Question 1

You are working on a distributed java application that will be storing messages in Amazon SQS. Some of these messages are greater than 256 KB. How can an Amazon SQS queue be created to manage messages with size greater than 256 KB?

- A. Create Amazon SQS queue using AWS SDK for Java to reference Amazon S3 buckets when message size exceeds 256 KB.right
- B. Create Amazon SQS queue using Amazon SQS console to reference Amazon S3 buckets when message size exceeds 256 KB.
- C. Create Amazon SQS queue using AWS CLI to reference Amazon S3 buckets when message size exceeds 256 KB.
- D. Create Amazon SQS queue using Amazon SQS HTTP API to reference Amazon S3 buckets when message size exceeds 256 KB.

Explanation:

Correct Answer: A

Amazon SQS Extended Client Library for Java can be used to manage messages in the Amazon SQS queue using Amazon S3. Messages with a size greater than 256 KB can be stored in the Amazon S3 bucket & can be referenced from Amazon SQS using Extended Client Library for Java.

- Option B is incorrect as the Amazon SQS console cannot create Amazon SQS Extended Client Library for Java.
- Option C is incorrect as AWS CLI cannot create Amazon SQS Extended Client Library for Java for storing large size Amazon SQS messages in Amazon S3.
- Option D is incorrect as Amazon SQS HTTP API cannot create Amazon SQS Extended Client Library for Java for storing large size Amazon SQS messages in Amazon S3.

For more information on Amazon SQS Extended Client Library for Java, refer to the following URL,

- https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-s3-messages.html

Question 2

A Developer is migrating an on-premises web application to the AWS Cloud. The application currently runs on a 32-processor server and stores session state in memory. On Friday afternoons the server runs at 75% CPU utilization, but only about 5% CPU utilization at other times.

How should the Developer change to code to better take advantage of running in the cloud?

- A. Compress the session state data in memory.
- B. Store session state on EC2 instance Store.
- C. Encrypt the session state data in memory.

- D. Store session state in an ElastiCache cluster.right

Explanation:

Answer – D

ElastiCache is the perfect solution for managing session state. This is also given in the AWS Documentation.

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 to this is to leverage an In-Memory Key/Value store such as Redis and Memcached.

Option A is incorrect since compression is not the ideal solution.

Option B is incorrect since EC2 Instance Store is too volatile.

Option C is incorrect since this is ok from a security standpoint but will just make the performance worse for the application.

For more information on Session Management, please refer to the below Link-

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

Question 3

An organization's application needs to monitor application-specific events with a standard AWS service. The service should capture the number of logged-in users and trigger events accordingly. During peak times, monitoring frequency will occur every 10 seconds.

What should be done to meet these requirements?

- A. Create an Amazon SNS notification.
- B. Create a standard resolution custom Amazon CloudWatch log.
- C. Create a high-resolution custom Amazon CloudWatch metric.right
- D. Create a custom Amazon CloudTrail log.

Explanation:

Answer – C

This is clearly mentioned in the AWS Documentation.

When creating an alarm, select a greater than or equal period to the frequency of the metric to be monitored. For example, basic monitoring for Amazon EC2 provides metrics for your instances every 5 minutes. When setting the alarm on a basic monitoring metric, select a period of at least 300 seconds (5 minutes). Detailed monitoring for Amazon EC2 provides metrics for your instances every 1 minute. When setting the alarm on a detailed monitoring metric, select a period of at least 60 seconds (1 minute).

If you set the alarm on a high-resolution metric, you can specify a high-resolution alarm with a period of 10 seconds or 30 seconds, or you can set a regular alarm with a period of any multiple of 60 seconds.

Option A is incorrect since the question does not mention anything on notifications.

Option B is incorrect since the standard resolution counters will not help define triggers within a 10 second interval.

Option D is incorrect since Cloudtrail is used for API Activity logging.

For more information on Cloudwatch metrics, please refer to the below Link-

- https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch_concepts.html

Question 4

An online educational institute uses a three-tier web application & is using AWS X-Ray to trace data between various services. User A is experiencing latency issues using this application & the Operations team has asked you to gather all traces for User A. Which of the following needs to be enabled to get Filtered output for User A from all other traces?

- A. Trace ID
- B. Annotationsright
- C. Segment ID
- D. Tracing header

Explanation:

Correct Answer – B

Annotations are key-value pairs indexed to use with filter expressions. In the above case, traces for a user A needs to be tracked, for which Annotations can be used along with a Filter expression to find all traces related to that user.

- Option A is incorrect as Trace ID will track a request's path through the application & will not be used in filtering messages.
- Option C is incorrect as Segment will provide details of resource name, request & work done. It will not help in filtering messages.
- Option D is incorrect as the Tracing Header consists of Root trace ID, Segment ID & sampling decision. It is not useful for filtering messages.

For more information on Annotations & Filter expressions on AWS X-Ray, refer to the following URL-

- https://docs.aws.amazon.com/xray/latest/devguide/xray-concepts.html

Question 5

A developer working on an AWS CodeBuild project wants to override a build command as part of a build run to test a change. The developer has access to run the builds but does not have access to the code and to edit the CodeBuild project.

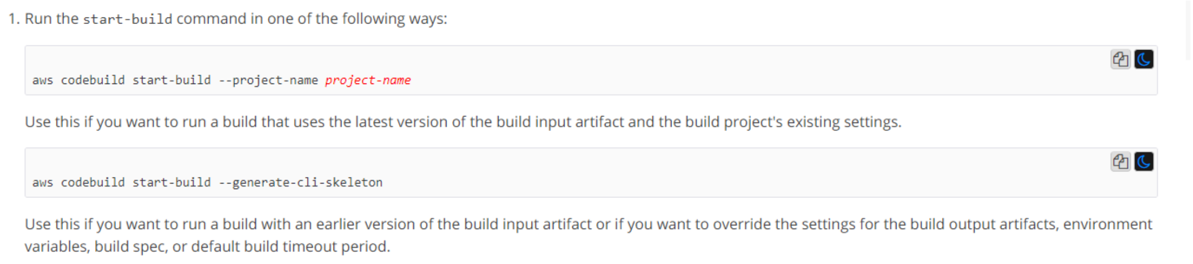
What process should the Developer use to override the build command?

- A. Update the buildspec.yml configuration file that is part of the source code and run a new build.
- B. Update the command in the Build Commands section during the build run in the AWS console.
- C. Run the start build AWS CLI command with buildspecOverride property set to the new buildspec.yml file.right
- D. Update the buildspec property in the StartBuild API to override the build command during build run.

Explanation:

Answer – C

Use the AWS CLI command to specify different parameters that need to be run for the build. Since the developer can run the build, he can run the build by changing the parameters from the command line. The same is also mentioned in the AWS Documentation.



1. Run the `start-build` command in one of the following ways:

```
aws codebuild start-build --project-name project-name
```

Use this if you want to run a build that uses the latest version of the build input artifact and the build project's existing settings.

```
aws codebuild start-build --generate-cli-skeleton
```

Use this if you want to run a build with an earlier version of the build input artifact or if you want to override the settings for the build output artifacts, environment variables, build spec, or default build timeout period.

Option A is incorrect because A buildspec is a collection of build commands and related settings, in YAML format, that CodeBuild uses to run a build. You can include a buildspec as part of the source code, or you can define a buildspec when you create a build project. However, the developer does not have access to the code.

Option B is incorrect because the developer does not have access to the code and to edit the CodeBuild project.

Option D is incorrect because it should be the buildspecOverride property instead of buildspec property.

For more information on running the command via the CLI, please refer to the below Link-

- https://docs.aws.amazon.com/codebuild/latest/userguide/run-build.html#run-build-cli

Note:
As per the question, the developer doesn't have access to edit the code build project but only have access to run the build. So for overriding the existing build we can make use of the BuildspecOverride attribute.

As per AWS,
`buildspecOverride`: Optional string. A build spec declaration that overrides for this build the one defined in the build project. If this value is set, it can be either an inline build spec definition or the path to an alternate build spec file relative to the value of the built-in `CODEBUILD_SRC_DIR` environment variable.

Question 6

You are working on a new project involving the creation of Lambda functions for a Serverless Web Application. A large team of developers will work on this project performing multiple changes to the Lambda function code. As the best practice, you have been asked to publish a version while creating a Lambda function or updating a function code. Which of the following is TRUE with regards to the published version of a Lambda Function?

- A. A published version is a snapshot of function code and has the same version number when a previous version is deleted & recreated.
- B. A published version is a snapshot of function code and has a unique Amazon Resource Name that can be updated using “UpdateFunctionCode.”
- C. A published version is a snapshot of function code and configuration that can be updated using the “Publish” parameter.
- D. A published version is a snapshot of function code and configuration that can't be changed.right

Explanation:

Correct Answer – D

A Publish version is a snapshot copy of a Lambda Function code & configuration in $LATEST version. No configuration changes can be done to a published version & it has a unique ARN which can't be modified.

Option A is incorrect as a published version can only have a different version from previous ones, even when the previous version is deleted & recreated.

Option B is incorrect as after a version is published, ARN can't be modified.

Option C is incorrect as when a version is published. No configuration changes can be made to this version.

For more information on AWS Lambda Versioning, refer to the following URL-

https://docs.aws.amazon.com/lambda/latest/dg/versioning-intro.html

Question 7

You are working on a mobile application that will be using AWS ElastiCache for caching application data to reduce latency & improve throughput. The management team has asked you to evaluate both in-memory cache supported by AWS ElastiCache engines – Memcached and Redis. Which of the following features are available only with Memcached which you should consider while developing the application? (Select Two)

- A. Simple caching modelright
- B. Pub/Sub capability support.

- C. Multithreaded performance with utilization of multiple coresright
- D. Data replication to multiple AZ's.Data persistence

Explanation:

Correct Answer – A, C

AWS ElastiCache Memcached cache engine supports multithreaded performance using multiple cores & a simple caching model.

- Options B & D are incorrect as these features are available with the AWS ElastiCache Redis Cache engine.

- For more information on Comparison between Memcached and Redis, refer to the following URLs-
  - https://aws.amazon.com/elasticache/redis-vs-memcached/
  - https://d0.awsstatic.com/whitepapers/performance-at-scale-with-amazon-elasticache.pdf

Question 8

A developer is building an application that needs access to an S3 bucket. An IAM role is created with the required permissions to access the S3 bucket. Which API call should the Developer use in the application so that the code can access to the S3 bucket?

- A. IAM: AccessRole

- B. STS: GetSessionToken

- C. IAM:GetRoleAccess

- D. STS:AssumeRoleright

Explanation:

Answer – D

This is given in the AWS Documentation.

A role specifies a set of permissions that you can use to access AWS resources. In that sense, it is similar to an IAM user. An application assumes a role to receive permissions to carry out required tasks and interact with AWS resources. The role can be in your own account or any other AWS account. For more information about roles, their benefits, and how to create and configure them, see IAM Roles, and Creating IAM Roles. To learn about the different methods that you can use to assume a role, see Using IAM Roles.

Important
The permissions of your IAM user and any roles that you assume are not cumulative. Only one set of permissions is active at a time. When you assume a role, you temporarily give up your previous user or role permissions and work with the permissions assigned to the role. When you exit the role, your user permissions are automatically restored.

To assume a role, an application calls the AWS STS AssumeRole API operation and passes the ARN of the role to use. When you call AssumeRole, you can optionally pass a JSON policy. This allows you to restrict permissions for that for the role's temporary credentials. This is useful when you need to give the temporary credentials to someone else. They can use the role's temporary credentials in subsequent AWS API calls to access resources in the account that owns the role. You cannot use the passed policy to grant permissions that are in excess of those allowed by the permissions policy of the role that is being assumed. To learn more about how AWS determines the effective permissions of a role, see Policy Evaluation Logic.

Option A is incorrect because IAM does not have this API.

Option B is incorrect because STS:GetSessionToken is used if you want to use MFA to protect programmatic calls to specific AWS API operations like Amazon EC2 StopInstances. MFA-enabled IAM users would need to call GetSessionToken and submit an MFA code associated with their MFA device.

Option C is incorrect because IAM does not have this API.

For more information on switching roles, please refer to the below Link-

- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-api.html

Question 9

A developer has recently deployed an AWS Lambda function that computes a Fibonacci sequence using recursive Lambda invocations. A pre-defined AWS IAM policy is being used for this function, and only the required dependencies were packaged. A few days after deployment, the Lambda function is being throttled.

What should the Developer have done to prevent this, according to best practices?

- A. Use more restrictive IAM policies.
- B. Avoid recursive Lambda invocations.right
- C. Request a concurrency service limit increase.
- D. Increase the memory allocation range.

Explanation:

Answer – B
The question's focus is on the best practice methods for Lambda functions. Since the question asks us to choose the best option that the developer might have done to prevent this throttling issue, he should have written a code that avoids the recursive call of the function within itself as it is not recommended as a best practice.

For the "Lambda function code" best practice, it is recommended that we should avoid recursive code in the Lambda function.

"Avoid using recursive code in your Lambda function, wherein the function automatically calls itself until some arbitrary criteria are met. This could lead to an unintended volume of function invocations and escalated costs. If you do accidentally do so, set the function concurrent execution limit to '0' (Zero) immediately to throttle all invocations to the function, while you update the code."

Option A is incorrect since using IAM Policies will not help in resolving the issue.
Option C is incorrect since this is about concurrency on the number of AWS Lambda executions.
Option D is incorrect since the issue here is with the number of executions and not on the amount of memory used for the executions.
For more information, please refer to the below Link-

- https://docs.aws.amazon.com/lambda/latest/dg/best-practices.html

Question 10

A company is writing a Lambda function that will run in multiple stages, such a dev, test, and production. The function is dependent upon several external services, and it must call different endpoints for these services based on the function's deployment stage.

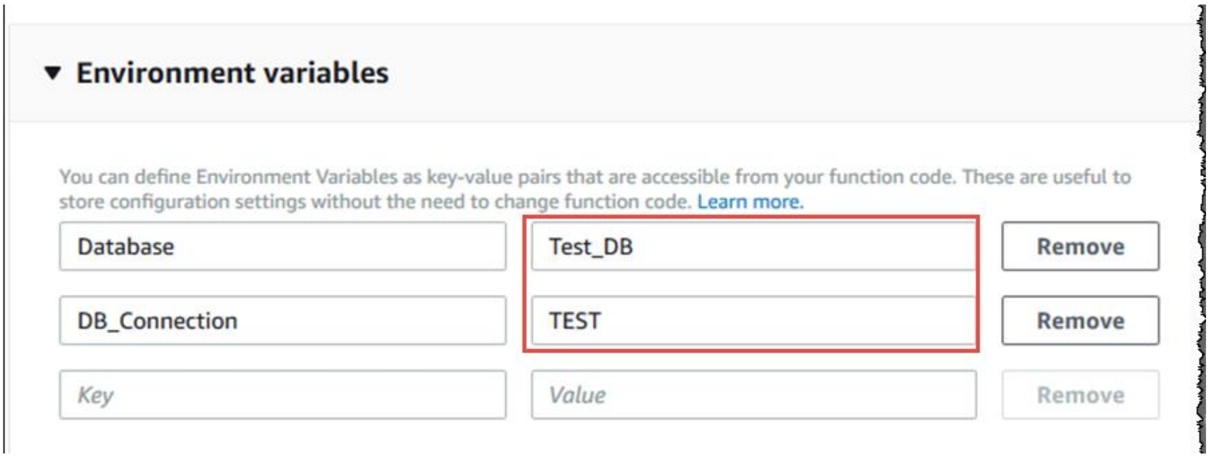
What Lambda feature will enable the developer to ensure that the code references the correct endpoints when running in each stage?

- A. Tagging
- B. Concurrency
- C. Aliases
- D. Environment variablesright

Explanation:

Answer – D

You can create different environment variables in the Lambda function that can be used to point to the different services. The below screenshot from the AWS Documentation shows how this can be done with databases.



▼ 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.

Database	Test_DB
DB_Connection	TEST

Option A is invalid since this can only be used to add metadata for the function.

Option B is invalid since this is used for managing the concurrency of execution.

Option C is invalid since this is used for managing the different versions of your Lambda function.

For more information on AWS Lambda environment variables, please refer to the below Link-

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

Question 11

You are using AWS SAM to define a Lambda function and configure CodeDeploy to manage deployment patterns. With the new Lambda function working as per expectation which of the following will shift traffic from the original Lambda function to the new Lambda function in the shortest time frame?

- A. Canary10Percent5Minutesright
- B. Linear10PercentEvery10Minutes
- C. Canary10Percent15Minutes
- D. Linear10PercentEvery5Minute

Explanation:

Correct Answer – A

With the Canary Deployment Preference type, Traffic is shifted in two intervals. With Canary10Percent5Minutes, 10 percent of traffic is shifted in the first interval while remaining all traffic is shifted after 5 minutes.

- Option B is incorrect as Linear10PercentEvery10Minutes will add 10 percent traffic linearly to a new version every 10 minutes. So, after 100 minutes all traffic will be shifted to the new version.
- Option C is incorrect as Canary10Percent15Minutes will send 10 percent traffic to the new version and 15 minutes later complete deployment by sending all traffic to the new version.
- Option D is incorrect as Linear10PercentEvery5Minute will add 10 percent traffic linearly to the new version every 5 minutes. So, after 50 minutes all traffic will be shifted to the new version.
- For more information on Deployment Preference Type for AWS SAM templates, refer to the following URL-
  - https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/automating-updates-to-serverless-apps.html

Question 12

A Developer is migrating an on-premises application to the AWS Cloud. The application currently uses Microsoft SQL, encrypting some of the data using Transparent Data Encryption. Which service should the Developer use to minimize code changes?

- A. Amazon RDSright
- B. Amazon Aurora
- C. Amazon Redshift
- D. Amazon DynamoDB

Explanation:

Answer – A

This is also mentioned in the AWS Documentation.

Amazon RDS supports using Transparent Data Encryption (TDE) to encrypt stored data on your DB instances running Microsoft SQL Server. TDE automatically encrypts data before it is written to storage and automatically decrypts data when the data is read from storage.

Amazon RDS supports TDE for the following SQL Server versions and editions:

- SQL Server 2017 Enterprise Edition
- SQL Server 2016 Enterprise Edition
- SQL Server 2014 Enterprise Edition
- SQL Server 2012 Enterprise Edition
- SQL Server 2008 R2 Enterprise Edition

To enable transparent data encryption for a DB instance running SQL Server, specify the TDE option in an Amazon RDS option group associated with that DB instance.

Option B is incorrect because Microsoft SQL is not compatible with Aurora.

Option C is incorrect because RedShift is used as a Data warehouse. Microsoft SQL does not support it.

Option D is incorrect because DynamoDB is a no-SQL database, primarily used with serverless architectures.

For more information on Encryption on Microsoft SQL Server AWS, please refer to the below Link-

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.SQLServer.Options.TDE.html

Question 13

A Web-application uses Amazon SQS to buffer messages processed by another application deployed in a fleet of Amazon EC2 instances. Application deployed on Amazon EC2 instances sends message confirmation to end-users. Due to the heavy load on Amazon EC2 instances, it takes a long time to process messages & users are receiving multiple messages. Which of the following changes can be done on the Amazon SQS queue to ensure users receive only a single message?

- A. Increase visibility timeout to 5 mins using ChangeMessageVisibility.right
- B. Increase visibility timeout to 5 mins using UpdateMessageVisibility.
- C. Decrease visibility timeout to 2 mins using UpdateMessageVisibility.
- D. Decrease visibility timeout to 2 mins using ChangeMessageVisibility.

Explanation:

Correct Answer – A

Visibility Timeout is used to hide messages from other consumers when one of the consumers is processing the message. In the above case, when one of the Amazon EC2 instances is processing messages from the Amazon SQS queue, it takes time to process messages due to load on the instance. Within that time period, visibility timeout is expired & another EC2 instance is processing the same message & sending updates to users. To avoid multiple processing of the same message, the Visibility timeout can be increased so that Amazon EC2 processes the message before the visibility timeout expires.

- Option B & D are incorrect as UpdateMessageVisibility is an invalid option to change the visibility timeout.
- Option C is incorrect as decreasing visibility timeout will not resolve the issue.

For more information on visibility timeout with Amazon SQS, refer to the following URL-

- https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html

Question 14

A developer is using Amazon API Gateway as an HTTP proxy to a backend endpoint. There are three separate environments: Development, Testing, Production, and three corresponding stages in the API gateway.

How should traffic be directed to different backend endpoints for each of these stages without creating a separate API for each?

- A. Add a model to the API and add a schema to differentiate different backend endpoints.
- B. Use stage variables and configure the stage variables in the HTTP integration Request of the API.right
- C. Use API Custom Authorizers to create an authorizer for each of the different stages.
- D. Update the Integration Response of the API to add different backend endpoints.

Explanation:

Answer – B

The AWS Documentation mentions the following to support this.

Stage variables are name-value pairs that you can define as configuration attributes associated with a deployment stage of an API. They act like environment variables and can be used in your API setup and mapping templates.

Option A is incorrect since this would only allow for additions of schema’s.

Option C is incorrect since this is only used for Authorization and would not help differentiate the environments.

Option D is incorrect since this would help in integrating the responses to the API gateway.

For more information on Stage variables in the API gateway, please refer to the below Link-

- https://docs.aws.amazon.com/apigateway/latest/developerguide/stage-variables.html

Question 15

An organization deployed its static website on Amazon S3. Now, the Developer has a requirement to serve dynamic content using a serverless solution. Which combination of services should be used to implement a serverless application for the dynamic content? (Select TWO)

- A. Amazon API Gatewayright
- B. Amazon EC2
- C. AWS ECS

- D. AWS Lambdaright
- E. Amazon kinesis

Explanation:

Correct Answer – A and D
Out of the above list, Given the scenario, API Gateway and AWS Lambda are the best two choices to build this serverless application.

AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume - there is no charge when your code is not running.

For more information on AWS Lambda, please refer to the below Link-

- https://aws.amazon.com/lambda/

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.

For more information on the API gateway, please refer to the below Link-

- https://aws.amazon.com/api-gateway/

Option B is incorrect because EC2 is not a serverless offering. To use serverless compute on Cloud, you can use Lambda.
Option C is incorrect because ECS is primarily used for hosting containers, not suitable for the requirement provided in the question.
Option E is incorrect because Kinesis Data Streams is a scalable and durable real-time data streaming service that can continuously capture gigabytes of data per second from hundreds of thousands of sources. It is not required in this scenario.

Question 16

An application is publishing a custom CloudWatch metric any time an HTTP 504 error appears in the application error logs. These errors are being received intermittently. There is a CloudWatch Alarm for this metric, and the Developer would like the alarm to trigger ONLY if it breaches two evaluation periods or more.

What should be done to meet these requirements?

- A. Update the CloudWatch Alarm to send a custom notification depending on results.
- B. Publish the value zero whenever there are no “HTTP 504” errors.
- C. Use high – resolution metrics to get data pushed to CloudWatch more frequently.
- D. The evaluation period and Data Points to Alarm should be set to 2 while creating this alarm.right

Explanation:

Answer – D

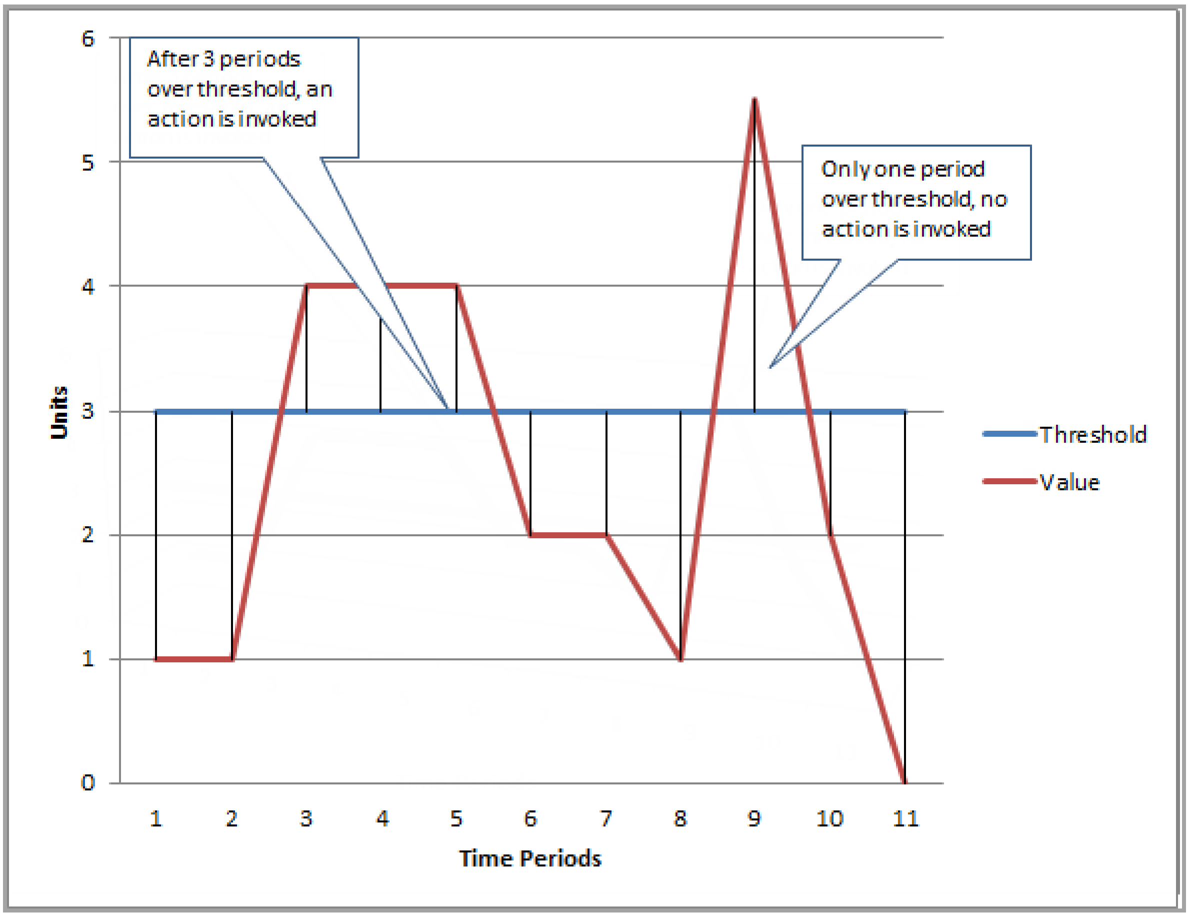
Our scenario states that we are receiving HTTP Error 504 intermittently. The scenario requires that the ALARM should trigger ONLY if it breaches 2 evaluation periods.

None of the options listed is a good choice.

When you create an alarm, you specify three settings to enable CloudWatch to evaluate when to change the alarm state:

- Period is the length of time to evaluate the metric to create each individual data point for a metric. It is expressed in seconds. If you choose one minute as the period, there is one data point every minute.
- Evaluation Period is the number of the most recent data points to evaluate when determining alarm state.
- Datapoints to Alarm is the number of data points within the evaluation period that must be breached to cause the alarm to go to the *ALARM* state. The breaching data points do not have to be consecutive. They must all be within the last number of data points equal to the Evaluation Period.

Let us look at an example.
In the following figure, the alarm threshold is set to three units. The alarm is configured to go to the ***ALARM*** state, and both Evaluation Period and Datapoints to Alarm are 3. That is, when all three data points in the most recent three consecutive periods are above the threshold, the alarm goes to the ***ALARM*** state. In the figure, this happens in the third through fifth time periods. At period six, the value dips below the threshold, so one of the periods being evaluated is not breaching, and the alarm state changes to ***OK***. During the ninth time period, the threshold is breached again, but for only one period. Consequently, the alarm state remains ***OK***.



Option A is incorrect since here there is no mention of any special kind of notification.

Option B is incorrect since you don't need to mention a 0 value. Place a 1 value when the result is received.

Option C is incorrect since there is no mention of the frequency, so we don't know if we need high resolution for metrics.

For more information on the aggregation of data in Cloudwatch, please refer to the below Link-

- https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Agent-common-scenarios.html#CloudWatch-Agent-aggregating-metrics

Question 17

A Developer has been asked to create an AWS Elastic Beanstalk environment for a production web application that needs to handle thousands of requests. Currently, the dev environment is running on a t1.micro instance.

What is the best way for the developer to provision a new production environment with a m4.large instance instead of a t1.micro?

- A. Use CloudFormation to migrate the Amazon EC2 instance type from t1.micro to m4.large.
- B. Create a new configuration file with the instance type as m4.large and reference this file when provisioning the new environment.right
- C. Provision a m4.large instance directly in the dev environment and deploy to the new production environment.
- D. Change the instance type value in the configurations file to m4.large by using the update autoscaling group CLI command.

Explanation:

Answer – B

The Elastic Beanstalk console and EB CLI set configuration options when you create an environment. You can also set configuration options in saved configurations and configuration files. If the same option is set in multiple locations, the value used is determined by order of precedence.
Configuration option settings can be composed in text format and saved before environment creation, applied during environment creation using any supported client, and added, modified, or removed after environment creation.

During environment creation, configuration options are applied from multiple sources with the following precedence, from highest to lowest:

- Settings applied directly to the environment – Settings specified during a create environment or update environment operation on the Elastic Beanstalk API by any client, including the AWS Management Console, EB CLI, AWS CLI, and SDKs. The AWS Management Console and EB CLI also apply recommended values for some options that apply at this level unless overridden.
- Saved Configurations – Settings for any options that are not applied directly to the environment are loaded from a saved configuration, if specified.
- Configuration Files (.ebextensions) – Settings for any options that are not applied directly to the environment and not specified in a saved configuration are loaded from configuration files in the *.ebextensions* folder at the root of the application source bundle.

Configuration files are executed in alphabetical order. For example, ***.ebextensions/01run.config*** is executed before ***.ebextensions/02do.config***.

- Default Values – If a configuration option has a default value, it only applies when the option is not set at any of the above levels.

If the same configuration option is defined in more than one location, the setting with the highest precedence is applied. When a setting is applied from a saved configuration or settings applied directly to the environment, the setting is stored as part of the environment's configuration. These settings can be removed with the AWS CLI or with the EB CLI.

.

Settings in configuration files are not applied directly to the environment and cannot be removed without modifying the configuration files and deploying a new application version. If a setting applied with one of the other methods is removed, the same setting will be loaded from configuration files in the source bundle.

- Option A is incorrect since the Elastic Beanstalk service already manages the environment, and we don't need Cloudformation for this.

- Option C is incorrect since the changes need to be done for the current configuration.

- For more information on making this change, please refer to the below Link-
  - https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.managing.ec2.html

Question 18

An organization has an Amazon Aurora RDS instance that handles all of its AWS-based e-commerce activity. The application accessing the database needs to create large sales reports on an hourly basis, running 15 minutes after the hour. This reporting activity is slowing down the e-commerce application.

Which combination of actions should be taken to reduce the impact on the main e-commerce application? Select 2 answers from the options given below.

- A. Point the reporting application to the read replica.right
- B. Migrate the data to a set of highly available Amazon EC2 instances.
- C. Use SQS Buffering to retrieve data for reports.
- D. Create a read replica of the database.right
- E. Create an SQS queue to implement SQS Buffering.

Explanation:

Answer – A and D

The AWS Documentation mentions the following.

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.

Option B is incorrect, since the AWS RDS service already has features to support the requirement.

Options C and E are incorrect since using SQS would be inefficient.

For more information on AWS Read Replica's, please refer to the below Link-

- https://aws.amazon.com/rds/details/read-replicas/

Question 19

An organization is using AWS Elastic Beanstalk for a web application. The Developer needs to configure the Elastic Beanstalk environment with deployment methods to create new instances and deploy code to those instances.

Which methods will deploy code ONLY to new instances? Choose 2 answers from the options given below.

- A. All at once deployment
- B. Immutable deploymentright
- C. Rolling deployment
- D. Linear deployment
- E. Blue/Green deploymentright

Explanation:

Answer – B and E

The AWS Documentation mentions the following.

Immutable deployments perform an immutable update to launch a full set of new instances running the new version of the application in a separate Auto Scaling group, alongside the instances running the old version. Immutable deployments can prevent issues caused by partially completed rolling deployments. If the new instances don't pass health checks, Elastic Beanstalk terminates them, leaving the original instances untouched.
And with Blue Green deployments, you can have a separate deployment environment as well.

Option A is incorrect because All at once deployment deploys the new version to all instances simultaneously. All instances in your environment are out of service for a short time while the deployment occurs.

Option C is incorrect because Rolling deployment deploys the new version in batches. Each batch is taken out of service during the deployment phase, reducing your environment's capacity by the number of instances in a batch.

Option D is incorrect because there is no Linear deployments.

For more information on Deployment options, please refer to the below Links-

- https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.rolling-version-deploy.html
- https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html

Question 20

A developer is writing an application that will store data in a DynamoDB table. The ratio of reads operations to write operations will be 1000 to 1, with the same data being accessed frequently.

What should the Developer enable on the DynamoDB table to optimize performance and minimize costs?

- A. Amazon DynamoDB auto scaling
- B. Amazon DynamoDB cross-region replication
- C. Amazon DynamoDB Streams
- D. Amazon DynamoDB Acceleratorright

Explanation:

Answer – D

The AWS Documentation mentions the following.

DAX is a DynamoDB-compatible caching service that enables you to benefit from fast in-memory performance for demanding applications. DAX addresses three core scenarios:

1. As an in-memory cache, DAX reduces the response times of eventually-consistent read workloads by order of magnitude, from single-digit milliseconds to microseconds.

2. DAX reduces operational and application complexity by providing a managed service that is API-compatible with Amazon DynamoDB and requires only minimal functional changes to use with an existing application.

3. For read-heavy or bursty workloads, DAX provides increased throughput and potential operational cost savings by reducing the need to over-provision read capacity units. This is especially beneficial for applications that require repeated reads for individual keys.

Option A is incorrect since this is good when you have unpredictable workloads.

Option B is incorrect since this is good for disaster recovery scenarios.

Option C is incorrect since this is good to stream data to other sources.

For more information on DynamoDB Accelerator, please refer to the below Link-

- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.html

Question 21

You are using AWS SAM templates to deploy a serverless application. Which of the following resource will embed nested applications from Amazon S3 buckets?

- A. AWS::Serverless::API
- B. AWS::Serverless::Applicationright
- C. AWS::Serverless::LayerVersion
- D. AWS::Serverless::Function

Explanation:

Correct Answer – B

AWS::Serverless::Application resource in AWS SAM template is used to embed application from Amazon S3 buckets.

Option A is incorrect as AWS::Serverless::API is used for creating API Gateway resources & methods that can be invoked through HTTPS endpoints.

Option C is incorrect as AWS::Serverless::LayerVersion resource type creates Lambda layered function.

Option D is incorrect as AWS::Serverless::Function resource describes the configuration for creating Lambda function.

For more information on using AWS SAM templates, refer to the following URLs-

https://aws.amazon.com/blogs/compute/announcing-nested-applications-for-aws-sam-and-the-aws-serverless-application-repository/
https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/serverless-sam-template.html

Question 22

You are a developer that has recently been hired for your API expertise. The company is currently using API Gateway services for development. You need to control the behavior of an API’s front-end interactions. Which of the following could be done to achieve this? (Select TWO.)

- A. Modify the configuration of the Method request.right
- B. Modify the configuration of the Integration request.

- C. Modify the configuration of the Method response.right
- D. Modify the configuration of the Integration response.

Explanation:

Answer – A and C

This is also mentioned in the AWS Documentation.

As an API developer, you control the behaviors of your API's frontend interactions by configuring the method request and a method response. You control the behaviors of your API's backend interactions by setting up the integration request and integration response. These involve data mappings between a method and its corresponding integration.

Options B and D are incorrect since these are used to control the behaviors of your API's backend interactions.

For more information on creating an API via the gateway, please refer to the below Link-

- https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-create-api-from-example-console.html

Question 23

You’re developing an AWS Lambda function that is interacting with a DynamoDB table. The function was working well, but now it is giving the results with a time delay. You need to debug the code to understand where the bottleneck is which is causing the performance issue. Which of the following is the ideal way to debug the code?

- A. Use Log statements in the code to detect the delay.

- B. Use Cloudwatch logs to detect where the delay could be.

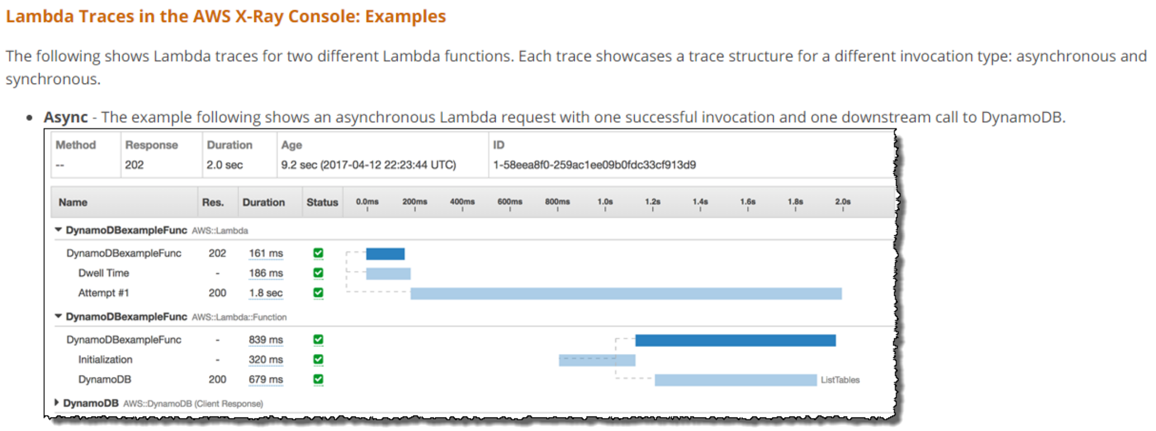
- C. Look at the throttling errors in Cloudwatch metrics.

- D. Use AWS X-Ray to see where the downstream delay could be.right

Explanation:

Answer – D

With AWS X-Ray, you can actually see traces in your AWS Lambda function, allowing you to see a detailed level of tracing to your downstream services. The below snapshot from the AWS documentation shows an example of this.



Lambda Traces in the AWS X-Ray Console: Examples

The following shows Lambda traces for two different Lambda functions. Each trace showcases a trace structure for a different invocation type: asynchronous and synchronous.

- **Async** - The example following shows an asynchronous Lambda request with one successful invocation and one downstream call to DynamoDB.

Method	Response	Duration	Age	ID
--	202	2.0 sec	9.2 sec (2017-04-12 22:23:44 UTC)	1-58eea8f0-259ac1ee09b0fdc33cf913d9

Name	Res.	Duration	Status
DynamoDBexampleFunc AWS::Lambda			
DynamoDBexampleFunc	202	161 ms	✓
Dwell Time	-	186 ms	✓
Attempt #1	200	1.8 sec	✓
DynamoDBexampleFunc AWS::Lambda::Function			
DynamoDBexampleFunc	-	839 ms	✓
Initialization	-	320 ms	✓
DynamoDB	200	679 ms	✓
DynamoDB AWS::DynamoDB (Client Response)			

Option A is incorrect since this is not an efficient way to check for performance errors.

Option B is incorrect since the logs might not be able to give you that level of tracing to detect the error.

Option C is incorrect since throttling errors will not give you the cause of the performance issue.

For more information on using AWS Lambda with X-Ray, please refer to the below Link-

- https://docs.aws.amazon.com/lambda/latest/dg/lambda-x-ray.html

Question 24

A company is planning on using AWS CodePipeline for their underlying CI/CD process. The code will be picked up from an S3 bucket. The company policy mandates that all data should be encrypted at rest and that the keys are managed by the customer. Which of the following measures would you take to ensure that the CI/CD process conforms to this policy? Choose 2 possible actions from the options given below.

- A. Ensure that server-side encryption is enabled on the S3 bucket and data is encrypted at-rest on the CodeBuild environment using customer-managed CMK.right
- B. Ensure that server-side encryption is enabled on the CodePipeline stage.
- C. Configure the code pickup stage in CodePipeline to use AWS KMS.
- D. Configure AWS KMS with customer managed keys and use it for S3 bucket encryption.right

Explanation:

Answer – A and D

This is also mentioned in the AWS Documentation.

There are two ways to configure server-side encryption for Amazon S3 artifacts.

- AWS CodePipeline creates an Amazon S3 artifact bucket and default AWS-managed SSE-KMS encryption keys when creating a pipeline using the Create Pipeline wizard. The master key is encrypted along with object data and managed by AWS.

- You can create and manage your own customer-managed SSE-KMS keys.

Options B and C are incorrect since this needs to be configured at the S3 bucket level.

For more information on Encryption in S3 with CodePipeline, please refer to the below Link-

- https://docs.aws.amazon.com/codepipeline/latest/userguide/S3-artifact-encryption.html

Question 25

An application hosted in AWS has been configured to use a DynamoDB table. Several items are written to the DynamoDB table. As a part of an archival strategy, these items will be accessible in a particular time frame, after which they can be archived & deleted. Which of the following is an ideal way to manage the deletion of the stale items?

- A. Perform a scan on the table for the stale items and issue the Delete operation.
- B. Create an additional column to store the date. Perform a query for the stale objects and then perform the Delete operation.
- C. Enable versioning for the items in DynamoDB and delete the last accessed version.
- D. Enable TTL for the items in DynamoDB.right

Explanation:

Answer – D
The AWS Documentation mentions the following.

Time To Live (TTL) for DynamoDB allows you to define when items in a table expire so that they can be automatically deleted from the database.

TTL is provided at no extra cost as a way to reduce storage usage and reduce the cost of storing irrelevant data without using provisioned throughput. With TTL enabled on a table, you can set a timestamp for deletion on a per-item basis, allowing you to limit storage usage to only those records that are relevant.

Options A and B are incorrect since these would not be cost-effective and have a performance issue on the underlying DynamoDB table.
Option C is incorrect since versioning is not possible in DynamoDB.
For more information on Time to Live for items in DynamoDB, please refer to the below Link-

- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html

Question 26

You are using AWS Envelope Encryption to encrypt all of your sensitive data. Which of the following is true with regards to the AWS Envelope Encryption service?

- A. First, the data is encrypted using an encrypted Data Key. The encrypted Data Key is then further encrypted using an encrypted Master Key.
- B. First, the data is encrypted using a plaintext Data Key. The Data Key is then further encrypted using an encrypted Master Key.
- C. First, the data is encrypted using an encrypted Data Key. The encrypted Data Key is then further encrypted using a plaintext Master Key.
- D. First, the data is encrypted using a plaintext Data Key. The Data Key is then further encrypted using a plaintext Master Key.right

Explanation:

Correct Answer – D

With Envelope Encryption, unencrypted data is encrypted using a plaintext Data key. This Data key is further encrypted using a plaintext Master key. This plaintext Master key is securely stored in AWS KMS & known as Customer Master Keys.

- Option A is incorrect as the Data Key used for encryption of data is plaintext along with the Master key used to encrypt Data Keys.

- Option B is incorrect as the Master key used to encrypt Data Keys is in plaintext format.

- Option C is incorrect as the Data Key used for encryption of data is in plaintext format.

- For more information on AWS KMS Envelope Encryption, refer to the following URL-
    - https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html

Question 27

Your team has been instructed to deploy a Microservices and an ETL based application onto AWS. There is a requirement to manage the containerization of the application using Docker. Which of the following would the ideal way to implement this with the least amount of administrative effort?

- A. Use AWS OpsWorks

- B. Use the Elastic Container Service.right
- C. Deploy Kubernetes on EC2 Instances.

- D. Use the CloudFormation service.

Explanation:

Answer – B

The Elastic Container Service is a fully managed container orchestration service available in AWS.

The AWS Documentation mentions the following.

Amazon Elastic Container Service (Amazon ECS) is a highly scalable, high-performance container orchestration service that supports Docker containers. It allows you to run and scale containerized applications on AWS easily. Amazon ECS eliminates the need for you to install and operate your own container orchestration software, manage and scale a cluster of virtual machines, or schedule containers on those virtual machines.

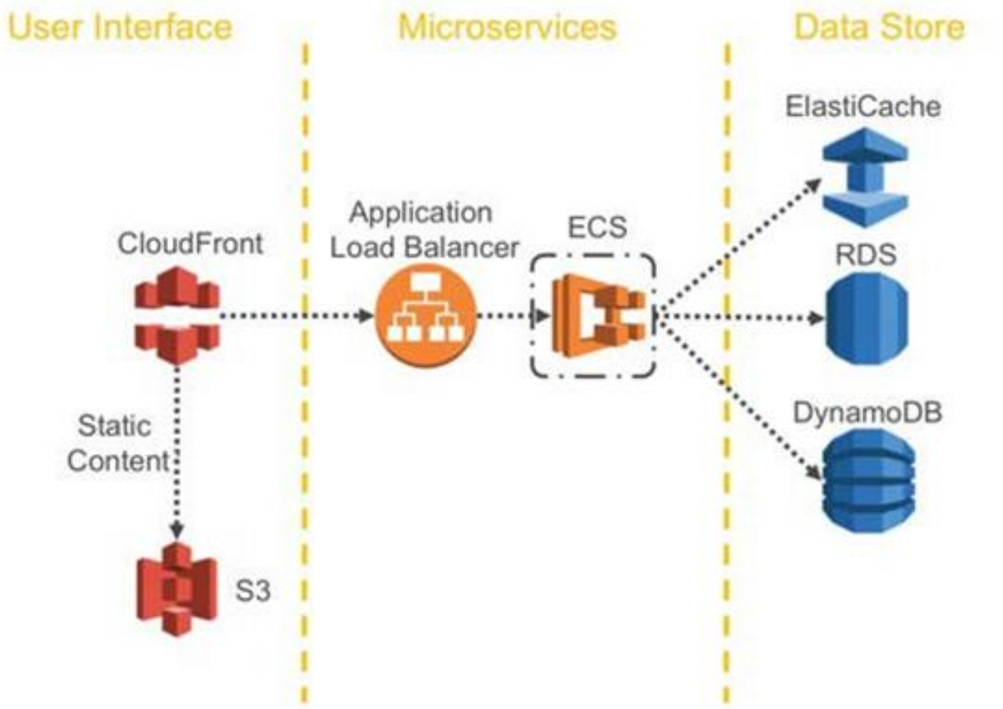
- Option A is incorrect because AWS OpsWorks helps to configure and operate applications in a cloud enterprise by using Puppet or Chef, which is not required in the question.

- Option C is incorrect since even though Kubernetes is a fully managed solution, hosting it on EC2 Instances will incur more administrative headache.

- Option D is incorrect because AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources. But it does not manage the Docker containers like ECS.

- For more information on Amazon ECS, please refer to the below Link-
    - https://aws.amazon.com/ecs/

The following diagram illustrates an architectural implementation of microservices on AWS.



The API of a microservice is the central entry point for all client requests. The application logic hides behind a set of programmatic interfaces, typically a RESTful web services API. This API accepts and processes calls from clients and might implement functionality such as traffic management, request filtering, routing, caching, and authentication and authorization.
Many AWS customers use the Elastic Load Balancing (ELB) Application Load Balancer together with Amazon EC2 Container Service (Amazon ECS) and Auto Scaling to implement a microservices application. The Application Load Balancer routes traffic based on advanced application-level information that includes the content of the request.

- For more information, please refer to:
  - https://docs.aws.amazon.com/aws-technical-content/latest/microservices-on-aws/simple-microservices-architecture-on-aws.html

Question 28

You are developing a banking application that will interact with a DynamoDB table. The table is going to take in a lot of read and write operations. Which of the following would be the ideal partition key for the DynamoDB table to ensure ideal performance?

- A. CustomerIDright
- B. CustomerName
- C. Location
- D. Age

Explanation:

Answer - A
The AWS Documentation gives the ideal way to construct partition Keys.

Recommendations for partition keys

Use high-cardinality attributes. These attributes have distinct values for each item, like e-mailid, employee_no, customerid, sessionid, orderid, and so on.
Use composite attributes. Try to combine more than one attribute to form a unique key, if that meets your access pattern. For example, consider an orders table with customerid+productid+countrycode as the partition key and order_date as the sort key.
Option B is incorrect because CustomerName may be the same.
Option C is incorrect because some customers can have the same location.
Option D is incorrect because Age can be the same for customers.
For more information on choosing the right partition Key, please refer to the below Link-

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

Question 29

You are developing an application that will be comprised of the following architecture -

1. A set of EC2 instances to process the messages.

2. These (EC2 instances) will be spun up by an Autoscaling group.

3. SQS Queues to maintain the processing messages.

4. There will be 2 pricing tiers.

How will you ensure that the premium customers' messages are given more preference?

- A. Create 2 Autoscaling Groups, one for normal and one for premium customers.

- B. Create 2 sets of EC2 Instances, one for normal and one for premium customers.

- C. Create 2 SQS queues, one for normal and one for premium customers.right
- D. Create 2 Elastic Load Balancers, one for normal and one for premium customers.

Explanation:

Answer – C

The ideal option would be to create 2 SQS queues. Messages can then be processed by the application from the high priority queue first.

Option A is incorrect because 2 Auto Scaling groups will still launch the same set of EC2 instances that are defined in the Launch Configuration/Template.

Option B is incorrect because launching 2 sets of EC2 instances involves lots of manual work.

Option D is incorrect because having 2 ELB will still require a different set of EC2 instances.

For more information on SQS, please refer to the below Link-

- https://aws.amazon.com/sqs/

Question 30

A software engineer is developing an application in AWS using AWS SDK. You need a mechanism implemented in the AWS SDK to deal with "re-trying" the errors. Which of the following mechanisms is suitable?

- A. Multiple SQS queues

- B. Exponential backoff algorithmright

- C. For-loop operations

- D. Amazon SNS notifications.

Explanation:

Answer – B

The AWS Documentation mentions the following.

Each AWS SDK implements automatic retry logic. If you're not using an AWS SDK, you should retry original requests that receive server (5xx) or throttling errors. However, client errors (4xx) indicate that you need to revise the request to correct the problem before trying again.

In addition to simple retries, each AWS SDK implements an exponential backoff algorithm for better flow control. The idea behind exponential backoff is to use progressively longer waits between retries for consecutive error responses. You should implement a maximum delay interval, as well as a maximum number of retries.

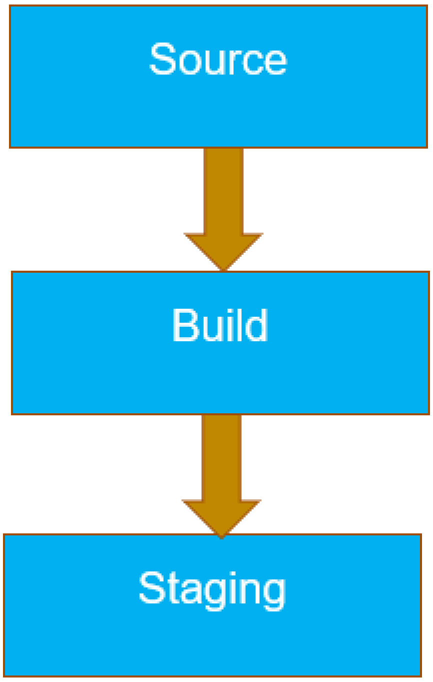
- Option A is incorrect because it is not a mechanism implemented in AWS SDK.
- Option C is incorrect because it does not help to deal with the errors.
- Option D is incorrect because it does not deal with the errors rather it is used notify.

For more information on API retries, please refer to the below Link-

- https://docs.aws.amazon.com/general/latest/gr/api-retries.html

Question 31

You have created the following stages in CodePipeline.



What happens if there is a failure detected in the "Build" stage?

- A. A rollback will happen at the "Source" stage.

- B. The "Build" step will be attempted again.

- C. The "Build" step will be skipped and the "Staging" step will start.

- D. The entire process will halt.right

Explanation:

Answer – D

The AWS Documentation mentions the following.

In AWS CodePipeline, an action is a task performed on an artifact in a stage. If an action or a set of parallel actions is not completed successfully, the pipeline stops running.

Options A, B and C are incorrect since the default action will be that the entire pipeline will be stopped if the build does not succeed.

For more information on Actions retry, please refer to the below Link-

- https://docs.aws.amazon.com/codepipeline/latest/userguide/actions-retry.html

Question 32

Your architect has drawn out the details for a mobile-based application. Below are the key requirements when it comes to authentication.

· Users should have the ability to sign-in using external identities such as Facebook or Google.

· There should be a facility to manage user profiles.

Which of the following would you consider as part of the development process for the application?

- A. Consider using IAM Roles which can be mapped to the individual users.

- B. Consider using User pools in AWS Cognito.right
- C. Consider building the logic into the application.

- D. Consider using SAML federation identities.

Explanation:

Answer – B

The AWS Documentation mentions the following.

User pools provide:

- Sign-up and sign-in services.

- A built-in, customizable web UI to sign in users.

- Social sign-in with Facebook, Google, and log in with Amazon, as well as sign-in with SAML identity providers from your user pool.

- User directory management and user profiles.

- Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification.

- Customized workflows and user migration through AWS Lambda triggers.

Options A and C is incorrect since this would require a lot of effort to develop and maintain.

Option D is incorrect since this is normally used for external directories such as Active Directory.

For more information on user identity pools, please refer to the below Link-

- https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools.html

Question 33

You are using AWS DynamoDB as a database to save sales data for a global appliance company. Which of the following keys can be used to encrypt the DynamoDB data at rest? (Select TWO)

- A. A customer managed keyright
- B. AWS managed CMK (aws/rds)

- C. AWS managed key for DynamoDB (aws/dynamodb)right
- D. AWS managed key for S3 (aws/s3)

Explanation:

Correct Answer – A and C
Encryption at rest protects your DynamoDB tables under an AWS KMS key. By default, DynamoDB uses an **AWS owned** key, a multi-tenant encryption key that is created and managed in a DynamoDB service account. But you can encrypt your DynamoDB tables under a **customer managed** key or the **AWS managed key** for DynamoDB (`aws/dynamodb`) in your AWS account.
For more information on AWS KMS, refer to the following URL-

- https://docs.aws.amazon.com/kms/latest/developerguide/services-dynamodb.html

Question 34

Your company is going to develop an application in .NET Core with DynamoDB. There is a requirement that all data needs to be encrypted at rest. If the DynamoDB table has already been created, what else is needed to achieve this?

- A. No additional configurations are required since server-side encryption is enabled on all DynamoDB table data.right
- B. Enable encryption on the existing table.

- C. You cannot enable encryption at rest. Consider using the AWS RDS service instead.

- D. You cannot enable encryption at rest. Consider using the S3 service instead.

Explanation:

Answer – A

Option B is incorrect since Encryption can only be configured during table creation time.

Options C and D are incorrect since Encryption is possible in DynamoDB.

The AWS Documentation mentions the following.

Amazon DynamoDB offers fully managed encryption at rest. DynamoDB encryption at rest provides enhanced security by encrypting your data at rest using an AWS Key Management Service (AWS KMS) managed encryption key for DynamoDB. This functionality eliminates the operational burden and complexity involved in protecting sensitive data.

For more information on DynamoDB Encryption at rest, please refer to the below Link-

- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/EncryptionAtRest.html

Question 35

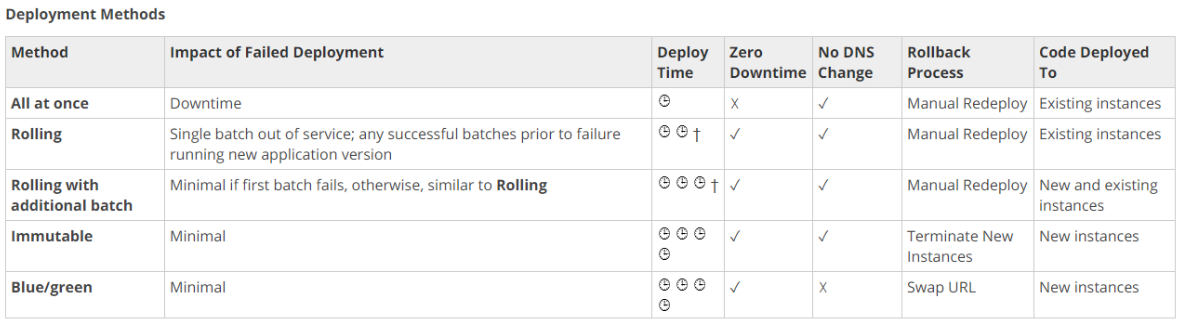
You have been instructed to manage the deployments of an application onto Elastic Beanstalk. Since this is just a development environment, you have been told to ensure that the least amount of time is taken for each deployment. Which of the following deployment mechanism would you consider based on this requirement?

- A. All at onceright
- B. Rolling
- C. Immutable
- D. Rolling with additional batch

Explanation:

Answer - A

Below is the screenshot of the deployment options. The ‘All at once’ is the least deployment option.



Deployment Methods

Method	Impact of Failed Deployment	Deploy Time	Zero Downtime	No DNS Change	Rollback Process	Code Deployed To
All at once	Downtime	🕒	X	✓	Manual Redeploy	Existing instances
Rolling	Single batch out of service; any successful batches prior to failure running new application version	🕒 🕒 †	✓	✓	Manual Redeploy	Existing instances
Rolling with additional batch	Minimal if first batch fails, otherwise, similar to **Rolling**	🕒 🕒 🕒 †	✓	✓	Manual Redeploy	New and existing instances
Immutable	Minimal	🕒 🕒 🕒 🕒	✓	✓	Terminate New Instances	New instances
Blue/green	Minimal	🕒 🕒 🕒 🕒	✓	X	Swap URL	New instances

Based on the above screenshot, all the other options become invalid.

For more information on the deployment options, please refer to the below Link-

- https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.deploy-existing-version.html

Question 36

You’re developing an application onto AWS which is based on the Microservices. These Microservices will be created based on AWS Lambda functions. Because of the complexity of the flow of these different components, you need some way to manage the workflow of execution of these various Lambda functions. How could you manage this effectively now and for the future addition of Lambda functions to the application?

- A. Consider creating a master Lambda function that would coordinate the execution of the other Lambda functions.

- B. Consider creating a separate application hosted on an EC2 Instance which would coordinate the execution of the other Lambda functions.

- C. Consider using Step Functions to coordinate the execution of the other Lambda functions.right
- D. Consider using SQS queues to coordinate the execution of the other Lambda functions.

Explanation:

Answer – C

The best way to manage this is to use Step Functions. The AWS Documentation mentions the following about Step Functions.

AWS Step Functions is a web service that enables you to coordinate the components of distributed applications and microservices using visual workflows. You build applications from individual components that perform a discrete function, or *task*, allowing you to scale and change applications quickly. Step Functions provide a reliable way to coordinate components and step through the functions of your application.
Options A and B are invalid. Even though feasible, it would just bring too much of effort and maintenance into the entire system.

Option D is invalid because this is good in managing the messaging between distributed components of an application.

For more information on Step Functions, please refer to the below Link-

- https://docs.aws.amazon.com/step-functions/latest/dg/welcome.html

Question 37

You are developing an application that will be used to receive data from multiple devices. You need to perform some preprocessing on the data before it can be analyzed by the Analytics tool. All the received data are compressed records that need to be decompressed to be analyzed further. Which of the following can be used to carry out this intermediate activity?

- A. Use Step Functions to pre-process the data.

- B. Use Kinesis with AWS Lambda functions to pre-process the data.right
- C. Use the AWS CloudFront service to pre-process the data.

- D. Use ELB to pre-process the data.

Explanation:

Answer – B
The AWS Documentation mentions the following.

Many customers use Amazon Kinesis to ingest, analyze, and persist their streaming data. One of the easiest ways to gain real-time insights into your streaming data is to use Kinesis Analytics. It enables you to query the data in your stream or build entire streaming applications using SQL. Customers use Kinesis Analytics for things like filtering, aggregation, and anomaly detection.

A data producer is compressing JSON records before sending them to a Kinesis stream or a Kinesis Firehose delivery stream. You want to use Kinesis Analytics to analyze these compressed records. Before you can use SQL to perform the analysis, you must first decompress each input record so that it’s

represented as decompressed JSON. This enables it to map to the schema you've created in the Kinesis Analytics application.
Option A is incorrect since this service is used to coordinate different parts of a distributed application.
Option C is incorrect since this service is used to cache static and dynamic content of a website hosted in AWS Cloud.
Option D is incorrect since CloudFront can not be used to pre-process the data.
For more information on preprocessing data in Kinesis, please refer to the below Link-

- https://aws.amazon.com/blogs/big-data/preprocessing-data-in-amazon-kinesis-analytics-with-aws-lambda/

Question 38

Your team has completed development of an application. Now this application needs to be deployed to run on an EC2 instance. The Application data will be stored on a separate volume which needs to be encrypted at rest. How can you ensure this requirement is met?

- A. Ensure that Encryption is enabled during volume creation time.right
- B. Ensure to use Throughput Optimized HDD to allow for Encryption.
- C. Create a Customer master key in the KMS service.
- D. Create an EBS Encryption Key.

Explanation:

Answer – A

The AWS Documentation mentions the following.

Amazon EBS encryption uses AWS Key Management Service (AWS KMS) customer master keys (CMKs) when creating encrypted volumes and any snapshots created from them. A unique AWS-managed CMK is created for you automatically in each region where you store AWS assets. This key is used for Amazon EBS encryption.

- Option B is incorrect since Encryption is possible on all EBS volume types.
- Option C is incorrect because encryption of an EBS volume can be done without generating a CMK in the console.
- Option D is incorrect since you need to create the Encryption Key in the KMS service.
- For more information on EBS Encryption, please refer to the below Link-
  - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

Question 39

You've been given the requirement to customize the content which is distributed to users via a Cloudfront Distribution with minimal efforts. The content origin is an S3 bucket. How could you achieve this?

- A. Add an event to the S3 bucket. Make the event invoke a Lambda function that would customize the content.
- B. Add a Step Function. Add a step with a Lambda function just before the content gets delivered to the users.
- C. Consider using Lambda@Edge.right
- D. Consider using a separate application on an EC2 Instance for this purpose.

Explanation:

Answer – C

The AWS Documentation mentions the following.

Lambda@Edge is an extension of AWS Lambda, a compute service that lets you execute functions that customize the content that CloudFront delivers. You can author functions in one region and execute them in AWS locations globally closer to the viewer, without provisioning or managing servers. Lambda@Edge scales automatically, from a few requests per day to thousands per second. Processing requests at AWS locations closer to the viewer than on origin servers significantly reduces latency and improves the user experience.

Option A is incorrect because although adding an event to the S3 bucket and then invoking the event by the Lambda function to customize the content may do the needful, a lot of manual intervention is required. With Lambda @ Edge, it can be done more easily.
Option B is incorrect because Step Function is normally used to sequence AWS Lambda functions and multiple AWS services. This scenario is not suitable.
Option D is incorrect because adding EC2 is not cost-efficient and not an easy solution.
For more information on Lambda@Edge, please refer to the below Link-

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-at-the-edge.html

Question 40

Your team has been instructed to develop a completely new solution for AWS. Currently, you have a limitation on the tools available to manage the complete lifecycle of the project. Which of the following service from AWS could help you handle all aspects of development and deployment?

- A. AWS CodePipeline
- B. AWS CodeBuild
- C. AWS CodeCommit
- D. AWS CodeStarright

Explanation:

Answer – D

The AWS Documentation mentions the following.

AWS CodeStar is a cloud-based service for creating, managing, and working with software development projects on AWS. You can quickly develop, build, and deploy applications on AWS with an AWS CodeStar project. An AWS CodeStar project creates and integrates AWS services for your project development toolchain. Depending on your choice of AWS CodeStar project template, that toolchain might include source control, build, deployment, virtual servers or serverless resources, and more. AWS CodeStar also manages the permissions required for project users (called team members). By adding users as team members to an AWS CodeStar project, project owners can quickly grant each team member role-appropriate access to a project and its resources.

Option A is incorrect since this service is used for managing CI/CD pipelines.

Option B is incorrect since this service is used for managing code builds.

Option C is incorrect since this service is used for managing source code versioning repositories.

For more information on AWS CodeStar, please refer to the below Link-

- https://docs.aws.amazon.com/codestar/latest/userguide/welcome.html

Question 41

Your team has just finished developing a new version of an existing application. This is a web-based application hosted on AWS. Currently, Route 53 is being used to point the company’s DNS name to the web site. Your Management has instructed you to deliver the new application to a portion of the users for testing. How can you achieve this?

- A. Port the application onto Elastic beanstalk and use the Swap URL feature.

- B. Use Route 53 weighted Routing policies.right
- C. Port the application onto Opswork by creating a new stack.

- D. Use Route 53 failover Routing policies.

Explanation:

Answer – B

The AWS Documentation mentions the following to support this.

Weighted Routing
Weighted routing lets you associate multiple resources with a single domain name (example.com) or subdomain name (acme.example.com) and choose how much traffic is routed to each resource. This can be useful for various purposes, including load balancing and testing new versions of software.

To configure weighted routing, you create records that have the same name and type for each of your resources. You assign each record a relative weight that corresponds with how much traffic you want to send to each resource. Amazon Route 53 sends traffic to a resource based on the weight that you assign to the record as a proportion of the total weight for all records in the group:

Formula for how much traffic is routed to a given resource:

weight for a specified record/sum of the weights for all records.

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 1/256th of the traffic (1/1+255), and the other resource gets 255/256ths (255/1+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.

Options A and C is incorrect since this would cause a full flown deployment of the new app and is just a maintenance overhead to port the application to a new service environment.

Option D is incorrect since this should only be used for failover conditions.

For more information on the weighted routing policy, please refer to the below Link-

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

Question 42

Your AWS Lambda function writes to an S3 bucket. Which of the following is the best practice to pass operational parameters, such as the bucket name, to your Lambda function?

- A. Configure Amazon S3 bucket name with AWS Lambda Environment Variables.right
- B. Hard Code Amazon S3 bucket name to Lambda Function.

- C. Configure Amazon S3 bucket name with AWS Lambda Function Variables.

- D. Configure an Alias with Amazon S3 bucket name & pass it to Lambda Function.

Explanation:

Correct Answer – A

For Lambda functions, Environment variables can be enabled to dynamically pass settings to function code and libraries without making changes to your code. Environment variables are key-value pairs that are created as a part of function configuration. Instead of hard coding the S3 bucket name in the Lambda function, it can pass as an environmental variable in the above requirement.

- Option B is incorrect as Hard coding the S3 Bucket name in a Lambda function is not a best practice.
- Option C is incorrect as Function Variables enable one or more Lambda functions to be published while environmental variables allow to pass settings to function codes dynamically. In the above case, the S3 bucket name needs to be passed to function codes.
- Option D is incorrect as this is not a correct way of passing the S3 bucket name to a Lambda function.

- For more information on AWS Lambda Environment Variables, refer to the following URL-
  - https://docs.aws.amazon.com/lambda/latest/dg/best-practices.html

Question 43

You have a number of Lambda functions that need to be deployed using AWS CodeDeploy. The lambda functions have gone through multiple code revisions, and versioning in Lambda is being used to maintain the revisions. Which of the following must be done to ensure that the right version of the function is deployed in AWS CodeDeploy?

- A. Specify the version to be deployed in the AppSpec file.right
- B. Specify the version to be deployed in the BuildSpec file.
- C. Create a Lambda function environment variable called ‘VER’ and mention the version that needs to be deployed.
- D. Create an ALIAS for the Lambda function. Mark this as the recent version. Use this ALIAS in CodeDeploy.

Explanation:

Answer - A

The AWS Documentation mentions the following.

If your application uses the AWS Lambda compute platform, the AppSpec file can be formatted with either YAML or JSON. It can also be typed directly into an editor in the console. The AppSpec file is used to specify.

- The AWS Lambda function version to deploy.
- The functions to be used as validation tests.

Option B is incorrect because you cannot specify the version in the BuildSpec file, as it is a collection of build commands and related settings, in YAML format, that CodeBuild uses to run a build.

Option C and D are incorrect because both options do not mention how to use the variable or alias of the Lambda function. The CodeDeploy AppSpec file should be used to specify the Lambda function version. Option A is more accurate.

For more information on the application specification files, please refer to the below Link-

- https://docs.aws.amazon.com/codedeploy/latest/userguide/application-specification-files.html

Question 44

You’ve been hired to develop a gaming application for a large company. The application will be developed using AWS resources. You need to ensure that the right services are used during the development and subsequent deployment of the application. Which of the following would you consider incorporating to ensure leaderboards can be maintained accurately in the application?

- A. AWS ElasticBeanstalk

- B. AWS ElastiCache – Redisright
- C. AWS ElastiCache – Memcached

- D. AWS Opswork

Explanation:

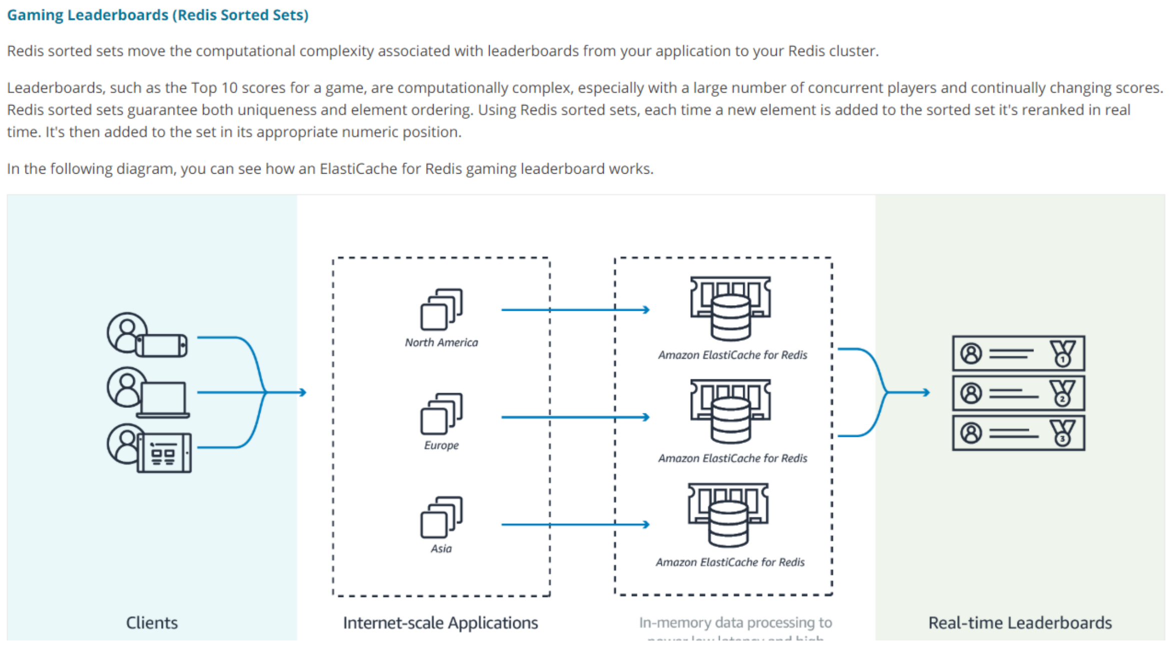
Answer - B

The AWS Documentation mentions the following as one of the key advantages of using AWS Redis ElastiCache.

Gaming Leaderboards (Redis Sorted Sets)
Redis sorted sets move the computational complexity associated with leaderboards from your application to your Redis cluster.

Leaderboards, such as the Top 10 scores for a game, are computationally complex, especially with a large number of concurrent players and continually changing scores. Redis sorted sets guarantee both uniqueness and element ordering. Using Redis sorted sets, each time a new element is added to the sorted set, it's reranked in real-time. It's then added to the set in its appropriate numeric position.

In the following diagram, you can see how an ElastiCache for Redis gaming leaderboard works.



Gaming Leaderboards (Redis Sorted Sets)

Redis sorted sets move the computational complexity associated with leaderboards from your application to your Redis cluster.

Leaderboards, such as the Top 10 scores for a game, are computationally complex, especially with a large number of concurrent players and continually changing scores. Redis sorted sets guarantee both uniqueness and element ordering. Using Redis sorted sets, each time a new element is added to the sorted set it's reranked in real time. It's then added to the set in its appropriate numeric position.

In the following diagram, you can see how an ElastiCache for Redis gaming leaderboard works.

North America
Europe
Asia
Amazon ElastiCache for Redis
Amazon ElastiCache for Redis
Amazon ElastiCache for Redis
Clients
Internet-scale Applications
In-memory data processing to
power low-latency and high
Real-time Leaderboards

Option A and D are incorrect because both Elastic BeanStalk and OpsWorks are orchestration services offered by Amazon Web Services for deploying applications. They do not provide the service required in the question.

Option C is incorrect because Redis provides more features than Memcached, such as backup and restore. Option B is better. For the differences between Memcached and Redis, please check https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/SelectEngine.html.
For more information on AWS ElastiCache Redis, please refer to the below Link-

- https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/elasticache-use-cases.html#elasticache-for-redis-use-cases

Question 45

You have a serverless application with AWS Lambda. This application has Lambda as a backend and has its data stored in DynamoDB. This application is very latency-sensitive. How could you alert your team if the application gets high latency in any of its components?

- A. Import the time library in the Lambda code. Calculate how much time it takes the Lambda to finish operations in DynamoDB, deploy these logs to Cloudwatch and create an alarm if the time in the logs is high.

- B. Enable X-Ray tracing on Lambda, use the AWS SDK inside Lambda code to monitor DynamoDB API calls in X-Ray, send this information to CloudWatch, and create a metric that triggers an SNS alert if the response times get too high.right
- C. Enable X-Ray tracing on Lambda, use the AWS SDK inside Lambda code to monitor DynamoDB API calls in X-Ray, send this information to CloudTrail, and create a metric that triggers an SNS alert if the response times get too high.

- D. Enable X-Ray in Lambda and DynamoDB. Create a Lambda that will retrieve the info from X-Ray every minute. Send this information to CloudWatch, create a metric that triggers an SNS alert if the response times get too high.

Explanation:

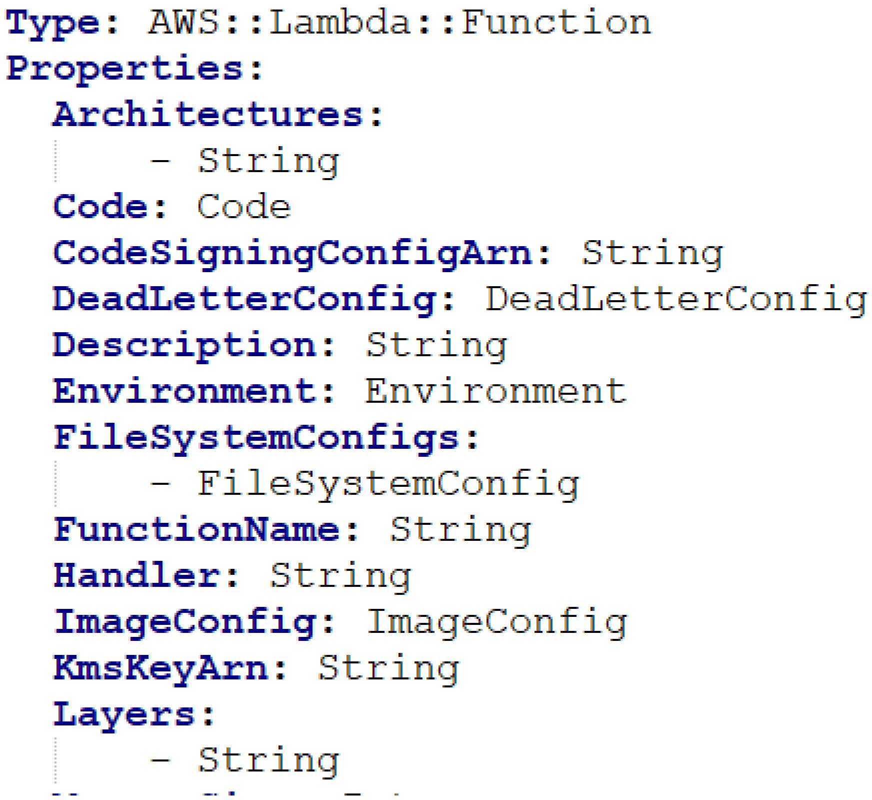
Correct Answer: B

- Option A is incorrect because this option considers how long it takes Lambda to establish a connection, perform operations in DynamoDB and return a response, in this question we only want to know how long it takes to connect with DynamoDB. Additionally, more factors can affect the performance of the Lambda, for instance, cold starts, code optimization, or CPU memory.
- Option B is CORRECT because AWS X-Ray allows you to record every call to the other AWS service like DynamoDB and trace the latency for AWS services. Mixing X-Ray with CloudWatch is a very good choice to get alarms if the latency becomes high.
- Option C is incorrect because with AWS CloudTrail you can track the API requests made by IAM users or services, Cloudtrail is not used to send alerts or to process logs.
- Option D is incorrect because until now, it is not possible to enable AWS X-Ray in DynamoDB. You can only track the traces generated by calls to DynamoDB in Lambda with the AWS SDK.

Question 46

You are using S3 buckets to store images. These S3 buckets invoke a lambda function on upload. The Lambda function creates thumbnails of the images and stores them in another S3 bucket. An AWS CloudFormation template is used to create the Lambda function with the resource "AWS::Lambda::Function". Which of the following attributes is the method name that Lambda calls to execute the function?

Sample CloudFormation template:



```
Type: AWS::Lambda::Function
Properties:
  Architectures:
      - String
  Code: Code
  CodeSigningConfigArn: String
  DeadLetterConfig: DeadLetterConfig
  Description: String
  Environment: Environment
  FileSystemConfigs:
      - FileSystemConfig
  FunctionName: String
  Handler: String
  ImageConfig: ImageConfig
  KmsKeyArn: String
  Layers:
      - String
```

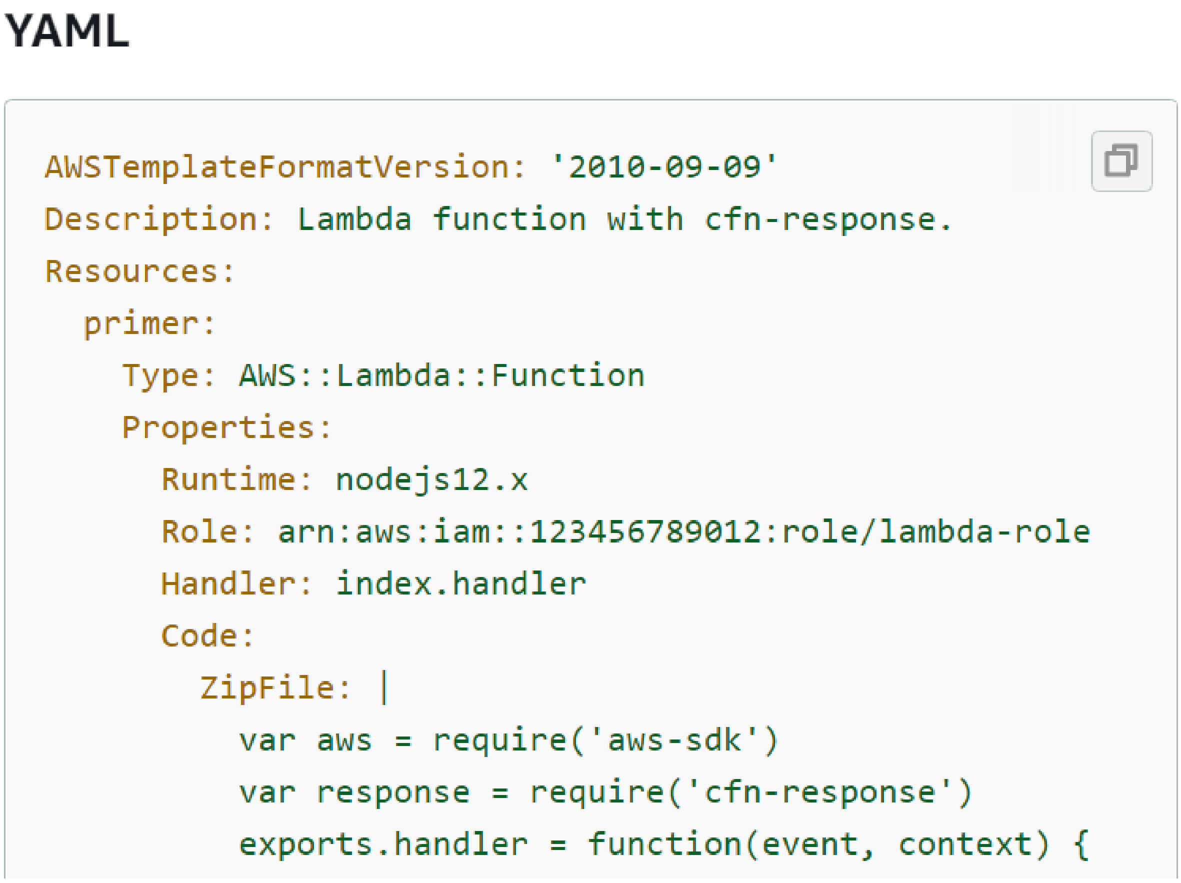
- A. FunctionName
- B. Layers
- C. Environment
- D. Handlerright

Explanation:

Correct Answer – D

The handler is the name of the method within a code that Lambda calls to execute the function.

- Option A is incorrect as the version number changes when the functions are "published", so FunctionName is incorrect.
- Option B is incorrect as it's a list of function layers added to the Lambda function execution environment.
- Option C is incorrect as these are variables that are accessible during Lambda function execution.



YAML

```yaml
AWSTemplateFormatVersion: '2010-09-09'
Description: Lambda function with cfn-response.
Resources:
  primer:
    Type: AWS::Lambda::Function
    Properties:
      Runtime: nodejs12.x
      Role: arn:aws:iam::123456789012:role/lambda-role
      Handler: index.handler
      Code:
        ZipFile: |
          var aws = require('aws-sdk')
          var response = require('cfn-response')
          exports.handler = function(event, context) {
```

For more information on declaring Lambda Function in AWS CloudFormation Template, refer to the following URL-

- https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-lambda-function.html

Question 47

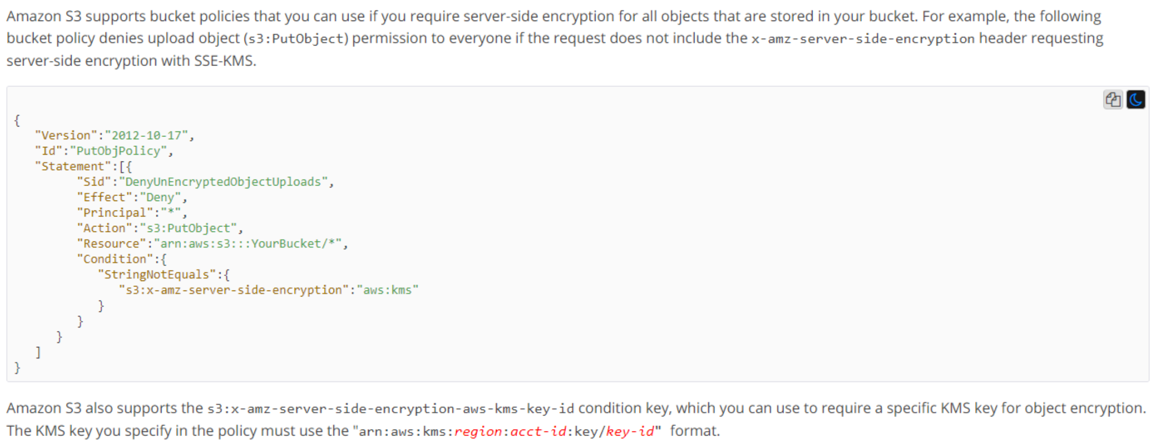
You’ve been asked to develop an application on the AWS Cloud. The application will be used to store confidential documents in an S3 bucket. You need to ensure that the bucket is defined in such a way that it does not accept objects that are not encrypted.

- A. Ensure a condition is set in the bucket policy.right
- B. Ensure that a condition is set in an IAM policy.
- C. Enable MFA for the underlying bucket.
- D. Enable CORS for the underlying bucket.

Explanation:

Answer – A

The AWS Documentation gives an example on the same.



Amazon S3 supports bucket policies that you can use if you require server-side encryption for all objects that are stored in your bucket. For example, the following bucket policy denies upload object (`s3:PutObject`) permission to everyone if the request does not include the `x-amz-server-side-encryption` header requesting server-side encryption with SSE-KMS.

```
{
   "Version":"2012-10-17",
   "Id":"PutObjPolicy",
   "Statement":[{
         "Sid":"DenyUnEncryptedObjectUploads",
         "Effect":"Deny",
         "Principal":"*",
         "Action":"s3:PutObject",
         "Resource":"arn:aws:s3:::YourBucket/*",
         "Condition":{
            "StringNotEquals":{
               "s3:x-amz-server-side-encryption":"aws:kms"
            }
         }
      }
   ]
}
```

Amazon S3 also supports the `s3:x-amz-server-side-encryption-aws-kms-key-id` condition key, which you can use to require a specific KMS key for object encryption. The KMS key you specify in the policy must use the "`arn:aws:kms:`*`region`*`:`*`acct-id`*`:key/`*`key-id`*" format.

Option B is incorrect since the condition needs to be put in the Bucket policy.

Option C is incorrect since this is only used for MFA Delete for accidental deletion of objects.

Option D is incorrect since CORS is only used for cross-domain access.

For more information on using KMS Encryption for S3, please refer to the below link-

- https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

Question 48

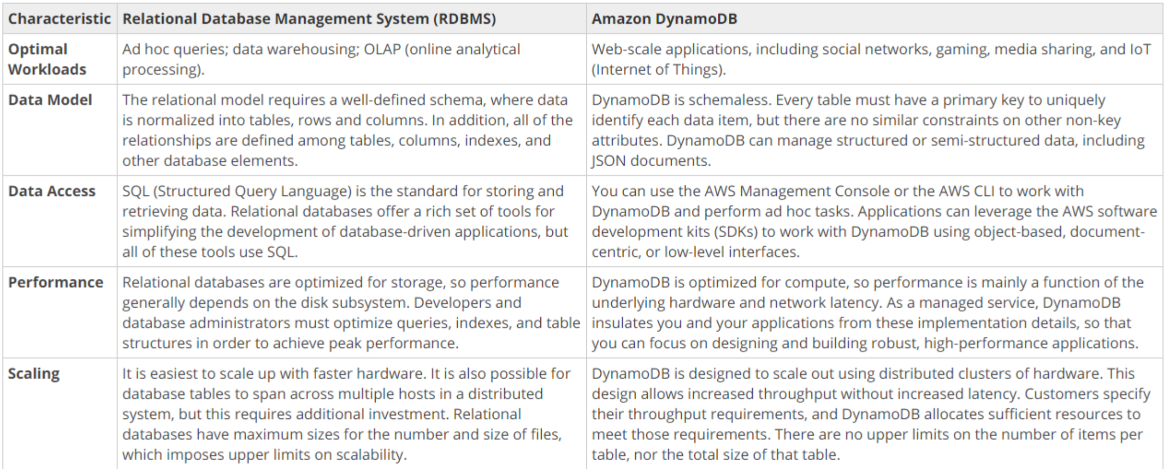
Your application has the requirement to store data in a backend data store. Indexing should be possible on the data, but the data does not conform to any schema. Which of the following would be the ideal data store to choose for this application?

- A. AWS RDS
- B. AWS DynamoDBright
- C. AWS Redshift
- D. AWS S3

Explanation:

Answer – B

The below AWS Documentation mentions the differences between AWS DynamoDB and other traditional database systems. One of the major differences is the schemaless nature of the 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.

- Option A is invalid since this is normally used for databases that perform to a particular schema.
- Option C is invalid since this is normally used for columnar based databases.
- Option D is invalid since this is normally used for object-level storage.

For more information on the differences, please refer to the below link-

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

Question 49

Developer Team is working on an event driven application that needs to process data stored in the Amazon S3 bucket & notify multiple subscribers using Amazon SNS. Thus, a single topic is created in Amazon SNS & messages are pushed to multiple Amazon SQS queues subscribed to this topic. Which of the following is a correct statement with regards to messages sent to the Amazon SQS queue?

- A. Each Queue will receive an identical message sent to that topic instantaneously.right
- B. Message sent to the topic will be evenly distributed among all the queues which have subscribed to this topic.
- C. Each Queue will receive a message sent to that topic asynchronously with a time delay.
- D. Messages sent to the topic will be visible to the queue, once processing of the message is completed by the first queue.

Explanation:

Correct Answer – A

When multiple Amazon SQS queues are subscribed to a single topic within an Amazon SNS, each queue will receive an identical message. This is useful for parallel independent processing of messaging.

- Option B is incorrect as All the queues subscribed to the topic will not get an evenly distributed message. But all queues will have identical messages each time a message is pushed for a topic.
- Option C is incorrect as there would be any time delay for receiving messages.
- Option D is incorrect as All queue receives identical message & can start processing messages parallelly independent of other queues.

For more information on Fanout with Amazon SNS, refer to the following URL-

- https://aws.amazon.com/getting-started/hands-on/send-fanout-event-notifications/

Question 50

You are in charge of deploying an application hosted on an EC2 Instance and sitting behind an Elastic Load Balancer. You have been requested to monitor the incoming client connections to the Elastic Load Balancer. Which of the below options can suffice this requirement?

- A. Use AWS CloudTrail with your load balancer.
- B. Enable access logs on the load balancer.right
- C. Use a CloudWatch Logs Agent by installing on EC2.
- D. Create a custom metric CloudWatch filter on your load balancer.

Explanation:

Answer – B

The AWS Documentation mentions the following.

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.

- Option A is INCORRECT because CloudTrail captures all API calls for Elastic Load Balancing as events. This is not the recommended approach to monitoring incoming connections to the ELB.
- Option B is CORRECT. 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 to troubleshoot issues.
- Option C is invalid since the Logs agents are installed on EC2 Instances and not on the ELB.
- Option D is invalid since the metrics will not provide detailed information on the incoming connections.
- For more information on Application Load balancer Logs, please refer to the below link-
    - https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html
- Please refer to page 99 on the below link-
    - https://docs.aws.amazon.com/elasticloadbalancing/latest/application/elb-ag.pdf

Question 51

You are in charge of developing an application that will make use of AWS services. There is a key requirement from an architectural point of view that the entire system should be decoupled to ensure less dependency. Which of the following are the suitable services to decouple different components of an application? (Select TWO)

- A. AWS CodePipeline
- B. AWS Simple Queue Serviceright
- C. AWS Simple Notification Serviceright
- D. AWS CodeBuild
- E. AWS CodeStar

Explanation:

Answer – B and C

The AWS Documentation mentions the following.

Amazon Simple Queue Service (Amazon SQS) offers a secure, durable, and available hosted queue that lets you integrate and decouple distributed software systems and components. Amazon SQS offers common constructs such as dead-letter queues and cost allocation tags.
Amazon SNS enables you to modernize your applications and decouple them into smaller, independent components that are easier to develop, deploy and maintain. AWS SNS topics can be subscribed to by multiple decoupled services. SNS is mostly used in conjunction with SQS to provide decoupled services.

Option A is incorrect since this service is used to build CI/CD pipelines for integration and deployment.
Option D is incorrect since this service is used as the build and test stage of the CI/CD deployments.
Option E is incorrect since AWS CodeStar is a cloud-based service for creating, managing, and working with software development projects on AWS.
For more information on the Simple Queue Service, please refer to the below link-

- https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html
- https://aws.amazon.com/sns

Question 52

A static web site has been hosted on a bucket and is now being accessed by users. One of the web pages javascript section has been changed to access data hosted in another S3 bucket. Now that same web page is no longer loading in the browser. Which of the following can help alleviate the error?

- A. Enable versioning for the underlying S3 bucket.
- B. Enable Replication so that the objects get replicated to the other bucket.
- C. Enable CORS on the bucket containing the data.right
- D. Change the Bucket policy for the bucket to allow access from the other bucket.

Explanation:

Answer – C

This is given as use case scenarios in the AWS Documentation.

Cross-Origin Resource Sharing: Use-case Scenarios
The following are example scenarios for using CORS.

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

- Scenario 2: Suppose that you want to host a web font from your S3 bucket. Again, browsers require a CORS check (also called a preflight check) for loading web fonts. You would configure the bucket that hosts the web font to allow any origin to make these requests. Option A is incorrect because Enabling versioning does not solve the problems of accessing form the different buckets. You need to enable CORS on the underlying bucket.

  Option B is incorrect because Enabling replication will cost you more as you are maintaining two copies of data.

  Option D is incorrect because changing the bucket policy allows access from another bucket, but this will open the whole bucket, not an ideal solution.

For more information on Cross-Origin Resource Sharing, please refer to the below link-

- https://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html

Question 53

Your company is using Amazon ECR for storing Docker images. There are multiple Docker images & you need to retag specific Docker images so that only those images can be used for new project deployment.

Which of the following options can be used to retag Docker images in Amazon ECR?

- A. Use the --image-retag option of the put-image command.
- B. Use the --image-tag option of the put-image command.right
- C. Pull the image & retag the image with --image-retag option
- D. Push the image & retag the image with --image-tag option

Explanation:

Correct Answer: B
To retag docker images in Amazon ECR, it is not required to pull or push these images again to the ECR depository. The --*image-tag* option of the put-image command can be used to retag the existing image in the repository. This command is useful for retagging large images as this will save network bandwidth by avoiding retrieving images.

- Option A is incorrect as this is an invalid option to retag a docker image stored in Amazon ECR.
- Options C and D are incorrect because pulling or pushing an image is not required for retagging any docker image in Amazon ECR.

For more information on pushing docker image to Amazon ECR, refer to the following URL,

- https://docs.aws.amazon.com/AmazonECR/latest/userguide/image-retag.html

Question 54

Your current log analysis application takes more than four hours to generate a report of the top 10 users of your web application. You have been asked to implement a system that can report this information in real-time, ensure that the report is always up to date, and handle increases in the number of requests to your web application. Choose the option that is cost-effective and can fulfill the requirements.

- A. Publish your data to CloudWatch Logs, and configure your application to Autoscale to handle the load on demand.

- B. Publish your log data to an Amazon S3 bucket. Use AWS CloudFormation to create an Auto Scaling group to scale your post-processing application which is configured to pull down your log files stored an Amazon S3.

- C. Post your log data to an Amazon Kinesis data stream, and subscribe your log-processing application so that is configured to process your logging data.right
- D. Create a multi-AZ Amazon RDS MySQL cluster, post the logging data to MySQL, and run a map reduce job to retrieve the required information on user counts.

Explanation:

Answer – C

When you see Amazon Kinesis as an option, this becomes the ideal option to process data in real-time.

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 process streaming data cost-effectively 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 application logs, website clickstreams, IoT telemetry data, and more into your databases, data lakes, and data warehouses, or build your own real-time applications using this data.
For more information on AWS Kinesis, please refer to the below link-

- https://aws.amazon.com/kinesis/

Option A is incorrect because logs in CloudWatch Logs are not in real-time.

Option B is incorrect because you have to pay for S3 buckets and EC2 instances cost, which is not a cost-effective solution. And the logs may not be in real-time.

Option D is incorrect because it is not cost-efficient to store the logs in RDS MySQL.

Question 55

You’ve been instructed to develop a mobile application that will make use of AWS services. You need to decide on a data store to store the user sessions. Which of the following would be an ideal data store for session management?

- A. AWS Simple Storage Service

- B. AWS DynamoDBright
- C. AWS RDS

- D. AWS Redshift

Explanation:

Answer – B

DynamoDB is an alternative solution that can be used for the storage of session management. The latency of access to data is less. Hence, this can be used as a data store for session management.

Option A is incorrect since this service is used for object-level storage.

Option C is incorrect since this service is used for storing relational data.

Option D is incorrect since this service is used as a data warehousing solution.

For more information on an example on this, please refer to the below link-

- https://aws.amazon.com/blogs/aws/scalable-session-handling-in-php-using-amazon-dynamodb/

Question 56

Your application currently interacts with a DynamoDB table. Records are inserted into the table via the application. There is now a requirement to ensure that another record is inserted into a secondary table whenever items are updated in the DynamoDB primary table. Which of the below feature should be used when developing such a solution?

- A. AWS DynamoDB Encryption

- B. AWS DynamoDB Streamsright
- C. AWS DynamoDB Accelerator

- D. AWSTable Accelerator

Explanation:

Answer – B

This is also mentioned as a use case in the AWS Documentation.

DynamoDB Streams Use Cases and Design Patterns
This post describes some common use cases you might encounter, along with their design options and solutions, when migrating data from relational data stores to Amazon DynamoDB.

We will consider how to manage the following scenarios.

- How do you set up a relationship across multiple tables in which, based on the value of an item from one table, you update the item in a second table?

- How do you trigger an event based on a particular transaction?

- How do you audit or archive transactions?

- How do you replicate data across multiple tables (similar to that of materialized views/streams/replication in relational data stores)?

Relational databases provide native support for transactions, triggers, auditing, and replication. Typically, a transaction in a database refers to performing create, read, update, and delete (CRUD) operations against multiple tables in a block. A transaction can have only two states—success or failure. In other words, there is no partial completion.

As a NoSQL database, DynamoDB is not designed to support transactions. Although client-side libraries are available to mimic the transaction capabilities, they are not scalable and cost-effective. For example, the Java Transaction Library for DynamoDB creates 7N+4 additional writes for every write operation. This is partly because the library holds metadata to manage the transactions to ensure that it's consistent and can be rolled back before commit.

You can use DynamoDB Streams to address all these use cases. DynamoDB Streams is a powerful service that you can combine with other AWS services to solve many similar problems. When enabled, DynamoDB Streams captures a time-ordered sequence of item-level modifications in a DynamoDB table and durably stores the information for up to 24 hours. Applications can access a series of stream records, which contain an item change, from a DynamoDB stream in near real-time.

AWS maintains separate endpoints for DynamoDB and DynamoDB Streams. To work with database tables and indexes, your application must access a DynamoDB endpoint. To read and process DynamoDB Streams records, your application must access a DynamoDB Streams endpoint in the same Region.

Option A is incorrect because DynamoDB Encryption helps you with the security, not adding the data to secondary tables.

Option C is incorrect because DynamoDB Accelerator is a fully managed, highly available, in-memory cache for DynamoDB that delivers up to a 10x performance improvement. It does not solve the problem.

Option D is incorrect because there is no service named Table Accelerator.

For more information on use cases and design patterns for DynamoDB streams, please refer to the below link-

- https://aws.amazon.com/blogs/database/dynamodb-streams-use-cases-and-design-patterns/

Question 57

An application has been making use of AWS DynamoDB for its back-end data store. The size of the table has now grown to 20 GB, and the scans on the table are causing throttling errors. Which of the following should now be implemented to avoid such errors?

- A. Large Page size
- B. Reduced page sizeright
- C. Parallel Scans
- D. Sequential scans

Explanation:

Answer – B

When you scan your table in Amazon DynamoDB, you should follow the DynamoDB best practices for avoiding sudden bursts of read activity.
You can use the following technique to minimize the impact of a scan on a table's provisioned throughput.
Reduce page size
Because a Scan operation reads an entire page (by default, 1 MB), you can reduce the scan operation's impact by setting a smaller page size. The ***Scan*** operation provides a *Limit* parameter that you can use to set the page size for your request. Each ***Query*** or ***Scan*** request with a smaller page size uses fewer read operations and creates a "pause" between each request. For example, suppose that, each item is 4 KB, and you set the page size to 40 items. A ***Query*** request would then consume only 20 eventually consistent read operations or 40 strongly consistent read operations. A larger number of smaller ***Query*** or ***Scan*** operations would allow your other critical requests to succeed without throttling.
Option A is incorrect because the page size should be reduced rather than enlarged.

Option C is incorrect because a parallel scan with many workers can easily consume all of the provisioned read capacity.

Option D is incorrect because the sequential scan processes data sequentially. It does not help to avoid the throttling errors.

For more information, please check below AWS Docs-

- https://aws.amazon.com/blogs/developer/rate-limited-scans-in-amazon-dynamodb/
- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-query-scan.html

Question 58

In API Gateway, when a stage variable is used as part of an HTTP integration URL, which of the following are correct ways of defining a "subdomain" and the "path"? (Select TWO)

- A. http://example.com/${<variable_name>}/prod
- B. http://example.com/${stageVariables.<variable_name>}/prodright
- C. http://${stageVariables.<variable_name>}.example.com/dev/operationright
- D. http://${stageVariables}.example.com/dev/operation
- E. http://${<variable_name>}.example.com/dev/operation
- F. http://example.com/${stageVariables}/prod

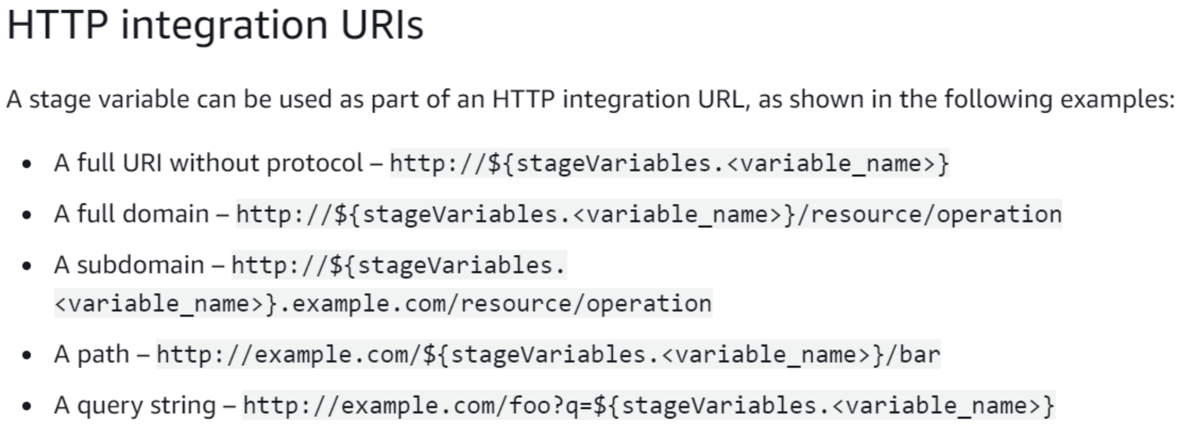
Explanation:

Correct Answers: B and C

A stage variable can be used as part of the HTTP integration URL in the following cases:

- A full URI without protocol
- A full domain
- A subdomain
- A path
- A query string

options B and C display the stage variable as a path & sub-domain.



HTTP integration URIs

A stage variable can be used as part of an HTTP integration URL, as shown in the following examples:

- A full URI without protocol – `http://${stageVariables.<variable_name>}`
- A full domain – `http://${stageVariables.<variable_name>}/resource/operation`
- A subdomain – `http://${stageVariables.<variable_name>}.example.com/resource/operation`
- A path – `http://example.com/${stageVariables.<variable_name>}/bar`
- A query string – `http://example.com/foo?q=${stageVariables.<variable_name>}`

For more information on Staging variables, refer to the following URL-

- https://docs.aws.amazon.com/apigateway/latest/developerguide/aws-api-gateway-stage-variables-reference.html

Question 59

Your company is planning to create new development environments in AWS. They want to use their existing Chef recipes that they use for their on-premise configuration for servers in AWS. Which of the following service would be ideal to use in this regard?

- A. AWS Elastic Beanstalk
- B. AWS OpsWorksright
- C. AWS Cloudformation
- D. AWS SQS

Explanation:

Answer – B

The AWS Documentation mentions the following.

AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments.
All other options are invalid since they cannot be used to work with Chef recipes for configuration management.

For more information on AWS Opswork, please refer to the below link-

- https://aws.amazon.com/opsworks/

Question 60

Your company has developed a web application and hosted it on an Amazon S3 bucket configured for static content. The users can log in to this app using their Google/Facebook login accounts. The application uses the AWS SDK for JavaScript in the browser to access data stored in an Amazon DynamoDB table. How can you ensure that API keys for access to your data in DynamoDB are secure?

- A. Create an Amazon S3 role in IAM with access to the specific DynamoDB tables, and assign it to the bucket hosting the website.
- B. Configure S3 bucket tags with your AWS access keys to the bucket hosting the website, so that the application can query them for access.
- C. Configure a web identity federation role within IAM to enable access to the correct DynamoDB resources and retrieve temporary credentials.right
- D. Store AWS keys in global variables within your application and configure the application to use these credentials when making requests.

Explanation:

Answer – C
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.
Option A is incorrect since Roles cannot be assigned to S3 buckets.
Options B and D are incorrect since the AWS Access keys should not be used.
For more information on Web Identity Federation, please refer to the below link AWS-

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

Question 61

You are planning to deploy a built application onto an EC2 Instance. There will be several tests conducted on this Instance. You want to have the ability to capture the logs from the web server to help diagnose any issues if they occur. How can you achieve this?

- A. Enable Cloudtrail for the region.
- B. Install the Cloudwatch agent on the Instance.right
- C. Use the VPC Flow logs to get the logs from the Instance.
- D. Create a dashboard for the key Cloudwatch metrics.

Explanation:

Answer – B

You can install the Cloudwatch agent on the machine and then configure it to send the web server's logs to a central location in Cloudwatch.

Option A is invalid since this is used for API monitoring activity.

Option C is invalid since it is used to get the network traffic coming to an Instance hosted in a VPC.

Option D is invalid since this will not give the detailed level of logs that is required.

For more information on the Cloudwatch agent, please refer to the below link-

- https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html

- Question 62

The software Team has created a new version of the messaging application deployed on a large number of Amazon EC2 instances. Existing application versions need to be upgraded to a new version separately in a group of EC2 instances without any degradation of the capacity during deployment. None of the Amazon EC2 instances should be replaced during this upgrade.

Which deployment option can be considered to complete the application upgrade to the new version?

- A. Traffic splitting deployment
- B. Rolling deployment
- C. Rolling with additional batch deploymentright
- D. Immutable deployment

Explanation:

Correct Answer: C
Explanation: Using Rolling with additional batch deployment, a new batch of the Amazon EC2 instance is launched before taking a batch of instances out of service for deploying a new version. Once all Amazon EC2 instances are upgraded to a new version of the application, this additional batch of Amazon EC2 instances is terminated. This will ensure full capacity during deployment.

Note: None of the Amazon EC2 instances should be replaced during this upgrade.

- Option A is incorrect as with Traffic splitting deployment, Amazon Elastic Beanstalk will launch a completely new set of instances with a new version in a separate Auto Scaling group & forward only a certain percentage of traffic to the new version during the evaluation period.

- Option B is incorrect as with Rolling Deployment, Amazon Elastic Beanstalk splits Amazon EC2 instances within the environment into batches & each batch is upgraded to a new version of the application. During this deployment, total capacity is reduced.
- Option D is incorrect as with Immutable deployment, Amazon Elastic Beanstalk will launch a completely new set of instances with new versions in a separate Auto Scaling group. All existing instances will get replaced with this new set of instances. This will help to roll back faster to older versions if any issues are found with the new version of the application. Since replacement of Amazon EC2 instances is not required, Immutable deployment is not a correct option.

For more information on deployment options with AWS Elastic Beanstalk, refer to the following URL,

Question 63

You've developed a set of scripts using AWS Lambda. These scripts need to access EC2 Instances in a VPC. Which of the following needs to be done to ensure that the AWS Lambda function can access the resources in the VPC? (Select TWO)

- A. Ensure that the subnet IDs are configured in the Lambda function.right
- B. Ensure that the NACL IDs are configured in the Lambda function.

- C. Ensure that the Security Group IDs are configured in the Lambda function.right
- D. Ensure that the VPC Flow Log IDs are configured in the Lambda function.

Explanation:

Answer – A and C
Options B and D are incorrect since you have to mention the Subnet and Security IDs for the Lambda function to access the resources in the VPC.
The AWS Documentation mentions the following.

You can enable AWS Lambda to access resources in a Virtual Private Cloud (VPC). Your Lambda functions can now access Amazon RDS databases, Amazon Redshift data warehouses, Amazon ElastiCache nodes, and other endpoints that are accessible only from within a particular VPC (e.g., web service running on EC2).

You must provide additional VPC-specific configuration information such as VPC subnet IDs and security group IDs in order to enable your Lambda functions to access resources in an Amazon VPC.

For more information on configuring a lambda function to access resources in a VPC, please refer to the below link-

- https://docs.aws.amazon.com/lambda/latest/dg/vpc.html
- https://aws.amazon.com/about-aws/whats-new/2016/02/access-resources-within-a-vpc-using-aws-lambda/

Question 64

You've currently been tasked to migrate an existing on-premises web application into Elastic Beanstalk. You can't find any relevant AMIs in the beanstalk service that would be suitable to host your application. What would you consider as an easy step among the following to host the application?

- A. Migrate your application to Docker containers and then migrate to the Elastic Beanstalk environment.

- B. Consider using CloudFormation to deploy your environment to Elastic Beanstalk

- C. Consider using Packer to create a custom platformright
- D. Consider deploying your application using the Elastic Container Service

Explanation:

Answer – C
The AWS Documentation mentions the following to support this.

Custom Platforms
Elastic Beanstalk supports custom platforms. A custom platform is more advanced customization than a Custom Image in several ways. A custom platform lets you develop an entirely new platform from scratch, customizing the operating system, additional software, and scripts that Elastic Beanstalk runs on platform instances. This flexibility allows you to build a platform for an application that uses a language or other infrastructure software.

To create a custom platform, you build an Amazon Machine Image (AMI) from one of the supported operating systems—Ubuntu, RHEL, or Amazon Linux and add further customizations. You create your own Elastic Beanstalk platform using Packer, an open-source tool for creating machine images for many platforms, including AMIs for Amazon EC2. An Elastic Beanstalk platform comprises an AMI configured to run a software set that supports an application, and metadata can include custom configuration options and default configuration option settings.

- Options A and D are incorrect because it could require a lot of effort to migrate the application to start using Docker containers.
- Option B is incorrect because using Cloudformation alone cannot be used alone for this requirement.

For more information on Custom Platforms, please refer to the below link-

- https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/custom-platforms.html

Question 65

Company B is writing 10 items to the Dynamo DB table every second. Each item is 15.5Kb in size. What would be the required provisioned write throughput for best performance? Choose the correct answer from the options below.

- A. 10
- B. 160right
- C. 155
- D. 16

Explanation:

Correct Answer – B
As per the documentation, when working with write capacity, the rule is to divide the item size by 1Kb. Hence, 15.5 divided by 1 is 15.5. When we round-off to the nearest 1Kb value, it's 16. Since we are writing 10 items per second, we need to multiply 10*16 = 160.

For more information on Read and Write capacity, please refer to the below link-