Question 1: Incorrect

You are working for a small organization that does not have a database administrator and are needing to install a database on the cloud quickly to support an accounting application used by thousands of users. The application will act as a backend and will perform (CRUD) operations such as create, read, update and delete as well as inner joins. Which database is best suited for this scenario?

* Redshift
* DynamoDB(Incorrect)
* RDS(Correct)
* ElastiCache

#### Explanation

Correct answer - "RDS" : Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. Amazon RDS supports the most demanding database applications. You can choose between two SSD-backed storage options: one optimized for high-performance OLTP applications, and the other for cost-effective general-purpose use.

Incorrect:

"DynamoDB" - RDS uses expensive joins which DynamoDB does not making DynamoDB a better choice for scaling by storing complex hierarchical data within a single item

"Redshift" - RDS is your best choice here but Amazon Redshift provides an excellent scale-out option as your data and query complexity grows

"ElastiCache" - You can use ElastiCache in combination with RDS. This would be a good option for slow performing database queries in RDS that need to be cached for your application users

For more information visit https://aws.amazon.com/rds/ <https://aws.amazon.com/blogs/database/automating-sql-caching-for-amazon-elasticache-and-amazon-rds/>

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

Notes:

The key for this question is that DynamoDB cannot do joins, therefore when the questions they want to do inner joins, I should have queued in that they want a RDS.

Question 2: Correct

You are a developer working on AWS Lambda functions that are triggered by Amazon API Gateway and would like to perform testing on a small amount of traffic for new API versions. Which of the following features will accomplish this task?

* Custom Authorizers
* Stage Variables
* Mapping Templates
* Canary Deployment(Correct)

#### Explanation

Correct answer - "Canary Deployment" : In a canary release deployment, total API traffic is separated at random into a production release and a canary release with a pre-configured ratio. Typically, the canary release receives a small percentage of API traffic and the production release takes up the rest. The updated API features are only visible to API traffic through the canary. You can adjust the canary traffic percentage to optimize test coverage or performance.

Incorrect:

"Stage Variables" - They act like environment variables and can be used in your API setup

"Mapping Templates" - Its a script to map the payload from a method request to the corresponding integration request and from an integration response to the corresponding method response

"Custom Authorizers" - Used for authentication purposes and must return AWS Identity and Access Management (IAM) policies

For more information visit <https://docs.aws.amazon.com/apigateway/latest/developerguide/canary-release.html>

<https://martinfowler.com/bliki/CanaryRelease.html>

Canary Deployment

* Canary release is a technique to reduce the risk of introducing a new software version in production by slowly rolling out the change to a small subset of users before rolling it out to the entire infrastructure and making it available to everybody.

Question 5: Incorrect

You were assigned to a project that requires the use of the AWS CLI to build a project with AWS CodeBuild. Your project's root directory includes the buildspec.yml file to run build commands and would like your build artifacts to be automatically encrypted at the end. How should you configure CodeBuild to accomplish this?

* Specify a KMS key to use(Correct)
* Use an AWS Lambda Hook
* Use the AWS Encryption SDK(Incorrect)
* ​Use In Flight encryption (SSL)

#### Explanation

Correct answer - "Specify a KMS key to use" : For AWS CodeBuild to encrypt its build output artifacts, it needs access to an AWS KMS customer master key (CMK). By default, AWS CodeBuild uses the AWS-managed CMK for Amazon S3 in your AWS account.

Incorrect:

"Use an AWS Lambda Hook" - Code hook is used for integration with Lambda

"Use the AWS Encryption SDK" - The SDK just makes it easier for you to implement encryption best practices in your application

"Use In Flight encryption (SSL)" - SSL is usually for internet traffic which in this case will be using internal traffic through AWS

For more information visit https://docs.aws.amazon.com/codebuild/latest/userguide/build-env-ref-env-vars.html https://docs.aws.amazon.com/codebuild/latest/userguide/setting-up.html

Question 6: Incorrect

You are responsible for an application that runs on multiple Amazon EC2 instances. In front of the instances is an Internet-facing load balancer that takes requests from clients over the internet and distributes them to the EC2 instances. A health check is configured to ping the index.html page found in the root directory for the health status. When accessing the website via the internet visitors of the website receive timeout errors. What should be checked first to resolve the issue?

* Security Groups(Correct)
* IAM Roles(Incorrect)
* The application is down​
* The ALB is warming up

#### Explanation

Correct answer - "Security Groups" : Check your security group rules of your EC2 instance. You need a security group rule that allows inbound traffic from your public IPv4 address on the proper port.

Incorrect:

"IAM Roles" - Usually you run into issues with authorization of APIs with roles but not for timeout

"The application is down" - Although you can set a health check for application ping or HTTP, timeouts are usually caused by blocked firewall access

"The ALB is warming up" - ALB has a slow start mode which allows a warm-up period before being able to respond to requests with optimal performance. So this is not the issue

For more information visit <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html#TroubleshootingInstancesConnectionTimeout>

A security group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you can specify one or more security groups; otherwise, we use the default security group . You can add rules to each security group that allows traffic to or from its associated instances. You can modify the rules for a security group at any time. New and modified rules are automatically applied to all instances that are associated with the security group. When we decide whether to allow traffic to reach an instance, we evaluate all of the rules from all of the security groups that are associated with the instance.

When you launch an instance in a VPC, you must specify a security group that’s created for tht VPC. After you launch an instance, you can change its security groups. Security groups are associated with network interfaces. Changing an instance’s security group changes the security groups associated with the primary network interface (eth0).

Security Group Rules:

Default Role:

A default security group is named default, and it has an ID assigned by AWS. The following are the default rules for each default security group:

* Allows all inbound traffic from other instances associated with the default security group. The security group specifies itself as a source security group in its inbound rules.
* Allows all outbound traffic from the instance.

You can add or remove inbound and outbound rules for any default security group.

You can't delete a default security group. If you try to delete a default security group, you see the following error: Client.CannotDelete: the specified group: "sg-51530134" name: "default" cannot be deleted by a user

For each rule, you specify the following:

* Protocol: The protocol to allow. The most common protocols are 6 (TCP), 17 (UDP), and 1 (ICMP).
* Port range: For TCP, UDP, or a custom protocol, the range of ports to allow. You can specify a single port number (for example, 22), or range of port numbers (for example, 7000-8000).
* ICMP type and code: For ICMP, the ICMP type and code.
* Source or destination: The source (inbound rules) or destination (outbound rules) for the traffic. Specify one of these options:
  + An individual IPv4 address. You must use the /32 prefix length; for example, 203.0.113.1/32.
  + An individual IPv6 address. You must use the /128 prefix length; for example, 2001:db8:1234:1a00::123/128.
  + A range of IPv4 addresses, in CIDR block notation; for example, 203.0.113.0/24.
  + A range of IPv6 addresses, in CIDR block notation; for example, 2001:db8:1234:1a00::/64.
  + The prefix list ID for the AWS service; for example, pl-1a2b3c4d. For more information, see [Gateway VPC Endpoints](https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html) in the Amazon VPC User Guide.
  + Another security group. This allows instances that are associated with the specified security group to access instances associated with this security group. Choosing this option does not add rules from the source security group to this security group. You can specify one of the following security groups:
    - The current security group
    - A different security group for the same VPC
    - A different security group for a peer VPC in a VPC peering connection
* (Optional) Description: You can add a description for the rule, which can help you identify it later. A description can be up to 255 characters in length. Allowed characters are a-z, A-Z, 0-9, spaces, and .\_-:/()#,@[]+=;{}!$\*.

Question 10: Incorrect

You are a DynamoDB developer for an aerospace company that requires you to write 6 objects per second of 4.5KB in size each. What write capacity unit is needed for your project?

* 46(Incorrect)
* 24
* 15
* 30(Correct)

#### Explanation

Correct answer - "30" : One write capacity unit represents one write per second for an item up to 1 KB in size. If you need to write an item that is larger than 1 KB, DynamoDB will need to consume additional write capacity units. The total number of write capacity units required depends on the item size.

Incorrect:

"24"

"15"

"46"

For more information visit <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ProvisionedThroughput.html>

Read Request Units and Write Request Units

For on-demand mode tables, you don't need to specify how much read and write throughput you expect your application to perform. DynamoDB charges you for the reads and writes that your application performs on your tables in terms of read request units and write request units.

* **One read request unit represents one strongly consistent read request, or two eventually consistent read requests, for an item up to 4 KB in size.**
* **Transactional read requests require 2 read request units to perform one read for items up to 4 KB.**
  + If you need to read an item that is larger than 4 KB, DynamoDB needs additional read request units. The total number of read request units required depends on the item size, and whether you want an eventually consistent or strongly consistent read.
    - For example, if your item size is 8 KB, you require 2 read request units to sustain one strongly consistent read, 1 read request unit if you choose eventually consistent reads, or 4 read request units for a transactional read request.

Note: To learn more about DynamoDB read consistency models, see [Read Consistency](https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadConsistency.html).

* **One write request unit represents one write for an item up to 1 KB in size.**
  + **If you need to write an item that is larger than 1 KB, DynamoDB needs to consume additional write request units.**
* **Transactional write requests require 2 write request units to perform one write for items up to 1 KB.**
* The total number of write request units required depends on the item size.
  + For example, if your item size is 2 KB, you require 2 write request units to sustain one write request or 4 write request units for a transactional write request.

|  | WRITE | TRANSACTIONAL | STRONGLY | EVENTUALLY |
| --- | --- | --- | --- | --- |
| READ (4KB) Round Up | N/A | 2 UNIT | 1 UNIT | ½ UNIT |
| WRITE (1KB) | 1 UNIT | 2 UNIT | N/A | N/A |
|  |  |  |  |  |

Question 13: Incorrect

You are a Developer working with AWS CloudFormation templates. Your templates provision a VPC with one subnet and would like other stacks to use the output value of the subnet created. What must you do to provide this information to another stack?

* Expose
* Export (Correct)
* Output(Correct)
* Import(Incorrect)
* Fn::Ref(Incorrect)

#### Explanation

Correct answer - "Export" & "Output" : To export a stack's output value, use the Export field in the Output section of the stack's template.

Incorrect:

"Expose" - There is no expose option

"Import" - This will allow you to import instead of exposing

"Fn::Ref" - this helps reference a variable within your template, but not to export a variable out of your template.

For more information visit <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-stack-exports.html>

Question 14: Incorrect

You are a developer working at a cloud company that embraces serverless. You have performed your initial deployment and would like to work towards adding API Gateway stages and associate them with existing deployments. Your stages will include prod, test, and dev and will match AWS Lambda function aliases. Which of the following features must you add to achieve this? (select two)

* Lambda X-Ray integration
* Stage Variables(Correct)
* Lambda Versions(Incorrect)
* Lambda Aliases(Correct)
* Mapping Templates

#### Explanation

Correct answers - "Stage Variables & Lambda Aliases" : 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. With deployment stages in API Gateway, you can manage multiple release stages for each API, such as alpha, beta, and production. Using stage variables you can configure an API deployment stage to interact with different backend endpoints.

Incorrect:

"Lambda Versions" - Aliases enable you to abstract the process of promoting new Lambda function version and becomes more manageable than new versions

"Lambda X-Ray integration" - This is good for tracing and debugging requests so it can be looked at as a good option for troubleshooting issues in the future

"Mapping Templates" - If you did use this template you can access your stage variables but its not required to use

For more information visit <https://docs.aws.amazon.com/apigateway/latest/developerguide/stage-variables.html>

Question 19: Incorrect

As a DynamoDB expert, companies in your area rely on your expertise to train their developers. You have been hired to consult with a company that uses the NoSQL database for mobile applications. The developers are using DynamoDB to perform operations such as GetItem but are limited in knowledge. They would like to be more efficient with retrieving some attributes rather than all. Which of the following recommendations would you provide?

* Use a FilterExpression(Incorrect)
* Specify a ProjectionExpression(Correct)
* Use the --query parameter
* ​Use a Scan

#### Explanation

Correct answer - "Specify a ProjectionExpression" : A projection expression is a string that identifies the attributes you want. To retrieve a single attribute, specify its name. For multiple attributes, the names must be comma-separated.

Incorrect:

"Use a FilterExpression" - If you need to further refine the Query results, you can optionally provide a filter expression

"Use the --query parameter" - The Query operation finds items based on primary key values

"Use a Scan" - This would return all the data from the table.

For more information visit <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Expressions.ProjectionExpressions.html>

–––START–––

Question 22: Incorrect

You are a Developer handling a deployment service that automates application deployments to Amazon EC2 instances. Most of the deployments consist of code, but sometimes web and configuration files. One of your deployments failed and was rolled back by AWS CodeDeploy to the last known good application revision. During rollback which of the following instances did AWS CodeDeploy deploy first to?

* To the non-failed instances(Incorrect)
* To the failed instances(Correct)
* To new instances
* ​You cannot rollback CodeDeploy

#### Explanation

Correct answer - "To the failed instances" : AWS CodeDeploy rolls back deployments by redeploying a previously deployed revision of an application as a new deployment on the failed instances.

Incorrect:

"To the non-failed instances" - Nothing happens to the non-failed instances if any

"To new instances" - Nothing is deployed to new instances

"You cannot rollback CodeDeploy" - It is possible to rollback

For more information visit https://docs.aws.amazon.com/codedeploy/latest/userguide/deployments-rollback-and-redeploy.html

Question 33: Incorrect

You are an administrator setting permissions to other IAM users with limited permissions. On the AWS Management Console, you created a dev group where new developers will be added to and on your workstation you configured a developer profile. You would like to test that this user cannot terminate instances. Which of the following options would you execute?

​

* Using the CLI, create a dummy EC2 and delete it using another CLI call(Incorrect)
* Use the AWS CLI --test option​
* Retrieve the policy using the EC2 meta data service and use the IAM policy simulator
* ​Use the AWS CLI --dry-run option(Correct)

#### Explanation

Correct answer - "Use the AWS CLI --dry-run option" : The --dry-run option checks whether you have the required permissions for the action, without actually making the request, and provides an error response. If you have the required permissions, the error response is DryRunOperation, otherwise it is UnauthorizedOperation.

Incorrect:

"Use the AWS CLI --test option" - Option does not exist

"Retrieve the policy using the EC2 meta data service and use the IAM policy simulator" - EC meta data service is use to retrieve dynamic information such as instance-id, local-hostname, public-hostname, etc

"Using the CLI, create a dummy EC2 and delete it using another CLI call" - That would not work as the current EC2 may have permissions that the dummy instance does not have. If permissions were the same it can be done but it would be more work

For more information visit https://docs.aws.amazon.com/cli/latest/reference/ec2/terminate-instances.html https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html#instancedata-data-categories

Question 39: Incorrect

A developer in your company was just promoted to Developer and will be in charge of code deployment using AWS CodeCommit and AWS CodeDeploy. New requirements have been given to control deployment details by changing file permissions when applications are deployed and verifying the deployment success. Which of the following actions should the new Developer take?

* define a appspec.yml file in the codebuild/ directory
* define a buildspec.yml file in the root directory(Incorrect)
* define a buildspec.yml file in the codebuild/ directory
* define a appspec.yml file in the root directory(Correct)

#### Explanation

Correct answer - "define a appspec.yml file in the root directory" : An AppSpec file must be a YAML-formatted file named appspec.yml and it must be placed in the root of the directory structure of an application's source code. Otherwise, deployments fail.

Incorrect:

"define a buildspec.yml file in the root directory" - This is a file used by AWS CodeBuild to run a build

"define a buildspec.yml file in the codebuild/ directory" - This is a file used by AWS CodeBuild to run a build. In this example we are not working with CodeBuild

"define a appspec.yml file in the codebuild/ directory" - This file is for AWS CodeDeploy and must be placed in the root of the directory structure of an application's source code

For more information visit <https://docs.aws.amazon.com/codedeploy/latest/userguide/reference-appspec-file.html>

Question 40: Incorrect

A university has created a student portal that is accessible through a smartphone app and web application. The smartphone app is available in both Android and IOS and the web application works on most major browsers. Students will be able to do group study online and create forum questions. All changes made in smartphone devices should be available even when offline and should synchronize with other devices. Which of the following AWS services will meet these requirements?

* S3
* Cognito Identity Pools
* Cognito Sync(Correct)
* EFS(Incorrect)

#### Explanation

Correct answer - "Cognito Sync" : Amazon Cognito Sync is an AWS service and client library that enables cross-device syncing of application-related user data. You can use it to synchronize user profile data across mobile devices and the web without requiring your own backend

Incorrect:

"Cognito Identity Pools" - Amazon Cognito identity pools provide temporary AWS credentials for users who are guests

"S3" - S3 is a storage service that can be used from different devices however when you are dealing with mobile app user data and syncing data Cognito Sync becomes a better solution as the client libraries cache data locally so your app can read and write data regardless of device connectivity status.

"EFS" - With Amazon EFS, you can create a file system, mount the file system on an Amazon EC2 instance, and then read and write data to and from your file system

For more information visit https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-sync.html

Question 44: Incorrect

As a senior architect, you are responsible for the development, support, maintenance and implementation of all database applications written using NoSQL technology. A new project demands a throughput requirement of 10 strongly consistent reads per second of 6KB in size each. How many read capacity units will you need when configuring your DynamoDB table?

​

* 10​
* 60
* 30(Incorrect)
* 20(Correct)

#### Explanation

Correct answer - "20" : One read capacity unit represents one strongly consistent read per second for an item up to 4 KB in size. If you need to read an item that is larger than 4 KB, DynamoDB will need to consume additional read capacity units. 1) Item Size / 4KB , rounding to nearest whole number. a. So, in the above case , 6KB / 4 KB = 1.5 or 2 read capacity units.

2) 1 read capacity unit per item (since strongly consistent read) × No of reads per second a. So, in the above case 2 x 10 = 20 read capacity units.

Incorrect:

"60"

"30"

"10"

For more information visit https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ProvisionedThroughput.html https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html

Question 46: Incorrect

You are a Developer working with data on an EC2 instance running Windows. You have installed Kinesis Agent for Windows to stream JSON-formatted log files to Amazon Simple Storage Service (S3) via Amazon Kinesis Data Firehose. You gathered a list of all available sink types to change the destination of the log if needed. Which of the following sink types is not supported by Kinesis Firehose?

​

* ElasticSearch(Incorrect)
* S3
* Redshift
* ElastiCache(Correct)

#### Explanation

Correct answer - "ElastiCache" : Amazon Kinesis Data Firehose is the easiest way to load streaming data into data stores and analytics tools. It can capture, transform, and load streaming data into Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk.

Incorrect:

"S3" - An available destination for data

"Redshift" - An available destination for data

"ElasticSearch" - An available destination for data

For more information visit https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html

Question 47: Incorrect

An AWS Lambda function written in Golang was deployed six months ago and recently a new version was released that included the use of the X-Ray SDK. The change called for permissions to be altered to the IAM role of the Lambda function to allow the X-Ray SDK to send data to X-Ray. While testing you find that data is not being sent to X-Ray, what is a likely reason?

* Authorize Lambda source in the X-Ray console
* The IAM permissions
* Lambda X-Ray active tracing must be enabled(Correct)
* ​The X-Ray agent must be loaded with the code(Incorrect)

#### Explanation

Correct answer - "Lambda X-Ray active tracing must be enabled" : To enable tracing on your Lambda function using the Lambda CLI, you must first add tracing permissions to your function's execution role. Then ensure the active tracing setting is enabled.

Incorrect:

"The IAM permissions" - Incorrect as we already know that permissions were set

"Authorize Lambda source in the X-Ray console" - Not required to set the source

"The X-Ray agent must be loaded with the code" - The X-ray agent is not needed with Lambda instead AWS X-Ray daemon automatically listens for traffic on UDP port 2000, gathers raw segment data, and relays it to the AWS X-Ray API.

For more information visit <https://docs.aws.amazon.com/xray/latest/devguide/xray-services-lambda.html>

Question 48: Incorrect

You are a Developer working with Amazon ECS container instances and would like to isolate credentials so that a container never has access to credentials intended for another container belonging to another task. Which of the following actions must you take to achieve that?

* Use the parameter store to pass in AWS credentials(Incorrect)
* Assign an IAM role to the EC2 instance
* Load the credentials within the docker container
* Create an IAM Role for ECS and assign it to the tasks(Correct)

#### Explanation

Correct answer - "Create an IAM Role for ECS and assign it to the tasks" : You must also create a role for your tasks to use before you can specify it in your task definitions. You can create the role using the Amazon Elastic Container Service Task Role service role in the IAM console. Then you can attach your specific IAM policy to the role that gives the containers in your task the permissions you desire.

Incorrect:

"Assign an IAM role to the EC2 instance" - To limit permissions a container does not need access to credentials that are intended for another container that belongs to another task

"Load the credentials within the docker container" - Instead of creating and distributing your AWS credentials to the containers or using the EC2 instance's role, you can associate an IAM role with an ECS task definition

"Use the parameter store to pass in AWS credentials" - A container can only retrieve credentials for the IAM role that is defined in the task definition to which it belongs

For more information visit <https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task-iam-roles.html>

Question 49: Incorrect

You are a Developer at a company and are responsible for the data management of the AWS Kinesis streams. The security team has required stricter requirements by leveraging security mechanisms available with the Kinesis Data Streams service that won't require code changes on your end. Which of the following features meet the requirements? (select two)

* Envelope Encryption(Incorrect)​
* SSE-C encryption​
* Encryption in flight with HTTPS endpoint(Correct)
* Client Side Encryption
* KMS encryption for data at rest(Correct)

#### Explanation

Correct answers - "KMS encryption for data at rest & Encryption in flight with HTTPS endpoint" : Server-side encryption is a feature in Amazon Kinesis Data Streams that automatically encrypts data before it's at rest by using an AWS KMS customer master key (CMK) you specify. Data is encrypted before it's written to the Kinesis stream storage layer, and decrypted after it's retrieved from storage. As a result, your data is encrypted at rest within the Kinesis Data Streams service. Also the HTTPS protocol ensures that data inflight is encrypted as well.

Incorrect:

"SSE-C encryption" - SSE-C is functionality in Amazon S3 where you encrypt your data, on your behalf, using keys that you provide. With Kinesis Streams you can choose to encrypt the data yourself to a data stream

"Client Side Encryption" - This involves work

"Envelope Encryption" - This involves work

For more information visit https://docs.aws.amazon.com/streams/latest/dev/what-is-sse.html

Question 52: Incorrect

You are producing data to AWS Kinesis using AWS Lambda which sits behind an API Gateway. Data represents a clickstream from the users navigating your website. What in case you want to make sure your Kinesis stream can scale over time due to increased volume, what would you need to do? (select two)

​

* The partition key must take a great number of different values(Correct)
* You need to add shards(Correct)
* You need to enable auto-scaling(Incorrect)
* The partition key must only take few values
* You need to remove shards

#### Explanation

Correct answers - "The partition key must take a great number of different values & You need to add shards" : Kinesis Data Streams segregates the data records belonging to a stream into multiple shards. It uses the partition key that is associated with each data record to determine which shard a given data record belongs to. Partition keys are Unicode strings with a maximum length limit of 256 bytes. A stream is composed of one or more shards, each of which provides a fixed unit of capacity. Each shard can support up to 5 transactions per second for reads, up to a maximum total data read rate of 2 MB per second and up to 1,000 records per second for writes, up to a maximum total data write rate of 1 MB per second (including partition keys). The data capacity of your stream is a function of the number of shards that you specify for the stream. The total capacity of the stream is the sum of the capacities of its shards.

Incorrect:

"You need to enable auto-scale" - You don't turn on a setting instead you can utilize other services to work together

"The partition key must only take few values" - You will need different partition keys to route to different shards

For more information visit https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html <https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html>

Question 53: Incorrect

You have launched several AWS Lambda functions written in Java. A new requirement was given that over 1MB of data should be passed to the functions and should be encrypted and decrypted at runtime. Which of the following methods is suitable for encrypting the data?

* KMS direct encryption and store as file
* Envelope Encryption and store as file within the code(Correct)
* Envelope Encryption and store as environment variable(Incorrect)
* KMS Encryption and store as environment variable

#### Explanation

Correct answer - "Envelope Encryption and store as file within the code" : AWS Lambda environment variables have a maximum size of a few KB. Additionally, the direct 'Encrypt' API of KMS also has a few KB limit. To encrypt 1 MB, you need to use the Encryption SDK and pack the encrypted file with the lambda function.

Incorrect:

"KMS direct encryption and store as file" - You can encrypt up to 4 kilobytes (4096 bytes) of arbitrary data such as an RSA key, a database password, or other sensitive information

"Envelope Encryption and store as environment variable" - Environment variables must not exceed 4 KB

"KMS Encryption and store as environment variable" -You can encrypt up to 4 kilobytes (4096 bytes) of arbitrary data such as an RSA key, a database password, or other sensitive information. Environment variables must not exceed 4 KB

For more information visit https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/introduction.html https://docs.aws.amazon.com/lambda/latest/dg/env\_variables.html#env\_encrypt

Question 54: Incorrect

You have created a continuous delivery service model with automated steps using AWS CodePipeline. Your pipeline uses your code, maintained in a CodeCommit repository, AWS CodeBuild, and AWS Elastic Beanstalk to automatically deploy your code every time there is a code change. However, the deployment part to Elastic Beanstalk is taking a very long time due to resolving dependencies on all of your 100 target EC2 instances. Which of the following actions should you take to improve performance with limited code changes?

* ​
* Store the dependencies in S3
* (Incorrect)
* ​
* Bundle the dependencies in the source code in CodeCommit
* ​
* Bundle the dependencies in the source code during the last stage of CodeBuild
* (Correct)
* ​
* Create a custom platform for Elastic Beanstalk

#### Explanation

Correct answer - "Bundle the dependencies in the source code during the last stage of CodeBuild" : This will allow the code bundle to be deployed to Elastic Beanstalk to have both the dependencies and the code, hence speeding up the deployment time to Elastic Beanstalk

Incorrect:

"Bundle the dependencies in the source code in CodeCommit" - This is not best practice and could make the CodeCommit repository huge.

"Store the dependencies in S3" - S3 can be used as a storage location for your source code, logs, and other artifacts that are created when you use Elastic Beanstalk however there is still a time issue to retrieve the files.

"Create a custom platform for Elastic Beanstalk" - This is a more advanced feature that may require you to have more complexity than you need

For more information visit https://aws.amazon.com/blogs/devops/how-to-enable-caching-for-aws-codebuild https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/AWSHowTo.S3.html

Question 60: Incorrect

You are a developer working remotely from home. The company has given you an IAM user account with an access key and secret access key that allows permissions to a few AWS services. You would like to be able to retrieve the CodeBuild logs for failed builds and analyze them in Athena. Which steps should you take to extract the logs out of CodeBuild?

* Use CloudWatch Events(Incorrect)
* Use AWS Lambda integration
* Enable S3 and CloudWatch Logs integration(Correct)
* Use Kinesis

#### Explanation

Correct answer - "Enable S3 and CloudWatch integration" : If there is any build output, the build environment uploads its output to an Amazon S3 bucket. While the build is running, you can use the AWS CodeBuild console, AWS CLI, or AWS SDKs, to get summarized build information from AWS CodeBuild and detailed build information from Amazon CloudWatch Logs.

Incorrect:

"Use AWS Lambda integration" - Lambda is always a great way to use boto3 library to read logs programmatically but the work has been done for you with S3 and CloudWatch

"Use CloudWatch Events" - You can integrate CloudWatch Events with CodeBuild however since we are looking for logs only CloudWatch logs already has what we need

"Use Kinesis" - Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information but an overkill for our requirement

For more information visit https://aws.amazon.com/cloudtrail/ https://docs.amazonaws.cn/en\_us/codebuild/latest/userguide/getting-started.html#getting-started-input-bucket

Question 63: Incorrect

Your web application front end consists of 5 EC2 instances behind an Application Load Balancer. You have configured your web application to capture the IP address of the client making requests. When viewing the data captured you notice that every IP address being captured is the same, which also happens to be the IP address of the Application Load Balancer. What should you do to identify the true IP address of the client?

​

* Look into the X-Forwarded-Proto header in the backend(Incorrect)
* Modify the front-end of the website so that the users send their IP in the requests
* Look into the X-Forwarded-For header in the backend(Correct)
* Look into the client's cookie

#### Explanation

Correct answer - "Look into the X-Forwarded-For header in the backend" : The X-Forwarded-For request header helps you identify the IP address of a client when you use an HTTP or HTTPS load balancer. Because load balancers intercept traffic between clients and servers, your server access logs contain only the IP address of the load balancer. To see the IP address of the client, use the X-Forwarded-For request header. Elastic Load Balancing stores the IP address of the client in the X-Forwarded-For request header and passes the header to your server.

Incorrect:

"Modify the front-end of the website so that the users send their IP in the requests" - When a user makes a request the IP address is sent with the request to the server and the load balancer intercepts it. There is no need to modify the application

"Look into the X-Forwarded-Proto header in the backend" - The X-Forwarded-Proto request header helps you identify the protocol (HTTP or HTTPS) that a client used to connect to your load balancer

"Look into the client's cookie" - For this we would need to modify the client side logic and server side logic, which would not be efficient

For more information visit <https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/x-forwarded-headers.html>

Question 65: Incorrect

A company has a cloud system in AWS with components that send and receive messages using SQS queues. While reviewing the system you see that it processes a lot of information and would like to be aware of any limits of the system. Which of the following is the maximum number of messages that can be stored in an SQS queue?

​

* no limit(Correct)
* 10000
* 100000(Incorrect)
* 10000000

#### Explanation

Correct answer - "no limit" : There are no message limits for storing in SQS, but 'in flight messages' do have limits. Make sure to delete messages after you have processed them. There can be a maximum of approximately 120,000 inflight messages (received from a queue by a consumer, but not yet deleted from the queue).

Incorrect:

"10000" - Please refer to correct answer

"100000" - Please refer to correct answer

"10000000" - Please refer to correct answer

For more information visit https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-limits.html

RESULTS

## Practice Test #2 (AWS Certified Developer Associate - DVA-C01) - Results

65 questions | 2 hours 10 minutes | 72% correct required to pass

Correct

Wrong

Skipped

Attempt 1: Failed (72% required to pass)

64% correct (42/65)

1 hour 6 minutes

May 4, 2020 12:19 AM

**Review questions**

## Knowledge areas

### ASG (1 question)

100%

### EBS (2 questions)

100%

### CloudFormation (7 questions)

86%

14%

### Kinesis (4 questions)

25%

75%

### DynamoDB (4 questions)

25%

75%

### Cognito (1 question)

100%

### ECS (5 questions)

80%

20%

### Elastic Beanstalk (3 questions)

67%

33%

### KMS (2 questions)

50%

50%

### AWS Lambda (2 questions)

100%

### S3 (7 questions)

100%

### X-Ray (2 questions)

50%

50%

### RDS (2 questions)

50%

50%

### API Gateway (5 questions)

80%

20%

### ELB (2 questions)

100%

### CodeDeploy (3 questions)

33%

67%

### EC2 (1 question)

100%

### CLI (2 questions)

50%

50%

### SNS (2 questions)

100%

### CodeBuild (2 questions)

100%

### CloudTrail (2 questions)

100%

### SES (1 question)

100%

### CodePipeline (1 question)

100%

### SQS (1 question)

100%

### IAM (1 question)

100%

Correct

Wrong

Skipped