged only when your function is being used. An Elastic Fabric Adapter (EFA) is simply a network device that you can attach to your Amazon EC2 instance that enables you to achieve the application performance of an on-premises HPC cluster, with scalability, flexibility, and elasticity provided by the AWS Cloud. Although EFA is scalable, the Spot Fleet configuration of this option doesn't have Auto Scaling involved.

#### References:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-with-lambda-integration.html>

<https://aws.amazon.com/lambda/pricing/>

Check out this AWS Lambda Cheat Sheet:

<https://tutorialsdojo.com/aws-lambda/>

EC2 Container Service (ECS) vs Lambda:

<https://tutorialsdojo.com/ec2-container-service-ecs-vs-lambda/>

## QUESTION 343

An application is hosted in an Auto Scaling group of EC2 instances and a Microsoft SQL Server on Amazon RDS. There is a requirement that all in-flight data between your web servers and RDS should be secured.

Which of the following options is the MOST suitable solution that you should implement? (Select TWO.)

- A. Download the Amazon RDS Root CA certificate. Import the certificate to your servers and configure your application to use SSL to encrypt the connection to RDS.
- B. Force all connections to your DB instance to use SSL by setting the rds.force\_ssl parameter to true. Once done, reboot your DB instance.
- C. Enable the IAM DB authentication in RDS using the AWS Management Console.
- D. Specify the TDE option in an RDS option group that is associated with that DB instance to enable transparent data encryption (TDE).
- E. Configure the security groups of your EC2 instances and RDS to only allow traffic to and from port 443.

Answer: A,B

Explanation:

You can use Secure Sockets Layer (SSL) to encrypt connections between your client applications and your Amazon RDS DB instances running Microsoft SQL Server. SSL support is available in all AWS regions for all supported SQL Server editions.

When you create an SQL Server DB instance, Amazon RDS creates an SSL certificate for it. The SSL certificate includes the DB instance endpoint as the Common Name (CN) for the SSL certificate to guard against spoofing attacks.

There are 2 ways to use SSL to connect to your SQL Server DB instance:

- Force SSL for all connections “” this happens transparently to the client, and the client doesn't have to do any work to use SSL.
- Encrypt specific connections “” this sets up an SSL connection from a specific client computer, and you must do work on the client to encrypt connections.

Issued To	Issued By	Expiration Date	Intended Purposes
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authentication
Amazon Corporate Systems Cert...	Amazon.com Internal Root Certific...	9/20/2018	<All>
Amazon Corporate Systems Cert...	Amazon.com Internal Root Certific...	10/9/2018	<All>
<b>Amazon RDS Root 2019 CA</b>	<b>Amazon RDS Root 2019 CA</b>	<b>8/22/2024</b>	<b>&lt;All&gt;</b>

You can force all connections to your DB instance to use SSL, or you can encrypt connections from specific client computers only. To use SSL from a specific client, you must obtain certificates for the client computer, import certificates on the client computer, and then encrypt the connections from the client computer.

If you want to force SSL, use the rds.force\_ssl parameter. By default, the rds.force\_ssl parameter is set to false. Set the rds.force\_ssl parameter to true to force connections to use SSL. The rds.force\_ssl parameter is static, so after you change the value, you must reboot your DB instance for the change to take effect.

Hence, the correct answers for this scenario are the options that say:

- Force all connections to your DB instance to use SSL by setting the rds.force\_ssl parameter to true.
- Once done, reboot your DB instance.
- Download the Amazon RDS Root CA certificate. Import the certificate to your servers and configure your application to use SSL to encrypt the connection to RDS.

Specifying the TDE option in an RDS option group that is associated with that DB instance to enable transparent data encryption (TDE) is incorrect because transparent data encryption (TDE) is primarily used to encrypt stored data on your DB instances running Microsoft SQL Server, and not the data that are in transit.

Enabling the IAM DB authentication in RDS using the AWS Management Console is incorrect because IAM database authentication is only supported in MySQL and PostgreSQL database engines. With IAM database authentication, you don't need to use a password when you connect to a DB instance but instead, you use an authentication token.

Configuring the security groups of your EC2 instances and RDS to only allow traffic to and from port 443 is incorrect because it is not enough to do this. You need to either force all connections to your DB instance to use SSL, or you can

encrypt connections from specific client computers, just as mentioned above.

#### References:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/SQLServer.Concepts.General.SSL.Using.html>

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.SQLServer.Options.TDE.html>

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

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

## QUESTION 344

A company requires corporate IT governance and cost oversight of all of its AWS resources across its divisions around the world. Their corporate divisions want to maintain administrative control of the discrete AWS resources they consume and ensure that those resources are separate from other divisions.

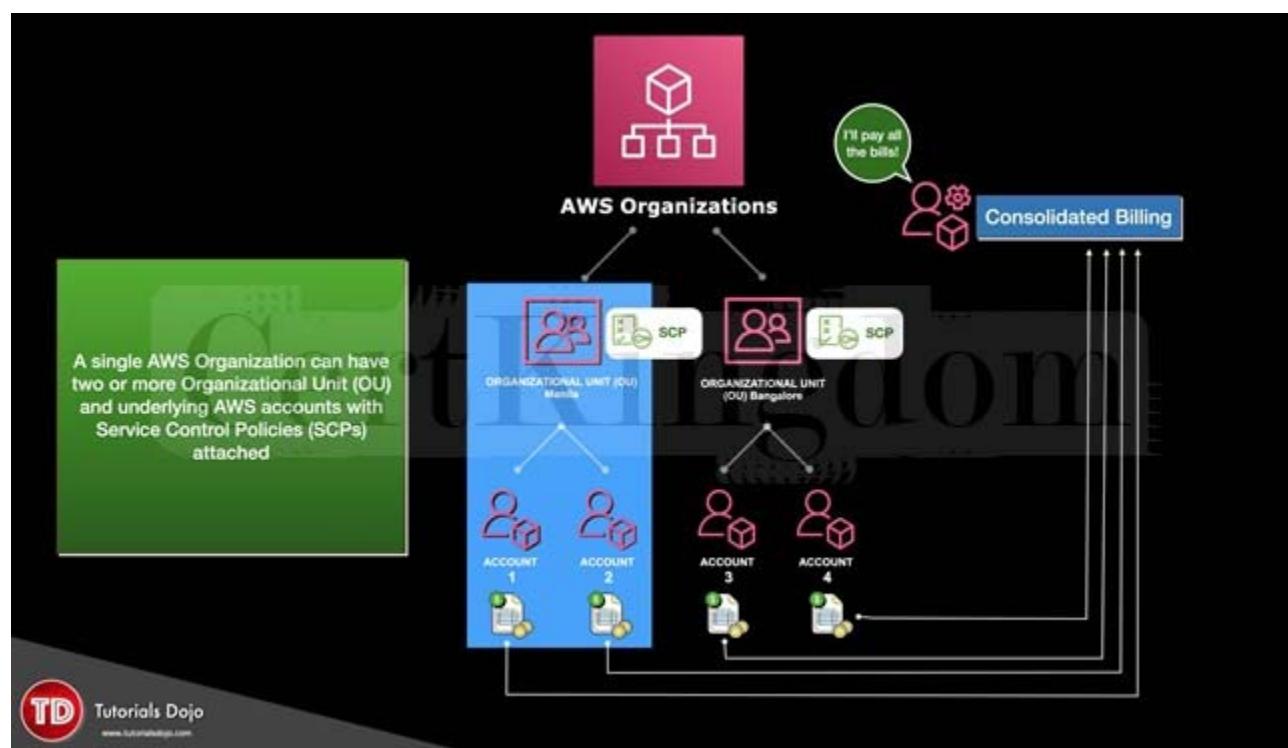
Which of the following options will support the autonomy of each corporate division while enabling the corporate IT to maintain governance and cost oversight? (Select TWO.)

- A. Create separate Availability Zones for each division within the corporate IT AWS account. Improve communication between the two AZs using the AWS Global Accelerator.
- B. Use AWS Trusted Advisor and AWS Resource Groups Tag Editor
- C. Create separate VPCs for each division within the corporate IT AWS account. Launch an AWS Transit Gateway with equal-cost multipath routing (ECMP) and VPN tunnels for intra-VPC communication.
- D. Enable IAM cross-account access for all corporate IT administrators in each child account.
- E. Use AWS Consolidated Billing by creating AWS Organizations to link the divisions' accounts to a parent corporate account.

Answer: D,E

#### Explanation:

You can use an IAM role to delegate access to resources that are in different AWS accounts that you own. You share resources in one account with users in a different account. By setting up cross-account access in this way, you don't need to create individual IAM users in each account. In addition, users don't have to sign out of one account and sign into another in order to access resources that are in different AWS accounts.



You can use the consolidated billing feature in AWS Organizations to consolidate payment for multiple AWS accounts or multiple AISPL accounts. With consolidated billing, you can see a combined view of AWS charges incurred by all of your

accounts. You can also get a cost report for each member account that is associated with your master account. Consolidated billing is offered at no additional charge. AWS and AISPL accounts can't be consolidated together.

The combined use of IAM and Consolidated Billing will support the autonomy of each corporate division while enabling corporate IT to maintain governance and cost oversight. Hence, the correct choices are:

- Enable IAM cross-account access for all corporate IT administrators in each child account
- Use AWS Consolidated Billing by creating AWS Organizations to link the divisions' accounts to a parent corporate account

Using AWS Trusted Advisor and AWS Resource Groups Tag Editor is incorrect. Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. It only provides you alerts on areas where you do not adhere to best practices and tells you how to improve them. It does not assist in maintaining governance over your AWS accounts.

Additionally, the AWS Resource Groups Tag Editor simply allows you to add, edit, and delete tags to multiple AWS resources at once for easier identification and monitoring.

Creating separate VPCs for each division within the corporate IT AWS account. Launch an AWS Transit Gateway with equal-cost multipath routing (ECMP) and VPN tunnels for intra-VPC communication is incorrect because creating separate VPCs would not separate the divisions from each other since they will still be operating under the same account and therefore contribute to the same billing each month. AWS Transit Gateway connects VPCs and on-premises networks through a central hub and acts as a cloud router where each new connection is only made once. For this particular scenario, it is suitable to use AWS Organizations instead of setting up an AWS Transit Gateway since the objective is for maintaining administrative control of the AWS resources and not for network connectivity.

Creating separate Availability Zones for each division within the corporate IT AWS account. Improve communication between the two AZs using the AWS Global Accelerator is incorrect because you do not need to create Availability Zones. They are already provided for you by AWS right from the start, and not all services support multiple AZ deployments. In addition, having separate Availability Zones in your VPC does not meet the requirement of supporting the autonomy of each corporate division. The AWS Global Accelerator is a service that uses the AWS global network to optimize the network path from your users to your applications and not between your Availability Zones.

References:

<http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>

[https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial\\_cross-account-with-roles.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html)

Check out this AWS Billing and Cost Management Cheat Sheet:

<https://tutorialsdojo.com/aws-billing-and-cost-management/>

---

## QUESTION 345

A multinational manufacturing company has multiple accounts in AWS to separate their various departments such as finance, human resources, engineering and many others. There is a requirement to that certain access to services and actions are properly controlled to comply with the security policy of the company.

As the Solutions Architect, which is the most suitable way to set up the multi-account AWS environment of the company?

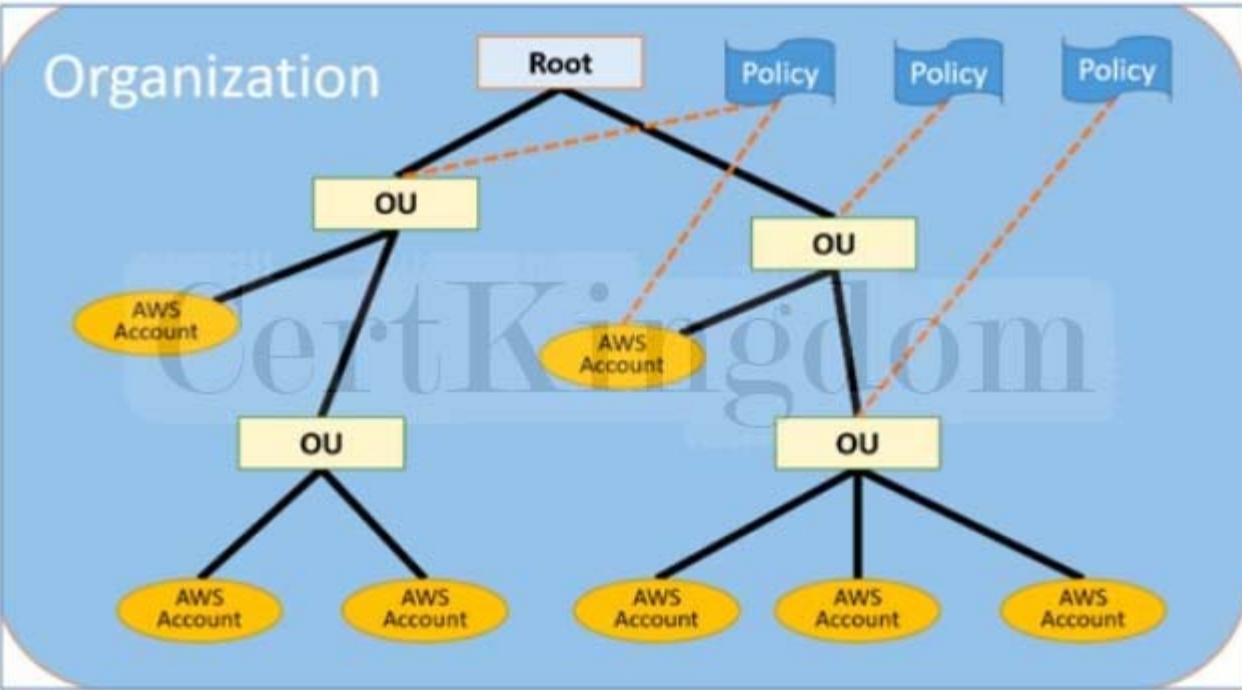
- A. Connect all departments by setting up a cross-account access to each of the AWS accounts of the company. Create and attach IAM policies to your resources based on their respective departments to control access.
- B. Provide access to externally authenticated users via Identity Federation. Set up an IAM role to specify permissions for users from each department whose identity is federated from your organization or a third-party identity provider.
- C. Use AWS Organizations and Service Control Policies to control services on each account.
- D. Set up a common IAM policy that can be applied across all AWS accounts.

Answer: C

Explanation:

Using AWS Organizations and Service Control Policies to control services on each account is the correct answer. Refer to the diagram below:

# Organization



AWS Organizations offers policy-based management for multiple AWS accounts. With Organizations, you can create groups of accounts, automate account creation, apply and manage policies for those groups. Organizations enables you to centrally manage policies across multiple accounts, without requiring custom scripts and manual processes. It allows you to create Service Control Policies (SCPs) that centrally control AWS service use across multiple AWS accounts.

Setting up a common IAM policy that can be applied across all AWS accounts is incorrect because it is not possible to create a common IAM policy for multiple AWS accounts.

The option that says: Connect all departments by setting up a cross-account access to each of the AWS accounts of the company. Create and attach IAM policies to your resources based on their respective departments to control access is incorrect because although you can set up cross-account access to each department, this entails a lot of configuration compared with using AWS Organizations and Service Control Policies (SCPs). Cross-account access would be a more suitable choice if you only have two accounts to manage, but not for multiple accounts.

The option that says: Provide access to externally authenticated users via Identity Federation. Set up an IAM role to specify permissions for users from each department whose identity is federated from your organization or a third-party identity provider is incorrect as this option is focused on the Identity Federation authentication set up for your AWS accounts but not the IAM policy management for multiple AWS accounts. A combination of AWS Organizations and Service Control Policies (SCPs) is a better choice compared to this option.

Reference:

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

Check out this AWS Organizations Cheat Sheet:

<https://tutorialsdojo.com/aws-organizations/>

Service Control Policies (SCP) vs IAM Policies:

<https://tutorialsdojo.com/service-control-policies-scp-vs-iam-policies/>

Comparison of AWS Services Cheat Sheets:

<https://tutorialsdojo.com/comparison-of-aws-services/>

## QUESTION 346

There is a technical requirement by a financial firm that does online credit card processing to have a secure application environment on AWS. They are trying to decide on whether to use KMS or CloudHSM.

Which of the following statements is right when it comes to CloudHSM and KMS?

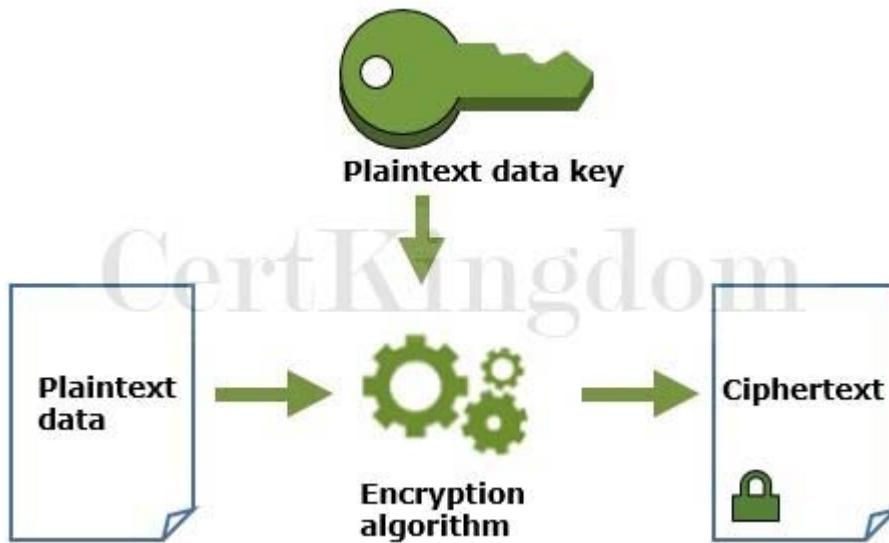
- A. AWS CloudHSM should always be used for any payment transactions.
- B. You should consider using AWS CloudHSM over AWS KMS if you require your keys stored in dedicated, third-party validated hardware security modules under your exclusive control.
- C. If you want a managed service for creating and controlling your encryption keys but don't want or need to operate your own HSM, consider using AWS CloudHSM.
- D. No major difference. They both do the same thing.

Answer: B

Explanation:

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. The master keys that you create in AWS KMS are protected by FIPS 140-2 validated cryptographic modules. AWS KMS is integrated with most other

AWS services that encrypt your data with encryption keys that you manage. AWS KMS is also integrated with AWS CloudTrail to provide encryption key usage logs to help meet your auditing, regulatory and compliance needs.



By using AWS KMS, you gain more control over access to data you encrypt. You can use the key management and cryptographic features directly in your applications or through AWS services that are integrated with AWS KMS. Whether you are writing applications for AWS or using AWS services, AWS KMS enables you to maintain control over who can use your customer master keys and gain access to your encrypted data. AWS KMS is integrated with AWS CloudTrail, a service that delivers log files to an Amazon S3 bucket that you designate. By using CloudTrail you can monitor and investigate how and when your master keys have been used and by whom.

If you want a managed service for creating and controlling your encryption keys, but you don't want or need to operate your own HSM, consider using AWS Key Management Service.

Hence, the correct answer is: You should consider using AWS CloudHSM over AWS KMS if you require your keys stored in dedicated, third-party validated hardware security modules under your exclusive control.

The option that says: No major difference. They both do the same thing is incorrect because KMS and CloudHSM are two different services. If you want a managed service for creating and controlling your encryption keys, without operating your own HSM, you have to consider using AWS Key Management Service.

The option that says: If you want a managed service for creating and controlling your encryption keys, but you don't want or need to operate your own HSM, consider using AWS CloudHSM is incorrect because you have to consider using AWS KMS if you want a managed service for creating and controlling your encryption keys, without operating your own HSM.

The option that says: AWS CloudHSM should always be used for any payment transactions is incorrect because this is not always the case. AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

References:

<https://docs.aws.amazon.com/kms/latest/developerguide/overview.html>

<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#data-keys>

<https://docs.aws.amazon.com/cloudhsm/latest/userguide/introduction.html>

Check out this AWS Key Management Service Cheat Sheet:

<https://tutorialsdojo.com/aws-key-management-service-aws-kms/>

## QUESTION 347

A company developed a financial analytics web application hosted in a Docker container using MEAN (MongoDB, Express.js, AngularJS, and Node.js) stack. You want to easily port that web application to AWS Cloud which can

automatically handle all the tasks such as balancing load, auto-scaling, monitoring, and placing your containers across your cluster.

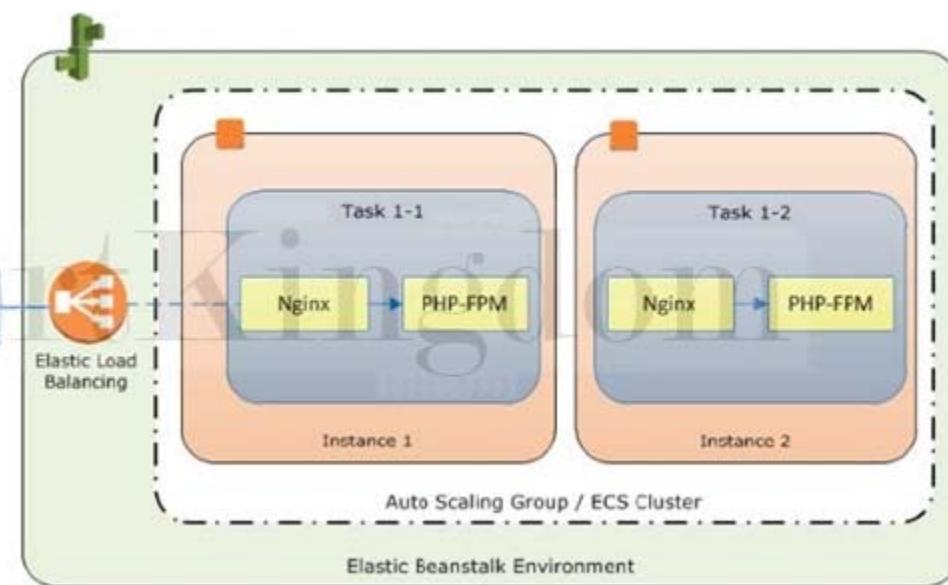
Which of the following services can be used to fulfill this requirement?

- A. Amazon Elastic Container Service (Amazon ECS)
- B. AWS Elastic Beanstalk
- C. AWS Compute Optimizer
- D. AWS CloudFormation

Answer: B

Explanation:

AWS Elastic Beanstalk supports the deployment of web applications from Docker containers. With Docker containers, you can define your own runtime environment. You can choose your own platform, programming language, and any application dependencies (such as package managers or tools), that aren't supported by other platforms. Docker containers are self-contained and include all the configuration information and software your web application requires to run.



By using Docker with Elastic Beanstalk, you have an infrastructure that automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring. You can manage your web application in an environment that supports the range of services that are integrated with Elastic Beanstalk, including but not limited to VPC, RDS, and IAM. Hence, the correct answer is: AWS Elastic Beanstalk.

Amazon Elastic Container Service (Amazon ECS) is incorrect. Although it also provides Service Auto Scaling, Service Load Balancing, and Monitoring with CloudWatch, these features are not automatically enabled by default unlike with Elastic Beanstalk. Take note that the scenario requires a service that will automatically handle all the tasks such as balancing load, auto-scaling, monitoring, and placing your containers across your cluster. You will have to manually configure these things if you wish to use ECS.

With Elastic Beanstalk, you can manage your web application in an environment that supports the range of services easier. AWS CloudFormation is incorrect. While you can deploy the infrastructure for your application thru CloudFormation templates, you will be the one responsible for connecting the AWS resources needed to build your application environment. With ElasticBeanstalk, all you have to do is upload your code; ElasticBeanstalk will automatically set up the environment for your application.

AWS Compute Optimizer is incorrect. Compute Optimizer simply analyzes your workload and recommends the optimal AWS resources needed to improve performance and reduce costs.

Reference:

[https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create\\_deploy\\_docker.html](https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_docker.html)

Check out this AWS Elastic Beanstalk Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-beanstalk/>

AWS Elastic Beanstalk Overview:

<https://youtu.be/rx7e7Fej1Oo>

Elastic Beanstalk vs CloudFormation vs OpsWorks vs CodeDeploy:

## QUESTION 348

A disaster recovery team is planning to back up on-premises records to a local file server share through SMB protocol. To meet the company's business continuity plan, the team must ensure that a copy of data from 48 hours ago is available for immediate access. Accessing older records with delay is tolerable.

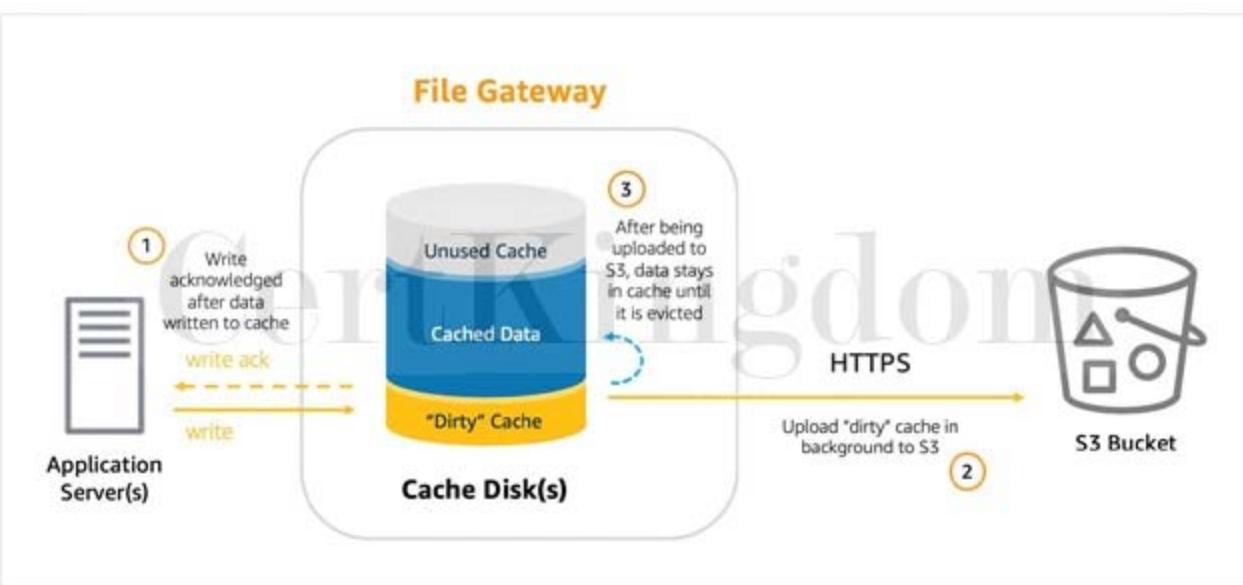
Which should the DR team implement to meet the objective with the LEAST amount of configuration effort?

- A. Create an AWS Backup plan to copy data backups to a local SMB share every 48 hours.
- B. Use an AWS Storage File gateway with enough storage to keep data from the last 48 hours. Send the backups to an SMB share mounted as a local disk.
- C. Create an SMB file share in Amazon FSx for Windows File Server that has enough storage to store all backups. Access the file share from on-premises.
- D. Mount an Amazon EFS file system on the on-premises client and copy all backups to an NFS share.

Answer: B

Explanation:

Amazon S3 File Gateway presents a file interface that enables you to store files as objects in Amazon S3 using the industry-standard NFS and SMB file protocols, and access those files via NFS and SMB from your data center or Amazon EC2, or access those files as objects directly in Amazon S3.



When you deploy File Gateway, you specify how much disk space you want to allocate for local cache. This local cache acts as a buffer for writes and provides low latency access to data that was recently written to or read from Amazon S3. When a client writes data to a file via File Gateway, that data is first written to the local cache disk on the gateway itself. Once the data has been safely persisted to the local cache, only then does the File Gateway acknowledge the write back to the client. From there, File Gateway transfers the data to the S3 bucket asynchronously in the background, optimizing data transfer using multipart parallel uploads, and encrypting data in transit using HTTPS.

In this scenario, you can deploy an AWS Storage File Gateway to the on-premises client. After activating the File Gateway, create an SMB share and mount it as a local disk at the on-premises end. Copy the backups to the SMB share. You must ensure that you size the File Gateway's local cache appropriately to the backup data that needs immediate access. After the backup is done, you will be able to access the older data but with a delay. There will be a small delay since data (not in cache) needs to be retrieved from Amazon S3.

Hence, the correct answer is: Use an AWS Storage File gateway with enough storage to keep data from the last 48 hours. Send the backups to an SMB share mounted as a local disk.

The option that says: Create an SMB file share in Amazon FSx for Windows File Server that has enough storage to store all backups. Access the file share from on-premises is incorrect because this requires additional setup. You need to set up a

Direct Connect or VPN connection from on-premises to AWS first in order for this to work.

The option that says: Mount an Amazon EFS file system on the on-premises client and copy all backups to an NFS share is incorrect because the file share required in the scenario needs to be using the SMB protocol.

The option that says: Create an AWS Backup plan to copy data backups to a local SMB share every 48 hours is incorrect.

AWS Backup only works on AWS resources.

References:

<https://aws.amazon.com/blogs/storage/easily-store-your-sql-server-backups-in-amazon-s3-using-file-gateway/>

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

AWS Storage Gateway Overview:

<https://www.youtube.com/watch?v=pNb7xOBJjHE>

Check out this AWS Storage Gateway Cheat Sheet:

<https://tutorialsdojo.com/aws-storage-gateway/>

---

## QUESTION 349

A company deployed a fleet of Windows-based EC2 instances with IPv4 addresses launched in a private subnet. Several software installed in the EC2 instances are required to be updated via the Internet.

Which of the following services can provide the firm a highly available solution to safely allow the instances to fetch the software patches from the Internet but prevent outside network from initiating a connection?

- A. NAT Instance
- B. VPC Endpoint
- C. Egress-Only Internet Gateway
- D. NAT Gateway

Answer: D

Explanation:

AWS offers two kinds of NAT devices – a NAT gateway or a NAT instance. It is recommended to use NAT gateways, as they provide better availability and bandwidth over NAT instances. The NAT Gateway service is also a managed service that does not require your administration efforts. A NAT instance is launched from a NAT AMI.

Just like a NAT instance, you can use a network address translation (NAT) gateway 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.

Here is a diagram showing the differences between NAT gateway and NAT instance:



Attribute	NAT gateway	NAT instance
Availability	Highly available. NAT gateways in each Availability Zone are implemented with redundancy. Create a NAT gateway in each Availability Zone to ensure zone-independent architecture.	Use a script to manage failover between instances
Bandwidth	Can scale up to 45 Gbps.	Depends on the bandwidth of the instance type
Maintenance	Manage by AWS	Manage by you.
Performance	Software is optimized for handling NAT traffic	A generic Amazon Linux AMI that's configured to perform NAT
Cost	Charged depending on the number of NAT gateways you use, duration of usage, and amount of data that you send through the NAT gateways.	Charged depending on the number of NAT instances that you use, duration of usage, and instance type and size.
Type and size	Uniform offering; you don't need to decide on the type or size.	Choose a suitable instance type and size, according to your predicted workload
Public IP addresses	Choose the Elastic IP address to associate with a NAT gateway at creation.	Use an elastic IP address or a public IP address with a NAT instance. You can change the public IP address at any time by associating a new elastic IP address with the instance.
Private IP addresses	Automatically selected from the subnet's IP address range when you create the gateway.	Assign a specific private IP address from the subnet's IP address range when you launch the instance.
Security groups	Cannot be associated with a NAT gateway	Associate with your NAT instance and the resources behind your NAT instance to control inbound and outbound traffic.
Network ACLs	Use a network ACL to control the traffic to and from the subnet in which your NAT gateway resides.	Use a network ACL to control the traffic to and from the subnet in which your NAT instance resides.
Flow logs	Use flow logs to capture the traffic.	Use flow logs to capture the traffic.
Port Forwarding	Not supported.	Manually customize the configuration to support port forwarding.
Bastion Servers	Not supported.	Use as a bastion server.
Traffic Metrics	Monitor your NAT gateway using CloudWatch Metrics.	View CloudWatch metrics for the instance.
Timeout Behavior	When a connection times out, a NAT gateway returns an RST packet to any resources behind the NAT gateway that attempt to continue the connection (it does not send a FIN packet).	When a connection times out, a NAT instance sends a FIN packet to resources behind the NAT instance to close the connection.
IP Fragmentation	Supports forwarding of IP fragmented packets for the UDP protocol. Does not support fragmentation for the TCP and ICMP protocols. Fragmented packets for these protocols will get dropped.	Supports reassembly of IP fragmented packets for the UDP, TCP, and ICMP protocols.

Egress-Only Internet Gateway is incorrect because this is primarily used for VPCs that use IPv6 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, just like what NAT Instance and NAT Gateway do. The scenario explicitly says that the EC2 instances are using IPv4 addresses which is why Egressonly Internet gateway is invalid, even though it can provide the required high availability.

VPC Endpoint is incorrect because this simply enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an Internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

NAT Instance is incorrect because although this can also enable instances in a private subnet to connect to the Internet or other AWS services and prevent the Internet from initiating a connection with those instances, it is not as highly available compared to a NAT Gateway.

#### References:

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

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

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

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

#### QUESTION 350

A company plans to design an application that can handle batch processing of large amounts of financial data. The Solutions

Architect is tasked to create two Amazon S3 buckets to store the input and output data. The application will transfer the data between multiple EC2 instances over the network to complete the data processing.

Which of the following options would reduce the data transfer costs?

- A. Deploy the Amazon EC2 instances in the same Availability Zone.
- B. Deploy the Amazon EC2 instances in the same AWS Region.
- C. Deploy the Amazon EC2 instances behind an Application Load Balancer.
- D. Deploy the Amazon EC2 instances in private subnets in different Availability Zones.

Answer: A

Explanation:

Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) Cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.



In this scenario, you should deploy all the EC2 instances in the same Availability Zone. If you recall, data transferred between Amazon EC2, Amazon RDS, Amazon Redshift, Amazon ElastiCache instances, and Elastic Network Interfaces in the same Availability Zone is free. Instead of using the public network to transfer the data, you can use the private network to reduce the overall data transfer costs.

Hence, the correct answer is: Deploy the Amazon EC2 instances in the same Availability Zone.

The option that says: Deploy the Amazon EC2 instances in the same AWS Region is incorrect because even if the instances are deployed in the same Region, they could still be charged with inter-Availability Zone data transfers if the instances are distributed across different availability zones. You must deploy the instances in the same Availability Zone to avoid the data transfer costs.

The option that says: Deploy the Amazon EC2 instances behind an Application Load Balancer is incorrect because this approach won't reduce the overall data transfer costs. An Application Load Balancer is primarily used to distribute the incoming traffic to underlying EC2 instances.

The option that says: Deploy the Amazon EC2 instances in private subnets in different Availability Zones is incorrect. Although the data transfer between instances in private subnets is free, there will be an issue with retrieving the data in Amazon S3. Remember that you won't be able to connect to your Amazon S3 bucket if you are using a private subnet unless you have a VPC Endpoint.

References:

<https://aws.amazon.com/ec2/pricing/on-demand/>

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

<https://aws.amazon.com/blogs/mt/using-aws-cost-explorer-to-analyze-data-transfer-costs/>

Amazon EC2 Overview:

[https://www.youtube.com/watch?v=7VsGIHT\\_jQE](https://www.youtube.com/watch?v=7VsGIHT_jQE)

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

---

## QUESTION 351

A startup is building an AI-based face recognition application in AWS, where they store millions of images in an S3 bucket. As the Solutions Architect, you have to ensure that each and every image uploaded to their system is stored without any issues.

What is the correct indication that an object was successfully stored when you put objects in Amazon S3?

- A. You will receive an SMS from Amazon SNS informing you that the object is successfully stored.
- B. You will receive an email from Amazon SNS informing you that the object is successfully stored.
- C. HTTP 200 result code and MD5 checksum.
- D. Amazon S3 has 99.999999999% durability hence, there is no need to confirm that data was inserted.

Answer: C

Explanation:

If you triggered an S3 API call and got HTTP 200 result code and MD5 checksum, then it is considered as a successful upload. The S3 API will return an error code in case the upload is unsuccessful.

The option that says: Amazon S3 has 99.999999999% durability hence, there is no need to confirm that data was inserted is incorrect because although S3 is durable, it is not an assurance that all objects uploaded using S3 API calls will be successful.

The options that say: You will receive an SMS from Amazon SNS informing you that the object is successfully stored and You will receive an email from Amazon SNS informing you that the object is successfully stored are both incorrect because you don't receive an SMS nor an email notification by default, unless you added an event notification.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectPOST.html>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

---

## QUESTION 352

A website hosted on Amazon ECS container instances loads slowly during peak traffic, affecting its availability. Currently, the container instances are run behind an Application Load Balancer, and CloudWatch alarms are configured to send notifications to the operations team if there is a problem in availability so they can scale out if needed. A solutions architect needs to create an automatic scaling solution when such problems occur.

Which solution could satisfy the requirement? (Select TWO.)

- A. Create an AWS Auto Scaling policy that scales out an ECS service when the ALB endpoint becomes unreachable.
- B. Create an AWS Auto Scaling policy that scales out the ECS cluster when the ALB target group's CPU utilization is too high.
- C. Create an AWS Auto Scaling policy that scales out the ECS service when the service's memory utilization is too high.
- D. Create an AWS Auto Scaling policy that scales out the ECS service when the ALB hits a high CPU utilization.
- E. Create an AWS Auto Scaling policy that scales out the ECS cluster when the cluster's CPU utilization is too high.

Answer: C,E

Explanation:

AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to set up application scaling for multiple resources across multiple services in minutes. The service provides a simple, powerful user interface that lets you build scaling plans for resources including Amazon EC2 instances and Spot Fleets, Amazon ECS tasks, Amazon DynamoDB tables and indexes, and Amazon Aurora Replicas.

In this scenario, you can set up a scaling policy that triggers a scale-out activity to an ECS service or ECS container instance

based on the metric that you prefer.

The following metrics are available for instances:

CPU Utilization

Disk Reads

Disk Read Operations

Disk Writes

Disk Write Operations

Network In

Network Out

Status Check Failed (Any)

Status Check Failed (Instance)

Status Check Failed (System)

The following metrics are available for ECS Service:

ECSServiceAverageCPUUtilization””Average CPU utilization of the service.

ECSServiceAverageMemoryUtilization””Average memory utilization of the service.

ALBRequestCountPerTarget””Number of requests completed per target in an Application Load Balancer target group.

Hence, the correct answers are:

- Create an AWS Auto scaling policy that scales out the ECS service when the service’s memory utilization is too high.
- Create an AWS Auto scaling policy that scales out the ECS cluster when the cluster’s CPU utilization is too high.

The option that says: Create an AWS Auto scaling policy that scales out an ECS service when the ALB endpoint becomes unreachable is incorrect. This would be a different problem that needs to be addressed differently if this is the case. An unreachable ALB endpoint could mean other things like a misconfigured security group or network access control lists.

The option that says: Create an AWS Auto scaling policy that scales out the ECS service when the ALB hits a high CPU utilization is incorrect. ALB is a managed resource. You cannot track nor view its resource utilization.

The option that says: Create an AWS Auto scaling policy that scales out the ECS cluster when the ALB target group’s CPU utilization is too high is incorrect. AWS Auto Scaling does not support this metric for ALB.

References:

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-configure-auto-scaling.html>

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

Check out this AWS Auto Scaling Cheat Sheet:

<https://tutorialsdojo.com/aws-auto-scaling/>

---

### QUESTION 353

A fast food company is using AWS to host their online ordering system which uses an Auto Scaling group of EC2 instances deployed across multiple Availability Zones with an Application Load Balancer in front. To better handle the incoming traffic from various digital devices, you are planning to implement a new routing system where requests which have a URL of <server>/api/android are forwarded to one specific target group named "Android-Target-Group". Conversely, requests which have a URL of <server>/api/ios are forwarded to another separate target group named "iOS-Target-Group".

How can you implement this change in AWS?

- A. Use path conditions to define rules that forward requests to different target groups based on the URL in the request.
- B. Replace your ALB with a Gateway Load Balancer then use path conditions to define rules that forward requests to different target groups based on the URL in the request.
- C. Replace your ALB with a Network Load Balancer then use host conditions to define rules that forward requests to different target groups based on the URL in the request.
- D. Use host conditions to define rules that forward requests to different target groups based on the hostname in the host header. This enables you to support multiple domains using a single load balancer.

Answer: A

Explanation:

If your application is composed of several individual services, an Application Load Balancer can route a request to a service based on the content of the request such as Host field, Path URL, HTTP header, HTTP method, Query string, or Source IP address. Path-based routing allows you to route a client request based on the URL path of the HTTP header. Each path

condition has one path pattern. If the URL in a request matches the path pattern in a listener rule exactly, the request is routed using that rule.

The screenshot shows the AWS ELB console interface. A new rule is being created for the 'Tutorials Dojo Palawan ELB | HTTP:80' listener. The 'IF' section is expanded, showing various path condition options. The 'THEN' section contains a single forward action to a target group. A note at the bottom left indicates that the rule cannot be moved or deleted.

A path pattern is case-sensitive, can be up to 128 characters in length, and can contain any of the following characters. You can include up to three wildcard characters.

A-Z, a-z, 0-9

\_ - . \$ / ~ ' ' @ : +

& (using &)

\* (matches 0 or more characters)

? (matches exactly 1 character)

Example path patterns

/img/\*

/js/\*

You can use path conditions to define rules that forward requests to different target groups based on the URL in the request (also known as path-based routing). This type of routing is the most appropriate solution for this scenario hence, the correct answer is: Use path conditions to define rules that forward requests to different target groups based on the URL in the request.

The option that says: Use host conditions to define rules that forward requests to different target groups based on the hostname in the host header. This enables you to support multiple domains using a single load balancer is incorrect because host-based routing defines rules that forward requests to different

target groups based on the hostname in the host header instead of the URL, which is what is needed in this scenario.

The option that says: Replace your ALB with a Gateway Load Balancer then use path conditions to define rules that forward requests to different target groups based on the URL in the request is incorrect because a Gateway Load Balancer does not support path-based routing. You must use an Application Load Balancer.

The option that says: Replace your ALB with a Network Load Balancer then use host conditions to define rules that forward requests to different target groups based on the URL in the request is incorrect because a Network Load Balancer is used for applications that need extreme network performance and static IP. It also does not support path-based routing which is what is needed in this scenario.

Furthermore, the statement mentions host-based routing even though the scenario is about path-based routing.

References:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html#application-load-balancer-benefits>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html#path-conditions>

Check out this AWS Elastic Load Balancing (ELB) Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

Application Load Balancer vs Network Load Balancer vs Classic Load Balancer:

<https://tutorialsdojo.com/application-load-balancer-vs-network-load-balancer-vs-classic-load-balancer/>

---

## QUESTION 354

A Solutions Architect needs to set up the required compute resources for the application which have workloads that require high, sequential read and write access to very large data sets on local storage.

Which of the following instance type is the most suitable one to use in this scenario?

- A. General Purpose Instances
- B. Memory Optimized Instances
- C. Compute Optimized Instances
- D. Storage Optimized Instances

Answer: D

Explanation:

Storage optimized instances are designed for workloads that require high, sequential read and write access to very large data sets on local storage. They are optimized to deliver tens of thousands of lowlatency, random I/O operations per second (IOPS) to applications.

---

<b>C: Compute Optimized Instances</b>	Cost-effective high performance at a low price per compute ratio
<b>D: Storage Optimized Instances</b>	High disk throughput
<b>G: Accelerated Computing Instances</b>	Graphics-intensive GPU instances
<b>H: Storage Optimized Instances</b>	HDD-based local storage for high disk throughput
<b>I: Storage Optimized Instances</b>	High storage instances, low latency, high random I/O performance, high sequential read throughput, and high IOPS
<b>M: General Purpose Instances</b>	Fixed performance
<b>P: Accelerated Computing Instances</b>	General purpose GPU instances
<b>F: Accelerated Computing Instances</b>	Reconfigurable FPGA instances
<b>R: Memory Optimized Instances</b>	Memory-intensive applications
<b>T: General Purpose Instances</b>	Burstable performance instances
<b>X: Memory Optimized Instances</b>	Large-scale, enterprise-class, in-memory applications, and high-performance databases

Hence, the correct answer is: Storage Optimized Instances.

Memory Optimized Instances is incorrect because these are designed to deliver fast performance for workloads that process large data sets in memory, which is quite different from handling high read and write capacity on local storage.

Compute Optimized Instances is incorrect because these are ideal for compute-bound applications that benefit from high-performance processors, such as batch processing workloads and media transcoding.

General Purpose Instances is incorrect because these are the most basic type of instances. They provide a balance of compute, memory, and networking resources, and can be used for a variety of workloads. Since you are requiring higher read and write capacity, storage optimized instances should be selected instead.

Reference:

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

Amazon EC2 Overview:

[https://www.youtube.com/watch?v=7VsGIHT\\_jQE](https://www.youtube.com/watch?v=7VsGIHT_jQE)

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

---

### QUESTION 355

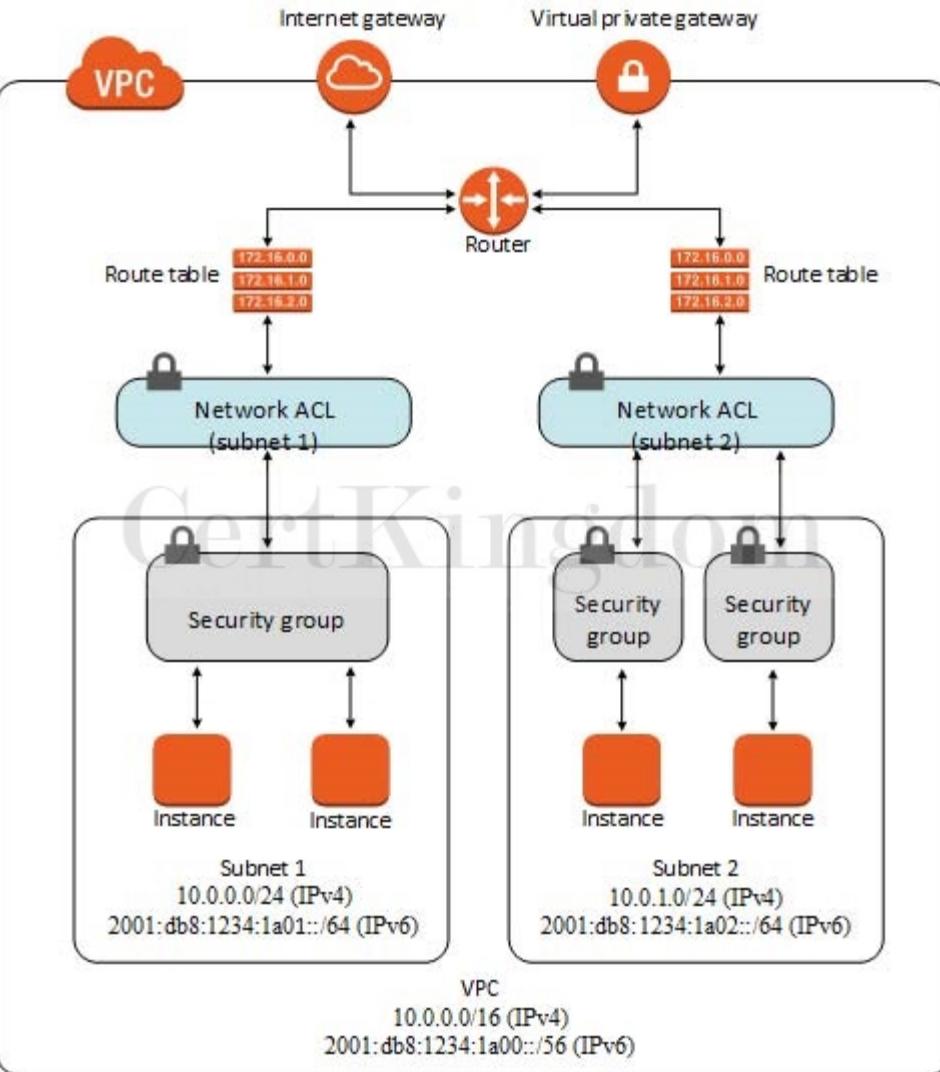
A Solutions Architect is developing a three-tier cryptocurrency web application for a FinTech startup. The Architect has been instructed to restrict access to the database tier to only accept traffic from the application-tier and deny traffic from other sources. The application-tier is composed of application servers hosted in an Auto Scaling group of EC2 instances. Which of the following options is the MOST suitable solution to implement in this scenario?

- A. Set up the Network ACL of the database subnet to deny all inbound non-database traffic from the subnet of the application-tier.
- B. Set up the security group of the database tier to allow database traffic from the security group of the application servers.
- C. Set up the Network ACL of the database subnet to allow inbound database traffic from the subnet of the application-tier.
- D. Set up the security group of the database tier to allow database traffic from a specified list of application server IP addresses.

Answer: B

Explanation:

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC.



For each security group, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic. This section describes the basic things you need to know about security groups for your VPC and their rules.

You can add or remove rules for a security group which is also referred to as authorizing or revoking inbound or outbound access. A rule applies either to inbound traffic (ingress) or outbound traffic (egress).

You can grant access to a specific CIDR range, or to another security group in your VPC or in a peer VPC (requires a VPC peering connection).

In the scenario, the servers of the application-tier are in an Auto Scaling group which means that the number of EC2 instances could grow or shrink over time. An Auto Scaling group could also cover one or more Availability Zones (AZ) which have their own subnets. Hence, the most suitable solution would be to set up the security group of the database tier to allow database traffic from the security group of the application servers since you can utilize the security group of the application-tier Auto Scaling group as the source for the security group rule in your database tier.

Setting up the security group of the database tier to allow database traffic from a specified list of application server IP addresses is incorrect because the list of application server IP addresses will change over time since an Auto Scaling group can add or remove EC2 instances based on the configured scaling policy. This will create inconsistencies in your application because the newly launched instances, which are not included in the initial list of IP addresses, will not be able to access the database.

Setting up the Network ACL of the database subnet to deny all inbound non-database traffic from the subnet of the application-tier is incorrect because doing this could affect the other EC2 instances of other applications, which are also hosted in the same subnet of the application-tier. For example, a large subnet with a CIDR block of could be shared by several applications. Denying all inbound nondatabase traffic from the entire subnet will impact other applications which use this subnet.

Setting up the Network ACL of the database subnet to allow inbound database traffic from the subnet of the application-tier is incorrect because although this solution can work, the subnet of the application-tier could be shared by another tier or another set of EC2 instances other than the application-tier. This means that you would inadvertently be granting database access to unauthorized servers hosted in the same subnet other than the application-tier.

References:

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Security.html#VPC\\_Security\\_Comparison](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html#VPC_Security_Comparison)

[http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_SecurityGroups.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html)

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

---

## QUESTION 356

A construction company has an online system that tracks all of the status and progress of their projects.

The system is hosted in AWS and there is a requirement to monitor the read and write IOPs metrics for their MySQL RDS instance and send real-time alerts to their DevOps team.

Which of the following services in AWS can you use to meet the requirements? (Select TWO.)

- A. Amazon Simple Queue Service
- B. Amazon Simple Notification Service
- C. CloudWatch
- D. Route 53
- E. SWF

Answer: B,C

Explanation:

In this scenario, you can use CloudWatch to monitor your AWS resources and SNS to provide notification. Hence, the correct answers are CloudWatch and Amazon Simple Notification Service.

Amazon Simple Notification Service (SNS) is a flexible, fully managed pub/sub messaging and mobile notifications service for coordinating the delivery of messages to subscribing endpoints and clients.

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources.

SWF is incorrect because this is mainly used for managing workflows and not for monitoring and notifications.

Amazon Simple Queue Service is incorrect because this is a messaging queue service and not suitable for this kind of scenario.

Route 53 is incorrect because this is primarily used for routing and domain name registration and management.

References:

[http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CW\\_Support\\_For\\_AWS.html](http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CW_Support_For_AWS.html)

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

Check out this Amazon CloudWatch Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudwatch/>

---

## QUESTION 357

An application is using a Lambda function to process complex financial data that runs for 15 minutes on average. Most invocations were successfully processed. However, you noticed that there are a few terminated invocations throughout the day, which caused data discrepancy in the application.

Which of the following is the most likely cause of this issue?

- A. The concurrent execution limit has been reached.
- B. The Lambda function contains a recursive code and has been running for over 15 minutes.
- C. The failed Lambda functions have been running for over 15 minutes and reached the maximum execution time.
- D. The failed Lambda Invocations contain a ServiceException error which means that the AWS Lambda service encountered an internal error.

Answer: C

Explanation:

A Lambda function consists of code and any associated dependencies. In addition, a Lambda function also has configuration information associated with it. Initially, you specify the configuration information when you create a Lambda function.

Lambda provides an API for you to update some of the configuration data.

You pay for the AWS resources that are used to run your Lambda function. To prevent your Lambda function from running indefinitely, you specify a timeout. When the specified timeout is reached, AWS Lambda terminates execution of your Lambda function. It is recommended that you set this value based on your expected execution time. The default timeout is 3 seconds and the maximum execution duration per request in AWS Lambda is 900 seconds, which is equivalent to 15 minutes. Hence, the correct answer is the option that says: The failed Lambda functions have been running for over 15 minutes and reached the maximum execution time.

The screenshot shows the AWS Lambda console interface. At the top, there are tabs for 'Throttle', 'Qualifiers', 'Actions', and 'Select a t'. Below these, the 'Basic settings' section is visible. Under 'Description', there is a large input field containing the placeholder text 'CertKingdom'. In the 'Memory (MB)' section, a slider is set to 128 MB. Below the slider, it says 'Your function is allocated CPU proportional to the memory configured.' In the 'Timeout' section, the value is set to 15 min 0 sec. A green rounded rectangle highlights the 'Timeout' input field.

Take note that you can invoke a Lambda function synchronously either by calling the Invoke operation or by using an AWS SDK in your preferred runtime. If you anticipate a long-running Lambda function, your client may time out before function execution completes. To avoid this, update the client timeout or your SDK configuration.

The option that says: The concurrent execution limit has been reached is incorrect because, by default, the AWS Lambda limits the total concurrent executions across all functions within a given region to 1000.

By setting a concurrency limit on a function, Lambda guarantees that allocation will be applied specifically to that function, regardless of the amount of traffic processing the remaining functions. If that limit is exceeded, the function will be throttled but not terminated, which is in contrast with what is happening in the scenario.

The option that says: The Lambda function contains a recursive code and has been running for over 15 minutes is incorrect because having a recursive code in your Lambda function does not directly result to an abrupt termination of the function execution. This is a scenario wherein the function automatically calls itself until some arbitrary criteria is met. This could lead to an unintended volume of function invocations and escalated costs, but not an abrupt termination because Lambda will throttle all invocations to the function.

The option that says: The failed Lambda Invocations contain a ServiceException error which means that the AWS Lambda service encountered an internal error is incorrect because although this is a valid root cause, it is unlikely to have several ServiceException errors throughout the day unless there is an outage or disruption in AWS. Since the scenario says that the Lambda function runs for about 10 to 15 minutes, the maximum execution duration is the most likely cause of the issue and not the AWS Lambda service encountering an internal error.

References:

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

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

AWS Lambda Overview - Serverless Computing in AWS:

<https://www.youtube.com/watch?v=bPVX1zHwAny>

Check out this AWS Lambda Cheat Sheet:

<https://tutorialsdojo.com/aws-lambda/>

## QUESTION 358

A company is using an Amazon RDS for MySQL 5.6 with Multi-AZ deployment enabled and several web servers across two AWS Regions. The database is currently experiencing highly dynamic reads due to the growth of the company's website. The Solutions Architect tried to test the read performance from the secondary AWS Region and noticed a notable slowdown on the SQL queries.

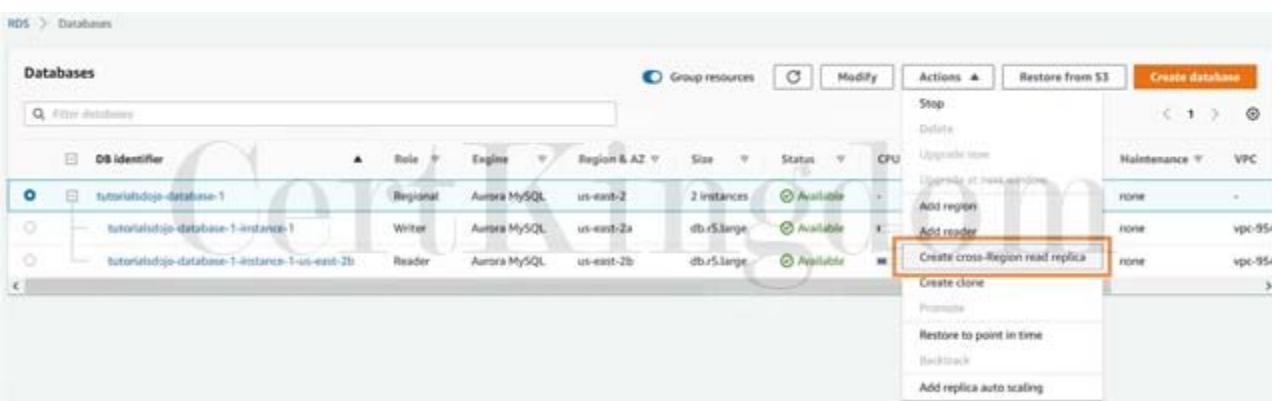
Which of the following options would provide a read replication latency of less than 1 second?

- A. Migrate the existing database to Amazon Aurora and create a cross-region read replica.
- B. Use Amazon ElastiCache to improve database performance.
- C. Upgrade the MySQL database engine.
- D. Create an Amazon RDS for MySQL read replica in the secondary AWS Region.

Answer: A

Explanation:

Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud, that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases. Amazon Aurora is up to five times faster than standard MySQL databases and three times faster than standard PostgreSQL databases.



It provides the security, availability, and reliability of commercial databases at 1th the cost. Amazon Aurora is fully managed by Amazon RDS, which automates time-consuming administration tasks like hardware provisioning, database setup, patching, and backups.

Based on the given scenario, there is a significant slowdown after testing the read performance from the secondary AWS Region. Since the existing setup is an Amazon RDS for MySQL, you should migrate the database to Amazon Aurora and create a cross-region read replica.

Feature	Amazon Aurora Replicas	MySQL Replicas
Number of replicas	Up to 15	Up to 5
Replication type	Asynchronous (milliseconds)	Asynchronous (seconds)
Performance impact on primary	Low	High
Replica location	In-region	Cross-region
Act as failover target	Yes (no data loss)	Yes (potentially minutes of data loss)
Automated failover	Yes	No
Support for user-defined replication delay	No	Yes
Support for different data or schema vs. primary	No	Yes

Less than 1 second!

The read replication latency of less than 1 second is only possible if you would use Amazon Aurora replicas. Aurora replicas are independent endpoints in an Aurora DB cluster, best used for scaling read operations and increasing availability. You can create up to 15 replicas within an AWS Region.

Hence, the correct answer is: Migrate the existing database to Amazon Aurora and create a cross-region read replica. The option that says: Upgrade the MySQL database engine is incorrect because upgrading the database engine wouldn't improve the read replication latency to milliseconds. To achieve the read replication latency of less than 1-second requirement, you need to use Amazon Aurora replicas.

The option that says: Use Amazon ElastiCache to improve database performance is incorrect. Amazon ElastiCache won't be able to improve the database performance because it is experiencing highly dynamic reads. This option would be helpful if the database frequently receives the same queries.

The option that says: Create an Amazon RDS for MySQL read replica in the secondary AWS Region is incorrect because MySQL replicas won't provide you a read replication latency of less than 1 second.

RDS Read Replicas can only provide asynchronous replication in seconds and not in milliseconds. You have to use Amazon Aurora replicas in this scenario.

References:

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

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

Amazon Aurora Overview:

<https://youtu.be/iwS1h7rLNQ>

Check out this Amazon Aurora Cheat Sheet:

<https://tutorialsdojo.com/amazon-aurora/>

---

### QUESTION 359

A top university has recently launched its online learning portal where the students can take e-learning courses from the comforts of their homes. The portal is on a large On-Demand EC2 instance with a single Amazon Aurora database.

How can you improve the availability of your Aurora database to prevent any unnecessary downtime of the online portal?

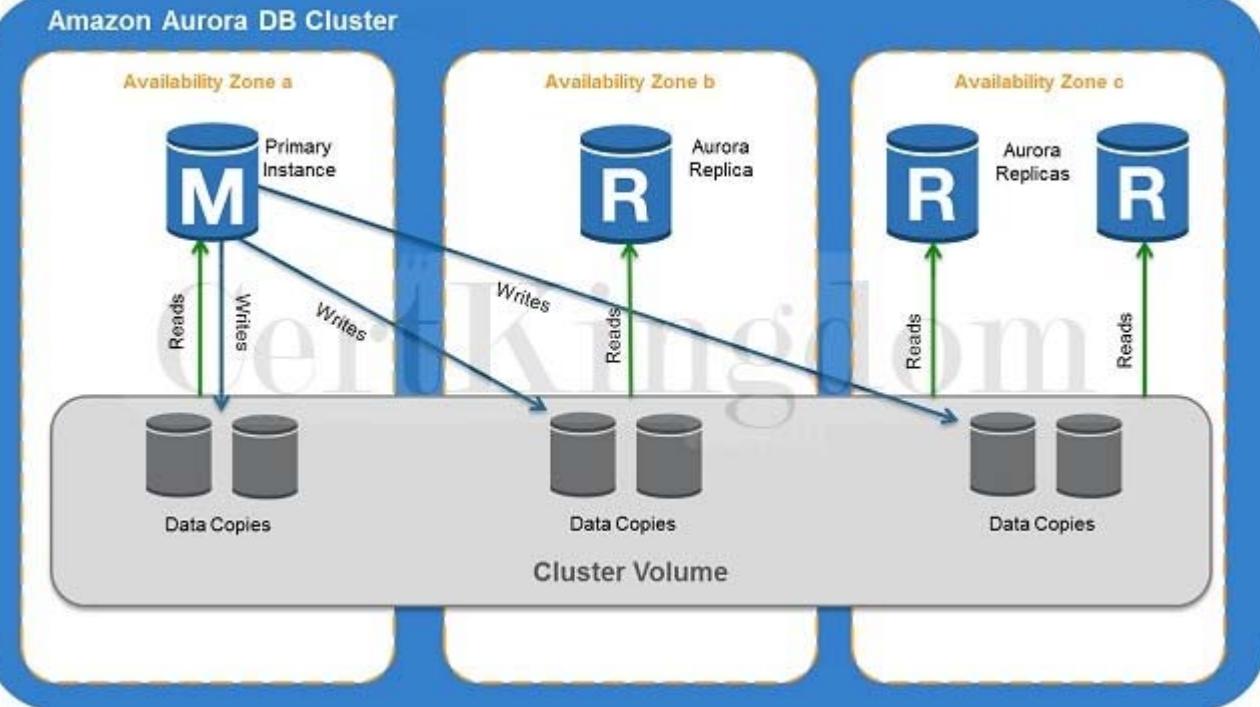
- A. Enable Hash Joins to improve the database query performance.
- B. Deploy Aurora to two Auto-Scaling groups of EC2 instances across two Availability Zones with an elastic load balancer which handles load balancing.
- C. Use an Asynchronous Key Prefetch in Amazon Aurora to improve the performance of queries that join tables across indexes.
- D. Create Amazon Aurora Replicas.

Answer: D

Explanation:

Amazon Aurora MySQL and Amazon Aurora PostgreSQL support Amazon Aurora Replicas, which share the same underlying volume as the primary instance. Updates made by the primary are visible to all Amazon Aurora Replicas.

## Amazon Aurora DB Cluster



With Amazon Aurora MySQL, you can also create MySQL Read Replicas based on MySQL's binlog-based replication engine. In MySQL Read Replicas, data from your primary instance is replayed on your replica as transactions. For most use cases, including read scaling and high availability, it is recommended using Amazon Aurora Replicas.

Read Replicas are primarily used for improving the read performance of the application. The most suitable solution in this scenario is to use Multi-AZ deployments instead but since this option is not available, you can still set up Read Replicas which you can promote as your primary stand-alone DB cluster in the event of an outage.

Hence, the correct answer here is to create Amazon Aurora Replicas.

Deploying Aurora to two Auto-Scaling groups of EC2 instances across two Availability Zones with an elastic load balancer which handles load balancing is incorrect because Aurora is a managed database engine for RDS and not deployed on typical EC2 instances that you manually provision.

Enabling Hash Joins to improve the database query performance is incorrect because Hash Joins are mainly used if you need to join a large amount of data by using an equijoin and not for improving availability.

Using an Asynchronous Key Prefetch in Amazon Aurora to improve the performance of queries that join tables across indexes is incorrect because the Asynchronous Key Prefetch is mainly used to improve the performance of queries that join tables across indexes.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/AuroraMySQL.BestPractices.html>

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

Amazon Aurora Overview:

<https://youtu.be/iwS1h7rLNQ>

Check out this Amazon Aurora Cheat Sheet:

<https://tutorialsdojo.com/amazon-aurora/>

## QUESTION 360

A company has a fleet of running Spot EC2 instances behind an Application Load Balancer. The incoming traffic comes from various users across multiple AWS regions and you would like to have the user's session shared among the fleet of instances. You are required to set up a distributed session management layer that will provide a scalable and shared data storage for the user sessions.

Which of the following would be the best choice to meet the requirement while still providing submillisecond latency for the users?

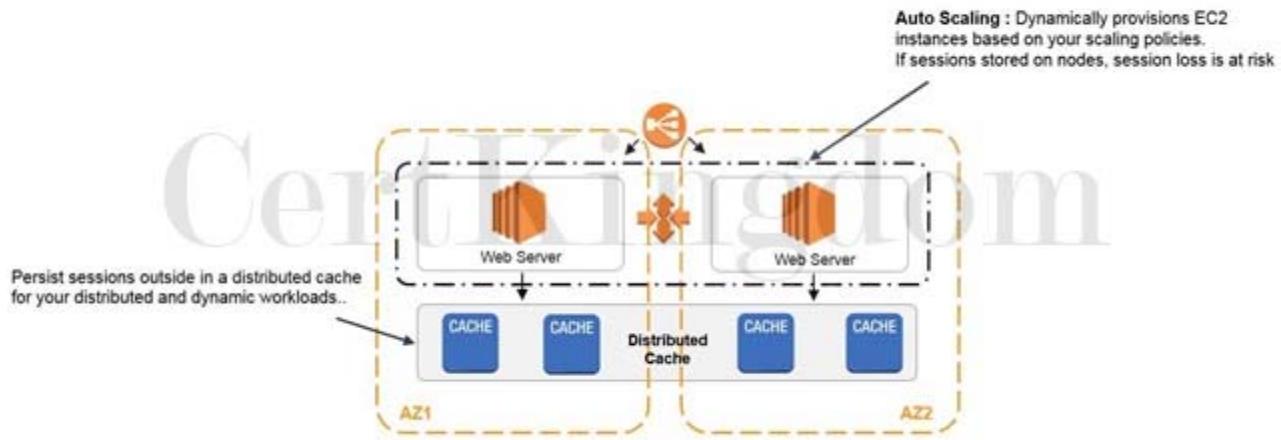
- A. ElastiCache in-memory caching
- B. Multi-AZ RDS
- C. ELB sticky sessions

## D. Multi-master DynamoDB

Answer: A

Explanation:

For sub-millisecond latency caching, ElastiCache is the best choice. In order to address scalability and to provide a shared data storage for sessions that can be accessed from any individual web server, you can abstract the HTTP sessions from the web servers themselves. A common solution for this is to leverage an In-Memory Key/Value store such as Redis and Memcached.



ELB sticky sessions is incorrect because the scenario does not require you to route a user to the particular web server that is managing that individual user's session. Since the session state is shared among the instances, the use of the ELB sticky sessions feature is not recommended in this scenario.

Multi-master DynamoDB and Multi-AZ RDS are incorrect. Although you can use DynamoDB and RDS for storing session state, these two are not the best choices in terms of cost-effectiveness and performance when compared to ElastiCache. There is a significant difference in terms of latency if you used DynamoDB and RDS when you store the session data.

References:

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

<https://d0.awsstatic.com/whitepapers/performance-at-scale-with-amazon-elasticsearch.pdf>

Check out this Amazon ElastiCache Cheat Sheet:

<https://tutorialsdojo.com/amazon-elasticache/>

Redis (cluster mode enabled vs disabled) vs Memcached:

<https://tutorialsdojo.com/redis-cluster-mode-enabled-vs-disabled-vs-memcached/>

---

## QUESTION 361

A tech company is having an issue whenever they try to connect to the newly created EC2 instance using a Remote Desktop connection from a computer. Upon checking, the Solutions Architect has verified that the instance has a public IP and the Internet gateway and route tables are in place.

What else should he do to resolve this issue?

- A. You should restart the EC2 instance since there might be some issue with the instance
- B. Adjust the security group to allow inbound traffic on port 3389 from the company's IP address.
- C. You should create a new instance since there might be some issue with the instance
- D. Adjust the security group to allow inbound traffic on port 22 from the company's IP address.

Answer: B

Explanation:

Since you are using a Remote Desktop connection to access your EC2 instance, you have to ensure that the Remote Desktop Protocol is allowed in the security group. By default, the server listens on TCP port 3389 and UDP port 3389.

The screenshot shows the AWS VPC Security Groups Inbound Rules configuration. A new rule is being created for port 3389 (TCP). The source is set to 125.185.225.183/32. The description is "Allow RDP access".

Hence, the correct answer is: Adjust the security group to allow inbound traffic on port 3389 from the company's IP address. The option that says: Adjust the security group to allow inbound traffic on port 22 from the company's IP address is incorrect as port 22 is used for SSH connections and not for RDP.

The options that say: You should restart the EC2 instance since there might be some issue with the instance and You should create a new instance since there might be some issue with the instance are incorrect as the EC2 instance is newly created and hence, unlikely to cause the issue. You have to check the security group first if it allows the Remote Desktop Protocol (3389) before investigating if there is indeed an issue on the specific instance.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/troubleshooting-windows-instances.html#dp-issues>

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_SecurityGroups.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html)

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

---

## QUESTION 362

A company has several EC2 Reserved Instances in their account that need to be decommissioned and shut down since they are no longer used by the development team. However, the data is still required by the audit team for compliance purposes. Which of the following steps can be taken in this scenario? (Select TWO.)

- A. You can opt to sell these EC2 instances on the AWS Reserved Instance Marketplace
- B. Convert the EC2 instances to Spot instances with a persistent Spot request type.
- C. Take snapshots of the EBS volumes and terminate the EC2 instances.
- D. Stop all the running EC2 instances.
- E. Convert the EC2 instance to On-Demand instances

Answer: A,C

Explanation:

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment.

The first requirement as per the scenario is to decommission and shut down several EC2 Reserved Instances. However, it is also mentioned that the audit team still requires the data for compliance purposes. To fulfill the given requirements, you can first create a snapshot of the instance to save its data and then sell the instance to the Reserved Instance Marketplace.

The Reserved Instance Marketplace is a platform that supports the sale of third-party and AWS customers' unused Standard Reserved Instances, which vary in terms of length and pricing options. For example, you may want to sell Reserved Instances after moving instances to a new AWS region, changing to a new instance type, ending projects before the term expiration, when your business needs change, or if you have unneeded capacity.

Hence, the correct answers are:

- You can opt to sell these EC2 instances on the AWS Reserved Instance Marketplace.
- Take snapshots of the EBS volumes and terminate the EC2 instances.

The option that says: Convert the EC2 instance to On-Demand instances is incorrect because it's stated in the scenario that the development team no longer needs several EC2 Reserved Instances. By converting it to On-Demand instances, the company will still have instances running in their infrastructure and this will result in additional costs.

The option that says: Convert the EC2 instances to Spot instances with a persistent Spot request type is incorrect because the requirement in the scenario is to terminate or shut down several EC2 Reserved Instances. Converting the existing instances

to Spot instances will not satisfy the given requirement.

The option that says: Stop all the running EC2 instances is incorrect because doing so will still incur storage cost. Take note that the requirement in the scenario is to decommission and shut down several EC2 Reserved Instances. Therefore, this approach won't fulfill the given requirement.

References:

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

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

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

AWS Container Services Overview:

<https://www.youtube.com/watch?v=5QBgDX7O7pw>

## QUESTION 363

A company is planning to deploy a High Performance Computing (HPC) cluster in its VPC that requires a scalable, high-performance file system. The storage service must be optimized for efficient workload processing, and the data must be accessible via a fast and scalable file system interface. It should also work natively with Amazon S3 that enables you to easily process your S3 data with a high-performance POSIX interface.

Which of the following is the MOST suitable service that you should use for this scenario?

- A. Amazon FSx for Windows File Server
- B. Amazon FSx for Lustre
- C. Amazon Elastic Block Storage (EBS)
- D. Amazon Elastic File System (EFS)

Answer: B

Explanation:

Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads such as machine learning, high performance computing (HPC), video processing, financial modeling, and electronic design automation (EDA). These workloads commonly require data to be presented via a fast and scalable file system interface, and typically have data sets stored on long-term data stores like Amazon S3.

Operating high-performance file systems typically require specialized expertise and administrative overhead, requiring you to provision storage servers and tune complex performance parameters. With Amazon FSx, you can launch and run a file system that provides sub-millisecond access to your data and allows you to read and write data at speeds of up to hundreds of gigabytes per second of throughput and millions of IOPS.

Amazon FSx for Lustre works natively with Amazon S3, making it easy for you to process cloud data sets with high-performance file systems. When linked to an S3 bucket, an FSx for Lustre file system transparently presents S3 objects as files and allows you to write results back to S3. You can also use FSx for Lustre as a standalone high-performance file system to burst your workloads from on-premises to the cloud. By copying on-premises data to an FSx for Lustre file system, you can make that data available for fast processing by compute instances running on AWS. With Amazon FSx, you pay for only the resources you use. There are no minimum commitments, upfront hardware or software costs, or additional fees.



For Windows-based applications, Amazon FSx provides fully managed Windows file servers with features and performance optimized for "lift-and-shift" business-critical application workloads including home directories (user shares), media

workflows, and ERP applications. It is accessible from Windows and Linux instances via the SMB protocol. If you have Linux-based applications, Amazon EFS is a cloudnative fully managed file system that provides simple, scalable, elastic file storage accessible from Linux instances via the NFS protocol.

For compute-intensive and fast processing workloads, like high-performance computing (HPC), machine learning, EDA, and media processing, Amazon FSx for Lustre, provides a file system that's optimized for performance, with input and output stored on Amazon S3.

Hence, the correct answer is: Amazon FSx for Lustre.

Amazon Elastic File System (EFS) is incorrect because although the EFS service can be used for HPC applications, it doesn't natively work with Amazon S3. It doesn't have the capability to easily process your S3 data with a high-performance POSIX interface, unlike Amazon FSx for Lustre.

Amazon FSx for Windows File Server is incorrect because although this service is a type of Amazon FSx, it does not work natively with Amazon S3. This service is a fully managed native Microsoft Windows file system that is primarily used for your Windows-based applications that require shared file storage to AWS.

Amazon Elastic Block Storage (EBS) is incorrect because this service is not a scalable, highperformance file system.

References:

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

<https://aws.amazon.com/getting-started/use-cases/hpc/>

Check out this Amazon FSx Cheat Sheet:

<https://tutorialsdojo.com/amazon-fsx/>

---

## QUESTION 364

A company plans to host a movie streaming app in AWS. The chief information officer (CIO) wants to ensure that the application is highly available and scalable. The application is deployed to an Auto Scaling group of EC2 instances on multiple AZs. A load balancer must be configured to distribute incoming requests evenly to all EC2 instances across multiple Availability Zones.

Which of the following features should the Solutions Architect use to satisfy these criteria?

- A. Amazon VPC IP Address Manager (IPAM)
- B. Cross-zone load balancing
- C. Path-based Routing
- D. AWS Direct Connect SiteLink

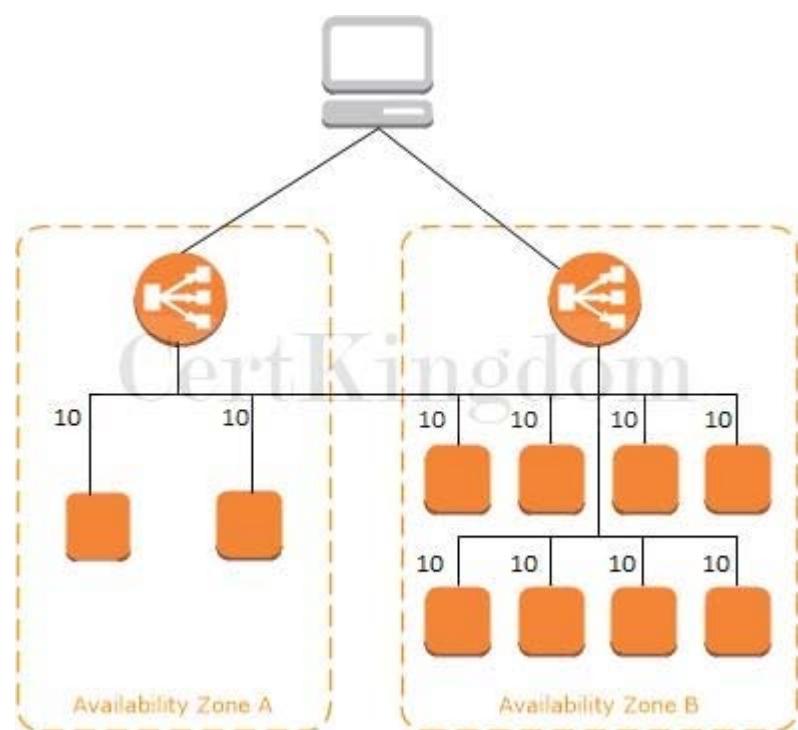
Answer: B

Explanation:

The nodes for your load balancer distribute requests from clients to registered targets. When cross-zone load balancing is enabled, each load balancer node distributes traffic across the registered targets in all enabled Availability Zones. When cross-zone load balancing is disabled, each load balancer node distributes traffic only across the registered targets in its Availability Zone.

The following diagrams demonstrate the effect of cross-zone load balancing. There are two enabled Availability Zones, with two targets in Availability Zone A and eight targets in Availability Zone B. Clients send requests, and Amazon Route 53 responds to each request with the IP address of one of the load balancer nodes. This distributes traffic such that each load balancer node receives 50% of the traffic from the clients. Each load balancer node distributes its share of the traffic across the registered targets in its scope.

If cross-zone load balancing is enabled, each of the 10 targets receives 10% of the traffic. This is because each load balancer node can route 50% of the client traffic to all 10 targets.

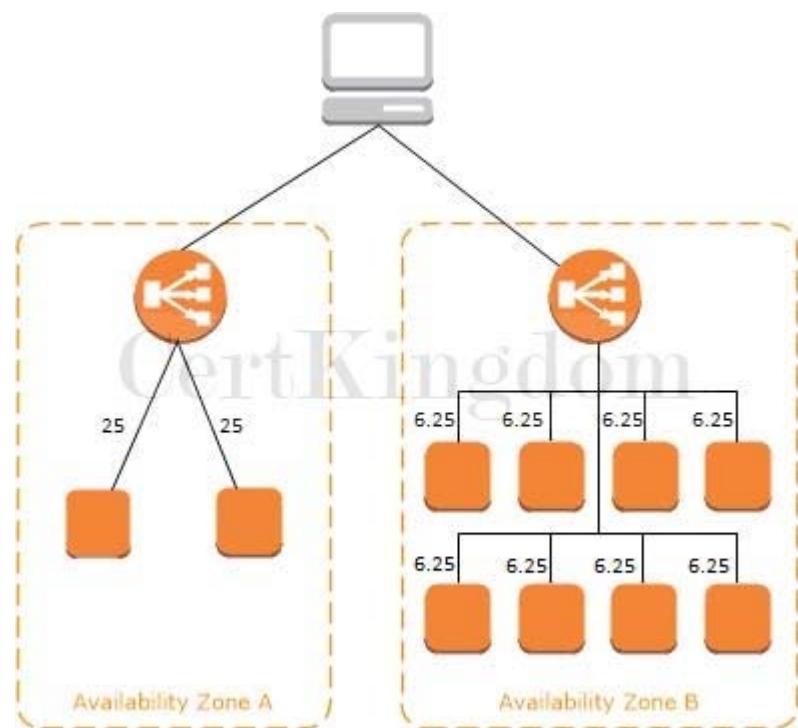


If cross-zone load balancing is disabled:

Each of the two targets in Availability Zone A receives 25% of the traffic.

Each of the eight targets in Availability Zone B receives 6.25% of the traffic.

This is because each load balancer node can route 50% of the client traffic only to targets in its Availability Zone.



With Application Load Balancers, cross-zone load balancing is always enabled. With Network Load Balancers and Gateway Load Balancers, cross-zone load balancing is disabled by default. After you create the load balancer, you can enable or disable cross-zone load balancing at any time.

When you create a Classic Load Balancer, the default for cross-zone load balancing depends on how you create the load balancer. With the API or CLI, cross-zone load balancing is disabled by default. With the AWS Management Console, the option to enable cross-zone load balancing is selected by default.

After you create a Classic Load Balancer, you can enable or disable cross-zone load balancing at any time. Hence, the right answer is to enable cross-zone load balancing.

Amazon VPC IP Address Manager (IPAM) is incorrect because this is merely a feature in Amazon VPC that provides network administrators with an automated IP management workflow. It does not enable your load balancers to distribute incoming requests evenly to all EC2 instances across multiple Availability Zones.

Path-based Routing is incorrect because this feature is based on the paths that are in the URL of the request. It automatically routes traffic to a particular target group based on the request URL. This feature will not set each of the load balancer nodes to distribute traffic across the registered targets in all enabled Availability Zones.

AWS Direct Connect SiteLink is incorrect because this is a feature of AWS Direct Connect connection and not of Amazon Elastic Load Balancing. The AWS Direct Connect SiteLink feature simply lets you create connections between your on-premises networks through the AWS global network backbone.

References:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html>

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

<https://aws.amazon.com/blogs/aws/network-address-management-and-auditing-at-scale-with-amazon-vpc-ip-address-manager/>

AWS Elastic Load Balancing Overview:

<https://youtu.be/UB15dw59DO8>

Check out this AWS Elastic Load Balancing (ELB) Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

---

## QUESTION 365

A Solutions Architect designed a real-time data analytics system based on Kinesis Data Stream and Lambda. A week after the system has been deployed, the users noticed that it performed slowly as the data rate increases. The Architect identified that the performance of the Kinesis Data Streams is causing this problem.

Which of the following should the Architect do to improve performance?

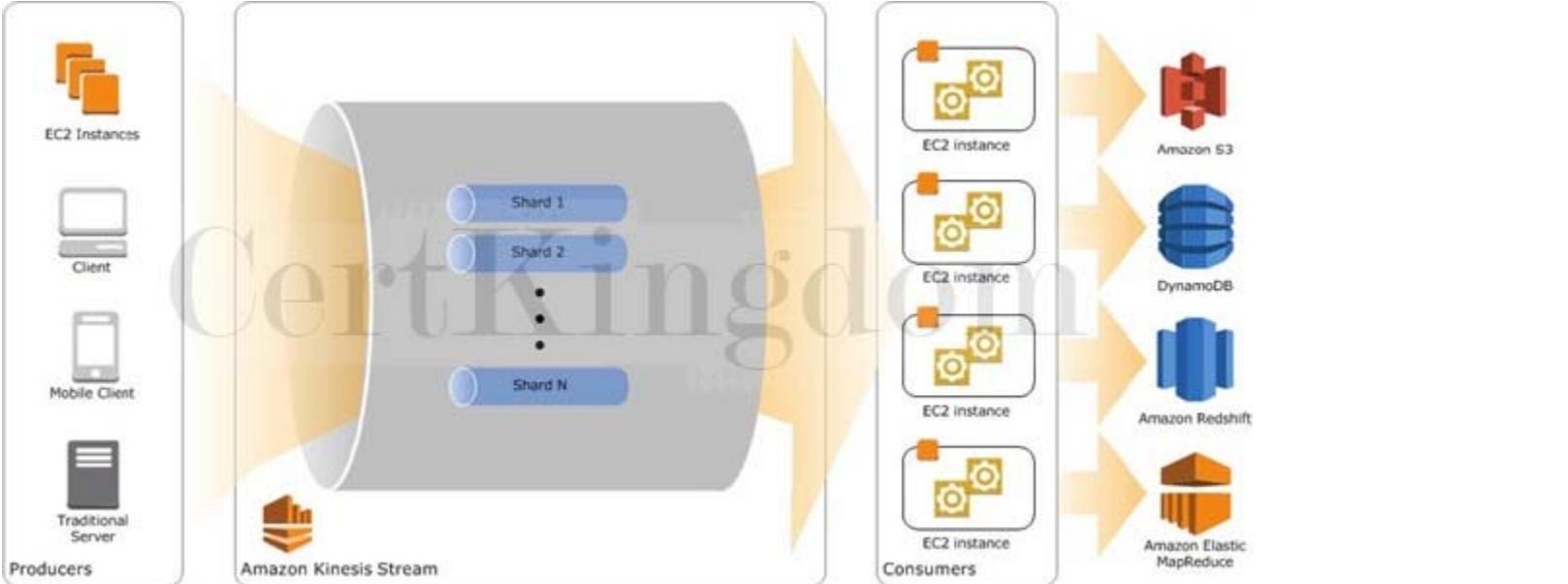
- A. Improve the performance of the stream by decreasing the number of its shards using the MergeShard command.
- B. Increase the number of shards of the Kinesis stream by using the UpdateShardCount command.
- C. Implement Step Scaling to the Kinesis Data Stream.
- D. Replace the data stream with Amazon Kinesis Data Firehose instead.

Answer: B

Explanation:

Amazon Kinesis Data Streams supports resharding, which lets you adjust the number of shards in your stream to adapt to changes in the rate of data flow through the stream. Resharding is considered an advanced operation.

There are two types of resharding operations: shard split and shard merge. In a shard split, you divide a single shard into two shards. In a shard merge, you combine two shards into a single shard. Resharding is always pairwise in the sense that you cannot split into more than two shards in a single operation, and you cannot merge more than two shards in a single operation. The shard or pair of shards that the resharding operation acts on are referred to as parent shards. The shard or pair of shards that result from the resharding operation are referred to as child shards.



Splitting increases the number of shards in your stream and therefore increases the data capacity of the stream. Because you are charged on a per-shard basis, splitting increases the cost of your stream.

Similarly, merging reduces the number of shards in your stream and therefore decreases the data capacity and cost of the stream.

If your data rate increases, you can also increase the number of shards allocated to your stream to maintain the application performance. You can reshuffle your stream using the UpdateShardCount API.

The throughput of an Amazon Kinesis data stream is designed to scale without limits via increasing the number of shards within a data stream. Hence, the correct answer is to increase the number of shards of the Kinesis stream by using the UpdateShardCount command.

Replacing the data stream with Amazon Kinesis Data Firehose instead is incorrect because the throughput of Kinesis Firehose is not exceptionally higher than Kinesis Data Streams. In fact, the throughput of an Amazon Kinesis data stream is designed to scale without limits via increasing the number of shards within a data stream.

Improving the performance of the stream by decreasing the number of its shards using the MergeShard command is incorrect because merging the shards will effectively decrease the performance of the stream rather than improve it.

Implementing Step Scaling to the Kinesis Data Stream is incorrect because there is no Step Scaling feature for Kinesis Data Streams. This is only applicable for EC2.

#### References:

<https://aws.amazon.com/blogs/big-data/scale-your-amazon-kinesis-stream-capacity-with-updateshardcount/>

<https://aws.amazon.com/kinesis/data-streams/faqs/>

<https://docs.aws.amazon.com/streams/latest/dev/kinesis-using-sdk-java-resharding.html>

Check out this Amazon Kinesis Cheat Sheet:

<https://tutorialsdojo.com/amazon-kinesis/>

## QUESTION 366

A company has a VPC for its Human Resource department and another VPC located in different AWS regions for its Finance department. The Solutions Architect must redesign the architecture to allow the finance department to access all resources that are in the human resource department, and vice versa.

An Intrusion Prevention System (IPS) must also be integrated for active traffic flow inspection and to block any vulnerability exploits.

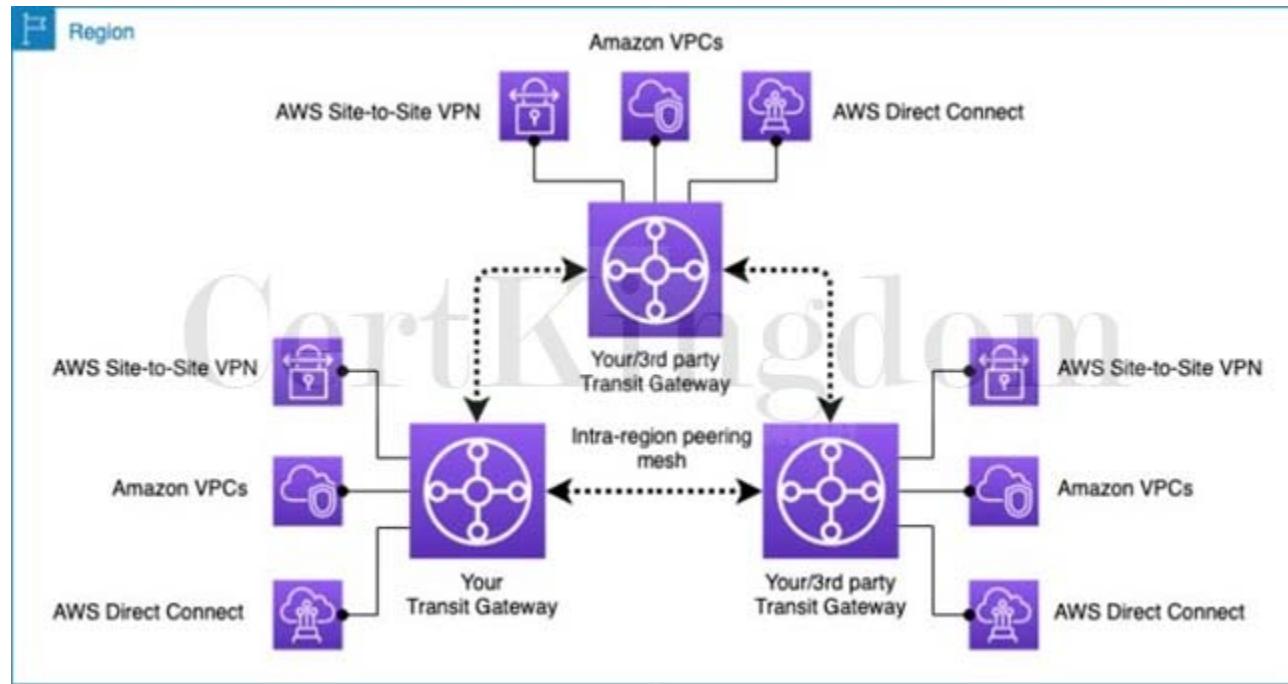
Which network architecture design in AWS should the Solutions Architect set up to satisfy the above requirement?

- Establish a secure connection between the two VPCs using a NAT Gateway. Manage user sessions via the AWS Systems Manager Session Manager service.
- Create a Traffic Policy in Amazon Route 53 to connect the two VPCs. Configure the Route 53 Resolver DNS Firewall to do active traffic flow inspection and block any vulnerability exploits.
- Create a Direct Connect Gateway and add VPC attachments to connect all departments. Configure AWS Security Hub to secure the application traffic travelling between the VPCs.
- Launch an AWS Transit Gateway and add VPC attachments to connect all departments. Set up AWS Network Firewall to secure the application traffic travelling between the VPCs.

Answer: D

Explanation:

A transit gateway is a network transit hub that you can use to interconnect your virtual private clouds (VPCs) and on-premises networks. As your cloud infrastructure expands globally, inter-Region peering connects transit gateways together using the AWS Global Infrastructure. Your data is automatically encrypted and never travels over the public internet.



A transit gateway attachment is both a source and a destination of packets. You can attach the following resources to your transit gateway:

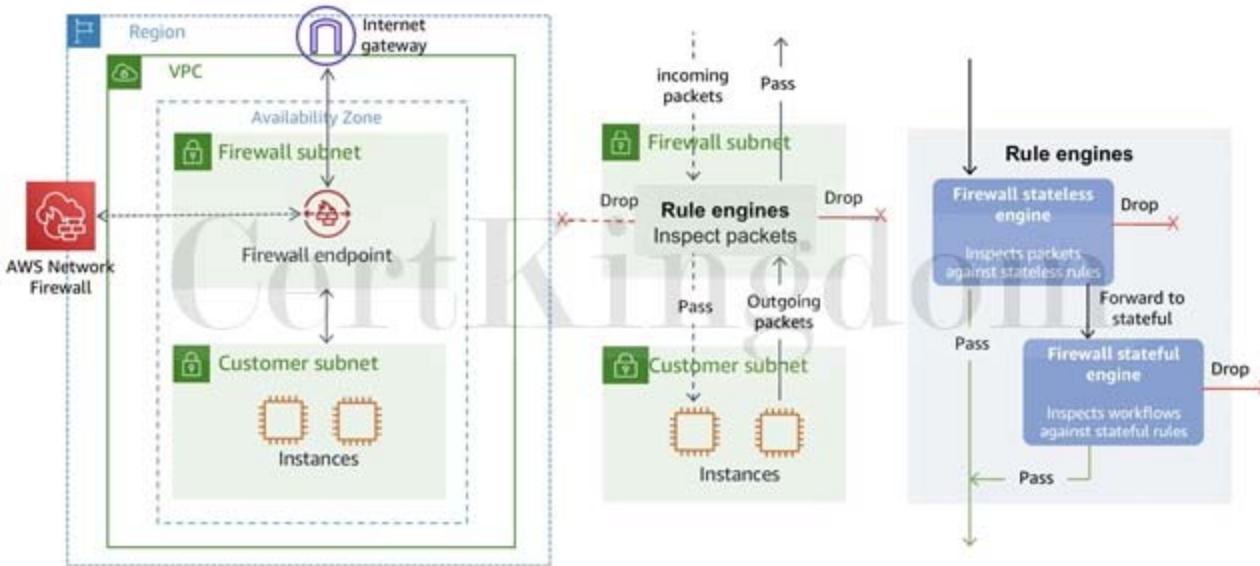
- One or more VPCs.
- One or more VPN connections
- One or more AWS Direct Connect gateways
- One or more Transit Gateway Connect attachments
- One or more transit gateway peering connections

AWS Transit Gateway deploys an elastic network interface within VPC subnets, which is then used by the transit gateway to route traffic to and from the chosen subnets. You must have at least one subnet for each Availability Zone, which then enables traffic to reach resources in every subnet of that zone.

During attachment creation, resources within a particular Availability Zone can reach a transit gateway only if a subnet is enabled within the same zone. If a subnet route table includes a route to the transit gateway, traffic is only forwarded to the transit gateway if the transit gateway has an attachment in the subnet of the same Availability Zone.

Intra-region peering connections are supported. You can have different transit gateways in different Regions.

AWS Network Firewall is a managed service that makes it easy to deploy essential network protections for all of your Amazon Virtual Private Clouds (VPCs). The service can be setup with just a few clicks and scales automatically with your network traffic, so you don't have to worry about deploying and managing any infrastructure. AWS Network Firewall's flexible rules engine lets you define firewall rules that give you fine-grained control over network traffic, such as blocking outbound Server Message Block (SMB) requests to prevent the spread of malicious activity.



AWS Network Firewall includes features that provide protections from common network threats. AWS Network Firewall's stateful firewall can incorporate context from traffic flows, like tracking connections and protocol identification, to enforce policies such as preventing your VPCs from accessing domains using an unauthorized protocol. AWS Network Firewall's intrusion prevention system (IPS) provides active traffic flow inspection so you can identify and block vulnerability exploits using signature-based detection. AWS Network Firewall also offers web filtering that can stop traffic to known bad URLs and monitor fully qualified domain names.

Hence, the correct answer is: Launch a Transit Gateway and add VPC attachments to connect all departments. Set up AWS Network Firewall to secure the application traffic travelling between the VPCs.

The option that says: Create a Traffic Policy in Amazon Route 53 to connect the two VPCs. Configure the Route 53 Resolver DNS Firewall to do active traffic flow inspection and block any vulnerability exploits is incorrect because the Traffic Policy feature is commonly used in tandem with the geoproximity routing policy for creating and maintaining records in large and complex configurations. Moreover, the Route 53 Resolver DNS Firewall can only filter and regulate outbound DNS traffic for your virtual private cloud (VPC). It can neither do active traffic flow inspection nor block any vulnerability exploits.

The option that says: Establish a secure connection between the two VPCs using a NAT Gateway. Manage user sessions via the AWS Systems Manager Session Manager service is incorrect because a NAT Gateway is simply a Network Address Translation (NAT) service and can't be used to connect two VPCs in different AWS regions. This service allows your instances in a private subnet to connect to services outside your VPC but external services cannot initiate a connection with those instances.

Furthermore, the AWS Systems Manager Session Manager service is meant for managing EC2 instances via remote SSH or PowerShell access. This is not used for managing user sessions.

The option that says: Create a Direct Connect Gateway and add VPC attachments to connect all departments. Configure AWS Security Hub to secure the application traffic travelling between the VPCs is incorrect. An AWS Direct Connect gateway is meant to be used in conjunction with an AWS Direct Connect connection to your on-premises network to connect with a Transit Gateway or a Virtual Private Gateway. You still need a Transit Gateway to connect the two VPCs that are in different AWS Regions.

The AWS Security Hub is simply a cloud security posture management service that automates best practice checks, aggregates alerts, and supports automated remediation. It's important to note that it doesn't secure application traffic just by itself.

#### References:

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>

<https://aws.amazon.com/transit-gateway>

<https://aws.amazon.com/network-firewall>

Check out these Amazon VPC and VPC Peering Cheat Sheets:

<https://tutorialsdojo.com/amazon-vpc/>

<https://tutorialsdojo.com/vpc-peering/>

## QUESTION 367

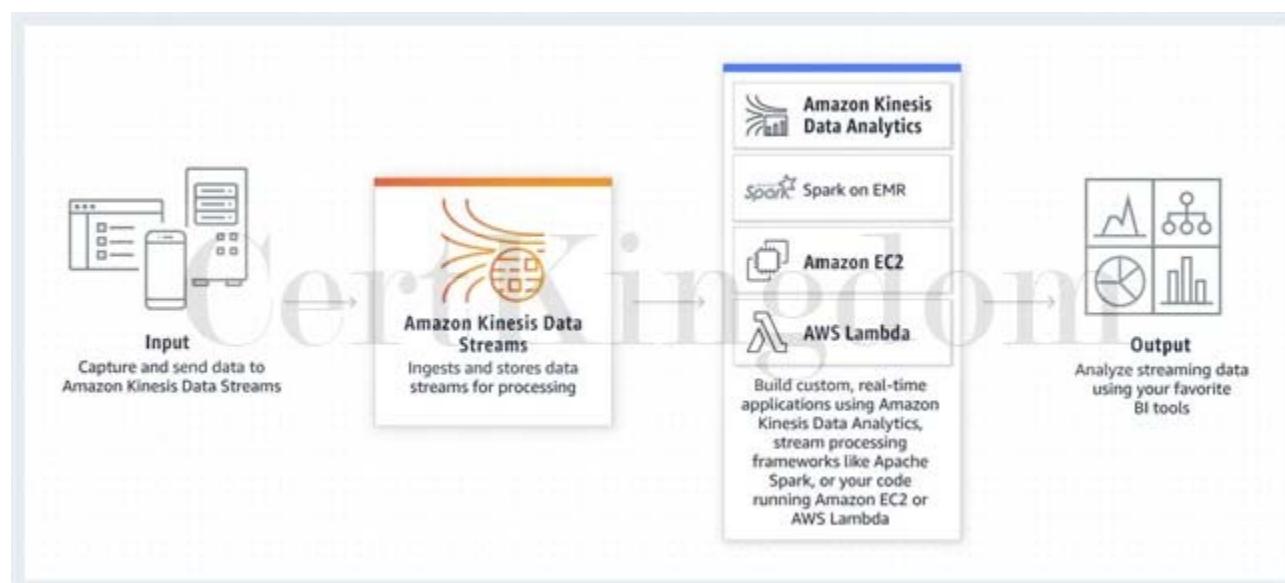
A manufacturing company launched a new type of IoT sensor. The sensor will be used to collect large streams of data records. You need to create a solution that can ingest and analyze the data in real-time with millisecond response times. Which of the following is the best option that you should implement in this scenario?

- A. Ingest the data using Amazon Simple Queue Service and create an AWS Lambda function to store the data in Amazon Redshift.
- B. Ingest the data using Amazon Kinesis Data Streams and create an AWS Lambda function to store the data in Amazon Redshift.
- C. Ingest the data using Amazon Kinesis Data Firehose and create an AWS Lambda function to store the data in Amazon DynamoDB.
- D. Ingest the data using Amazon Kinesis Data Streams and create an AWS Lambda function to store the data in Amazon DynamoDB.

Answer: D

Explanation:

Amazon Kinesis Data Streams enables you to build custom applications that process or analyze streaming data for specialized needs. You can continuously add various types of data such as clickstreams, application logs, and social media to an Amazon Kinesis data stream from hundreds of thousands of sources. Within seconds, the data will be available for your Amazon Kinesis Applications to read and process from the stream.



Based on the given scenario, the key points are "ingest and analyze the data in real-time" and "millisecond response times". For the first key point and based on the given options, you can use Amazon Kinesis Data Streams because it can collect and process large streams of data records in realtime.

For the second key point, you should use Amazon DynamoDB since it supports single-digit millisecond response times at any scale.

Hence, the correct answer is: Ingest the data using Amazon Kinesis Data Streams and create an AWS Lambda function to store the data in Amazon DynamoDB.

The option that says: Ingest the data using Amazon Kinesis Data Streams and create an AWS Lambda function to store the data in Amazon Redshift is incorrect because Amazon Redshift only delivers subsecond response times. Take note that as per the scenario, the solution must have millisecond response times to meet the requirements. Amazon DynamoDB Accelerator (DAX), which is a fully managed, highly available, in-memory cache for Amazon DynamoDB, can deliver microsecond response times.

The option that says: Ingest the data using Amazon Kinesis Data Firehose and create an AWS Lambda function to store the data in Amazon DynamoDB is incorrect. Amazon Kinesis Data Firehose only supports Amazon S3, Amazon Redshift, Amazon Elasticsearch, and an HTTP endpoint as the destination.

The option that says: Ingest the data using Amazon Simple Queue Service and create an AWS Lambda function to store the data in Amazon Redshift is incorrect because Amazon SQS can't analyze data in real-time. You have to use an Amazon Kinesis Data Stream to process the data in near-real-time.

References:

<https://aws.amazon.com/kinesis/data-streams/faqs/>

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

Check out this Amazon Kinesis Cheat Sheet:

<https://tutorialsdojo.com/amazon-kinesis/>

---

### QUESTION 368

A commercial bank has designed its next-generation online banking platform to use a distributed system architecture. As their Software Architect, you have to ensure that their architecture is highly scalable, yet still cost-effective. Which of the following will provide the most suitable solution for this scenario?

- A. Launch multiple EC2 instances behind an Application Load Balancer to host your application services, and SWF which will act as a highly-scalable buffer that stores messages as they travel between distributed applications.
- B. Launch multiple EC2 instances behind an Application Load Balancer to host your application services and SNS which will act as a highly-scalable buffer that stores messages as they travel between distributed applications.
- C. Launch an Auto-Scaling group of EC2 instances to host your application services and an SQS queue. Include an Auto Scaling trigger to watch the SQS queue size which will either scale in or scale out the number of EC2 instances based on the queue.
- D. Launch multiple On-Demand EC2 instances to host your application services and an SQS queue which will act as a highly-scalable buffer that stores messages as they travel between distributed applications.

Answer: C

Explanation:

There are three main parts in a distributed messaging system: the components of your distributed system which can be hosted on EC2 instance; your queue (distributed on Amazon SQS servers); and the messages in the queue.

To improve the scalability of your distributed system, you can add Auto Scaling group to your EC2 instances.

References:

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

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

Check out this AWS Auto Scaling Cheat Sheet:

<https://tutorialsdojo.com/aws-auto-scaling/>

---

### QUESTION 369

A company launched a cryptocurrency mining server on a Reserved EC2 instance in us-east-1 region's private subnet that uses IPv6. Due to the financial data that the server contains, the system should be secured to prevent any unauthorized access and to meet the regulatory compliance requirements.

In this scenario, which VPC feature allows the EC2 instance to communicate to the Internet but prevents inbound traffic?

- A. NAT instances
- B. Internet Gateway
- C. Egress-only Internet gateway
- D. NAT Gateway

Answer: C

Explanation:

An egress-only Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows outbound communication over IPv6 from instances in your VPC to the Internet, and prevents the Internet from initiating an IPv6 connection with your instances.

Take note that an egress-only Internet gateway is for use with IPv6 traffic only. To enable outbound-only Internet communication over IPv4, use a NAT gateway instead.

## Create egress only internet gateway Info

An Internet Gateway is a virtual router that connects a VPC to the internet.

### Egress only internet gateway settings

#### Name - optional

Creates a tag with a key of 'Name' and a value that you specify:

tutorialsdojo-egress-only-gateway

#### VPC

Attach the egress only internet gateway to this VPC:

vpc-b0968fc8

#### Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

#### Key

Q Name

#### Value - optional

Q tutorialsdojo-egress-only-gateway

You can add 49 more tags.

## Create egress only internet gateway

An egress-only internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows outbound communication over IPv6 from instances in your VPC to the internet, and prevents the internet from initiating an IPv6 connection with your instances.

[Learn more](#)

[Adding an egress only internet gateway to your VPC](#)

Hence, the correct answer is: Egress-only Internet gateway.

NAT Gateway and NAT instances are incorrect because these are only applicable for IPv4 and not IPv6.

Even though these two components can enable the EC2 instance in a private subnet to communicate to the Internet and prevent inbound traffic, it is only limited to instances which are using IPv4 addresses and not IPv6. The most suitable VPC component to use is the egress-only Internet gateway.

Internet Gateway is incorrect because this is primarily used to provide Internet access to your instances in the public subnet of your VPC, and not for private subnets. However, with an Internet gateway, traffic originating from the public Internet will also be able to reach your instances. The scenario is asking you to prevent inbound access, so this is not the correct answer.

Reference:

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

Amazon VPC Overview:

<https://www.youtube.com/watch?v=oIDHKeNxvQQ>

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

## QUESTION 370

A Solutions Architect created a brand new IAM User with a default setting using AWS CLI. This is intended to be used to send API requests to Amazon S3, DynamoDB, Lambda, and other AWS resources of the company's cloud infrastructure. Which of the following must be done to allow the user to make API calls to the AWS resources?

- A. Create a set of Access Keys for the user and attach the necessary permissions.
- B. Do nothing as the IAM User is already capable of sending API calls to your AWS resources.
- C. Enable Multi-Factor Authentication for the user.
- D. Assign an IAM Policy to the user to allow it to send API calls.

Answer: A

Explanation:

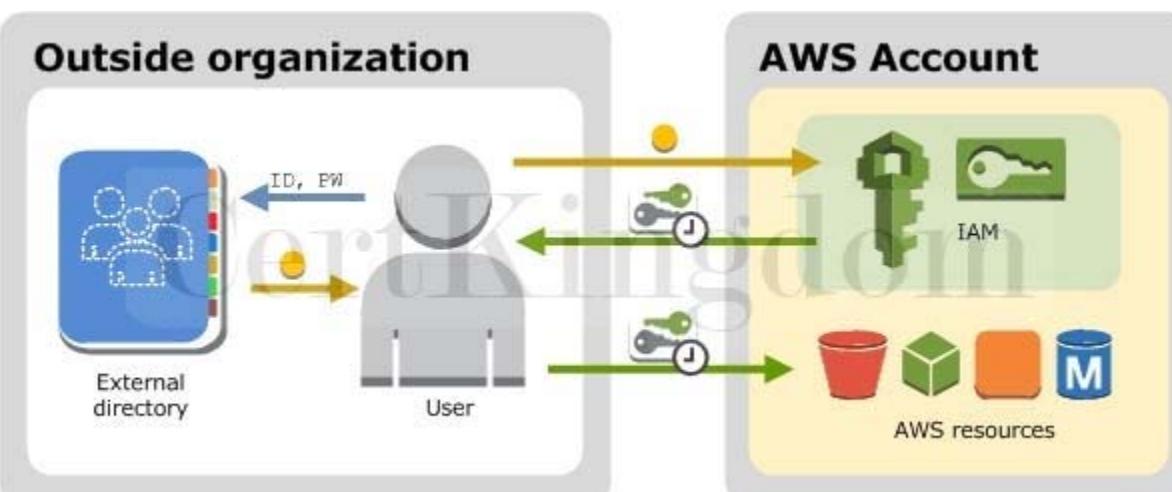
You can choose the credentials that are right for your IAM user. When you use the AWS Management Console to create a user, you must choose to at least include a console password or access keys. By default, a brand new IAM user created using

the AWS CLI or AWS API has no credentials of any kind. You must create the type of credentials for an IAM user based on the needs of your user.

Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK). Users need their own access keys to make programmatic calls to AWS from the AWS Command

Line Interface (AWS CLI), Tools for Windows PowerShell, the AWS SDKs, or direct HTTP calls using the APIs for individual AWS services.

To fill this need, you can create, modify, view, or rotate access keys (access key IDs and secret access keys) for IAM users. When you create an access key, IAM returns the access key ID and secret access key. You should save these in a secure location and give them to the user.



The option that says: Do nothing as the IAM User is already capable of sending API calls to your AWS resources is incorrect because by default, a brand new IAM user created using the AWS CLI or AWS API has no credentials of any kind. Take note that in the scenario, you created the new IAM user using the AWS CLI and not via the AWS Management Console, where you must choose to at least include a console password or access keys when creating a new IAM user. Enabling Multi-Factor Authentication for the user is incorrect because this will still not provide the required Access Keys needed to send API calls to your AWS resources. You have to grant the IAM user with Access Keys to meet the requirement.

Assigning an IAM Policy to the user to allow it to send API calls is incorrect because adding a new IAM policy to the new user will not grant the needed Access Keys needed to make API calls to the AWS resources.

References:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_access-keys.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html)

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_users.html#id\\_users\\_creds](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html#id_users_creds)

Check out this AWS IAM Cheat Sheet:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

## QUESTION 371

A company is using Amazon S3 to store frequently accessed data. The S3 bucket is shared with external users that will upload files regularly. A Solutions Architect needs to implement a solution that will grant the bucket owner full access to all uploaded objects in the S3 bucket.

What action should be done to achieve this task?

- A. Enable server access logging and set up an IAM policy that will require the users to set the object's ACL to bucket-owner-full-control.
- B. Create a bucket policy that will require the users to set the object's ACL to bucket-owner-full-control.
- C. Create a CORS configuration in the S3 bucket.
- D. Enable the Requester Pays feature in the Amazon S3 bucket.

Answer: 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.



#### Amazon S3 Access Points

Create Access Points for each application and/or user that requires access to objects in your new or existing bucket

#### Configure S3 Access Points

Configure permissions per Access Point to limit public access, and restrict access by object prefixes, and object tags

#### Limit Access to VPC

You can create Access Points that limit all S3 storage access to a Virtual Private Cloud (VPC)

#### Easily scale your access

Access Points are easy to scale as you build more applications for your large shared data sets

By default, an S3 object is owned by the AWS account that uploaded it even though the bucket is owned by another account. To get full access to the object, the object owner must explicitly grant the bucket owner access. You can create a bucket policy to require external users to grant bucket-owner-full-control when uploading objects so the bucket owner can have full access to the objects.

Hence, the correct answer is: Create a bucket policy that will require the users to set the object's ACL to bucket-owner-full-control.

The option that says: Enable the Requester Pays feature in the Amazon S3 bucket is incorrect because this option won't grant the bucket owner full access to the uploaded objects in the S3 bucket. With

Requester Pays buckets, the requester, instead of the bucket owner, pays the cost of the request and the data download from the bucket.

The option that says: Create a CORS configuration in the S3 bucket is incorrect because this option only allows cross-origin access to your Amazon S3 resources. If you need to grant the bucket owner full control in the uploaded objects, you must create a bucket policy and require external users to grant bucket-owner-full-control when uploading objects.

The option that says: Enable server access logging and set up an IAM policy that will require the users to set the bucket's ACL to bucket-owner-full-control is incorrect because this option only provides detailed records for the requests that are made to a bucket. In addition, the bucket-owner-full-control canned ACL must be associated with the bucket policy and not to an IAM policy. This will require the users to set the object's ACL (not the bucket's) to bucket-owner-full-control.

References:

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

<https://aws.amazon.com/premiumsupport/knowledge-center/s3-require-object-ownership/>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

## QUESTION 372

A cryptocurrency company wants to go global with its international money transfer app. Your project is to make sure that the database of the app is highly available in multiple regions.

What are the benefits of adding Multi-AZ deployments in Amazon RDS? (Select TWO.)

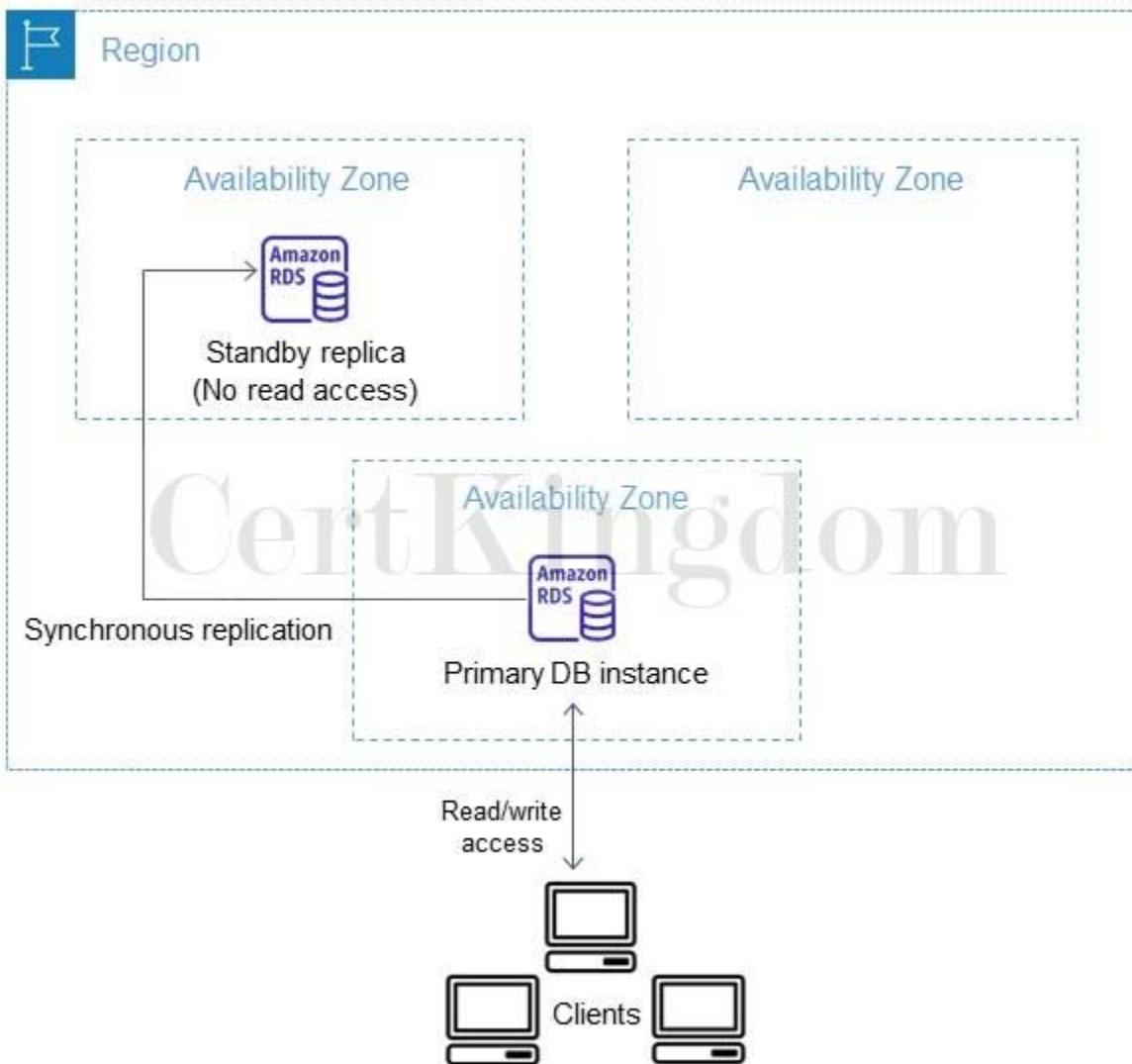
- A. Increased database availability in the case of system upgrades like OS patching or DB Instance scaling.
- B. Provides enhanced database durability in the event of a DB instance component failure or an Availability Zone outage.
- C. Provides SQL optimization.
- D. Significantly increases the database performance.
- E. Creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ) in a different region.

Answer: A,B

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.



The chief benefits of running your DB instance as a Multi-AZ deployment are enhanced database durability and availability. The increased availability and fault tolerance offered by Multi-AZ deployments make them a natural fit for production environments.

Hence, the correct answers are the following options:

- Increased database availability in the case of system upgrades like OS patching or DB Instance scaling.
- Provides enhanced database durability in the event of a DB instance component failure or an Availability Zone outage.

The option that says: Creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ) in a different region is almost correct. RDS synchronously replicates the data to a standby instance in a different Availability Zone (AZ) that is in the same region and not in a different one.

The options that say: Significantly increases the database performance and Provides SQL optimization are incorrect as it does not affect the performance nor provide SQL optimization.

References:

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

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

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

## QUESTION 373

A company deployed a web application that stores static assets in an Amazon Simple Storage Service (S3) bucket. The Solutions Architect expects the S3 bucket to immediately receive over 2000 PUT requests and 3500 GET requests per second at peak hour.

What should the Solutions Architect do to ensure optimal performance?

- A. Do nothing. Amazon S3 will automatically manage performance at this scale.
- B. Use a predictable naming scheme in the key names such as sequential numbers or date time sequences.
- C. Add a random prefix to the key names.
- D. Use Byte-Range Fetches to retrieve multiple ranges of an object data per GET request.

Answer: A

Explanation:

Amazon S3 now provides increased performance to support at least 3,500 requests per second to add data and 5,500 requests per second to retrieve data, which can save significant processing time for no additional charge. Each S3 prefix can support these request rates, making it simple to increase performance significantly.

Applications running on Amazon S3 today will enjoy this performance improvement with no changes, and customers building new applications on S3 do not have to make any application customizations to achieve this performance. Amazon S3's support for parallel requests means you can scale your S3 performance by the factor of your compute cluster, without making any customizations to your application. Performance scales per prefix, so you can use as many prefixes as you need in parallel to achieve the required throughput. There are no limits to the number of prefixes.



This S3 request rate performance increase removes any previous guidance to randomize object prefixes to achieve faster performance. That means you can now use logical or sequential naming patterns in S3 object naming without any performance implications. This improvement is now available in all AWS Regions.

Using Byte-Range Fetches to retrieve multiple ranges of an object data per GET request is incorrect because although a Byte-Range Fetch helps you achieve higher aggregate throughput, Amazon S3 does not support retrieving multiple ranges of data per GET request. Using the Range HTTP header in a GET Object request, you can fetch a byte-range from an object, transferring only the specified portion.

You can use concurrent connections to Amazon S3 to fetch different byte ranges from within the same object. Fetching smaller ranges of a large object also allows your application to improve retry times when requests are interrupted.

Adding a random prefix to the key names is incorrect. Adding a random prefix is not required in this scenario because S3 can now scale automatically to adjust performance. You do not need to add a random prefix anymore for this purpose since S3 has increased performance to support at least 3,500 requests per second to add data and 5,500 requests per second to retrieve data, which covers the workload in the scenario.

Using a predictable naming scheme in the key names such as sequential numbers or date time sequences is incorrect because Amazon S3 already maintains an index of object key names in each AWS region. S3 stores key names in alphabetical order.

The key name dictates which partition the key is stored in. Using a sequential prefix increases the likelihood that Amazon S3 will target a specific partition for a large number of your keys, overwhelming the I/O capacity of the partition.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/request-rate-perf-considerations.html>

<https://d1.awsstatic.com/whitepapers/AmazonS3BestPractices.pdf>

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

---

### QUESTION 374

An On-Demand EC2 instance is launched into a VPC subnet with the Network ACL configured to allow all inbound traffic and deny all outbound traffic. The instance's security group has an inbound rule to allow SSH from any IP address and does not have any outbound rules.

In this scenario, what are the changes needed to allow SSH connection to the instance?

- A. The network ACL needs to be modified to allow outbound traffic.
- B. Both the outbound security group and outbound network ACL need to be modified to allow outbound traffic.
- C. No action needed. It can already be accessed from any IP address using SSH.
- D. The outbound security group needs to be modified to allow outbound traffic.

Answer: A

Explanation:

In order for you to establish an SSH connection from your home computer to your EC2 instance, you need to do the following:

- On the Security Group, add an Inbound Rule to allow SSH traffic to your EC2 instance.
- On the NACL, add both an Inbound and Outbound Rule to allow SSH traffic to your EC2 instance.

The reason why you have to add both Inbound and Outbound SSH rule is due to the fact that Network ACLs are stateless which means that responses to allow inbound traffic are subject to the rules for outbound traffic (and vice versa). In other words, if you only enabled an Inbound rule in NACL, the traffic can only go in but the SSH response will not go out since there is no Outbound rule. Security groups are stateful which means that if an incoming request is granted, then the outgoing traffic will be automatically granted as well, regardless of the outbound rules.

References:

[https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_ACLs.html](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html)

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html>

---

### QUESTION 375

A multimedia company needs to deploy web services to an AWS region that they have never used before. The company currently has an IAM role for its Amazon EC2 instance that permits the instance to access Amazon DynamoDB. They want their EC2 instances in the new region to have the exact same privileges.

What should be done to accomplish this?

- A. Duplicate the IAM role and associated policies to the new region and attach it to the instances.
- B. In the new Region, create a new IAM role and associated policies then assign it to the new instance.
- C. Create an Amazon Machine Image (AMI) of the instance and copy it to the new region.
- D. Assign the existing IAM role to instances in the new region.

Answer: D

Explanation:

In this scenario, the company has an existing IAM role hence you don't need to create a new one. IAM roles are global services that are available to all regions hence, all you have to do is assign the existing IAM role to the instance in the new region.

**1**

## IAM Role

**2**

## Permissions

**Trust**  
Who can assume this role



**What you can do after assuming a role**

Defined by the role trust policy

Defined by IAM permissions policies

The option that says: In the new Region, create a new IAM role and associated policies then assign it to the new instance is incorrect because you don't need to create another IAM role - there is already an existing one.

Duplicating the IAM role and associated policies to the new region and attaching it to the instances is incorrect as you don't need duplicate IAM roles for each region. One IAM role suffices for the instances on two regions.

Creating an Amazon Machine Image (AMI) of the instance and copying it to the new region is incorrect because creating an AMI image does not affect the IAM role of the instance.

Reference:

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

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

---

### QUESTION 376

A Solutions Architect is migrating several Windows-based applications to AWS that require a scalable file system storage for high-performance computing (HPC). The storage service must have full support for the SMB protocol and Windows NTFS, Active Directory (AD) integration, and Distributed File System (DFS).

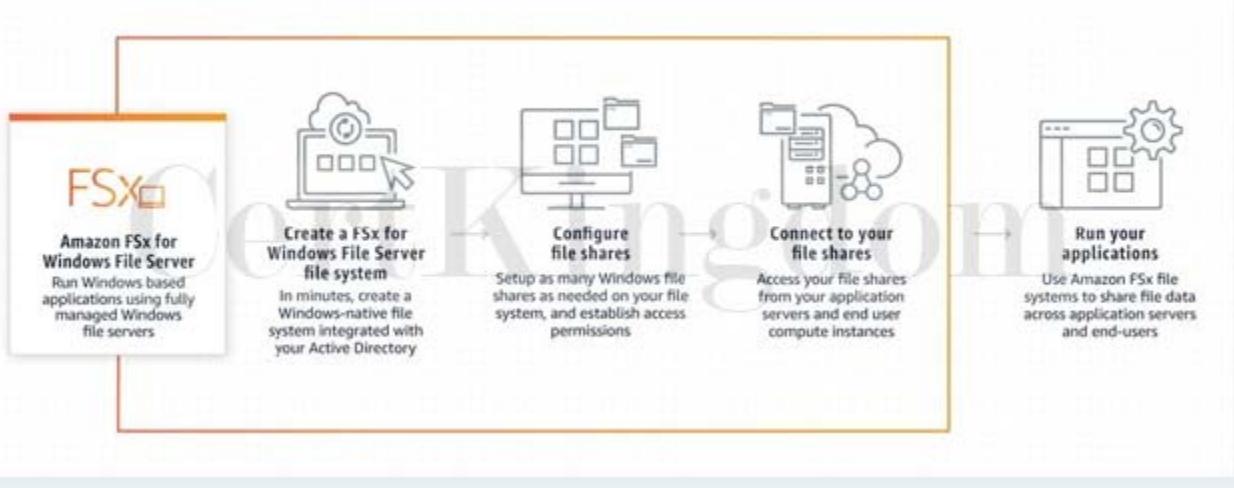
Which of the following is the MOST suitable storage service that the Architect should use to fulfill this scenario?

- A. Amazon S3 Glacier Deep Archive
- B. AWS DataSync
- C. Amazon FSx for Lustre
- D. Amazon FSx for Windows File Server

Answer: D

Explanation:

Amazon FSx provides fully managed third-party file systems. Amazon FSx provides you with the native compatibility of third-party file systems with feature sets for workloads such as Windows-based storage, high-performance computing (HPC), machine learning, and electronic design automation (EDA). You don't have to worry about managing file servers and storage, as Amazon FSx automates the timeconsuming administration tasks such as hardware provisioning, software configuration, patching, and backups. Amazon FSx integrates the file systems with cloud-native AWS services, making them even more useful for a broader set of workloads.



Amazon FSx provides you with two file systems to choose from: Amazon FSx for Windows File Server for Windows-based applications and Amazon FSx for Lustre for compute-intensive workloads.

For Windows-based applications, Amazon FSx provides fully managed Windows file servers with features and performance optimized for "lift-and-shift" business-critical application workloads including home directories (user shares), media workflows, and ERP applications. It is accessible from Windows and Linux instances via the SMB protocol. If you have Linux-based applications, Amazon EFS is a cloudnative fully managed file system that provides simple, scalable, elastic file storage accessible from Linux instances via the NFS protocol.

For compute-intensive and fast processing workloads, like high-performance computing (HPC), machine learning, EDA, and media processing, Amazon FSx for Lustre, provides a file system that's optimized for performance, with input and output stored on Amazon S3.

Hence, the correct answer is: Amazon FSx for Windows File Server.

Amazon S3 Glacier Deep Archive is incorrect because this service is primarily used as a secure, durable, and extremely low-cost cloud storage for data archiving and long-term backup.

AWS DataSync is incorrect because this service simply provides a fast way to move large amounts of data online between on-premises storage and Amazon S3 or Amazon Elastic File System (Amazon EFS).

Amazon FSx for Lustre is incorrect because this service doesn't support the Windows-based applications as well as Windows servers.

References:

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

<https://aws.amazon.com/getting-started/use-cases/hpc/>

Check out this Amazon FSx Cheat Sheet:

<https://tutorialsdojo.com/amazon-fsx/>

## QUESTION 377

A top investment bank is in the process of building a new Forex trading platform. To ensure high availability and scalability, you designed the trading platform to use an Elastic Load Balancer in front of an Auto Scaling group of On-Demand EC2 instances across multiple Availability Zones. For its database tier, you chose to use a single Amazon Aurora instance to take advantage of its distributed, fault-tolerant, and self-healing storage system.

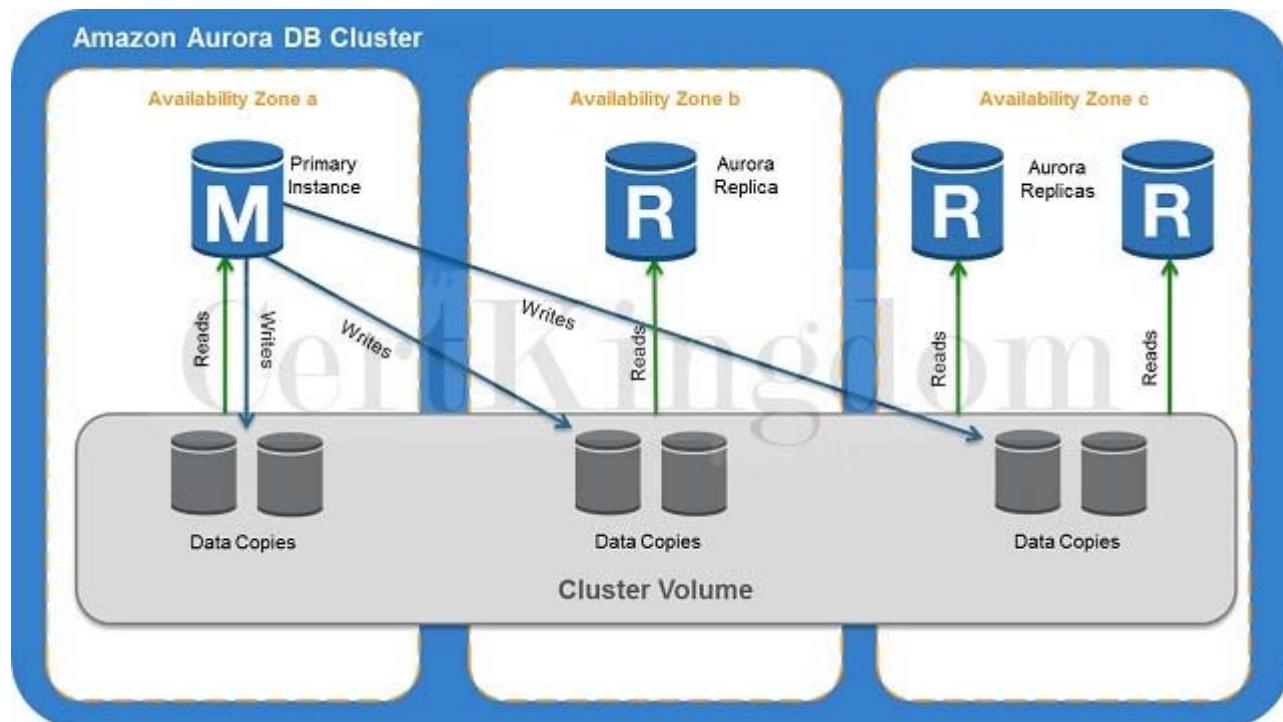
In the event of system failure on the primary database instance, what happens to Amazon Aurora during the failover?

- A. Amazon Aurora flips the A record of your DB Instance to point at the healthy replica, which in turn is promoted to become the new primary.
- B. Aurora will first attempt to create a new DB Instance in a different Availability Zone of the original instance. If unable to do so, Aurora will attempt to create a new DB Instance in the original Availability Zone in which the instance was first launched.
- C. Aurora will attempt to create a new DB Instance in the same Availability Zone as the original instance and is done on a best-effort basis.
- D. Amazon Aurora flips the canonical name record (CNAME) for your DB Instance to point at the healthy replica, which in turn is promoted to become the new primary.

Answer: C

## Explanation:

Failover is automatically handled by Amazon Aurora so that your applications can resume database operations as quickly as possible without manual administrative intervention.



If you have an Amazon Aurora Replica in the same or a different Availability Zone, when failing over, Amazon Aurora flips the canonical name record (CNAME) for your DB Instance to point at the healthy replica, which in turn is promoted to become the new primary. Start-to-finish, failover typically completes within 30 seconds.

If you are running Aurora Serverless and the DB instance or AZ become unavailable, Aurora will automatically recreate the DB instance in a different AZ.

If you do not have an Amazon Aurora Replica (i.e. single instance) and are not running Aurora Serverless, Aurora will attempt to create a new DB Instance in the same Availability Zone as the original instance. This replacement of the original instance is done on a best-effort basis and may not succeed, for example, if there is an issue that is broadly affecting the Availability Zone.

Hence, the correct answer is the option that says: Aurora will attempt to create a new DB Instance in the same Availability Zone as the original instance and is done on a best-effort basis.

The options that say: Amazon Aurora flips the canonical name record (CNAME) for your DB Instance to point at the healthy replica, which in turn is promoted to become the new primary and Amazon Aurora flips the A record of your DB Instance to point at the healthy replica, which in turn is promoted to become the new primary are incorrect because this will only happen if you are using an Amazon Aurora Replica.

In addition, Amazon Aurora flips the canonical name record (CNAME) and not the A record (IP address) of the instance. The option that says: Aurora will first attempt to create a new DB Instance in a different Availability Zone of the original instance. If unable to do so, Aurora will attempt to create a new DB Instance in the original Availability Zone in which the instance was first launched is incorrect because Aurora will first attempt to create a new DB Instance in the same Availability Zone as the original instance. If unable to do so,

Aurora will attempt to create a new DB Instance in a different Availability Zone and not the other way around.

## References:

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

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Concepts.AuroraHighAvailability.html>

## Amazon Aurora Overview:

<https://youtu.be/iwS1h7rLNQ>

Check out this Amazon Aurora Cheat Sheet:

<https://tutorialsdojo.com/amazon-aurora/>

## QUESTION 378

The start-up company that you are working for has a batch job application that is currently hosted on an EC2 instance. It is set to process messages from a queue created in SQS with default settings. You configured the application to process the messages once a week. After 2 weeks, you noticed that not all messages are being processed by the application. What is the root cause of this issue?

- A. Missing permissions in SQS.
- B. The batch job application is configured to long polling.
- C. Amazon SQS has automatically deleted the messages that have been in a queue for more than the maximum message retention period.
- D. The SQS queue is set to short-polling.

Answer: C

Explanation:

Amazon SQS automatically deletes messages that have been in a queue for more than the maximum message retention period. The default message retention period is 4 days. Since the queue is configured to the default settings and the batch job application only processes the messages once a week, the messages that are in the queue for more than 4 days are deleted. This is the root cause of the issue.

To fix this, you can increase the message retention period to a maximum of 14 days using the SetQueueAttributes action.

References:

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

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

Check out this Amazon SQS Cheat Sheet:

<https://tutorialsdojo.com/amazon-sqs/>

---

## QUESTION 379

A company has recently adopted a hybrid cloud architecture and is planning to migrate a database hosted on-premises to AWS. The database currently has over 50 TB of consumer data, handles highly transactional (OLTP) workloads, and is expected to grow. The Solutions Architect should ensure that the database is ACID-compliant and can handle complex queries of the application.

Which type of database service should the Architect use?

- A. Amazon RDS
- B. Amazon Aurora
- C. Amazon DynamoDB
- D. Amazon Redshift

Answer: B

Explanation:

Amazon Aurora (Aurora) is a fully managed relational database engine that's compatible with MySQL and PostgreSQL. You already know how MySQL and PostgreSQL combine the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases.

The code, tools, and applications you use today with your existing MySQL and PostgreSQL databases can be used with Aurora. With some workloads, Aurora can deliver up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.

Aurora includes a high-performance storage subsystem. Its MySQL- and PostgreSQL-compatible database engines are customized to take advantage of that fast distributed storage. The underlying storage grows automatically as needed, up to 64 terabytes (TiB). Aurora also automates and standardizes database clustering and replication, which are typically among the most challenging aspects of database configuration and administration.

	Relational databases	NoSQL databases
Optimal workloads	Relational databases are designed for transactional and strongly consistent online transaction processing (OLTP) applications and are good for online analytical processing (OLAP).	NoSQL key-value, document, graph, and in-memory databases are designed for OLTP for a number of data access patterns that include low-latency applications. NoSQL search databases are designed for analytics over semi-structured data.
Data model	The relational model normalizes data into tables that are composed of rows and columns. A schema strictly defines the tables, rows, columns, indexes, relationships between tables, and other database elements. The database enforces the referential integrity in relationships between tables.	NoSQL databases provide a variety of data models that includes document, graph, key-value, in-memory, and search.
ACID properties	<p>Relational databases provide atomicity, consistency, isolation, and durability (ACID) properties:</p> <ul style="list-style-type: none"> <li>Atomicity requires a transaction to execute completely or not at all.</li> <li>Consistency requires that when a transaction has been committed, the data must conform to the database schema.</li> <li>Isolation requires that concurrent transactions execute separately from each other.</li> <li>Durability requires the ability to recover from an unexpected system failure or power outage to the last known state.</li> </ul>	NoSQL databases often make tradeoffs by relaxing some of the ACID properties of relational databases for a more flexible data model that can scale horizontally. This makes NoSQL databases an excellent choice for high throughput, low-latency use cases that need to scale horizontally beyond the limitations of a single instance.
Performance	Performance is generally dependent on the disk subsystem. The optimization of queries, indexes, and table structure is often required to achieve peak performance.	Performance is generally a function of the underlying hardware cluster size, network latency, and the calling application.
Scale	Relational databases typically scale up by increasing the compute capabilities of the hardware or scale-out by adding replicas for read-only workloads.	NoSQL databases typically are partitionable because key-value access patterns are able to scale out by using distributed architecture to increase throughput that provides consistent performance at near boundless scale.
APIs	Requests to store and retrieve data are communicated using queries that conform to a structured query language (SQL). These queries are parsed and executed by the relational database.	Object-based APIs allow app developers to easily store and retrieve in-memory data structures. Partition keys let apps look up key-value pairs, column sets, or semistructured documents that contain serialized app objects and attributes.

For Amazon RDS MariaDB DB instances, the maximum provisioned storage limit constrains the size of a table to a maximum size of 64 TB when using InnoDB file-per-table tablespaces. This limit also constrains the system tablespace to a maximum size of 16 TB. InnoDB file-per-table tablespaces (with tables each in their own tablespace) is set by default for Amazon RDS MariaDB DB instances.

Hence, the correct answer is Amazon Aurora.

Amazon Redshift is incorrect because this is primarily used for OLAP applications and not for OLTP.

Moreover, it doesn't scale automatically to handle the exponential growth of the database.

Amazon DynamoDB is incorrect. Although you can use this to have an ACID-compliant database, it is not capable of handling complex queries and highly transactional (OLTP) workloads.

Amazon RDS is incorrect. Although this service can host an ACID-compliant relational database that can handle complex queries and transactional (OLTP) workloads, it is still not scalable to handle the growth of the database. Amazon Aurora is the better choice as its underlying storage can grow automatically as needed.

References:

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

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

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

Amazon Aurora Overview:

<https://youtu.be/iwS1h7rLNQ>

Check out this Amazon Aurora Cheat Sheet:

<https://tutorialsdojo.com/amazon-aurora/>

## QUESTION 380

A social media company needs to capture the detailed information of all HTTP requests that went through their public-facing Application Load Balancer every five minutes. The client's IP address and network latencies must also be tracked. They want to use this data for analyzing traffic patterns and for troubleshooting their Docker applications orchestrated by the Amazon ECS Anywhere service.

Which of the following options meets the customer requirements with the LEAST amount of overhead?

- Enable AWS CloudTrail for their Application Load Balancer. Use the AWS CloudTrail Lake to analyze and troubleshoot the application traffic.
- Enable access logs on the Application Load Balancer. Integrate the Amazon ECS cluster with Amazon CloudWatch Application Insights to analyze traffic patterns and simplify troubleshooting.

C. Install and run the AWS X-Ray daemon on the Amazon ECS cluster. Use the Amazon CloudWatch ServiceLens to analyze the traffic that goes through the application.

D. Integrate Amazon EventBridge (Amazon CloudWatch Events) metrics on the Application Load Balancer to capture the client IP address. Use Amazon CloudWatch Container Insights to analyze traffic patterns.

Answer: B

Explanation:

Amazon CloudWatch Application Insights facilitates observability for your applications and underlying AWS resources. It helps you set up the best monitors for your application resources to continuously analyze data for signs of problems with your applications. Application Insights, which is powered by SageMaker and other AWS technologies, provides automated dashboards that show potential problems with monitored applications, which help you to quickly isolate ongoing issues with your applications and infrastructure. The enhanced visibility into the health of your applications that Application Insights provides helps reduce the "mean time to repair" (MTTR) to troubleshoot your application issues.

The screenshot shows the AWS CloudWatch Application Insights console. On the left, a sidebar lists various services: Services, CloudWatch (selected), Favorites and recent, All alarms, Billing, Logs (selected), Log groups, Log Insights, Metrics, X-Ray traces, Events, Application monitoring (ServiceLens Map, Resource Health, Synthetics Canaries, Evidently, RUM), Insights (Container Insights, Lambda Insights, Contributor Insights), Application Insights (selected), Settings, and Getting Started. A green box highlights the 'Application Insights' button. The main area displays the 'tutorialsdojo-portal-dev' application summary. It includes sections for Application summary, Monitored components (2), and Unmonitored components (0). The Monitored components section lists two items: 'tutorialsdojo-rdb-database' (RDS database instance, Type: Default) and 'i-0783710fcf14820a9: DEV' (Amazon EC2 instance, Type: Default). The Unmonitored components section indicates that no components need configuration for Application Insights to begin monitoring them. A watermark for 'Tutorialspoint.com' is visible across the page.

When you add your applications to Amazon CloudWatch Application Insights, it scans the resources in the applications and recommends and configures metrics and logs on CloudWatch for application components. Example application components include SQL Server backend databases and Microsoft

IIS/Web tiers. Application Insights analyzes metric patterns using historical data to detect anomalies and continuously detects errors and exceptions from your application, operating system, and infrastructure logs. It correlates these observations using a combination of classification algorithms and built-in rules.

Then, it automatically creates dashboards that show the relevant observations and problem severity information to help you prioritize your actions.

Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues.

**ELB Access Logs**

Access logging is an optional feature of Elastic Load Balancing that is disabled by default. After you enable access logging for your load balancer, Elastic Load Balancing captures the logs and stores them in the Amazon S3 bucket that you specify as compressed files. You can disable access logging at any time.

Hence, the correct answer is: Enable access logs on the Application Load Balancer. Integrate the Amazon ECS cluster with Amazon CloudWatch Application Insights to analyze traffic patterns and simplify troubleshooting.

The option that says: Enable AWS CloudTrail for their Application Load Balancer. Use the AWS CloudTrail Lake to analyze and troubleshoot the application traffic is incorrect because AWS CloudTrail is primarily used to monitor and record the account activity across your AWS resources and not your web applications. You cannot use CloudTrail to capture the detailed information of all HTTP requests that go through your public-facing Application Load Balancer (ALB). CloudTrail can only track the resource changes made to your ALB, but not the actual IP traffic that goes through it. For this use case, you have to enable the access logs feature instead. In addition, the AWS CloudTrail Lake feature is more suitable for running SQL-based queries on your API events and not for analyzing application traffic.

The option that says: Install and run the AWS X-Ray daemon on the Amazon ECS cluster. Use the Amazon CloudWatch ServiceLens to analyze the traffic that goes through the application is incorrect.

Although this solution is possible, this won't track the client's IP address since the access log feature in the ALB is not enabled. Take note that the scenario explicitly mentioned that the client's IP address and network latencies must also be tracked.

The option that says: Integrate Amazon EventBridge (Amazon CloudWatch Events) metrics on the Application Load Balancer to capture the client IP address. Use Amazon CloudWatch Container Insights to analyze traffic patterns is incorrect because Amazon EventBridge doesn't track the actual traffic to your ALB. It is the Amazon CloudWatch service that monitors the changes to your ALB itself and the actual IP traffic that it distributes to the target groups. The primary function of CloudWatch Container

Insights is to collect, aggregate, and summarize metrics and logs from your containerized applications and microservices.

References:

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

<http://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-monitoring.html>

AWS Elastic Load Balancing Overview:

<https://youtu.be/UBL5dw59DO8>

Check out this AWS Elastic Load Balancing (ELB) Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

Application Load Balancer vs Network Load Balancer vs Gateway Load Balancer:

<https://tutorialsdojo.com/application-load-balancer-vs-network-load-balancer-vs-classic-load-balancer/>

## QUESTION 381

A company plans to deploy a Docker-based batch application in AWS. The application will be used to process both mission-critical data as well as non-essential batch jobs.

Which of the following is the most cost-effective option to use in implementing this architecture?

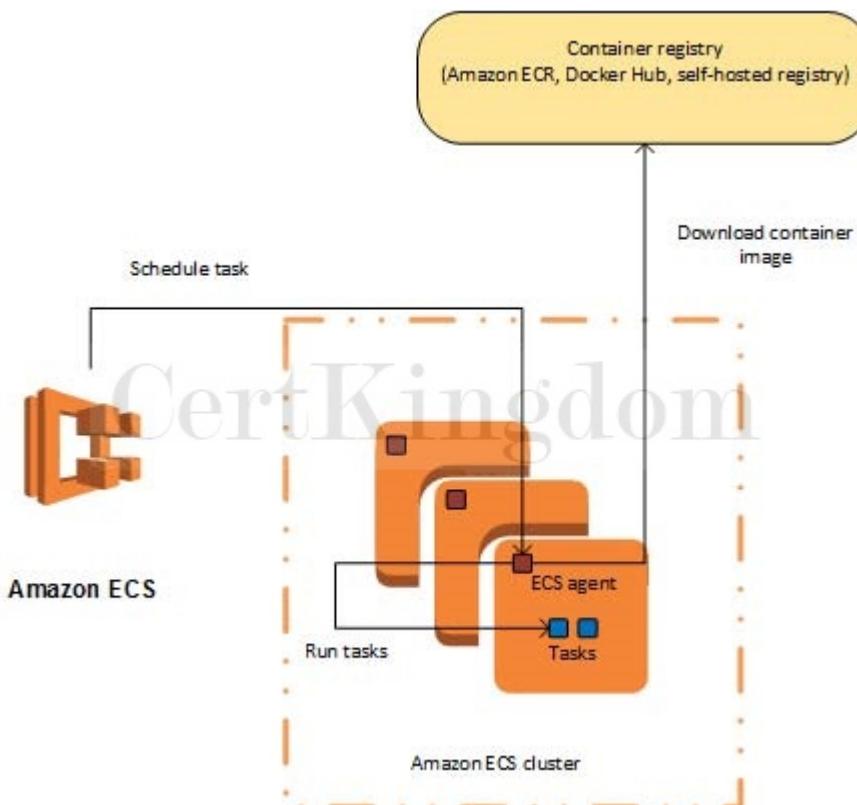
- A. Use ECS as the container management service then set up Reserved EC2 Instances for processing both mission-critical and non-essential batch jobs.
- B. Use ECS as the container management service then set up On-Demand EC2 Instances for processing both mission-critical and non-essential batch jobs.
- C. Use ECS as the container management service then set up a combination of Reserved and Spot EC2 Instances for processing mission-critical and non-essential batch jobs respectively.
- D. Use ECS as the container management service then set up Spot EC2 Instances for processing bot mission-critical and non-essential batch jobs.

Answer: C

Explanation:

Amazon ECS lets you run batch workloads with managed or custom schedulers on Amazon EC2 On- Demand Instances, Reserved Instances, or Spot Instances. You can launch a combination of EC2 instances to set up a cost-effective architecture depending on your workload. You can launch Reserved EC2 instances to process the mission-critical data and Spot EC2 instances for processing non-essential batch jobs.

There are two different charge models for Amazon Elastic Container Service (ECS): Fargate Launch Type Model and EC2 Launch Type Model. With Fargate, you pay for the amount of vCPU and memory resources that your containerized application requests while for EC2 launch type model, there is no additional charge. You pay for AWS resources (e.g. EC2 instances or EBS volumes) you create to store and run your application. You only pay for what you use, as you use it; there are no minimum fees and no upfront commitments.



In this scenario, the most cost-effective solution is to use ECS as the container management service then set up a combination of Reserved and Spot EC2 Instances for processing mission-critical and nonessential batch jobs respectively. You can use Scheduled Reserved Instances (Scheduled Instances) which enables you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. This will ensure that you have an uninterrupted compute capacity to process your mission-critical batch jobs.

Hence, the correct answer is the option that says: Use ECS as the container management service then set up a combination of

Reserved and Spot EC2 Instances for processing mission-critical and nonessential batch jobs respectively. Using ECS as the container management service then setting up Reserved EC2 Instances for processing both mission-critical and non-essential batch jobs is incorrect because processing the nonessential batch jobs can be handled much cheaper by using Spot EC2 instances instead of Reserved Instances.

Using ECS as the container management service then setting up On-Demand EC2 Instances for processing both mission-critical and non-essential batch jobs is incorrect because an On-Demand instance costs more compared to Reserved and Spot EC2 instances. Processing the non-essential batch jobs can be handled much cheaper by using Spot EC2 instances instead of On-Demand instances.

Using ECS as the container management service then setting up Spot EC2 Instances for processing both mission-critical and non-essential batch jobs is incorrect because although this set up provides the cheapest solution among other options, it will not be able to meet the required workload. Using Spot instances to process mission-critical workloads is not suitable since these types of instances can be terminated by AWS at any time, which can affect critical processing.

References:

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide>Welcome.html>

<https://aws.amazon.com/ec2/spot/containers-for-less/get-started/>

Check out this Amazon ECS Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-container-service-amazon-ecs/>

AWS Container Services Overview:

<https://www.youtube.com/watch?v=5QBgDX7O7pw>

---

## QUESTION 382

A web application hosted in an Auto Scaling group of EC2 instances in AWS. The application receives a burst of traffic every morning, and a lot of users are complaining about request timeouts. The EC2 instance takes 1 minute to boot up before it can respond to user requests. The cloud architecture must be redesigned to better respond to the changing traffic of the application.

How should the Solutions Architect redesign the architecture?

- A. Create a CloudFront distribution and set the EC2 instance as the origin.
- B. Create a step scaling policy and configure an instance warm-up time condition.
- C. Create a Network Load Balancer with slow-start mode.
- D. Create a new launch template and upgrade the size of the instance.

Answer: B

Explanation:

Amazon EC2 Auto Scaling helps you maintain application availability and allows you to automatically add or remove EC2 instances according to conditions you define. You can use the fleet management features of EC2 Auto Scaling to maintain the health and availability of your fleet. You can also use the dynamic and predictive scaling features of EC2 Auto Scaling to add or remove EC2 instances. Dynamic scaling responds to changing demand and predictive scaling automatically schedules the right number of EC2 instances based on predicted demand. Dynamic scaling and predictive scaling can be used together to scale faster.

## Create scaling policy

**Policy type**

Step scaling

**Scaling policy name**

TutorialsDojo\_Step\_Scaling\_Makati

**CloudWatch alarm**  
Choose an alarm that can scale capacity whenever:

StatusCheckFailed\_Alarm\_TutorialsDojo

Create a CloudWatch alarm 

breaches the alarm threshold: StatusCheckFailed > 50 for 1 consecutive periods of 300 seconds for the metric dimensions:

InstanceId = i-029b2f4a3e6a25eeef

**Take the action**

Add

1 Percent of group when 50 <= StatusCheckFailed < +infinity

Add step

Add capacity units in increments of at least 1 capacity units

Instances need  
300 seconds warm up before including in metric



Cancel Create

Tutorials Dojo

Step scaling applies step adjustments' which means you can set multiple actions to vary the scaling depending on the size of the alarm breach. When you create a step scaling policy, you can also specify the number of seconds that it takes for a newly launched instance to warm up.

Hence, the correct answer is: Create a step scaling policy and configure an instance warm-up time condition.

The option that says: Create a Network Load Balancer with slow start mode is incorrect because Network Load Balancer does not support slow start mode. If you need to enable slow start mode, you should use Application Load Balancer.

The option that says: Create a new launch template and upgrade the size of the instance is incorrect because a larger instance does not always improve the boot time. Instead of upgrading the instance, you should create a step scaling policy and add a warm-up time.

The option that says: Create a CloudFront distribution and set the EC2 instance as the origin is incorrect because this approach only resolves the traffic latency. Take note that the requirement in the scenario is to resolve the timeout issue and not the traffic latency.

References:

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

<https://aws.amazon.com/ec2/autoscaling/faqs/>

Check out these AWS Cheat Sheets:

<https://tutorialsdojo.com/aws-auto-scaling/>

<https://tutorialsdojo.com/step-scaling-vs-simple-scaling-policies-in-amazon-ec2/>

## QUESTION 383

A company has an infrastructure that allows EC2 instances from a private subnet to fetch objects from Amazon S3 via a NAT Instance. The company's Solutions Architect was instructed to lower down the cost incurred by the current solution. How should the Solutions Architect redesign the architecture in the most cost-efficient manner?

- A. Use a smaller instance type for the NAT instance.
- B. Replace the NAT instance with NAT Gateway to access S3 objects.
- C. Remove the NAT instance and create an S3 interface endpoint to access S3 objects.
- D. Remove the NAT instance and create an S3 gateway endpoint to access S3 objects.

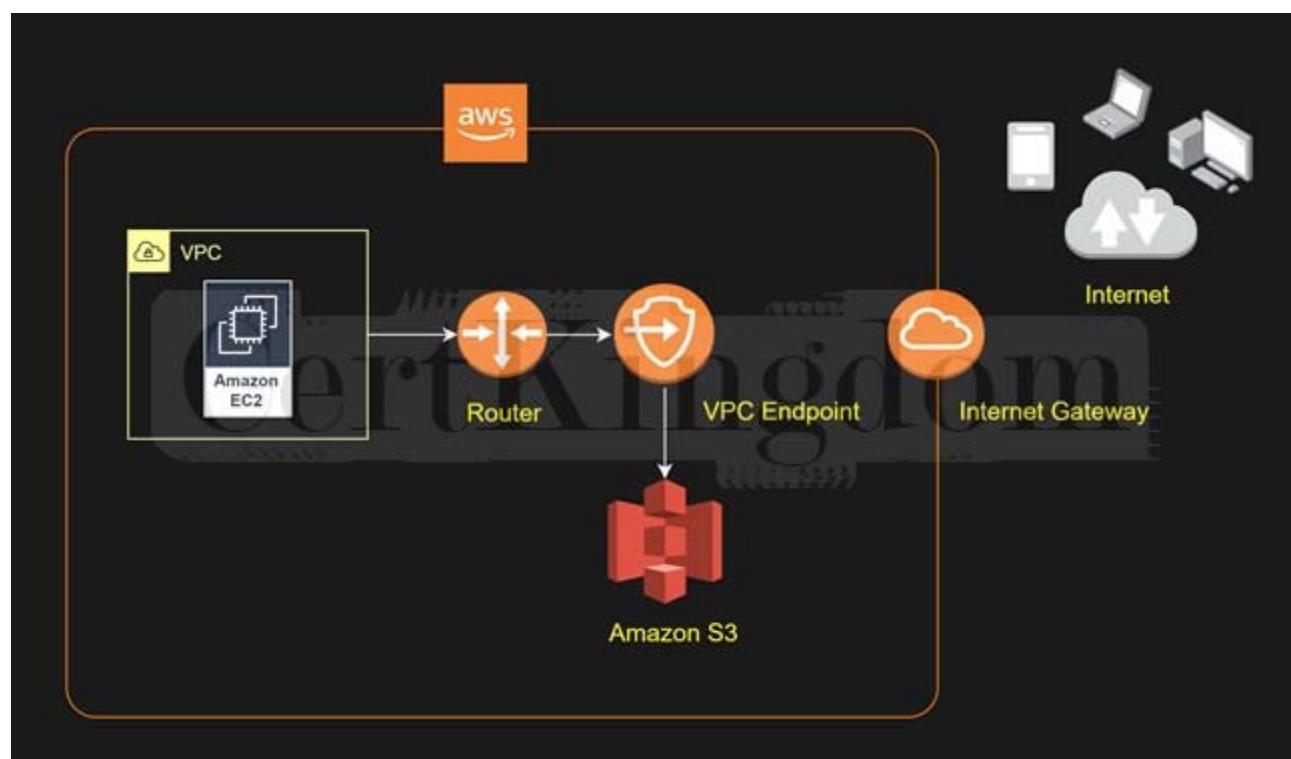
Answer: D

Explanation:

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an Internet gateway, NAT device, 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 services does not leave the Amazon network.

Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.

There are two types of VPC endpoints: interface endpoints and gateway endpoints. You should create the type of VPC endpoint required by the supported service. As a rule of thumb, most AWS services use VPC Interface Endpoint except for S3 and DynamoDB, which use VPC Gateway Endpoint.



There is no additional charge for using gateway endpoints. However, standard charges for data transfer and resource usage still apply.

Let's assume you created a NAT gateway and you have an EC2 instance routing to the Internet through the NAT gateway. Your EC2 instance behind the NAT gateway sends a 1 GB file to one of your S3 buckets. The EC2 instance, NAT gateway, and S3 Bucket are in the same region US East (Ohio), and the NAT gateway and EC2 instance are in the same availability zone.

Your cost will be calculated as follows:

- NAT Gateway Hourly Charge: NAT Gateway is charged on an hourly basis. For example, the rate is \$0.045 per hour in this region.
- NAT Gateway Data Processing Charge: 1 GB data went through NAT gateway. The NAT Gateway Data Processing charge is applied and will result in a charge of \$0.045.

- **Data Transfer Charge:** This is the standard EC2 Data Transfer charge. 1 GB data was transferred from the EC2 instance to S3 via the NAT gateway. There was no charge for the data transfer from the EC2 instance to S3 as it is Data Transfer Out to Amazon EC2 to S3 in the same region. There was also no charge for the data transfer between the NAT Gateway and the EC2 instance since the traffic stays in the same availability zone using private IP addresses. There will be a data transfer charge between your NAT Gateway and EC2 instance if they are in the different availability zone.

In summary, your charge will be \$0.045 for 1 GB of data processed by the NAT gateway and a charge of \$0.045 per hour will always apply once the NAT gateway is provisioned and available. The data transfer has no charge in this example. However, if you send the file to a non-AWS Internet location instead, there will be a data transfer charge as it is data transfer out from Amazon EC2 to the Internet.

To avoid the NAT Gateway Data Processing charge in this example, you could set up a Gateway Type VPC endpoint and route the traffic to/from S3 through the VPC endpoint instead of going through the NAT Gateway.

There is no data processing or hourly charges for using Gateway Type VPC endpoints.

Hence, the correct answer is the option that says: Remove the NAT instance and create an S3 gateway endpoint to access S3 objects.

The option that says: Replace the NAT instance with NAT Gateway to access S3 objects is incorrect. A NAT Gateway is just a NAT instance that is managed for you by AWS. It provides less operational management and you pay for the hour that your NAT Gateway is running. This is not the most effective solution since you will still pay for the idle time.

The option that says: Use a smaller instance type for the NAT instance is incorrect. Although this might reduce the cost, it still is not the most cost-efficient solution. An S3 Gateway endpoint is still the best solution because it comes with no additional charge.

The option that says: Remove the NAT instance and create an S3 interface endpoint to access S3 objects is incorrect. An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet. Unlike a Gateway endpoint, you still get billed for the time your interface endpoint is running and the GB data it has processed. From a cost standpoint, using the S3 Gateway endpoint is the most favorable solution.

References:

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

<https://aws.amazon.com/blogs/architecture/reduce-cost-and-increase-security-with-amazon-vpc-endpoints/>

<https://aws.amazon.com/vpc/pricing/>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

---

## QUESTION 384

A company needs to accelerate the performance of its AI-powered medical diagnostic application by running its machine learning workloads on the edge of telecommunication carriers' 5G networks. The application must be deployed to a Kubernetes cluster and have role-based access control (RBAC) access to IAM users and roles for cluster authentication. Which of the following should the Solutions Architect implement to ensure single-digit millisecond latency for the application?

- A. Launch the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Create node groups in Wavelength Zones for the Amazon EKS cluster via the AWS Wavelength service. Apply the AWS authenticator configuration map (aws-auth ConfigMap) to your cluster.
- B. Launch the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Create VPC endpoints for the AWS Wavelength Zones and apply them to the Amazon EKS cluster. Install the AWS IAM Authenticator for Kubernetes (aws-iam-authenticator) to your cluster.
- C. Host the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Set up node groups in AWS Wavelength Zones for the Amazon EKS cluster. Attach the Amazon EKS connector agent role (AmazonECSConnectorAgentRole) to your cluster and use AWS Control Tower for RBAC access.
- D. Host the application to an Amazon EKS cluster and run the Kubernetes pods on AWS Fargate. Create node groups in AWS Wavelength Zones for the Amazon EKS cluster. Add the EKS pod execution IAM role (AmazonEKSFargatePodExecutionRole) to your cluster and ensure that the Fargate profile has the same IAM role as your Amazon EC2 node groups.

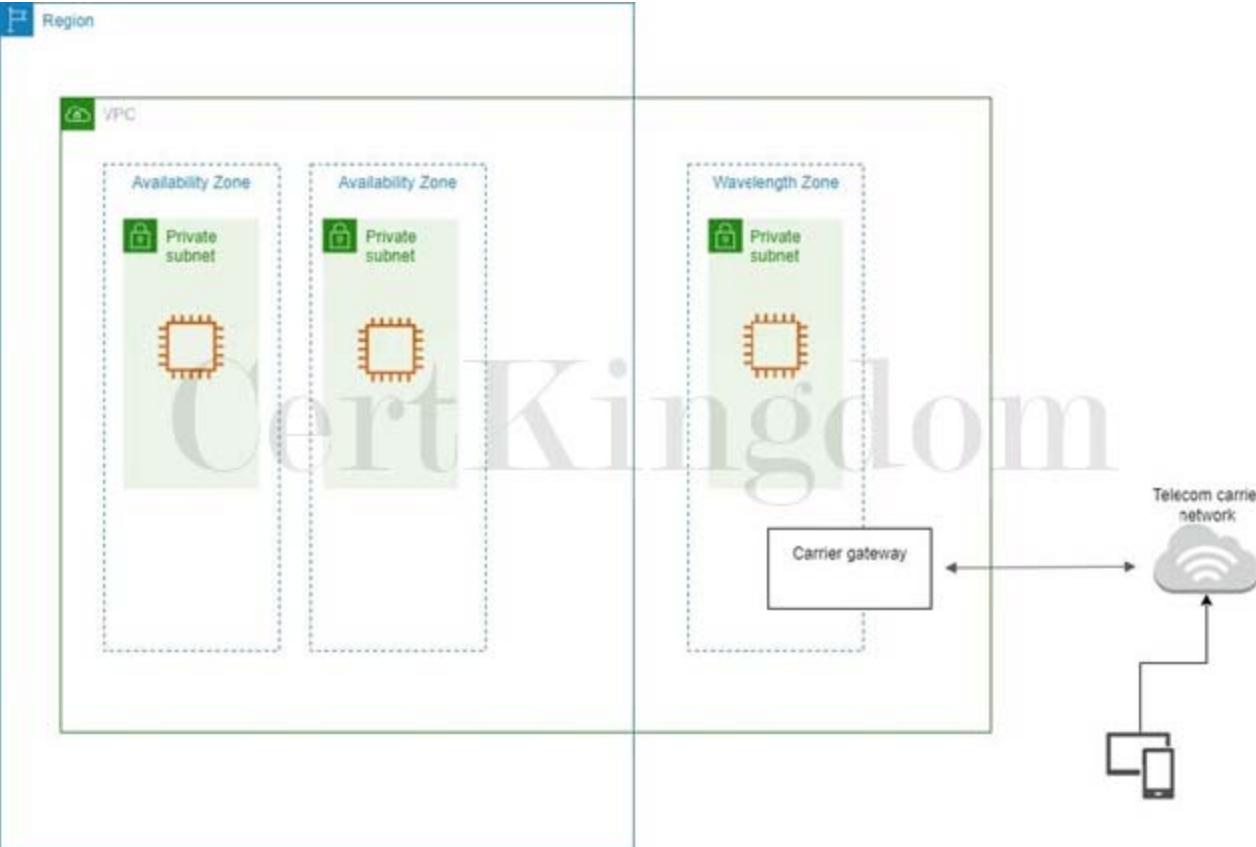
Answer: A

Explanation:

AWS Wavelength combines the high bandwidth and ultralow latency of 5G networks with AWS compute and storage services so that developers can innovate and build a new class of applications.

Wavelength Zones are AWS infrastructure deployments that embed AWS compute and storage services within telecommunications providers' data centers at the edge of the 5G network, so application traffic can reach application servers running in Wavelength Zones without leaving the mobile providers' network. This prevents the latency that would result from multiple hops to the internet and enables customers to take full advantage of 5G networks.

Wavelength Zones extend AWS to the 5G edge, delivering a consistent developer experience across multiple 5G networks around the world. Wavelength Zones also allow developers to build the next generation of ultra-low latency applications using the same familiar AWS services, APIs, tools, and functionality they already use today.



Amazon EKS uses IAM to provide authentication to your Kubernetes cluster, but it still relies on native Kubernetes Role-Based Access Control (RBAC) for authorization. This means that IAM is only used for the authentication of valid IAM entities. All permissions for interacting with your Amazon EKS cluster's Kubernetes API are managed through the native Kubernetes RBAC system.

Access to your cluster using AWS Identity and Access Management (IAM) entities is enabled by the AWS IAM Authenticator for Kubernetes, which runs on the Amazon EKS control plane. The authenticator gets its configuration information from the aws-auth ConfigMap (AWS authenticator configuration map).

The aws-auth ConfigMap is automatically created and applied to your cluster when you create a managed node group or when you create a node group using eksctl. It is initially created to allow nodes to join your cluster, but you also use this ConfigMap to add role-based access control (RBAC) access to IAM users and roles.

Hence, the correct answer is: Launch the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Create node groups in Wavelength Zones for the Amazon EKS cluster via the AWS Wavelength service. Apply the AWS authenticator configuration map (aws-auth ConfigMap) to your cluster.

The option that says: Host the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Set up node groups in AWS Wavelength Zones for the Amazon EKS cluster. Attach the Amazon EKS connector agent role (AmazonECSConnectorAgentRole) to your cluster and use AWS Control Tower for RBAC access is incorrect. An Amazon EKS connector agent is only used to connect your externally hosted Kubernetes clusters and to allow them to be viewed in your AWS Management Console. The AWS Control Tower doesn't provide RBAC access too to your EKS cluster. This service is commonly used for setting up a secure multi-account AWS environment and not for providing cluster authentication using IAM users and roles.

The option that says: Launch the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Create VPC endpoints for the AWS Wavelength Zones and apply them to the Amazon EKS cluster. Install the AWS IAM Authenticator

for Kubernetes (aws-iam-authenticator) to your cluster is incorrect because you cannot create VPC Endpoints in AWS Wavelength Zones. In addition, it is more appropriate to apply the AWS authenticator configuration map (aws-auth ConfigMap) to your Amazon EKS cluster to enable RBAC access.

The option that says: Host the application to an Amazon EKS cluster and run the Kubernetes pods on AWS Fargate. Create node groups in AWS Wavelength Zones for the Amazon EKS cluster. Add the EKS pod execution IAM role (AmazonEKSFargatePodExecutionRole) to your cluster and ensure that the Fargate profile has the same IAM role as your Amazon EC2 node groups is incorrect. Although this solution is possible, the security configuration of the Amazon EKS control plane is wrong. You have to ensure that the Fargate profile has a different IAM role as your Amazon EC2 node groups and not the other way around.

References:

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

<https://docs.aws.amazon.com/eks/latest/userguide/add-user-role.html#aws-auth-configmap>

<https://docs.aws.amazon.com/eks/latest/userguide/cluster-auth.html>

---

## QUESTION 385

A company is using AWS IAM to manage access to AWS services. The Solutions Architect of the company created the following IAM policy for AWS Lambda:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "lambda>CreateFunction",  
        "lambda>DeleteFunction"  
      ],  
      "Resource": "*"  
    },  
    {  
      "Effect": "Deny",  
      "Action": [  
        "lambda>CreateFunction",  
        "lambda>DeleteFunction",  
        "lambda>InvokeFunction",  
        "lambda>TagResource"  
      ],  
      "Resource": "*",  
      "Condition": {  
        "IpAddress": {  
          "aws:SourceIp": "187.5.104.11./32"  
        }  
      }  
    }  
  ]  
}
```

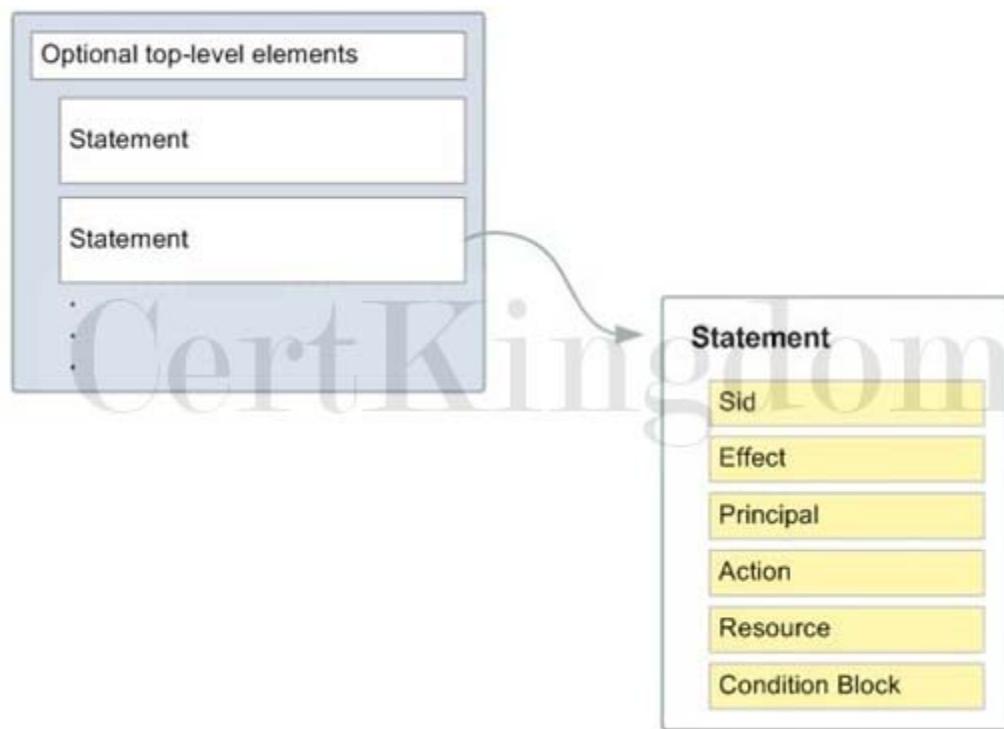
Which of the following options are allowed by this policy?

- A. Delete an AWS Lambda function from any network address.
- B. Create an AWS Lambda function using the 100.220.0.11./32 address.
- C. Delete an AWS Lambda function using the 187.5.104.11./32 address.
- D. Create an AWS Lambda function using the 187.5.104.11./32 address.

Answer: B

Explanation:

You manage access in AWS by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when an IAM principal (user or role) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents.



You can use AWS Identity and Access Management (IAM) to manage access to the Lambda API and resources like functions and layers. Based on the given IAM policy, you can create and delete a Lambda function from any network address except for the IP address 187.5.104.11./32. Since the IP address, 100.220.0.11./32 is not denied in the policy, you can use this address to create a Lambda function.

Hence, the correct answer is: Create an AWS Lambda function using the 100.220.0.11./32 address.

The option that says: Delete an AWS Lambda function using the 187.5.104.11./32 address is incorrect because the source IP used in this option is denied by the IAM policy.

The option that says: Delete an AWS Lambda function from any network address is incorrect. You can't delete a Lambda function from any network address because the address 187.5.104.11./32 is denied by the policy.

The option that says: Create an AWS Lambda function using the 187.5.104.11./32 address is incorrect.

Just like the option above, the IAM policy denied the IP address 187.5.104.11./32

References:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html)

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

Check out this AWS IAM Cheat Sheet:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>