# Exam #4

## Question 2: Correct

You are employed by a large electronics company that uses Amazon Simple Storage Service. 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?

Explanation

You can use AWS CloudTrail logs together with **server access logs** for Amazon S3. CloudTrail logs provide you with detailed API tracking for Amazon S3 bucket-level and object-level operations, while server access logs for Amazon S3 provide you visibility into object-level operations on your data in Amazon S3.

You can also use CloudTrail logs together with CloudWatch for Amazon S3. CloudTrail integration with CloudWatch Logs delivers S3 bucket-level API activity captured by CloudTrail to a CloudWatch log stream in the CloudWatch log group you specify. You can create CloudWatch alarms for monitoring specific API activity and receive email notifications when the specific API activity occurs.

For this scenario, you can use CloudTrail and the Server Access Logging feature of Amazon S3. However, the question mentioned that it needs 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 which is why the correct answer is Option 2.

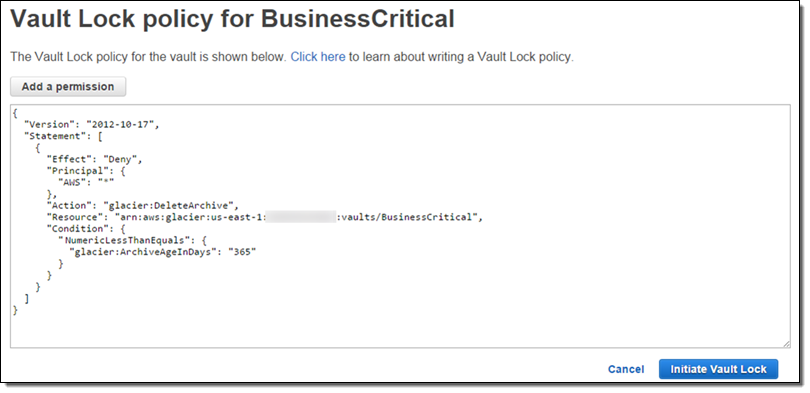
## Question 5: Correct

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?

Explanation

An Amazon S3 Glacier (Glacier) vault (\*a vault is a container for storing archives) 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.



A vault lock policy is different than a vault access policy. Both policies govern access controls to your vault. However, a vault lock policy can be locked to prevent future changes, providing strong enforcement for your **compliance controls**. You can use the vault lock policy to deploy regulatory and compliance controls, which typically require tight controls on data access. In contrast, you use a vault access policy to implement access controls that are not compliance related, temporary, and subject to frequent modification. Vault lock and vault access policies can be used together. For example, you can implement time-based data retention rules in the vault lock policy (deny deletes), and grant read access to designated third parties or your business partners (allow reads).

## Question 6: Correct

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?

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.

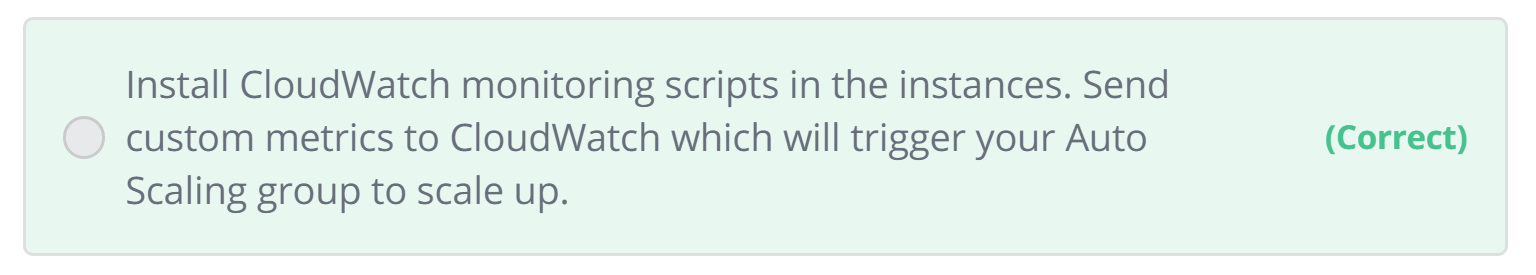
Amazon MQ, Amazon SQS, and Amazon SNS are messaging services that are suitable for anyone from startups to enterprises. If you're using messaging with existing applications and want to move your messaging service to the cloud quickly and easily, it is recommended that you consider Amazon MQ.

## Question 9: Incorrect

An auto-scaling group of Linux EC2 instances is created with basic monitoring enabled in CloudWatch. You noticed that your application is slow so you asked one of your engineers to check all of your EC2 instances. After checking your instances, you noticed that the auto scaling group is not launching more instances as it should be, even though the servers already have high memory usage.

What is the best solution that will fix this issue?

Explanation



The **Amazon CloudWatch Monitoring Scripts** for Amazon Elastic Compute Cloud (Amazon EC2) Linux-based instances demonstrate how to produce and consume Amazon CloudWatch custom metrics.

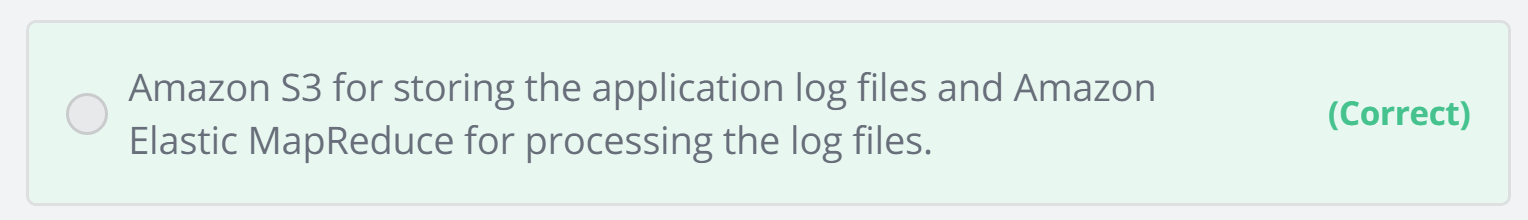
Option 2 is correct because CloudWatch does not monitor EC2 memory usage as well as disk space utilization. You would have to send custom metrics to CloudWatch.

## Question 10: Incorrect

You have 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 the best to use in this case?

Explanation

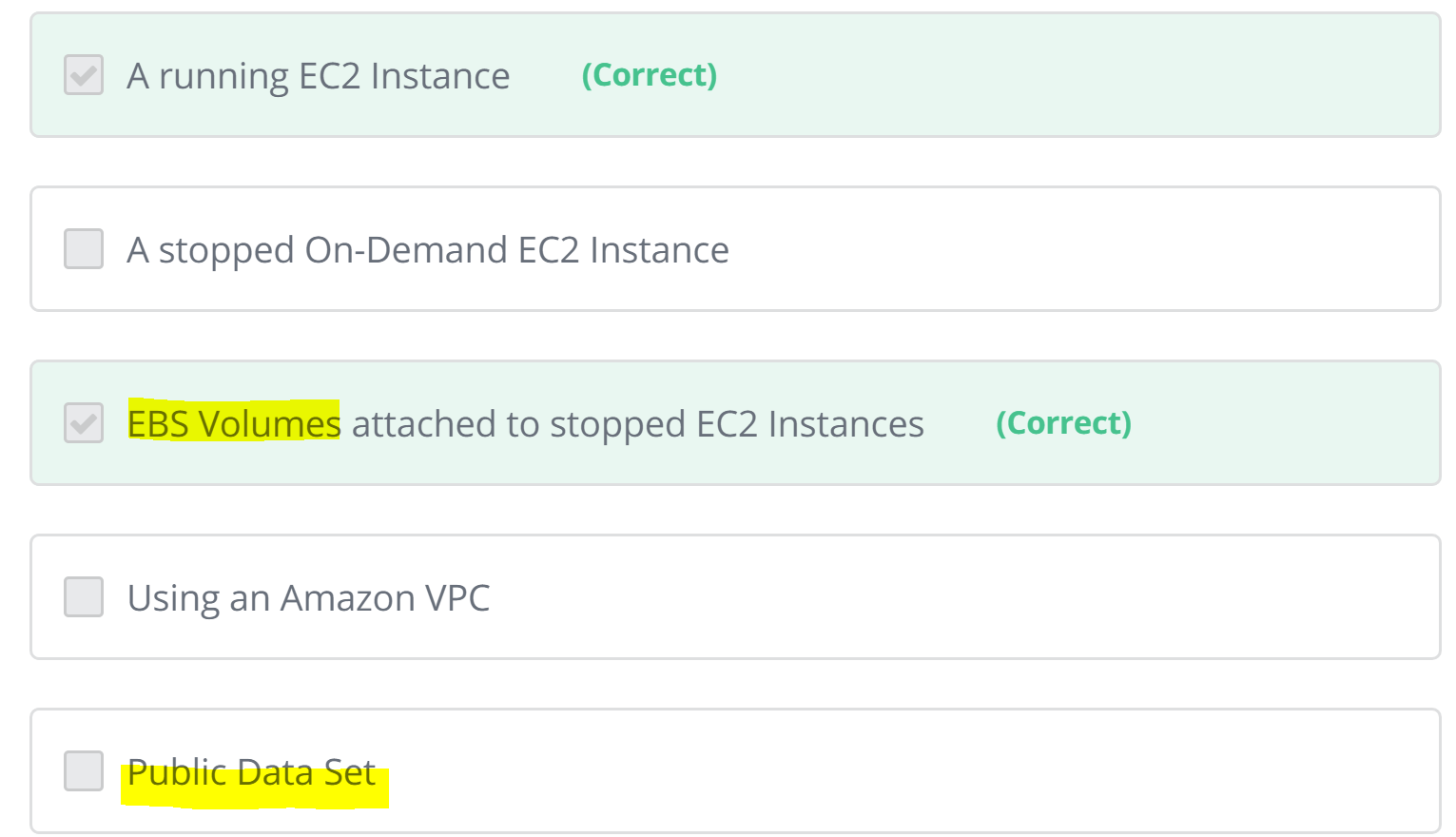


## Question 11: Correct

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? (Choose 2)

Explanation

When you stop an instance, AWS shuts it down but don't charge hourly usage for a stopped instance or data transfer fees, but AWS does charge for the storage of any Amazon EBS volumes.



## Question 12: Incorrect

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?

Explanation

**AWS Step Functions** provides serverless orchestration for modern application, using visual workflows. 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.

## Question 15: Incorrect

You have 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?

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.

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

## Question 16: Incorrect [Review this]

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?

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, RCFile, 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.

## Question 18: Incorrect

You are the technical lead of the Cloud Infrastructure team in your company and you were consulted by a software developer regarding the required AWS resources of the web application that he is building. He 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 his web application persists, the app should be launched in an EC2 instance that has a durable, block-level storage volume attached. He 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? (Choose 2)

Explanation

General Purpose (SSD) is the new, SSD-backed, general purpose EBS volume type that we recommend 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 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.

## Question 19: Incorrect

A company is using hundreds of AWS resources in multiple AWS regions. They require a way to uniquely identify all of their AWS resources that will allow them to specify a resource unambiguously across all of AWS, such as in IAM policies, Amazon Relational Database Service (Amazon RDS) tags, and API calls.

Which of the following is the most suitable option to use in this scenario?

Explanation

Amazon Resource Names (ARNs) uniquely identify AWS resources. We require an ARN when you need to specify a resource unambiguously across all of AWS, such as in IAM policies, Amazon Relational Database Service (Amazon RDS) tags, and API calls.

AWS Resource ID is primarily used to find your resources in the Amazon EC2 console only and not your entire VPC or AWS account.

AWS Service Namespaces only helps you identify an AWS service and not a unique resource. For example, the namespace for Amazon S3 is s3, and the namespace for Amazon EC2 is ec2.

## Question 22: Correct [????????????]

You are creating a Provisioned IOPS volume in AWS. The size of the volume is 10 GiB.

Which of the following is the correct value that should be put for the IOPS of the volume?

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 × 1,280 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.

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 × 640 GiB = 32,000).

## Question 24: Incorrect

Your company has a two-tier environment in their 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:

a) There is an application load balancer that would distribute the incoming traffic among the servers in the application tier.

b) 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.

c) 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.

d) 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?

Explanation

**One subnet can only exist one AZ. VPC spans all AZs in the region.**

## Question 26: Incorrect

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?

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.

## Question 28: Correct

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?

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 autocompletion, and log field discovery to help you get started quickly. Sample queries are included for several types of AWS service logs.

## Question 32: Correct

You are working as a Solutions Architect for a startup in which you are tasked 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 will be lost, no duplicates will be produced and that they are processed in EMR in the same order as their arrival.

Which of the following options should you implement to meet the startup's requirements?

Explanation

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).

## Question 34: Correct

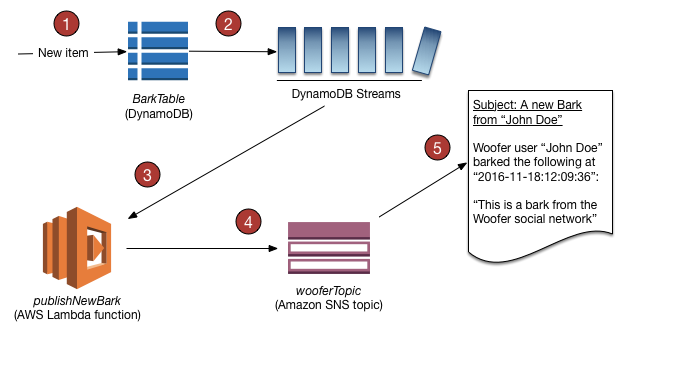
A leading IT consulting company has an application which processes a large stream of financial data by an Amazon ECS Cluster then stores the result to a DynamoDB table. You have to design a solution to detect new entries in the DynamoDB table then automatically trigger a Lambda function to run some tests 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?

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.



## Question 36: Correct

You are working as a Junior Solutions Architect where you are responsible in enhancing the availability and durability of the database instances in your VPC. Your company has a Multi-AZ RDS instance in the ap-northeast-1 region. If a storage volume on the primary instance fails in a Multi-AZ deployment, Amazon RDS automatically initiates a failover to the up-to-date standby instance.

In case of a failover, which record in Route 53 is changed?

Explanation

Failover is automatically handled by Amazon RDS so that you can resume database operations as quickly as possible without administrative intervention. When failing over, Amazon RDS simply flips the canonical name record (CNAME) in Route53 (\*Route 53-RDS is associated in CNAME originally since RDS instance has domain name, but IP) for your DB instance to point at the standby, which in turn is promoted to become the new primary.

## Question 38: Incorrect

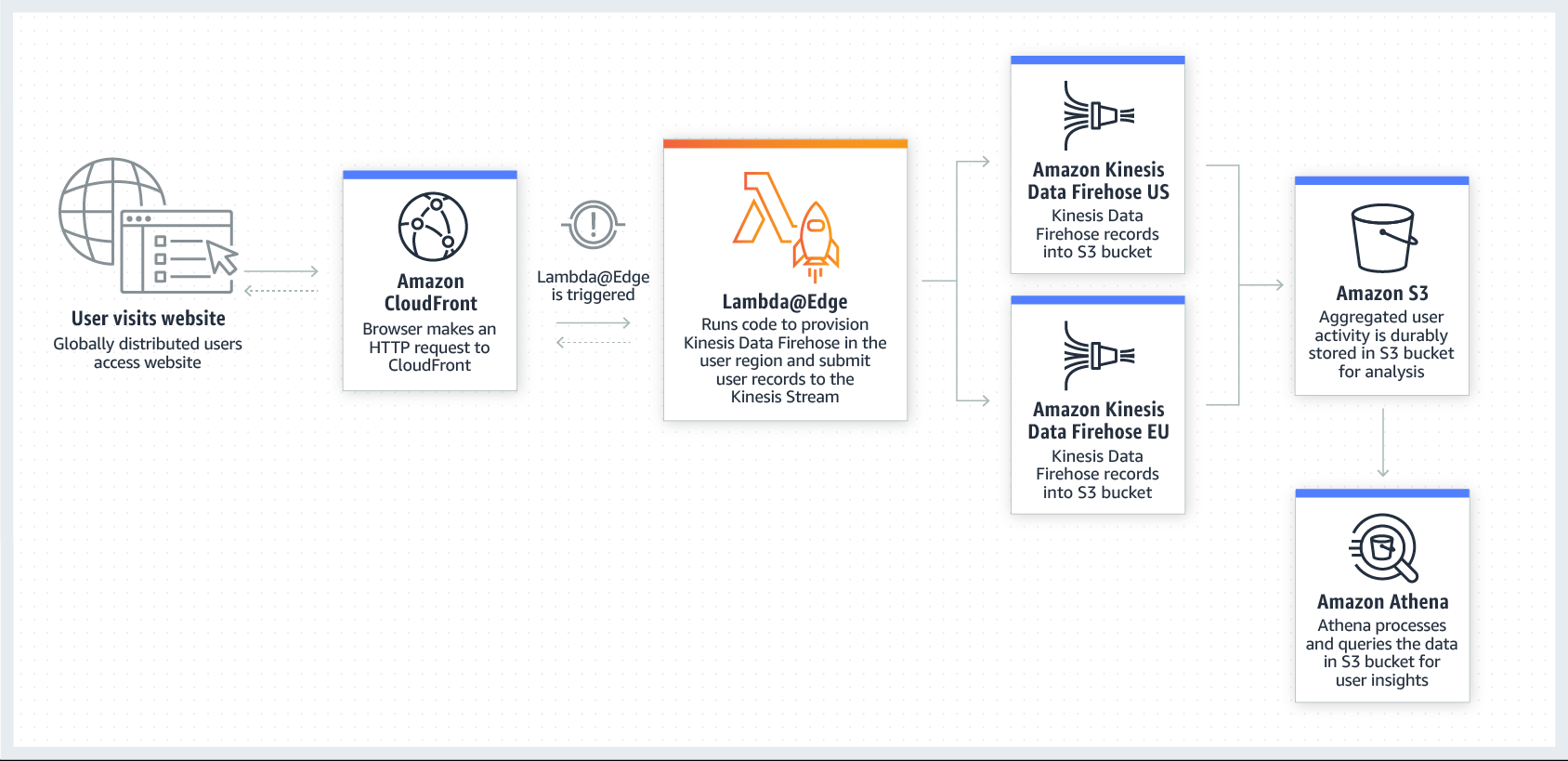
You are working as a Solutions Architect for a leading data analytics company in which you are tasked to process real-time streaming data of your users across the globe. This will enable you to track and analyze globally-distributed user activity on your website and mobile applications, including click stream analysis. Your cloud architecture should process the data in close geographical proximity to your users and to respond to user requests at low latencies.

Which of the following options is the most ideal solution that you should implement?

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, Option 4 is the correct answer in this scenario.

Options 1 and 3 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.

## Question 40: Incorrect [\*\*\*\*\*\*\*\*\*\*]

You are a Big Data Engineer who is assigned to handle the online enrollment system database of a prestigious university, which is hosted in RDS. You are 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? (Choose 2)

Explanation

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.

## Question 43: Incorrect

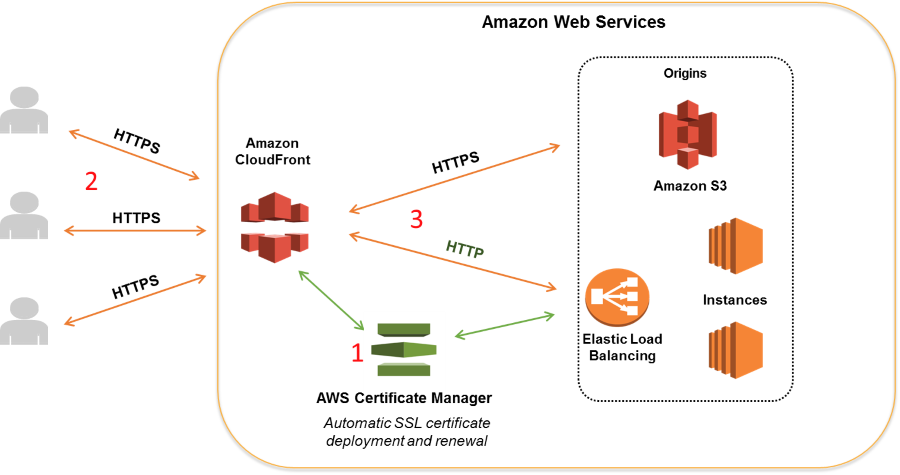
A web application is hosted in an Auto Scaling group of EC2 instances deployed across multiple Availability Zones in front of an Application Load Balancer. You need to implement an SSL solution for your system to improve its security which is why you requested an SSL/TLS certificate from a third-party certificate authority (CA).

Where can you safely import the SSL/TLS certificate of your application? (Choose 2)

Explanation

If you got your certificate from a third-party CA, import the certificate into ACM or upload it to the IAM certificate store.

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.



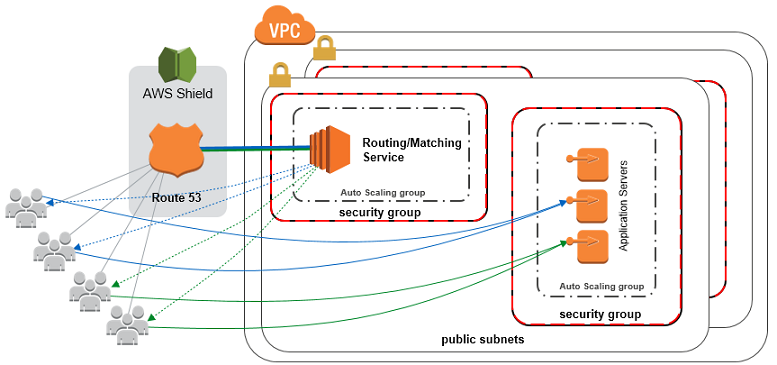
## Question 46: Incorrect

You are working as a Solutions Architect for a leading financial firm where you are responsible in ensuring that their 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?

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 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.

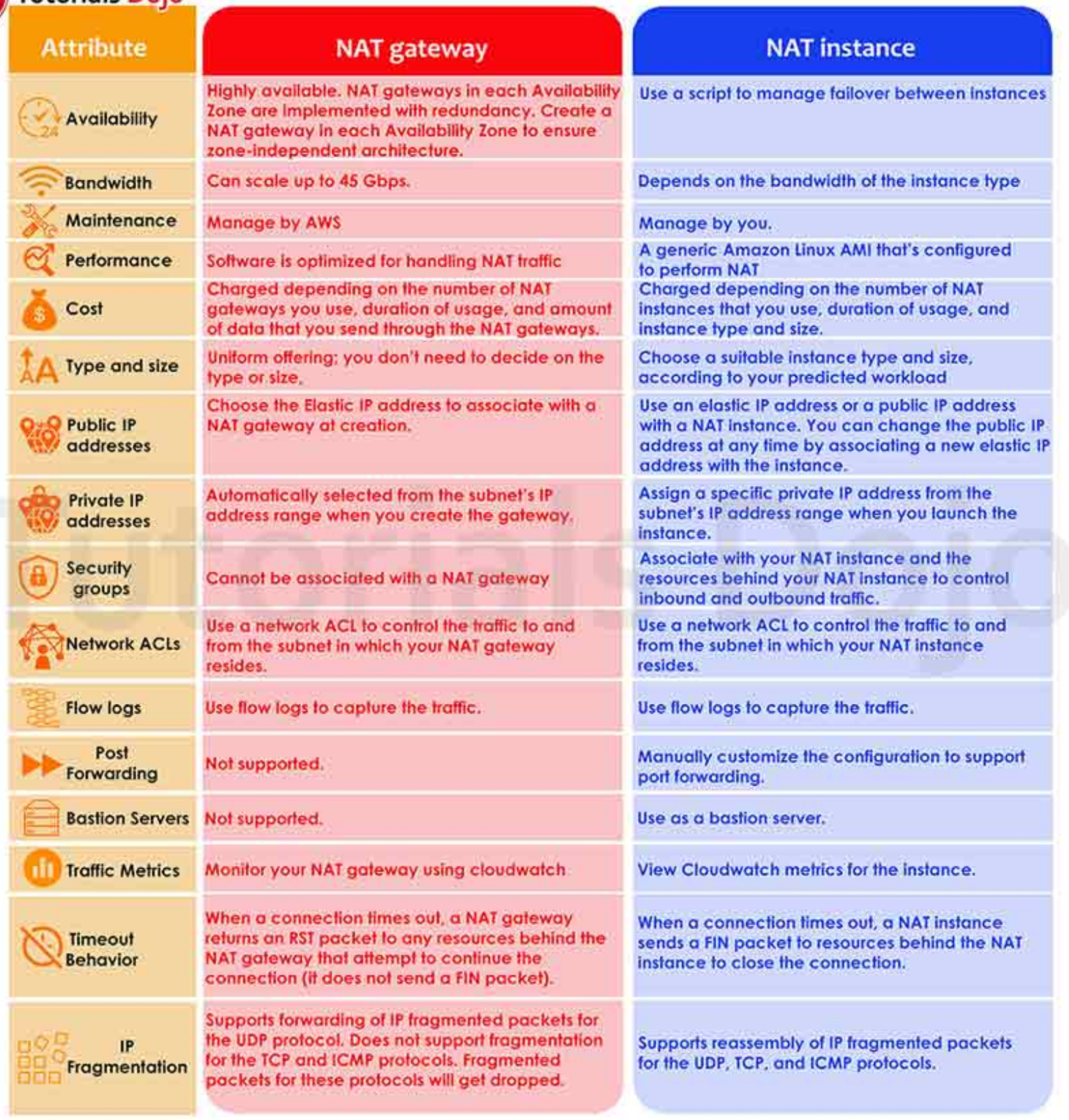
## Question 47: Incorrect

<bucket-name>.s3-website-<AWS-region>.amazonaws.com

## Question 64: Correct

You are working as a Network Engineer for an electronics and communications company in Japan. You are told to implement a NAT instance in your VPC to allow certain EC2 instances to initiate connections to the Internet but restrict any requests coming from the Internet.

In this scenario, what is the best way to configure a fault-tolerant NAT instance in your VPC?



## Question 65: Incorrect

A bank portal application is hosted in an Auto Scaling group of EC2 instances behind a Classic Load Balancer (CLB). You are required to set up the architecture so that any back-end EC2 instances that you de-register should complete the in-progress requests first before the de-registration process takes effect. Conversely, if a back-end instance fails health checks, the load balancer should not send any new requests to the unhealthy instance but should allow existing requests to complete.

How will you configure your load balancer to satisfy the above requirement?

Explanation

To ensure that a Classic Load Balancer stops sending requests to instances that are de-registering or unhealthy while keeping the existing connections open, use **connection draining**. This enables the load balancer to complete in-flight requests made to instances that are de-registering or unhealthy.