## AWS Certified Developer Associate PT 2 - Results

Back to result overview

**Beta**

[Share feedback](https://survey.alchemer.com/s3/7719142/Practice-tests-learner-csat/?user_id=52182326&course_id=2981704&quiz_id=4852736)

**Attempt 1**

All domains

65 all39 correct26 incorrect0 skipped30 marked

Collapse all questions

**Question 1Correct**

A developer is working on a serverless application using AWS Cloud Development Kit (AWS CDK) and intends to set up several AWS Lambda functions and Amazon API Gateway APIs during the creation of an AWS CloudFormation stack. The developer's local machine is equipped with AWS Serverless Application Model (AWS SAM) and the AWS CDK.

What is the best way for the developer to locally test a particular Lambda function?

**Test the Lambda function through the AWS Management Console.**

**Directly execute the Lambda function on the local machine.**

**Your answer is correct**

**Use the sam local invoke command specifying the specific Lambda function.**

**Use the AWS CDK command line to locally run the Lambda function.**

Overall explanation

AWS SAM CLI is a developer tool that allows you to locally test and debug your AWS Lambda functions defined by AWS Serverless Application Model (SAM) templates. Using the **sam local invoke** command with the specific Lambda function as an argument, you can execute the function locally.

**CORRECT:**"Use the sam local invoke command specifying the specific Lambda function" is the correct answer (as explained above.)

**INCORRECT:** "Test the Lambda function through the AWS Management Console" is incorrect.

The AWS Management Console allows you to create and manage AWS Lambda functions but doesn't provide a feature to test functions locally.

**INCORRECT:** "Use the AWS CDK command line to locally run the Lambda function" is incorrect.

AWS CDK is a software development framework to define cloud infrastructure in code and provision it through AWS CloudFormation, but it doesn't allow local execution of Lambda functions.

**INCORRECT:** "Directly execute the Lambda function on the local machine" is incorrect.

AWS Lambda functions cannot be executed directly on a local machine without a local testing tool like AWS SAM CLI.

**References:**

<https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/serverless-sam-cli-using-invoke.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-sam/>

**Domain**

AWS Compute

**Question 2Incorrect**

A company uses Amazon DynamoDB to store sensitive data that must be encrypted. The company security policy mandates that data must be encrypted before it is submitted to DynamoDB

How can a Developer meet these requirements?

**Use AWS Certificate Manager (ACM) to create one certificate for each DynamoDB table.**

**Correct answer**

**Use the DynamoDB Encryption Client to enable end-to-end protection using client-side encryption.**

**Use the UpdateTable operation to switch to an AWS managed customer master key (CMK).**

**Your answer is incorrect**

**Use the UpdateTable operation to switch to a customer managed customer master key (CMK).**

Overall explanation

In addition to encryption at rest, which is a server-side encryption feature, AWS provides the Amazon DynamoDB Encryption Client. This client-side encryption library enables you to protect your table data before submitting it to DynamoDB. With server-side encryption, your data is encrypted in transit over an HTTPS connection, decrypted at the DynamoDB endpoint, and then re-encrypted before being stored in DynamoDB. Client-side encryption provides end-to-end protection for your data from its source to storage in DynamoDB.

**CORRECT:**"Use the DynamoDB Encryption Client to enable end-to-end protection using client-side encryption" is the correct answer.

**INCORRECT:** "Use the UpdateTable operation to switch to a customer managed customer master key (CMK)" is incorrect. This will not ensure data is encrypted before it is submitted to DynamoDB; to meet this requirement, client-side encryption must be used.

**INCORRECT:** "Use the UpdateTable operation to switch to an AWS managed customer master key (CMK)" is incorrect. is will not ensure data is encrypted before it is submitted to DynamoDB; to meet this requirement, client-side encryption must be used.

**INCORRECT:** "Use AWS Certificate Manager (ACM) to create one certificate for each DynamoDB table" is incorrect. ACM is used to create SSL/TLS certificates and you cannot attach these to a DynamoDB table.

**References:**

[https://docs.aws.amazon.com/kms/latest/Developerguide/services-dynamodb.html](https://docs.aws.amazon.com/kms/latest/developerguide/services-dynamodb.html)

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-dynamodb/>

**Domain**

AWS Database

**Question 3Correct**

An organization wants to ensure that there is minimal latency for their customers on both the east and west coast of the United States. What can they do to provide optimal performance with minimal latency?

**Your answer is correct**

**Use Amazon Route 53 with latency-based routing by creating latency records in multiple AWS Regions.**

**Use Amazon CloudWatch to monitor traffic spikes and identify how to scale horizontally.**

**Use Amazon Route 53 to direct the traffic based on health checks.**

**Use AWS CloudTrail to monitor traffic and identify where requests are coming from and deploy the application to those Regions.**

Overall explanation

**CORRECT:**"Use Amazon Route 53 with latency-based routing by creating latency records in multiple AWS Regions" is the correct answer (as explained above.)

**INCORRECT:** "Use Amazon Route 53 to direct the traffic based on health checks" is incorrect. Health checks just show that the resource is healthy, and do not ensure that the best performing endpoint is chosen. Reducing latency is the best option here.

**INCORRECT:** "Use AWS CloudTrail to monitor traffic and identify where requests are coming from and deploy the application to those Regions" is incorrect. CloudTrail is used to monitor API calls.

**INCORRECT:** "Use Amazon CloudWatch to monitor traffic spikes and identify how to scale horizontally" is incorrect. CloudWatch does monitor spikes in usage, but it is not used to improve latency to end users.

**References**:

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-route-53/>

**Domain**

AWS Networking & Content Delivery

**Question 4Correct**

An organization has an account for each environment: Production, Testing, Development. A Developer with an IAM user in the Development account needs to launch resources in the Production and Testing accounts. What is the MOST efficient way to provide access

**Create a separate IAM user in each account and have the Developer login separately to each account**

**Create an IAM permissions policy in the Production and Testing accounts and reference the IAM user in the Development account**

**Create an IAM group in the Production and Testing accounts and add the Developer’s user from the Development account to the groups**

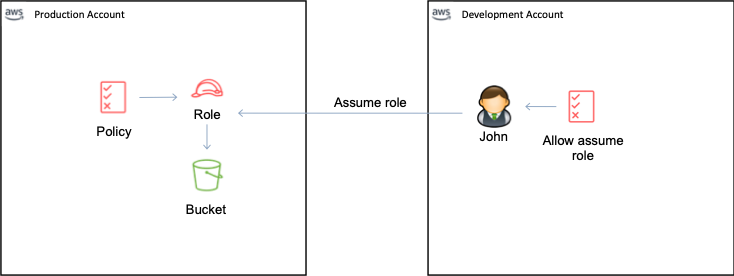
**Your answer is correct**

**Create a role with the required permissions in the Production and Testing accounts and have the Developer assume that role**

Overall explanation

You can grant your IAM users’ permission to switch to roles within your AWS account or to roles defined in other AWS accounts that you own. This is known as cross-account access.

In the image below a user in the Development account needs to access an S3 bucket in the Production account:



The user is able to assume the role in the Production account and access the S3 bucket. This is more efficient than providing the user with multiple accounts. In this scenario the user requests to switch to the role through either the console or the API/CLI.

**CORRECT:**"Create a role with the required permissions in the Production and Testing accounts and have the Developer assume that role" is the correct answer.

**INCORRECT:** "Create a separate IAM user in each account and have the Developer login separately to each account" is incorrect as this is not the most efficient method of providing access. Cross-account access is preferred .

**INCORRECT:** "Create an IAM group in the Production and Testing accounts and add the Developer’s user from the Development account to the groups" is incorrect as you cannot add an IAM user from another AWS account to a group.

**INCORRECT:** "Create an IAM permissions policy in the Production and Testing accounts and reference the IAM user in the Development account" is incorrect as you cannot reference an IAM user from another AWS account in a permissions policy.

**References:**

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_aws-accounts.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-iam/>

**Domain**

AWS Security, Identity, & Compliance

**Question 5Correct**

A serverless application uses an IAM role to authenticate and authorize access to an Amazon DynamoDB table. A Developer is troubleshooting access issues affecting the application. The Developer has access to the IAM role that the application is using.

Which of the following commands will help the Developer to test the role permissions using the AWS CLI?

**aws dynamodb describe-endpoints**

**Your answer is correct**

**aws sts assume-role**

**aws sts get-session-token**

**aws iam get-role-policy**

Overall explanation

The AWS CLI “aws sts assume role” command will enable the Developer to assume the role and gain temporary security credentials. The Developer can then use those security credentials to troubleshoot access issues that are affecting the application.

**CORRECT:**"aws sts assume-role" is the correct answer.

**INCORRECT:** "aws sts get-session-token" is incorrect. This is used to get temporary credentials for an AWS account or IAM user. It can subsequently be used to call the assume-role API.

**INCORRECT:** "aws iam get-role-policy" is incorrect. This command retrieves the specified inline policy document that is embedded with the specified IAM role.

**INCORRECT:** "aws dynamodb describe-endpoints" is incorrect. This command returns the regional endpoint information.

**References:**

<https://docs.aws.amazon.com/cli/latest/reference/sts/assume-role.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-dynamodb/>

**Domain**

AWS Security, Identity, & Compliance

**Question 6Incorrect**

A developer is using AWS AppConfig to deploy an application. The application's data needs to be encrypted when at rest. Which statement describes how this requirement is met?

**Data is automatically encrypted using AWS owned keys and AWS Key Management Service (KMS). The developer can disable this layer and instead add their own customer managed key.**

**Correct answer**

**Data is automatically encrypted using AWS owned keys. This cannot be disabled. The developer can add an additional layer of encryption using customer managed keys.**

**Data is stored in S3 buckets unencrypted by default. The developer can use AWS Key Management Service (KMS) to apply encryption keys to the data at rest.**

**Your answer is incorrect**

**Data is unencrypted by default. The developer can choose to use AWS managed keys or customer managed keys to encrypt the data.**

Overall explanation

AWS AppConfig will automatically encrypt data at rest using AWS owned keys and AWS Key Management Service (KMS). This layer cannot be disabled or altered by the customer. The customer can add a second layer of encryption protection that they can control and manage using customer managed keys.

**CORRECT**: "Data is automatically encrypted using AWS owned keys. This cannot be disabled. The developer can add an additional layer of encryption using customer managed keys" is the correct answer (as explained above.)

**INCORRECT**: "Data is automatically encrypted using AWS owned keys and AWS Key Management Service (KMS). The developer can disable this layer and instead add their own customer managed key" is incorrect. The default layer of encryption cannot be disabled. The developer can add a second layer of a customer managed key.

**INCORRECT**: "Data is stored in S3 buckets unencrypted by default. The developer can use AWS Key Management Service (KMS) to apply encryption keys to the data at rest" is incorrect. Data is encrypted by default using AWS owned keys. The developer can use customer managed keys to add a second layer of encryption.

**INCORRECT**: "Data is unencrypted by default. The developer can choose to use AWS managed keys or customer managed keys to encrypt the data" is incorrect. Data is encrypted by default using AWS managed keys and AWS Key Management Service (KMS). A second layer can be added using customer managed keys.

**References:**

<https://docs.aws.amazon.com/appconfig/latest/userguide/appconfig-security.html>

**Domain**

AWS Developer Tools

**Question 7Incorrect**

A company has deployed a REST API using Amazon API Gateway with a Lambda authorizer. The company needs to log who has accessed the API and how the caller accessed the API. They also require logs that include errors and execution traces for the Lambda authorizer.

Which combination of actions should the Developer take to meet these requirements? (Select TWO.)

**Your selection is incorrect**

**Enable detailed logging in Amazon CloudWatch.**

**Create an API Gateway usage plan.**

**Enable server access logging.**

**Correct selection**

**Enable API Gateway execution logging.**

**Your selection is correct**

**Enable API Gateway access logs.**

Overall explanation

There are two types of API logging in CloudWatch: execution logging and access logging. In execution logging, API Gateway manages the CloudWatch Logs. The process includes creating log groups and log streams, and reporting to the log streams any caller's requests and responses.

The logged data includes errors or execution traces (such as request or response parameter values or payloads), data used by Lambda authorizers, whether API keys are required, whether usage plans are enabled, and so on.

In access logging, you, as an API Developer, want to log who has accessed your API and how the caller accessed the API. You can create your own log group or choose an existing log group that could be managed by API Gateway.

**CORRECT:**"Enable API Gateway execution logging" is a correct answer.

**CORRECT:**"Enable API Gateway access logs" is also a correct answer.

**INCORRECT:** "Enable detailed logging in Amazon CloudWatch" is incorrect. Detailed logging does not provide the requested information.

**INCORRECT:** "Create an API Gateway usage plan" is incorrect. This will not enable logging.

**INCORRECT:** "Enable server access logging" is incorrect. This is a type of logging that applies to Amazon S3 buckets.

**References:**

[https://docs.aws.amazon.com/apigateway/latest/Developerguide/set-up-logging.html](https://docs.aws.amazon.com/apigateway/latest/developerguide/set-up-logging.html)

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-cloudwatch/>

**Domain**

AWS Networking & Content Delivery

**Question 8Incorrect**

A company has an application that provides access to objects in Amazon S3 based on the type of user. The user types are registered user and guest user. The company has 30,000 users. Information is read from an S3 bucket depending on the user type.

Which approaches are recommended to provide access to both user types MOST efficiently? (Select TWO.)

**Correct selection**

**Use the AWS IAM service and let the application assume different roles depending on the type of user.**

**Your selection is incorrect**

**Store separate access keys in the application code for registered users and guest users to provide access to the objects.**

**Create a new IAM user for each user and grant access to the S3 objects.**

**Use S3 bucket policies to restrict read access to specific IAM users.**

**Your selection is correct**

**Use Amazon Cognito to provide access using authenticated and unauthenticated roles.**

Overall explanation

Amazon Cognito can be used with identity pools. A Cognito identity pool supports both authenticated and unauthenticated identities. Authenticated identities belong to users who are authenticated by any supported identity provider. Unauthenticated identities typically belong to guest users.

The most secure way of using the IAM service for this solution would be to use separate roles. IAM roles can be securely assumed based on the type of user. Each role can be configured with different permission sets as applicable to registered and guest users.

**CORRECT:**"Use Amazon Cognito to provide access using authenticated and unauthenticated roles" is a correct answer (as explained above.)

**CORRECT:**"Use the AWS IAM service and let the application assume different roles depending on the type of user" is also a correct answer (as explained above.)

**INCORRECT:** "Store separate access keys in the application code for registered users and guest users to provide access to the objects" is incorrect.

This is highly insecure. You should avoid embedding access keys in application code and use IAM roles instead.

**INCORRECT:** "Create a new IAM user for each user and grant access to the S3 objects" is incorrect.

This would be a lot of users and is an inefficient solution.

**INCORRECT:** "Use S3 bucket policies to restrict read access to specific IAM users" is incorrect.

This would also be highly complex with so many users and would need constant updating when users need to be added or removed.

**References:**

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

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-iam/>

<https://digitalcloud.training/amazon-cognito/>

**Domain**

AWS Security, Identity, & Compliance

**Question 9Correct**

A Developer is creating a serverless application that will process sensitive data. The AWS Lambda function must encrypt all data that is written to /tmp storage at rest.

How should the Developer encrypt this data?

**Enable secure connections over HTTPS for the AWS Lambda API endpoints using Transport Layer Security (TLS).**

**Attach the Lambda function to a VPC and encrypt Amazon EBS volumes at rest using the AWS managed CMK. Mount the EBS volume to /tmp.**

**Enable default encryption on an Amazon S3 bucket using an AWS KMS customer managed customer master key (CMK). Mount the S3 bucket to /tmp.**

**Your answer is correct**

**Configure Lambda to use an AWS KMS customer managed customer master key (CMK). Use the CMK to generate a data key and encrypt all data prior to writing to /tmp storage.**

Overall explanation

On a per-function basis, you can configure Lambda to use an encryption key that you create and manage in AWS Key Management Service. These are referred to as customer managed customer master keys (CMKs) or customer managed keys. If you don't configure a customer managed key, Lambda uses an AWS managed CMK named aws/lambda, which Lambda creates in your account.

The CMK can be used to generate a data encryption key that can be used for encrypting all data uploaded to Lambda or generated by Lambda.

**CORRECT:**"Configure Lambda to use an AWS KMS customer managed customer master key (CMK). Use the CMK to generate a data key and encrypt all data prior to writing to /tmp storage" is the correct answer.

**INCORRECT:** "Attach the Lambda function to a VPC and encrypt Amazon EBS volumes at rest using the AWS managed CMK. Mount the EBS volume to /tmp" is incorrect. You cannot attach an EBS volume to a Lambda function.

**INCORRECT:** "Enable default encryption on an Amazon S3 bucket using an AWS KMS customer managed customer master key (CMK). Mount the S3 bucket to /tmp" is incorrect. You cannot mount an S3 bucket to a Lambda function.

**INCORRECT:** "Enable secure connections over HTTPS for the AWS Lambda API endpoints using Transport Layer Security (TLS)" is incorrect. The Lambda API endpoints are always encrypted using TLS and this is encryption in-transit not encryption at-rest.

**References:**

<https://docs.aws.amazon.com/lambda/latest/dg/security-dataprotection.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-lambda/>

**Domain**

AWS Security, Identity, & Compliance

**Question 10Incorrect**

A developer received the following error message during an AWS CloudFormation deployment:

DELETE\_FAILED (The following resource(s) failed to delete: (sg-11223344).)

Which action should the developer take to resolve this error?

**Manually delete the security group. Then execute a change set to force deletion of the CloudFormation stack.**

**Correct answer**

**Modify the CloudFormation template to retain the security group resource. Then manually delete the resource after deployment.**

**Your answer is incorrect**

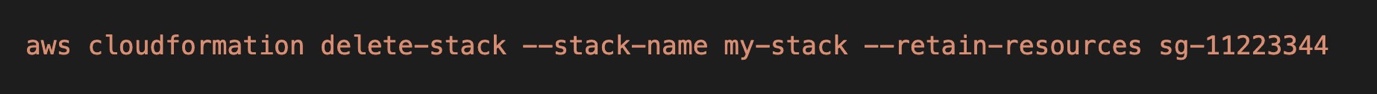
**Add a DependsOn attribute to the sg-11223344 resource in the CloudFormation template. Then delete the stack.**

**Update the logical ID of the security group resource with the security groups ARN. Then delete the stack.**

Overall explanation

The stack may be stuck in the DELETE\_FAILED state because the dependent object (security group), can't be deleted. This can be for many reasons, for example, the security group could have an ENI attached that’s not part of the CloudFormation stack.

To delete the stack you must choose to delete the stack in the console and then select to retain the resource(s) that failed to delete. This can also be achieved from the AWS CLI:



**CORRECT:**"Modify the CloudFormation template to retain the security group resource. Then manually delete the resource after deployment" is the correct answer (as explained above.)

**INCORRECT:** "Add a DependsOn attribute to the sg-11223344 resource in the CloudFormation template. Then delete the stack" is incorrect.

This creates a dependency for stack creation. It does not assist with resolving the issue that is preventing the stack from deleting successfully.

**INCORRECT:** "Manually delete the security group. Then execute a change set to force deletion of the CloudFormation stack" is incorrect.

You can manually delete the security group. However, you would not then use a change set to continue with the deletion. You would instead simply choose to delete the stack from the console or the CLI.

**INCORRECT:** "Update the logical ID of the security group resource with the security groups ARN. Then delete the stack" is incorrect.

The issue has nothing to do with logical IDs or ARNs. The resource cannot be deleted by CloudFormation so the developer simply needs to choose to retain the resource before continuing with the stack deletion process.

**References:**

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stacks-changesets.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-cloudformation/>

**Domain**

AWS Management & Governance

**Question 11Correct**

A team of Developers are working on a shared project and need to be able to collaborate on code. The shared application code must be encrypted at rest, stored on a highly available and durable architecture, and support multiple versions and batch change tracking.

Which AWS service should the Developer use?

**Your answer is correct**

**AWS CodeCommit**

**AWS Cloud9**

**Amazon S3**

**AWS CodeBuild**

Overall explanation

AWS CodeCommit is a fully managed source control service that hosts secure Git-based repositories. It makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem. AWS CodeCommit automatically encrypts your files in transit and at rest.

AWS CodeCommit helps you collaborate on code with teammates via pull requests, branching, and merging. You can implement workflows that include code reviews and feedback by default, and control who can make changes to specific branches.

**CORRECT:**"AWS CodeCommit" is the correct answer.

**INCORRECT:** "AWS CodeBuild" is incorrect. AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages

**INCORRECT:** "Amazon S3" is incorrect. Amazon S3 is an object-based storage system and does not support the features required here.

**INCORRECT:** "AWS Cloud9" is incorrect. AWS Cloud9 is a cloud-based integrated development environment (IDE) that lets you write, run, and debug your code with just a browser.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-developer-tools/>

**Domain**

AWS Developer Tools

**Question 12Incorrect**

A start-up organization imported their X.509 certificate from another issuer into AWS Certificate Manager (ACM) approximately 11 months ago. What needs to be done to ensure that visitors will continue to have secure access to the website? (Select TWO.)

**Your selection is correct**

**A new certificate will need to be imported into ACM.**

**Correct selection**

**A new certificate will need to be requested from ACM.**

**Your selection is incorrect**

**A new certificate will automatically be created prior to the certificate expiring at 13 months.**

**A new certificate will be automatically imported into ACM.**

**A new certificate will automatically be created prior to the certificate expiring at 12 months.**

Overall explanation

AWS ACM issued certificates are valid for 13 months. They are also renewed automatically. Imported certificates are not automatically renewed and would need to be imported once created from the third party.

**CORRECT:**"A new certificate will need to be requested from ACM" is the correct answer (as explained above.)

**CORRECT:**"A new certificate will need to be imported into ACM” is also a correct answer (as explained above.)

**INCORRECT:** "A new certificate will automatically be created prior to the certificate expiring at 12 months" is incorrect. Imported certificates are not automatically renewed by AWS ACM.

**INCORRECT:** "A new certificate will automatically be created prior to the certificate expiring at 13 months" is incorrect. Imported certificates are not automatically renewed by AWS ACM.

**INCORRECT:** "A new certificate will be automatically imported into ACM" is incorrect. A new certificate issued by a third-party can be imported but it is not automatically done.

**References**:

<https://docs.aws.amazon.com/acm/latest/userguide/managed-renewal.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-certificate-manager/>

**Domain**

AWS Security, Identity, & Compliance

**Question 13Correct**

A developer is implementing Amazon ElastiCache in an application that needs to reflect real-time data on dashboards. The data is sourced from a database and needs to be stored in the cache.

What would be the ideal caching mechanism for this requirement?

**A write-behind cache**

**Your answer is correct**

**A write-through cache**

**A read-through cache**

**A lazy-loading cache**

Overall explanation

The write-through caching strategy ensures that data is written into the cache every time it's updated in the database. This makes it an ideal strategy for scenarios where real-time data is required on dashboards as it reduces the chances of a cache miss, and any read request will have the latest data.

**CORRECT:**"A write-through cache" is the correct answer (as explained above.)

**INCORRECT:** "A lazy-loading cache" is incorrect.

Lazy-loading strategy only caches the data when a request for that data is made. This might cause a delay in populating real-time dashboards during the first request for data.

**INCORRECT:** "A write-behind cache" is incorrect.

Write-behind caching is not supported by Amazon ElastiCache. This strategy can lead to data inconsistency between the cache and the database.

**INCORRECT:** "A read-through cache" is incorrect.

Read-through caches are not supported by Amazon ElastiCache.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-elasticache/>

**Domain**

AWS Database

**Question 14Correct**

A Developer implemented a static website hosted in Amazon S3 that makes web service requests hosted in Amazon API Gateway and AWS Lambda. The site is showing an error that reads:

“No ‘Access-Control-Allow-Origin’ header is present on the requested resource. Origin ‘null’ is therefore not allowed access.”

What should the Developer do to resolve this issue?

**Enable cross-origin resource sharing (CORS) on the S3 bucket**

**Add the Access-Control-Request-Method header to the request**

**Your answer is correct**

**Enable cross-origin resource sharing (CORS) for the method in API Gateway**

**Add the Access-Control-Request-Headers header to the request**

Overall explanation

Cross-origin resource sharing (CORS) defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. In this scenario the S3 bucket is the requestor and is requesting access to resources served by Amazon API Gateway and AWS Lambda. Therefore, the CORS configuration must be enabled on the requested endpoint which is the method in API Gateway.

**CORRECT:**"Enable cross-origin resource sharing (CORS) for the method in API Gateway" is the correct answer.

**INCORRECT:** "Enable cross-origin resource sharing (CORS) on the S3 bucket" is incorrect as CORS must be enabled on the requested endpoint which is API Gateway, not S3.

**INCORRECT:** "Add the Access-Control-Request-Method header to the request" is incorrect as this is a request header value that asks permission to use a specific HTTP method.

**INCORRECT:** "Add the Access-Control-Request-Headers header to the request" is incorrect as this notifies a server what headers will be sent in a request.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-s3-and-glacier/>

**Domain**

AWS Storage

**Question 15Incorrect**

A developer needs to create a serverless application that uses an event-driven architecture.

How can the developer configure the application to automatically receive and process events?

**Create an Amazon SQS topic and an Amazon EC2 instance. Subscribe the instance to the SNS topic and submit events to the topic.**

**Correct answer**

**Create an Amazon SNS topic and an AWS Lambda function. Subscribe the Lambda function to the SNS topic and submit events to the SNS topic.**

**Create an Amazon SQS queue and publish events to the queue. Configure an Amazon EC2 instance to poll the queue and consume the messages.**

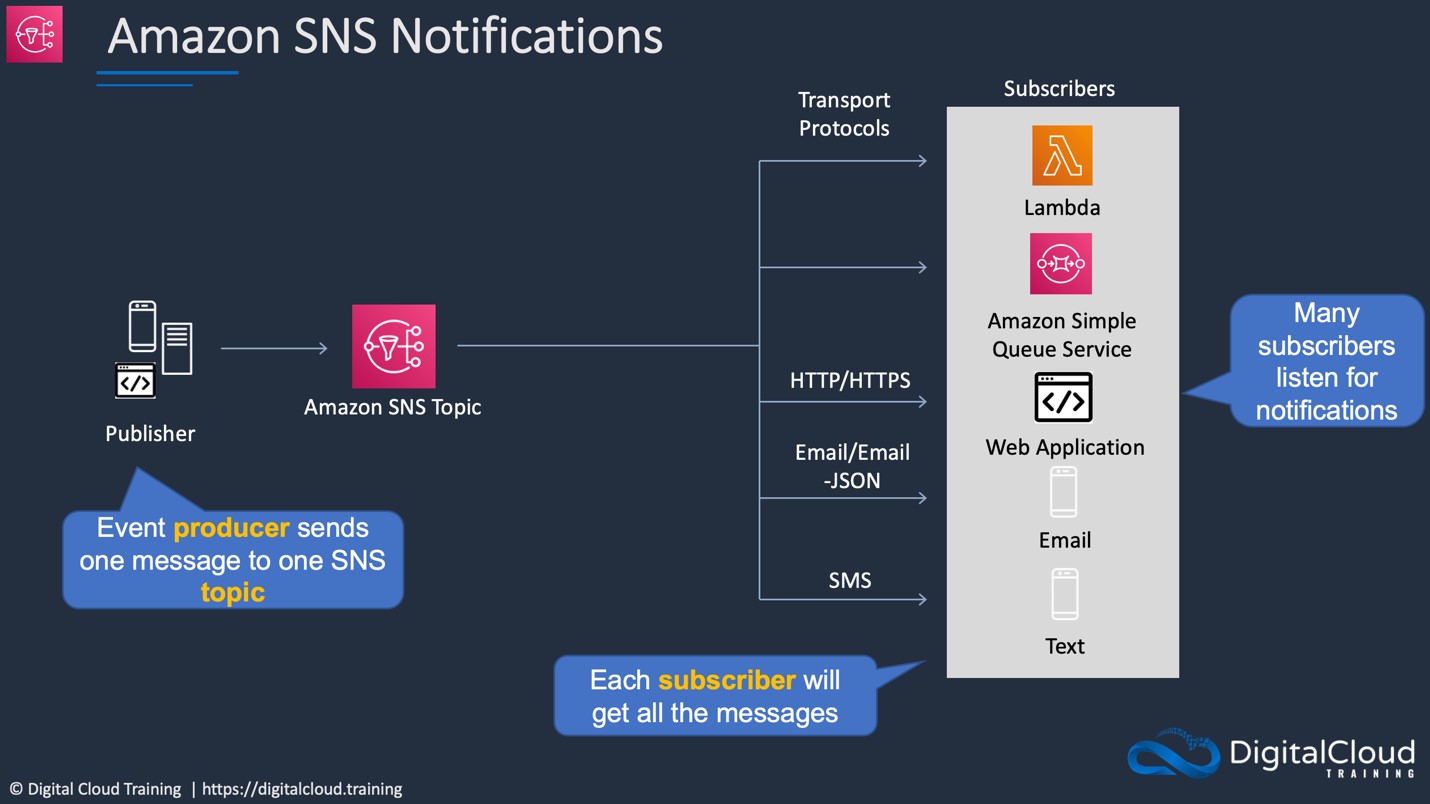
**Your answer is incorrect**

**Create an Amazon SNS topic and an AWS Lambda function. Configure an HTTP endpoint on the Lambda function and subscribe the HTTP endpoint to the SNS topic. Submit events to the SNS topic.**

Overall explanation

You can use a Lambda function to process Amazon Simple Notification Service (Amazon SNS) notifications. Amazon SNS supports Lambda functions as a target for messages sent to a topic. You can subscribe your function to topics in the same account or in other AWS accounts.

When an event is submitted to the SNS topic it will be sent to AWS Lambda which can then process the event. This is an example of a simple event-driven architecture.



**CORRECT:**"Create an Amazon SNS topic and an AWS Lambda function. Subscribe the Lambda function to the SNS topic and submit events to the SNS topic" is the correct answer (as explained above.)

**INCORRECT:** "Create an Amazon SQS queue and publish events to the queue. Configure an Amazon EC2 instance to poll the queue and consume the messages" is incorrect.

Amazon EC2 is not a serverless service so cannot if the application must be serverless.

**INCORRECT:** "Create an Amazon SQS topic and an Amazon EC2 instance. Subscribe the instance to the SNS topic and submit events to the topic" is incorrect.

EC2 is not serverless and cannot be subscribed to an SNS topic.

**INCORRECT:** "Create an Amazon SNS topic and an AWS Lambda function. Configure an HTTP endpoint on the Lambda function and subscribe the HTTP endpoint to the SNS topic. Submit events to the SNS topic" is incorrect.

An HTTP endpoint is not required for the serverless application. Lambda can be subscribed directly to an SNS topic.

**References:**

<https://docs.aws.amazon.com/lambda/latest/dg/with-sns.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-application-integration-services/>

**Domain**

AWS Application Integration

**Question 16Incorrect**

A static website that serves a collection of images runs from an Amazon S3 bucket in the us-east-1 region. The website is gaining in popularity and is now being viewed around the world. How can a Developer improve the performance of the website for global users?

**Correct answer**

**Use Amazon CloudFront to cache the website content**

**Use Amazon ElastiCache to cache the website content**

**Your answer is incorrect**

**Use cross region replication to replicate the bucket to several global regions**

**Use Amazon S3 Transfer Acceleration to improve the performance of the website**

Overall explanation

CloudFront is a web service that gives businesses and web application developers an easy and cost-effective way to distribute content with low latency and high data transfer speeds. CloudFront is a good choice for distribution of frequently accessed static content that benefits from edge delivery—like popular website images, videos, media files or software downloads.

**CORRECT:**"Use Amazon CloudFront to cache the website content" is the correct answer.

**INCORRECT:** "Use Amazon ElastiCache to cache the website content" is incorrect as ElastiCache is used for caching the contents of databases, not S3 buckets.

**INCORRECT:** "Use cross region replication to replicate the bucket to several global regions" is incorrect as though this would get the content closer to users it would not provide a mechanism for connecting to those copies. This could be achieved using Route 53 latency based routing however it would be easier to use CloudFront.

**INCORRECT:** "Use Amazon S3 Transfer Acceleration to improve the performance of the website" is incorrect as this service is used for improving the performance of uploads to Amazon S3.

**References:**

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

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-cloudfront/>

**Domain**

AWS Networking & Content Delivery

**Question 17Incorrect**

A company maintains a REST API service using Amazon API Gateway with native API key validation. The company recently launched a new registration page, which allows users to sign up for the service. The registration page creates a new API key using CreateApiKey and sends the new key to the user. When the user attempts to call the API using this key, the user receives a 403 Forbidden error. Existing users are unaffected and can still call the API.

What code updates will grant these new users’ access to the API?

**The importApiKeys method must be called to import all newly created API keys into the current stage of the API**

**Correct answer**

**The createUsagePlanKey method must be called to associate the newly created API key with the correct usage plan**

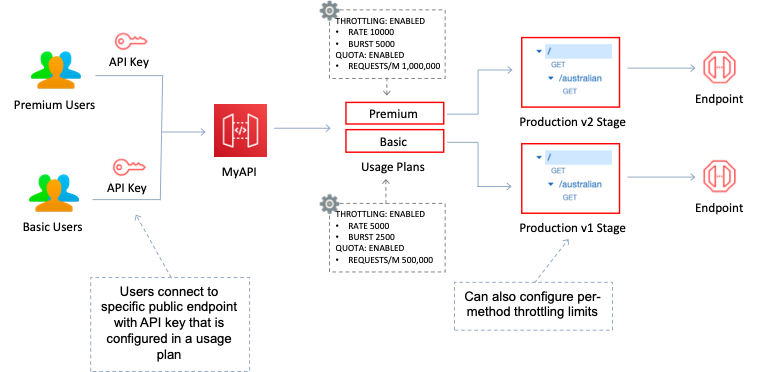
**Your answer is incorrect**

**The updateAuthorizer method must be called to update the API’s authorizer to include the newly created API key**

**The createDeployment method must be called so the API can be redeployed to include the newly created API key**

Overall explanation

A usage plan specifies who can access one or more deployed API stages and methods—and also how much and how fast they can access them. The plan uses API keys to identify API clients and meters access to the associated API stages for each key. It also lets you configure throttling limits and quota limits that are enforced on individual client API keys.



API keys are alphanumeric string values that you distribute to application developer customers to grant access to your API. You can use API keys together with [usage plans](https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html) or [Lambda authorizers](https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-use-lambda-authorizer.html) to control access to your APIs. API Gateway can generate API keys on your behalf, or you can import them from a [CSV file](https://docs.aws.amazon.com/apigateway/latest/developerguide/api-key-file-format.html). You can generate an API key in API Gateway, or import it into API Gateway from an external source.

To associate the newly created key with a usage plan the CreatUsagePlanKey API can be called. This creates a usage plan key for adding an existing API key to a usage plan.

**CORRECT:**"The createUsagePlanKey method must be called to associate the newly created API key with the correct usage plan" is the correct answer.

**INCORRECT:** "The createDeployment method must be called so the API can be redeployed to include the newly created API key" is incorrect as you do not need to redeploy an API to a stage in order to associate an API key.

**INCORRECT:** "The updateAuthorizer method must be called to update the API’s authorizer to include the newly created API key" is incorrect as this updates and authorizer resource, not an API key.

**INCORRECT:** "The importApiKeys method must be called to import all newly created API keys into the current stage of the API" is incorrect as this imports API keys to API Gateway from an external source such as a CSV file which is not relevant to this scenario.

**References:**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>

<http://docs.amazonaws.cn/en_us/sdkfornet/v3/apidocs/items/APIGateway/MAPIGatewayCreateUsagePlanKeyCreateUsagePlanKeyRequest.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-api-gateway/>

**Domain**

AWS Networking & Content Delivery

**Question 18Correct**

A Developer is attempting to call the Amazon CloudWatch API and is receiving HTTP 400: ThrottlingException errors intermittently. When a call fails, no data is retrieved.

What best practice should the Developer first attempt to resolve this issue?

**Analyze the applications and remove the API call**

**Contact AWS Support for a limit increase**

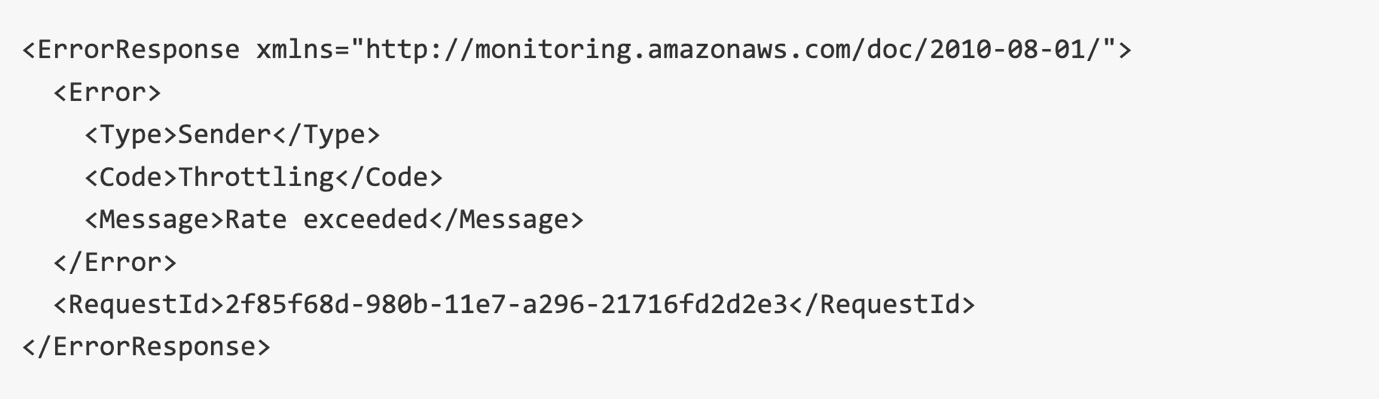
**Use the AWS CLI to get the metrics**

**Your answer is correct**

**Retry the call with exponential backoff**

Overall explanation

Occasionally ,you may receive the 400 ThrottlingException error for PutMetricData API calls in Amazon CloudWatch with a detailed response similar the following:



CloudWatch requests are throttled for each Amazon Web Services (AWS) account on a per-Region basis to help service performance. For current PutMetricData API request limits, see CloudWatch Limits.

All calls to the PutMetricData API in an AWS Region count towards the maximum allowed request rate. This number includes calls from any custom or third-party application, such as calls from the CloudWatch Agent, the AWS Command Line Interface (AWS CLI), or the AWS Management Console.

**Resolutions:**It's a best practice to use the following methods to reduce your call rate and avoid API throttling:

- Distribute your API calls evenly over time rather than making several API calls in a short time span. If you require data to be available with a one-minute resolution, you have an entire minute to emit that metric. Use jitter (randomized delay) to send data points at various times.

- Combine as many metrics as possible into a single API call. For example, a single PutMetricData call can include 20 metrics and 150 data points. You can also use pre-aggregated data sets, such as StatisticSet, to publish aggregated data points, thus reducing the number of PutMetricData calls per second.

- Retry your call with exponential backoff and jitter.

Following attempting the above resolutions AWS suggest the following: “If you still require a higher limit, you can [request a limit increase](https://console.aws.amazon.com/support/home#/case/create?issueType=service-limit-increase&limitType=service-code-amazon-cloudwatch). Increasing the rate limit can have a high financial impact on your AWS bill.”

Therefore, the first thing the Developer should do, from the list of options presented, is to retry the call with exponential backoff.

**CORRECT:**"Retry the call with exponential backoff" is the correct answer.

**INCORRECT:** "Contact AWS Support for a limit increase" is incorrect. As mentioned above, there are other resolutions the Developer should attempt before contacting support to raise the limit.

**INCORRECT:** "Use the AWS CLI to get the metrics" is incorrect as this will still make the same API calls.

**INCORRECT:** "Analyze the applications and remove the API call" is incorrect as this is not a good resolution to the issue as this may mean that important monitoring and logging data is not recorded for the application.

**References:**

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudwatch-400-error-throttling/>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-cloudwatch/>

**Domain**

AWS Management & Governance

**Question 19Correct**

A programmer is rolling out a new solution to Amazon ECS. This solution necessitates secure handling and access to diverse variables such as credentials, remote API authentication details, and the API URL. The remote API authentication information and API URL should be accessible across all versions of the solution, spanning development, testing, and production environments.

What is the most efficient method for the programmer to access these variables with minimal modifications to the solution?

**Use AWS S3 to store these variables and access them via AWS SDK within the application.**

**Create environment variables for these details and access them within the application code.**

**Your answer is correct**

**Utilize AWS Secrets Manager to store these variables and retrieve them directly within the application using AWS SDK.**

**Include these variables directly in the application code and use version control system to manage different versions.**

Overall explanation

AWS Secrets Manager is designed to handle sensitive data like this. It enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Using AWS Secrets Manager, you can secure and manage secrets used to access resources in the AWS Cloud, on third-party services, and on-premises.

**CORRECT:**"Utilize AWS Secrets Manager to store these variables and retrieve them directly within the application using AWS SDK" is the correct answer (as explained above.)

**INCORRECT:** "Include these variables directly in the application code and use version control system to manage different versions" is incorrect.

Including sensitive data directly in the application code is not a secure practice and doesn't comply with the principle of least privilege or best security practices.

**INCORRECT:** "Create environment variables for these details and access them within the application code" is incorrect.

Although environment variables can be used to pass some configuration to the application, they're typically visible in plaintext in multiple places such as ECS Task Definitions or the ECS console. This makes them unsuitable for sensitive data like credentials or API keys.

**INCORRECT:** "Use AWS S3 to store these variables and access them via AWS SDK within the application" is incorrect.

AWS S3 is primarily a storage service and using it to store and manage secrets doesn't align with security best practices.

**References:**

<https://aws.amazon.com/secrets-manager/>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-secrets-manager/>

**Domain**

AWS Security, Identity, & Compliance

**Question 20Correct**

An organization is modernizing a software solution by migrating its database operations from Amazon EC2 instances to a serverless architecture. The software utilizes an Amazon RDS for PostgreSQL database and operates within a single VPC on AWS. Both the software and the database are currently deployed on a private subnet in the VPC. The organization needs to enable AWS Lambda functions to interact with the PostgreSQL database.

Which solution would securely satisfy these needs?

**Establish an AWS Direct Connect link between the Lambda functions and the RDS instance.**

**Configure the Lambda functions to connect directly to the RDS instance by using its public IP address.**

**Deploy an AWS AppRunner service in the VPC, which will host the Lambda functions and connect them to the RDS instance.**

**Your answer is correct**

**Place the Lambda functions within the same VPC as the RDS instance and ensure they have an appropriate security group rule to access the RDS instance.**

Overall explanation

Placing the Lambda functions within the same VPC as the RDS instance and ensuring they have an appropriate security group rule to access the RDS instance would allow the Lambda functions to interact with the PostgreSQL database without exposing the database to the public internet, keeping the operations secure and in line with the existing infrastructure.

**CORRECT:**"Place the Lambda functions within the same VPC as the RDS instance and ensure they have an appropriate security group rule to access the RDS instance" is the correct answer (as explained above.)

**INCORRECT:** "Configure the Lambda functions to connect directly to the RDS instance by using its public IP address" is incorrect.

Configuring the Lambda functions to connect directly to the RDS instance using its public IP address is insecure and goes against best practices for keeping resources in private subnets isolated.

**INCORRECT:** "Deploy an AWS AppRunner service in the VPC, which will host the Lambda functions and connect them to the RDS instance" is incorrect.

AWS App Runner is primarily designed for building, deploying, and scaling containerized applications quickly, and is not suited to hosting Lambda functions or establishing connections with an RDS instance.

**INCORRECT:** "Establish an AWS Direct Connect link between the Lambda functions and the RDS instance" is incorrect.

AWS Direct Connect is used for establishing a dedicated network connection from your premises to AWS and would not be applicable or necessary for Lambda functions trying to connect to an RDS instance within the same AWS environment.

**References:**

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-lambda/>

**Domain**

AWS Compute

**Question 21Correct**

A developer is creating a serverless web application that includes AWS Lambda functions and a REST API deployed using Amazon API Gateway. The developer maintains multiple branches of code. The developer wants to avoid updating the API gateway target endpoint when a new code push is performed.

What solution would allow the developer to update the Lambda code without needing to update the REST API configuration?

**Create multiple stages and deployments.**

**Your answer is correct**

**Create aliases and versions in AWS Lambda.**

**Create multiple private API endpoints and use CNAMEs.**

**Create different tags for each Lambda function.**

Overall explanation

You can create one or more aliases for your Lambda function. A Lambda alias is like a pointer to a specific function version. Users can access the function version using the alias Amazon Resource Name (ARN). You can then release new versions of your code without needing to change the alias that applications use to invoke the function.

In this case the REST API could be configured with aliases for the functions. The developer could also use different stages with different endpoints using the aliases. This would enable calling different versions of the application by changing the stage name in the REST API URL.

**CORRECT:**"Create aliases and versions in AWS Lambda" is the correct answer (as explained above.)

**INCORRECT:** "Create multiple stages and deployments" is incorrect.

Stages and stage variables could be used to reference different functions or aliases. But if only stages and deployments are used (and not a Lambda alias) then the REST API would need to have the endpoint updated every time a new function version is released.

**INCORRECT:** "Create different tags for each Lambda function" is incorrect.

Tags cannot be used to define the Lambda endpoints in the REST API.

**INCORRECT:** "Create multiple private API endpoints and use CNAMEs" is incorrect.

There is no value here in creating multiple private API endpoints as that would be completely different APIs.

**References:**

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-aliases.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-lambda/>

**Domain**

AWS Compute

**Question 22Incorrect**

A company is deploying a serverless application on AWS, using an AWS Lambda function for handling customer orders. This function utilizes an external HTTP API for processing payments, which occasionally times out. The requirement is to notify the support team via an existing Amazon SNS topic when the error rate of this API surpasses 10% per hour.

How can this be achieved?

**Correct answer**

**Implement Amazon CloudWatch Metrics with a custom threshold and link it to the existing SNS topic.**

**Your answer is incorrect**

**Use AWS X-Ray to monitor the error rate and configure it to send alerts through the SNS topic.**

**Configure the AWS Lambda function to directly send alerts to the SNS topic when there is a timeout.**

**Enable AWS CloudTrail to monitor the Lambda function and send alerts to the SNS topic when the error rate exceeds 10%.**

Overall explanation

Amazon CloudWatch Metrics can monitor and track API error rates and can be configured to trigger an alert when a particular threshold is surpassed. By linking this to the existing Amazon SNS topic, the support team can be notified in near real-time when the payment processing external API error rate exceeds 10% of the total number of transactions in an hour.

**CORRECT:**"Implement Amazon CloudWatch Metrics with a custom threshold and link it to the existing SNS topic" is the correct answer (as explained above.)

**INCORRECT:** "Use AWS X-Ray to monitor the error rate and configure it to send alerts through the SNS topic" is incorrect.

AWS X-Ray is more suited for tracing applications to debug and analyze individual user paths, rather than for real-time alerting on API error rates.

**INCORRECT:** "Configure the AWS Lambda function to directly send alerts to the SNS topic when there is a timeout" is incorrect.

Modifying the Lambda function to directly send alerts may increase the complexity of the function and may not be as reliable or timely as using a dedicated monitoring service like CloudWatch.

**INCORRECT:** "Enable AWS CloudTrail to monitor the Lambda function and send alerts to the SNS topic when the error rate exceeds 10%" is incorrect.

AWS CloudTrail is a service that provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services. It is not designed to monitor error rates of APIs or Lambda functions and trigger alerts based on those.

**References:**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/welcome.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-cloudwatch/>

**Domain**

AWS Management & Governance

**Question 23Correct**

An application runs on a fleet of Amazon EC2 instances in an Auto Scaling group. The application stores data in an Amazon DynamoDB table and all instances make updates to the table. When querying data, EC2 instances sometimes retrieve stale data. The Developer needs to update the application to ensure the most up-to-date data is retrieved for all queries.

How can the Developer accomplish this?

**Cache the database writes using Amazon DynamoDB Accelerator.**

**Your answer is correct**

**Set the ConsistentRead parameter to true when calling GetItem.**

**Use the TransactWriteItems API when issuing PutItem actions.**

**Use the UpdateGlobalTable API to create a global secondary index.**

Overall explanation

DynamoDB supports eventually consistent and strongly consistent reads. When using eventually consistent reads the response might not reflect the results of a recently completed write operation. The response might include some stale data.

When using strongly consistent reads DynamoDB returns a response with the most up-to-date data, reflecting the updates from all prior write operations that were successful.

DynamoDB uses eventually consistent reads unless you specify otherwise. Read operations (such as GetItem, Query, and Scan) provide a ConsistentRead parameter. If you set this parameter to true, DynamoDB uses strongly consistent reads during the operation.

**CORRECT:**"Set the ConsistentRead parameter to true when calling GetItem" is the correct answer.

**INCORRECT:** "Cache the database writes using Amazon DynamoDB Accelerator" is incorrect. DynamoDB DAX caches items from DynamoDB to improve read performance but will not ensure the latest data is retrieved.

**INCORRECT:** "Use the TransactWriteItems API when issuing PutItem actions" is incorrect. This operation is used to group transactions in an all-or-nothing update.

**INCORRECT:** "Use the UpdateGlobalTable API to create a global secondary index" is incorrect. A GSI does not assist in any way in this solution.

**References:**

[https://docs.aws.amazon.com/amazondynamodb/latest/Developerguide/HowItWorks.ReadConsistency.html](https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadConsistency.html)

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-dynamodb/>

**Domain**

AWS Database

**Question 24Correct**

A new application will be hosted on the domain name dctlabs.com using an Amazon API Gateway REST API front end. The Developer needs to configure the API with a path to dctlabs.com/products that will be accessed using the HTTP GET verb. How MUST the Developer configure the API? (Select TWO

**Your selection is correct**

**Create a GET method**

**Create a /products method**

**Create a /GET method**

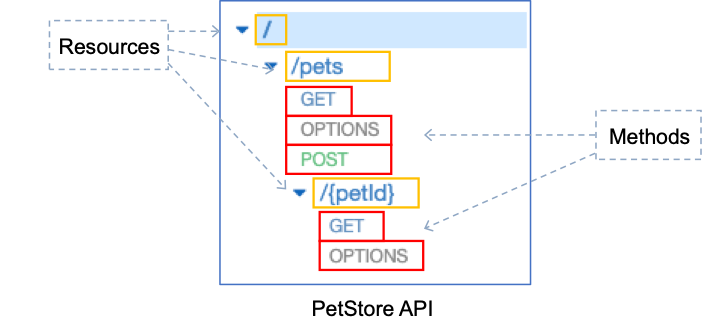
**Your selection is correct**

**Create a /products resource**

**Create a GET resource**

Overall explanation

An API Gateway REST API is a collection of HTTP resources and methods that are integrated with backend HTTP endpoints, Lambda functions, or other AWS services. You can deploy this collection in one or more stages. Typically, API resources are organized in a resource tree according to the application logic. Each API resource can expose one or more API methods that have unique HTTP verbs supported by API Gateway.



As you can see from the image above, the Developer would need to create a resource which in this case would be /products. The Developer would then create a GET method within the resource.

**CORRECT:**"Create a /products resource" is a correct answer.

**CORRECT:**"Create a GET method" is a correct answer.

**INCORRECT:** "Create a /products method" is incorrect as a resource should be created.

**INCORRECT:** "Create a GET resource" is incorrect as a method should be created.

**INCORRECT:** "Create a /GET method" is incorrect as a method is not preceded by a slash.

**References:**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-basic-concept.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-api-gateway/>

**Domain**

AWS Networking & Content Delivery

**Question 25Correct**

An application will be hosted on the AWS Cloud. Developers will be using an Agile software development methodology with regular updates deployed through a continuous integration and delivery (CI/CD) model. Which AWS service can assist the Developers with automating the build, test, and deploy phases of the release process every time there is a code change?

**AWS Elastic Beanstalk**

**AWS CloudFormation**

**Your answer is correct**

**AWS CodePipeline**

**AWS CodeBuild**

Overall explanation

AWS CodePipeline is a continuous delivery service you can use to model, visualize, and automate the steps required to release your software. You can quickly model and configure the different stages of a software release process. CodePipeline automates the steps required to release your software changes continuously.

Specifically, you can:

**Automate your release processes**: CodePipeline fully automates your release process from end to end, starting from your source repository through build, test, and deployment. You can prevent changes from moving through a pipeline by including a manual approval action in any stage except a Source stage. You can release when you want, in the way you want, on the systems of your choice, across one instance or multiple instances.

**Establish a consistent release process**: Define a consistent set of steps for every code change. CodePipeline runs each stage of your release according to your criteria.

**Speed up delivery while improving quality**: You can automate your release process to allow your developers to test and release code incrementally and speed up the release of new features to your customers.

**Use your favorite tools**: You can incorporate your existing source, build, and deployment tools into your pipeline.

**View progress at a glance**: You can review real-time status of your pipelines, check the details of any alerts, retry failed actions, view details about the source revisions used in the latest pipeline execution in each stage, and manually rerun any pipeline.

**View pipeline history details**: You can view details about executions of a pipeline, including start and end times, run duration, and execution IDs.

Therefore, AWS CodePipeline is the perfect tool for the Developer’s requirements.

**CORRECT:**"AWS CodePipeline" is the correct answer.

**INCORRECT:** "AWS CloudFormation" is incorrect as CloudFormation is not triggered by changes in a source code repository. You must create change sets for deploying updates.

**INCORRECT:** "AWS Elastic Beanstalk" is incorrect as this is a platform service that can be used to deploy code to managed runtimes such as Nodejs. It does not update automatically based on changes to source code. You must update that environment when you need to release new code.

**INCORRECT:** "AWS CodeBuild" is incorrect as CodeBuild is used for compiling code, running unit tests and creating the deployment package. It does not manage the deployment of the code.

**References:**

<https://docs.aws.amazon.com/codepipeline/latest/userguide/welcome-what-can-I-do.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-developer-tools/>

**Domain**

AWS Developer Tools

**Question 26Incorrect**

A Development team would like to migrate their existing application code from a GitHub repository to AWS CodeCommit.

What needs to be created before they can migrate a cloned repository to CodeCommit over HTTPS?

**A public and private SSH key file**

**Your answer is incorrect**

**A GitHub secure authentication token**

**An Amazon EC2 IAM role with CodeCommit permissions**

**Correct answer**

**A set of credentials generated from IAM**

Overall explanation

The simplest way to set up connections to AWS CodeCommit repositories is to configure Git credentials for CodeCommit in the IAM console, and then use those credentials for HTTPS connections.

You can also use these same credentials with any third-party tool or individual development environment (IDE) that supports HTTPS authentication using a static user name and password. For examples, see [For Connections from Development Tools](https://docs.aws.amazon.com/codecommit/latest/userguide/setting-up-ide.html).

**CORRECT:**"A set of credentials generated from IAM" is the correct answer.

**INCORRECT:** "A GitHub secure authentication token" is incorrect as this is not how you authenticated to CodeCommit.

**INCORRECT:** "A public and private SSH key file" is incorrect as that is required for accessing CodeCommit using SSH.

**INCORRECT:** "An Amazon EC2 IAM role with CodeCommit permissions" is incorrect as that would be used to provide access to administer CodeCommit. However, the question is asking how to authenticate a Git client to CodeCommit using HTTPS.

**References:**

<https://docs.aws.amazon.com/codecommit/latest/userguide/setting-up-gc.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-developer-tools/>

**Domain**

AWS Security, Identity, & Compliance

**Question 27Incorrect**

An application running on Amazon EC2 generates a large number of small files (1KB each) containing personally identifiable information that must be converted to ciphertext. The data will be stored on a proprietary network-attached file system. What is the SAFEST way to encrypt the data using AWS KMS?

**Your answer is incorrect**

**Create a data encryption key from a customer master key and encrypt the data with the data encryption key**

**Create a data encryption key from a customer master key and encrypt the data with the customer master key**

**Correct answer**

**Encrypt the data directly with a customer managed customer master key**

**Encrypt the data directly with an AWS managed customer master key**

Overall explanation

With AWS KMS you can encrypt files directly with a customer master key (CMK). A CMK can encrypt up to 4KB (4096 bytes) of data in a single encrypt, decrypt, or reencrypt operation. As CMKs cannot be exported from KMS this is a very safe way to encrypt small amounts of data.

Customer managed CMKs are CMKs in your AWS account that you create, own, and manage. You have full control over these CMKs, including establishing and maintaining their [key policies, IAM policies, and grants](https://docs.aws.amazon.com/kms/latest/developerguide/control-access.html), [enabling and disabling](https://docs.aws.amazon.com/kms/latest/developerguide/enabling-keys.html) them, [rotating their cryptographic material](https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html), [adding tags](https://docs.aws.amazon.com/kms/latest/developerguide/tagging-keys.html), [creating aliases](https://docs.aws.amazon.com/kms/latest/developerguide/programming-aliases.html) that refer to the CMK, and [scheduling the CMKs for deletion](https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys.html).

AWS managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an AWS service that is integrated with AWS KMS. Some AWS services support only an AWS managed CMK. In this example the Amazon EC2 instance is saving files on a proprietary network-attached file system and this will not have support for AWS managed CMKs.

Data keys are encryption keys that you can use to encrypt data, including large amounts of data and other data encryption keys. You can use AWS KMS CMKs to generate, encrypt, and decrypt data keys. However, AWS KMS does not store, manage, or track your data keys, or perform cryptographic operations with data keys. You must use and manage data keys outside of AWS KMS – this is potentially less secure as you need to manage the security of these keys.

**CORRECT:**"Encrypt the data directly with a customer managed customer master key" is the correct answer.

**INCORRECT:** "Create a data encryption key from a customer master key and encrypt the data with the data encryption key" is incorrect as this is not the most secure option here as you need to secure the data encryption key outside of KMS. It is also unwarranted as you can use a CMK directly to encrypt files up to 4KB in size.

**INCORRECT:** "Create a data encryption key from a customer master key and encrypt the data with the customer master key" is incorrect as the creation of the data encryption key is of no use here. It does not necessarily pose a security risk as the data key hasn’t been used (and you can use the CMK to encrypt the data), however this is not the correct process to follow.

**INCORRECT:** "Encrypt the data directly with an AWS managed customer master key" is incorrect as the network-attached file system is proprietary and therefore will not be supported by AWS managed CMKs.

**References:**

<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-kms/>

**Domain**

AWS Security, Identity, & Compliance

**Question 28Correct**

An engineer is using a Border Gateway Protocol (BGP) enabled AWS VPN connection to establish communication between on-site servers and Amazon EC2 instances in their account. The engineer is successful in accessing an EC2 instance in Subnet-X but is facing issues when attempting to reach an EC2 instance in Subnet-Y within the same VPC.

Which logging mechanism can the engineer employ to confirm if the traffic is getting to Subnet-Y?

**Use AWS CloudTrail logs to verify traffic to Subnet-Y. CloudTrail primarily logs API calls in AWS and not the traffic flow at the network interface level.**

**Consult AWS Config logs to trace the traffic. AWS Config tracks changes in resource configurations and doesn't provide insight into traffic flow.**

**Your answer is correct**

**Use VPC Flow Logs to check the inbound and outbound traffic of Subnet-Y.**

**Check Amazon CloudWatch Logs for the EC2 instance in Subnet-Y. CloudWatch Logs for EC2 instances primarily provide information about instance status and operations, not about network traffic.**

Overall explanation

In this scenario, AWS VPC Flow Logs would provide the required visibility. These logs capture information about the IP traffic going to and from network interfaces in the VPC. Therefore, it's the appropriate tool to verify if the traffic is reaching Subnet-Y.

**CORRECT:**"Use VPC Flow Logs to check the inbound and outbound traffic of Subnet-Y" is the correct answer (as explained above.)

**INCORRECT:** "Check Amazon CloudWatch Logs for the EC2 instance in Subnet-Y" is incorrect.

CloudWatch Logs for EC2 instances primarily provide information about instance status and operations, not about network traffic

**INCORRECT:** "Use AWS CloudTrail logs to verify traffic to Subnet-Y" is incorrect.

CloudTrail primarily logs API calls in AWS and not the traffic flow at the network interface level

**INCORRECT:** "Consult AWS Config logs to trace the traffic" is incorrect.

AWS Config tracks changes in resource configurations and doesn't provide insight into traffic flow.

**References:**

<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-vpc/>

**Domain**

AWS Networking & Content Delivery

**Question 29Correct**

A developer needs a long-term mountable storage solution for an Amazon Elastic Compute Cloud (EC2) instance using a compute optimized C6i instance type that meets heavily regulated compliance standards on data encryption for data at rest and in transit. What solution would provide this?

**Your answer is correct**

**Attach an Amazon Elastic Block Store (EBS) volume to the instance and enable encryption during creation.**

**Attach an Amazon Elastic Block Store (EBS) volume to the instance. Encryption is enabled automatically.**

**Attach an AWS Simple Storage Service (S3) bucket to the instance and enable encryption during creation.**

**Attach an AWS Simple Storage Service (S3) bucket to the instance. Encryption is enabled automatically.**

Overall explanation

Amazon EBS is permanent, mountable storage solution for Amazon EC2 instances. Amazon EBS volumes are not encrypted by default but can be encrypted for all current generation instance types and specific previous generation instance types. Amazon EBS volumes are not encrypted by default without additional configuration.

**CORRECT:**"Attach an Amazon Elastic Block Store (EBS) volume to the instance and enable encryption during creation" is the correct answer (as explained above.)

**INCORRECT:** "Attach an Amazon Elastic Block Store (EBS) volume to the instance. Encryption is enabled automatically" is incorrect.

Amazon EBS volumes can be configured to be encrypted upon creation or can be configured to encrypt new instances by default. AWS does not have Amazon EBS volumes encrypted by default.

**INCORRECT:** "Attach an AWS Simple Storage Service (S3) bucket to the instance and enable encryption during creation" is incorrect.

Amazon S3 provides a block storage solution. It is not mountable to instances. In January 2023, AWS announced that new objects in AWS S3 would be encrypted by default.

**INCORRECT:** Attach an AWS Simple Storage Service (S3) bucket to the instance. Encryption is enabled automatically" is incorrect.

Amazon S3 provide a block storage solution. It is not mountable to instances.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-ebs/>

**Domain**

AWS Storage

**Question 30Incorrect**

An AWS Lambda function is being developed in a VPC. When a file is added to an Amazon S3 bucket, this Lambda function is triggered, processes the file, and logs the results into a file. These result and log files need to be accessible by other AWS services and on-premises resources.

What should the developer use to meet these requirements?

**Your answer is incorrect**

**Store the result and log files in Amazon S3 and append the new log entries to existing objects.**

**Correct answer**

**Keep the result and log files in Amazon Elastic File System (EFS) accessible by Lambda functions.**

**Use Amazon DynamoDB to store the files and enable DynamoDB Streams to send notifications of changes.**

**Use AWS Glue to consolidate and catalog all result and log files and append log entries.**

Overall explanation

The correct solution is Amazon EFS as it provides a scalable, fully managed elastic NFS file system for AWS Cloud and on-premises resources. EFS can scale to petabytes without disrupting applications, making it suitable for Lambda functions to read/write large amounts of data.

Furthermore, AWS Lambda can now mount an Amazon EFS file system, making it easy for Lambda functions to read and write large amounts of data or to share data across a fleet of functions.

**CORRECT:**"Keep the result and log files in Amazon Elastic File System (EFS) accessible by Lambda functions" is the correct answer (as explained above.)

**INCORRECT:** "Store the result and log files in Amazon S3 and append the new log entries to existing objects" is incorrect.

Amazon S3 does not support appending data to existing S3 objects.

**INCORRECT:** "Use Amazon DynamoDB to store the files and enable DynamoDB Streams to send notifications of changes" is incorrect.

While Amazon DynamoDB can store data and Streams can notify services of changes, it is not designed for the type of file storage and sharing described in this scenario.

**INCORRECT:** "Use AWS Glue to consolidate and catalog all result and log files and append log entries" is incorrect.

AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for users to prepare and load their data for analytics, but it is not used for direct file storage and sharing.

**References:**

<https://docs.aws.amazon.com/lambda/latest/dg/services-efs.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-efs/>

**Domain**

AWS Storage

**Question 31Correct**

A Developer has deployed an application that runs on an Auto Scaling group of Amazon EC2 instances. The application data is stored in an Amazon DynamoDB table and records are constantly updated by all instances. An instance sometimes retrieves old data. The Developer wants to correct this by making sure the reads are strongly consistent.

How can the Developer accomplish this?

**Set consistency to strong when calling UpdateTable**

**Use the GetShardIterator command**

**Create a new DynamoDB Accelerator (DAX) table**

**Your answer is correct**

**Set ConsistentRead to true when calling GetItem**

Overall explanation

When you request a strongly consistent read, DynamoDB returns a response with the most up-to-date data, reflecting the updates from all prior write operations that were successful.

The GetItem operation returns a set of attributes for the item with the given primary key. If there is no matching item, GetItem does not return any data and there will be no Item element in the response.

GetItem provides an eventually consistent read by default. If your application requires a strongly consistent read, set ConsistentRead to true. Although a strongly consistent read might take more time than an eventually consistent read, it always returns the last updated value.

Therefore, the Developer should set ConsistentRead to true when calling GetItem.

**CORRECT:**"Set ConsistentRead to true when calling GetItem" is the correct answer.

**INCORRECT:** "Create a new DynamoDB Accelerator (DAX) table" is incorrect as DAX is not used to enable strongly consistent reads. DAX is used for improving read performance as it caches data in an in-memory cache.

**INCORRECT:** "Set consistency to strong when calling UpdateTable" is incorrect as you cannot use this API action to configure consistency at a table level.

**INCORRECT:** "Use the GetShardIterator command" is incorrect as this is not related to DynamoDB, it is related to Amazon Kinesis.

**References:**

<https://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_GetItem.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-dynamodb/>

**Domain**

AWS Database

**Question 32Incorrect**

A developer is configuring health checks using Amazon Route 53 and needs to set values to determine the health of critical endpoints. What is the parameter that Amazon Route 53 reviews before deciding if an endpoint is unhealthy?

**latency.**

**fault tolerance.**

**Correct answer**

**failure threshold.**

**Your answer is incorrect**

**network response.**

Overall explanation

The failure threshold is specified by the AWS customer. A failure is when the endpoint does not respond to a request.

**CORRECT:**"failure threshold" is the correct answer (as explained above.)

**INCORRECT:** "latency" is incorrect. Latency is not a parameter that Route 53 uses to determine if an endpoint is healthy.

**INCORRECT:** "fault tolerance" is incorrect. Fault tolerance is not a parameter that Route 53 uses to determine if an endpoint is healthy.

**INCORRECT:** "network response" is incorrect. Network response is not a parameter that Route 53 uses to determine if an endpoint is healthy.

**References**:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/welcome-health-checks.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-route-53/>

**Domain**

AWS Networking & Content Delivery

**Question 33Incorrect**

A junior developer has been assigned the project of making updates to a current application using AWS Cloud Development Kit (CDK).

How can the developer revert to a previous version if there is an error?

**Correct answer**

**Only make changes in the deployment phase, and never during synthesis.**

**Once CloudFormation has been installed, it can be used to track changes in application stacks.**

**Once CloudFormation has been added to the application, it can be used to manage the scope.**

**Your answer is incorrect**

**Once CloudFormation has been installed, it can be used to revert to previous versions.**

Overall explanation

Synthesis is the process of converting AWS CDK stacks to AWS CloudFormation templates and assets. Changes should only be during the deployment phase and after AWS CloudFormation template has been created. This will allow it to roll back the change if there are any problems.

**CORRECT:** "Only make changes in the deployment phase, and never during synthesis" is the correct answer (as explained above.)

**INCORRECT:** "Once CloudFormation has been installed, it can be used to revert to previous versions" is incorrect. The CDK Toolkit already provides the ability to convert CDK stacks into CloudFormation templates. There is no need to install CloudFormation.

**INCORRECT:** "Once CloudFormation has been added to the application, it can be used to manage the scope" is incorrect. The CDK Toolkit already provides the ability to convert CDK stacks into CloudFormation templates. It is not used to manage the scope.

**INCORRECT:** "Once synthesis is complete, it can be used to track drift changes" is incorrect. CloudFormation can detect drift changes if changes are made outside of CloudFormation management. Synthesis is the process of converting AWS CDK stacks to AWS CloudFormation templates.

**References:**

<https://docs.aws.amazon.com/cdk/v2/guide/best-practices.html>

**Domain**

AWS Developer Tools

**Question 34Incorrect**

In an organization, AWS CloudFormation templates are used to deploy all Amazon RDS DB instances as part of AWS CodePipeline CI/CD automation. As part of the deployment process, the main password for the DB instance needs to be auto generated.

What approach can be taken to fulfill these prerequisites with the minimum possible development effort?

**Utilize AWS::EC2::KeyPair to generate a secure string and assign it as the password for the DB instance.**

**Correct answer**

**Use AWS Secrets Manager via the AWS SDK to generate a secure string. Use a dynamic reference to create the DB instance with the secret value.**

**Write custom AWS Lambda function code that, when triggered, creates an encrypted string, and uses it as the password for the DB instance.**

**Your answer is incorrect**

**Use AWS KMS to generate a random encryption key, then use this key as the password for the DB instance.**

Overall explanation

This answer is correct because it leverages AWS Secrets Manager, a service designed specifically for secure storage and retrieval of secrets.

It does this without the added complexity and potential security concerns of using a custom Lambda function or CodeBuild action.

By using the secretsmanager dynamic reference in the CloudFormation template, you can retrieve the secret value directly, reducing the risk of exposure.

**CORRECT:**"Use AWS Secrets Manager via the AWS SDK to generate a secure string. Use a dynamic reference to create the DB instance with the secret value" is the correct answer (as explained above.)

**INCORRECT:** "Use AWS KMS to generate a random encryption key, then use this key as the password for the DB instance" is incorrect.

This is incorrect because AWS KMS is used for creating and managing cryptographic keys and controlling their use across a wide range of AWS services and in your applications, not for generating random strings.

**INCORRECT:** "Utilize AWS::EC2::KeyPair to generate a secure string and assign it as the password for the DB instance" is incorrect.

This approach is incorrect as the AWS::EC2::KeyPair is used for SSH login information for EC2 instances, not for generating passwords for RDS DB instances.

**INCORRECT:** "Write custom AWS Lambda function code that, when triggered, creates an encrypted string, and uses it as the password for the DB instance" is incorrect.

This approach introduces unnecessary complexity and development effort.

**References:**

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-secrets-manager/>

**Domain**

AWS Security, Identity, & Compliance

**Question 35Correct**

An application stores data in Amazon RDS and uses Amazon ElastiCache to improve read performance. The developer has configured ElastiCache to update the cache immediately after any writes to the primary database.

What will be the result of this approach to caching?

**Your answer is correct**

**The cache will become large and expensive because the infrequently requested data is also written to the cache.**

**Caching will slow performance of the read queries because the cache is updated when the cache cannot find the requested data.**

**Load on the RDS database instance will increase because the cache is updated for every database update.**

**There is a cache miss penalty because the cache is updated only after a cache miss, resulting in response latency.**

Overall explanation

The ElastiCache deployment is using a write-through caching strategy. The write-through strategy adds data or updates data in the cache whenever data is written to the database. This means data in the cache is never stale. There is a write penalty, but not a read penalty (in terms of latency added).

However, with a write-through strategy, most data are never read so the cache can become large and expensive. Adding a TTL to records can assist with this.

**CORRECT:**"The cache will become large and expensive because the infrequently requested data is also written to the cache" is the correct answer (as explained above.)

**INCORRECT:** "Caching will slow performance of the read queries because the cache is updated when the cache cannot find the requested data" is incorrect.

This is true of a lazy loading strategy. With a write-through strategy there is a write penalty, but not a read penalty.

**INCORRECT:** "Load on the RDS database instance will increase because the cache is updated for every database update" is incorrect.

There is still only one write to the RDS database instance.

**INCORRECT:** "There is a cache miss penalty because the cache is updated only after a cache miss, resulting in response latency" is incorrect.

This is a description of a lazy loading strategy, not a write-through strategy.

**References:**

<https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/Strategies.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-elasticache/>

**Domain**

AWS Database

**Question 36Incorrect**

A developer is planning on using AWS Cloud9 to build a new application. The developer wants to spend minimal time configuring resources. What solution should the developer choose?

**Correct answer**

**Create an AWS Cloud9 Elastic Compute Cloud (EC2) environment that will provision many of the resources and manage the lifecycle.**

**Create an SSH environment that will provision many of the resources and manage the lifecycle.**

**Your answer is incorrect**

**Use AWS Toolkit to create an Elastic Compute Cloud (EC2) environment that will provision many of the resources and manage the lifecycle.**

**Use AWS Toolkit to create an SSH environment that will provision many of the resources and manage the lifecycle.**

Overall explanation

An AWS Cloud9 Elastic Compute Cloud (EC2) Environment has many of the configuration and management taken care of by AWS. This includes creating and managing the instance lifecycle, setting up the Command Line Interface (CLI), and access to packages that are already installed and configured like Git, Node.js, and Python.

**CORRECT**: "Create an AWS Cloud9 Elastic Compute Cloud (EC2) environment that will provision many of the resources and manage the lifecycle" is the correct answer (as explained above.)

**INCORRECT**: "Create an SSH environment that will provision many of the resources and manage the lifecycle" is incorrect.

An AWS Cloud9 SSH environment does not provide instance lifecycle management and will require the developer to manually configure or add many features such as the Command Line Interface (CLI) and popular packages like Git, Node.js and Python.

**INCORRECT**: "Use AWS Toolkit to create an EC2 environment that will provision many of the resources and manage the lifecycle" is incorrect.

AWS Toolkit is an extension of the AWS Cloud9 integrated development environment (IDE). It is not used to create an EC2 environment.

**INCORRECT**: "Use AWS Toolkit to create an SSH environment that will provision many of the resources and manage the lifecycle" is incorrect.

AWS Toolkit is an extension of the AWS Cloud9 integrated development environment (IDE). It is not used to create an SSH environment.

**References:**

<https://docs.aws.amazon.com/cloud9/latest/user-guide/ec2-env-versus-ssh-env.html>

**Domain**

AWS Developer Tools

**Question 37Incorrect**

A company has a production application deployed using AWS Elastic Beanstalk. A new version of the application must be installed, and the company cannot tolerate any website downtime. If the application update fails, rollback should be fast and easy.

What deployment method should be used?

**Your answer is incorrect**

**Rolling**

**Correct answer**

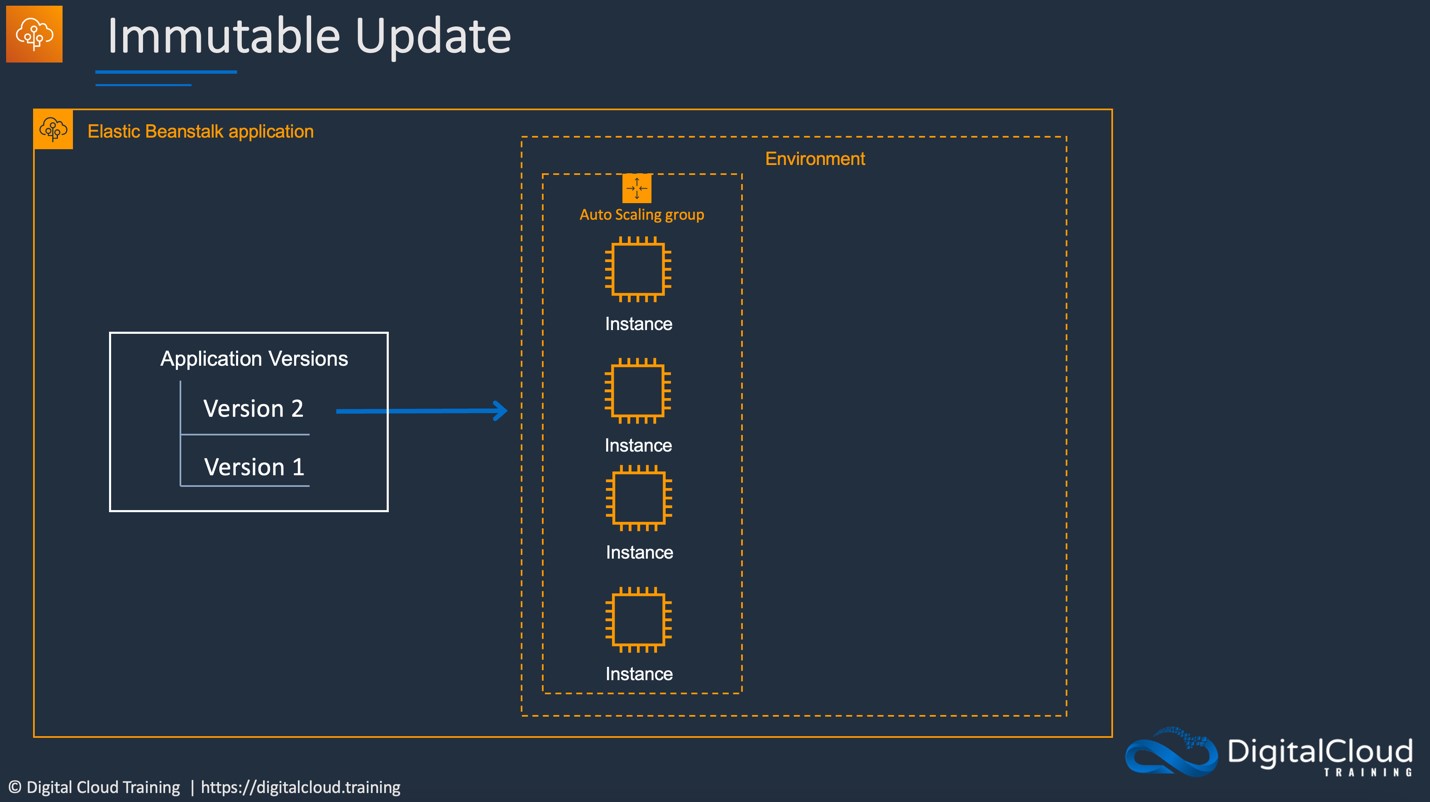
**Immutable**

**Incremental**

**All at once**

Overall explanation

The immutable deployment type launches new instances in a new ASG and deploys the version update to these instances before swapping traffic to these instances once healthy. There is zero downtime and a quick rollback in case of failures.



**CORRECT:**"Immutable" is the correct answer (as explained above.)

**INCORRECT:** "Rolling" is incorrect.

With a rolling update a few instances are updated at a time (batch), and then the deployment moves onto the next batch once the first batch is healthy. Each batch is taken out of service during deployment leading to downtime. If the update fails, you need to perform an additional rolling update to roll back the changes. This would not be ideal for this production environment.

**INCORRECT:** "All at once" is incorrect.

This would take all instances down at the same time. This is not suitable for a production environment.

**INCORRECT:** "Incremental" is incorrect.

This is not actually a type of deployment model in Elastic Beanstalk.

**References:**

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environmentmgmt-updates-immutable.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-elastic-beanstalk/>

**Domain**

AWS Compute

**Question 38Correct**

An application must be refactored for the cloud. The application data is stored in an Amazon DynamoDB table and is processed by a Lambda function which prepares the data for analytics. The data processing currently takes place once a day, but the data analysts require it to be performed in near-real time.

Which architecture pattern could be used to enable the data to be processed as it is received?

**Use a scheduled architecture.**

**Your answer is correct**

**Use an event-driven architecture.**

**Use a microservices architecture.**

**Use a fan-out architecture.**

Overall explanation

An event driven architecture will ensure that the records are processed as they are received. This can be achieved by creating a DynamoDB Stream for the existing table and then configuring the Lambda function to retrieve messages from the stream. This would be an event-driven architecture as the event (a record being written to the stream) causes the processing layer to do work.

**CORRECT:**"Use an event-driven architecture" is the correct answer (as explained above.)

**INCORRECT:** "Use a microservices architecture" is incorrect.

A microservices architecture is where you have many small individual components of an application that are loosely coupled. Though the architecture described may have components of a microservices architecture, this is not the defining characteristic that meets the requirement of near-real time processing.

**INCORRECT:** "Use a fan-out architecture" is incorrect.

An example of a fan-out architecture is using SNS to send a single notification to many SQS queues.

**INCORRECT:** "Use a scheduled architecture" is incorrect.

A scheduled architecture would not process events as they occur. It would only process them on a fixed schedule.

**References:**

<https://aws.amazon.com/event-driven-architecture/>

**Domain**

AWS Compute

**Question 39Incorrect**

Twelve months ago, an organization requested a public certificate for their domain via AWS Certificate Manager (ACM). It was validated using DNS validation. What will ACM do prior to expiration? (Select TWO.)

**If the certificate was issued by a third party, AWS ACM will send a request to the third party to verify the domain owner.**

**Correct selection**

**If the domain is not validated, it will send Health events or EventBridge events to notify the domain owner prior to expiration.**

**Your selection is correct**

**If the certificate is being used by an AWS service and ACM-provided CNAME records are accessible via the public DNS, ACM will consider the domain name validated and auto renew the certificate.**

**Your selection is incorrect**

**If the certificate was validated through DNS validation with a valid CNAME record provided by ACM and is currently being used by an AWS service, it will use SNS to send notifications of pending expiration.**

**If the certificate is being used by an AWS service and ACM-provided CNAME records are accessible via the public DNS, ACM will consider the domain name validated and send Health events or EventBridge events to notify the owner to renew the certificate.**

Overall explanation

An AWS ACM certificate that was validated using DNS validation will automatically renew if the certificate is still being using by an AWS service 60 days prior to its expiration and has an ACM-provided CNAME that is accessible via public DNS. If the certificate is not being used or if the CNAME is not correct, ACM will not automatically validate the DNS and will send notifications starting at 45 days prior to the expiration date.

**CORRECT:**“If the certificate is being used by an AWS service and ACM-provided CNAME records are accessible via the public DNS, ACM will consider the domain name validated and auto renew the certificate" is the correct answer (as explained above.)

**CORRECT:** "If the domain is not validated, it will send Health events or EventBridge events to notify the domain owner prior to expiration" is the correct answer (as explained above.)

**INCORRECT:** "If the certificate is being used by an AWS service and ACM-provided CNAME records are accessible via the public DNS, ACM will consider the domain name validated and send Health events or EventBridge events to notify the owner to renew the certificate" is incorrect. If criteria are met, DNS can be automatically validated and auto renewed without further action.

**INCORRECT:** "If the certificate was validated through DNS validation with a valid CNAME record provided by ACM and is currently being used by an AWS service, it will use SNS to send notifications of pending expiration" is incorrect. If criteria are met, certificate is auto renewed with no further action or notifications required.

**INCORRECT:** "If the certificate was issued by a third party, AWS ACM will send a request to the third party to verify the domain owner" is incorrect. The AWS ACM will not send a request. A new certificate will need to be created using AWS ACM or imported.

**References**:

<https://docs.aws.amazon.com/acm/latest/userguide/dns-renewal-validation.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-certificate-manager/>

**Domain**

AWS Security, Identity, & Compliance

**Question 40Correct**

There are multiple AWS accounts across multiple regions managed by a company. The operations team require a single operational dashboard that displays some key performance metrics from these accounts and regions. What is the SIMPLEST solution?

**Create an Amazon CloudTrail trail that applies to all regions and deliver the logs to a single Amazon S3 bucket. Create a dashboard using the data in the bucket**

**Create an Amazon CloudWatch dashboard in one account and region and import the data from the other accounts and regions**

**Create an AWS Lambda function that collects metrics from each account and region and pushes the metrics to the account where the dashboard has been created**

**Your answer is correct**

**Create an Amazon CloudWatch cross-account cross-region dashboard**

Overall explanation

You can create cross-account cross-Region dashboards, which summarize your CloudWatch data from multiple AWS accounts and multiple Regions into one dashboard. From this high-level dashboard you can get a view of your entire application, and also drill down into more specific dashboards without having to log in and out of accounts or switch Regions.

You can create cross-account cross-Region dashboards in the AWS Management Console and programmatically.

**CORRECT:**"Create an Amazon CloudWatch cross-account cross-region dashboard" is the correct answer.

**INCORRECT:** "Create an Amazon CloudWatch dashboard in one account and region and import the data from the other accounts and regions" is incorrect as this is more complex and unnecessary.

**INCORRECT:** "Create an AWS Lambda function that collects metrics from each account and region and pushes the metrics to the account where the dashboard has been created" is incorrect as this is not a simple solution.

**INCORRECT:** "Create an Amazon CloudTrail trail that applies to all regions and deliver the logs to a single Amazon S3 bucket. Create a dashboard using the data in the bucket" is incorrect as CloudTrail logs API activity, not performance metrics.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-cloudwatch/>

**Domain**

AWS Management & Governance

**Question 41Correct**

A company runs a popular website behind an Amazon CloudFront distribution that uses an Application Load Balancer as the origin. The Developer wants to set up custom HTTP responses to 404 errors for content that has been removed from the origin that redirects the users to another page.

The Developer wants to use an AWS Lambda@Edge function that is associated with the current CloudFront distribution to accomplish this goal. The solution must use a minimum amount of resources.

Which CloudFront event type should the Developer use to invoke the Lambda@Edge function that contains the redirect logic?

**Viewer request**

**Your answer is correct**

**Origin response**

**Viewer response**

**Origin request**

Overall explanation

When CloudFront receives an HTTP response from the origin server, if there is an origin-response trigger associated with the cache behavior, you can modify the HTTP response to override what was returned from the origin.

Some common scenarios for updating HTTP responses include the following:

   • Changing the status to set an HTTP 200 status code and creating static body content to return to the viewer when an origin returns an error status code (4xx or 5xx)

   • Changing the status to set an HTTP 301 or HTTP 302 status code, to redirect the user to another website when an origin returns an error status code (4xx or 5xx)

You can also replace the HTTP responses in viewer and origin request events. However, in this case it is the error response being returned from the origin that must be modified when a 404 error is encountered for a page that has been removed.

**CORRECT:**"Origin response" is the correct answer.

**INCORRECT:** "Origin request" is incorrect as explained above.

**INCORRECT:** "Viewer response" is incorrect as explained above.

**INCORRECT:** "Viewer request" is incorrect as explained above.

**References:**

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-updating-http-responses.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-lambda/>

**Domain**

AWS Networking & Content Delivery

**Question 42Correct**

An organization needs to create a central file storage solution that scales on demand and can be used by multiple Amazon Elastic Compute Cloud (EC2) instances and AWS Lambda functions. Which storage solution will meet these requirements?

**Create an Amazon EBS Multi-Attach volume.**

**Create an AWS Storage Gateway volume gateway.**

**Create an Amazon ElastiCache cluster.**

**Your answer is correct**

**Create an Amazon Elastic File System (EFS) file system.**

Overall explanation

Amazon Elastic File System (EFS) provides a scalable storage solution that does not require provisioning. It can scale up and down based on files stored. It can be used as a file source for multiple computing services such as Amazon Elastic Compute Cloud (EC2), Amazon Elastic Container Service (ECS), AWS Lambda.

**CORRECT**: "Create an Amazon Elastic File System (EFS) file system" is the correct answer (as explained above.)

**INCORRECT**: "Create an Amazon ElastiCache cluster" is incorrect.

Amazon ElastiCache is a database caching service; it cannot be used for file storage.

**INCORRECT**: "Create an Amazon EBS Multi-Attach volume" is incorrect.

Amazon EBS Multi-Attach Provisioned IOPS SSD can be used to attach a volume to multiple EC2 instances but not to other computing services such as Lambda.

**INCORRECT**: "Create an AWS Storage Gateway volume gateway" is incorrect.

Amazon Storage Gateway is used for hybrid infrastructure set-ups that allows on-premises infrastructure to use AWS cloud storage.

**References:**

<https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-efs/>

**Domain**

AWS Storage

**Question 43Incorrect**

A Developer is deploying an application using Docker containers running on the Amazon Elastic Container Service (ECS). The Developer is testing application latency and wants to capture trace information between the microservices.

Which solution will meet these requirements?

**Your answer is incorrect**

**Install the AWS X-Ray daemon on each of the Amazon ECS instances.**

**Correct answer**

**Create a Docker image that runs the X-Ray daemon, upload it to a Docker image repository, and then deploy it to the Amazon ECS cluster.**

**Install the AWS X-Ray daemon locally on an Amazon EC2 instance and instrument the Amazon ECS microservices using the X-Ray SDK.**

**Install the Amazon CloudWatch agent on the container image. Use the CloudWatch SDK to publish custom metrics from each of the microservices.**

Overall explanation

In Amazon ECS, create a Docker image that runs the X-Ray daemon, upload it to a Docker image repository, and then deploy it to your Amazon ECS cluster. You can use port mappings and network mode settings in your task definition file to allow your application to communicate with the daemon container.

**CORRECT:**"Create a Docker image that runs the X-Ray daemon, upload it to a Docker image repository, and then deploy it to the Amazon ECS cluster." is the correct answer.

**INCORRECT:** "Install the Amazon CloudWatch agent on the container image. Use the CloudWatch SDK to publish custom metrics from each of the microservices" is incorrect. The CloudWatch agent does not capture trace information between Docker containers.

**INCORRECT:** "Install the AWS X-Ray daemon on each of the Amazon ECS instances" is incorrect. The X-Ray daemon must be installed on the Docker containers, not the ECS hosts.

**INCORRECT:** "Install the AWS X-Ray daemon locally on an Amazon EC2 instance and instrument the Amazon ECS microservices using the X-Ray SDK" is incorrect. You cannot trace Docker microservices from an Amazon EC2 instance.

**References:**

<https://docs.aws.amazon.com/xray/latest/devguide/xray-daemon-ecs.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-developer-tools/>

**Domain**

AWS Compute

**Question 44Correct**

An organization has a new containerized application that needs to be launched quickly. The team lead has stated to choose the option that would reduce the burden of infrastructure maintenance for the team.

Which solution best meets this requirement?

**Use Amazon Elastic Container Service (ECS) to provide a template that supports a quick launch of AWS Fargate applications on Amazon Elastic Compute Cloud (EC2).**

**Your answer is correct**

**Use AWS Copilot to provide a template that supports a quick launch of Amazon Elastic Container Service (ECS) applications on AWS Fargate.**

**Use AWS Fargate to provide a template that supports a quick launch of Amazon Elastic Container Service (ECS) applications on Amazon Elastic Compute Cloud (EC2).**

**Use AWS Copilot to provide a template that supports a quick launch of Amazon Elastic Container Service (ECS) applications on Amazon Elastic Compute Cloud (EC2).**

Overall explanation

Copilot can run tasks and services on serverless infrastructures such as AWS Fargate. This can provide the support of containers using ECS and serverless services like Fargate does not require customers to manage.

**CORRECT**: “Use AWS Copilot to provide a template that supports a quick launch of Amazon Elastic Container Service (ECS) applications on AWS Fargate” is the correct answer (as explained above.)

**INCORRECT**: "Use AWS Copilot to provide a template that supports a quick launch of Amazon Elastic Container Service (ECS) applications on Amazon Elastic Compute Cloud (EC2)" is incorrect.

EC2 is not a serverless service and would require additional maintenance and support from the development team.

**INCORRECT**: "Use AWS Fargate to provide a template that supports a quick launch of Amazon Elastic Container Service (ECS) applications on Amazon Elastic Compute Cloud (EC2)" is incorrect.

EC2 is not a serverless service and would require additional maintenance and support from the development team. Fargate is a serverless compute engine. It would not provide a template to support a quick launch.

**INCORRECT**: "Use Amazon Elastic Container Service (ECS) to provide a template that supports a quick launch of AWS Fargate applications on Amazon Elastic Compute Cloud (EC2)" is incorrect.

EC2 is not a serverless service and would require additional maintenance and support from the development team. ECS is a container orchestration service that would not provide a template.

**References:**

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/deploy-a-clustered-application-to-amazon-ecs-by-using-aws-copilot.html>

**Domain**

AWS Compute

**Question 45Incorrect**

A company has launched a web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The connection between clients and the ALB should use the HTTPS protocol. A developer uses AWS Certificate Manager (ACM) to issue an X.509 certificate.

What steps must the developer take to secure the connection?

**Correct answer**

**Configure the ALB to use the X.509 certificate by using the AWS Management Console.**

**Configure each EC2 instance to use the X.509 certificate by using the AWS Management Console.**

**Export the root key of the X.509 certificate to an Amazon S3 bucket. Configure each EC2 instance to use the same X.509 certificate from the S3 bucket.**

**Your answer is incorrect**

**Export the root key of the X.509 certificate to an Amazon S3 bucket. Configure the ALB to use the X.509 certificate from the S3 bucket.**

Overall explanation

To secure the connection between clients and the ALB the developer must simply attach the certificate to the ALB. This can be performed using the AWS Management Console. There is no need to add the certificate to each EC2 instance. If end-to-end encryption is required, self-signed certificates or certificates issued by a private CA can be used on the EC2 instances (not required by the solution requirements).

**CORRECT:**"Configure the ALB to use the X.509 certificate by using the AWS Management Console" is the correct answer (as explained above.)

**INCORRECT:** "Configure each EC2 instance to use the X.509 certificate by using the AWS Management Console" is incorrect. This is not required as explained above.

**INCORRECT:** "Export the root key of the X.509 certificate to an Amazon S3 bucket. Configure the ALB to use the X.509 certificate from the S3 bucket" is incorrect. This is the wrong procedure, the certificate can simply be attached to the ALB.

**INCORRECT:** "Export the root key of the X.509 certificate to an Amazon S3 bucket. Configure each EC2 instance to use the same X.509 certificate from the S3 bucket" is incorrect. As explained above, this is not required and is the wrong procedure.

**References:**

<https://aws.amazon.com/premiumsupport/knowledge-center/associate-acm-certificate-alb-nlb/>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-certificate-manager/>

**Domain**

AWS Security, Identity, & Compliance

**Question 46Correct**

A company is developing a new online game that will run on top of Amazon ECS. Four distinct Amazon ECS services will be part of the architecture, each requiring specific permissions to various AWS services. The company wants to optimize the use of the underlying Amazon EC2 instances by bin packing the containers based on memory reservation.

Which configuration would allow the Development team to meet these requirements MOST securely

**Create four distinct IAM roles, each containing the required permissions for the associated ECS services, then configure each ECS service to reference the associated IAM role**

**Create a new Identity and Access Management (IAM) instance profile containing the required permissions for the various ECS services, then associate that instance role with the underlying EC2 instances**

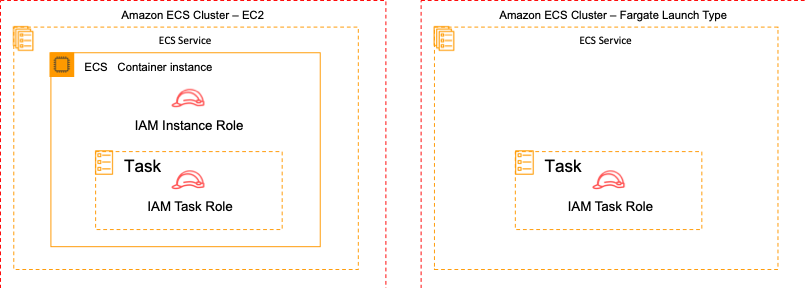
**Create four distinct IAM roles, each containing the required permissions for the associated ECS services, then, create an IAM group and configure the ECS cluster to reference that group**

**Your answer is correct**

**Create four distinct IAM roles, each containing the required permissions for the associated ECS services, then configure each ECS task definition to reference the associated IAM role**

Overall explanation

With IAM roles for Amazon ECS tasks, you can specify an IAM role that can be used by the containers in a task. Applications must sign their AWS API requests with AWS credentials, and this feature provides a strategy for managing credentials for your applications to use, similar to the way that Amazon EC2 instance profiles provide credentials to EC2 instances.



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 or RunTask API operation. The applications in the task’s containers can then use the AWS SDK or CLI to make API requests to authorized AWS services.

In this case each service requires access to different AWS services so following the principal of least privilege it is best to assign as a separate role to each task definition.

**CORRECT:**"Create four distinct IAM roles, each containing the required permissions for the associated ECS services, then configure each ECS task definition to reference the associated IAM role" is the correct answer.

**INCORRECT:** "Create a new Identity and Access Management (IAM) instance profile containing the required permissions for the various ECS services, then associate that instance role with the underlying EC2 instances" is incorrect. It is a best practice to use IAM roles for tasks instead of assigning the roles to the container instances.

**INCORRECT:** "Create four distinct IAM roles, each containing the required permissions for the associated ECS services, then configure each ECS service to reference the associated IAM role" is incorrect as the reference should be made within the task definition.

**INCORRECT:** "Create four distinct IAM roles, each containing the required permissions for the associated ECS services, then, create an IAM group and configure the ECS cluster to reference that group" is incorrect as the reference should be made within the task definition.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-ecs-and-eks/>

**Domain**

AWS Security, Identity, & Compliance

**Question 47Correct**

A Developer is creating a serverless application. The application looks up information about a customer using a separate Lambda function for each item such as address and phone number. The Developer has created branches in AWS Step Functions for each lookup function.

How can the Developer optimize the performance, so the lookups complete faster?

**Use a Map state to iterate over all the items.**

**Use a Choice state to lookup the specific information required.**

**Your answer is correct**

**Use a Parallel state to iterate over all the branches parallel.**

**Use a Wait state to reduce the wait time for function execution.**

Overall explanation

The Parallel state ("Type": "Parallel") can be used to create parallel branches of execution in your AWS Step Functions state machine. This will improve the performance of the application by ensuring that all information lookups occur in parallel.

**CORRECT:**"Use a Parallel state to iterate over all the branches parallel" is the correct answer.

**INCORRECT:** "Use a Choice state to lookup the specific information required" is incorrect. This is used to add additional logic but is not required and is unlikely to improve performance.

**INCORRECT:** "Use a Wait state to reduce the wait time for function execution" is incorrect. The Wait state delays the state machine from continuing for a specified time.

**INCORRECT:** "Use a Map state to iterate over all the items" is incorrect. The Map state executes the same steps for multiple entries of an array in the state input.

**References:**

<https://docs.aws.amazon.com/step-functions/latest/dg/amazon-states-language-parallel-state.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-application-integration-services/>

**Domain**

AWS Application Integration

**Question 48Incorrect**

Customers who use a REST API have reported performance issues. A Developer needs to measure the time between when API Gateway receives a request from a client and when it returns a response to the client.

Which metric should the Developer monitor?

**Correct answer**

**Latency**

**CacheHitCount**

**Your answer is incorrect**

**IntegrationLatency**

**5XXError**

Overall explanation

The Latency metric measures the time between when API Gateway receives a request from a client and when it returns a response to the client. The latency includes the integration latency and other API Gateway overhead.

**CORRECT:**"Latency" is the correct answer.

**INCORRECT:** "IntegrationLatency" is incorrect. This measures the time between when API Gateway relays a request to the backend and when it receives a response from the backend.

**INCORRECT:** "CacheHitCount" is incorrect. This measures the number of requests served from the API cache in a given period.

**INCORRECT:** "5XXError" is incorrect. This measures the number of server-side errors captured in a given period.

**References:**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-metrics-and-dimensions.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-api-gateway/>

<https://digitalcloud.training/amazon-cloudwatch/>

**Domain**

AWS Networking & Content Delivery

**Question 49Correct**

A Developer is building a WebSocket API using Amazon API Gateway. The payload sent to this API is JSON that includes an action key which can have multiple values. The Developer must integrate with different routes based on the value of the action key of the incoming JSON payload.

How can the Developer accomplish this task with the LEAST amount of configuration?

**Create a mapping template to map the action key to an integration request.**

**Your answer is correct**

**Set the value of the route selection expression to $request.body.action.**

**Create a separate stage for each possible value of the action key.**

**Set the value of the route selection expression to $default.**

Overall explanation

In your WebSocket API, incoming JSON messages are directed to backend integrations based on routes that you configure. (Non-JSON messages are directed to a $default route that you configure.)

A route includes a route key, which is the value that is expected once a route selection expression is evaluated. The routeSelectionExpression is an attribute defined at the API level. It specifies a JSON property that is expected to be present in the message payload.

For example, if your JSON messages contain an action property and you want to perform different actions based on this property, your route selection expression might be ${request.body.action}. Your routing table would specify which action to perform by matching the value of the action property against the custom route key values that you have defined in the table.

**CORRECT:**"Set the value of the route selection expression to $request.body.action" is the correct answer.

**INCORRECT:** "Create a separate stage for each possible value of the action key" is incorrect. There is no need to create separate stages, the action key can be used for routing as described above.

**INCORRECT:** "Create a mapping template to map the action key to an integration request" is incorrect. Mapping templates are not used for routing to different integrations, they are used for transforming data.

**INCORRECT:** "Set the value of the route selection expression to $default" is incorrect. The $default route is used for routing non-JSON messages.

**References:**

[https://docs.aws.amazon.com/apigateway/latest/Developerguide/websocket-api-develop-routes.html](https://docs.aws.amazon.com/apigateway/latest/developerguide/websocket-api-develop-routes.html)

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-api-gateway/>

**Domain**

AWS Networking & Content Delivery

**Question 50Correct**

A developer wants to use a cron job to schedule key rotation for an Amazon RDS database. What steps should the developer take to complete this task?

**Your answer is correct**

**Use AWS Secrets Manager to create a managed rotation under the Rotation Schedule and schedule the time for the automatic rotation using a cron expression.**

**Use AWS Identity and Access Management (IAM) to create a managed rotation under the Rotation Schedule and schedule the time for the automatic rotation using a cron expression.**

**Use AWS Relational Database Service to create a managed rotation under the Rotation Schedule and schedule the time for the automatic rotation using a cron expression.**

**Use AWS Systems Manager (SSM) Parameter Store to create a managed rotation under the Rotation Schedule and schedule the time for the automatic rotation using a cron expression.**

Overall explanation

Rotation is the process of periodically updating a secret. When you rotate a secret, you update the credentials in both the secret and the database or service. In Secrets Manager, you can set up automatic rotation for your secrets.

Some services offer managed rotation, where the service configures and manages rotation for you. With managed rotation, you don't use an AWS Lambda function to update the secret and the credentials in the database. Amazon RDS can be used with managed rotation.

**CORRECT:**"Use AWS Secrets Manager to create a managed rotation under the Rotation Schedule and schedule the time for the automatic rotation using a cron expression" is the correct answer (as explained above.)

**INCORRECT:** "Use AWS Identity and Access Management (IAM) to create a managed rotation under the Rotation Schedule and schedule the time for the automatic rotation using a cron expression" is incorrect. IAM is an identity and management services to help assign permissions to users, groups and roles. It does not manage secrets such as passwords or access keys.

**INCORRECT:** "Use AWS Relational Database Service to create a managed rotation under the Rotation Schedule and schedule the time for the automatic rotation using a cron expression" is incorrect. RDS is a used to simplify the set-up of relational databases. It is not used for managing secrets.

**INCORRECT:** "Use AWS Systems Manager Parameter Store to create a managed rotation under the Rotation Schedule and schedule the time for the automatic rotation using a cron expression" is incorrect. The SSM Parameter store does not use cron jobs to manage rotations.

**References:**

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotate-secrets_schedule.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-secrets-manager/>

**Domain**

AWS Security, Identity, & Compliance

**Question 51Correct**

An engineer is tasked with creating an AWS CloudFormation template that is capable of automatically determining the AWS Region where it is being deployed.

What is the MOST efficient method to ascertain the Region during deployment of the template?

**Request the Region as an input parameter during CloudFormation deployment.**

**Dynamically fetch the Region by referencing the corresponding entry in AWS Systems Manager Parameter Store.**

**Extract the Region from the AWS::StackId pseudo parameter by applying the Fn::Split intrinsic function.**

**Your answer is correct**

**Utilize the AWS::Region pseudo parameter.**

Overall explanation

In AWS CloudFormation, the AWS::Region pseudo parameter automatically resolves to the Region where the stack is being created or updated. This makes it the most operationally efficient way to determine the Region in which the template is being deployed, as it doesn't require any additional input, processing, or external service calls.

**CORRECT:**"Utilize the AWS::Region pseudo parameter" is the correct answer (as explained above.)

**INCORRECT:** "Request the Region as an input parameter during CloudFormation deployment" is incorrect.

This method is not operationally efficient as it relies on manual input from the user each time the template is deployed. It also increases the risk of human error or inconsistencies, especially in multi-region deployments.

**INCORRECT:** "Extract the Region from the AWS::StackId pseudo parameter by applying the Fn::Split intrinsic function" is incorrect.

Although this method technically works because the stack ID contains the region, it's not the most efficient approach. This requires additional processing to extract the region from the stack ID, which makes it less efficient than directly using the AWS::Region pseudo parameter.

**INCORRECT:** "Dynamically fetch the Region by referencing the corresponding entry in AWS Systems Manager Parameter Store" is incorrect.

This method requires an external service and assumes that the region has been correctly stored as a parameter. This adds additional complexity and dependency on another service, making it less efficient than using the built-in AWS::Region pseudo parameter.

**References:**

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/pseudo-parameter-reference.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-cloudformation/>

**Domain**

AWS Management & Governance

**Question 52Correct**

A development team using AWS Amplify is testing new features for an application. How can the team test the features with the current production code without impacting the last published application version?

**Your answer is correct**

**Connect a new branch that will deploy a version named https://dev.applicationId.amplifyapp.com to test new features.**

**Connect the production environment into AWS Cloud9 and test the features after committing them.**

**Connect the production environment into AWS Cloud9 and test the features after publishing them.**

**Connect a new branch that will deploy a version named https://main.applicationId.amplifyapp.com to test new features.**

Overall explanation

Features testing on an application should not be done on production code. AWS Amplify supports connecting branches from the production code environment that will clone a repository so that features can be developed, tested and rolled back, if necessary, without impacting the latest version of the published application.

**CORRECT**: “Connect a new branch that will deploy a version named https://dev.applicationId.amplifyapp.com to test new features” is the correct answer (as explained above.)

**INCORRECT**: "Connect a new branch that will deploy a version named https://main.applicationId.amplifyapp.com to test new features" is incorrect.

The “main” branch indicated in the URL indicates this is the main production environment and not the one to test features on.

**INCORRECT**: “Connect the production environment into AWS Cloud9 and test the features after publishing them" is incorrect.

AWS Cloud9 is an IDE that can be used to develop new features if the development chooses to use it. Other IDEs can also be used and integrated in the development process. Once features have passed all the checks, it can be pushed.

**INCORRECT**: "Connect the production environment into AWS Cloud9 and test the features after committing them" is incorrect.

AWS Cloud9 is an IDE that can be used to develop new features if the development chooses to use it. Other IDEs can also be used and integrated in the development process. Committing the features captures a snapshot of the staged changes.

**References:**

<https://docs.aws.amazon.com/amplify/latest/userguide/multi-environments.html>

**Domain**

AWS Developer Tools

**Question 53Correct**

An organization has applied a public certificate to a domain name using AWS Certificate Manager (ACM). What will the browser show to indicate that the site is trusted and is connected via SSL/TLS?

**ECDSA key algorithm.**

**RSA key algorithm.**

**Your answer is correct**

**Lock icon on the address bar.**

**DNS validation.**

Overall explanation

ACM certificates are trusted by all major browsers. When connected by SSL/TLS sites using ACM certificates, this trust is indicated by the lock icon in browser address bar.

**CORRECT:**"Lock icon on the address bar" is the correct answer (as explained above.)

**INCORRECT:** "DNS validation" is incorrect. DNS validation is used to validate domain ownership and is completed when the certificate is requested.

**INCORRECT:** "RSA key algorithm" is incorrect. The RSA key algorithm is selected when requesting the certificate. It is not shown in the browser.

**INCORRECT:** "ECDSA key algorithm" is incorrect. The RSA key algorithm is selected when requesting the certificate. It is not shown in the browser.

**References**:

<https://docs.aws.amazon.com/acm/latest/userguide/acm-certificate.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-certificate-manager/>

**Domain**

AWS Security, Identity, & Compliance

**Question 54Correct**

A developer is using AWS AppSync to develop an application that will be used by a healthcare provider that is subject to HIPAA compliance regulations that require data encryption. The team lead has requested to optimize performance and reduce latency as much as possible.

How can a developer meet the compliance and team lead requirements?

**Set the API Cache for per-resolver caching and leaving the default encryption settings.**

**Your answer is correct**

**Set the API Cache for full request caching and adjust the settings for data encryption at rest and in transit.**

**Set the API Cache for “None" to prevent any changed being made from the default cache settings and adjust the settings for data encryption at rest and in transit.**

**Set the API Cache for full request caching and leaving the default encryption settings.**

Overall explanation

AWS AppSync’s API Cache settings provides three options: None, Full request caching, and Per-resolver caching. To meet the team lead’s requirements for high performance and low latency, the cache settings can be configured for full request caching to cache all requests and responses. To meet HIPAA compliance, the settings would be configured for data encryption at rest and in transit.

**CORRECT**: “Set the API Cache for full request caching and adjust the settings for data encryption at rest and in transit” is the correct answer (as explained above.)

**INCORRECT**: "Set the API Cache for full request caching and leaving the default encryption settings" is incorrect. The API Cache set to full request caching is correct.

The default settings for API Cache are for no encryption. To meet HIPAA compliance, data should be protected, and encryption should be enabled for in transit and at rest.

**INCORRECT**: “Set the API Cache for “None" to prevent any changed being made from the default cache settings and adjust the settings for data encryption at rest and in transit" is incorrect.

“None” is the default setting for the API Cache and would not cache any requests and responses. This would not meet the goal of optimizing performance and decreasing latency. The change in the encryption settings is correct.

**INCORRECT**: "Set the API Cache for per-resolver caching and leaving the default encryption settings " is incorrect.

The per-resolver caching will only cache specific calls. The default encryption leaves the data unencrypted which does not meet the HIPAA requirements.

**References:**

<https://docs.aws.amazon.com/appsync/latest/devguide/enabling-caching.html>

**Domain**

AWS Developer Tools

**Question 55Correct**

A development team is working with Amazon MemoryDB for Redis. The team lead wants to limit the default access of the service-linked role and implement a custom-managed policy instead.

What needs to be done prior to making this change?

**Your answer is correct**

**The team lead would need to have permission to call `iam:createServiceLinkedRole`.**

**The team lead would need permission from an AWS Technical Account Manager.**

**The team lead would have to login as the root user to change the permission setting.**

**The team lead would edit the default policy named `AmazonMemoryDBFullAccess`.**

Overall explanation

Service-linked roles are tied to the resource with predefined permissions. The default policy associated Amazon MemoryDB for Redis is “AmazonMemoryDBFullAccess”. This comes pre-provisioned with permission that the service requires to create a service link that is used to create resources and access other AWS resources and services.

You might decide not to use the default policy and instead to use a custom-managed policy. In this case, make sure that you have either permissions to call iam:createServiceLinkedRole or that you have created the MemoryDB service-linked role.

**CORRECT**: "The team lead would need to have permission to call `iam:createServiceLinkedRole`" is the correct answer (as explained above.)

**INCORRECT**: "The team lead would have to login as the root user to change the permission setting" is incorrect.

The team lead may not be the root user. Logging in and accessing the root user should be limited to the tasks that are necessary and limited to the root user. A Cloud Administrator, for example, could update the IAM roles needed for the team lead to make the appropriate service-linked policy changes.

**INCORRECT**: "The team lead would need permission from an AWS Technical Account Manager" is incorrect.

There are some changes to an account or services that an organization would need to contact their technical account manager to change. An update to the IAM policy or changing a service-linked role is not one of them.

**INCORRECT**: "The team lead would edit the default policy named `AmazonMemoryDBFullAccess`" is incorrect.

AWS managed policies cannot be edited. A custom service policy would need to create and attached with the appropriate IAM role.

**References:**

<https://docs.aws.amazon.com/memorydb/latest/devguide/set-up.html>

**Domain**

AWS Database

**Question 56Correct**

A start-up organization is launching a new website. Which statement correctly describes how to set up the domain, routing, and health checks in AWS?

**Use Route 53 to specify the IP address to perform health checks, register a domain name, and route the internet traffic to domain.**

**Use Route 53 to register a domain name and perform routing to the domain and Shield to perform health checks on resources.**

**Use Route 53 to register a domain name and AWS Certificate Manager to perform routing to the domain and Shield to perform health checks on resources.**

**Your answer is correct**

**Use Route 53 to register a domain name, route the internet traffic to domain, and specify the values to perform health checks on resources.**

Overall explanation

Route 53 can be used as a DNS to register a domain name, route the internet traffic, and perform health checks on resources. If being used for all three tasks, the order of register domain, route the traffic, and perform health checks must be sequential. ACM and Shield are not needed for this task.

**CORRECT:**"Use Route 53 to register a domain name, route the internet traffic to domain, and specify the values to perform health checks on resources" is the correct answer (as explained above.)

**INCORRECT:** "Use Route 53 to register a domain name and AWS Certificate Manager to perform routing to the domain and Shield to perform health checks on resources" is incorrect. Route 53 can do all the tasks. ACM and Shield cannot perform these tasks.

**INCORRECT:** "Use Route 53 to specify the IP address to perform health checks, register a domain name, and route the internet traffic to domain" is incorrect. Route 53 can be used to perform these tasks but must done in a specific order starting with registering a domain.

**INCORRECT:** "Use Route 53 to register a domain name and perform routing to the domain and Shield to perform health checks on resources" is incorrect. Route 53 can do all these tasks. Shield does not perform health checks on resources.

**References**:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-route-53/>

**Domain**

AWS Networking & Content Delivery

**Question 57Incorrect**

A Developer is creating a REST service using Amazon API Gateway with AWS Lambda integration. The service adds data to a spreadsheet and the data is sent as query string parameters in the method request.

How should the Developer convert the query string parameters to arguments for the Lambda function?

**Enable request validation**

**Your answer is incorrect**

**Change the integration type**

**Correct answer**

**Create a mapping template**

**Include the Amazon Resource Name (ARN) of the Lambda function**

Overall explanation

Standard API Gateway [parameter and response code mapping templates](https://docs.aws.amazon.com/apigateway/latest/developerguide/models-mappings.html) allow you to map parameters one-to-one and map a family of integration response status codes (matched by a regular expression) to a single response status code.

Mapping template overrides provides you with the flexibility to perform many-to-one parameter mappings; override parameters after standard API Gateway mappings have been applied; conditionally map parameters based on body content or other parameter values; programmatically create new parameters on the fly; and override status codes returned by your integration endpoint.

Any type of request parameter, response header, or response status code may be overridden.

Following are example uses for a mapping template override:

To create a new header (or overwrite an existing header) as a concatenation of two parameters

To override the response code to a success or failure code based on the contents of the body

To conditionally remap a parameter based on its contents or the contents of some other parameter

To iterate over the contents of a json body and remap key value pairs to headers or query strings

Therefore, the Developer can convert the query string parameters by creating a mapping template.

**CORRECT:**"Create a mapping template" is the correct answer.

**INCORRECT:** "Enable request validation" is incorrect as this is used to configure API Gateway to perform basic validation of an API request before proceeding with the integration request.

**INCORRECT:** "Include the Amazon Resource Name (ARN) of the Lambda function" is incorrect as that doesn’t assist with converting the query string parameters.

**INCORRECT:** "Change the integration type" is incorrect as to perform a conversion the Lambda integration does not need to have a different integration type such as Lambda proxy.

**References:**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-override-request-response-parameters.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-api-gateway/>

**Domain**

AWS Networking & Content Delivery

**Question 58Correct**

A company has deployed a new web application that uses Amazon Cognito for authentication. The company wants to allow sign-in from any source but wants to automatically block all sign-in attempts if the risk level is elevated.

Which Amazon Cognito feature will meet these requirements?

**Your answer is correct**

**Adaptive authentication.**

**Advanced security metrics.**

**Case sensitive user pools.**

**Multi-factor authentication (MFA).**

Overall explanation

With adaptive authentication, you can configure your user pool to block suspicious sign-ins or add second factor authentication in response to an increased risk level.

For each sign-in attempt, Amazon Cognito generates a risk score for how likely the sign-in request is to be from a compromised source. This risk score is based on many factors, including whether it detects a new device, user location, or IP address.

**For each risk level, you can choose from the following options:**

•  Allow - Users can sign in without an additional factor.

•  Optional MFA - Users who have a second factor configured must complete a second factor challenge to sign in.

•  Require MFA - Users who have a second factor configured must complete a second factor challenge to sign in. Amazon Cognito blocks sign-in for users who don't have a second factor configured.

•  Block - Amazon Cognito blocks all sign-in attempts at the designated risk level.

In this case the company should use adaptive authentication and configure Cognito to block sign-in attempts at the specific risk level they feel is appropriate.

**CORRECT:**"Adaptive authentication" is the correct answer (as explained above.)

**INCORRECT:** "Advanced security metrics" is incorrect.

Amazon Cognito publishes sign-in attempts, their risk levels, and failed challenges to Amazon CloudWatch. These are known as advanced security metrics. This information is useful for analysis, but adaptive authentication is required to automatically block sign-in attempts.

**INCORRECT:** "Multi-factor authentication (MFA)" is incorrect.

This is not a method of blocking. In this case adaptive authentication with a block response should be configured.

**INCORRECT:** "Case sensitive user pools" is incorrect.

This has nothing to do with responding to security threats. This is a configuration that determines whether Cognito considers the case of email addresses and usernames.

**References:**

<https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pool-settings-adaptive-authentication.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-cognito/>

**Domain**

AWS Security, Identity, & Compliance

**Question 59Incorrect**

A Developer has created an Amazon S3 bucket and uploaded some objects that will be used for a publicly available static website. What steps MUST be performed to configure the bucket as a static website? (Select TWO.)

**Upload an index and error document and enter the name of the index and error documents when enabling static website hosting**

**Correct selection**

**Enable public access and grant everyone the s3:GetObject permissions**

**Upload a certificate from AWS Certificate Manager**

**Your selection is incorrect**

**Create an object access control list (ACL) granting READ permissions to the AllUsers group**

**Your selection is correct**

**Upload an index document and enter the name of the index document when enabling static website hosting**

Overall explanation

You can use Amazon S3 to host a static website. On a static website, individual webpages include static content. They might also contain client-side scripts.

To host a static website on Amazon S3, you configure an Amazon S3 bucket for website hosting and then upload your website content to the bucket. When you configure a bucket as a static website, you enable static website hosting, set permissions, and add an index document.

When you enable static website hosting for your bucket, you enter the name of the index document (for example, index.html). After you enable static website hosting for your bucket, you upload an HTML file with the index document name to your bucket. Note that an error document is optional.

To provide permissions, it is necessary to disable “block public access” settings and then create a bucket policy that grants everyone the s3:GetObject permission. For example:

1. {
2. "Version": "2012-10-17",
3. "Statement": [
4. {
5. "Sid": "PublicReadGetObject",
6. "Effect": "Allow",
7. "Principal": "\*",
8. "Action": [
9. "s3:GetObject"
10. ],
11. "Resource": [
12. "arn:aws:s3:::example.com/\*"
13. ]
14. }
15. ]
16. }

**CORRECT:**"Upload an index document and enter the name of the index document when enabling static website hosting" is a correct answer.

**CORRECT:**"Enable public access and grant everyone the s3:GetObject permissions" is also a correct answer.

**INCORRECT:** "Upload an index and error document and enter the name of the index and error documents when enabling static website hosting" is incorrect as the error document is optional and the question specifically asks for the steps that MUST be completed.

**INCORRECT:** "Create an object access control list (ACL) granting READ permissions to the AllUsers group" is incorrect. This may be necessary if the bucket objects are not owned by the bucket owner but the question states that the Developer created the bucket and uploaded the objects and so must be the object owner.

**INCORRECT:** "Upload a certificate from AWS Certificate Manager" is incorrect as this is not supported or necessary for static websites on Amazon S3.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-s3-and-glacier/>

**Domain**

AWS Storage

**Question 60Incorrect**

A company is creating an application that must support Security Assertion Markup Language (SAML) and authentication with social identity providers. The application must also be authorized to access data in Amazon S3 buckets and Amazon DynamoDB tables.

Which AWS service or feature will meet these requirements with the LEAST amount of additional coding?

**Your answer is incorrect**

**Amazon API Gateway REST API.**

**AWS AppSync GraphQL API.**

**Amazon Cognito user pools.**

**Correct answer**

**Amazon Cognito identity pools.**

Overall explanation

Amazon Cognito identity pools (federated identities) enable you to create unique identities for your users and federate them with identity providers. With an identity pool, you can obtain temporary, limited-privilege AWS credentials to access other AWS services.

Amazon Cognito identity pools support the following identity providers:

• Public providers: Amazon, Facebook, Google, Apple

• Amazon Cognito user pools

• Open ID Connect providers (identity pools)

• SAML identity providers (identity pools)

• Developer authenticated identities (identity pools)

Identity pools are well suited to use cases where you need to authenticate users through one of the above IdPs and then authorize access to AWS services such as Amazon S3 and DynamoDB.

**CORRECT:**"Amazon Cognito identity pools" is the correct answer (as explained above.)

**INCORRECT:** "Amazon Cognito user pools" is incorrect.

You can use a user pool for authentication but you would then need to use the identity pool for authorization to AWS services. Therefore, this option would require more additional coding.

**INCORRECT:** "AWS AppSync GraphQL API" is incorrect.

There is no need to implement an API for this use case. The developer simply needs a solution for authorization and access control.

**INCORRECT:** "Amazon API Gateway REST API" is incorrect.

There is no need to implement an API for this use case. The developer simply needs a solution for authorization and access control.

**References:**

<https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-identity.html>

<https://aws.amazon.com/premiumsupport/knowledge-center/cognito-user-pools-identity-pools/>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-cognito/>

**Domain**

AWS Security, Identity, & Compliance

**Question 61Correct**

A Developer needs to be notified by email for all new object creation events in a specific Amazon S3 bucket. Amazon SNS will be used for sending the messages. How can the Developer enable these notifications?

**Create an event notification for all s3:ObjectRestore:Post API calls**

**Create an event notification for all s3:ObjectCreated:Put API calls**

**Create an event notification for all s3:ObjectRemoved:Delete API calls**

**Your answer is correct**

**Create an event notification for all s3:ObjectCreated:\* API calls**

Overall explanation

The Amazon S3 notification feature enables you to receive notifications when certain events happen in your bucket. To enable notifications, you must first add a notification configuration that identifies the events you want Amazon S3 to publish and the destinations where you want Amazon S3 to send the notifications. You store this configuration in the notification subresource that is associated with a bucket.

Currently, Amazon S3 can publish notifications for the following events:

**New object created events** — Amazon S3 supports multiple APIs to create objects. You can request notification when only a specific API is used (for example, s3:ObjectCreated:Put), or you can use a wildcard (for example, s3:ObjectCreated:\*) to request notification when an object is created regardless of the API used.

**Object removal events** — Amazon S3 supports deletes of versioned and unversioned objects. For information about object versioning, see [Object Versioning](https://docs.aws.amazon.com/AmazonS3/latest/dev/ObjectVersioning.html) and [Using Versioning](https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html).

**Restore object events**— Amazon S3 supports the restoration of objects archived to the S3 Glacier storage class. You request to be notified of object restoration completion by using s3:ObjectRestore:Completed. You use s3:ObjectRestore:Post to request notification of the initiation of a restore.

**Reduced Redundancy Storage (RRS) object lost events** — Amazon S3 sends a notification message when it detects that an object of the RRS storage class has been lost.

**Replication events** — Amazon S3 sends event notifications for replication configurations that have S3 Replication Time Control (S3 RTC) enabled. It sends these notifications when an object fails replication, when an object exceeds the 15-minute threshold, when an object is replicated after the 15-minute threshold, and when an object is no longer tracked by replication metrics. It publishes a second event when that object replicates to the destination Region.

Therefore, the Developer should create an event notification for all s3:ObjectCreated:\* API calls as this will capture all new object creation events.

**CORRECT:**"Create an event notification for all s3:ObjectCreated:\* API calls" is the correct answer.

**INCORRECT:** "Create an event notification for all s3:ObjectCreated:Put API calls" is incorrect as this will not capture all new object creation events (e.g. POST or COPY). The wildcard should be used instead.

**INCORRECT:** "Create an event notification for all s3:ObjectRemoved:Delete API calls" is incorrect as this is used for object deletions.

**INCORRECT:** "Create an event notification for all s3:ObjectRestore:Post API calls" is incorrect as this is used for restore events from Amazon S3 Glacier archives.

**References:**

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

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-s3-and-glacier/>

<https://digitalcloud.training/aws-application-integration-services/>

**Domain**

AWS Storage

**Question 62Incorrect**

A start-up has launched a website using Route 53 for domain name, routing, and health checks. They failed to configure Amazon CloudWatch alarms with the health checks. How can the organization be made aware of any endpoint health issues?

**They can subscribe to SNS topics to receive notifications.**

**They can create an alarm using CloudTrail and receive SNS notifications.**

**Your answer is incorrect**

**They can see the status of Route 53 health checks on the Shield dashboard.**

**Correct answer**

**They can see the status of Route 53 health checks on the Route 53 dashboard.**

Overall explanation

Configuring CloudWatch alarms to send a SNS notification if there is an unhealthy endpoint is optional. AWS customers can also review the Route 53 dashboard to identify any health issues.

**CORRECT:**"They can see the status of Route 53 health checks on the Route 53 dashboard" is the correct answer (as explained above.)

**INCORRECT:** "They can see the status of Route 53 health checks on the Shield dashboard" is incorrect. Route 53 health checks are not available on the Shield dashboard.

**INCORRECT:** "They can subscribe to SNS topics to receive notifications" is incorrect. SNS topics can be used to send notifications but must be triggered by CloudWatch alarm first.

**INCORRECT:** "They can create an alarm using CloudTrail and receive SNS notifications" is incorrect. CloudTrail is used to track API activity not for monitoring healthy resources.

**References**:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/welcome-health-checks.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-route-53/>

**Domain**

AWS Networking & Content Delivery

**Question 63Correct**

A company operates a multimedia sharing service on AWS. The service is hosted on Amazon EC2 instances in an Auto Scaling group, serving as the target for an Application Load Balancer (ALB).

The multimedia files are stored in an Amazon S3 bucket. The company is developing a feature for system request testing, which will redirect these requests to a separate target group hosting a test version of the application.

How can this be accomplished most efficiently?

**Create a new S3 bucket to host the test variant of the application. Redirect all test requests to this new bucket.**

**Create a separate AWS Lambda function to handle the test requests and direct them to the new target group.**

**Replicate the existing application and host it on a distinct EC2 instance. Manually route test requests to this instance.**

**Your answer is correct**

**Use ALB content-based routing. Create a separate target group for the test version of the application and route requests identified by a specific cookie.**

Overall explanation

The most efficient solution is to use the ALB's content-based routing feature with a cookie-based strategy. This way, test requests identified by a specific cookie can be directed to the new target group hosting the test variant of the application, without any significant changes to the existing setup.

**CORRECT:**"Use ALB content-based routing. Create a separate target group for the test version of the application and route requests identified by a specific cookie" is the correct answer (as explained above.)

**INCORRECT:** "Replicate the existing application and host it on a distinct EC2 instance. Manually route test requests to this instance" is incorrect.

This approach doesn't leverage the ALB's content-based routing and adds unnecessary manual work

**INCORRECT:** "Create a new S3 bucket to host the test variant of the application. Redirect all test requests to this new bucket" is incorrect.

This method doesn't make use of the ALB and EC2 instances for application hosting, thus inefficient

**INCORRECT:** "Create a separate AWS Lambda function to handle the test requests and direct them to the new target group" is incorrect.

This is inefficient as it adds unnecessary complexity and circumvents the routing features of the ALB

**References:**

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-elastic-load-balancing-aws-elb/>

**Domain**

AWS Compute

**Question 64Correct**

A new AWS Lambda function processes data and sends it to another service. The data is around 1 MB in size. A developer has been asked to update the function so it encrypts the data before sending it on to the other service.

Which API call is required to perform the encryption?

**Pass the data directly to AWS KMS and issue the Encrypt API for encryption.**

**Your answer is correct**

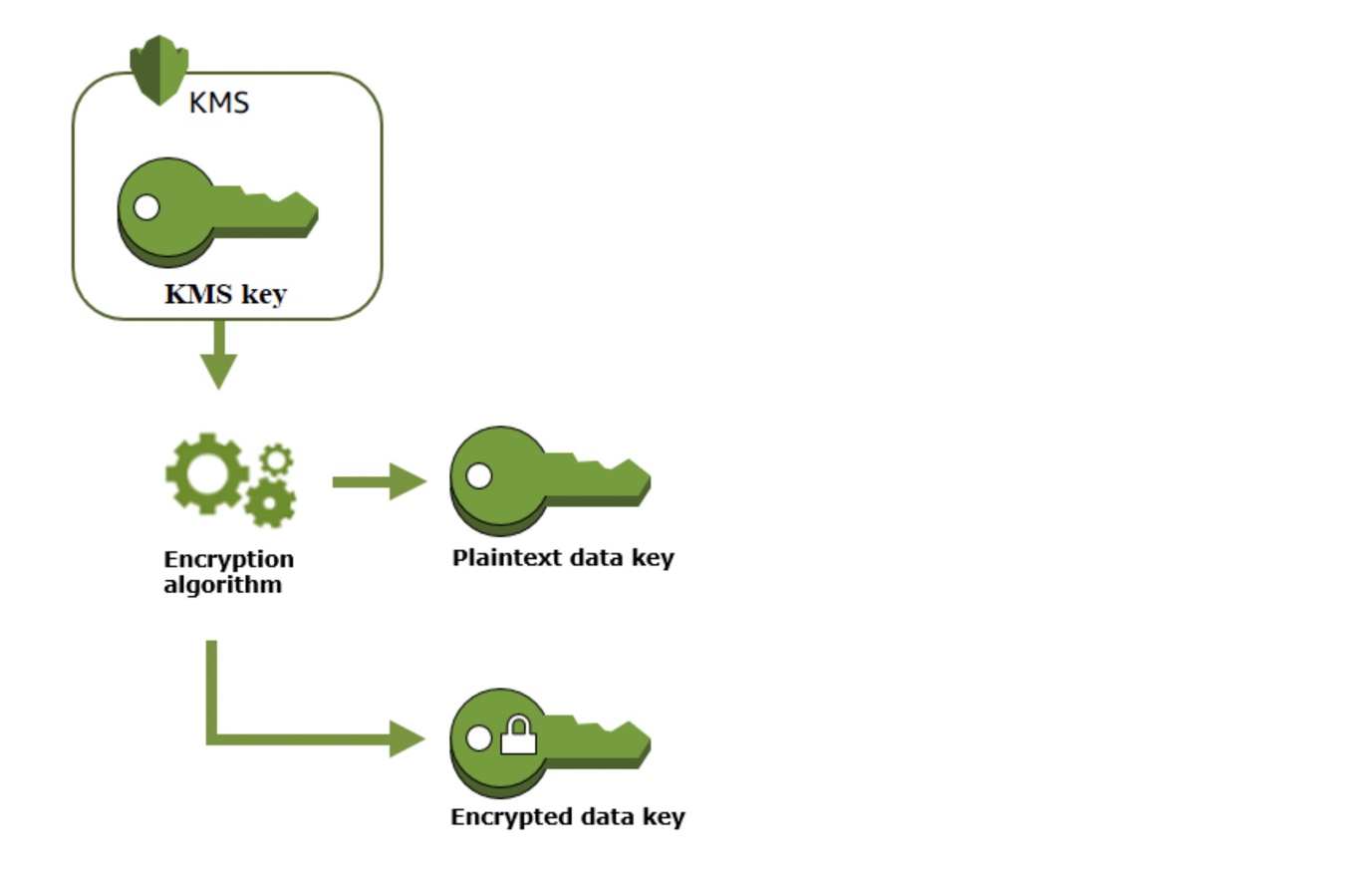
**Issue the AWS KMS GenerateDataKey API to return an encryption key.**

**Issue the AWS KMS GenerateDataKeyWithoutPlainText API to return an encryption key.**

**Pass the data directly to AWS KMS and issue the ReEncrypt API for encryption.**

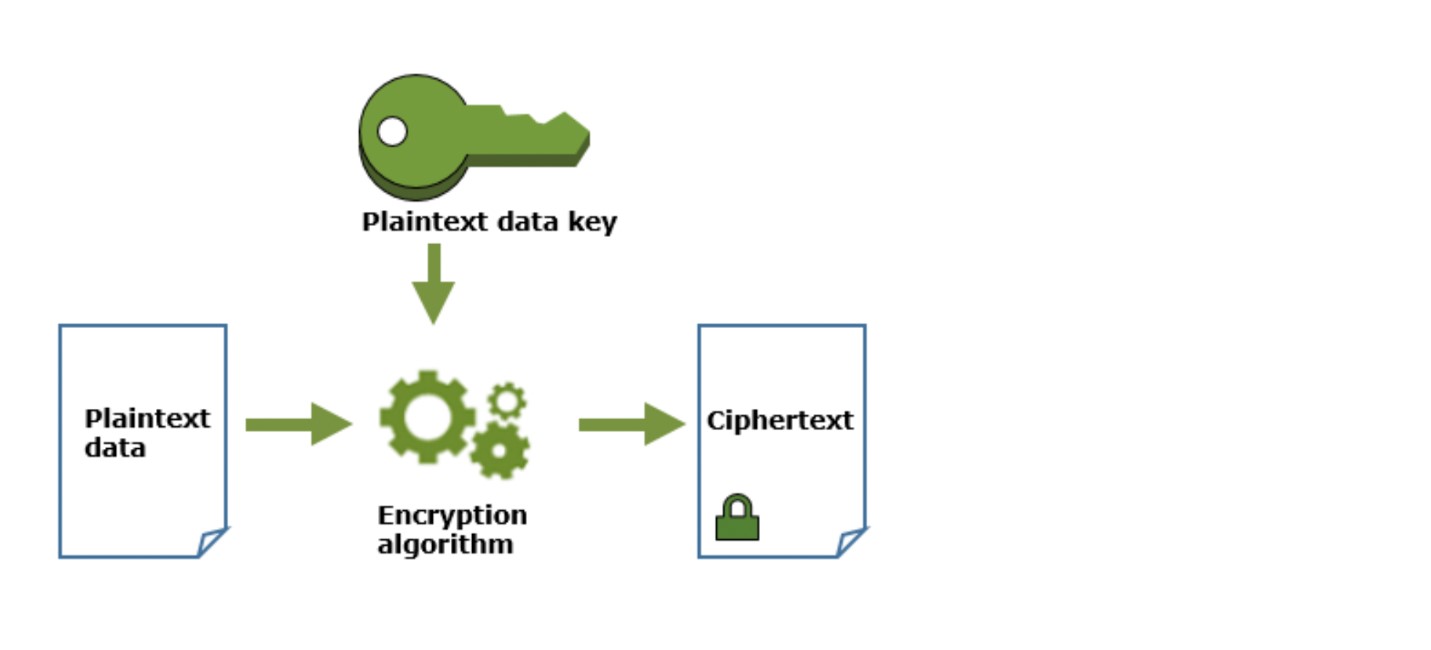
Overall explanation

To create a data key, call the GenerateDataKey operation. AWS KMS generates the data key. Then it encrypts a copy of the data key under a symmetric encryption KMS key that you specify. The operation returns a plaintext copy of the data key and the copy of the data key encrypted under the KMS key. The following image shows this operation.



AWS KMS cannot use a data key to encrypt data. But you can use the data key outside of AWS KMS, such as by using OpenSSL or a cryptographic library like the AWS Encryption SDK.

After using the plaintext data key to encrypt data, remove it from memory as soon as possible. You can safely store the encrypted data key with the encrypted data, so it is available to decrypt the data.



In this case, the Lambda function can use the encryption keys generated to encrypt the data before sending it to the other service. The GenerateDataKey API is the correct API action to use.

**CORRECT:**"Issue the AWS KMS GenerateDataKey API to return an encryption key" is the correct answer (as explained above.)

**INCORRECT:** "Issue the AWS KMS GenerateDataKeyWithoutPlainText API to return an encryption key" is incorrect.

This API action returns only an encrypted data key. When you need to use the data key, ask AWS KMS to decrypt it. The correct API for directly encrypting larger amounts of data is the GenerateDataKey API.

**INCORRECT:** "Pass the data directly to AWS KMS and issue the Encrypt API for encryption" is incorrect.

AWS KMS can only encrypt data up to 4096 bytes. Therefore, the data must be encrypted outside of KMS and a data key must be generated for this purpose.

**INCORRECT:** "Pass the data directly to AWS KMS and issue the ReEncrypt API for encryption" is incorrect.

The reencrypt API decrypts data before reencrypting it within AWS KMS. In this case the data is not currently encrypted and the operations cannot take place within KMS as the data is larger than the KMS maximum of 4096 bytes.

**References:**

<https://docs.aws.amazon.com/kms/latest/APIReference/API_GenerateDataKey.html>

<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#data-keys>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-kms/>

**Domain**

AWS Security, Identity, & Compliance

**Question 65Correct**

An Amazon DynamoDB table has been created using provisioned capacity. A manager needs to understand whether the DynamoDB table is cost-effective. How can the manager query how much provisioned capacity is actually being used?

**Use Amazon CloudTrail and monitor the DescribeLimits API action**

**Your answer is correct**

**Monitor the ConsumedReadCapacityUnits and ConsumedWriteCapacityUnits over a specified time period**

**Monitor the ReadThrottleEvents and WriteThrottleEvents metrics for the table**

**1. Use AWS X-Ray to instrument the DynamoDB table and monitor sub segments**

Overall explanation

You can monitor Amazon DynamoDB using CloudWatch, which collects and processes raw data from DynamoDB into readable, near real-time metrics. These statistics are retained for a period of time, so that you can access historical information for a better perspective on how your web application or service is performing. By default, DynamoDB metric data is sent to CloudWatch automatically.

To determine how much of the provisioned capacity is being used you can monitor ConsumedReadCapacityUnits or ConsumedWriteCapacityUnits over the specified time period.

**CORRECT:**"Monitor the ConsumedReadCapacityUnits and ConsumedWriteCapacityUnits over a specified time period" is the correct answer.

**INCORRECT:** "Monitor the ReadThrottleEvents and WriteThrottleEvents metrics for the table" is incorrect as these metrics are used to determine which requests exceed the provisioned throughput limits of a table.

**INCORRECT:** "Use Amazon CloudTrail and monitor the DescribeLimits API action" is incorrect as CloudTrail records API actions, not performance metrics.

**INCORRECT:** "Use AWS X-Ray to instrument the DynamoDB table and monitor subsegments" is incorrect. DynamoDB does not directly integrate with X-Ray but you can record information in subsegments for downstream requests. This is not, however, a method for monitoring provisioned capacity utilization.

**References:**

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/monitoring-cloudwatch.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/amazon-dynamodb/>

<https://digitalcloud.training/amazon-cloudwatch/>

**Domain**

AWS Database