# 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.

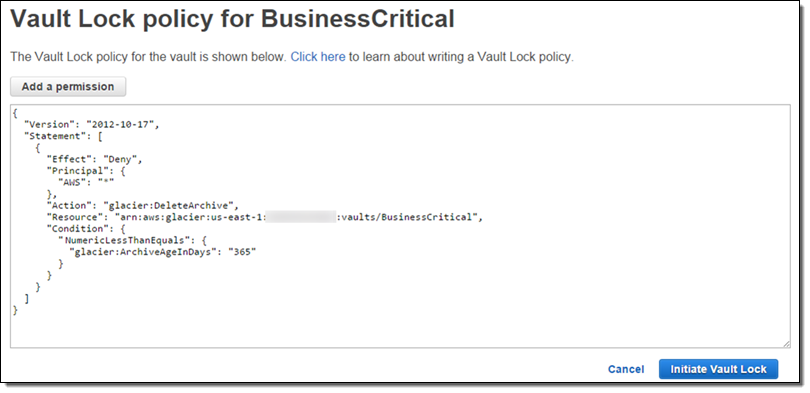
## Question 5: Correct

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.

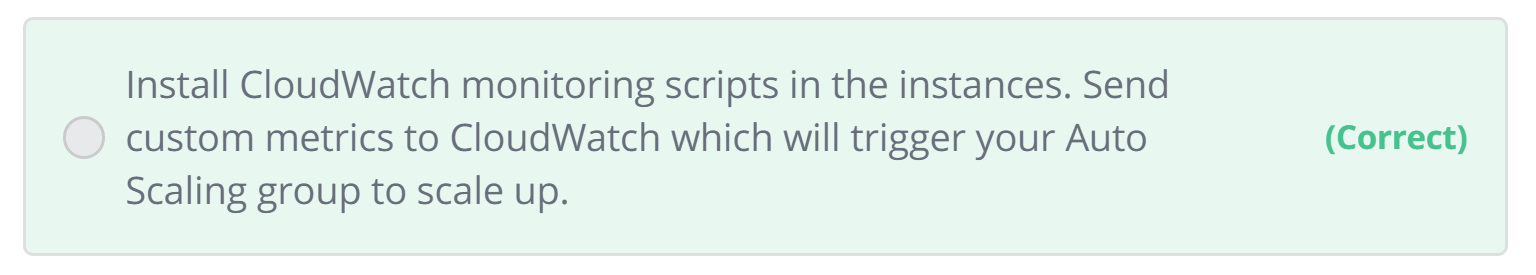
Amazon MQ, Amazon SQS, and Amazon SNS are messaging services that are suitable for anyone from startups to enterprises. If you're using messaging with existing applications and want to move your messaging service to the cloud quickly and easily, it is recommended that you consider Amazon MQ.

## 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.

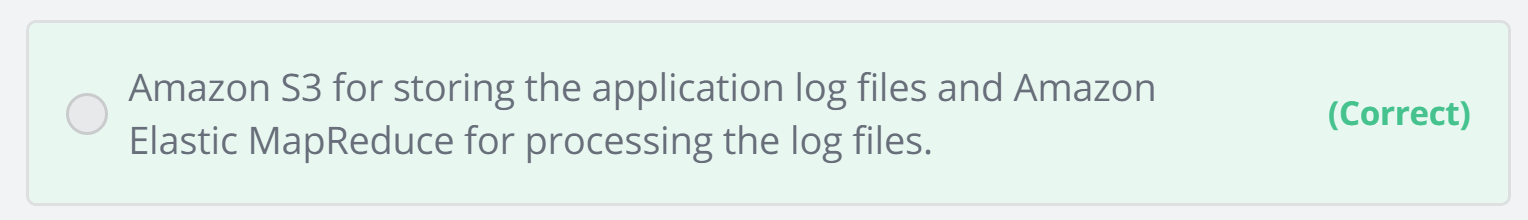
Option 2 is correct because CloudWatch does not monitor EC2 memory usage as well as disk space utilization. You would have to send custom metrics to CloudWatch.

## 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

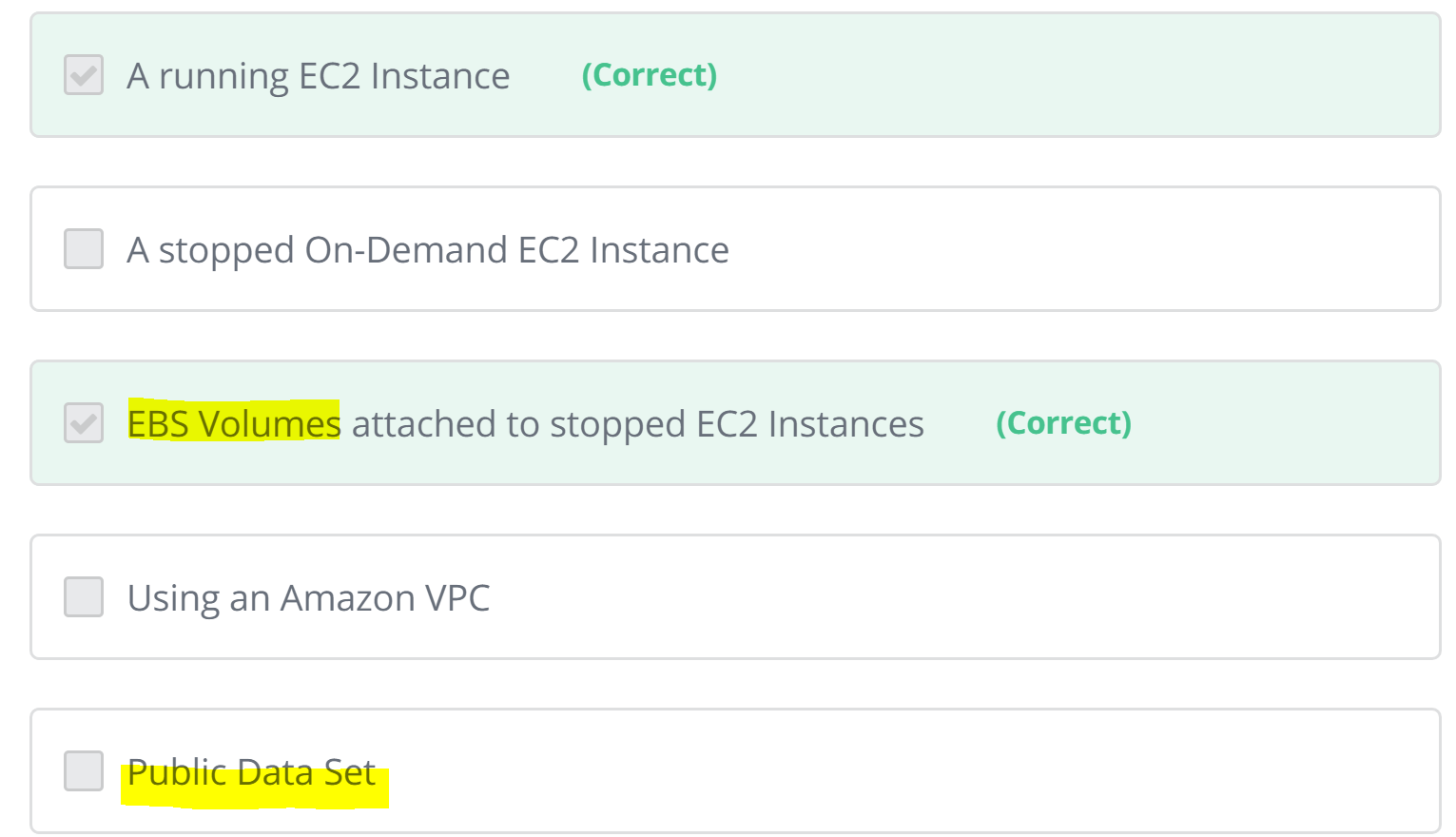


## Question 11: Correct

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.