



CertyIQ

Premium exam material

Get certification quickly with the CertyIQ Premium exam material.
Everything you need to prepare, learn & pass your certification exam easily. Lifetime free updates
First attempt guaranteed success.

<https://www.CertyIQ.com>



CompTIA

About CertyIQ

We here at CertyIQ eventually got enough of the industry's greedy exam paid for. Our team of IT professionals comes with years of experience in the IT industry Prior to training CertyIQ we worked in test areas where we observed the horrors of the paywall exam preparation system.

The misuse of the preparation system has left our team disillusioned. And for that reason, we decided it was time to make a difference. We had to make In this way, CertyIQ was created to provide quality materials without stealing from everyday people who are trying to make a living.

Doubt Support

We have developed a very scalable solution using which we are able to solve 400+ doubts every single day with an average rating of 4.8 out of 5.

<https://www.certyiq.com>

Mail us on - certyiqofficial@gmail.com



Lifetime Free Updates

We provide lifetime free updates to our customers. To make life easier for our valued customers and fulfill their needs



Free Exam PDF

You are sure to pass the exam completely free of charge



Money Back Guarantee

We Provide 100% money back guarantee to our customer in case of any failure

John

October 19, 2022



Thanks you so much for your help. I scored 972 in my exam today. More than 90% were from your PDFs!

October 22, 2022



Passed my exam today with 891 marks. Out of 52 questions, 51 were from certyiQ PDFs including Contoso case study. Thank You certyiQ team!

Dana

September 04, 2022



Thanks a lot for this updated AZ-900 Q&A. I just passed my exam and got 974, I followed both of your Az-900 videos and the 6 PDF, the PDFs are very much valid, all answers are correct. Could you please create a similar video/PDF for DP900, your content/PDF's is really awesome. The team did a really good job. Thank You 😊.

Henry Rome

2 months ago



These questions are real and 100 % valid. Thank you so much for your efforts, also your 4 PDFs are awesome, I passed the DP900 exam on 1 Sept. With 968 marks. Thanks a lot, buddy!

Esmaria

2 months ago



Simple easy to understand explanations. To anyone out there wanting to write AZ900, I highly recommend 6 PDF's. Thank you so much, appreciate all your hard work in having such great content. Passed my exam Today - 3 September with 942 score.

Ahamed Shibly

2 months ago



Customer support is really fast and helpful, I just finished my exam and this video along with the 6 PDF helped me pass! Definitely recommend getting the PDFs. Thank you!

Amazon

(AWS Certified Developer - Associate DVA-C02)

AWS Certified Developer - Associate DVA-C02

Total: **357 Questions**

Link: <https://certiq.com/papers?provider=amazon&exam=aws-certified-developer-associate-dva-c02>

Question: 1

CertyIQ

A company is implementing an application on Amazon EC2 instances. The application needs to process incoming transactions. When the application detects a transaction that is not valid, the application must send a chat message to the company's support team. To send the message, the application needs to retrieve the access token to authenticate by using the chat API.

A developer needs to implement a solution to store the access token. The access token must be encrypted at rest and in transit. The access token must also be accessible from other AWS accounts.

Which solution will meet these requirements with the LEAST management overhead?

- A.Use an AWS Systems Manager Parameter Store SecureString parameter that uses an AWS Key Management Service (AWS KMS) AWS managed key to store the access token. Add a resource-based policy to the parameter to allow access from other accounts. Update the IAM role of the EC2 instances with permissions to access Parameter Store. Retrieve the token from Parameter Store with the decrypt flag enabled. Use the decrypted access token to send the message to the chat.
- B.Encrypt the access token by using an AWS Key Management Service (AWS KMS) customer managed key. Store the access token in an Amazon DynamoDB table. Update the IAM role of the EC2 instances with permissions to access DynamoDB and AWS KMS. Retrieve the token from DynamoDB Decrypt the token by using AWS KMS on the EC2 instances. Use the decrypted access token to send the message to the chat.
- C.Use AWS Secrets Manager with an AWS Key Management Service (AWS KMS) customer managed key to store the access token. Add a resource-based policy to the secret to allow access from other accounts. Update the IAM role of the EC2 instances with permissions to access Secrets Manager. Retrieve the token from Secrets Manager. Use the decrypted access token to send the message to the chat.
- D.Encrypt the access token by using an AWS Key Management Service (AWS KMS) AWS managed key. Store the access token in an Amazon S3 bucket. Add a bucket policy to the S3 bucket to allow access from other accounts. Update the IAM role of the EC2 instances with permissions to access Amazon S3 and AWS KMS. Retrieve the token from the S3 bucket. Decrypt the token by using AWS KMS on the EC2 instances. Use the decrypted access token to send the message to the chat.

Answer: C

Explanation:

The correct answer is C.

<https://aws.amazon.com/premiumsupport/knowledge-center/secrets-manager-share-between-accounts/>

https://docs.aws.amazon.com/secretsmanager/latest/userguide/auth-and-access_examples_cross.html

Option A is wrong. It seems to be a good solution. However, AWS managed keys cannot be used for cross account accessing.

Question: 2

CertyIQ

A company is running Amazon EC2 instances in multiple AWS accounts. A developer needs to implement an application that collects all the lifecycle events of the EC2 instances. The application needs to store the lifecycle events in a single Amazon Simple Queue Service (Amazon SQS) queue in the company's main AWS account for further processing.

Which solution will meet these requirements?

- A.Configure Amazon EC2 to deliver the EC2 instance lifecycle events from all accounts to the Amazon EventBridge event bus of the main account. Add an EventBridge rule to the event bus of the main account that matches all EC2 instance lifecycle events. Add the SQS queue as a target of the rule.
- B.Use the resource policies of the SQS queue in the main account to give each account permissions to write to that SQS queue. Add to the Amazon EventBridge event bus of each account an EventBridge rule that matches all EC2 instance lifecycle events. Add the SQS queue in the main account as a target of the rule.
- C.Write an AWS Lambda function that scans through all EC2 instances in the company accounts to detect EC2 instance lifecycle changes. Configure the Lambda function to write a notification message to the SQS queue in the main account if the function detects an EC2 instance lifecycle change. Add an Amazon EventBridge scheduled rule that invokes the Lambda function every minute.

D.Configure the permissions on the main account event bus to receive events from all accounts. Create an Amazon EventBridge rule in each account to send all the EC2 instance lifecycle events to the main account event bus. Add an EventBridge rule to the main account event bus that matches all EC2 instance lifecycle events. Set the SQS queue as a target for the rule.

Answer: D

Explanation:

The correct answer is D. Amazon EC2 instances can send the state-change notification events to Amazon Event Bridge. Amazon Event Bridge can send and receive events between event buses in AWS accounts.

Reference:

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-cross-account.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-instance-state-changes.html>

CertyIQ

An application is using Amazon Cognito user pools and identity pools for secure access. A developer wants to integrate the user-specific file upload and download features in the application with Amazon S3. The developer must ensure that the files are saved and retrieved in a secure manner and that users can access only their own files. The file sizes range from 3 KB to 300 MB.

Which option will meet these requirements with the HIGHEST level of security?

- A.Use S3 Event Notifications to validate the file upload and download requests and update the user interface (UI).
- B.Save the details of the uploaded files in a separate Amazon DynamoDB table. Filter the list of files in the user interface (UI) by comparing the current user ID with the user ID associated with the file in the table.
- C.Use Amazon API Gateway and an AWS Lambda function to upload and download files. Validate each request in the Lambda function before performing the requested operation.
- D.Use an IAM policy within the Amazon Cognito identity prefix to restrict users to use their own folders in Amazon S3.

Answer: D

Explanation:

DI actually apply this solution the production applications.

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_s3_cognito-bucket.html

<https://docs.amplify.aws/lib/storage/getting-started/q/platform/js/>

CertyIQ

A company is building a scalable data management solution by using AWS services to improve the speed and agility of development. The solution will ingest large volumes of data from various sources and will process this data through multiple business rules and transformations.

The solution requires business rules to run in sequence and to handle reprocessing of data if errors occur when the business rules run. The company needs the solution to be scalable and to require the least possible maintenance. Which AWS service should the company use to manage and automate the orchestration of the data flows to meet these requirements?

- A.AWS Batch
- B.AWS Step Functions
- C.AWS Glue
- D.AWS Lambda

Answer: B

Explanation:

B in it

You can use Step functions to create a workflow of functions that should be invoked in a sequence. You can also push output from one one-step function and use it as an input for next-step function. Also, Step functions have very useful Retry and Catch -> error-handling features.

Question: 5

CertyIQ

A developer has created an AWS Lambda function that is written in Python. The Lambda function reads data from objects in Amazon S3 and writes data to an Amazon DynamoDB table. The function is successfully invoked from an S3 event notification when an object is created. However, the function fails when it attempts to write to the DynamoDB table.

What is the MOST likely cause of this issue?

- A.The Lambda function's concurrency limit has been exceeded.
- B.DynamoDB table requires a global secondary index (GSI) to support writes.
- C.The Lambda function does not have IAM permissions to write to DynamoDB.
- D.The DynamoDB table is not running in the same Availability Zone as the Lambda function.

Answer: C

Explanation:

Correct answer is C

It is clearly something about permissions. So not A or B. Lambda functions can run in multiple Availability Zones (AZs) to ensure high availability and resilience. So it is not D.

Question: 6

CertyIQ

A developer is creating an AWS CloudFormation template to deploy Amazon EC2 instances across multiple AWS accounts. The developer must choose the EC2 instances from a list of approved instance types.

How can the developer incorporate the list of approved instance types in the CloudFormation template?

- A.Create a separate CloudFormation template for each EC2 instance type in the list.
- B.In the Resources section of the CloudFormation template, create resources for each EC2 instance type in the list.
- C.In the CloudFormation template, create a separate parameter for each EC2 instance type in the list.
- D.In the CloudFormation template, create a parameter with the list of EC2 instance types as AllowedValues.

Answer: D

Explanation:

D is the correct answer. In the Cloud Formation template, the developer should create a parameter with the list of approved EC2 instance types as Allowed Values. This way, users can select the instance type they want to use when launching the Cloud Formation stack, but only from the approved list. Option A is not a scalable solution as it requires creating a separate Cloud Formation template for each EC2 instance type, which can become cumbersome and difficult to manage as the number of approved instance types grows. Option B is not necessary as creating resources for each EC2 instance type in the list would not enforce the requirement to choose only from the approved list. It would also increase the complexity of the template and make it difficult to manage. Option C is not ideal as it would require creating a separate parameter for each EC2 instance type, which can become difficult to manage as the number of approved instance types grows. Also, it does not enforce the requirement to choose only from the approved list.

Question: 7

CertyIQ

A developer has an application that makes batch requests directly to Amazon DynamoDB by using the BatchGetItem low-level API operation. The responses frequently return values in the UnprocessedKeys element. Which actions should the developer take to increase the resiliency of the application when the batch response includes values in UnprocessedKeys? (Choose two.)

- A.Retry the batch operation immediately.
- B.Retry the batch operation with exponential backoff and randomized delay.
- C.Update the application to use an AWS software development kit (AWS SDK) to make the requests.
- D.Increase the provisioned read capacity of the DynamoDB tables that the operation accesses.
- E.Increase the provisioned write capacity of the DynamoDB tables that the operation accesses.

Answer: BD

Explanation:

B and D is correct answer. AWS SDK automatically takes care of both retry and exponential back off. If we choose C, selecting only C will answer our question(no need of B) but We need to choose 2 answer. In addition, question does not specifically say to change core logic from low level api to SDK. by choosing B and D we can improve resiliency.

Reference:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Programming.Errors.html#Programming.Errors.RetryAndBackoff>.

Question: 8

CertyIQ

A company is running a custom application on a set of on-premises Linux servers that are accessed using Amazon API Gateway. AWS X-Ray tracing has been enabled on the API test stage. How can a developer enable X-Ray tracing on the on-premises servers with the LEAST amount of configuration?

- A.Install and run the X-Ray SDK on the on-premises servers to capture and relay the data to the X-Ray service.
- B.Install and run the X-Ray daemon on the on-premises servers to capture and relay the data to the X-Ray service.
- C.Capture incoming requests on-premises and configure an AWS Lambda function to pull, process, and relay relevant data to X-Ray using the PutTraceSegments API call.
- D.Capture incoming requests on-premises and configure an AWS Lambda function to pull, process, and relay relevant data to X-Ray using the PutTelemetryRecords API call.

Answer: B**Explanation:**

Install and run the X-Ray daemon on the on-premises servers to capture and relay the data to the X-Ray service is the correct option. The X-Ray daemon can be installed and configured on the on-premises servers to capture data and send it to the X-Ray service. This requires minimal configuration and setup. Option A is incorrect because while the X-Ray SDK can be used to capture data on the on-premises servers, it requires more configuration and development effort than the X-Ray daemon. Option C and D are also incorrect because they involve setting up an AWS Lambda function, which is not necessary for enabling X-Ray tracing on the on-premises servers.

Question: 9**CertyIQ**

A company wants to share information with a third party. The third party has an HTTP API endpoint that the company can use to share the information. The company has the required API key to access the HTTP API. The company needs a way to manage the API key by using code. The integration of the API key with the application code cannot affect application performance.

Which solution will meet these requirements MOST securely?

- A.Store the API credentials in AWS Secrets Manager. Retrieve the API credentials at runtime by using the AWS SDK. Use the credentials to make the API call.
- B.Store the API credentials in a local code variable. Push the code to a secure Git repository. Use the local code variable at runtime to make the API call.
- C.Store the API credentials as an object in a private Amazon S3 bucket. Restrict access to the S3 object by using IAM policies. Retrieve the API credentials at runtime by using the AWS SDK. Use the credentials to make the API call.
- D.Store the API credentials in an Amazon DynamoDB table. Restrict access to the table by using resource-based policies. Retrieve the API credentials at runtime by using the AWS SDK. Use the credentials to make the API call.

Answer: A**Explanation:**

Correct answer is A:Store the API credentials in AWS Secrets Manager. Retrieve the API credentials at runtime by using the AWS SDK. Use the credentials to make the API call.

Question: 10**CertyIQ**

A developer is deploying a new application to Amazon Elastic Container Service (Amazon ECS). The developer needs to securely store and retrieve different types of variables. These variables include authentication information for a remote API, the URL for the API, and credentials. The authentication information and API URL must be available to all current and future deployed versions of the application across development, testing, and production environments.

How should the developer retrieve the variables with the FEWEST application changes?

- A.Update the application to retrieve the variables from AWS Systems Manager Parameter Store. Use unique paths in Parameter Store for each variable in each environment. Store the credentials in AWS Secrets Manager in each environment.
- B.Update the application to retrieve the variables from AWS Key Management Service (AWS KMS). Store the API URL and credentials as unique keys for each environment.
- C.Update the application to retrieve the variables from an encrypted file that is stored with the application. Store the API URL and credentials in unique files for each environment.

D.Update the application to retrieve the variables from each of the deployed environments. Define the authentication information and API URL in the ECS task definition as unique names during the deployment process.

Answer: A

Explanation:

The application has credentials and URL, so it's convenient to store them in ssm parameter store restive them.

AWS Systems Manager Parameter Store is a service that allows you to securely store configuration data such as API URLs, credentials, and other variables. By updating the application to retrieve the variables from Parameter Store, you can separate the configuration from the application code, making it easier to manage and update the variables without modifying the application itself. Storing the credentials in AWS Secrets Manager provides an additional layer of security for sensitive information.

Question: 11

CertyIQ

A company is migrating legacy internal applications to AWS. Leadership wants to rewrite the internal employee directory to use native AWS services. A developer needs to create a solution for storing employee contact details and high-resolution photos for use with the new application.

Which solution will enable the search and retrieval of each employee's individual details and high-resolution photos using AWS APIs?

- A.Encode each employee's contact information and photos using Base64. Store the information in an Amazon DynamoDB table using a sort key.
- B.Store each employee's contact information in an Amazon DynamoDB table along with the object keys for the photos stored in Amazon S3.
- C.Use Amazon Cognito user pools to implement the employee directory in a fully managed software-as-a-service (SaaS) method.
- D.Store employee contact information in an Amazon RDS DB instance with the photos stored in Amazon Elastic File System (Amazon EFS).

Answer: B

Explanation:

B. Store each employee's contact information in an Amazon DynamoDB table along with the object keys for the photos stored in Amazon S3. Storing each employee's contact information in an Amazon DynamoDB table along with the object keys for the photos stored in Amazon S3 provides a scalable and efficient solution for storing and retrieving employee details and high-resolution photos using AWS APIs. The developer can use the DynamoDB table to query and retrieve employee details, while the S3 bucket can be used to store the high-resolution photos. By using S3, the solution can support large amounts of data while enabling fast retrieval times. The combination of DynamoDB and S3 can provide a cost-effective and scalable solution for storing employee data and photos.

Question: 12

CertyIQ

A developer is creating an application that will give users the ability to store photos from their cellphones in the cloud. The application needs to support tens of thousands of users. The application uses an Amazon API Gateway REST API that is integrated with AWS Lambda functions to process the photos. The application stores details about the photos in Amazon DynamoDB.

Users need to create an account to access the application. In the application, users must be able to upload photos and retrieve previously uploaded photos. The photos will range in size from 300 KB to 5 MB.

Which solution will meet these requirements with the LEAST operational overhead?

- A.Use Amazon Cognito user pools to manage user accounts. Create an Amazon Cognito user pool authorizer in API Gateway to control access to the API. Use the Lambda function to store the photos and details in the DynamoDB table. Retrieve previously uploaded photos directly from the DynamoDB table.
- B.Use Amazon Cognito user pools to manage user accounts. Create an Amazon Cognito user pool authorizer in API Gateway to control access to the API. Use the Lambda function to store the photos in Amazon S3. Store the object's S3 key as part of the photo details in the DynamoDB table. Retrieve previously uploaded photos by querying DynamoDB for the S3 key.
- C.Create an IAM user for each user of the application during the sign-up process. Use IAM authentication to access the API Gateway API. Use the Lambda function to store the photos in Amazon S3. Store the object's S3 key as part of the photo details in the DynamoDB table. Retrieve previously uploaded photos by querying DynamoDB for the S3 key.
- D.Create a users table in DynamoDB. Use the table to manage user accounts. Create a Lambda authorizer that validates user credentials against the users table. Integrate the Lambda authorizer with API Gateway to control access to the API. Use the Lambda function to store the photos in Amazon S3. Store the object's S3 key as part of the photo details in the DynamoDB table. Retrieve previously uploaded photos by querying DynamoDB for the S3 key.

Answer: B

Explanation:

B is the most valid solution. A nearest, but invalid, because you cannot store object in Dynamo.

Reference:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html>

<https://aws.amazon.com/blogs/big-data/building-and-maintaining-an-amazon-s3-metadata-index-without-servers/>

Question: 13

CertyIQ

A company receives food orders from multiple partners. The company has a microservices application that uses Amazon API Gateway APIs with AWS Lambda integration. Each partner sends orders by calling a customized API that is exposed through API Gateway. The API call invokes a shared Lambda function to process the orders. Partners need to be notified after the Lambda function processes the orders. Each partner must receive updates for only the partner's own orders. The company wants to add new partners in the future with the fewest code changes possible.

Which solution will meet these requirements in the MOST scalable way?

- A.Create a different Amazon Simple Notification Service (Amazon SNS) topic for each partner. Configure the Lambda function to publish messages for each partner to the partner's SNS topic.
- B.Create a different Lambda function for each partner. Configure the Lambda function to notify each partner's service endpoint directly.
- C.Create an Amazon Simple Notification Service (Amazon SNS) topic. Configure the Lambda function to publish messages with specific attributes to the SNS topic. Subscribe each partner to the SNS topic. Apply the appropriate filter policy to the topic subscriptions.
- D.Create one Amazon Simple Notification Service (Amazon SNS) topic. Subscribe all partners to the SNS topic.

Answer: C

Explanation:

Option C is the most scalable way to meet the requirements. This solution allows for a single SNS topic to be used for all partners, which minimizes the need for code changes when adding new partners. By publishing messages with specific attributes to the SNS topic and applying the appropriate filter policy to the topic

subscriptions, partners will only receive notifications for their own orders. This approach allows for a more flexible and scalable solution, where new partners can be added to the system with minimal changes to the existing codebase. Option A and D may not be scalable when there are a large number of partners, as creating a separate SNS topic for each partner or subscribing all partners to a single topic may not be feasible. Option B may result in a large number of Lambda functions that need to be managed separately.

Question: 14

CertyIQ

A financial company must store original customer records for 10 years for legal reasons. A complete record contains personally identifiable information (PII). According to local regulations, PII is available to only certain people in the company and must not be shared with third parties. The company needs to make the records available to third-party organizations for statistical analysis without sharing the PII. A developer wants to store the original immutable record in Amazon S3. Depending on who accesses the S3 document, the document should be returned as is or with all the PII removed. The developer has written an AWS Lambda function to remove the PII from the document. The function is named removePii. What should the developer do so that the company can meet the PII requirements while maintaining only one copy of the document?

- A. Set up an S3 event notification that invokes the removePii function when an S3 GET request is made. Call Amazon S3 by using a GET request to access the object without PII.
- B. Set up an S3 event notification that invokes the removePii function when an S3 PUT request is made. Call Amazon S3 by using a PUT request to access the object without PII.
- C. Create an S3 Object Lambda access point from the S3 console. Select the removePii function. Use S3 Access Points to access the object without PII.
- D. Create an S3 access point from the S3 console. Use the access point name to call the GetObjectLegalHold S3 API function. Pass in the removePii function name to access the object without PII.

Answer: C

Explanation:

Create an S3 Object Lambda access point from the S3 console. Select the remove Pii function. Use S3 Access Points to access the object without PII.

Reference:

<https://aws.amazon.com/s3/features/object-lambda/>

Question: 15

CertyIQ

A developer is deploying an AWS Lambda function. The developer wants the ability to return to older versions of the function quickly and seamlessly.

How can the developer achieve this goal with the LEAST operational overhead?

- A. Use AWS OpsWorks to perform blue/green deployments.
- B. Use a function alias with different versions.
- C. Maintain deployment packages for older versions in Amazon S3.
- D. Use AWS CodePipeline for deployments and rollbacks.

Answer: B

Explanation:

Correct answer is B: Use a function alias with different versions.

Reference:

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

CertyIQ

Question: 16

A developer has written an AWS Lambda function. The function is CPU-bound. The developer wants to ensure that the function returns responses quickly.

How can the developer improve the function's performance?

- A.Increase the function's CPU core count.
- B.Increase the function's memory.
- C.Increase the function's reserved concurrency.
- D.Increase the function's timeout.

Answer: B

Explanation:

Option B is correct, the only adjustable parameter (in terms of hardware) is lambda memory. Increasing lambda memory will result in automatic adjustment of CPU. Lambda memory is adjustable from 128 MB up to 10 GB.

CertyIQ

Question: 17

For a deployment using AWS Code Deploy, what is the run order of the hooks for in-place deployments?

- A.BeforeInstall -> ApplicationStop -> ApplicationStart -> AfterInstall
- B.ApplicationStop -> BeforeInstall -> AfterInstall -> ApplicationStart
- C.BeforeInstall -> ApplicationStop -> ValidateService -> ApplicationStart
- D.ApplicationStop -> BeforeInstall -> ValidateService -> ApplicationStart

Answer: B

Explanation:

Application must be stopped before installation. Otherwise the installation may corrupt the running application's files and cause damages. Not good.

Reference:

<https://docs.aws.amazon.com/codedeploy/latest/userguide/reference-appspec-file-structure-hooks.html#appspec-hooks-server>

CertyIQ

Question: 18

A company is building a serverless application on AWS. The application uses an AWS Lambda function to process customer orders 24 hours a day, 7 days a week. The Lambda function calls an external vendor's HTTP API to process payments.

During load tests, a developer discovers that the external vendor payment processing API occasionally times out and returns errors. The company expects that some payment processing API calls will return errors.

The company wants the support team to receive notifications in near real time only when the payment processing external API error rate exceed 5% of the total number of transactions in an hour. Developers need to use an existing Amazon Simple Notification Service (Amazon SNS) topic that is configured to notify the support team. Which solution will meet these requirements?

- A. Write the results of payment processing API calls to Amazon CloudWatch. Use Amazon CloudWatch Logs Insights to query the CloudWatch logs. Schedule the Lambda function to check the CloudWatch logs and notify the existing SNS topic.
- B. Publish custom metrics to CloudWatch that record the failures of the external payment processing API calls. Configure a CloudWatch alarm to notify the existing SNS topic when error rate exceeds the specified rate.
- C. Publish the results of the external payment processing API calls to a new Amazon SNS topic. Subscribe the support team members to the new SNS topic.
- D. Write the results of the external payment processing API calls to Amazon S3. Schedule an Amazon Athena query to run at regular intervals. Configure Athena to send notifications to the existing SNS topic when the error rate exceeds the specified rate.

Answer: B

Explanation:

B. Publish custom metrics to Cloud Watch that record the failures of the external payment processing API calls. Configure a Cloud Watch alarm to notify the existing SNS topic when the error rate exceeds the specified rate is the best solution to meet the requirements. With Cloud Watch custom metrics, developers can publish and monitor custom data points, including the number of failed requests to the external payment processing API. A Cloud Watch alarm can be configured to notify an SNS topic when the error rate exceeds the specified rate, allowing the support team to be notified in near real-time. Option A is not optimal since it involves scheduling a Lambda function to check the Cloud Watch logs. Option C may not provide the desired functionality since it does not specify a rate at which to notify the support team. Option D is more complex than necessary, as it involves writing the results to S3 and configuring an Athena query to send notifications to an SNS topic.

Question: 19

CertyIQ

A company is offering APIs as a service over the internet to provide unauthenticated read access to statistical information that is updated daily. The company uses Amazon API Gateway and AWS Lambda to develop the APIs. The service has become popular, and the company wants to enhance the responsiveness of the APIs. Which action can help the company achieve this goal?

- A. Enable API caching in API Gateway.
- B. Configure API Gateway to use an interface VPC endpoint.
- C. Enable cross-origin resource sharing (CORS) for the APIs.
- D. Configure usage plans and API keys in API Gateway.

Answer: A

Explanation:

A. Enable API caching in API Gateway can help the company enhance the responsiveness of the APIs. By enabling caching, API Gateway stores the responses from the API and returns them for subsequent requests instead of forwarding the requests to Lambda. This reduces the number of requests to Lambda, improves API performance, and reduces latency for users.

Question: 20

A developer wants to store information about movies. Each movie has a title, release year, and genre. The movie information also can include additional properties about the cast and production crew. This additional information is inconsistent across movies. For example, one movie might have an assistant director, and another movie might have an animal trainer.

The developer needs to implement a solution to support the following use cases:

For a given title and release year, get all details about the movie that has that title and release year.

For a given title, get all details about all movies that have that title.

For a given genre, get all details about all movies in that genre.

Which data store configuration will meet these requirements?

A.Create an Amazon DynamoDB table. Configure the table with a primary key that consists of the title as the partition key and the release year as the sort key. Create a global secondary index that uses the genre as the partition key and the title as the sort key.

B.Create an Amazon DynamoDB table. Configure the table with a primary key that consists of the genre as the partition key and the release year as the sort key. Create a global secondary index that uses the title as the partition key.

C.On an Amazon RDS DB instance, create a table that contains columns for title, release year, and genre. Configure the title as the primary key.

D.On an Amazon RDS DB instance, create a table where the primary key is the title and all other data is encoded into JSON format as one additional column.

Answer: A**Explanation:**

A. Create an Amazon DynamoDB table. Configure the table with a primary key that consists of the title as the partition key and the release year as the sort key. Create a global secondary index that uses the genre as the partition key and the title as the sort key. This option is the best choice for the given requirements. By using DynamoDB, the developer can store the movie information in a flexible and scalable NoSQL database. The primary key can be set to the title and release year, allowing for efficient retrieval of information about a specific movie. The global secondary index can be created using the genre as the partition key, allowing for efficient retrieval of information about all movies in a specific genre. Additionally, the use of a NoSQL database like DynamoDB allows for the flexible storage of additional properties about the cast and crew, as each movie can have different properties without affecting the structure of the database.

Question: 21

A developer maintains an Amazon API Gateway REST API. Customers use the API through a frontend UI and Amazon Cognito authentication.

The developer has a new version of the API that contains new endpoints and backward-incompatible interface changes. The developer needs to provide beta access to other developers on the team without affecting customers.

Which solution will meet these requirements with the LEAST operational overhead?

A.Define a development stage on the API Gateway API. Instruct the other developers to point the endpoints to the development stage.

B.Define a new API Gateway API that points to the new API application code. Instruct the other developers to point the endpoints to the new API.

C.Implement a query parameter in the API application code that determines which code version to call.

D.Specify new API Gateway endpoints for the API endpoints that the developer wants to add.

Answer: A**Explanation:**

Option A is the correct solution to meet the requirements with the least operational overhead. Defining a development stage on the API Gateway API enables other developers to test the new version of the API without affecting the production environment. This approach allows the developers to work on the new version of the API independently and avoid conflicts with the production environment. The other options involve creating a new API or new endpoints, which could introduce additional operational overhead, such as managing multiple APIs or endpoints, configuring access control, and updating the frontend UI to point to the new endpoints or API. Option C also introduces additional complexity by requiring the implementation of a query parameter to determine which code version to call.

Question: 22

CertyIQ

A developer is creating an application that will store personal health information (PHI). The PHI needs to be encrypted at all times. An encrypted Amazon RDS for MySQL DB instance is storing the data. The developer wants to increase the performance of the application by caching frequently accessed data while adding the ability to sort or rank the cached datasets.

Which solution will meet these requirements?

- A.Create an Amazon ElastiCache for Redis instance. Enable encryption of data in transit and at rest. Store frequently accessed data in the cache.
- B.Create an Amazon ElastiCache for Memcached instance. Enable encryption of data in transit and at rest. Store frequently accessed data in the cache.
- C.Create an Amazon RDS for MySQL read replica. Connect to the read replica by using SSL. Configure the read replica to store frequently accessed data.
- D.Create an Amazon DynamoDB table and a DynamoDB Accelerator (DAX) cluster for the table. Store frequently accessed data in the DynamoDB table.

Answer: A

Explanation:

To meet the requirements of caching frequently accessed data while adding the ability to sort or rank cached datasets, a developer should choose Amazon Elastic Cache for Redis. Elastic cache is a web service that provides an in-memory data store in the cloud, and it supports both Memcached and Redis engines. While both engines are suitable for caching frequently accessed data, Redis is a better choice for this use case because it provides sorted sets and other data structures that allow for sorting and ranking of cached datasets. The data in Elastic Cache can be encrypted at rest and in transit, ensuring the security of the PHI. Therefore, option A is the correct answer.

Question: 23

CertyIQ

A company has a multi-node Windows legacy application that runs on premises. The application uses a network shared folder as a centralized configuration repository to store configuration files in .xml format. The company is migrating the application to Amazon EC2 instances. As part of the migration to AWS, a developer must identify a solution that provides high availability for the repository.

Which solution will meet this requirement MOST cost-effectively?

- A.Mount an Amazon Elastic Block Store (Amazon EBS) volume onto one of the EC2 instances. Deploy a file system on the EBS volume. Use the host operating system to share a folder. Update the application code to read and write configuration files from the shared folder.
- B.Deploy a micro EC2 instance with an instance store volume. Use the host operating system to share a folder. Update the application code to read and write configuration files from the shared folder.
- C.Create an Amazon S3 bucket to host the repository. Migrate the existing .xml files to the S3 bucket. Update the application code to use the AWS SDK to read and write configuration files from Amazon S3.

D.Create an Amazon S3 bucket to host the repository. Migrate the existing .xml files to the S3 bucket. Mount the S3 bucket to the EC2 instances as a local volume. Update the application code to read and write configuration files from the disk.

Answer: C

Explanation:

Create an Amazon S3 bucket to host the repository. Migrate the existing .xml files to the S3 bucket. Update the application code to use the AWS SDK to read and write configuration files from Amazon S3.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/AmazonS3.html>
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingAWSSDK.html>

CertyIQ

Question: 24

A company wants to deploy and maintain static websites on AWS. Each website's source code is hosted in one of several version control systems, including AWS CodeCommit, Bitbucket, and GitHub.

The company wants to implement phased releases by using development, staging, user acceptance testing, and production environments in the AWS Cloud. Deployments to each environment must be started by code merges on the relevant Git branch. The company wants to use HTTPS for all data exchange. The company needs a solution that does not require servers to run continuously.

Which solution will meet these requirements with the LEAST operational overhead?

- A.Host each website by using AWS Amplify with a serverless backend. Connect the repository branches that correspond to each of the desired environments. Start deployments by merging code changes to a desired branch.
- B.Host each website in AWS Elastic Beanstalk with multiple environments. Use the EB CLI to link each repository branch. Integrate AWS CodePipeline to automate deployments from version control code merges.
- C.Host each website in different Amazon S3 buckets for each environment. Configure AWS CodePipeline to pull source code from version control. Add an AWS CodeBuild stage to copy source code to Amazon S3.
- D.Host each website on its own Amazon EC2 instance. Write a custom deployment script to bundle each website's static assets. Copy the assets to Amazon EC2. Set up a workflow to run the script when code is merged.

Answer: A

Explanation:

The correct answer is A.AWS Amplify is an all in one service for the requirement. Option C is almost correct, but it does not mention how to implement HTTPS. Option B and D are wrong. They need to keep running servers.

Reference:

<https://docs.aws.amazon.com/amplify/latest/userguide/welcome.html>

CertyIQ

Question: 25

A company is migrating an on-premises database to Amazon RDS for MySQL. The company has read-heavy workloads. The company wants to refactor the code to achieve optimum read performance for queries. Which solution will meet this requirement with LEAST current and future effort?

- A.Use a multi-AZ Amazon RDS deployment. Increase the number of connections that the code makes to the database or increase the connection pool size if a connection pool is in use.
- B.Use a multi-AZ Amazon RDS deployment. Modify the code so that queries access the secondary RDS instance.
- C.Deploy Amazon RDS with one or more read replicas. Modify the application code so that queries use the URL for the read replicas.
- D.Use open source replication software to create a copy of the MySQL database on an Amazon EC2 instance. Modify the application code so that queries use the IP address of the EC2 instance.

Answer: C

Explanation:

Read heavy access need read replicas as the right solution.

Keyword: heavy read

CertyIQ

Question: 26

A developer is creating an application that will be deployed on IoT devices. The application will send data to a RESTful API that is deployed as an AWS Lambda function. The application will assign each API request a unique identifier. The volume of API requests from the application can randomly increase at any given time of day. During periods of request throttling, the application might need to retry requests. The API must be able to handle duplicate requests without inconsistencies or data loss.
Which solution will meet these requirements?

- A.Create an Amazon RDS for MySQL DB instance. Store the unique identifier for each request in a database table. Modify the Lambda function to check the table for the identifier before processing the request.
- B.Create an Amazon DynamoDB table. Store the unique identifier for each request in the table. Modify the Lambda function to check the table for the identifier before processing the request.
- C.Create an Amazon DynamoDB table. Store the unique identifier for each request in the table. Modify the Lambda function to return a client error response when the function receives a duplicate request.
- D.Create an Amazon ElastiCache for Memcached instance. Store the unique identifier for each request in the cache. Modify the Lambda function to check the cache for the identifier before processing the request.

Answer: B

Explanation:

B The resolution is to make the Lambda function idempotent.<https://repost.aws/knowledge-center/lambda-function-idempotent><https://aws.amazon.com/builders-library/making-retries-safe-with-idempotent-APIs/>

CertyIQ

Question: 27

A developer wants to expand an application to run in multiple AWS Regions. The developer wants to copy Amazon Machine Images (AMIs) with the latest changes and create a new application stack in the destination Region. According to company requirements, all AMIs must be encrypted in all Regions. However, not all the AMIs that the company uses are encrypted.
How can the developer expand the application to run in the destination Region while meeting the encryption requirement?

- A.Create new AMIs, and specify encryption parameters. Copy the encrypted AMIs to the destination Region. Delete the unencrypted AMIs.
- B.Use AWS Key Management Service (AWS KMS) to enable encryption on the unencrypted AMIs. Copy the encrypted AMIs to the destination Region.

C.Use AWS Certificate Manager (ACM) to enable encryption on the unencrypted AMIs. Copy the encrypted AMIs to the destination Region.

D.Copy the unencrypted AMIs to the destination Region. Enable encryption by default in the destination Region.

Answer: A

Explanation:

It's A. Option D is also correct, but in this case, your source AMI stay unencrypted. Options B and C - are incorrect, you can't just encrypt existing unencrypted AMI or create encrypted AMI from unencrypted EC2.

we can use kms to encrypt ami and use in multiple regions. but you cannot direct applying kms encryption on non encrypted AMI. Answer B is wrong.

CertyIQ

Question: 28

A company hosts a client-side web application for one of its subsidiaries on Amazon S3. The web application can be accessed through Amazon CloudFront from <https://www.example.com>. After a successful rollout, the company wants to host three more client-side web applications for its remaining subsidiaries on three separate S3 buckets. To achieve this goal, a developer moves all the common JavaScript files and web fonts to a central S3 bucket that serves the web applications. However, during testing, the developer notices that the browser blocks the JavaScript files and web fonts.

What should the developer do to prevent the browser from blocking the JavaScript files and web fonts?

- A.Create four access points that allow access to the central S3 bucket. Assign an access point to each web application bucket.
- B.Create a bucket policy that allows access to the central S3 bucket. Attach the bucket policy to the central S3 bucket
- C.Create a cross-origin resource sharing (CORS) configuration that allows access to the central S3 bucket. Add the CORS configuration to the central S3 bucket.
- D.Create a Content-MD5 header that provides a message integrity check for the central S3 bucket. Insert the Content-MD5 header for each web application request.

Answer: C

Explanation:

C This is a frequent trouble. Web applications cannot access the resources in other domains by default, except some exceptions. You must configure CORS on the resources to be accessed.

Reference:

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

CertyIQ

Question: 29

An application is processing clickstream data using Amazon Kinesis. The clickstream data feed into Kinesis experiences periodic spikes. The PutRecords API call occasionally fails and the logs show that the failed call returns the response shown below:

```

{
  "FailedRecordCount": 1,
  "Records": [
    {
      "SequenceNumber": "21269319989900637946712965403778482371",
      "ShardId": "shardId-000000000001"
    },
    {
      "ErrorCode": "ProvisionedThroughputExceededException",
      "ErrorMessage": "Rate exceeded for shard shardId-000000000001 in
                      stream exampleStreamName under account 123456789."
    },
    {
      "SequenceNumber": "21269319989999637946712965403778482985",
      "ShardId": "shardId-000000000002"
    }
  ]
}

```

Which techniques will help mitigate this exception? (Choose two.)

- A.Implement retries with exponential backoff.
- B.Use a PutRecord API instead of PutRecords.
- C.Reduce the frequency and/or size of the requests.
- D.Use Amazon SNS instead of Kinesis.
- E.Reduce the number of KCL consumers.

Answer: AC

Explanation:

AC as per AWS : Provisioned Throughput Exceeded Exception The request rate for the stream is too high, or the requested data is too large for the available throughput. Reduce the frequency or size of your requests. For more information, see Streams Limits in the Amazon Kinesis Data Streams Developer Guide, and Error Retries and Exponential Back off in AWS in the AWS General Reference.

https://docs.aws.amazon.com/kinesis/latest/APIReference/API_PutRecords.html

Question: 30

CertyIQ

A company has an application that uses Amazon Cognito user pools as an identity provider. The company must secure access to user records. The company has set up multi-factor authentication (MFA). The company also wants to send a login activity notification by email every time a user logs in.

What is the MOST operationally efficient solution that meets this requirement?

- A.Create an AWS Lambda function that uses Amazon Simple Email Service (Amazon SES) to send the email notification. Add an Amazon API Gateway API to invoke the function. Call the API from the client side when login confirmation is received.
- B.Create an AWS Lambda function that uses Amazon Simple Email Service (Amazon SES) to send the email notification. Add an Amazon Cognito post authentication Lambda trigger for the function.
- C.Create an AWS Lambda function that uses Amazon Simple Email Service (Amazon SES) to send the email notification. Create an Amazon CloudWatch Logs log subscription filter to invoke the function based on the

login status.

D.Configure Amazon Cognito to stream all logs to Amazon Kinesis Data Firehose. Create an AWS Lambda function to process the streamed logs and to send the email notification based on the login status of each user.

Answer: B

Explanation:

B. Create an AWS Lambda function that uses Amazon Simple Email Service (Amazon SES) to send the email notification. Add an Amazon Cognito post authentication Lambda trigger for the function. The most operationally efficient solution for sending login activity notifications by email for Amazon Cognito user pools is to use a Lambda trigger that is automatically invoked by Amazon Cognito every time a user logs in. This eliminates the need for client-side calls to an API or log subscription filter. A Lambda function can be used to send email notifications using Amazon SES. Option B satisfies these requirements and is the most operationally efficient solution.

Reference:

<https://docs.aws.amazon.com/cognito/latest/developerguide/user-pool-lambda-post-authentication.html>

CertyIQ

Question: 31

A developer has an application that stores data in an Amazon S3 bucket. The application uses an HTTP API to store and retrieve objects. When the PutObject API operation adds objects to the S3 bucket the developer must encrypt these objects at rest by using server-side encryption with Amazon S3 managed keys (SSE-S3).

Which solution will meet this requirement?

- A.Create an AWS Key Management Service (AWS KMS) key. Assign the KMS key to the S3 bucket.
- B.Set the x-amz-server-side-encryption header when invoking the PutObject API operation.
- C.Provide the encryption key in the HTTP header of every request.
- D.Apply TLS to encrypt the traffic to the S3 bucket.

Answer: B

Explanation:

B. Set the x-amz-server-side-encryption header when invoking the Put Object API operation. When using the Put Object API operation to store objects in an S3 bucket, the x- amz-server-side-encryption header can be set to specify the server-side encryption algorithm used to encrypt the object. Setting this header to "AES256" or "aws: kms" enables server-side encryption with SSE-S3 or SSE-KMS respectively. Option A is incorrect because assigning a KMS key to the S3 bucket will not enable SSE-S3 encryption. Option C is incorrect because providing the encryption key in the HTTP header of every request is not a valid way to enable SSE-S3 encryption. Option D is incorrect because applying TLS encryption to the traffic to the S3 bucket only encrypts the data in transit, but does not encrypt the objects at rest in the bucket.

CertyIQ

Question: 32

A developer needs to perform geographic load testing of an API. The developer must deploy resources to multiple AWS Regions to support the load testing of the API.

How can the developer meet these requirements without additional application code?

- A.Create and deploy an AWS Lambda function in each desired Region. Configure the Lambda function to create a stack from an AWS CloudFormation template in that Region when the function is invoked.

- B.Create an AWS CloudFormation template that defines the load test resources. Use the AWS CLI create-stack-set command to create a stack set in the desired Regions.
- C.Create an AWS Systems Manager document that defines the resources. Use the document to create the resources in the desired Regions.
- D.Create an AWS CloudFormation template that defines the load test resources. Use the AWS CLI deploy command to create a stack from the template in each Region.

Answer: B

Explanation:

B. Create an AWS Cloud Formation template that defines the load test resources. Use the AWS CLI create-stack-set command to create a stack set in the desired Regions. AWS Cloud Formation Stack Sets allow developers to deploy Cloud Formation stacks across multiple AWS accounts and regions with a single Cloud Formation template. By using the AWS CLI create-stack-set command, the developer can deploy the same Cloud Formation stack to multiple regions without additional application code, thereby meeting the requirement for geographic load testing of an API.

Reference:

<https://aws.amazon.com/ru/about-aws/whats-new/2021/04/deploy-cloudformation-stacks-concurrently-across-multiple-aws-regions-using-aws-cloudformation-stacksets/>

CertyIQ

A developer is creating an application that includes an Amazon API Gateway REST API in the us-east-2 Region. The developer wants to use Amazon CloudFront and a custom domain name for the API. The developer has acquired an SSL/TLS certificate for the domain from a third-party provider.

How should the developer configure the custom domain for the application?

- A.Import the SSL/TLS certificate into AWS Certificate Manager (ACM) in the same Region as the API. Create a DNS A record for the custom domain.
- B.Import the SSL/TLS certificate into CloudFront. Create a DNS CNAME record for the custom domain.
- C.Import the SSL/TLS certificate into AWS Certificate Manager (ACM) in the same Region as the API. Create a DNS CNAME record for the custom domain.
- D.Import the SSL/TLS certificate into AWS Certificate Manager (ACM) in the us-east-1 Region. Create a DNS CNAME record for the custom domain.

Answer: D

Explanation:

To use a certificate in AWS Certificate Manager (ACM) to require HTTPS between viewers and Cloud Front, make sure you request (or import) the certificate in the US East (N. Virginia) Region (us-east-1).
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html>

The correct answer is D.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html>

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

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/CNAMEs.html>

Question: 34

CertyIQ

A developer is creating a template that uses AWS CloudFormation to deploy an application. The application is serverless and uses Amazon API Gateway, Amazon DynamoDB, and AWS Lambda. Which AWS service or tool should the developer use to define serverless resources in YAML?

- A.CloudFormation serverless intrinsic functions
- B.AWS Elastic Beanstalk
- C.AWS Serverless Application Model (AWS SAM)
- D.AWS Cloud Development Kit (AWS CDK)

Answer: C**Explanation:**

AWS Serverless Application Model (AWS SAM)

Question: 35

CertyIQ

A developer wants to insert a record into an Amazon DynamoDB table as soon as a new file is added to an Amazon S3 bucket.

Which set of steps would be necessary to achieve this?

- A.Create an event with Amazon EventBridge that will monitor the S3 bucket and then insert the records into DynamoDB.
- B.Configure an S3 event to invoke an AWS Lambda function that inserts records into DynamoDB.
- C.Create an AWS Lambda function that will poll the S3 bucket and then insert the records into DynamoDB.
- D.Create a cron job that will run at a scheduled time and insert the records into DynamoDB.

Answer: B**Explanation:**

The correct answer is B .To insert a record into DynamoDB as soon as a new file is added to an S3 bucket, you can configure an S3 event notification to invoke an AWS Lambda function that inserts the records into DynamoDB. When a new file is added to the S3 bucket, the S3 event notification will trigger the Lambda function, which will insert the record into the DynamoDB table. Option A is incorrect because Amazon Event Bridge is not necessary to achieve this. S3 event notifications can directly invoke a Lambda function to insert records into DynamoDB. Option C is incorrect because polling the S3 bucket periodically to check for new files is inefficient and not necessary with S3 event notifications. Option D is incorrect because running a cron job at a scheduled time is not real-time and would not insert the record into DynamoDB as soon as a new file is added to the S3 bucket.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/NotificationHowTo.html>

Question: 36

CertyIQ

A development team maintains a web application by using a single AWS CloudFormation template. The template defines web servers and an Amazon RDS database. The team uses the Cloud Formation template to deploy the

Cloud Formation stack to different environments.

During a recent application deployment, a developer caused the primary development database to be dropped and recreated. The result of this incident was a loss of data. The team needs to avoid accidental database deletion in the future.

Which solutions will meet these requirements? (Choose two.)

- A.Add a CloudFormation Deletion Policy attribute with the Retain value to the database resource.
- B.Update the CloudFormation stack policy to prevent updates to the database.
- C.Modify the database to use a Multi-AZ deployment.
- D.Create a CloudFormation stack set for the web application and database deployments.
- E.Add a Cloud Formation DeletionPolicy attribute with the Retain value to the stack.

Answer: AB

Explanation:

AB<https://aws.amazon.com/ru/premiumsupport/knowledge-center/cloudformation-accidental-updates/>

Question: 37

CertyIQ

A company has an Amazon S3 bucket that contains sensitive data. The data must be encrypted in transit and at rest. The company encrypts the data in the S3 bucket by using an AWS Key Management Service (AWS KMS) key. A developer needs to grant several other AWS accounts the permission to use the S3 GetObject operation to retrieve the data from the S3 bucket.

How can the developer enforce that all requests to retrieve the data provide encryption in transit?

- A.Define a resource-based policy on the S3 bucket to deny access when a request meets the condition "aws:SecureTransport": "false".
- B.Define a resource-based policy on the S3 bucket to allow access when a request meets the condition "aws:SecureTransport": "false".
- C.Define a role-based policy on the other accounts' roles to deny access when a request meets the condition of "aws:SecureTransport": "false".
- D.Define a resource-based policy on the KMS key to deny access when a request meets the condition of "aws:SecureTransport": "false".

Answer: A

Explanation:

Reference:

<https://repost.aws/knowledge-center/s3-bucket-policy-for-config-rule>

Question: 38

CertyIQ

An application that is hosted on an Amazon EC2 instance needs access to files that are stored in an Amazon S3 bucket. The application lists the objects that are stored in the S3 bucket and displays a table to the user. During testing, a developer discovers that the application does not show any objects in the list.

What is the MOST secure way to resolve this issue?

- A.Update the IAM instance profile that is attached to the EC2 instance to include the S3:* permission for the S3 bucket.
- B.Update the IAM instance profile that is attached to the EC2 instance to include the S3>ListBucket permission for the S3 bucket.

- C.Update the developer's user permissions to include the S3>ListBucket permission for the S3 bucket.
- D.Update the S3 bucket policy by including the S3>ListBucket permission and by setting the Principal element to specify the account number of the EC2 instance.

Answer: B

Explanation:

The s3>ListBucket permission allows the user to use the Amazon S3 GET Bucket (List Objects) operation.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-policy-language-overview.html>

Question: 39

CertyIQ

A company is planning to securely manage one-time fixed license keys in AWS. The company's development team needs to access the license keys in automation scripts that run in Amazon EC2 instances and in AWS CloudFormation stacks.

Which solution will meet these requirements MOST cost-effectively?

- A.Amazon S3 with encrypted files prefixed with "config"
- B.AWS Secrets Manager secrets with a tag that is named SecretString
- C.AWS Systems Manager Parameter Store SecureString parameters
- D.CloudFormation NoEcho parameters

Answer: C

Explanation:

AWS Systems Manager Parameter Store Secure String parameters.

Reference:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-parameter-store.html>

Question: 40

CertyIQ

A company has deployed infrastructure on AWS. A development team wants to create an AWS Lambda function that will retrieve data from an Amazon Aurora database. The Amazon Aurora database is in a private subnet in company's VPC. The VPC is named VPC1. The data is relational in nature. The Lambda function needs to access the data securely.

Which solution will meet these requirements?

- A.Create the Lambda function. Configure VPC1 access for the function. Attach a security group named SG1 to both the Lambda function and the database. Configure the security group inbound and outbound rules to allow TCP traffic on Port 3306.
- B.Create and launch a Lambda function in a new public subnet that is in a new VPC named VPC2. Create a peering connection between VPC1 and VPC2.
- C.Create the Lambda function. Configure VPC1 access for the function. Assign a security group named SG1 to the Lambda function. Assign a second security group named SG2 to the database. Add an inbound rule to SG1 to allow TCP traffic from Port 3306.
- D.Export the data from the Aurora database to Amazon S3. Create and launch a Lambda function in VPC1. Configure the Lambda function query the data from Amazon S3.

Answer: A

Explanation:

Correct Answer is Answer A For B creating new VPC for lambda does not seems a suitable solution For C Assigning different security groups to both will not work Option D will not be suitable for relational data and involve S3 in solution

Reference:

<https://repost.aws/knowledge-center/s3-bucket-policy-for-config-rule>

CertyIQ

Question: 41

A developer is building a web application that uses Amazon API Gateway to expose an AWS Lambda function to process requests from clients. During testing, the developer notices that the API Gateway times out even though the Lambda function finishes under the set time limit.

Which of the following API Gateway metrics in Amazon CloudWatch can help the developer troubleshoot the issue? (Choose two.)

- A.CacheHitCount
- B.IntegrationLatency
- C.CacheMissCount
- D.Latency
- E.Count

Answer: BD

Explanation:

- B. Integration Latency
- D. Latency

Reference:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/monitoring-cloudwatch.html>

CertyIQ

Question: 42

A development team wants to build a continuous integration/continuous delivery (CI/CD) pipeline. The team is using AWS CodePipeline to automate the code build and deployment. The team wants to store the program code to prepare for the CI/CD pipeline.

Which AWS service should the team use to store the program code?

- A.AWS CodeDeploy
- B.AWS CodeArtifact
- C.AWS CodeCommit
- D.Amazon CodeGuru

Answer: C

Explanation:

Reference:

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

CertyIQ

Question: 43

A developer is designing an AWS Lambda function that creates temporary files that are less than 10 MB during invocation. The temporary files will be accessed and modified multiple times during invocation. The developer has no need to save or retrieve these files in the future.

Where should the temporary files be stored?

- A.the /tmp directory
- B.Amazon Elastic File System (Amazon EFS)
- C.Amazon Elastic Block Store (Amazon EBS)
- D.Amazon S3

Answer: A

Explanation:

A Lambda function has access to local storage in the /tmp directory. Each execution environment provides between 512 MB and 10,240 MB, in 1-MB increments, of disk space in the /tmp directory.

<https://docs.aws.amazon.com/lambda/latest/dg/foundation-progmodel.html>

CertyIQ

Question: 44

A developer is designing a serverless application with two AWS Lambda functions to process photos. One Lambda function stores objects in an Amazon S3 bucket and stores the associated metadata in an Amazon DynamoDB table. The other Lambda function fetches the objects from the S3 bucket by using the metadata from the DynamoDB table. Both Lambda functions use the same Python library to perform complex computations and are approaching the quota for the maximum size of zipped deployment packages.

What should the developer do to reduce the size of the Lambda deployment packages with the LEAST operational overhead?

- A.Package each Python library in its own .zip file archive. Deploy each Lambda function with its own copy of the library.
- B.Create a Lambda layer with the required Python library. Use the Lambda layer in both Lambda functions.
- C.Combine the two Lambda functions into one Lambda function. Deploy the Lambda function as a single .zip file archive.
- D.Download the Python library to an S3 bucket. Program the Lambda functions to reference the object URLs.

Answer: B

Explanation:

Create a Lambda layer with the required Python library. Use the Lambda layer in both Lambda functions.

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/invocation-layers.html>

Question: 45

A developer is writing an AWS Lambda function. The developer wants to log key events that occur while the Lambda function runs. The developer wants to include a unique identifier to associate the events with a specific function invocation. The developer adds the following code to the Lambda function:

```
function handler(event, context) {  
}  
}
```

Which solution will meet this requirement?

- A.Obtain the request identifier from the AWS request ID field in the context object. Configure the application to write logs to standard output.
- B.Obtain the request identifier from the AWS request ID field in the event object. Configure the application to write logs to a file.
- C.Obtain the request identifier from the AWS request ID field in the event object. Configure the application to write logs to standard output.
- D.Obtain the request identifier from the AWS request ID field in the context object. Configure the application to write logs to a file.

Answer: A**Explanation:**

[Ahttps://docs.aws.amazon.com/lambda/latest/dg/nodejs-context.html](https://docs.aws.amazon.com/lambda/latest/dg/nodejs-context.html)
<https://docs.aws.amazon.com/lambda/latest/dg/nodejs-logging.html>There is no explicit information for the runtime, the code is written in Node.js.

Both A and D could work here, as both rely on the context object to get access to execution ID
https://docs.aws.amazon.com/us_en/lambda/latest/dg/python-context.html While A uses stoud to send log to Cloud Watch Log, D writes to a file. D is less specific (where is the file stored? A single file for each execution?) and looks more complex (manage file(s), manage concurrency access to the file .), thus I'll go for A

Question: 46

A developer is working on a serverless application that needs to process any changes to an Amazon DynamoDB table with an AWS Lambda function.

How should the developer configure the Lambda function to detect changes to the DynamoDB table?

- A.Create an Amazon Kinesis data stream, and attach it to the DynamoDB table. Create a trigger to connect the data stream to the Lambda function.
- B.Create an Amazon EventBridge rule to invoke the Lambda function on a regular schedule. Conned to the DynamoDB table from the Lambda function to detect changes.
- C.Enable DynamoDB Streams on the table. Create a trigger to connect the DynamoDB stream to the Lambda function.
- D.Create an Amazon Kinesis Data Firehose delivery stream, and attach it to the DynamoDB table. Configure the delivery stream destination as the Lambda function.

Answer: C**Explanation:**

Enable DynamoDB Streams on the table. Create a trigger to connect the DynamoDB stream to the Lambda

function.

Reference:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.html>

Question: 47

CertyIQ

An application uses an Amazon EC2 Auto Scaling group. A developer notices that EC2 instances are taking a long time to become available during scale-out events. The User Data script is taking a long time to run.

The developer must implement a solution to decrease the time that elapses before an EC2 instance becomes available. The solution must make the most recent version of the application available at all times and must apply all available security updates. The solution also must minimize the number of images that are created. The images must be validated.

Which combination of steps should the developer take to meet these requirements? (Choose two.)

- A. Use EC2 Image Builder to create an Amazon Machine Image (AMI). Install all the patches and agents that are needed to manage and run the application. Update the Auto Scaling group launch configuration to use the AMI.
- B. Use EC2 Image Builder to create an Amazon Machine Image (AMI). Install the latest version of the application and all the patches and agents that are needed to manage and run the application. Update the Auto Scaling group launch configuration to use the AMI.
- C. Set up AWS CodeDeploy to deploy the most recent version of the application at runtime.
- D. Set up AWS CodePipeline to deploy the most recent version of the application at runtime.
- E. Remove any commands that perform operating system patching from the User Data script.

Answer: AE

Explanation:

Problem is that B will tie an AMI with a specific version, so if there is a new version, we need to create a new AMI, and that contradicts with "minimize the number of images that are created". Then E over C, D? E is obviously complementary to A, where removing commands from User Data will make the instance booting process much faster (and of course with A you don't need that anymore). C and D also works but 1/not complementary with any other options; 2/Code Deploy takes time to execute. Hope this helps somebody struggling with this question.

AE Not AC because app deployment from User Data is nonsense. Therefore, you don't need to change anything about deployment

Question: 48

CertyIQ

A developer is creating an AWS Lambda function that needs credentials to connect to an Amazon RDS for MySQL database. An Amazon S3 bucket currently stores the credentials. The developer needs to improve the existing solution by implementing credential rotation and secure storage. The developer also needs to provide integration with the Lambda function.

Which solution should the developer use to store and retrieve the credentials with the LEAST management overhead?

- A. Store the credentials in AWS Systems Manager Parameter Store. Select the database that the parameter will access. Use the default AWS Key Management Service (AWS KMS) key to encrypt the parameter. Enable automatic rotation for the parameter. Use the parameter from Parameter Store on the Lambda function to connect to the database.
- B. Encrypt the credentials with the default AWS Key Management Service (AWS KMS) key. Store the credentials as environment variables for the Lambda function. Create a second Lambda function to generate new credentials and to rotate the credentials by updating the environment variables of the first Lambda

function. Invoke the second Lambda function by using an Amazon EventBridge rule that runs on a schedule. Update the database to use the new credentials. On the first Lambda function, retrieve the credentials from the environment variables. Decrypt the credentials by using AWS KMS, Connect to the database.

C.Store the credentials in AWS Secrets Manager. Set the secret type to Credentials for Amazon RDS database. Select the database that the secret will access. Use the default AWS Key Management Service (AWS KMS) key to encrypt the secret. Enable automatic rotation for the secret. Use the secret from Secrets Manager on the Lambda function to connect to the database.

D.Encrypt the credentials by using AWS Key Management Service (AWS KMS). Store the credentials in an Amazon DynamoDB table. Create a second Lambda function to rotate the credentials. Invoke the second Lambda function by using an Amazon EventBridge rule that runs on a schedule. Update the DynamoDB table. Update the database to use the generated credentials. Retrieve the credentials from DynamoDB with the first Lambda function. Connect to the database.

Answer: C

Explanation:

Reference:

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

https://docs.aws.amazon.com/secretsmanager/latest/userguide/retrieving-secrets_lambda.html

CertyIQ

Question: 49

A developer has written the following IAM policy to provide access to an Amazon S3 bucket:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/secrets*"
        }
    ]
}
```

Which access does the policy allow regarding the s3:GetObject and s3:PutObject actions?

- A.Access on all buckets except the “DOC-EXAMPLE-BUCKET” bucket
- B.Access on all buckets that start with “DOC-EXAMPLE-BUCKET” except the “DOC-EXAMPLE-BUCKET/secrets” bucket

C.Access on all objects in the “DOC-EXAMPLE-BUCKET” bucket along with access to all S3 actions for objects in the “DOC-EXAMPLE-BUCKET” bucket that start with “secrets”

D.Access on all objects in the “DOC-EXAMPLE-BUCKET” bucket except on objects that start with “secrets”

Answer: D

Explanation:

Access on all objects in the “DOC-EXAMPLE-BUCKET” bucket except on objects that start with “secrets”

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/using-with-s3-actions.html>

CertyIQ

Question: 50

A developer is creating a mobile app that calls a backend service by using an Amazon API Gateway REST API. For integration testing during the development phase, the developer wants to simulate different backend responses without invoking the backend service.

Which solution will meet these requirements with the LEAST operational overhead?

A.Create an AWS Lambda function. Use API Gateway proxy integration to return constant HTTP responses.

B.Create an Amazon EC2 instance that serves the backend REST API by using an AWS CloudFormation template.

C.Customize the API Gateway stage to select a response type based on the request.

D.Use a request mapping template to select the mock integration response.

Answer: D

Explanation:

[Dhttps://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-mock-integration.html](https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-mock-integration.html)

D as per doc <https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-mock-integration.html> Wording confused me a bit, with mapping template you do not "select" a response, instead you actually craft it in this case

CertyIQ

Question: 51

A developer has a legacy application that is hosted on-premises. Other applications hosted on AWS depend on the on-premises application for proper functioning. In case of any application errors, the developer wants to be able to use Amazon CloudWatch to monitor and troubleshoot all applications from one place.

How can the developer accomplish this?

A.Install an AWS SDK on the on-premises server to automatically send logs to CloudWatch.

B.Download the CloudWatch agent to the on-premises server. Configure the agent to use IAM user credentials with permissions for CloudWatch.

C.Upload log files from the on-premises server to Amazon S3 and have CloudWatch read the files.

D.Upload log files from the on-premises server to an Amazon EC2 instance and have the instance forward the logs to CloudWatch.

Answer: B

Explanation:

Download the Cloud Watch agent to the on-premises server. Configure the agent to use IAM user credentials with permissions for Cloud Watch.

Reference:

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

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-on-premise.html>

Question: 52

CertyIQ

An Amazon Kinesis Data Firehose delivery stream is receiving customer data that contains personally identifiable information. A developer needs to remove pattern-based customer identifiers from the data and store the modified data in an Amazon S3 bucket.

What should the developer do to meet these requirements?

- A.Implement Kinesis Data Firehose data transformation as an AWS Lambda function. Configure the function to remove the customer identifiers. Set an Amazon S3 bucket as the destination of the delivery stream.
- B.Launch an Amazon EC2 instance. Set the EC2 instance as the destination of the delivery stream. Run an application on the EC2 instance to remove the customer identifiers. Store the transformed data in an Amazon S3 bucket.
- C.Create an Amazon OpenSearch Service instance. Set the OpenSearch Service instance as the destination of the delivery stream. Use search and replace to remove the customer identifiers. Export the data to an Amazon S3 bucket.
- D.Create an AWS Step Functions workflow to remove the customer identifiers. As the last step in the workflow, store the transformed data in an Amazon S3 bucket. Set the workflow as the destination of the delivery stream.

Answer: A

Explanation:

Implement Kinesis Data Firehose data transformation as an AWS Lambda function. Configure the function to remove the customer identifiers. Set an Amazon S3 bucket as the destination of the delivery stream.

Reference:

<https://docs.aws.amazon.com/firehose/latest/dev/data-transformation.html>

Question: 53

CertyIQ

A developer is using an AWS Lambda function to generate avatars for profile pictures that are uploaded to an Amazon S3 bucket. The Lambda function is automatically invoked for profile pictures that are saved under the /original/ S3 prefix. The developer notices that some pictures cause the Lambda function to time out. The developer wants to implement a fallback mechanism by using another Lambda function that resizes the profile picture.

Which solution will meet these requirements with the LEAST development effort?

- A.Set the image resize Lambda function as a destination of the avatar generator Lambda function for the events that fail processing.
- B.Create an Amazon Simple Queue Service (Amazon SQS) queue. Set the SQS queue as a destination with an on failure condition for the avatar generator Lambda function. Configure the image resize Lambda function to poll from the SQS queue.
- C.Create an AWS Step Functions state machine that invokes the avatar generator Lambda function and uses the image resize Lambda function as a fallback. Create an Amazon EventBridge rule that matches events from the S3 bucket to invoke the state machine.

D.Create an Amazon Simple Notification Service (Amazon SNS) topic. Set the SNS topic as a destination with an on failure condition for the avatar generator Lambda function. Subscribe the image resize Lambda function to the SNS topic.

Answer: A

Explanation:

Previously, you needed to write the SQS/SNS/Event Bridge handling code within your Lambda function and manage retries and failures yourself .With Destinations, you can route asynchronous function results as an execution record to a destination resource without writing additional code.

<https://aws.amazon.com/ru/blogs/compute/introducing-aws-lambda-destinations/>

CertyIQ

A developer needs to migrate an online retail application to AWS to handle an anticipated increase in traffic. The application currently runs on two servers: one server for the web application and another server for the database. The web server renders webpages and manages session state in memory. The database server hosts a MySQL database that contains order details. When traffic to the application is heavy, the memory usage for the web server approaches 100% and the application slows down considerably.

The developer has found that most of the memory increase and performance decrease is related to the load of managing additional user sessions. For the web server migration, the developer will use Amazon EC2 instances with an Auto Scaling group behind an Application Load Balancer.

Which additional set of changes should the developer make to the application to improve the application's performance?

- A.Use an EC2 instance to host the MySQL database. Store the session data and the application data in the MySQL database.
- B.Use Amazon ElastiCache for Memcached to store and manage the session data. Use an Amazon RDS for MySQL DB instance to store the application data.
- C.Use Amazon ElastiCache for Memcached to store and manage the session data and the application data.
- D.Use the EC2 instance store to manage the session data. Use an Amazon RDS for MySQL DB instance to store the application data.

Answer: B

Explanation:

B Session stores are easy to create with Amazon Elastic Cache for Memcached.

<https://aws.amazon.com/elasticache/memcached/> With Amazon RDS, you can deploy scalable MySQL servers in minutes with cost-efficient and resizable hardware capacity.<https://aws.amazon.com/rds/mysql/>

CertyIQ

Question: 55

An application uses Lambda functions to extract metadata from files uploaded to an S3 bucket; the metadata is stored in Amazon DynamoDB. The application starts behaving unexpectedly, and the developer wants to examine the logs of the Lambda function code for errors.

Based on this system configuration, where would the developer find the logs?

- A.Amazon S3
- B.AWS CloudTrail
- C.Amazon CloudWatch

Answer: C**Explanation:**

Correct answer is C:Amazon Cloud Watch.

Reference:

<https://docs.aws.amazon.com/prescriptive-guidance/latest/implementing-logging-monitoring-cloudwatch/lambda-logging-metrics.html>

CertyIQ**Question: 56**

A company is using an AWS Lambda function to process records from an Amazon Kinesis data stream. The company recently observed slow processing of the records. A developer notices that the iterator age metric for the function is increasing and that the Lambda run duration is constantly above normal. Which actions should the developer take to increase the processing speed? (Choose two.)

- A.Increase the number of shards of the Kinesis data stream.
- B.Decrease the timeout of the Lambda function.
- C.Increase the memory that is allocated to the Lambda function.
- D.Decrease the number of shards of the Kinesis data stream.
- E.Increase the timeout of the Lambda function.

Answer: AC**Explanation:**

- A. Increase the number of shards of the Kinesis data stream.
- C. Increase the memory that is allocated to the Lambda function.

Reference:

<https://repost.aws/knowledge-center/lambda-iterator-age>

CertyIQ**Question: 57**

A company needs to harden its container images before the images are in a running state. The company's application uses Amazon Elastic Container Registry (Amazon ECR) as an image registry. Amazon Elastic Kubernetes Service (Amazon EKS) for compute, and an AWS CodePipeline pipeline that orchestrates a continuous integration and continuous delivery (CI/CD) workflow.

Dynamic application security testing occurs in the final stage of the pipeline after a new image is deployed to a development namespace in the EKS cluster. A developer needs to place an analysis stage before this deployment to analyze the container image earlier in the CI/CD pipeline.

Which solution will meet these requirements with the MOST operational efficiency?

- A.Build the container image and run the docker scan command locally. Mitigate any findings before pushing changes to the source code repository. Write a pre-commit hook that enforces the use of this workflow before commit.
- B.Create a new CodePipeline stage that occurs after the container image is built. Configure ECR basic image scanning to scan on image push. Use an AWS Lambda function as the action provider. Configure the Lambda function to check the scan results and to fail the pipeline if there are findings.

C.Create a new CodePipeline stage that occurs after source code has been retrieved from its repository. Run a security scanner on the latest revision of the source code. Fail the pipeline if there are findings.

D.Add an action to the deployment stage of the pipeline so that the action occurs before the deployment to the EKS cluster. Configure ECR basic image scanning to scan on image push. Use an AWS Lambda function as the action provider. Configure the Lambda function to check the scan results and to fail the pipeline if there are findings.

Answer: B

Explanation:

The below blog post refers to the solution using Amazon Inspector and ECS, but the architecture is almost same as required in this scenario. The built in image scanning in Amazon ECR provides a simpler solution.<https://aws.amazon.com/blogs/security/use-amazon-inspector-to-manage-your-build-and-deploy-pipelines-for-containerized-applications/>

This approach integrates security scanning directly into the CI/CD pipeline and leverages AWS services for image scanning. Here's how it works: A new Code Pipeline stage is added after the container image is built, but before it's pushed to Amazon ECR. ECR basic image scanning is configured to scan the image automatically upon push. This ensures that security scanning is part of the process. An AWS Lambda function is used as an action provider in the pipeline. This Lambda function can be configured to analyse the scan results of the image. If the Lambda function detects any security findings in the scan results, it can fail the pipeline, preventing the deployment of images with security vulnerabilities.

Reference:

<https://docs.aws.amazon.com/AmazonECR/latest/userguide/image-scanning-basic.html>

Question: 58

CertyIQ

A developer is testing a new file storage application that uses an Amazon CloudFront distribution to serve content from an Amazon S3 bucket. The distribution accesses the S3 bucket by using an origin access identity (OAI). The S3 bucket's permissions explicitly deny access to all other users.

The application prompts users to authenticate on a login page and then uses signed cookies to allow users to access their personal storage directories. The developer has configured the distribution to use its default cache behavior with restricted viewer access and has set the origin to point to the S3 bucket. However, when the developer tries to navigate to the login page, the developer receives a 403 Forbidden error.

The developer needs to implement a solution to allow unauthenticated access to the login page. The solution also must keep all private content secure.

Which solution will meet these requirements?

A.Add a second cache behavior to the distribution with the same origin as the default cache behavior. Set the path pattern for the second cache behavior to the path of the login page, and make viewer access unrestricted. Keep the default cache behavior's settings unchanged.

B.Add a second cache behavior to the distribution with the same origin as the default cache behavior. Set the path pattern for the second cache behavior to *, and make viewer access restricted. Change the default cache behavior's path pattern to the path of the login page, and make viewer access unrestricted.

C.Add a second origin as a failover origin to the default cache behavior. Point the failover origin to the S3 bucket. Set the path pattern for the primary origin to *, and make viewer access restricted. Set the path pattern for the failover origin to the path of the login page, and make viewer access unrestricted.

D.Add a bucket policy to the S3 bucket to allow read access. Set the resource on the policy to the Amazon Resource Name (ARN) of the login page object in the S3 bucket. Add a CloudFront function to the default cache behavior to redirect unauthorized requests to the login page's S3 URL.

Answer: A

Explanation:

By adding a second cache behaviour with unrestricted viewer access to the login page's path pattern, unauthenticated users will be allowed to access the login page. At the same time, the default cache behaviour's settings remain unchanged, and private content remains secure because it still requires signed cookies for access.

Question: 59

CertyIQ

A developer is using AWS Amplify Hosting to build and deploy an application. The developer is receiving an increased number of bug reports from users. The developer wants to add end-to-end testing to the application to eliminate as many bugs as possible before the bugs reach production.

Which solution should the developer implement to meet these requirements?

- A.Run the amplify add test command in the Amplify CLI.
- B.Create unit tests in the application. Deploy the unit tests by using the amplify push command in the Amplify CLI.
- C.Add a test phase to the amplify.yml build settings for the application.
- D.Add a test phase to the aws-exports.js file for the application.

Answer: C

Explanation:

Adding a test phase to the amplify. yml build settings allows the developer to define and execute end-to-end tests as part of the build and deployment process in AWS Amplify Hosting. This will help ensure that bugs are caught and fixed before the application reaches production, improving the overall quality of the application.

Question: 60

CertyIQ

An ecommerce company is using an AWS Lambda function behind Amazon API Gateway as its application tier. To process orders during checkout, the application calls a POST API from the frontend. The POST API invokes the Lambda function asynchronously. In rare situations, the application has not processed orders. The Lambda application logs show no errors or failures.

What should a developer do to solve this problem?

- A.Inspect the frontend logs for API failures. Call the POST API manually by using the requests from the log file.
- B.Create and inspect the Lambda dead-letter queue. Troubleshoot the failed functions. Reprocess the events.
- C.Inspect the Lambda logs in Amazon CloudWatch for possible errors. Fix the errors.
- D.Make sure that caching is disabled for the POST API in API Gateway.

Answer: B

Explanation:

Ans: B Create and inspect the Lambda dead-letter queue. Troubleshoot the failed functions. Reprocess the events. Since the Lambda application logs show no errors or failures, it is possible that the asynchronous invocation is not being processed successfully. In this case, the best solution would be to inspect the Lambda dead-letter queue, which stores failed asynchronous invocations. By doing this, the developer can troubleshoot any failed functions and reprocess the events.

Question: 61

CertyIQ

A company is building a web application on AWS. When a customer sends a request, the application will generate reports and then make the reports available to the customer within one hour. Reports should be accessible to the customer for 8 hours. Some reports are larger than 1 MB. Each report is unique to the customer. The application should delete all reports that are older than 2 days.

Which solution will meet these requirements with the LEAST operational overhead?

- A.Generate the reports and then store the reports as Amazon DynamoDB items that have a specified TTL. Generate a URL that retrieves the reports from DynamoDB. Provide the URL to customers through the web application.
- B.Generate the reports and then store the reports in an Amazon S3 bucket that uses server-side encryption. Attach the reports to an Amazon Simple Notification Service (Amazon SNS) message. Subscribe the customer to email notifications from Amazon SNS.
- C.Generate the reports and then store the reports in an Amazon S3 bucket that uses server-side encryption. Generate a presigned URL that contains an expiration date. Provide the URL to customers through the web application. Add S3 Lifecycle configuration rules to the S3 bucket to delete old reports.
- D.Generate the reports and then store the reports in an Amazon RDS database with a date stamp. Generate an URL that retrieves the reports from the RDS database. Provide the URL to customers through the web application. Schedule an hourly AWS Lambda function to delete database records that have expired date stamps.

Answer: C

Explanation:

- 1. Presigned URL
- 2. Dynamo DB cannot store object > 400KB -> option A is out immediately. Limited access to S3 calls for presigned URL which is option C. C also has lifecycle config to delete old object while B does not have that. D is possible but too much effort compared to design pattern in C.

Question: 62

CertyIQ

A company has deployed an application on AWS Elastic Beanstalk. The company has configured the Auto Scaling group that is associated with the Elastic Beanstalk environment to have five Amazon EC2 instances. If the capacity is fewer than four EC2 instances during the deployment, application performance degrades. The company is using the all-at-once deployment policy.

What is the MOST cost-effective way to solve the deployment issue?

- A.Change the Auto Scaling group to six desired instances.
- B.Change the deployment policy to traffic splitting. Specify an evaluation time of 1 hour.
- C.Change the deployment policy to rolling with additional batch. Specify a batch size of 1.
- D.Change the deployment policy to rolling. Specify a batch size of 2.

Answer: C

Explanation:

The rolling with additional batch deployment policy allows Elastic Beanstalk to launch additional instances in a new batch before terminating the old instances. In this case, specifying a batch size of 1 means that Elastic Beanstalk will deploy the application updates to 1 new instance at a time, ensuring that there are always at least 4 instances available during the deployment process. This method maintains application performance while minimizing the additional cost.

Question: 63

CertyIQ

A developer is incorporating AWS X-Ray into an application that handles personal identifiable information (PII). The

application is hosted on Amazon EC2 instances. The application trace messages include encrypted PII and go to Amazon CloudWatch. The developer needs to ensure that no PII goes outside of the EC2 instances. Which solution will meet these requirements?

- A.Manually instrument the X-Ray SDK in the application code.
- B.Use the X-Ray auto-instrumentation agent.
- C.Use Amazon Macie to detect and hide PII. Call the X-Ray API from AWS Lambda.
- D.Use AWS Distro for Open Telemetry.

Answer: A

Explanation:

By manually instrumenting the X-Ray SDK in the application code, the developer can have full control over which data is included in the trace messages. This way, the developer can ensure that no PII is sent to X-Ray by carefully handling the PII within the application and not including it in the trace messages.

Question: 64

CertyIQ

A developer is migrating some features from a legacy monolithic application to use AWS Lambda functions instead. The application currently stores data in an Amazon Aurora DB cluster that runs in private subnets in a VPC. The AWS account has one VPC deployed. The Lambda functions and the DB cluster are deployed in the same AWS Region in the same AWS account.

The developer needs to ensure that the Lambda functions can securely access the DB cluster without crossing the public internet.

Which solution will meet these requirements?

- A.Configure the DB cluster's public access setting to Yes.
- B.Configure an Amazon RDS database proxy for the Lambda functions.
- C.Configure a NAT gateway and a security group for the Lambda functions.
- D.Configure the VPC, subnets, and a security group for the Lambda functions.

Answer: D

Explanation:

D is the right answer. When we want the lambda to privately access the DB cluster instead of moving the traffic over the public internet, we need to have the lambda and db cluster to be in the same VPC. When we configure the VPC, subnets, and a security group for the lambda function, the lambda function will be able to communicate with the db cluster using the private IPs that are associated to the VPC. NAT gateway comes into use when you have the lambda deployed in a private subnet and you would want to provide internet access to it.

Question: 65

CertyIQ

A developer is building a new application on AWS. The application uses an AWS Lambda function that retrieves information from an Amazon DynamoDB table. The developer hard coded the DynamoDB table name into the Lambda function code. The table name might change over time. The developer does not want to modify the Lambda code if the table name changes.

Which solution will meet these requirements MOST efficiently?

- A.Create a Lambda environment variable to store the table name. Use the standard method for the programming language to retrieve the variable.

B.Store the table name in a file. Store the file in the /tmp folder. Use the SDK for the programming language to retrieve the table name.

C.Create a file to store the table name. Zip the file and upload the file to the Lambda layer. Use the SDK for the programming language to retrieve the table name.

D.Create a global variable that is outside the handler in the Lambda function to store the table name.

Answer: A

Explanation:

1. You need to use environment variables
2. You can use environment variables to adjust your function's behavior without updating code. An environment variable is a pair of strings that is stored in a function's version-specific configuration. The Lambda runtime makes environment variables available to your code and sets additional environment variables that contain information about the function and invocation request.

Question: 66

CertyIQ

A company has a critical application on AWS. The application exposes an HTTP API by using Amazon API Gateway. The API is integrated with an AWS Lambda function. The application stores data in an Amazon RDS for MySQL DB instance with 2 virtual CPUs (vCPUs) and 64 GB of RAM.

Customers have reported that some of the API calls return HTTP 500 Internal Server Error responses. Amazon CloudWatch Logs shows errors for “too many connections.” The errors occur during peak usage times that are unpredictable.

The company needs to make the application resilient. The database cannot be down outside of scheduled maintenance hours.

Which solution will meet these requirements?

- A.Decrease the number of vCPUs for the DB instance. Increase the max_connections setting.
- B.Use Amazon RDS Proxy to create a proxy that connects to the DB instance. Update the Lambda function to connect to the proxy.
- C.Add a CloudWatch alarm that changes the DB instance class when the number of connections increases to more than 1,000.
- D.Add an Amazon EventBridge rule that increases the max_connections setting of the DB instance when CPU utilization is above 75%.

Answer: B

Explanation:

B: RDS Proxy establishes and manages the necessary connection pools to your database so that your Lambda function creates fewer database connections¹. RDS Proxy also handles failovers and retries automatically, which improves the availability of your application. A will reduce the performance and capacity of the database. C may incur additional charges for scaling up the DB instance. It may also cause downtime during the scaling process, which violates the requirement that the database cannot be down outside of scheduled maintenance hours. D may not react fast enough to handle unpredictable peak usage times. It may also cause memory issues if the max_connections setting is too high.

Question: 67

CertyIQ

A company has installed smart meters in all its customer locations. The smart meters measure power usage at 1-minute intervals and send the usage readings to a remote endpoint for collection. The company needs to create an

endpoint that will receive the smart meter readings and store the readings in a database. The company wants to store the location ID and timestamp information.

The company wants to give its customers low-latency access to their current usage and historical usage on demand. The company expects demand to increase significantly. The solution must not impact performance or include downtime while scaling.

Which solution will meet these requirements MOST cost-effectively?

- A.Store the smart meter readings in an Amazon RDS database. Create an index on the location ID and timestamp columns. Use the columns to filter on the customers' data.
- B.Store the smart meter readings in an Amazon DynamoDB table. Create a composite key by using the location ID and timestamp columns. Use the columns to filter on the customers' data.
- C.Store the smart meter readings in Amazon ElastiCache for Redis. Create a SortedSet key by using the location ID and timestamp columns. Use the columns to filter on the customers' data.
- D.Store the smart meter readings in Amazon S3. Partition the data by using the location ID and timestamp columns. Use Amazon Athena to filter on the customers' data.

Answer: B

Explanation:

The most cost-effective solution to meet these requirements would be to store the smart meter readings in an Amazon DynamoDB table and create a composite key using the location ID and timestamp columns.

Question: 68

CertyIQ

A company is building a serverless application that uses AWS Lambda functions. The company needs to create a set of test events to test Lambda functions in a development environment. The test events will be created once and then will be used by all the developers in an IAM developer group. The test events must be editable by any of the IAM users in the IAM developer group.

Which solution will meet these requirements?

- A.Create and store the test events in Amazon S3 as JSON objects. Allow S3 bucket access to all IAM users.
- B.Create the test events. Configure the event sharing settings to make the test events shareable.
- C.Create and store the test events in Amazon DynamoDB. Allow access to DynamoDB by using IAM roles.
- D.Create the test events. Configure the event sharing settings to make the test events private.

Answer: B

Explanation:

To create a set of test events that can be used by all developers in an IAM developer group and that are editable by any of the IAM users in the group, the company should create and store the test events in Amazon S3 as JSON objects and allow S3 bucket access to all IAM users (Option A). This will allow all developers in the IAM developer group to access and edit the test events as needed. The other options do not provide a way for multiple developers to access and edit the test events.

Question: 69

CertyIQ

A developer is configuring an application's deployment environment in AWS CodePipeline. The application code is stored in a GitHub repository. The developer wants to ensure that the repository package's unit tests run in the new deployment environment. The developer has already set the pipeline's source provider to GitHub and has

specified the repository and branch to use in the deployment.

Which combination of steps should the developer take next to meet these requirements with the LEAST overhead? (Choose two.)

- A.Create an AWS CodeCommit project. Add the repository package's build and test commands to the project's buildspec.
- B.Create an AWS CodeBuild project. Add the repository package's build and test commands to the project's buildspec.
- C.Create an AWS CodeDeploy project. Add the repository package's build and test commands to the project's buildspec.
- D.Add an action to the source stage. Specify the newly created project as the action provider. Specify the build artifact as the action's input artifact.
- E.Add a new stage to the pipeline after the source stage. Add an action to the new stage. Specify the newly created project as the action provider. Specify the source artifact as the action's input artifact.

Answer: BE

Explanation:

1. For those who just skim the question, keyword between D and E is "unit tests run in the new deployment environment.", which signifies a new stage should be created instead of just adding an action.
2. As MrTee says.

Question: 70

CertyIQ

An engineer created an A/B test of a new feature on an Amazon CloudWatch Evidently project. The engineer configured two variations of the feature (Variation A and Variation B) for the test. The engineer wants to work exclusively with Variation A. The engineer needs to make updates so that Variation A is the only variation that appears when the engineer hits the application's endpoint.

Which solution will meet this requirement?

- A.Add an override to the feature. Set the identifier of the override to the engineer's user ID. Set the variation to Variation A.
- B.Add an override to the feature. Set the identifier of the override to Variation A. Set the variation to 100%.
- C.Add an experiment to the project. Set the identifier of the experiment to Variation B. Set the variation to 0%.
- D.Add an experiment to the project. Set the identifier of the experiment to the AWS account's account ID. Set the variation to Variation A.

Answer: A

Explanation:

1. Overrides let you pre-define the variation for selected users. to always receive the editable variation.
<https://aws.amazon.com/blogs/aws/cloudwatch-evidently/>
2. Check Bullet point 9 in the link
[belowhttps://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Evidently-newfeature.html](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Evidently-newfeature.html)

Question: 71

CertyIQ

A developer is working on an existing application that uses Amazon DynamoDB as its data store. The DynamoDB table has the following attributes: partNumber (partition key), vendor (sort key), description, productFamily, and productType. When the developer analyzes the usage patterns, the developer notices that there are application modules that frequently look for a list of products based on the productFamily and productType attributes.

The developer wants to make changes to the application to improve performance of the query operations.

Which solution will meet these requirements?

- A.Create a global secondary index (GSI) with productFamily as the partition key and productType as the sort key.
- B.Create a local secondary index (LSI) with productFamily as the partition key and productType as the sort key.
- C.Recreate the table. Add partNumber as the partition key and vendor as the sort key. During table creation, add a local secondary index (LSI) with productFamily as the partition key and productType as the sort key.
- D.Update the queries to use Scan operations with productFamily as the partition key and productType as the sort key.

Answer: A

Explanation:

relate a Global Secondary Index (GSI): The developer should create a new GSI on the DynamoDB table with the product Family attribute as the partition key and the product Type attribute as the sort key. This will allow the application to perform fast queries on these attributes without scanning the entire table.

Question: 72

CertyIQ

A developer creates a VPC named VPC-A that has public and private subnets. The developer also creates an Amazon RDS database inside the private subnet of VPC-A. To perform some queries, the developer creates an AWS Lambda function in the default VPC. The Lambda function has code to access the RDS database. When the Lambda function runs, an error message indicates that the function cannot connect to the RDS database.

How can the developer solve this problem?

- A.Modify the RDS security group. Add a rule to allow traffic from all the ports from the VPC CIDR block.
- B.Redeploy the Lambda function in the same subnet as the RDS instance. Ensure that the RDS security group allows traffic from the Lambda function.
- C.Create a security group for the Lambda function. Add a new rule in the RDS security group to allow traffic from the new Lambda security group.
- D.Create an IAM role. Attach a policy that allows access to the RDS database. Attach the role to the Lambda function.

Answer: B

Explanation:

To solve this problem, the developer should redeploy the Lambda function in the same subnet as the RDS instance and ensure that the RDS security group allows traffic from the Lambda function. This will allow the Lambda function to access the RDS database within the private subnet of VPC-A. The developer should also make sure that the Lambda function is configured with the appropriate network settings and permissions to access resources within the VPC.

Question: 73

CertyIQ

A company runs an application on AWS. The company deployed the application on Amazon EC2 instances. The application stores data on Amazon Aurora.

The application recently logged multiple application-specific custom DECRYP_ERROR errors to Amazon CloudWatch logs. The company did not detect the issue until the automated tests that run every 30 minutes failed.

A developer must implement a solution that will monitor for the custom errors and alert a development team in real time when these errors occur in the production environment.

Which solution will meet these requirements with the LEAST operational overhead?

- A.Configure the application to create a custom metric and to push the metric to CloudWatch. Create an AWS CloudTrail alarm. Configure the CloudTrail alarm to use an Amazon Simple Notification Service (Amazon SNS) topic to send notifications.
- B.Create an AWS Lambda function to run every 5 minutes to scan the CloudWatch logs for the keyword DECRYP_ERROR. Configure the Lambda function to use Amazon Simple Notification Service (Amazon SNS) to send a notification.
- C.Use Amazon CloudWatch Logs to create a metric filter that has a filter pattern for DECRYP_ERROR. Create a CloudWatch alarm on this metric for a threshold ≥ 1 . Configure the alarm to send Amazon Simple Notification Service (Amazon SNS) notifications.
- D.Install the CloudWatch unified agent on the EC2 instance. Configure the application to generate a metric for the keyword DECRYP_ERROR errors. Configure the agent to send Amazon Simple Notification Service (Amazon SNS) notifications.

Answer: C

Explanation:

To monitor for custom DECRYP_ERROR errors and alert a development team in real time when these errors occur in the production environment with the least operational overhead, the developer should use Amazon Cloud Watch Logs to create a metric filter that has a filter pattern for DECRYP_ERROR. The developer should then create a Cloud Watch alarm on this metric for a threshold ≥ 1 and configure the alarm to send Amazon Simple Notification Service (Amazon SNS) notifications (Option C). This solution will allow the developer to monitor for custom errors in real time and receive notifications when they occur with minimal operational overhead.

Question: 74

CertyIQ

A developer created an AWS Lambda function that accesses resources in a VPC. The Lambda function polls an Amazon Simple Queue Service (Amazon SQS) queue for new messages through a VPC endpoint. Then the function calculates a rolling average of the numeric values that are contained in the messages. After initial tests of the Lambda function, the developer found that the value of the rolling average that the function returned was not accurate.

How can the developer ensure that the function calculates an accurate rolling average?

- A.Set the function's reserved concurrency to 1. Calculate the rolling average in the function. Store the calculated rolling average in Amazon ElastiCache.
- B.Modify the function to store the values in Amazon ElastiCache. When the function initializes, use the previous values from the cache to calculate the rolling average.
- C.Set the function's provisioned concurrency to 1. Calculate the rolling average in the function. Store the calculated rolling average in Amazon ElastiCache.
- D.Modify the function to store the values in the function's layers. When the function initializes, use the previously stored values to calculate the rolling average.

Answer: B

Explanation:

1. By using ElastiCache, the Lambda function can store the values of the previous messages it has received, which can be used to calculate an accurate rolling average.
2. The best way for the developer to ensure that the function calculates an accurate rolling average is to modify the function to store the values in Amazon ElastiCache. When the function initializes, use the previous

values from the cache to calculate the rolling average. This solution is the best because it ensures that the rolling average is always calculated from the latest values, even if the Lambda function is scaled out to multiple instances.

CertyIQ

Question: 75

A developer is writing unit tests for a new application that will be deployed on AWS. The developer wants to validate all pull requests with unit tests and merge the code with the main branch only when all tests pass.

The developer stores the code in AWS CodeCommit and sets up AWS CodeBuild to run the unit tests. The developer creates an AWS Lambda function to start the CodeBuild task. The developer needs to identify the CodeCommit events in an Amazon EventBridge event that can invoke the Lambda function when a pull request is created or updated.

Which CodeCommit event will meet these requirements?

A.

```
{  
    "source": ["aws.codecommit"],  
    "detail": {  
        "event": ["pullRequestMergeStatusUpdated"],  
    }  
}
```

B.

```
{  
    "source": ["aws.codecommit"],  
    "detail": {  
        "event": ["pullRequestApprovalRuleCreated"]  
    }  
}
```

C.

```
{  
    "source": ["aws.codecommit"],  
    "detail": {  
        "event": ["pullRequestSourceBranchUpdated", "pullRequestCreated"]  
    }  
}
```

D.

```
{  
    "source": ["aws.codecommit"],  
    "detail": {  
        "event": ["pullRequestUpdated", "pullRequestSourceBranchCreated"]  
    }  
}
```

Answer: C

Explanation:

C. Events in answer D are not real. A & B are clearly wrong since two events are required.

Question: 76

CertyIQ

A developer deployed an application to an Amazon EC2 instance. The application needs to know the public IPv4 address of the instance.

How can the application find this information?

- A.Query the instance metadata from <http://169.254.169.254/latest/meta-data/>.
- B.Query the instance user data from <http://169.254.169.254/latest/user-data/>.
- C.Query the Amazon Machine Image (AMI) information from <http://169.254.169.254/latest/meta-data/ami/>.
- D.Check the hosts file of the operating system.

Answer: A**Explanation:**

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instancedata-data-retrieval.html>

Question: 77

CertyIQ

An application under development is required to store hundreds of video files. The data must be encrypted within the application prior to storage, with a unique key for each video file.

How should the developer code the application?

- A.Use the KMS Encrypt API to encrypt the data. Store the encrypted data key and data.
- B.Use a cryptography library to generate an encryption key for the application. Use the encryption key to encrypt the data. Store the encrypted data.
- C.Use the KMS GenerateDataKey API to get a data key. Encrypt the data with the data key. Store the encrypted data key and data.
- D.Upload the data to an S3 bucket using server side-encryption with an AWS KMS key.

Answer: C**Explanation:**

Option C: use the KMS Generate Data Key API to get a data key. Encrypt the data with the data key. Store the encrypted data key and data.

Question: 78

CertyIQ

A company is planning to deploy an application on AWS behind an Elastic Load Balancer. The application uses an HTTP/HTTPS listener and must access the client IP addresses.

Which load-balancing solution meets these requirements?

- A.Use an Application Load Balancer and the X-Forwarded-For headers.
- B.Use a Network Load Balancer (NLB). Enable proxy protocol support on the NLB and the target application.
- C.Use an Application Load Balancer. Register the targets by the instance ID.
- D.Use a Network Load Balancer and the X-Forwarded-For headers.

Answer: A

Explanation:

Use an Application Load Balancer (ALB) and the X-Forwarded-For headers. When an ALB is used, the X-Forwarded-For header can be used to pass the client IP address to the backend servers.

CertyIQ

Question: 79

A developer wants to debug an application by searching and filtering log data. The application logs are stored in Amazon CloudWatch Logs. The developer creates a new metric filter to count exceptions in the application logs. However, no results are returned from the logs.

What is the reason that no filtered results are being returned?

- A.A setup of the Amazon CloudWatch interface VPC endpoint is required for filtering the CloudWatch Logs in the VPC.
- B.CloudWatch Logs only publishes metric data for events that happen after the filter is created.
- C.The log group for CloudWatch Logs should be first streamed to Amazon OpenSearch Service before metric filtering returns the results.
- D.Metric data points for logs groups can be filtered only after they are exported to an Amazon S3 bucket.

Answer: B

Explanation:

Filters do not retroactively filter data. Filters only publish the metric data points for events that happen after the filter was created.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/MonitoringLogData.html>

CertyIQ

Question: 80

A company is planning to use AWS CodeDeploy to deploy an application to Amazon Elastic Container Service (Amazon ECS). During the deployment of a new version of the application, the company initially must expose only 10% of live traffic to the new version of the deployed application. Then, after 15 minutes elapse, the company must route all the remaining live traffic to the new version of the deployed application.

Which CodeDeploy predefined configuration will meet these requirements?

- A.CodeDeployDefault.ECSCanary10Percent15Minutes
- B.CodeDeployDefault.LambdaCanary10Percent5Minutes
- C.CodeDeployDefault.LambdaCanary10Percent15Minutes
- D.CodeDeployDefault.ECSLinear10PercentEvery1Minutes

Answer: A

Explanation:

This predefined deployment configuration for AWS Code Deploy with Amazon ECS will initially shift 10% of the traffic to the new version and wait for 15 minutes before shifting the remaining 90% of the traffic to the new version.

Reference:

Question: 81

CertyIQ

A company hosts a batch processing application on AWS Elastic Beanstalk with instances that run the most recent version of Amazon Linux. The application sorts and processes large datasets.

In recent weeks, the application's performance has decreased significantly during a peak period for traffic. A developer suspects that the application issues are related to the memory usage. The developer checks the Elastic Beanstalk console and notices that memory usage is not being tracked.

How should the developer gather more information about the application performance issues?

- A.Configure the Amazon CloudWatch agent to push logs to Amazon CloudWatch Logs by using port 443.
- B.Configure the Elastic Beanstalk .ebextensions directory to track the memory usage of the instances.
- C.Configure the Amazon CloudWatch agent to track the memory usage of the instances.
- D.Configure an Amazon CloudWatch dashboard to track the memory usage of the instances.

Answer: C

Explanation:

Configure the Amazon Cloud Watch agent to track the memory usage of the instances.

Amazon Cloud Watch does not collect memory metrics by default. You need to install the Cloud Watch agent on your instances to collect this additional system-level metric like memory utilization.

Question: 82

CertyIQ

A developer is building a highly secure healthcare application using serverless components. This application requires writing temporary data to /tmp storage on an AWS Lambda function.

How should the developer encrypt this data?

- A.Enable Amazon EBS volume encryption with an AWS KMS key in the Lambda function configuration so that all storage attached to the Lambda function is encrypted.
- B.Set up the Lambda function with a role and key policy to access an AWS KMS key. Use the key to generate a data key used to encrypt all data prior to writing to /tmp storage.
- C.Use OpenSSL to generate a symmetric encryption key on Lambda startup. Use this key to encrypt the data prior to writing to /tmp.
- D.Use an on-premises hardware security module (HSM) to generate keys, where the Lambda function requests a data key from the HSM and uses that to encrypt data on all requests to the function.

Answer: B

Explanation:

Set up the Lambda function with a role and key policy to access an AWS KMS key. Use the key to generate a data key used to encrypt all data prior to writing to /tmp storage.

Question: 83

CertyIQ

A developer has created an AWS Lambda function to provide notification through Amazon Simple Notification Service (Amazon SNS) whenever a file is uploaded to Amazon S3 that is larger than 50 MB. The developer has deployed and tested the Lambda function by using the CLI. However, when the event notification is added to the S3 bucket and a 3,000 MB file is uploaded, the Lambda function does not launch.

Which of the following is a possible reason for the Lambda function's inability to launch?

- A.The S3 event notification does not activate for files that are larger than 1,000 MB.
- B.The resource-based policy for the Lambda function does not have the required permissions to be invoked by Amazon S3.
- C.Lambda functions cannot be invoked directly from an S3 event.
- D.The S3 bucket needs to be made public.

Answer: B

Explanation:

B - is right answer A is incorrect because the size of the file should not affect whether the event notification is triggered. C is incorrect because Lambda functions can indeed be invoked directly from an S3 event. D is incorrect because the S3 bucket does not need to be made public for the Lambda function to be invoked.

Question: 84

CertyIQ

A developer is creating a Ruby application and needs to automate the deployment, scaling, and management of an environment without requiring knowledge of the underlying infrastructure.

Which service would best accomplish this task?

- A.AWS CodeDeploy
- B.AWS CloudFormation
- C.AWS OpsWorks
- D.AWS Elastic Beanstalk

Answer: D

Explanation:

AWS Elastic Beanstalk is designed for developers like the one in your scenario who want to deploy and manage applications without worrying about the underlying infrastructure. It automates the deployment process and automatically handles capacity provisioning, load balancing, auto-scaling, and application health monitoring. You can use it with various platforms including Ruby.

Question: 85

CertyIQ

A company has a web application that is deployed on AWS. The application uses an Amazon API Gateway API and an AWS Lambda function as its backend.

The application recently demonstrated unexpected behavior. A developer examines the Lambda function code, finds an error, and modifies the code to resolve the problem. Before deploying the change to production, the developer needs to run tests to validate that the application operates properly.

The application has only a production environment available. The developer must create a new development environment to test the code changes. The developer must also prevent other developers from overwriting these changes during the test cycle.

Which combination of steps will meet these requirements with the LEAST development effort? (Choose two.)

- A.Create a new resource in the current stage. Create a new method with Lambda proxy integration. Select the Lambda function. Add the hotfix alias. Redeploy the current stage. Test the backend.
- B.Update the Lambda function in the API Gateway API integration request to use the hotfix alias. Deploy the API Gateway API to a new stage named hotfix. Test the backend.
- C.Modify the Lambda function by fixing the code. Test the Lambda function. Create the alias hotfix. Point the alias to the \$LATEST version.
- D.Modify the Lambda function by fixing the code. Test the Lambda function. When the Lambda function is working as expected, publish the Lambda function as a new version. Create the alias hotfix. Point the alias to the new version.
- E.Create a new API Gateway API for the development environment. Add a resource and method with Lambda integration. Choose the Lambda function and the hotfix alias. Deploy to a new stage. Test the backend.

Answer: BD

Explanation:

It is B & D. Clearly E isn't operationally efficient. So we got to choose from A & B one, and C & D the second. Between A & B, we gotta pick B since in the question it clearly states that we don't want to touch the existing solution. Regarding C & D, seems like D is more thorough and also pointing to \$LATEST is not sufficiently explicit when you troubleshoot.

Question: 86

CertyIQ

A developer is implementing an AWS Cloud Development Kit (AWS CDK) serverless application. The developer will provision several AWS Lambda functions and Amazon API Gateway APIs during AWS CloudFormation stack creation. The developer's workstation has the AWS Serverless Application Model (AWS SAM) and the AWS CDK installed locally.

How can the developer test a specific Lambda function locally?

- A.Run the sam package and sam deploy commands. Create a Lambda test event from the AWS Management Console. Test the Lambda function.
- B.Run the cdk synth and cdk deploy commands. Create a Lambda test event from the AWS Management Console. Test the Lambda function.
- C.Run the cdk synth and sam local invoke commands with the function construct identifier and the path to the synthesized CloudFormation template.
- D.Run the cdk synth and sam local start-lambda commands with the function construct identifier and the path to the synthesized CloudFormation template.

Answer: C

Explanation:

1. To test a specific Lambda function locally when using the AWS Cloud Development Kit (AWS CDK), the developer can use the AWS Serverless Application Model (AWS SAM) CLI's local testing capabilities in conjunction with the CDK. The typical process would be:
Run cdk synth to synthesize the AWS CDK app into a CloudFormation template.
Use sam local invoke to run the specific Lambda function locally, providing the function's logical identifier and the path to the synthesized CloudFormation template as arguments.
2. Use the AWS SAM CLI sam local invoke subcommand to initiate a one-time invocation of an AWS Lambda function locally.
<https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/using-sam-cli-local-invoke.html>

Question: 87

CertyIQ

A company's new mobile app uses Amazon API Gateway. As the development team completes a new release of its APIs, a developer must safely and transparently roll out the API change.

What is the SIMPLEST solution for the developer to use for rolling out the new API version to a limited number of users through API Gateway?

- A.Create a new API in API Gateway. Direct a portion of the traffic to the new API using an Amazon Route 53 weighted routing policy.
- B.Validate the new API version and promote it to production during the window of lowest expected utilization.
- C.Implement an Amazon CloudWatch alarm to trigger a rollback if the observed HTTP 500 status code rate exceeds a predetermined threshold.
- D.Use the canary release deployment option in API Gateway. Direct a percentage of the API traffic using the canarySettings setting.

Answer: D

Explanation:

Canary deployments allow you to divert a percentage of your API traffic to a new API version, enabling you to test how the new version will perform under real-world conditions without fully replacing the previous version. This is especially useful for reducing the risk associated with deploying new versions.

Question: 88

CertyIQ

A company caches session information for a web application in an Amazon DynamoDB table. The company wants an automated way to delete old items from the table.

What is the simplest way to do this?

- A.Write a script that deletes old records; schedule the script as a cron job on an Amazon EC2 instance.
- B.Add an attribute with the expiration time; enable the Time To Live feature based on that attribute.
- C.Each day, create a new table to hold session data; delete the previous day's table.
- D.Add an attribute with the expiration time; name the attribute ItemExpiration.

Answer: B

Explanation:

The simplest way to automatically delete old items from an Amazon DynamoDB table is to use DynamoDB's Time to Live (TTL) feature. This feature allows you to define an attribute that stores the expiration time for each item. Once the specified time has passed, DynamoDB automatically deletes the expired items, freeing up storage and reducing costs without the need for custom scripts or manual intervention.

Question: 89

CertyIQ

A company is using an Amazon API Gateway REST API endpoint as a webhook to publish events from an on-premises source control management (SCM) system to Amazon EventBridge. The company has configured an EventBridge rule to listen for the events and to control application deployment in a central AWS account. The company needs to receive the same events across multiple receiver AWS accounts.

How can a developer meet these requirements without changing the configuration of the SCM system?

- A.Deploy the API Gateway REST API to all the required AWS accounts. Use the same custom domain name for all the gateway endpoints so that a single SCM webhook can be used for all events from all accounts.
- B.Deploy the API Gateway REST API to all the receiver AWS accounts. Create as many SCM webhooks as the number of AWS accounts.
- C.Grant permission to the central AWS account for EventBridge to access the receiver AWS accounts. Add an EventBridge event bus on the receiver AWS accounts as the targets to the existing EventBridge rule.
- D.Convert the API Gateway type from REST API to HTTP API.

Answer: C

Explanation:

It's C - event bridge event buses in one (target) account can be a target of another event rule in a source account.

Reference:

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-cross-account.html>

Question: 90

CertyIQ

A company moved some of its secure files to a private Amazon S3 bucket that has no public access. The company wants to develop a serverless application that gives its employees the ability to log in and securely share the files with other users.

Which AWS feature should the company use to share and access the files securely?

- A.Amazon Cognito user pool
- B.S3 presigned URLs
- C.S3 bucket policy
- D.Amazon Cognito identity pool

Answer: B

Explanation:

Employees log into the serverless application using an Amazon Cognito User Pool. Once logged in, the application's back-end logic (possibly a Lambda function) generates an S3 pre-signed URL for the requested file. The pre-signed URL is then given to the authenticated user, allowing them secure, time-limited access to that specific S3 object. So, while both Amazon Cognito User Pool and S3 Pre-signed URLs would be used in the solution, S3 Pre-signed URLs (Option B) are the specific feature that allows for the secure, temporary sharing of S3 files. Therefore, Option B would be the best answer to the question of how to "share and access the files securely."

Question: 91

CertyIQ

A company needs to develop a proof of concept for a web service application. The application will show the weather forecast for one of the company's office locations. The application will provide a REST endpoint that clients can call. Where possible, the application should use caching features provided by AWS to limit the number of requests to the backend service. The application backend will receive a small amount of traffic only during testing.

Which approach should the developer take to provide the REST endpoint MOST cost-effectively?

- A.Create a container image. Deploy the container image by using Amazon Elastic Kubernetes Service (Amazon EKS). Expose the functionality by using Amazon API Gateway.
- B.Create an AWS Lambda function by using the AWS Serverless Application Model (AWS SAM). Expose the Lambda functionality by using Amazon API Gateway.
- C.Create a container image. Deploy the container image by using Amazon Elastic Container Service (Amazon ECS). Expose the functionality by using Amazon API Gateway.
- D.Create a microservices application. Deploy the application to AWS Elastic Beanstalk. Expose the AWS Lambda functionality by using an Application Load Balancer.

Answer: B

Explanation:

Create an AWS Lambda function by using the AWS Serverless Application Model (AWS SAM). Expose the Lambda functionality by using Amazon API Gateway.

CertyIQ

Question: 92

An e-commerce web application that shares session state on-premises is being migrated to AWS. The application must be fault tolerant, natively highly scalable, and any service interruption should not affect the user experience.

What is the best option to store the session state?

- A.Store the session state in Amazon ElastiCache.
- B.Store the session state in Amazon CloudFront.
- C.Store the session state in Amazon S3.
- D.Enable session stickiness using elastic load balancers.

Answer: A

Explanation:

Correct answer is A:Store the session state in Amazon Elastic Cache.

CertyIQ

Question: 93

A developer is building an application that uses Amazon DynamoDB. The developer wants to retrieve multiple specific items from the database with a single API call.

Which DynamoDB API call will meet these requirements with the MINIMUM impact on the database?

- A.BatchGetItem
- B.GetItem
- C.Scan
- D.Query

Answer: A

Explanation:

A Is the correct answer with the minimum impact on the database.

Reference:

Question: 94

A developer has written an application that runs on Amazon EC2 instances. The developer is adding functionality for the application to write objects to an Amazon S3 bucket.

Which policy must the developer modify to allow the instances to write these objects?

- A.The IAM policy that is attached to the EC2 instance profile role
- B.The session policy that is applied to the EC2 instance role session
- C.The AWS Key Management Service (AWS KMS) key policy that is attached to the EC2 instance profile role
- D.The Amazon VPC endpoint policy

Answer: A

Explanation:

The IAM policy that is attached to the EC2 instance profile role

Reference:

<https://repost.aws/knowledge-center/ec2-instance-access-s3-bucket>

Question: 95

A developer is leveraging a Border Gateway Protocol (BGP)-based AWS VPN connection to connect from on-premises to Amazon EC2 instances in the developer's account. The developer is able to access an EC2 instance in subnet A, but is unable to access an EC2 instance in subnet B in the same VPC.

Which logs can the developer use to verify whether the traffic is reaching subnet B?

- A.VPN logs
- B.BGP logs
- C.VPC Flow Logs
- D.AWS CloudTrail logs

Answer: C

Explanation:

VPC Flow Logs capture information about the IP traffic going to and from network interfaces in a VPC. This includes traffic that traverses a VPN connection. VPC Flow Logs can be used to monitor and troubleshoot connectivity issues, including verifying whether traffic is reaching a particular subnet within the VPC.

Question: 96

A developer is creating a service that uses an Amazon S3 bucket for image uploads. The service will use an AWS Lambda function to create a thumbnail of each image. Each time an image is uploaded, the service needs to send an email notification and create the thumbnail. The developer needs to configure the image processing and email notifications setup.

Which solution will meet these requirements?

- A.Create an Amazon Simple Notification Service (Amazon SNS) topic. Configure S3 event notifications with a destination of the SNS topic. Subscribe the Lambda function to the SNS topic. Create an email notification subscription to the SNS topic.
- B.Create an Amazon Simple Notification Service (Amazon SNS) topic. Configure S3 event notifications with a destination of the SNS topic. Subscribe the Lambda function to the SNS topic. Create an Amazon Simple Queue Service (Amazon SQS) queue. Subscribe the SQS queue to the SNS topic. Create an email notification subscription to the SQS queue.
- C.Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure S3 event notifications with a destination of the SQS queue. Subscribe the Lambda function to the SQS queue. Create an email notification subscription to the SQS queue.
- D.Create an Amazon Simple Queue Service (Amazon SQS) queue. Send S3 event notifications to Amazon EventBridge. Create an EventBridge rule that runs the Lambda function when images are uploaded to the S3 bucket. Create an EventBridge rule that sends notifications to the SQS queue. Create an email notification subscription to the SQS queue.

Answer: A

Explanation:

This solution will allow the developer to receive notifications for each image uploaded to the S3 bucket, and also create a thumbnail using the Lambda function. The SNS topic will serve as a trigger for both the Lambda function and the email notification subscription. When an image is uploaded, S3 will send a notification to the SNS topic, which will trigger the Lambda function to create the thumbnail and also send an email notification to the specified email address.

Question: 97

CertyIQ

A developer has designed an application to store incoming data as JSON files in Amazon S3 objects. Custom business logic in an AWS Lambda function then transforms the objects, and the Lambda function loads the data into an Amazon DynamoDB table. Recently, the workload has experienced sudden and significant changes in traffic. The flow of data to the DynamoDB table is becoming throttled.

The developer needs to implement a solution to eliminate the throttling and load the data into the DynamoDB table more consistently.

Which solution will meet these requirements?

- A.Refactor the Lambda function into two functions. Configure one function to transform the data and one function to load the data into the DynamoDB table. Create an Amazon Simple Queue Service (Amazon SQS) queue in between the functions to hold the items as messages and to invoke the second function.
- B.Turn on auto scaling for the DynamoDB table. Use Amazon CloudWatch to monitor the table's read and write capacity metrics and to track consumed capacity.
- C.Create an alias for the Lambda function. Configure provisioned concurrency for the application to use.
- D.Refactor the Lambda function into two functions. Configure one function to store the data in the DynamoDB table. Configure the second function to process the data and update the items after the data is stored in DynamoDB. Create a DynamoDB stream to invoke the second function after the data is stored.

Answer: A

Explanation:

1. A. Refactor the Lambda function into two functions. Configure one function to transform the data and one function to load the data into the DynamoDB table. Create an Amazon Simple Queue Service (Amazon SQS) queue in between the functions to hold the items as messages and to invoke the second function. By breaking the Lambda function into two separate functions and using an SQS queue to hold the transformed data as messages, you can decouple the data transformation and loading processes. This allows for more controlled

loading of data into the DynamoDB table and helps eliminate throttling issues.

2. Refactoring the Lambda function into two functions and introducing an Amazon Simple Queue Service (Amazon SQS) queue between them would provide a buffering mechanism. The first Lambda function would transform the data and push it to the SQS queue. The second Lambda function would be triggered by messages in the SQS queue to write the data into DynamoDB. This decouples the two operations and allows for more controlled and consistent data loading into DynamoDB, helping to avoid throttling.

Question: 98

CertyIQ

A developer is creating an AWS Lambda function in VPC mode. An Amazon S3 event will invoke the Lambda function when an object is uploaded into an S3 bucket. The Lambda function will process the object and produce some analytic results that will be recorded into a file. Each processed object will also generate a log entry that will be recorded into a file.

Other Lambda functions, AWS services, and on-premises resources must have access to the result files and log file. Each log entry must also be appended to the same shared log file. The developer needs a solution that can share files and append results into an existing file.

Which solution should the developer use to meet these requirements?

- A.Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system in Lambda. Store the result files and log file in the mount point. Append the log entries to the log file.
- B.Create an Amazon Elastic Block Store (Amazon EBS) Multi-Attach enabled volume. Attach the EBS volume to all Lambda functions. Update the Lambda function code to download the log file, append the log entries, and upload the modified log file to Amazon EBS.
- C.Create a reference to the /tmp local directory. Store the result files and log file by using the directory reference. Append the log entry to the log file.
- D.Create a reference to the /opt storage directory. Store the result files and log file by using the directory reference. Append the log entry to the log file.

Answer: A

Explanation:

The requirement is to have a shared file system that allows for appending to files and can be accessed by multiple Lambda functions, AWS services, and on-premises resources. Amazon Elastic File System (Amazon EFS) is a good fit for these requirements. EFS provides a scalable and elastic NFS file system which can be mounted to multiple EC2 instances and Lambda functions at the same time, making it easier for these resources to share files. You can also append to existing files on an EFS file system, which meets the requirement for a shared log file that can have new entries appended to it.

Question: 99

CertyIQ

A company has an AWS Lambda function that processes incoming requests from an Amazon API Gateway API. The API calls the Lambda function by using a Lambda alias. A developer updated the Lambda function code to handle more details related to the incoming requests. The developer wants to deploy the new Lambda function for more testing by other developers with no impact to customers that use the API.

Which solution will meet these requirements with the LEAST operational overhead?

- A.Create a new version of the Lambda function. Create a new stage on API Gateway with integration to the new Lambda version. Use the new API Gateway stage to test the Lambda function.
- B.Update the existing Lambda alias used by API Gateway to a weighted alias. Add the new Lambda version as an additional Lambda function with a weight of 10%. Use the existing API Gateway stage for testing.
- C.Create a new version of the Lambda function. Create and deploy a second Lambda function to filter incoming

requests from API Gateway. If the filtering Lambda function detects a test request, the filtering Lambda function will invoke the new Lambda version of the code. For other requests, the filtering Lambda function will invoke the old Lambda version. Update the API Gateway API to use the filtering Lambda function.

D.Create a new version of the Lambda function. Create a new API Gateway API for testing purposes. Update the integration of the new API with the new Lambda version. Use the new API for testing.

Answer: A

Explanation:

Create a new version of the Lambda function. Create a new stage on API Gateway with integration to the new Lambda version. Use the new API Gateway stage to test the Lambda function.

Question: 100

CertyIQ

A company uses AWS Lambda functions and an Amazon S3 trigger to process images into an S3 bucket. A development team set up multiple environments in a single AWS account.

After a recent production deployment, the development team observed that the development S3 buckets invoked the production environment Lambda functions. These invocations caused unwanted execution of development S3 files by using production Lambda functions. The development team must prevent these invocations. The team must follow security best practices.

Which solution will meet these requirements?

- A.Update the Lambda execution role for the production Lambda function to add a policy that allows the execution role to read from only the production environment S3 bucket.
- B.Move the development and production environments into separate AWS accounts. Add a resource policy to each Lambda function to allow only S3 buckets that are within the same account to invoke the function.
- C.Add a resource policy to the production Lambda function to allow only the production environment S3 bucket to invoke the function.
- D.Move the development and production environments into separate AWS accounts. Update the Lambda execution role for each function to add a policy that allows the execution role to read from the S3 bucket that is within the same account.

Answer: C

Explanation:

C. Add a resource policy to the production Lambda function to allow only the production environment S3 bucket to invoke the function. In this scenario, the goal is to prevent unwanted invocations of production Lambda functions by development S3 buckets. Adding a resource policy directly to the production Lambda function that restricts invocations to only the production S3 bucket ensures that the function is only invoked by the intended bucket.

Question: 101

CertyIQ

A developer is creating an application. New users of the application must be able to create an account and register by using their own social media accounts.

Which AWS service or resource should the developer use to meet these requirements?

- A.IAM role
- B.Amazon Cognito identity pools

C.Amazon Cognito user pools

D.AWS Directory Service

Answer: C

Explanation:

For creating an application where new users can create accounts and register using their social media accounts, Amazon Cognito is the most suitable service. Specifically, you'd want to use Amazon Cognito User Pools. Amazon Cognito User Pools support sign-ins using social identity providers like Facebook, Google, and Amazon, as well as enterprise identity providers via SAML 2.0. With a user pool, you can create a fully managed user directory to enable user sign-up and sign-in, as well as handle password recovery, user verification, and other user management tasks.

Reference:

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

CertyIQ

Question: 102

A social media application uses the AWS SDK for JavaScript on the frontend to get user credentials from AWS Security Token Service (AWS STS). The application stores its assets in an Amazon S3 bucket. The application serves its content by using an Amazon CloudFront distribution with the origin set to the S3 bucket.

The credentials for the role that the application assumes to make the SDK calls are stored in plaintext in a JSON file within the application code. The developer needs to implement a solution that will allow the application to get user credentials without having any credentials hardcoded in the application code.

Which solution will meet these requirements?

A.Add a Lambda@Edge function to the distribution. Invoke the function on viewer request. Add permissions to the function's execution role to allow the function to access AWS STS. Move all SDK calls from the frontend into the function.

B.Add a CloudFront function to the distribution. Invoke the function on viewer request. Add permissions to the function's execution role to allow the function to access AWS STS. Move all SDK calls from the frontend into the function.

C.Add a Lambda@Edge function to the distribution. Invoke the function on viewer request. Move the credentials from the JSON file into the function. Move all SDK calls from the frontend into the function.

D.Add a CloudFront function to the distribution. Invoke the function on viewer request. Move the credentials from the JSON file into the function. Move all SDK calls from the frontend into the function.

Answer: A

Explanation:

The answer is A. Here is a reference directly from AWS docs:"If you need some of the capabilities of Lambda@ Edge that are not available with Cloud Front Functions, such as network access or a longer execution time, you can still use Lambda@ Edge before and after content is cached by Cloud Front." Since the requirement is to access the STS service, network access is required. Therefore, it can't be Cloud front functions. Also, as a side note it's worth to mention that Cloud front functions can only execute for up to 1ms. Apparently this isn't enough to fetch user creds (tokens) from STS. The table in the following link summarises the differences between Cloud front functions and Lambda@edge

<https://aws.amazon.com/blogs/aws/introducing-cloudfront-functions-run-your-code-at-the-edge-with-low-latency-at-any-scale/>

Question: 103

CertyIQ

An ecommerce website uses an AWS Lambda function and an Amazon RDS for MySQL database for an order fulfillment service. The service needs to return order confirmation immediately.

During a marketing campaign that caused an increase in the number of orders, the website's operations team noticed errors for "too many connections" from Amazon RDS. However, the RDS DB cluster metrics are healthy. CPU and memory capacity are still available.

What should a developer do to resolve the errors?

- A. Initialize the database connection outside the handler function. Increase the max_user_connections value on the parameter group of the DB cluster. Restart the DB cluster.
- B. Initialize the database connection outside the handler function. Use RDS Proxy instead of connecting directly to the DB cluster.
- C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to queue the orders. Ingest the orders into the database. Set the Lambda function's concurrency to a value that equals the number of available database connections.
- D. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to queue the orders. Ingest the orders into the database. Set the Lambda function's concurrency to a value that is less than the number of available database connections.

Answer: B

Explanation:

1. Use an RDS Proxy instead of connecting directly to the DB cluster.
2. We can use an RDS proxy to handle a lot of connections. We are choosing this option because the load on the RDS is normal. If the RDS was unable to handle loads, we would've checked other options like queues or transactions.

Question: 104

CertyIQ

A company stores its data in data tables in a series of Amazon S3 buckets. The company received an alert that customer credit card information might have been exposed in a data table on one of the company's public applications. A developer needs to identify all potential exposures within the application environment.

Which solution will meet these requirements?

- A. Use Amazon Athena to run a job on the S3 buckets that contain the affected data. Filter the findings by using the SensitiveData:S3Object/Personal finding type.
- B. Use Amazon Macie to run a job on the S3 buckets that contain the affected data. Filter the findings by using the SensitiveData:S3Object/Financial finding type.
- C. Use Amazon Macie to run a job on the S3 buckets that contain the affected data. Filter the findings by using the SensitiveData:S3Object/Personal finding type.
- D. Use Amazon Athena to run a job on the S3 buckets that contain the affected data. Filter the findings by using the SensitiveData:S3Object/Financial finding type.

Answer: B

Explanation:

Use Amazon Macie to run a job on the S3 buckets that contain the affected data. Filter the findings by using the SensitiveData:S3Object/Financial finding type. Option A and D suggest using Amazon Athena, which is an interactive query service that can be used to analyze data stored in S3 using standard SQL queries. While Athena can help identify data in S3 buckets, it does not provide the same level of automated scanning and

pattern matching that Amazon Macie does. Option C is incorrect because the SensitiveData:S3Object/Personal finding type is designed to identify personally identifiable information (PII), such as names and addresses, but not credit card information.

<https://docs.aws.amazon.com/macie/latest/user/findings-types.html>

Question: 105

CertyIQ

A software company is launching a multimedia application. The application will allow guest users to access sample content before the users decide if they want to create an account to gain full access. The company wants to implement an authentication process that can identify users who have already created an account. The company also needs to keep track of the number of guest users who eventually create an account.

Which combination of steps will meet these requirements? (Choose two.)

- A.Create an Amazon Cognito user pool. Configure the user pool to allow unauthenticated users. Exchange user tokens for temporary credentials that allow authenticated users to assume a role.
- B.Create an Amazon Cognito identity pool. Configure the identity pool to allow unauthenticated users. Exchange unique identity for temporary credentials that allow all users to assume a role.
- C.Create an Amazon CloudFront distribution. Configure the distribution to allow unauthenticated users. Exchange user tokens for temporary credentials that allow all users to assume a role.
- D.Create a role for authenticated users that allows access to all content. Create a role for unauthenticated users that allows access to only the sample content.
- E.Allow all users to access the sample content by default. Create a role for authenticated users that allows access to the other content.

Answer: BD

Explanation:

1. option B because by configuring the identity pool to allow unauthenticated users, you can enable guest users to access the sample content. When users create an account, they can be authenticated, and then given access to the full content by assuming a role that allows them access. Option D is correct because creating roles for authenticated and unauthenticated users with different levels of access is an appropriate way to meet the requirement of identifying users who have created an account and keeping track of the number of guest users who eventually create an account.

2. "who alreaady created account" means User Pool not required. - NOT A

Question: 106

CertyIQ

A company is updating an application to move the backend of the application from Amazon EC2 instances to a serverless model. The application uses an Amazon RDS for MySQL DB instance and runs in a single VPC on AWS. The application and the DB instance are deployed in a private subnet in the VPC.

The company needs to connect AWS Lambda functions to the DB instance.

Which solution will meet these requirements?

- A.Create Lambda functions inside the VPC with the AWSLambdaBasicExecutionRole policy attached to the Lambda execution role. Modify the RDS security group to allow inbound access from the Lambda security group.
- B.Create Lambda functions inside the VPC with the AWSLambdaVPCAccessExecutionRole policy attached to the Lambda execution role. Modify the RDS security group to allow inbound access from the Lambda security group.
- C.Create Lambda functions with the AWSLambdaBasicExecutionRole policy attached to the Lambda execution role. Create an interface VPC endpoint for the Lambda functions. Configure the interface endpoint policy to

allow the lambda:InvokeFunction action for each Lambda function's Amazon Resource Name (ARN).

D.Create Lambda functions with the AWSLambdaVPCAccessExecutionRole policy attached to the Lambda execution role. Create an interface VPC endpoint for the Lambda functions. Configure the interface endpoint policy to allow the lambda:InvokeFunction action for each Lambda function's Amazon Resource Name (ARN).

Answer: B

Explanation:

The AWS Lambda VPC Access Execution Role policy allows the Lambda function to create elastic network interfaces (ENIs) in the VPC and use the security groups attached to those ENIs for controlling inbound and outbound traffic.

CertyIQ

Question: 107

A company has a web application that runs on Amazon EC2 instances with a custom Amazon Machine Image (AMI). The company uses AWS CloudFormation to provision the application. The application runs in the us-east-1 Region, and the company needs to deploy the application to the us-west-1 Region.

An attempt to create the AWS CloudFormation stack in us-west-1 fails. An error message states that the AMI ID does not exist. A developer must resolve this error with a solution that uses the least amount of operational overhead.

Which solution meets these requirements?

- A.Change the AWS CloudFormation templates for us-east-1 and us-west-1 to use an AWS AMI. Relaunch the stack for both Regions.
- B.Copy the custom AMI from us-east-1 to us-west-1. Update the AWS CloudFormation template for us-west-1 to refer to AMI ID for the copied AMI. Relaunch the stack.
- C.Build the custom AMI in us-west-1. Create a new AWS CloudFormation template to launch the stack in us-west-1 with the new AMI ID.
- D.Manually deploy the application outside AWS CloudFormation in us-west-1.

Answer: B

Explanation:

Copy the custom AMI from us-east-1 to us-west-1. Update the AWS Cloud Formation template for us-west-1 to refer to AMI ID for the copied AMI. Relaunch the stack.

CertyIQ

Question: 108

A developer is updating several AWS Lambda functions and notices that all the Lambda functions share the same custom libraries. The developer wants to centralize all the libraries, update the libraries in a convenient way, and keep the libraries versioned.

Which solution will meet these requirements with the LEAST development effort?

- A.Create an AWS CodeArtifact repository that contains all the custom libraries.
- B.Create a custom container image for the Lambda functions to save all the custom libraries.
- C.Create a Lambda layer that contains all the custom libraries.
- D.Create an Amazon Elastic File System (Amazon EFS) file system to store all the custom libraries.

Answer: C**Explanation:**

The most efficient solution is to use a Lambda layer to store the common libraries, update them in one place, and reference them from each Lambda function that requires them.

The Lambda layer of option C provides a simpler solution without the need to introduce an additional Code Artifact service.

CertyIQ**Question: 109**

A developer wants to use AWS Elastic Beanstalk to test a new version of an application in a test environment.

Which deployment method offers the FASTEST deployment?

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

Answer: D**Explanation:**

The "All at once" deployment method deploys the new version of the application to all instances simultaneously. It updates all instances of the environment in a short period of time, resulting in the fastest overall deployment.

Reference:

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

CertyIQ**Question: 110**

A company is providing read access to objects in an Amazon S3 bucket for different customers. The company uses IAM permissions to restrict access to the S3 bucket. The customers can access only their own files.

Due to a regulation requirement, the company needs to enforce encryption in transit for interactions with Amazon S3.

Which solution will meet these requirements?

- A.Add a bucket policy to the S3 bucket to deny S3 actions when the aws:SecureTransport condition is equal to false.
- B.Add a bucket policy to the S3 bucket to deny S3 actions when the s3:x-amz-acl condition is equal to public-read.
- C.Add an IAM policy to the IAM users to enforce the usage of the AWS SDK.
- D.Add an IAM policy to the IAM users that allows S3 actions when the s3:x-amz-acl condition is equal to bucket-owner-read.

Answer: A**Explanation:**

1. This solution enforces encryption in transit for interactions with Amazon S3 by denying access to the S3 bucket if the request is not made over an HTTPS connection. This condition can be enforced by using the "aws:SecureTransport" condition key in a bucket policy.
2. To enforce encryption in transit for interactions with Amazon S3, you can add a bucket policy to the S3 bucket that denies S3 actions when the aws:SecureTransport condition is equal to false. This condition checks whether the requests to S3 are made over a secure (HTTPS) connection.

Question: 111

CertyIQ

A company has an image storage web application that runs on AWS. The company hosts the application on Amazon EC2 instances in an Auto Scaling group. The Auto Scaling group acts as the target group for an Application Load Balancer (ALB) and uses an Amazon S3 bucket to store the images for sale.

The company wants to develop a feature to test system requests. The feature will direct requests to a separate target group that hosts a new beta version of the application.

Which solution will meet this requirement with the LEAST effort?

- Create a new Auto Scaling group and target group for the beta version of the application. Update the ALB routing rule with a condition that looks for a cookie named version that has a value of beta. Update the test system code to use this cookie to test the beta version of the application.
- Create a new ALB, Auto Scaling group, and target group for the beta version of the application. Configure an alternate Amazon Route 53 record for the new ALB endpoint. Use the alternate Route 53 endpoint in the test system requests to test the beta version of the application.
- Create a new ALB, Auto Scaling group, and target group for the beta version of the application. Use Amazon CloudFront with Lambda@Edge to determine which specific request will go to the new ALB. Use the CloudFront endpoint to send the test system requests to test the beta version of the application.
- Create a new Auto Scaling group and target group for the beta version of the application. Update the ALB routing rule with a condition that looks for a cookie named version that has a value of beta. Use Amazon CloudFront with Lambda@Edge to update the test system requests to add the required cookie when the requests go to the ALB.

Answer: A

Explanation:

- This solution will allow the company to direct requests to a separate target group that hosts the new beta version of the application without having to create a new ALB or use additional services such as Amazon Route 53 or Amazon CloudFront. Option D adds additional complexity and effort compared to option A, which simply involves updating the ALB routing rule with a condition that looks for a cookie named version that has a value of beta and updating the test system code to use this cookie to test the beta version of the application.
- Option A is the least effort. With option B, you have to additionally create a new ALB *and* also a new route 53 record. With option A, you can create a new listener based on HTTP header:
<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-update-rules.html> and it will fulfill the requirements. You will also need a new auto scaling group and target group with option A - but you also need this with option B as well, so option A is the least effort.

Question: 112

CertyIQ

A team is developing an application that is deployed on Amazon EC2 instances. During testing, the team receives an error. The EC2 instances are unable to access an Amazon S3 bucket.

Which steps should the team take to troubleshoot this issue? (Choose two.)

- Check whether the policy that is assigned to the IAM role that is attached to the EC2 instances grants access to Amazon S3.

- B.Check the S3 bucket policy to validate the access permissions for the S3 bucket.
- C.Check whether the policy that is assigned to the IAM user that is attached to the EC2 instances grants access to Amazon S3.
- D.Check the S3 Lifecycle policy to validate the permissions that are assigned to the S3 bucket.
- E.Check the security groups that are assigned to the EC2 instances. Make sure that a rule is not blocking the access to Amazon S3.

Answer: AB

Explanation:

- 1. Option A is correct because IAM roles are used to grant permissions to AWS services, such as EC2 instances, to access other AWS services, such as S3 buckets. The policy assigned to the IAM role attached to the EC2 instances should be checked to ensure that it grants access to the S3 bucket. Option B is also correct because the S3 bucket policy controls access to the S3 bucket. The S3 bucket policy should be checked to ensure that the access permissions are correctly configured.
- 2. A: Make sure EC2 instance profile has permission to access s3B: Make sure S3 resource policy allows the access from instance

Question: 113

CertyIQ

A developer is working on an ecommerce website. The developer wants to review server logs without logging in to each of the application servers individually. The website runs on multiple Amazon EC2 instances, is written in Python, and needs to be highly available.

How can the developer update the application to meet these requirements with MINIMUM changes?

- A.Rewrite the application to be cloud native and to run on AWS Lambda, where the logs can be reviewed in Amazon CloudWatch.
- B.Set up centralized logging by using Amazon OpenSearch Service, Logstash, and OpenSearch Dashboards.
- C.Scale down the application to one larger EC2 instance where only one instance is recording logs.
- D.Install the unified Amazon CloudWatch agent on the EC2 instances. Configure the agent to push the application logs to CloudWatch.

Answer: D

Explanation:

Option D is the best option because it requires minimum changes and leverages the existing infrastructure.

Question: 114

CertyIQ

A company is creating an application that processes .csv files from Amazon S3. A developer has created an S3 bucket. The developer has also created an AWS Lambda function to process the .csv files from the S3 bucket.

Which combination of steps will invoke the Lambda function when a .csv file is uploaded to Amazon S3? (Choose two.)

- A.Create an Amazon EventBridge rule. Configure the rule with a pattern to match the S3 object created event.
- B.Schedule an Amazon EventBridge rule to run a new Lambda function to scan the S3 bucket.
- C.Add a trigger to the existing Lambda function. Set the trigger type to EventBridge. Select the Amazon EventBridge rule.
- D.Create a new Lambda function to scan the S3 bucket for recently added S3 objects.
- E.Add S3 Lifecycle rules to invoke the existing Lambda function.

Answer: AC**Explanation:**

Option A is correct because an Amazon Event Bridge rule can be created to detect when an object is created in an S3 bucket. The rule should be configured with a pattern to match the S3 object created event. Option C is correct because the existing Lambda function can be updated with an Event Bridge trigger. The trigger type should be set to Event Bridge, and the Amazon Event Bridge rule created in step A should be selected.

Question: 115**CertyIQ**

A developer needs to build an AWS CloudFormation template that self-populates the AWS Region variable that deploys the CloudFormation template.

What is the MOST operationally efficient way to determine the Region in which the template is being deployed?

- A.Use the AWS::Region pseudo parameter.
- B.Require the Region as a CloudFormation parameter.
- C.Find the Region from the AWS::StackId pseudo parameter by using the Fn::Split intrinsic function.
- D.Dynamically import the Region by referencing the relevant parameter in AWS Systems Manager Parameter Store.

Answer: A**Explanation:**

- A. Use the AWS::Region pseudo parameter.

Reference:

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

Question: 116**CertyIQ**

A company has hundreds of AWS Lambda functions that the company's QA team needs to test by using the Lambda function URLs. A developer needs to configure the authentication of the Lambda functions to allow access so that the QA IAM group can invoke the Lambda functions by using the public URLs.

Which solution will meet these requirements?

- A.Create a CLI script that loops on the Lambda functions to add a Lambda function URL with the AWS_IAM auth type. Run another script to create an IAM identity-based policy that allows the lambda:InvokeFunctionUrl action to all the Lambda function Amazon Resource Names (ARNs). Attach the policy to the QA IAM group.
- B.Create a CLI script that loops on the Lambda functions to add a Lambda function URL with the NONE auth type. Run another script to create an IAM resource-based policy that allows the lambda:InvokeFunctionUrl action to all the Lambda function Amazon Resource Names (ARNs). Attach the policy to the QA IAM group.
- C.Create a CLI script that loops on the Lambda functions to add a Lambda function URL with the AWS_IAM auth type. Run another script to loop on the Lambda functions to create an IAM identity-based policy that allows the lambda:InvokeFunctionUrl action from the QA IAM group's Amazon Resource Name (ARN).
- D.Create a CLI script that loops on the Lambda functions to add a Lambda function URL with the NONE auth type. Run another script to loop on the Lambda functions to create an IAM resource-based policy that allows the lambda:InvokeFunctionUrl action from the QA IAM group's Amazon Resource Name (ARN).

Answer: A

Explanation:

Create a CLI script that loops on the Lambda functions to add a Lambda function URL with the AWS_IAM auth type. Run another script to create an IAM identity-based policy that allows the lambda: Invoke Function Url action to all the Lambda function Amazon Resource Names (ARNs). Attach the policy to the QA IAM group

CertyIQ**Question: 117**

A developer maintains a critical business application that uses Amazon DynamoDB as the primary data store. The DynamoDB table contains millions of documents and receives 30-60 requests each minute. The developer needs to perform processing in near-real time on the documents when they are added or updated in the DynamoDB table.

How can the developer implement this feature with the LEAST amount of change to the existing application code?

- A. Set up a cron job on an Amazon EC2 instance. Run a script every hour to query the table for changes and process the documents.
- B. Enable a DynamoDB stream on the table. Invoke an AWS Lambda function to process the documents.
- C. Update the application to send a PutEvents request to Amazon EventBridge. Create an EventBridge rule to invoke an AWS Lambda function to process the documents.
- D. Update the application to synchronously process the documents directly after the DynamoDB write.

Answer: B**Explanation:**

Option B is the best solution because it proposes enabling a DynamoDB stream on the table, which allows the developer to capture document-level changes in near-real time without modifying the application code. Then, the stream can be configured to invoke an AWS Lambda function to process the documents in near-real time. This solution requires minimal changes to the existing application code, and the Lambda function can be developed and deployed separately, enabling the developer to easily maintain and update it as needed.

CertyIQ**Question: 118**

A developer is writing an application for a company. The application will be deployed on Amazon EC2 and will use an Amazon RDS for Microsoft SQL Server database. The company's security team requires that database credentials are rotated at least weekly.

How should the developer configure the database credentials for this application?

- A. Create a database user. Store the user name and password in an AWS Systems Manager Parameter Store secure string parameter. Enable rotation of the AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter.
- B. Enable IAM authentication for the database. Create a database user for use with IAM authentication. Enable password rotation.
- C. Create a database user. Store the user name and password in an AWS Secrets Manager secret that has daily rotation enabled.
- D. Use the EC2 user data to create a database user. Provide the user name and password in environment variables to the application.

Answer: C**Explanation:**

option C: Create a database user. Store the user name and password in an AWS Secrets Manager secret that

has daily rotation enabled. This will allow the developer to securely store the database credentials and automatically rotate them at least weekly to meet the company's security requirements.

Question: 119

CertyIQ

A real-time messaging application uses Amazon API Gateway WebSocket APIs with backend HTTP service. A developer needs to build a feature in the application to identify a client that keeps connecting to and disconnecting from the WebSocket connection. The developer also needs the ability to remove the client.

Which combination of changes should the developer make to the application to meet these requirements? (Choose two.)

- A.Switch to HTTP APIs in the backend service.
- B.Switch to REST APIs in the backend service.
- C.Use the callback URL to disconnect the client from the backend service.
- D.Add code to track the client status in Amazon ElastiCache in the backend service.
- E.Implement \$connect and \$disconnect routes in the backend service.

Answer: CE

Explanation:

1. C => https://docs.aws.amazon.com/ko_kr/apigateway/latest/developerguide/apigateway-how-to-call-websocket-api-connections.html E => https://docs.aws.amazon.com/ko_kr/apigateway/latest/developerguide/apigateway-websocket-api-route-keys-connect-disconnect.html
2. I go with C and E.<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-websocket-api-route-keys-connect-disconnect.html><https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-how-to-call-websocket-api-connections.html>

Question: 120

CertyIQ

A developer has written code for an application and wants to share it with other developers on the team to receive feedback. The shared application code needs to be stored long-term with multiple versions and batch change tracking.

Which AWS service should the developer use?

- A.AWS CodeBuild
- B.Amazon S3
- C.AWS CodeCommit
- D.AWS Cloud9

Answer: C

Explanation:

option C, AWS CodeCommit.

Question: 121

CertyIQ

A company's developer is building a static website to be deployed in Amazon S3 for a production environment. The website integrates with an Amazon Aurora PostgreSQL database by using an AWS Lambda function. The website that is deployed to production will use a Lambda alias that points to a specific version of the Lambda function.

The company must rotate the database credentials every 2 weeks. Lambda functions that the company deployed previously must be able to use the most recent credentials.

Which solution will meet these requirements?

- A.Store the database credentials in AWS Secrets Manager. Turn on rotation. Write code in the Lambda function to retrieve the credentials from Secrets Manager.
- B.Include the database credentials as part of the Lambda function code. Update the credentials periodically and deploy the new Lambda function.
- C.Use Lambda environment variables. Update the environment variables when new credentials are available.
- D.Store the database credentials in AWS Systems Manager Parameter Store. Turn on rotation. Write code in the Lambda function to retrieve the credentials from Systems Manager Parameter Store.

Answer: A

Explanation:

Option A is the correct solution; Option D is also a valid solution, but it is not the best option since Secrets Manager provides built-in rotation, which ensures that the latest credentials are automatically updated. Additionally, AWS Systems Manager Parameter Store does not provide the ability to rotate secrets automatically.

Question: 122

CertyIQ

A developer is developing an application that uses signed requests (Signature Version 4) to call other AWS services. The developer has created a canonical request, has created the string to sign, and has calculated signing information.

Which methods could the developer use to complete a signed request? (Choose two.)

- A.Add the signature to an HTTP header that is named Authorization.
- B.Add the signature to a session cookie.
- C.Add the signature to an HTTP header that is named Authentication.
- D.Add the signature to a query string parameter that is named X-Amz-Signature.
- E.Add the signature to an HTTP header that is named WWW-Authenticate.

Answer: AD

Explanation:

- A. Add the signature to an HTTP header that is named Authorization.
- D. Add the signature to a query string parameter that is named X-Amz-Signature.

Reference:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/create-signed-request.html>

Question: 123

CertyIQ

A company must deploy all its Amazon RDS DB instances by using AWS CloudFormation templates as part of AWS CodePipeline continuous integration and continuous delivery (CI/CD) automation. The primary password for the DB instance must be automatically generated as part of the deployment process.

Which solution will meet these requirements with the LEAST development effort?

- A.Create an AWS Lambda-backed CloudFormation custom resource. Write Lambda code that generates a secure string. Return the value of the secure string as a data field of the custom resource response object. Use the CloudFormation Fn::GetAtt intrinsic function to get the value of the secure string. Use the value to create the DB instance.
- B.Use the AWS CodeBuild action of CodePipeline to generate a secure string by using the following AWS CLI command: aws secretsmanager get-random-password. Pass the generated secure string as a CloudFormation parameter with the NoEcho attribute set to true. Use the parameter reference to create the DB instance.
- C.Create an AWS Lambda-backed CloudFormation custom resource. Write Lambda code that generates a secure string. Return the value of the secure string as a data field of the custom resource response object. Use the CloudFormation Fn::GetAtt intrinsic function to get a value of the secure string. Create secrets in AWS Secrets Manager. Use the secretsmanager dynamic reference to use the value stored in the secret to create the DB instance.
- D.Use the AWS::SecretsManager::Secret resource to generate a secure string. Store the secure string as a secret in AWS Secrets Manager. Use the secretsmanager dynamic reference to use the value stored in the secret to create the DB instance.

Answer: D

Explanation:

The correct option is D. Create the password from secrets manager.

CertyIQ

Question: 124

An organization is storing large files in Amazon S3, and is writing a web application to display meta-data about the files to end-users. Based on the metadata a user selects an object to download. The organization needs a mechanism to index the files and provide single-digit millisecond latency retrieval for the metadata.

What AWS service should be used to accomplish this?

- A.Amazon DynamoDB
- B.Amazon EC2
- C.AWS Lambda
- D.Amazon RDS

Answer: A

Explanation:

In this scenario, the metadata about the files can be stored in a DynamoDB table with a primary key based on the metadata attributes. This would enable the organization to quickly query and retrieve metadata about the files in real-time, with single-digit millisecond latency.

CertyIQ

Question: 125

A developer is creating an AWS Serverless Application Model (AWS SAM) template. The AWS SAM template contains the definition of multiple AWS Lambda functions, an Amazon S3 bucket, and an Amazon CloudFront distribution. One of the Lambda functions runs on Lambda@Edge in the CloudFront distribution. The S3 bucket is configured as an origin for the CloudFront distribution.

When the developer deploys the AWS SAM template in the eu-west-1 Region, the creation of the stack fails.

Which of the following could be the reason for this issue?

- A.CloudFront distributions can be created only in the us-east-1 Region.
- B.Lambda@Edge functions can be created only in the us-east-1 Region.
- C.A single AWS SAM template cannot contain multiple Lambda functions.
- D.The CloudFront distribution and the S3 bucket cannot be created in the same Region.

Answer: B

Explanation:

It must be deployed to a region where Lambda @ Edge is supported, such as us-east-1.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/edge-functions-restrictions.html> The Lambda function must be in the US East (N. Virginia) Region.

Question: 126

CertyIQ

A developer is integrating Amazon ElastiCache in an application. The cache will store data from a database. The cached data must populate real-time dashboards.

Which caching strategy will meet these requirements?

- A.A read-through cache
- B.A write-behind cache
- C.A lazy-loading cache
- D.A write-through cache

Answer: D

Explanation:

The best caching strategy for populating real-time dashboards using Amazon Elastic Cache would be a write-through caching strategy. In this strategy, when new data is written to the database, it is also written to the cache. This ensures that the most current data is always available in the cache for the real-time dashboards to access, reducing the latency of the data retrieval. Additionally, using a write-through cache ensures that data consistency is maintained between the database and the cache, as any changes to the data are written to both locations simultaneously.

Question: 127

CertyIQ

A developer is creating an AWS Lambda function. The Lambda function needs an external library to connect to a third-party solution. The external library is a collection of files with a total size of 100 MB. The developer needs to make the external library available to the Lambda execution environment and reduce the Lambda package space.

Which solution will meet these requirements with the LEAST operational overhead?

- A.Create a Lambda layer to store the external library. Configure the Lambda function to use the layer.
- B.Create an Amazon S3 bucket. Upload the external library into the S3 bucket. Mount the S3 bucket folder in the Lambda function. Import the library by using the proper folder in the mount point.

C.Load the external library to the Lambda function's /tmp directory during deployment of the Lambda package. Import the library from the /tmp directory.

D.Create an Amazon Elastic File System (Amazon EFS) volume. Upload the external library to the EFS volume. Mount the EFS volume in the Lambda function. Import the library by using the proper folder in the mount point.

Answer: A

Explanation:

1. Create a Lambda layer to store the external library. Configure the Lambda function to use the layer. This will allow the developer to make the external library available to the Lambda execution environment without having to include it in the Lambda package, which will reduce the Lambda package space. Using a Lambda layer is a simple and straightforward solution that requires minimal operational overhead.
2. By creating a Lambda layer, you can separate the external library from the Lambda function code itself and make it available to multiple functions. This approach offers the following benefits:

Question: 128

CertyIQ

A company has a front-end application that runs on four Amazon EC2 instances behind an Elastic Load Balancer (ELB) in a production environment that is provisioned by AWS Elastic Beanstalk. A developer needs to deploy and test new application code while updating the Elastic Beanstalk platform from the current version to a newer version of Node.js. The solution must result in zero downtime for the application.

Which solution meets these requirements?

- A.Clone the production environment to a different platform version. Deploy the new application code, and test it. Swap the environment URLs upon verification.
- B.Deploy the new application code in an all-at-once deployment to the existing EC2 instances. Test the code. Redeploy the previous code if verification fails.
- C.Perform an immutable update to deploy the new application code to new EC2 instances. Serve traffic to the new instances after they pass health checks.
- D.Use a rolling deployment for the new application code. Apply the code to a subset of EC2 instances until the tests pass. Redeploy the previous code if the tests fail.

Answer: C

Explanation:

1. Option C is the correct solution that meets the requirements. Performing an immutable update to deploy the new application code to new EC2 instances and serving traffic to the new instances after they pass health checks will ensure zero downtime for the application. Option A would work but cloning the production environment to a different platform version will result in a longer deployment time and can impact the cost of the environment.
2. Key terminology in question is "Test". So it should be immutable for quick rollback in case of test not working.

Question: 129

CertyIQ

A developer is creating an AWS Lambda function. The Lambda function will consume messages from an Amazon Simple Queue Service (Amazon SQS) queue. The developer wants to integrate unit testing as part of the function's continuous integration and continuous delivery (CI/CD) process.

How can the developer unit test the function?

- A.Create an AWS CloudFormation template that creates an SQS queue and deploys the Lambda function. Create a stack from the template during the CI/CD process. Invoke the deployed function. Verify the output.
- B.Create an SQS event for tests. Use a test that consumes messages from the SQS queue during the function's

CI/CD process.

C.Create an SQS queue for tests. Use this SQS queue in the application's unit test. Run the unit tests during the CI/CD process.

D.Use the aws lambda invoke command with a test event during the CI/CD process.

Answer: C

Explanation:

Unit testing is a type of testing that verifies the correctness of individual units of source code, typically functions or methods. When unit testing a Lambda function that interacts with Amazon SQS, you can create a separate test SQS queue that the Lambda function interacts with during testing. You would then validate the behaviour of the function based on its interactions with the test queue. This approach isolates the function's behaviour from the rest of the system, which is a key principle of unit testing. Option A is incorrect because AWS Cloud Formation is typically used for infrastructure deployment, not for unit testing. Option B is incorrect because it does not actually test the function; it only creates an event. Option D is incorrect because the 'aws lambda invoke' command is used to manually trigger a Lambda function, but doesn't necessarily facilitate testing the function's behaviour when consuming messages from an SQS queue.

C. Unit test should be isolated.

<https://aws.amazon.com/blogs/devops/unit-testing-aws-lambda-with-python-and-mock-aws-services/>

Question: 130

CertyIQ

A developer is working on a web application that uses Amazon DynamoDB as its data store. The application has two DynamoDB tables: one table that is named artists and one table that is named songs. The artists table has artistName as the partition key. The songs table has songName as the partition key and artistName as the sort key.

The table usage patterns include the retrieval of multiple songs and artists in a single database operation from the webpage. The developer needs a way to retrieve this information with minimal network traffic and optimal application performance.

Which solution will meet these requirements?

A.Perform a BatchGetItem operation that returns items from the two tables. Use the list of songName/artistName keys for the songs table and the list of artistName key for the artists table.

B.Create a local secondary index (LSI) on the songs table that uses artistName as the partition key. Perform a query operation for each artistName on the songs table that filters by the list of songName. Perform a query operation for each artistName on the artists table.

C.Perform a BatchGetItem operation on the songs table that uses the songName/artistName keys. Perform a BatchGetItem operation on the artists table that uses artistName as the key.

D.Perform a Scan operation on each table that filters by the list of songName/artistName for the songs table and the list of artistName in the artists table.

Answer: A

Explanation:

The correct answer is A. Batch GetItem can return one or multiple items from one or more tables. the

Reference:

https://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_BatchGetItem.html

Question: 131

CertyIQ

A company is developing an ecommerce application that uses Amazon API Gateway APIs. The application uses AWS Lambda as a backend. The company needs to test the code in a dedicated, monitored test environment before the company releases the code to the production environment.

Which solution will meet these requirements?

- A.Use a single stage in API Gateway. Create a Lambda function for each environment. Configure API clients to send a query parameter that indicates the environment and the specific Lambda function.
- B.Use multiple stages in API Gateway. Create a single Lambda function for all environments. Add different code blocks for different environments in the Lambda function based on Lambda environment variables.
- C.Use multiple stages in API Gateway. Create a Lambda function for each environment. Configure API Gateway stage variables to route traffic to the Lambda function in different environments.
- D.Use a single stage in API Gateway. Configure API clients to send a query parameter that indicates the environment. Add different code blocks for different environments in the Lambda function to match the value of the query parameter.

Answer: C**Explanation:**

The answer is C - we should create multiple stages and different Lambdas that will be utilised based on API Gateway stages variables.

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

Question: 132

CertyIQ

A developer creates an AWS Lambda function that retrieves and groups data from several public API endpoints. The Lambda function has been updated and configured to connect to the private subnet of a VPC. An internet gateway is attached to the VPC. The VPC uses the default network ACL and security group configurations.

The developer finds that the Lambda function can no longer access the public API. The developer has ensured that the public API is accessible, but the Lambda function cannot connect to the API

How should the developer fix the connection issue?

- A.Ensure that the network ACL allows outbound traffic to the public internet.
- B.Ensure that the security group allows outbound traffic to the public internet.
- C.Ensure that outbound traffic from the private subnet is routed to a public NAT gateway.
- D.Ensure that outbound traffic from the private subnet is routed to a new internet gateway.

Answer: C**Explanation:**

1. When a Lambda function is configured to connect to a VPC, it loses its default internet access. To allow the Lambda function to access the public internet, it must be connected to a private subnet in the VPC that is configured to route its traffic through a NAT Gateway (Network Address Translation Gateway). The Internet Gateway is usually used to provide internet access to resources in the public subnet, but for resources in the private subnet, a NAT Gateway is required.
2. NAT Gateway from a public subnet is required.

Question: 133

CertyIQ

A developer needs to store configuration variables for an application. The developer needs to set an expiration date and time for the configuration. The developer wants to receive notifications before the configuration expires.

Which solution will meet these requirements with the LEAST operational overhead?

- A.Create a standard parameter in AWS Systems Manager Parameter Store. Set Expiration and ExpirationNotification policy types.
- B.Create a standard parameter in AWS Systems Manager Parameter Store. Create an AWS Lambda function to expire the configuration and to send Amazon Simple Notification Service (Amazon SNS) notifications.
- C.Create an advanced parameter in AWS Systems Manager Parameter Store. Set Expiration and ExpirationNotification policy types.
- D.Create an advanced parameter in AWS Systems Manager Parameter Store. Create an Amazon EC2 instance with a cron job to expire the configuration and to send notifications.

Answer: C**Explanation:**

1. You can't set expiration policy on standard parameter
2. C is correct. You have to use "advanced parameter in AWS Systems Manager Parameter Store" to be able to Set Expiration and ExpirationNotification policy types.

Question: 134

CertyIQ

A company is developing a serverless application that consists of various AWS Lambda functions behind Amazon API Gateway APIs. A developer needs to automate the deployment of Lambda function code. The developer will deploy updated Lambda functions with AWS CodeDeploy. The deployment must minimize the exposure of potential errors to end users. When the application is in production, the application cannot experience downtime outside the specified maintenance window.

Which deployment configuration will meet these requirements with the LEAST deployment time?

- A.Use the AWS CodeDeploy in-place deployment configuration for the Lambda functions. Shift all traffic immediately after deployment.
- B.Use the AWS CodeDeploy linear deployment configuration to shift 10% of the traffic every minute.
- C.Use the AWS CodeDeploy all-at-once deployment configuration to shift all traffic to the updated versions immediately.
- D.Use the AWS CodeDeploy predefined canary deployment configuration to shift 10% of the traffic immediately and shift the remaining traffic after 5 minutes.

Answer: D**Explanation:**

1. Canary is faster than linear in this case.
2. Canary deployment

Question: 135

CertyIQ

A company created four AWS Lambda functions that connect to a relational database server that runs on an Amazon RDS instance. A security team requires the company to automatically change the database password every 30 days.

Which solution will meet these requirements MOST securely?

- A.Store the database credentials in the environment variables of the Lambda function. Deploy the Lambda

function with the new credentials every 30 days.

B.Store the database credentials in AWS Secrets Manager. Configure a 30-day rotation schedule for the credentials.

C.Store the database credentials in AWS Systems Manager Parameter Store secure strings. Configure a 30-day schedule for the secure strings.

D.Store the database credentials in an Amazon S3 bucket that uses server-side encryption with customer-provided encryption keys (SSE-C). Configure a 30-day key rotation schedule for the customer key.

Answer: B

Explanation:

1. The most secure and automated way to handle database credential rotation is to use AWS Secrets Manager. Secrets Manager can automatically rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. You can configure Secrets Manager to automatically rotate the secrets for you according to a schedule you specify, making it easier to adhere to best practices for security.

2. Secrets Manager supports auto rotation. Systems Manager does not do that.

CertyIQ

A developer is setting up a deployment pipeline. The pipeline includes an AWS CodeBuild build stage that requires access to a database to run integration tests. The developer is using a buildspec.yml file to configure the database connection. Company policy requires automatic rotation of all database credentials.

Which solution will handle the database credentials MOST securely?

A.Retrieve the credentials from variables that are hardcoded in the buildspec.yml file. Configure an AWS Lambda function to rotate the credentials.

B.Retrieve the credentials from an environment variable that is linked to a SecureString parameter in AWS Systems Manager Parameter Store. Configure Parameter Store for automatic rotation.

C.Retrieve the credentials from an environment variable that is linked to an AWS Secrets Manager secret. Configure Secrets Manager for automatic rotation.

D.Retrieve the credentials from an environment variable that contains the connection string in plaintext. Configure an Amazon EventBridge event to rotate the credentials.

Answer: C

Explanation:

1. Secure + Rotation are key words for Secrets Manager

2. C is correct.Explanation: "requires automatic rotation of all database credentials" => "Secrets Manager for automatic rotation."With the Systems Manager Parameter Store, you have to do that manually.

CertyIQ

A company is developing a serverless multi-tier application on AWS. The company will build the serverless logic tier by using Amazon API Gateway and AWS Lambda.

While the company builds the logic tier, a developer who works on the frontend of the application must develop integration tests. The tests must cover both positive and negative scenarios, depending on success and error HTTP status codes.

Which solution will meet these requirements with the LEAST effort?

A.Set up a mock integration for API methods in API Gateway. In the integration request from Method Execution, add simple logic to return either a success or error based on HTTP status code. In the integration response, add messages that correspond to the HTTP status codes.

B.Create two mock integration resources for API methods in API Gateway. In the integration request, return a

success HTTP status code for one resource and an error HTTP status code for the other resource. In the integration response, add messages that correspond to the HTTP status codes.

C.Create Lambda functions to perform tests. Add simple logic to return either success or error, based on the HTTP status codes. Build an API Gateway Lambda integration. Select appropriate Lambda functions that correspond to the HTTP status codes.

D.Create a Lambda function to perform tests. Add simple logic to return either success or error-based HTTP status codes. Create a mock integration in API Gateway. Select the Lambda function that corresponds to the HTTP status codes.

Answer: A

Explanation:

1. A is correct (with the LEAST effort)"API Gateway supports mock integrations for API methods""As an API developer, you decide how API Gateway responds to a mock integration request. For this, you configure the method's integration request and integration response to associate a response with a given status code.

"<https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-mock-integration.html>

2. A because set up a mock integration for API methods in API Gateway with the least effort.

CertyIQ

Question: 138

Users are reporting errors in an application. The application consists of several microservices that are deployed on Amazon Elastic Container Service (Amazon ECS) with AWS Fargate.

Which combination of steps should a developer take to fix the errors? (Choose two.)

A.Deploy AWS X-Ray as a sidecar container to the microservices. Update the task role policy to allow access to the X-Ray API.

B.Deploy AWS X-Ray as a daemonset to the Fargate cluster. Update the service role policy to allow access to the X-Ray API.

C.Instrument the application by using the AWS X-Ray SDK. Update the application to use the PutXRayTrace API call to communicate with the X-Ray API.

D.Instrument the application by using the AWS X-Ray SDK. Update the application to communicate with the X-Ray daemon.

E.Instrument the ECS task to send the stdout and stderr output to Amazon CloudWatch Logs. Update the task role policy to allow the cloudwatch:PullLogs action.

Answer: D

Explanation:

1. D and E Option D: Instrumenting the application using the AWS X-Ray SDK is essential for collecting traces and telemetry data. The X-Ray SDK helps you identify bottlenecks, errors, and other issues within your microservices. Communicating with the X-Ray daemon allows your microservices to send trace data to X-Ray for analysis and visualization. This requires minimal configuration and is efficient for capturing and analyzing traces. Option E: Instrumenting the ECS task to send the application's standard output (stdout) and standard error (stderr) logs to Amazon CloudWatch Logs provides visibility into the application's behavior, errors, and issues. Updating the task role policy to allow the cloudwatch:PullLogs action ensures that the ECS task has the necessary permissions to access and send logs to CloudWatch Logs.

CertyIQ

Question: 139

A developer is creating an application for a company. The application needs to read the file doc.txt that is placed in the root folder of an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET. The company's security team requires the principle of least privilege to be applied to the application's IAM policy.

Which IAM policy statement will meet these security requirements?

- A.
- ```
{
 "Action": [
 "s3:GetObject"
],
 "Effect": "Allow",
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/doc.txt"
}

{
 "Action": [
 "s3:*"
],
 "Effect": "Allow",
 "Resource": "*"
}

B.

{
 "Action": [
 "s3:GetObject"
],
 "Effect": "Allow",
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
}

C.

D.

{
 "Action": [
 "s3:*"
],
 "Effect": "Allow",
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/doc.txt"
}
```
- C.
- D.

**Answer: A**

**Explanation:**

1. Only read permission for the file
2. Only allow to get this one file. A

**Question: 140**

A company has an application that uses AWS CodePipeline to automate its continuous integration and continuous

**CertyIQ**

delivery (CI/CD) workflow. The application uses AWS CodeCommit for version control. A developer who was working on one of the tasks did not pull the most recent changes from the main branch. A week later, the developer noticed merge conflicts.

How can the developer resolve the merge conflicts in the developer's branch with the LEAST development effort?

- A.Clone the repository. Create a new branch. Update the branch with the changes.
- B.Create a new branch. Apply the changes from the previous branch.
- C.Use the Commit Visualizer view to compare the commits when a feature was added. Fix the merge conflicts.
- D.Stop the pull from the main branch to the feature branch. Rebase the feature branch from the main branch.

**Answer: D**

**Explanation:**

D is the best approach for resolving the merge conflicts with minimal development effort. Here's how it works:  
Stop Pull from Main: By stopping the pull from the main branch to the feature branch, the developer can prevent the introduction of new conflicts while they are resolving the existing ones. Rebase the Feature Branch: After stopping the pull, the developer can rebase the feature branch onto the main branch. This essentially replays the feature branch's changes on top of the main branch's latest changes. This allows the developer to resolve conflicts one commit at a time, addressing any conflicts that arise from the difference between the feature branch and the main branch.

**Question: 141**

**CertyIQ**

A developer wants to add request validation to a production environment Amazon API Gateway API. The developer needs to test the changes before the API is deployed to the production environment. For the test, the developer will send test requests to the API through a testing tool.

Which solution will meet these requirements with the LEAST operational overhead?

- A.Export the existing API to an OpenAPI file. Create a new API. Import the OpenAPI file. Modify the new API to add request validation. Perform the tests. Modify the existing API to add request validation. Deploy the existing API to production.
- B.Modify the existing API to add request validation. Deploy the updated API to a new API Gateway stage. Perform the tests. Deploy the updated API to the API Gateway production stage.
- C.Create a new API. Add the necessary resources and methods, including new request validation. Perform the tests. Modify the existing API to add request validation. Deploy the existing API to production
- D.Clone the existing API. Modify the new API to add request validation. Perform the tests. Modify the existing API to add request validation. Deploy the existing API to production.

**Answer: B**

**Explanation:**

In this option, you are making changes directly to the existing API, adding request validation. Then, you deploy the updated API to a new API Gateway stage, which allows you to test the changes without affecting the production environment. After performing the tests and ensuring everything works as expected, you can then deploy the updated API to the production stage, thus minimizing operational overhead

**Question: 142**

**CertyIQ**

An online food company provides an Amazon API Gateway HTTP API to receive orders for partners. The API is

integrated with an AWS Lambda function. The Lambda function stores the orders in an Amazon DynamoDB table.

The company expects to onboard additional partners. Some of the partners require additional Lambda functions to receive orders. The company has created an Amazon S3 bucket. The company needs to store all orders and updates in the S3 bucket for future analysis.

How can the developer ensure that all orders and updates are stored to Amazon S3 with the LEAST development effort?

- A.Create a new Lambda function and a new API Gateway API endpoint. Configure the new Lambda function to write to the S3 bucket. Modify the original Lambda function to post updates to the new API endpoint.
- B.Use Amazon Kinesis Data Streams to create a new data stream. Modify the Lambda function to publish orders to the data stream. Configure the data stream to write to the S3 bucket.
- C.Enable DynamoDB Streams on the DynamoDB table. Create a new Lambda function. Associate the stream's Amazon Resource Name (ARN) with the Lambda function. Configure the Lambda function to write to the S3 bucket as records appear in the table's stream.
- D.Modify the Lambda function to publish to a new Amazon Simple Notification Service (Amazon SNS) topic as the Lambda function receives orders. Subscribe a new Lambda function to the topic. Configure the new Lambda function to write to the S3 bucket as updates come through the topic.

**Answer: C**

**Explanation:**

By enabling DynamoDB Streams on the DynamoDB table, you can capture changes (orders and updates) to the table. Whenever a new order or an update is made to the table, a stream record is generated. You can then create a new Lambda function, associate the stream's ARN with this Lambda function, and configure it to write the stream records (orders and updates) to the S3 bucket. This approach leverages built-in features of DynamoDB and Lambda, minimizing the development effort required to achieve the desired outcome.

**CertyIQ**

**Question: 143**

A company's website runs on an Amazon EC2 instance and uses Auto Scaling to scale the environment during peak times. Website users across the world are experiencing high latency due to static content on the EC2 instance, even during non-peak hours.

Which combination of steps will resolve the latency issue? (Choose two.)

- A.Double the Auto Scaling group's maximum number of servers.
- B.Host the application code on AWS Lambda.
- C.Scale vertically by resizing the EC2 instances.
- D.Create an Amazon CloudFront distribution to cache the static content.
- E.Store the application's static content in Amazon S3.

**Answer: DE**

**Explanation:**

Option (D), creating an Amazon Cloud Front distribution to cache static content, is the most recommended solution. Cloud Front is a global content delivery network (CDN) that can cache static content on servers distributed around the world. This can help significantly reduce latency for users around the world. Option (E), storing your application's static content in Amazon S3, can also help reduce latency. S3 is a high-performance object storage service that can be used to store static content.

**Question: 144**

CertyIQ

A company has an Amazon S3 bucket containing premier content that it intends to make available to only paid subscribers of its website. The S3 bucket currently has default permissions of all objects being private to prevent inadvertent exposure of the premier content to non-paying website visitors.

How can the company limit the ability to download a premier content file in the S3 bucket to paid subscribers only?

- A.Apply a bucket policy that allows anonymous users to download the content from the S3 bucket.
- B.Generate a pre-signed object URL for the premier content file when a paid subscriber requests a download.
- C.Add a bucket policy that requires multi-factor authentication for requests to access the S3 bucket objects.
- D.Enable server-side encryption on the S3 bucket for data protection against the non-paying website visitors.

**Answer: B****Explanation:**

The correct answer is (B).By generating a pre-signed object URL for the main content file when a paid subscriber requests a download, the company can control who can download the file. The pre-signed object URL will be valid for a limited period of time and can only be used by the paid subscriber who requested the download.

**Question: 145**

CertyIQ

A developer is creating an AWS Lambda function that searches for items from an Amazon DynamoDB table that contains customer contact information. The DynamoDB table items have the customer's email\_address as the partition key and additional properties such as customer\_type, name and job\_title.

The Lambda function runs whenever a user types a new character into the customer\_type text input. The developer wants the search to return partial matches of all the email\_address property of a particular customer\_type. The developer does not want to recreate the DynamoDB table.

What should the developer do to meet these requirements?

- A.Add a global secondary index (GSI) to the DynamoDB table with customer\_type as the partition key and email\_address as the sort key. Perform a query operation on the GSI by using the begins\_with key condition expression with the email\_address property.
- B.Add a global secondary index (GSI) to the DynamoDB table with email\_address as the partition key and customer\_type as the sort key. Perform a query operation on the GSI by using the begins\_with key condition expression with the email\_address property.
- C.Add a local secondary index (LSI) to the DynamoDB table with customer\_type as the partition key and email\_address as the sort key. Perform a query operation on the LSI by using the begins\_with key condition expression with the email\_address property.
- D.Add a local secondary index (LSI) to the DynamoDB table with job\_title as the partition key and email\_address as the sort key. Perform a query operation on the LSI by using the begins\_with key condition expression with the email\_address property.

**Answer: A****Explanation:**

The correct answer is (A).By adding a global secondary index (GSI) to the DynamoDB table with customer\_type as the partition key and email\_address as the sort key, the developer can perform a query operation on the GSI using the Begins\_ with key condition expression with the email\_address property. This will return partial matches of all email\_address properties of a specific customer\_type.

**Question: 146**

CertyIQ

A developer is building an application that uses AWS API Gateway APIs, AWS Lambda functions, and AWS DynamoDB tables. The developer uses the AWS Serverless Application Model (AWS SAM) to build and run serverless applications on AWS. Each time the developer pushes changes for only to the Lambda functions, all the artifacts in the application are rebuilt.

The developer wants to implement AWS SAM Accelerate by running a command to only redeploy the Lambda functions that have changed.

Which command will meet these requirements?

- A.sam deploy --force-upload
- B.sam deploy --no-execute-changeset
- C.sam package
- D.sam sync --watch

**Answer: D****Explanation:**

The correct answer is (D).The sam sync --watch command will only deploy the Lambda functions that have changed. This command uses AWS SAM Accelerate to compare the local versions of your Lambda functions to the versions deployed in AWS. If there are differences, the command deploys only the changed Lambda functions.

**Question: 147**

CertyIQ

A developer is building an application that gives users the ability to view bank accounts from multiple sources in a single dashboard. The developer has automated the process to retrieve API credentials for these sources. The process invokes an AWS Lambda function that is associated with an AWS CloudFormation custom resource.

The developer wants a solution that will store the API credentials with minimal operational overhead.

Which solution will meet these requirements in the MOST secure way?

- A.Add an AWS Secrets Manager GenerateSecretString resource to the CloudFormation template. Set the value to reference new credentials for the CloudFormation resource.
- B.Use the AWS SDK ssm:PutParameter operation in the Lambda function from the existing custom resource to store the credentials as a parameter. Set the parameter value to reference the new credentials. Set the parameter type to SecureString.
- C.Add an AWS Systems Manager Parameter Store resource to the CloudFormation template. Set the CloudFormation resource value to reference the new credentials. Set the resource NoEcho attribute to true.
- D.Use the AWS SDK ssm:PutParameter operation in the Lambda function from the existing custom resource to store the credentials as a parameter. Set the parameter value to reference the new credentials. Set the parameter NoEcho attribute to true.

**Answer: B****Explanation:**

Answer is B A is not correct as the requirement asked to store API credentials, Generate Secret String will create a random string as password. C the API credential will be retrieved by the Lambda function, it is unavailable to the template. D no echo is a attribute of cloud formation template.

**Question: 149****CertyIQ**

An organization is using Amazon CloudFront to ensure that its users experience low-latency access to its web application. The organization has identified a need to encrypt all traffic between users and CloudFront, and all traffic between CloudFront and the web application.

How can these requirements be met? (Choose two.)

- A.Use AWS KMS to encrypt traffic between CloudFront and the web application.
- B.Set the Origin Protocol Policy to “HTTPS Only”.
- C.Set the Origin’s HTTP Port to 443.
- D.Set the Viewer Protocol Policy to “HTTPS Only” or “Redirect HTTP to HTTPS”.
- E.Enable the CloudFront option Restrict Viewer Access.

**Answer: BD****Explanation:**

The correct answers are (B) and (D).To meet the requirement to encrypt all traffic between users and Cloud Front, your organization must set the Viewer Protocol Policy to “HTTPS Only” or “Redirect HTTP to HTTPS”. This will force users to use HTTPS to connect to Cloud Front. To meet the requirement to encrypt all traffic between Cloud Front and the web application, your organization must set the Origin Protocol Policy to “HTTPS Only”. This will force Cloud Front to use HTTPS to connect to the web application.

**Question: 150****CertyIQ**

A developer is planning to migrate on-premises company data to Amazon S3. The data must be encrypted, and the encryption keys must support automatic annual rotation. The company must use AWS Key Management Service (AWS KMS) to encrypt the data.

Which type of keys should the developer use to meet these requirements?

- A.Amazon S3 managed keys
- B.Symmetric customer managed keys with key material that is generated by AWS
- C.Asymmetric customer managed keys with key material that is generated by AWS
- D.Symmetric customer managed keys with imported key material

**Answer: A****Explanation:**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingServerSideEncryption.html>

A) Amazon S3 Managed Keys [https://docs.aws.amazon.com/pt\\_br/AmazonS3/latest/userguide/serv-side-encryption.html](https://docs.aws.amazon.com/pt_br/AmazonS3/latest/userguide/serv-side-encryption.html)

**Question: 151****CertyIQ**

A team of developers is using an AWS CodePipeline pipeline as a continuous integration and continuous delivery (CI/CD) mechanism for a web application. A developer has written unit tests to programmatically test the functionality of the application code. The unit tests produce a test report that shows the results of each individual

check. The developer now wants to run these tests automatically during the CI/CD process.

Which solution will meet this requirement with the LEAST operational effort?

- A. Write a Git pre-commit hook that runs the tests before every commit. Ensure that each developer who is working on the project has the pre-commit hook installed locally. Review the test report and resolve any issues before pushing changes to AWS CodeCommit.
- B. Add a new stage to the pipeline. Use AWS CodeBuild as the provider. Add the new stage after the stage that deploys code revisions to the test environment. Write a buildspec that fails the CodeBuild stage if any test does not pass. Use the test reports feature of CodeBuild to integrate the report with the CodeBuild console. View the test results in CodeBuild. Resolve any issues.
- C. Add a new stage to the pipeline. Use AWS CodeBuild as the provider. Add the new stage before the stage that deploys code revisions to the test environment. Write a buildspec that fails the CodeBuild stage if any test does not pass. Use the test reports feature of CodeBuild to integrate the report with the CodeBuild console. View the test results in CodeBuild. Resolve any issues.
- D. Add a new stage to the pipeline. Use Jenkins as the provider. Configure CodePipeline to use Jenkins to run the unit tests. Write a Jenkinsfile that fails the stage if any test does not pass. Use the test report plugin for Jenkins to integrate the report with the Jenkins dashboard. View the test results in Jenkins. Resolve any issues.

**Answer: C**

**Explanation:**

C is correct. Typical consists of stages are. Build -> Test -> Deploy(test) -> Load Test -> and others

**Question: 153**

**CertyIQ**

A company uses a custom root certificate authority certificate chain (Root CA Cert) that is 10 KB in size to generate SSL certificates for its on-premises HTTPS endpoints. One of the company's cloud-based applications has hundreds of AWS Lambda functions that pull data from these endpoints. A developer updated the trust store of the Lambda execution environment to use the Root CA Cert when the Lambda execution environment is initialized. The developer bundled the Root CA Cert as a text file in the Lambda deployment bundle.

After 3 months of development, the Root CA Cert is no longer valid and must be updated. The developer needs a more efficient solution to update the Root CA Cert for all deployed Lambda functions. The solution must not include rebuilding or updating all Lambda functions that use the Root CA Cert. The solution must also work for all development, testing, and production environments. Each environment is managed in a separate AWS account.

Which combination of steps should the developer take to meet these requirements MOST cost-effectively? (Choose two.)

- A. Store the Root CA Cert as a secret in AWS Secrets Manager. Create a resource-based policy. Add IAM users to allow access to the secret.
- B. Store the Root CA Cert as a SecureString parameter in AWS Systems Manager Parameter Store. Create a resource-based policy. Add IAM users to allow access to the policy.
- C. Store the Root CA Cert in an Amazon S3 bucket. Create a resource-based policy to allow access to the bucket.
- D. Refactor the Lambda code to load the Root CA Cert from the Root CA Cert's location. Modify the runtime trust store inside the Lambda function handler.
- E. Refactor the Lambda code to load the Root CA Cert from the Root CA Cert's location. Modify the runtime trust store outside the Lambda function handler.

**Answer: BE**

**Explanation:**

B. AWS Systems Manager Parameter Store can store data both in plain text and encrypted format (using the SecureString type). It's a cost-effective solution for centralized configuration management across

environments and accounts. E. Modifying the runtime trust store outside the Lambda function handler ensures that the trust store is modified only once when the Lambda container is initialized, making it a more efficient approach than option D where it's initialized in every lambda function.

### Question: 154

CertyIQ

A developer maintains applications that store several secrets in AWS Secrets Manager. The applications use secrets that have changed over time. The developer needs to identify required secrets that are still in use. The developer does not want to cause any application downtime.

What should the developer do to meet these requirements?

- A.Configure an AWS CloudTrail log file delivery to an Amazon S3 bucket. Create an Amazon CloudWatch alarm for the GetSecretValue Secrets Manager API operation requests.
- B.Create a secretsmanager-secret-unused AWS Config managed rule. Create an Amazon EventBridge rule to initiate notifications when the AWS Config managed rule is met.
- C.Deactivate the applications secrets and monitor the applications error logs temporarily.
- D.Configure AWS X-Ray for the applications. Create a sampling rule to match the GetSecretValue Secrets Manager API operation requests.

**Answer: B**

**Explanation:**

Create a secrets manager-secret-unused AWS Config managed rule. Create an Amazon Event Bridge rule to initiate notifications when the AWS Config managed rule is met.

### Question: 155

CertyIQ

A developer is writing a serverless application that requires an AWS Lambda function to be invoked every 10 minutes.

What is an automated and serverless way to invoke the function?

- A.Deploy an Amazon EC2 instance based on Linux, and edit its /etc/crontab file by adding a command to periodically invoke the Lambda function.
- B.Configure an environment variable named PERIOD for the Lambda function. Set the value to 600.
- C.Create an Amazon EventBridge rule that runs on a regular schedule to invoke the Lambda function.
- D.Create an Amazon Simple Notification Service (Amazon SNS) topic that has a subscription to the Lambda function with a 600-second timer.

**Answer: C**

**Explanation:**

C is correct. Amazon Event Bridge can be used to run Lambda functions on a regular schedule. You can set a cron or rate expression to define the schedule.

### Question: 156

CertyIQ

A company is using Amazon OpenSearch Service to implement an audit monitoring system. A developer needs to

create an AWS CloudFormation custom resource that is associated with an AWS Lambda function to configure the OpenSearch Service domain. The Lambda function must access the OpenSearch Service domain by using OpenSearch Service internal master user credentials.

What is the MOST secure way to pass these credentials to the Lambda function?

- A.Use a CloudFormation parameter to pass the master user credentials at deployment to the OpenSearch Service domain's MasterUserOptions and the Lambda function's environment variable. Set the NoEcho attribute to true.
- B.Use a CloudFormation parameter to pass the master user credentials at deployment to the OpenSearch Service domain's MasterUserOptions and to create a parameter in AWS Systems Manager Parameter Store. Set the NoEcho attribute to true. Create an IAM role that has the ssm:GetParameter permission. Assign the role to the Lambda function. Store the parameter name as the Lambda function's environment variable. Resolve the parameter's value at runtime.
- C.Use a CloudFormation parameter to pass the master user credentials at deployment to the OpenSearch Service domain's MasterUserOptions and the Lambda function's environment variable. Encrypt the parameter's value by using the AWS Key Management Service (AWS KMS) encrypt command.
- D.Use CloudFormation to create an AWS Secrets Manager secret. Use a CloudFormation dynamic reference to retrieve the secret's value for the OpenSearch Service domain's MasterUserOptions. Create an IAM role that has the secretsmanager:GetSecretValue permission. Assign the role to the Lambda function. Store the secret's name as the Lambda function's environment variable. Resolve the secret's value at runtime.

**Answer: D**

**Explanation:**

The correct answer is (D).Solution (D) is the most secure way to pass the credentials to the Lambda function because it uses AWS Secrets Manager to store the credentials in encrypted form.

### Question: 157

CertyIQ

An application runs on multiple EC2 instances behind an ELB.

Where is the session data best written so that it can be served reliably across multiple requests?

- A.Write data to Amazon ElastiCache.
- B.Write data to Amazon Elastic Block Store.
- C.Write data to Amazon EC2 Instance Store.
- D.Write data to the root filesystem.

**Answer: A**

**Explanation:**

The correct answer is (A).Amazon Elastic Cache is a distributed memory caching solution that is ideal for session data. Elastic Cache provides high-performance and durable session data storage that can be shared across multiple EC2 instances.

### Question: 158

CertyIQ

An ecommerce application is running behind an Application Load Balancer. A developer observes some unexpected load on the application during non-peak hours. The developer wants to analyze patterns for the client IP addresses that use the application.

Which HTTP header should the developer use for this analysis?

- A.The X-Forwarded-Proto header
- B.The X-Forwarded-Host header
- C.The X-Forwarded-For header
- D.The X-Forwarded-Port header

**Answer: C**

**Explanation:**

The correct answer is (C).The X-Forwarded-For HTTP header contains the IP address of the original client that made the request. The developer can use this header to analyse patterns for the IP addresses of clients using the application.

X-Forwarded-For HTTP header contains the IP address of the original client

**Question: 159**

**CertyIQ**

A developer migrated a legacy application to an AWS Lambda function. The function uses a third-party service to pull data with a series of API calls at the end of each month. The function then processes the data to generate the monthly reports. The function has been working with no issues so far.

The third-party service recently issued a restriction to allow a fixed number of API calls each minute and each day. If the API calls exceed the limit for each minute or each day, then the service will produce errors. The API also provides the minute limit and daily limit in the response header. This restriction might extend the overall process to multiple days because the process is consuming more API calls than the available limit.

What is the MOST operationally efficient way to refactor the serverless application to accommodate this change?

- A.Use an AWS Step Functions state machine to monitor API failures. Use the Wait state to delay calling the Lambda function.
- B.Use an Amazon Simple Queue Service (Amazon SQS) queue to hold the API calls. Configure the Lambda function to poll the queue within the API threshold limits.
- C.Use an Amazon CloudWatch Logs metric to count the number of API calls. Configure an Amazon CloudWatch alarm that stops the currently running instance of the Lambda function when the metric exceeds the API threshold limits.
- D.Use Amazon Kinesis Data Firehose to batch the API calls and deliver them to an Amazon S3 bucket with an event notification to invoke the Lambda function.

**Answer: B**

**Explanation:**

The correct answer is (B).Solution (B) is the most operationally efficient way to refactor the serverless application to accommodate this change. This solution allows the Lambda function to continue executing API calls even if the API call limit is reached. The Amazon SQS queue will act as a buffer for API calls that exceed the limit. The Lambda function can then poll the queue within the API limits.

**Question: 160**

**CertyIQ**

A developer must analyze performance issues with production-distributed applications written as AWS Lambda functions. These distributed Lambda applications invoke other components that make up the applications.

How should the developer identify and troubleshoot the root cause of the performance issues in production?

- A.Add logging statements to the Lambda functions, then use Amazon CloudWatch to view the logs.
- B.Use AWS CloudTrail and then examine the logs.
- C.Use AWS X-Ray, then examine the segments and errors.
- D.Run Amazon Inspector agents and then analyze performance.

**Answer: C**

**Explanation:**

The correct answer is (C).AWS X-Ray is the best tool for identifying and addressing the root cause of performance issues in distributed production applications. X-Ray provides an overview of the entire call stack, including the Lambda functions and other components they invoke.

### Question: 161

**CertyIQ**

A developer wants to deploy a new version of an AWS Elastic Beanstalk application. During deployment, the application must maintain full capacity and avoid service interruption. Additionally, the developer must minimize the cost of additional resources that support the deployment.

Which deployment method should the developer use to meet these requirements?

- A.All at once
- B.Rolling with additional batch
- C.Blue/green
- D.Immutable

**Answer: C**

**Explanation:**

The correct answer is (C).The blue/green deployment method is the best option to meet the developer's requirements. Blue/green allows the developer to deploy a new version of the application without service interruption. This is done by creating a blue production environment and a green production environment. The blue environment is the current production environment and the green environment is the new version of the application. The developer can then test the new version of the application in the green environment before putting it into production.

### Question: 162

**CertyIQ**

A developer has observed an increase in bugs in the AWS Lambda functions that a development team has deployed in its Node.js application. To minimize these bugs, the developer wants to implement automated testing of Lambda functions in an environment that closely simulates the Lambda environment.

The developer needs to give other developers the ability to run the tests locally. The developer also needs to integrate the tests into the team's continuous integration and continuous delivery (CI/CD) pipeline before the AWS Cloud Development Kit (AWS CDK) deployment.

Which solution will meet these requirements?

- A.Create sample events based on the Lambda documentation. Create automated test scripts that use the cdk local invoke command to invoke the Lambda functions. Check the response. Document the test scripts for the other developers on the team. Update the CI/CD pipeline to run the test scripts.
- B.Install a unit testing framework that reproduces the Lambda execution environment. Create sample events

based on the Lambda documentation. Invoke the handler function by using a unit testing framework. Check the response. Document how to run the unit testing framework for the other developers on the team. Update the CI/CD pipeline to run the unit testing framework.

C.Install the AWS Serverless Application Model (AWS SAM) CLI tool. Use the sam local generate-event command to generate sample events for the automated tests. Create automated test scripts that use the sam local invoke command to invoke the Lambda functions. Check the response. Document the test scripts for the other developers on the team. Update the CI/CD pipeline to run the test scripts.

D.Create sample events based on the Lambda documentation. Create a Docker container from the Node.js base image to invoke the Lambda functions. Check the response. Document how to run the Docker container for the other developers on the team. Update the CI/CD pipeline to run the Docker container.

**Answer: C**

**Explanation:**

The correct answer is (C).Solution (C) is the best option to meet the developer's requirements. The AWS SAM CLI tool provides an easy way to generate sample events and invoke Lambda functions locally. The solution is also easy to document and integrate into the CI/CD pipeline.

**Question: 163**

**CertyIQ**

A developer is troubleshooting an application that uses Amazon DynamoDB in the us-west-2 Region. The application is deployed to an Amazon EC2 instance. The application requires read-only permissions to a table that is named Cars. The EC2 instance has an attached IAM role that contains the following IAM policy:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "ReadOnlyAPIActions",
 "Effect": "Allow",
 "Action": [
 "dynamodb:GetItem",
 "dynamodb:BatchGetItem",
 "dynamodb:Scan",
 "dynamodb:Query",
 "dynamodb:ConditionCheckItem"
],
 "Resource": "arn:aws:dynamodb:us-west-2:account-id:table/Cars"
 }
]
}
```

When the application tries to read from the Cars table, an Access Denied error occurs.

How can the developer resolve this error?

- A.Modify the IAM policy resource to be "arn:aws:dynamodb:us-west-2:account-id:table/\*".
- B.Modify the IAM policy to include the dynamodb:\* action.
- C.Create a trust policy that specifies the EC2 service principal. Associate the role with the policy.
- D.Create a trust relationship between the role and dynamodb.amazonaws.com.

**Answer: C**

**Explanation:**

Create a trust policy that specifies the EC2 service principal. Associate the role with the policy.

**CertyIQ**

**Question: 164**

When using the AWS Encryption SDK, how does the developer keep track of the data encryption keys used to encrypt data?

- A.The developer must manually keep track of the data encryption keys used for each data object.
- B.The SDK encrypts the data encryption key and stores it (encrypted) as part of the returned ciphertext.
- C.The SDK stores the data encryption keys automatically in Amazon S3.
- D.The data encryption key is stored in the Userdata for the EC2 instance.

**Answer: B**

**Explanation:**

The SDK encrypts the data encryption key and stores it (encrypted) as part of the returned ciphertext.

**CertyIQ**

**Question: 165**

An application that runs on AWS Lambda requires access to specific highly confidential objects in an Amazon S3 bucket. In accordance with the principle of least privilege, a company grants access to the S3 bucket by using only temporary credentials.

How can a developer configure access to the S3 bucket in the MOST secure way?

- A.Hardcode the credentials that are required to access the S3 objects in the application code. Use the credentials to access the required S3 objects.
- B.Create a secret access key and access key ID with permission to access the S3 bucket. Store the key and key ID in AWS Secrets Manager. Configure the application to retrieve the Secrets Manager secret and use the credentials to access the S3 objects.
- C.Create a Lambda function execution role. Attach a policy to the role that grants access to specific objects in the S3 bucket.
- D.Create a secret access key and access key ID with permission to access the S3 bucket. Store the key and key ID as environment variables in Lambda. Use the environment variables to access the required S3 objects.

**Answer: C**

**Explanation:**

C. Create a Lambda function execution role. Attach a policy to the role that grants access to specific objects in the S3 bucket.

**Reference:**

<https://docs.aws.amazon.com/lambda/latest/operatorguide/least-privilege.html>

**Question: 166**

CertyIQ

A developer has code that is stored in an Amazon S3 bucket. The code must be deployed as an AWS Lambda function across multiple accounts in the same AWS Region as the S3 bucket. An AWS CloudFormation template that runs for each account will deploy the Lambda function.

What is the MOST secure way to allow CloudFormation to access the Lambda code in the S3 bucket?

- A.Grant the CloudFormation service role the S3 ListBucket and GetObject permissions. Add a bucket policy to Amazon S3 with the principal of “AWS”: [account numbers].
- B.Grant the CloudFormation service role the S3 GetObject permission. Add a bucket policy to Amazon S3 with the principal of “\*”.
- C.Use a service-based link to grant the Lambda function the S3 ListBucket and GetObject permissions by explicitly adding the S3 bucket’s account number in the resource.
- D.Use a service-based link to grant the Lambda function the S3 GetObject permission. Add a resource of “\*” to allow access to the S3 bucket.

**Answer: A****Explanation:**

The correct answer is (A). Option (A) is the safest way to allow Cloud Formation to access the Lambda code in the S3 bucket because it limits access to the specific accounts that need to deploy the Lambda functions. The bucket policy grants S3 List Bucket and Get Object permissions to the Cloud Formation service role only for the accounts specified in the principal.

**Question: 167**

CertyIQ

A developer at a company needs to create a small application that makes the same API call once each day at a designated time. The company does not have infrastructure in the AWS Cloud yet, but the company wants to implement this functionality on AWS.

Which solution meets these requirements in the MOST operationally efficient manner?

- A.Use a Kubernetes cron job that runs on Amazon Elastic Kubernetes Service (Amazon EKS).
- B.Use an Amazon Linux crontab scheduled job that runs on Amazon EC2.
- C.Use an AWS Lambda function that is invoked by an Amazon EventBridge scheduled event.
- D.Use an AWS Batch job that is submitted to an AWS Batch job queue.

**Answer: C****Explanation:**

Use an AWS Lambda function that is invoked by an Amazon Event Bridge scheduled event.

**Question: 168**

CertyIQ

A developer is building a serverless application that is based on AWS Lambda. The developer initializes the AWS software development kit (SDK) outside of the Lambda handler function.

What is the PRIMARY benefit of this action?

- A.Improves legibility and stylistic convention
- B.Takes advantage of runtime environment reuse

- C.Provides better error handling
- DCreates a new SDK instance for each invocation

**Answer: B**

**Explanation:**

The correct answer is (B). Initializing the AWS SDK outside of the Lambda handler function takes advantage of runtime environment reuse. This means that the SDK only needs to be initialized once for all Lambda function invocations. This can improve application performance and efficiency.

**Question: 169**

**CertyIQ**

A company is using Amazon RDS as the backend database for its application. After a recent marketing campaign, a surge of read requests to the database increased the latency of data retrieval from the database. The company has decided to implement a caching layer in front of the database. The cached content must be encrypted and must be highly available.

Which solution will meet these requirements?

- A.Amazon CloudFront
- B.Amazon ElastiCache for Memcached
- C.Amazon ElastiCache for Redis in cluster mode
- D.Amazon DynamoDB Accelerator (DAX)

**Answer: C**

**Explanation:**

Amazon Elastic Cache for Redis in cluster mode

**Question: 170**

**CertyIQ**

A developer at a company recently created a serverless application to process and show data from business reports. The application's user interface (UI) allows users to select and start processing the files. The UI displays a message when the result is available to view. The application uses AWS Step Functions with AWS Lambda functions to process the files. The developer used Amazon API Gateway and Lambda functions to create an API to support the UI.

The company's UI team reports that the request to process a file is often returning timeout errors because of the size or complexity of the files. The UI team wants the API to provide an immediate response so that the UI can display a message while the files are being processed. The backend process that is invoked by the API needs to send an email message when the report processing is complete.

What should the developer do to configure the API to meet these requirements?

- A.Change the API Gateway route to add an X-Amz-Invocation-Type header with a static value of 'Event' in the integration request. Deploy the API Gateway stage to apply the changes.
- B.Change the configuration of the Lambda function that implements the request to process a file. Configure the maximum age of the event so that the Lambda function will run asynchronously.
- C.Change the API Gateway timeout value to match the Lambda function timeout value. Deploy the API Gateway stage to apply the changes.
- D.Change the API Gateway route to add an X-Amz-Target header with a static value of 'Async' in the integration request. Deploy the API Gateway stage to apply the changes.

**Answer: A**

**Explanation:**

Change the API Gateway route to add an X-Amz-Invocation-Type header with a static value of ‘Event’ in the integration request. Deploy the API Gateway stage to apply the changes.

**Question: 171**

CertyIQ

A developer has an application that is composed of many different AWS Lambda functions. The Lambda functions all use some of the same dependencies. To avoid security issues, the developer is constantly updating the dependencies of all of the Lambda functions. The result is duplicated effort for each function.

How can the developer keep the dependencies of the Lambda functions up to date with the LEAST additional complexity?

- A.Define a maintenance window for the Lambda functions to ensure that the functions get updated copies of the dependencies.
- B.Upgrade the Lambda functions to the most recent runtime version.
- C.Define a Lambda layer that contains all of the shared dependencies.
- D.Use an AWS CodeCommit repository to host the dependencies in a centralized location.

**Answer: C**

**Explanation:**

Define a Lambda layer that contains all of the shared dependencies.

**Question: 172**

CertyIQ

A mobile app stores blog posts in an Amazon DynamoDB table. Millions of posts are added every day, and each post represents a single item in the table. The mobile app requires only recent posts. Any post that is older than 48 hours can be removed.

What is the MOST cost-effective way to delete posts that are older than 48 hours?

- A.For each item, add a new attribute of type String that has a timestamp that is set to the blog post creation time. Create a script to find old posts with a table scan and remove posts that are older than 48 hours by using the BatchWriteItem API operation. Schedule a cron job on an Amazon EC2 instance once an hour to start the script.
- B.For each item, add a new attribute of type String that has a timestamp that is set to the blog post creation time. Create a script to find old posts with a table scan and remove posts that are older than 48 hours by using the BatchWriteItem API operation. Place the script in a container image. Schedule an Amazon Elastic Container Service (Amazon ECS) task on AWS Fargate that invokes the container every 5 minutes.
- C.For each item, add a new attribute of type Date that has a timestamp that is set to 48 hours after the blog post creation time. Create a global secondary index (GSI) that uses the new attribute as a sort key. Create an AWS Lambda function that references the GSI and removes expired items by using the BatchWriteItem API operation. Schedule the function with an Amazon CloudWatch event every minute.
- D.For each item, add a new attribute of type Number that has a timestamp that is set to 48 hours after the blog post creation time. Configure the DynamoDB table with a TTL that references the new attribute.

**Answer: D**

**Explanation:**

D is correct. DynamoDB tables can clean up data itself based on provided configuration.

The correct answer is (D). Solution (D) is the most cost-effective because it uses DynamoDB's Time to Live (TTL) to automatically remove expired items. The TTL is an item attribute that specifies the duration of time that an item should remain in the table. When an item's TTL expires, the item is automatically deleted from the table.

CertyIQ

### Question: 173

A developer is modifying an existing AWS Lambda function. While checking the code, the developer notices hardcoded parameter values for an Amazon RDS for SQL Server user name, password, database, host, and port. There are also hardcoded parameter values for an Amazon DynamoDB table, an Amazon S3 bucket, and an Amazon Simple Notification Service (Amazon SNS) topic.

The developer wants to securely store the parameter values outside the code in an encrypted format and wants to turn on rotation for the credentials. The developer also wants to be able to reuse the parameter values from other applications and to update the parameter values without modifying code.

Which solution will meet these requirements with the LEAST operational overhead?

- A.Create an RDS database secret in AWS Secrets Manager. Set the user name, password, database, host, and port. Turn on secret rotation. Create encrypted Lambda environment variables for the DynamoDB table, S3 bucket, and SNS topic.
- B.Create an RDS database secret in AWS Secrets Manager. Set the user name, password, database, host, and port. Turn on secret rotation. Create SecureString parameters in AWS Systems Manager Parameter Store for the DynamoDB table, S3 bucket, and SNS topic.
- C.Create RDS database parameters in AWS Systems Manager Parameter Store for the user name, password, database, host, and port. Create encrypted Lambda environment variables for the DynamoDB table, S3 bucket, and SNS topic. Create a Lambda function and set the logic for the credentials rotation task. Schedule the credentials rotation task in Amazon EventBridge.
- D.Create RDS database parameters in AWS Systems Manager Parameter Store for the user name, password, database, host, and port. Store the DynamoDB table, S3 bucket, and SNS topic in Amazon S3. Create a Lambda function and set the logic for the credentials rotation. Invoke the Lambda function on a schedule.

**Answer: B**

**Explanation:**

Create an RDS database secret in AWS Secrets Manager. Set the user name, password, database, host, and port. Turn on secret rotation. Create Secure String parameters in AWS Systems Manager Parameter Store for the DynamoDB table, S3 bucket, and SNS topic.

CertyIQ

### Question: 174

A developer accesses AWS CodeCommit over SSH. The SSH keys configured to access AWS CodeCommit are tied to a user with the following permissions:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "codecommit:BatchGetRepositories",
 "codecommit:Get*",
 "codecommit>List*",
 "codecommit:GitPull"
],
 "Resource": "*"
 }
]
}
```

The developer needs to create/delete branches.

Which specific IAM permissions need to be added, based on the principle of least privilege?

- A."codecommit>CreateBranch"  
"codecommit>DeleteBranch"
- B."codecommit:Put\*"
- C."codecommit:Update\*"
- D."codecommit:\*

**Answer: A**

**Explanation:**

"code commit: Create Branch"  
"code commit: Delete Branch"

**Question: 175**

**CertyIQ**

An application that is deployed to Amazon EC2 is using Amazon DynamoDB. The application calls the DynamoDB REST API. Periodically, the application receives a ProvisionedThroughputExceededException error when the application writes to a DynamoDB table.

Which solutions will mitigate this error MOST cost-effectively? (Choose two.)

- A.Modify the application code to perform exponential backoff when the error is received.
- B.Modify the application to use the AWS SDKs for DynamoDB.
- C.Increase the read and write throughput of the DynamoDB table.
- D.Create a DynamoDB Accelerator (DAX) cluster for the DynamoDB table.
- E.Create a second DynamoDB table. Distribute the reads and writes between the two tables.

**Answer: AB**

**Explanation:**

- A. Modify the application code to perform exponential back off when the error is received.
- B. Modify the application to use the AWS SDKs for DynamoDB.

### Question: 176

**CertyIQ**

When a developer tries to run an AWS CodeBuild project, it raises an error because the length of all environment variables exceeds the limit for the combined maximum of characters.

What is the recommended solution?

- A.Add the export LC\_ALL="en\_US.utf8" command to the pre\_build section to ensure POSIX localization.
- B.Use Amazon Cognito to store key-value pairs for large numbers of environment variables.
- C.Update the settings for the build project to use an Amazon S3 bucket for large numbers of environment variables.
- D.Use AWS Systems Manager Parameter Store to store large numbers of environment variables.

**Answer: D**

**Explanation:**

Use AWS Systems Manager Parameter Store to store large numbers of environment variables.

### Question: 177

**CertyIQ**

A company is expanding the compatibility of its photo-sharing mobile app to hundreds of additional devices with unique screen dimensions and resolutions. Photos are stored in Amazon S3 in their original format and resolution. The company uses an Amazon CloudFront distribution to serve the photos. The app includes the dimension and resolution of the display as GET parameters with every request.

A developer needs to implement a solution that optimizes the photos that are served to each device to reduce load time and increase photo quality.

Which solution will meet these requirements MOST cost-effectively?

- A.Use S3 Batch Operations to invoke an AWS Lambda function to create new variants of the photos with the required dimensions and resolutions. Create a dynamic CloudFront origin that automatically maps the request of each device to the corresponding photo variant.
- B.Use S3 Batch Operations to invoke an AWS Lambda function to create new variants of the photos with the required dimensions and resolutions. Create a Lambda@Edge function to route requests to the corresponding photo variant by using request headers.
- C.Create a Lambda@Edge function that optimizes the photos upon request and returns the photos as a

response. Change the CloudFront TTL cache policy to the maximum value possible.

D.Create a Lambda@Edge function that optimizes the photos upon request and returns the photos as a response. In the same function, store a copy of the processed photos on Amazon S3 for subsequent requests.

**Answer: D**

**Explanation:**

Create a Lambda@ Edge function that optimizes the photos upon request and returns the photos as a response. In the same function, store a copy of the processed photos on Amazon S3 for subsequent requests.

**CertyIQ**

**Question: 178**

A company is building an application for stock trading. The application needs sub-millisecond latency for processing trade requests. The company uses Amazon DynamoDB to store all the trading data that is used to process each trading request.

A development team performs load testing on the application and finds that the data retrieval time is higher than expected. The development team needs a solution that reduces the data retrieval time with the least possible effort.

Which solution meets these requirements?

- A.Add local secondary indexes (LSIs) for the trading data.
- B.Store the trading data in Amazon S3, and use S3 Transfer Acceleration.
- C.Add retries with exponential backoff for DynamoDB queries.
- D.Use DynamoDB Accelerator (DAX) to cache the trading data.

**Answer: D**

**Explanation:**

Use DynamoDB Accelerator (DAX) to cache the trading data.

**CertyIQ**

**Question: 179**

A developer is working on a Python application that runs on Amazon EC2 instances. The developer wants to enable tracing of application requests to debug performance issues in the code.

Which combination of actions should the developer take to achieve this goal? (Choose two.)

- A.Install the Amazon CloudWatch agent on the EC2 instances.
- B.Install the AWS X-Ray daemon on the EC2 instances.
- C.Configure the application to write JSON-formatted logs to /var/log/cloudwatch.
- D.Configure the application to write trace data to /var/log/xray.
- E.Install and configure the AWS X-Ray SDK for Python in the application.

**Answer: BE**

**Explanation:**

The correct answers are (E) and (B).(E) is the most important action to enable application request tracking using AWS X-Ray. The AWS X-Ray SDK for Python provides a set of APIs that a developer can use to

instrument their application code for tracing.(B) is the second most important action. The AWS X-Ray daemon runs on each EC2 instance and collects application trace data.

### Question: 180

CertyIQ

A company has an application that runs as a series of AWS Lambda functions. Each Lambda function receives data from an Amazon Simple Notification Service (Amazon SNS) topic and writes the data to an Amazon Aurora DB instance.

To comply with an information security policy, the company must ensure that the Lambda functions all use a single securely encrypted database connection string to access Aurora.

Which solution will meet these requirements?

- A.Use IAM database authentication for Aurora to enable secure database connections for all the Lambda functions.
- B.Store the credentials and read the credentials from an encrypted Amazon RDS DB instance.
- C.Store the credentials in AWS Systems Manager Parameter Store as a secure string parameter.
- D.Use Lambda environment variables with a shared AWS Key Management Service (AWS KMS) key for encryption.

#### Answer: C

#### Explanation:

C.AWS Systems Manager Parameter Store offers a more centralized way to manage encrypted secrets across multiple services than Lambda environment variables, making it a better fit for this scenario.

### Question: 181

CertyIQ

A developer is troubleshooting an Amazon API Gateway API. Clients are receiving HTTP 400 response errors when the clients try to access an endpoint of the API.

How can the developer determine the cause of these errors?

- A.Create an Amazon Kinesis Data Firehose delivery stream to receive API call logs from API Gateway. Configure Amazon CloudWatch Logs as the delivery stream's destination.
- B.Turn on AWS CloudTrail Insights and create a trail. Specify the Amazon Resource Name (ARN) of the trail for the stage of the API.
- C.Turn on AWS X-Ray for the API stage. Create an Amazon CloudWatch Logs log group. Specify the Amazon Resource Name (ARN) of the log group for the API stage.
- D.Turn on execution logging and access logging in Amazon CloudWatch Logs for the API stage. Create a CloudWatch Logs log group. Specify the Amazon Resource Name (ARN) of the log group for the API stage.

#### Answer: D

#### Explanation:

Turn on execution logging and access logging in Amazon Cloud Watch Logs for the API stage. Create a Cloud Watch Logs log group. Specify the Amazon Resource Name (ARN) of the log group for the API stage.

**Question: 182**

CertyIQ

A company developed an API application on AWS by using Amazon CloudFront, Amazon API Gateway, and AWS Lambda. The API has a minimum of four requests every second. A developer notices that many API users run the same query by using the POST method. The developer wants to cache the POST request to optimize the API resources.

Which solution will meet these requirements?

- A.Configure the CloudFront cache. Update the application to return cached content based upon the default request headers.
- B.Override the cache method in the selected stage of API Gateway. Select the POST method.
- C.Save the latest request response in Lambda /tmp directory. Update the Lambda function to check the /tmp directory.
- D.Save the latest request in AWS Systems Manager Parameter Store. Modify the Lambda function to take the latest request response from Parameter Store.

**Answer: B****Explanation:**

The correct answer is (B). Solution (B) is the best option because it uses the Amazon API Gateway cache to cache POST requests.

**Question: 183**

CertyIQ

A company is building a microservices application that consists of many AWS Lambda functions. The development team wants to use AWS Serverless Application Model (AWS SAM) templates to automatically test the Lambda functions. The development team plans to test a small percentage of traffic that is directed to new updates before the team commits to a full deployment of the application.

Which combination of steps will meet these requirements in the MOST operationally efficient way? (Choose two.)

- A.Use AWS SAM CLI commands in AWS CodeDeploy to invoke the Lambda functions to test the deployment.
- B.Declare the EventInvokeConfig on the Lambda functions in the AWS SAM templates with OnSuccess and onFailure configurations.
- C.Enable gradual deployments through AWS SAM templates.
- D.Set the deployment preference type to Canary10Percent30Minutes. Use hooks to test the deployment.
- E.Set the deployment preference type to Linear10PercentEvery10Minutes. Use hooks to test the deployment.

**Answer: CD****Explanation:**

C and D should be correct. Given that "The development team plans to test a small percentage of traffic that is directed to new updates before the team commits to a full deployment of the application." then Option D makes more sense than Option E.

**Question: 184**

CertyIQ

A company is using AWS CloudFormation to deploy a two-tier application. The application will use Amazon RDS as its backend database. The company wants a solution that will randomly generate the database password during deployment. The solution also must automatically rotate the database password without requiring changes to the application.

What is the MOST operationally efficient solution that meets these requirements?

- A.Use an AWS Lambda function as a CloudFormation custom resource to generate and rotate the password.
- B.Use an AWS Systems Manager Parameter Store resource with the SecureString data type to generate and rotate the password.
- C.Use a cron daemon on the application's host to generate and rotate the password.
- D.Use an AWS Secrets Manager resource to generate and rotate the password.

**Answer: D**

**Explanation:**

Correct answer is D:Use an AWS Secrets Manager resource to generate and rotate the password.

### Question: 185

CertyIQ

A developer has been asked to create an AWS Lambda function that is invoked any time updates are made to items in an Amazon DynamoDB table. The function has been created, and appropriate permissions have been added to the Lambda execution role. Amazon DynamoDB streams have been enabled for the table, but the function is still not being invoked.

Which option would enable DynamoDB table updates to invoke the Lambda function?

- A.Change the StreamViewType parameter value to NEW\_AND\_OLD\_IMAGES for the DynamoDB table.
- B.Configure event source mapping for the Lambda function.
- C.Map an Amazon Simple Notification Service (Amazon SNS) topic to the DynamoDB streams.
- D.Increase the maximum runtime (timeout) setting of the Lambda function.

**Answer: B**

**Explanation:**

Configure event source mapping for the Lambda function.

### Question: 186

CertyIQ

A developer needs to deploy an application running on AWS Fargate using Amazon ECS. The application has environment variables that must be passed to a container for the application to initialize.

How should the environment variables be passed to the container?

- A.Define an array that includes the environment variables under the environment parameter within the service definition.
- B.Define an array that includes the environment variables under the environment parameter within the task definition.
- C.Define an array that includes the environment variables under the entryPoint parameter within the task definition.
- D.Define an array that includes the environment variables under the entryPoint parameter within the service definition.

**Answer: B**

**Explanation:**

Define an array that includes the environment variables under the environment parameter within the task definition.

### Question: 187

CertyIQ

A development team maintains a web application by using a single AWS RDS template. The template defines web servers and an Amazon RDS database. The team uses the CloudFormation template to deploy the CloudFormation stack to different environments.

During a recent application deployment, a developer caused the primary development database to be dropped and recreated. The result of this incident was a loss of data. The team needs to avoid accidental database deletion in the future.

Which solutions will meet these requirements? (Choose two.)

- A.Add a CloudFormation DeletionPolicy attribute with the Retain value to the database resource.
- B.Update the CloudFormation stack policy to prevent updates to the database.
- C.Modify the database to use a Multi-AZ deployment.
- D.Create a CloudFormation stack set for the web application and database deployments.
- E.Add a CloudFormation DeletionPolicy attribute with the Retain value to the stack.

### Answer: AB

#### Explanation:

- A. Add a Cloud Formation Deletion Policy attribute with the Retain value to the database resource.
- B. Update the Cloud Formation stack policy to prevent updates to the database.

### Question: 188

CertyIQ

A developer is storing sensitive data generated by an application in Amazon S3. The developer wants to encrypt the data at rest. A company policy requires an audit trail of when the AWS Key Management Service (AWS KMS) key was used and by whom.

Which encryption option will meet these requirements?

- A.Server-side encryption with Amazon S3 managed keys (SSE-S3)
- B.Server-side encryption with AWS KMS managed keys (SSE-KMS)
- C.Server-side encryption with customer-provided keys (SSE-C)
- D.Server-side encryption with self-managed keys

### Answer: B

#### Explanation:

Server-side encryption with AWS KMS managed keys (SSE-KMS)

### Question: 189

CertyIQ

A company has an ecommerce application. To track product reviews, the company's development team uses an

Amazon DynamoDB table.

Every record includes the following:

- A Review ID, a 16-digit universally unique identifier (UUID)
- A Product ID and User ID, 16-digit UUIDs that reference other tables
- A Product Rating on a scale of 1-5
- An optional comment from the user

The table partition key is the Review ID. The most performed query against the table is to find the 10 reviews with the highest rating for a given product.

Which index will provide the FASTEST response for this query?

- A.A global secondary index (GSI) with Product ID as the partition key and Product Rating as the sort key
- B.A global secondary index (GSI) with Product ID as the partition key and Review ID as the sort key
- C.A local secondary index (LSI) with Product ID as the partition key and Product Rating as the sort key
- D.A local secondary index (LSI) with Review ID as the partition key and Product ID as the sort key

**Answer: A**

**Explanation:**

A global secondary index (GSI) with Product ID as the partition key and Product Rating as the sort key.

### Question: 190

CertyIQ

A company needs to distribute firmware updates to its customers around the world.

Which service will allow easy and secure control of the access to the downloads at the lowest cost?

- A.Use Amazon CloudFront with signed URLs for Amazon S3.
- B.Create a dedicated Amazon CloudFront Distribution for each customer.
- C.Use Amazon CloudFront with AWS Lambda@Edge.
- D.Use Amazon API Gateway and AWS Lambda to control access to an S3 bucket.

**Answer: A**

**Explanation:**

Use Amazon Cloud Front with signed URLs for Amazon S3.

### Question: 191

CertyIQ

A developer is testing an application that invokes an AWS Lambda function asynchronously. During the testing phase, the Lambda function fails to process after two retries.

How can the developer troubleshoot the failure?

- A.Configure AWS CloudTrail logging to investigate the invocation failures.
- B.Configure Dead Letter Queues by sending events to Amazon SQS for investigation.
- C.Configure Amazon Simple Workflow Service to process any direct unprocessed events.
- D.Configure AWS Config to process any direct unprocessed events.

**Answer: B**

**Explanation:**

Dead Letter Queues (DLQ) can be configured for Lambda functions to capture failed asynchronous invocations. Events that cannot be processed will be sent to an SQS queue (or an SNS topic) you specify, allowing for further investigation and reprocessing.

CertyIQ

**Question: 192**

A company is migrating its PostgreSQL database into the AWS Cloud. The company wants to use a database that will secure and regularly rotate database credentials. The company wants a solution that does not require additional programming overhead.

Which solution will meet these requirements?

- A.Use Amazon Aurora PostgreSQL for the database. Store the database credentials in AWS Systems Manager Parameter Store. Turn on rotation.
- B.Use Amazon Aurora PostgreSQL for the database. Store the database credentials in AWS Secrets Manager. Turn on rotation.
- C.Use Amazon DynamoDB for the database. Store the database credentials in AWS Systems Manager Parameter Store. Turn on rotation.
- D.Use Amazon DynamoDB for the database. Store the database credentials in AWS Secrets Manager. Turn on rotation.

**Answer: B**

**Explanation:**

B) The correct answer is (B). Solution (B) is the best option because it meets all the requirements: Using a database that secures and regularly changes database credentials: Amazon Aurora PostgreSQL offers built-in credential rotation, which allows you to change database credentials at regular intervals. Solution that requires no additional programming overhead: Amazon Aurora PostgreSQL credential rotation is fully automated, so it requires no additional programming overhead.

CertyIQ

**Question: 193**

A developer is creating a mobile application that will not require users to log in.

What is the MOST efficient method to grant users access to AWS resources?

- A.Use an identity provider to securely authenticate with the application.
- B.Create an AWS Lambda function to create an IAM user when a user accesses the application.
- C.Create credentials using AWS KMS and apply these credentials to users when using the application.
- D.Use Amazon Cognito to associate unauthenticated users with an IAM role that has limited access to resources.

**Answer: D**

**Explanation:**

Use Amazon Cognito to associate unauthenticated users with an IAM role that has limited access to resources.

**Question: 194****CertyIQ**

A company has developed a new serverless application using AWS Lambda functions that will be deployed using the AWS Serverless Application Model (AWS SAM) CLI.

Which step should the developer complete prior to deploying the application?

- A.Compress the application to a .zip file and upload it into AWS Lambda.
- B.Test the new AWS Lambda function by first tracing it in AWS X-Ray.
- C.Bundle the serverless application using a SAM package.
- D.Create the application environment using the eb create my-env command.

**Answer: C****Explanation:**

Bundle the serverless application using a SAM package.

**Question: 195****CertyIQ**

A company wants to automate part of its deployment process. A developer needs to automate the process of checking for and deleting unused resources that supported previously deployed stacks but that are no longer used.

The company has a central application that uses the AWS Cloud Development Kit (AWS CDK) to manage all deployment stacks. The stacks are spread out across multiple accounts. The developer's solution must integrate as seamlessly as possible within the current deployment process.

Which solution will meet these requirements with the LEAST amount of configuration?

- A.In the central AWS CDK application, write a handler function in the code that uses AWS SDK calls to check for and delete unused resources. Create an AWS CloudFormation template from a JSON file. Use the template to attach the function code to an AWS Lambda function and to invoke the Lambda function when the deployment stack runs.
- B.In the central AWS CDK application, write a handler function in the code that uses AWS SDK calls to check for and delete unused resources. Create an AWS CDK custom resource. Use the custom resource to attach the function code to an AWS Lambda function and to invoke the Lambda function when the deployment stack runs.
- C.In the central AWS CDK, write a handler function in the code that uses AWS SDK calls to check for and delete unused resources. Create an API in AWS Amplify. Use the API to attach the function code to an AWS Lambda function and to invoke the Lambda function when the deployment stack runs.
- D.In the AWS Lambda console, write a handler function in the code that uses AWS SDK calls to check for and delete unused resources. Create an AWS CDK custom resource. Use the custom resource to import the Lambda function into the stack and to invoke the Lambda function when the deployment stack runs.

**Answer: B****Explanation:**

The correct answer is (B). Solution (B) is the best option because: Requires the LEAST amount of configuration: Solution (B) uses an AWS CDK custom resource, which is a type of resource that can be defined in AWS CDK code. Custom resources are a convenient way to add custom functionality to your AWS Cloud Formation stacks. Integrates seamlessly into the current deployment process: Solution (B) uses the AWS CDK custom resource to attach function code to an AWS Lambda function and to invoke the Lambda function when the deployment stack runs. This means that the solution does not require any changes to the existing AWS CDK code.

**Question: 196**

CertyIQ

A company built a new application in the AWS Cloud. The company automated the bootstrapping of new resources with an Auto Scaling group by using AWS CloudFormation templates. The bootstrap scripts contain sensitive data.

The company needs a solution that is integrated with CloudFormation to manage the sensitive data in the bootstrap scripts.

Which solution will meet these requirements in the MOST secure way?

- A.Put the sensitive data into a CloudFormation parameter. Encrypt the CloudFormation templates by using an AWS Key Management Service (AWS KMS) key.
- B.Put the sensitive data into an Amazon S3 bucket. Update the CloudFormation templates to download the object from Amazon S3 during bootstrap.
- C.Put the sensitive data into AWS Systems Manager Parameter Store as a secure string parameter. Update the CloudFormation templates to use dynamic references to specify template values.
- D.Put the sensitive data into Amazon Elastic File System (Amazon EFS). Enforce EFS encryption after file system creation. Update the CloudFormation templates to retrieve data from Amazon EFS.

**Answer: C****Explanation:**

The correct answer is (C). Solution (C) is the best option because: It's the most secure solution: Sensitive data is stored in AWS Systems Manager Parameter Store, which is a secret management service managed by AWS. Secure string parameters in AWS Systems Manager Parameter Store are encrypted with an AWS KMS key. It's integrated with CloudFormation: Secure string parameters can be referenced in CloudFormation templates using dynamic references. This means that sensitive data does not need to be stored in CloudFormation code.

**Question: 197**

CertyIQ

A company needs to set up secure database credentials for all its AWS Cloud resources. The company's resources include Amazon RDS DB instances, Amazon DocumentDB clusters, and Amazon Aurora DB instances. The company's security policy mandates that database credentials be encrypted at rest and rotated at a regular interval.

Which solution will meet these requirements MOST securely?

- A.Set up IAM database authentication for token-based access. Generate user tokens to provide centralized access to RDS DB instances, Amazon DocumentDB clusters, and Aurora DB instances.
- B.Create parameters for the database credentials in AWS Systems Manager Parameter Store. Set the Type parameter to SecureString. Set up automatic rotation on the parameters.
- C.Store the database access credentials as an encrypted Amazon S3 object in an S3 bucket. Block all public access on the S3 bucket. Use S3 server-side encryption to set up automatic rotation on the encryption key.
- D.Create an AWS Lambda function by using the SecretsManagerRotationTemplate template in the AWS Secrets Manager console. Create secrets for the database credentials in Secrets Manager. Set up secrets rotation on a schedule.

**Answer: D****Explanation:**

D. Create an AWS Lambda function by using the SecretsManagerRotationTemplate template in the AWS

Secrets Manager console.

The correct answer is (D). Solution (D) is the best option because: It's the most secure solution: AWS Secrets Manager is an AWS-managed secrets management service that provides encryption at rest and automatic secret rotation. Meets the company's security requirements: The solution meets the company's security requirements because: Database credentials are encrypted at rest using AWS Key Management Service (AWS KMS). Database credentials are automatically rotated at regular intervals.

CertyIQ

### Question: 198

A developer has created an AWS Lambda function that makes queries to an Amazon Aurora MySQL DB instance. When the developer performs a test, the DB instance shows an error for too many connections.

Which solution will meet these requirements with the LEAST operational effort?

- A.Create a read replica for the DB instance. Query the replica DB instance instead of the primary DB instance.
- B.Migrate the data to an Amazon DynamoDB database.
- C.Configure the Amazon Aurora MySQL DB instance for Multi-AZ deployment.
- D.Create a proxy in Amazon RDS Proxy. Query the proxy instead of the DB instance.

**Answer: D**

**Explanation:**

Create a proxy in Amazon RDS Proxy. Query the proxy instead of the DB instance.

CertyIQ

### Question: 199

A developer is creating a new REST API by using Amazon API Gateway and AWS Lambda. The development team tests the API and validates responses for the known use cases before deploying the API to the production environment.

The developer wants to make the REST API available for testing by using API Gateway locally.

Which AWS Serverless Application Model Command Line Interface (AWS SAM CLI) subcommand will meet these requirements?

- A.Sam local invoke
- B.Sam local generate-event
- C.Sam local start-lambda
- D.Sam local start-api

**Answer: D**

**Explanation:**

The correct answer is (D). The AWS SAM CLI `sam local start-api` subcommand is used to start a local API Gateway instance. This allows you to test your REST API locally before deploying it to the production environment. The other subcommands will not meet the developer's requirements: Local invocation of Sam is used to invoke a Lambda function locally. Sam's local event generation is used to generate a local event file to be used to invoke a Lambda function locally. Sam local start-lambda is used to start a local instance of a Lambda function.

**Question: 200**

CertyIQ

A company has a serverless application on AWS that uses a fleet of AWS Lambda functions that have aliases. The company regularly publishes new Lambda function by using an in-house deployment solution. The company wants to improve the release process and to use traffic shifting. A newly published function version should initially make available only to a fixed percentage of production users.

Which solution will meet these requirements?

- A.Configure routing on the alias of the new function by using a weighted alias.
- B.Configure a canary deployment type for Lambda.
- C.Configure routing on the new versions by using environment variables.
- D.Configure a linear deployment type for Lambda.

**Answer: A****Explanation:**

The correct answer is (A).Weighted aliases allow you to route traffic to different versions of a function based on weights that you assign. This allows you to implement a canary deployment, where you initially route a small percentage of your traffic to the new version of the function, and then gradually increase the percentage as you gain confidence in the new version.

**Question: 201**

CertyIQ

A company has an application that stores data in Amazon RDS instances. The application periodically experiences surges of high traffic that cause performance problems. During periods of peak traffic, a developer notices a reduction in query speed in all database queries.

The team's technical lead determines that a multi-threaded and scalable caching solution should be used to offload the heavy read traffic. The solution needs to improve performance.

Which solution will meet these requirements with the LEAST complexity?

- A.Use Amazon ElastiCache for Memcached to offload read requests from the main database.
- B.Replicate the data to Amazon DynamoDSet up a DynamoDB Accelerator (DAX) cluster.
- C.Configure the Amazon RDS instances to use Multi-AZ deployment with one standby instance. Offload read requests from the main database to the standby instance.
- D.Use Amazon ElastiCache for Redis to offload read requests from the main database.

**Answer: A****Explanation:**

The correct answer is (A).Amazon Elastic Cache for Memcached is a scalable, multithreaded caching solution that can be used to offload heavy read traffic from Amazon RDS instances. Elastic Cache for Memcached is easy to configure and manage, making it a low-effort solution to meet technical lead requirements.

**Question: 202**

CertyIQ

A developer must provide an API key to an AWS Lambda function to authenticate with a third-party system. The Lambda function will run on a schedule. The developer needs to ensure that the API key remains encrypted at rest.

Which solution will meet these requirements?

- A.Store the API key as a Lambda environment variable by using an AWS Key Management Service (AWS KMS) customer managed key.
- B.Configure the application to prompt the user to provide the password to the Lambda function on the first run.
- C.Store the API key as a value in the application code.
- D.Use Lambda@Edge and only communicate over the HTTPS protocol.

**Answer: A**

**Explanation:**

The correct answer is (A). Storing the API key as a Lambda environment variable using an AWS Key Management Service (AWS KMS) customer-managed key is the most secure solution. AWS KMS is a managed encryption service that provides customer-managed keys. Customer-managed keys are encrypted with an AWS KMS master key, which is stored in an AWS KMS vault.

**Question: 203**

**CertyIQ**

An IT department uses Amazon S3 to store sensitive images. After more than 1 year, the company moves the images into archival storage. The company rarely accesses the images, but the company wants a storage solution that maximizes resiliency. The IT department needs access to the images that have been moved to archival storage within 24 hours.

Which solution will meet these requirements MOST cost-effectively?

- A.Use S3 Standard-Infrequent Access (S3 Standard-IA) to store the images. Use S3 Glacier Deep Archive with standard retrieval to store and retrieve archived images.
- B.Use S3 Standard-Infrequent Access (S3 Standard-IA) to store the images. Use S3 Glacier Deep Archive with bulk retrieval to store and retrieve archived images.
- C.Use S3 Intelligent-Tiering to store the images. Use S3 Glacier Deep Archive with standard retrieval to store and retrieve archived images.
- D.Use S3 One Zone-Infrequent Access (S3 One Zone-IA) to store the images. Use S3 Glacier Deep Archive with bulk retrieval to store and retrieve archived images.

**Answer: A**

**Explanation:**

A) Correct A) because the standard recovery is carried out within 12 hours and the requirement says that it must be recovered within 24 hours. Bulk recovery takes up to 48 hours

**Question: 204**

**CertyIQ**

A developer is building a serverless application by using the AWS Serverless Application Model (AWS SAM). The developer is currently testing the application in a development environment. When the application is nearly finished, the developer will need to set up additional testing and staging environments for a quality assurance team.

The developer wants to use a feature of the AWS SAM to set up deployments to multiple environments.

Which solution will meet these requirements with the LEAST development effort?

- A.Add a configuration file in TOML format to group configuration entries to every environment. Add a table for

each testing and staging environment. Deploy updates to the environments by using the sam deploy command and the --config-env flag that corresponds to each environment.

B.Create additional AWS SAM templates for each testing and staging environment. Write a custom shell script that uses the sam deploy command and the --template-file flag to deploy updates to the environments.

C.Create one AWS SAM configuration file that has default parameters. Perform updates to the testing and staging environments by using the --parameter-overrides flag in the AWS SAM CLI and the parameters that the updates will override.

D.Use the existing AWS SAM template. Add additional parameters to configure specific attributes for the serverless function and database table resources that are in each environment. Deploy updates to the testing and staging environments by using the sam deploy command.

#### Answer: A

#### Explanation:

Add a configuration file in TOML format to group configuration entries to every environment. Add a table for each testing and staging environment. Deploy updates to the environments by using the sam deploy command and the --config-env flag that corresponds to each environment.

Reference:

<https://stackoverflow.com/questions/68826108/how-to-deploy-to-different-environments-with-aws-sam>

**CertyIQ**

#### Question: 205

A developer is working on an application that processes operating data from IoT devices. Each IoT device uploads a data file once every hour to an Amazon S3 bucket. The developer wants to immediately process each data file when the data file is uploaded to Amazon S3.

The developer will use an AWS Lambda function to process the data files from Amazon S3. The Lambda function is configured with the S3 bucket information where the files are uploaded. The developer wants to configure the Lambda function to immediately invoke after each data file is uploaded.

Which solution will meet these requirements?

- A.Add an asynchronous invocation to the Lambda function. Select the S3 bucket as the source.
- B.Add an Amazon EventBridge event to the Lambda function. Select the S3 bucket as the source.
- C.Add a trigger to the Lambda function. Select the S3 bucket as the source.
- D.Add a layer to the Lambda function. Select the S3 bucket as the source.

#### Answer: C

#### Explanation:

The correct answer is (C).Adding a trigger to your Lambda function is the solution that will meet these requirements. A trigger is an event that can invoke a Lambda function. In the case of this issue, the trigger must be an Amazon S3 event that fires when a new file is uploaded to the bucket.

**CertyIQ**

#### Question: 206

A developer is setting up infrastructure by using AWS CloudFormation. If an error occurs when the resources described in the Cloud Formation template are provisioned, successfully provisioned resources must be preserved. The developer must provision and update the CloudFormation stack by using the AWS CLI.

Which solution will meet these requirements?

- A.Add an --enable-termination-protection command line option to the create-stack command and the update-stack command.
- B.Add a --disable-rollback command line option to the create-stack command and the update-stack command.
- C.Add a --parameters ParameterKey=PreserveResources,ParameterValue=True command line option to the create-stack command and the update-stack command.
- D.Add a --tags Key=PreserveResources,Value=True command line option to the create-stack command and the update-stack command.

**Answer: B**

**Explanation:**

Add a --disable-rollback command line option to the create-stack command and the update-stack command.

## Question: 207

CertyIQ

A developer is building a serverless application that connects to an Amazon Aurora PostgreSQL database. The serverless application consists of hundreds of AWS Lambda functions. During every Lambda function scale out, a new database connection is made that increases database resource consumption.

The developer needs to decrease the number of connections made to the database. The solution must not impact the scalability of the Lambda functions.

Which solution will meet these requirements?

- A.Configure provisioned concurrency for each Lambda function by setting the ProvisionedConcurrentExecutions parameter to 10.
- B.Enable cluster cache management for Aurora PostgreSQL. Change the connection string of each Lambda function to point to cluster cache management.
- C.Use Amazon RDS Proxy to create a connection pool to manage the database connections. Change the connection string of each Lambda function to reference the proxy.
- D.Configure reserved concurrency for each Lambda function by setting the ReservedConcurrentExecutions parameter to 10.

**Answer: C**

**Explanation:**

1. C: Amazon RDS Proxy is designed to improve application scalability and resilience by pooling and reusing database connections. This can significantly reduce the number of connections each Lambda function has to establish
2. The correct answer is (C).Amazon RDS Proxy is a solution that allows you to create a connection pool to manage database connections. This can help reduce the number of connections made to the database.

## Question: 208

CertyIQ

A developer is preparing to begin development of a new version of an application. The previous version of the application is deployed in a production environment. The developer needs to deploy fixes and updates to the current version during the development of the new version of the application. The code for the new version of the application is stored in AWS CodeCommit.

Which solution will meet these requirements?

- A.From the main branch, create a feature branch for production bug fixes. Create a second feature branch from the main branch for development of the new version.
- B.Create a Git tag of the code that is currently deployed in production. Create a Git tag for the development of

the new version. Push the two tags to the CodeCommit repository.

C.From the main branch, create a branch of the code that is currently deployed in production. Apply an IAM policy that ensures no other users can push or merge to the branch.

D.Create a new CodeCommit repository for development of the new version of the application. Create a Git tag for the development of the new version.

**Answer: A**

**Explanation:**

From the main branch, create a feature branch for production bug fixes. Create a second feature branch from the main branch for development of the new version.

**CertyIQ**

**Question: 209**

A developer is creating an AWS CloudFormation stack. The stack contains IAM resources with custom names. When the developer tries to deploy the stack, they receive an InsufficientCapabilities error.

What should the developer do to resolve this issue?

- A.Specify the CAPABILITY\_AUTO\_EXPAND capability in the CloudFormation stack.
- B.Use an administrators role to deploy IAM resources with CloudFormation.
- C.Specify the CAPABILITY\_IAM capability in the CloudFormation stack.
- D.Specify the CAPABILITY\_NAMED\_IAM capability in the CloudFormation stack.

**Answer: D**

**Explanation:**

The correct answer is (D).To deploy IAM resources with custom names, you must specify the CAPABILITY\_NAMED\_IAM resource in the Cloud Formation stack. The CAPABILITY\_IAM resource allows Cloud Formation to create and modify IAM resources. The CAPABILITY\_NAMED\_IAM resource allows Cloud Formation to create IAM resources with custom names. To resolve the issue, the developer must specify the CAPABILITY\_NAMED\_IAM resource in the Cloud Formation stack.

**CertyIQ**

**Question: 210**

A company uses Amazon API Gateway to expose a set of APIs to customers. The APIs have caching enabled in API Gateway. Customers need a way to invalidate the cache for each API when they test the API.

What should a developer do to give customers the ability to invalidate the API cache?

- A.Ask the customers to use AWS credentials to call the InvalidateCache API operation.
- B.Attach an InvalidateCache policy to the IAM execution role that the customers use to invoke the API. Ask the customers to send a request that contains the Cache-Control:max-age=0 HTTP header when they make an API call.
- C.Ask the customers to use the AWS SDK API Gateway class to invoke the InvalidateCache API operation.
- D.Attach an InvalidateCache policy to the IAM execution role that the customers use to invoke the API. Ask the customers to add the INVALIDATE\_CACHE query string parameter when they make an API call.

**Answer: B**

**Explanation:**

Attach an Invalidate Cache policy to the IAM execution role that the customers use to invoke the API. Ask the customers to send a request that contains the Cache- Control: max-age=0 HTTP header when they make an API call.

### Question: 211

CertyIQ

A developer is creating an AWS Lambda function that will generate and export a file. The function requires 100 MB of temporary storage for temporary files while running. These files will not be needed after the function is complete.

How can the developer MOST efficiently handle the temporary files?

- A.Store the files in Amazon Elastic Block Store (Amazon EBS) and delete the files at the end of the Lambda function.
- B.Copy the files to Amazon Elastic File System (Amazon EFS) and delete the files at the end of the Lambda function.
- C.Store the files in the /tmp directory and delete the files at the end of the Lambda function.
- D.Copy the files to an Amazon S3 bucket with a lifecycle policy to delete the files.

### Answer: C

#### Explanation:

C. Store the files in the /tmp directory and delete the files at the end of the Lambda function. The /tmp directory is a dedicated temporary storage location provided by AWS Lambda for storing temporary files during the execution of the function. It's cost-effective and efficient because it doesn't involve additional AWS services or storage costs. AWS Lambda automatically manages the /tmp directory for you, including clearing its contents after the function execution is complete. You don't need to explicitly delete the files; Lambda takes care of it.

### Question: 212

CertyIQ

A company uses Amazon DynamoDB as a data store for its order management system. The company frontend application stores orders in a DynamoDB table. The DynamoDB table is configured to send change events to a DynamoDB stream. The company uses an AWS Lambda function to log and process the incoming orders based on data from the DynamoDB stream.

An operational review reveals that the order quantity of incoming orders is sometimes set to 0. A developer needs to create a dashboard that will show how many unique customers this problem affects each day.

What should the developer do to implement the dashboard?

- A.Grant the Lambda function's execution role permissions to upload logs to Amazon CloudWatch Logs. Implement a CloudWatch Logs Insights query that selects the number of unique customers for orders with order quantity equal to 0 and groups the results in 1-day periods. Add the CloudWatch Logs Insights query to a CloudWatch dashboard.
- B.Use Amazon Athena to query AWS CloudTrail API logs for API calls. Implement an Athena query that selects the number of unique customers for orders with order quantity equal to 0 and groups the results in 1-day periods. Add the Athena query to an Amazon CloudWatch dashboard.
- C.Configure the Lambda function to send events to Amazon EventBridge. Create an EventBridge rule that groups the number of unique customers for orders with order quantity equal to 0 in 1-day periods. Add a CloudWatch dashboard as the target of the rule.
- D.Turn on custom Amazon CloudWatch metrics for the DynamoDB stream of the DynamoDB table. Create a CloudWatch alarm that groups the number of unique customers for orders with order quantity equal to 0 in 1-day periods. Add the CloudWatch alarm to a CloudWatch dashboard.

**Answer: A**

**Explanation:**

A. Grant the Lambda function's execution role permissions to upload logs to Amazon CloudWatch Logs. Implement a CloudWatch Logs Insights query that selects the number of unique customers for orders with order quantity equal to 0 and groups the results in 1-day periods. Add the CloudWatch Logs Insights query to a CloudWatch dashboard. Here's why this option is the best choice: CloudWatch Logs Insights is designed for querying and analyzing log data, making it well-suited for this task. By configuring the Lambda function's execution role to upload logs to CloudWatch Logs, you ensure that the log data is available for analysis. You can use a CloudWatch Logs Insights query to identify unique customers for orders with a quantity of 0 and group the results by day, providing the desired daily count of affected customers. The results of the query can be added to a CloudWatch dashboard, making it easily accessible for monitoring.

**Question: 213**

CertyIQ

A developer needs to troubleshoot an AWS Lambda function in a development environment. The Lambda function is configured in VPC mode and needs to connect to an existing Amazon RDS for SQL Server DB instance. The DB instance is deployed in a private subnet and accepts connections by using port 1433.

When the developer tests the function, the function reports an error when it tries to connect to the database.

Which combination of steps should the developer take to diagnose this issue? (Choose two.)

- A.Check that the function's security group has outbound access on port 1433 to the DB instance's security group. Check that the DB instance's security group has inbound access on port 1433 from the function's security group.
- B.Check that the function's security group has inbound access on port 1433 from the DB instance's security group. Check that the DB instance's security group has outbound access on port 1433 to the function's security group.
- C.Check that the VPC is set up for a NAT gateway. Check that the DB instance has the public access option turned on.
- D.Check that the function's execution role permissions include rds:DescribeDBInstances, rds:ModifyDBInstance, and rds:DescribeDBSecurityGroups for the DB instance.
- E.Check that the function's execution role permissions include ec2:CreateNetworkInterface, ec2:DescribeNetworkInterfaces, and ec2:DeleteNetworkInterface.

**Answer: AD**

**Explanation:**

- A. Check that the function's security group has outbound access on port 1433 to the DB instance's security group. Check that the DB instance's security group has inbound access on port 1433 from the function's security group.
- D. Check that the function's execution role permissions include rds:DescribeDBInstances, rds:ModifyDBInstance, and rds:DescribeDBSecurityGroups for the DB instance.

**Question: 214**

CertyIQ

A developer needs to launch a new Amazon EC2 instance by using the AWS CLI.

Which AWS CLI command should the developer use to meet this requirement?

- A.aws ec2 bundle-instance
- B.aws ec2 start-instances
- C.aws ec2 confirm-product-instance
- D.aws ec2 run-instances

**Answer: D**

**Explanation:**

D. aws ec2 run-instances So, to create a new EC2 instance using the AWS CLI, you would typically use the aws ec2 run-instances command, providing the necessary parameters such as the AMI ID, instance type, security groups, and key pair, among others.

### Question: 215

**CertyIQ**

A developer needs to manage AWS infrastructure as code and must be able to deploy multiple identical copies of the infrastructure, stage changes, and revert to previous versions.

Which approach addresses these requirements?

- A.Use cost allocation reports and AWS OpsWorks to deploy and manage the infrastructure.
- B.Use Amazon CloudWatch metrics and alerts along with resource tagging to deploy and manage the infrastructure.
- C.Use AWS Elastic Beanstalk and AWS CodeCommit to deploy and manage the infrastructure.
- D.Use AWS CloudFormation and AWS CodeCommit to deploy and manage the infrastructure.

**Answer: D**

**Explanation:**

D. Use AWS CloudFormation and AWS CodeCommit to deploy and manage the infrastructure. Here's why this is the most appropriate choice:  
AWS CloudFormation: It allows you to define your infrastructure as code using templates, which can be version-controlled. You can create, update, and delete stacks of AWS resources in a controlled and predictable manner. This aligns with the requirement to deploy multiple identical copies of the infrastructure, stage changes, and revert to previous versions.  
AWS CodeCommit: It provides a fully managed source control service, allowing you to store and version-control your CloudFormation templates. This ensures that you can manage and track changes to your infrastructure configurations.

### Question: 216

**CertyIQ**

A developer is working on an AWS Lambda function that accesses Amazon DynamoDB. The Lambda function must retrieve an item and update some of its attributes, or create the item if it does not exist. The Lambda function has access to the primary key.

Which IAM permissions should the developer request for the Lambda function to achieve this functionality?

- A.dynamodb:DeleteItem  
dynamodb:GetItem  
dynamodb:PutItem
- B.dynamodb:UpdateItem  
dynamodb:GetItem  
dynamodb:DescribeTable
- C.dynamodb:GetRecords

dynamodb:PutItem  
dynamodb:UpdateTable  
D.dynamodb:UpdateItem  
dynamodb:GetItem  
dynamodb:PutItem

**Answer: D**

**Explanation:**

D. dynamodb:UpdateItem, dynamodb:.GetItem, and dynamodb:PutItem  
Here's why:  
dynamodb:UpdateItem: This permission allows the Lambda function to update the attributes of an item in DynamoDB.  
dynamodb:PutItem: This permission allows the Lambda function to create a new item if it doesn't already exist in the DynamoDB table.

**Question: 217**

CertyIQ

A developer has built a market application that stores pricing data in Amazon DynamoDB with Amazon ElastiCache in front. The prices of items in the market change frequently. Sellers have begun complaining that, after they update the price of an item, the price does not actually change in the product listing.

What could be causing this issue?

- A.The cache is not being invalidated when the price of the item is changed.
- B.The price of the item is being retrieved using a write-through ElastiCache cluster.
- C.The DynamoDB table was provisioned with insufficient read capacity.
- D.The DynamoDB table was provisioned with insufficient write capacity.

**Answer: A**

**Explanation:**

A. The cache is not being invalidated when the price of the item is changed.In a caching setup using Amazon ElastiCache in front of Amazon DynamoDB, if the cache is not being invalidated or updated when data in DynamoDB is changed, it can result in stale data being served from the cache, leading to the observed behavior.To resolve this issue, you should implement a mechanism to invalidate or update the cache whenever the price of an item is changed in DynamoDB to ensure that the most up-to-date data is retrieved from the cache or DynamoDB.

**Question: 218**

CertyIQ

A company requires that all applications running on Amazon EC2 use IAM roles to gain access to AWS services. A developer is modifying an application that currently relies on IAM user access keys stored in environment variables to access Amazon DynamoDB tables using boto, the AWS SDK for Python.

The developer associated a role with the same permissions as the IAM user to the EC2 instance, then deleted the IAM user. When the application was restarted, the AWS AccessDeniedException messages started appearing in the application logs. The developer was able to use their personal account on the server to run DynamoDB API commands using the AWS CLI.

What is the MOST likely cause of the exception?

- A.IAM policies might take a few minutes to propagate to resources.

- B.Disabled environment variable credentials are still being used by the application.
- C.The AWS SDK does not support credentials obtained using an instance role.
- D.The instance's security group does not allow access to http://169.254.169.254.

**Answer: B**

**Explanation:**

B. Disabled environment variable credentials are still being used by the application.

**CertyIQ**

**Question: 219**

A company has an existing application that has hardcoded database credentials. A developer needs to modify the existing application. The application is deployed in two AWS Regions with an active-passive failover configuration to meet company's disaster recovery strategy.

The developer needs a solution to store the credentials outside the code. The solution must comply with the company's disaster recovery strategy.

Which solution will meet these requirements in the MOST secure way?

- A.Store the credentials in AWS Secrets Manager in the primary Region. Enable secret replication to the secondary Region. Update the application to use the Amazon Resource Name (ARN) based on the Region.
- B.Store credentials in AWS Systems Manager Parameter Store in the primary Region. Enable parameter replication to the secondary Region. Update the application to use the Amazon Resource Name (ARN) based on the Region.
- C.Store credentials in a config file. Upload the config file to an S3 bucket in the primary Region. Enable Cross-Region Replication (CRR) to an S3 bucket in the secondary region. Update the application to access the config file from the S3 bucket, based on the Region.
- D.Store credentials in a config file. Upload the config file to an Amazon Elastic File System (Amazon EFS) file system. Update the application to use the Amazon EFS file system Regional endpoints to access the config file in the primary and secondary Regions.

**Answer: A**

**Explanation:**

Store the credentials in AWS Secrets Manager in the primary Region. Enable secret replication to the secondary Region. Update the application to use the Amazon Resource Name (ARN) based on the Region.

Reference:

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/create-manage-multi-region-secrets.html>

**CertyIQ**

**Question: 220**

A developer is receiving HTTP 400: ThrottlingException errors intermittently when calling the Amazon CloudWatch API. When a call fails, no data is retrieved.

What best practice should first be applied to address this issue?

- A.Contact AWS Support for a limit increase.
- B.Use the AWS CLI to get the metrics.
- C.Analyze the applications and remove the API call.

D.Retry the call with exponential backoff.

**Answer: D**

**Explanation:**

Retry the call with exponential backoff.

**CertyIQ**

An application needs to use the IP address of the client in its processing. The application has been moved into AWS and has been placed behind an Application Load Balancer (ALB). However, all the client IP addresses now appear to be the same. The application must maintain the ability to scale horizontally.

Based on this scenario, what is the MOST cost-effective solution to this problem?

- A.Remove the application from the ALB. Delete the ALB and change Amazon Route 53 to direct traffic to the instance running the application.
- B.Remove the application from the ALB. Create a Classic Load Balancer in its place. Direct traffic to the application using the HTTP protocol.
- C.Alter the application code to inspect the X-Forwarded-For header. Ensure that the code can work properly if a list of IP addresses is passed in the header.
- D.Alter the application code to inspect a custom header. Alter the client code to pass the IP address in the custom header.

**Answer: C**

**Explanation:**

C. Alter the application code to inspect the X-Forwarded-For header. Ensure that the code can work properly if a list of IP addresses is passed in the header.

**CertyIQ**

**Question: 222**

A developer is designing a serverless application that customers use to select seats for a concert venue. Customers send the ticket requests to an Amazon API Gateway API with an AWS Lambda function that acknowledges the order and generates an order ID. The application includes two additional Lambda functions: one for inventory management and one for payment processing. These two Lambda functions run in parallel and write the order to an Amazon Dynamo DB table.

The application must provide seats to customers according to the following requirements. If a seat is accidentally sold more than once, the first order that the application received must get the seat. In these cases, the application must process the payment for only the first order. However, if the first order is rejected during payment processing, the second order must get the seat. In these cases, the application must process the payment for the second order.

Which solution will meet these requirements?

- A.Send the order ID to an Amazon Simple Notification Service (Amazon SNS) FIFO topic that fans out to one Amazon Simple Queue Service (Amazon SQS) FIFO queue for inventory management and another SQS FIFO queue for payment processing.
- B.Change the Lambda function that generates the order ID to initiate the Lambda function for inventory management. Then initiate the Lambda function for payment processing.
- C.Send the order ID to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the Lambda functions for inventory management and payment processing to the topic.

D.Deliver the order ID to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the Lambda functions for inventory management and payment processing to poll the queue.

**Answer: D**

**Explanation:**

D. Deliver the order ID to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the Lambda functions for inventory management and payment processing to poll the queue.

**Question: 223**

**CertyIQ**

An application uses AWS X-Ray to generate a large amount of trace data on an hourly basis. A developer wants to use filter expressions to limit the returned results through user-specified custom attributes.

How should the developer use filter expressions to filter the results in X-Ray?

- A.Add custom attributes as annotations in the segment document.
- B.Add custom attributes as metadata in the segment document.
- C.Add custom attributes as new segment fields in the segment document.
- D.Create new sampling rules that are based on custom attributes.

**Answer: B**

**Explanation:**

B. Add custom attributes as metadata in the segment document. Custom attributes are best added as metadata in the segment document because X-Ray filter expressions can use metadata to filter traces. Annotations and new segment fields are not typically used for filtering traces in this context.

**Question: 224**

**CertyIQ**

A web application is using Amazon Kinesis Data Streams for clickstream data that may not be consumed for up to 12 hours.

How can the developer implement encryption at rest for data within the Kinesis Data Streams?

- A.Enable SSL connections to Kinesis.
- B.Use Amazon Kinesis Consumer Library.
- C.Encrypt the data once it is at rest with a Lambda function.
- D.Enable server-side encryption in Kinesis Data Streams.

**Answer: D**

**Explanation:**

D. Enable server-side encryption in Kinesis Data Streams. Amazon Kinesis Data Streams allows you to enable server-side encryption, which encrypts data at rest. This ensures that data stored within the Kinesis Data Streams is protected with encryption.

**Question: 225**

CertyIQ

An application is real-time processing millions of events that are received through an API.

What service could be used to allow multiple consumers to process the data concurrently and MOST cost-effectively?

- A.Amazon SNS with fanout to an SQS queue for each application
- B.Amazon SNS with fanout to an SQS FIFO (first-in, first-out) queue for each application
- C.Amazon Kinesis Firehose
- D.Amazon Kinesis Data Streams

**Answer: D****Explanation:**

D. Amazon Kinesis Data Streams. Amazon Kinesis Data Streams is designed for real-time data streaming and allows multiple consumers to process data concurrently and in real-time. It can handle millions of events and provides a scalable and cost-effective solution for handling high-throughput data streams.

**Question: 226**

CertyIQ

Given the following AWS CloudFormation template:

```
Description: Creates a new Amazon S3 bucket for shared content. Uses a random bucket name to avoid conflicts.
```

**Resources:**

```
ContentBucket:
 Type: AWS::S3::Bucket
Outputs:

 ContentBucketName:
 Value: !Ref ContentBucket
```

What is the MOST efficient way to reference the new Amazon S3 bucket from another AWS CloudFormation template?

- A.Add an Export declaration to the Outputs section of the original template and use ImportValue in other templates.
- B.Add Exported: true to the Content.Bucket in the original template and use ImportResource in other templates.
- C.Create a custom AWS CloudFormation resource that gets the bucket name from the ContentBucket resource of the first stack.
- D.Use Fn::Include to include the existing template in other templates and use the ContentBucket resource directly.

**Answer: A****Explanation:**

A. Add an Export declaration to the Outputs section of the original template and use ImportValue in other templates.

**Question: 227**

CertyIQ

A developer has built an application that inserts data into an Amazon DynamoDB table. The table is configured to use provisioned capacity. The application is deployed on a burstable nano Amazon EC2 instance. The application logs show that the application has been failing because of a ProvisionedThroughputExceededException error.

Which actions should the developer take to resolve this issue? (Choose two.)

- A.Move the application to a larger EC2 instance.
- B.Increase the number of read capacity units (RCUs) that are provisioned for the DynamoDB table.
- C.Reduce the frequency of requests to DynamoDB by implementing exponential backoff.
- D.Increase the frequency of requests to DynamoDB by decreasing the retry delay.
- E.Change the capacity mode of the DynamoDB table from provisioned to on-demand.

**Answer: CE**

**Explanation:**

- C. Reduce the frequency of requests to DynamoDB by implementing exponential back off.
- E. Change the capacity mode of the DynamoDB table from provisioned to on-demand.

**CertyIQ**

A company is hosting a workshop for external users and wants to share the reference documents with the external users for 7 days. The company stores the reference documents in an Amazon S3 bucket that the company owns.

What is the MOST secure way to share the documents with the external users?

- A.Use S3 presigned URLs to share the documents with the external users. Set an expiration time of 7 days.
- B.Move the documents to an Amazon WorkDocs folder. Share the links of the WorkDocs folder with the external users.
- C.Create temporary IAM users that have read-only access to the S3 bucket. Share the access keys with the external users. Expire the credentials after 7 days.
- D.Create a role that has read-only access to the S3 bucket. Share the Amazon Resource Name (ARN) of this role with the external users.

**Answer: A**

**Explanation:**

- A. Use S3 presigned URLs to share the documents with the external users. Set an expiration time of 7 days.

**CertyIQ**

**Question: 229**

A developer is planning to use an Amazon API Gateway and AWS Lambda to provide a REST API. The developer will have three distinct environments to manage: development, test, and production.

How should the application be deployed while minimizing the number of resources to manage?

- A.Create a separate API Gateway and separate Lambda function for each environment in the same Region.
- B.Assign a Region for each environment and deploy API Gateway and Lambda to each Region.
- C.Create one API Gateway with multiple stages with one Lambda function with multiple aliases.
- D.Create one API Gateway and one Lambda function, and use a REST parameter to identify the environment.

**Answer: C**

**Explanation:**

C. Create one API Gateway with multiple stages with one Lambda function with multiple aliases.

**CertyIQ**

**Question: 230**

A developer registered an AWS Lambda function as a target for an Application Load Balancer (ALB) using a CLI command. However, the Lambda function is not being invoked when the client sends requests through the ALB.

Why is the Lambda function not being invoked?

- A.A Lambda function cannot be registered as a target for an ALB.
- B.A Lambda function can be registered with an ALB using AWS Management Console only.
- C.The permissions to invoke the Lambda function are missing.
- D.Cross-zone is not enabled on the ALB.

**Answer: C**

**Explanation:**

C. The permissions to invoke the Lambda function are missing.

**CertyIQ**

**Question: 231**

A developer is creating an AWS Lambda function that will connect to an Amazon RDS for MySQL instance. The developer wants to store the database credentials. The database credentials need to be encrypted and the database password needs to be automatically rotated.

Which solution will meet these requirements?

- A.Store the database credentials as environment variables for the Lambda function. Set the environment variables to rotate automatically.
- B.Store the database credentials in AWS Secrets Manager. Set up managed rotation on the database credentials.
- C.Store the database credentials in AWS Systems Manager Parameter Store as secure string parameters. Set up managed rotation on the parameters.
- D.Store the database credentials in the X-Amz-Security-Token parameter. Set up managed rotation on the parameter.

**Answer: B**

**Explanation:**

B. Store the database credentials in AWS Secrets Manager. Set up managed rotation on the database credentials

**CertyIQ**

**Question: 232**

A developer wants to reduce risk when deploying a new version of an existing AWS Lambda function. To test the Lambda function, the developer needs to split the traffic between the existing version and the new version of the

Lambda function.

Which solution will meet these requirements?

- A.Configure a weighted routing policy in Amazon Route 53. Associate the versions of the Lambda function with the weighted routing policy.
- B.Create a function alias. Configure the alias to split the traffic between the two versions of the Lambda function.
- C.Create an Application Load Balancer (ALB) that uses the Lambda function as a target. Configure the ALB to split the traffic between the two versions of the Lambda function.
- D.Create the new version of the Lambda function as a Lambda layer on the existing version. Configure the function to split the traffic between the two layers.

**Answer: B**

**Explanation:**

- B. Create a function alias. Configure the alias to split the traffic between the two versions of the Lambda function.

### Question: 233

CertyIQ

A developer has created a large AWS Lambda function. Deployment of the function is failing because of an InvalidParameterValueException error. The error message indicates that the unzipped size of the function exceeds the maximum supported value.

Which actions can the developer take to resolve this error? (Choose two.)

- A.Submit a quota increase request to AWS Support to increase the function to the required size.
- B.Use a compression algorithm that is more efficient than ZIP.
- C.Break up the function into multiple smaller functions.
- D.Zip the .zip file twice to compress the file more.
- E.Move common libraries, function dependencies, and custom runtimes into Lambda layers.

**Answer: CE**

**Explanation:**

- C. Break up the function into multiple smaller functions.
- E. Move common libraries, function dependencies, and custom runtimes into Lambda layers.

### Question: 234

CertyIQ

A developer is troubleshooting an application in an integration environment. In the application, an Amazon Simple Queue Service (Amazon SQS) queue consumes messages and then an AWS Lambda function processes the messages. The Lambda function transforms the messages and makes an API call to a third-party service.

There has been an increase in application usage. The third-party API frequently returns an HTTP 429 Too Many Requests error message. The error message prevents a significant number of messages from being processed successfully.

How can the developer resolve this issue?

- A.Increase the SQS event source's batch size setting.

- B.Configure provisioned concurrency for the Lambda function based on the third-party API's documented rate limits.
- C.Increase the retry attempts and maximum event age in the Lambda function's asynchronous configuration.
- D.Configure maximum concurrency on the SQS event source based on the third-party service's documented rate limits.

**Answer: C**

**Explanation:**

A. increase the batch size does not change how many items being processed. C is from Configuring error handling for asynchronous invocation — You can set it up when creating the lambda. Maximum age of event — The maximum amount of time Lambda retains an event in the asynchronous event queue, up to 6 hours. Retry attempts — The number of times Lambda retries when the function returns an error, between 0 and 2.

**Question: 235**

**CertyIQ**

A company has a three-tier application that is deployed in Amazon Elastic Container Service (Amazon ECS). The application is using an Amazon RDS for MySQL DB instance. The application performs more database reads than writes.

During times of peak usage, the application's performance degrades. When this performance degradation occurs, the DB instance's ReadLatency metric in Amazon CloudWatch increases suddenly.

How should a developer modify the application to improve performance?

- A.Use Amazon ElastiCache to cache query results.
- B.Scale the ECS cluster to contain more ECS instances.
- C.Add read capacity units (RCUs) to the DB instance.
- D.Modify the ECS task definition to increase the task memory.

**Answer: A**

**Explanation:**

A. Use Amazon ElastiCache to cache query results.

**Question: 236**

**CertyIQ**

A company has an online web application that includes a product catalog. The catalog is stored in an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET. The application must be able to list the objects in the S3 bucket and must be able to download objects through an IAM policy.

Which policy allows MINIMUM access to meet these requirements?

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "s3>ListBucket",
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
 },
 {
 "Effect": "Allow",
 "Action": [
 "s3GetObject"
],
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
 }
]
}
```

A.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "s3>ListBucket",
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
 },
 {
 "Effect": "Allow",
 "Action": [
 "s3:*"
],
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
 }
]
}
```

B.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "s3>ListBucket",
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
 },
 {
 "Effect": "Allow",
 "Action": [
 "s3:GetObject",
 "s3:PutObject",
 "s3>DeleteObject"
],
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
 }
]
}
```

C.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "s3>ListBucket",
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
 },
 {
 "Effect": "Deny",
 "Action": [
 "s3:GetObject"
],
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
 }
]
}
```

D.

**Answer: A**

**Explanation:**

A is the correct answer.

**Question: 237**

CertyIQ

A developer is writing an application to encrypt files outside of AWS before uploading the files to an Amazon S3 bucket. The encryption must be symmetric and must be performed inside the application.

How can the developer implement the encryption in the application to meet these requirements?

- A.Create a data key in AWS Key Management Service (AWS KMS). Use the AWS Encryption SDK to encrypt the files.
- B.Create a Hash-Based Message Authentication Code (HMAC) key in AWS Key Management Service (AWS KMS). Use the AWS Encryption SDK to encrypt the files.
- C.Create a data key pair in AWS Key Management Service (AWS KMS). Use the AWS CLI to encrypt the files.
- D.Create a data key in AWS Key Management Service (AWS KMS). Use the AWS CLI to encrypt the files.

**Answer: A****Explanation:**

- A. Create a data key in AWS Key Management Service (AWS KMS). Use the AWS Encryption SDK to encrypt the files.

**Question: 238**

CertyIQ

A developer is working on an application that is deployed on an Amazon EC2 instance. The developer needs a solution that will securely transfer files from the application to an Amazon S3 bucket.

What should the developer do to meet these requirements in the MOST secure way?

- A.Create an IAM user. Create an access key for the IAM user. Store the access key in the application's environment variables.
- B.Create an IAM role. Create an access key for the IAM role. Store the access key in the application's environment variables.
- C.Create an IAM role. Configure the IAM role to access the specific Amazon S3 API calls the application requires. Associate the IAM role with the EC2 instance.
- D.Configure an S3 bucket policy for the S3 bucket. Configure the S3 bucket policy to allow access for the EC2 instance ID.

**Answer: C****Explanation:**

- C. Create an IAM role. Configure the IAM role to access the specific Amazon S3 API calls the application requires. Associate the IAM role with the EC2 instance.

**Question: 239**

CertyIQ

A developer created a web API that receives requests by using an internet-facing Application Load Balancer (ALB) with an HTTPS listener. The developer configures an Amazon Cognito user pool and wants to ensure that every request to the API is authenticated through Amazon Cognito.

What should the developer do to meet this requirement?

- A.Add a listener rule to the listener to return a fixed response if the Authorization header is missing. Set the

fixed response to 401 Unauthorized.

B.Create an authentication action for the listener rules of the ALSet the rule action type to authenticate-cognito. Set the OnUnauthenticatedRequest field to “deny.”

C.Create an Amazon API Gateway API. Configure all API methods to be forwarded to the ALB endpoint. Create an authorizer of the COGNITO\_USER\_POOLS type. Configure every API method to use that authorizer.

D.Create a new target group that includes an AWS Lambda function target that validates the Authorization header by using Amazon Cognito. Associate the target group with the listener.

**Answer: B**

**Explanation:**

B. Create an authentication action for the listener rules of the ALSet the rule action type to authenticate-cognito. Set the OnUnauthenticatedRequest field to “deny.”

**Question: 240**

**CertyIQ**

A company recently deployed an AWS Lambda function. A developer notices an increase in the function throttle metrics in Amazon CloudWatch.

What are the MOST operationally efficient solutions to reduce the function throttling? (Choose two.)

A.Migrate the function to Amazon Elastic Kubernetes Service (Amazon EKS).

B.Increase the maximum age of events in Lambda.

C.Increase the function’s reserved concurrency.

D.Add the lambda:GetFunctionConcurrency action to the execution role.

E.Request a service quota change for increased concurrency.

**Answer: CE**

**Explanation:**

C. Increase the function’s reserved concurrency: Reserved concurrency ensures that a specific number of concurrent executions are always available for your function. E. Request a service quota change for increased concurrency: If your application is experiencing throttling and the reserved concurrency isn’t sufficient, you can request a service quota increase for additional concurrency.

**Question: 241**

**CertyIQ**

A company is creating a REST service using an Amazon API Gateway with AWS Lambda integration. The service must run different versions for testing purposes.

What would be the BEST way to accomplish this?

A.Use an X-Version header to denote which version is being called and pass that header to the Lambda function(s).

B.Create an API Gateway Lambda authorizer to route API clients to the correct API version.

C.Create an API Gateway resource policy to isolate versions and provide context to the Lambda function(s).

D.Deploy the API versions as unique stages with unique endpoints and use stage variables to provide further context.

**Answer: D**

**Explanation:**

D. Deploy the API versions as unique stages with unique endpoints and use stage variables to provide further context.

**CertyIQ**

A company is using AWS CodePipeline to deliver one of its applications. The delivery pipeline is triggered by changes to the main branch of an AWS CodeCommit repository and uses AWS CodeBuild to implement the test and build stages of the process and AWS CodeDeploy to deploy the application.

The pipeline has been operating successfully for several months and there have been no modifications. Following a recent change to the application's source code, AWS CodeDeploy has not deployed the updated application as expected.

What are the possible causes? (Choose two.)

- A.The change was not made in the main branch of the AWS CodeCommit repository.
- B.One of the earlier stages in the pipeline failed and the pipeline has terminated.
- C.One of the Amazon EC2 instances in the company's AWS CodePipeline cluster is inactive.
- D.The AWS CodePipeline is incorrectly configured and is not invoking AWS CodeDeploy.
- E.AWS CodePipeline does not have permissions to access AWS CodeCommit.

**Answer: AB****Explanation:**

A. The change was not made in the main branch of the AWS Code Commit repository: In this pipeline setup, if the change was made in a branch other than the main branch, it would not trigger the pipeline, and therefore, AWS Code Deploy wouldn't deploy the updated application. B. One of the earlier stages in the pipeline failed and the pipeline has terminated: If one of the preceding stages in the pipeline failed, it would prevent the subsequent stages, including AWS Code Deploy, from being executed.

**CertyIQ**

A developer is building a serverless application by using AWS Serverless Application Model (AWS SAM) on multiple AWS Lambda functions. When the application is deployed, the developer wants to shift 10% of the traffic to the new deployment of the application for the first 10 minutes after deployment. If there are no issues, all traffic must switch over to the new version.

Which change to the AWS SAM template will meet these requirements?

- A.Set the Deployment Preference Type to Canary10Percent10Minutes. Set the AutoPublishAlias property to the Lambda alias.
- B.Set the Deployment Preference Type to Linear10PercentEvery10Minutes. Set AutoPublishAlias property to the Lambda alias.
- C.Set the Deployment Preference Type to Canary10Percent10Minutes. Set the PreTraffic and PostTraffic properties to the Lambda alias.
- D.Set the Deployment Preference Type to Linear10PercentEvery10Minutes. Set PreTraffic and PostTraffic properties to the Lambda alias.

**Answer: C****Explanation:**

Set the Deployment Preference Type to Canary10Percent10Minutes. Set the Pre Traffic and Post Traffic properties to the Lambda alias.

Reference:

<https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/automating-updates-to-serverless-apps.html>

CertyIQ

### Question: 244

An AWS Lambda function is running in a company's shared AWS account. The function needs to perform an additional ec2:DescribeInstances action that is directed at the company's development accounts. A developer must configure the required permissions across the accounts.

How should the developer configure the permissions to adhere to the principle of least privilege?

- A.Create an IAM role in the shared account. Add the ec2:DescribeInstances permission to the role. Establish a trust relationship between the development accounts for this role. Update the Lambda function IAM role in the shared account by adding the ec2:DescribeInstances permission to the role.
- B.Create an IAM role in the development accounts. Add the ec2:DescribeInstances permission to the role. Establish a trust relationship with the shared account for this role. Update the Lambda function IAM role in the shared account by adding the iam:AssumeRole permissions.
- C.Create an IAM role in the shared account. Add the ec2:DescribeInstances permission to the role. Establish a trust relationship between the development accounts for this role. Update the Lambda function IAM role in the shared account by adding the iam:AssumeRole permissions.
- D.Create an IAM role in the development accounts. Add the ec2:DescribeInstances permission to the role. Establish a trust relationship with the shared account for this role. Update the Lambda function IAM role in the shared account by adding the ec2:DescribeInstances permission to the role.

Answer: C

Explanation:

Create an IAM role in the shared account. Add the ec2:DescribeInstances permission to the role. Establish a trust relationship between the development accounts for this role. Update the Lambda function IAM role in the shared account by adding the iam: Assume Role permissions.

CertyIQ

### Question: 245

A developer is building a new application that will be deployed on AWS. The developer has created an AWS CodeCommit repository for the application. The developer has initialized a new project for the application by invoking the AWS Cloud Development Kit (AWS CDK) cdk init command.

The developer must write unit tests for the infrastructure as code (IaC) templates that the AWS CDK generates. The developer also must run a validation tool across all constructs in the CDK application to ensure that critical security configurations are activated.

Which combination of actions will meet these requirements with the LEAST development overhead? (Choose two.)

- A.Use a unit testing framework to write custom unit tests against the cdk.out file that the AWS CDK generates. Run the unit tests in a continuous integration and continuous delivery (CI/CD) pipeline that is invoked after any commit to the repository.
- B.Use the CDK assertions module to integrate unit tests with the application. Run the unit tests in a continuous integration and continuous delivery (CI/CD) pipeline that is invoked after any commit to the repository.
- C.Use the CDK runtime context to set key-value pairs that must be present in the cdk.out file that the AWS CDK generates. Fail the stack synthesis if any violations are present.

D. Write a script that searches the application for specific key configuration strings. Configure the script to produce a report of any security violations.

E. Use the CDK Aspects class to create custom rules to apply to the CDK application. Fail the stack synthesis if any violations are present.

**Answer: BE**

**Explanation:**

B. Use the CDK assertions module to integrate unit tests with the application. Run the unit tests in a continuous integration and continuous delivery (CI/CD) pipeline that is invoked after any commit to the repository. E. Use the CDK Aspects class to create custom rules to apply to the CDK application. Fail the stack synthesis if any violations are present.

**Question: 246**

CertyIQ

An online sales company is developing a serverless application that runs on AWS. The application uses an AWS Lambda function that calculates order success rates and stores the data in an Amazon DynamoDB table. A developer wants an efficient way to invoke the Lambda function every 15 minutes.

Which solution will meet this requirement with the LEAST development effort?

- A. Create an Amazon EventBridge rule that has a rate expression that will run the rule every 15 minutes. Add the Lambda function as the target of the EventBridge rule.
- B. Create an AWS Systems Manager document that has a script that will invoke the Lambda function on Amazon EC2. Use a Systems Manager Run Command task to run the shell script every 15 minutes.
- C. Create an AWS Step Functions state machine. Configure the state machine to invoke the Lambda function execution role at a specified interval by using a Wait state. Set the interval to 15 minutes.
- D. Provision a small Amazon EC2 instance. Set up a cron job that invokes the Lambda function every 15 minutes.

**Answer: A**

**Explanation:**

Run Lambda as cron = Event Bridge

option A is the most efficient and least development effort option for invoking the Lambda function every 15 minutes, as it leverages Amazon EventBridge's built-in scheduling capabilities and is fully serverless.

**Question: 247**

CertyIQ

A company deploys a photo-processing application to an Amazon EC2 instance. The application needs to process each photo in less than 5 seconds. If processing takes longer than 5 seconds, the company's development team must receive a notification.

How can a developer implement the required time measurement and notification with the LEAST operational overhead?

- A. Create an Amazon CloudWatch custom metric. Each time a photo is processed, publish the processing time as a metric value. Create a CloudWatch alarm that is based on a static threshold of 5 seconds. Notify the development team by using an Amazon Simple Notification Service (Amazon SNS) topic.
- B. Create an Amazon Simple Queue Service (Amazon SQS) queue. Each time a photo is processed, publish the processing time to the queue. Create an application to consume from the queue and to determine whether any values are more than 5 seconds. Notify the development team by using an Amazon Simple Notification Service (Amazon SNS) topic.

C.Create an Amazon CloudWatch custom metric. Each time a photo is processed, publish the processing time as a metric value. Create a CloudWatch alarm that enters ALARM state if the average of values is greater than 5 seconds. Notify the development team by sending an Amazon Simple Email Service (Amazon SES) message.

D.Create an Amazon Kinesis data stream. Each time a photo is processed, publish the processing time to the data stream. Create an Amazon CloudWatch alarm that enters ALARM state if any values are more than 5 seconds. Notify the development team by using an Amazon Simple Notification Service (Amazon SNS) topic.

**Answer: A**

**Explanation:**

A. Create an Amazon CloudWatch custom metric. Each time a photo is processed, publish the processing time as a metric value. Create a CloudWatch alarm that is based on a static threshold of 5 seconds. Notify the development team by using an Amazon Simple Notification Service (Amazon SNS) topic.

**Question: 248**

**CertyIQ**

A company is using AWS Elastic Beanstalk to manage web applications that are running on Amazon EC2 instances. A developer needs to make configuration changes. The developer must deploy the changes to new instances only.

Which types of deployment can the developer use to meet this requirement? (Choose two.)

- A.All at once
- B.Immutable
- C.Rolling
- D.Blue/green
- E.Rolling with additional batch

**Answer: BD**

**Explanation:**

- B. Immutable.
- D. Blue/green.

**Question: 249**

**CertyIQ**

A developer needs to use Amazon DynamoDB to store customer orders. The developer's company requires all customer data to be encrypted at rest with a key that the company generates.

What should the developer do to meet these requirements?

- A.Create the DynamoDB table with encryption set to None. Code the application to use the key to decrypt the data when the application reads from the table. Code the application to use the key to encrypt the data when the application writes to the table.
- B.Store the key by using AWS Key Management Service (AWS KMS). Choose an AWS KMS customer managed key during creation of the DynamoDB table. Provide the Amazon Resource Name (ARN) of the AWS KMS key.
- C.Store the key by using AWS Key Management Service (AWS KMS). Create the DynamoDB table with default encryption. Include the kms:Encrypt parameter with the Amazon Resource Name (ARN) of the AWS KMS key when using the DynamoDB software development kit (SDK).
- D.Store the key by using AWS Key Management Service (AWS KMS). Choose an AWS KMS AWS managed key during creation of the DynamoDB table. Provide the Amazon Resource Name (ARN) of the AWS KMS key.

**Answer: B**

**Explanation:**

B. Store the key by using AWS Key Management Service (AWS KMS). Choose an AWS KMS customer managed key during the creation of the DynamoDB table. Provide the Amazon Resource Name (ARN) of the AWS KMS key.

**CertyIQ**

**Question: 250**

A company uses AWS CloudFormation to deploy an application that uses an Amazon API Gateway REST API with AWS Lambda function integration. The application uses Amazon DynamoDB for data persistence. The application has three stages: development, testing, and production. Each stage uses its own DynamoDB table.

The company has encountered unexpected issues when promoting changes to the production stage. The changes were successful in the development and testing stages. A developer needs to route 20% of the traffic to the new production stage API with the next production release. The developer needs to route the remaining 80% of the traffic to the existing production stage. The solution must minimize the number of errors that any single customer experiences.

Which approach should the developer take to meet these requirements?

- A.Update 20% of the planned changes to the production stage. Deploy the new production stage. Monitor the results. Repeat this process five times to test all planned changes.
- B.Update the Amazon Route 53 DNS record entry for the production stage API to use a weighted routing policy. Set the weight to a value of 80. Add a second record for the production domain name. Change the second routing policy to a weighted routing policy. Set the weight of the second policy to a value of 20. Change the alias of the second policy to use the testing stage API.
- C.Deploy an Application Load Balancer (ALB) in front of the REST API. Change the production API Amazon Route 53 record to point traffic to the ALB. Register the production and testing stages as targets of the ALB with weights of 80% and 20%, respectively.
- D.Configure canary settings for the production stage API. Change the percentage of traffic directed to canary deployment to 20%. Make the planned updates to the production stage. Deploy the changes

**Answer: D**

**Explanation:**

D. Configure canary settings for the production stage API. Change the percentage of traffic directed to canary deployment to 20%. Make the planned updates to the production stage. Deploy the changes.

**CertyIQ**

**Question: 251**

A developer has created a data collection application that uses Amazon API Gateway, AWS Lambda, and Amazon S3. The application's users periodically upload data files and wait for the validation status to be reflected on a processing dashboard. The validation process is complex and time-consuming for large files.

Some users are uploading dozens of large files and have to wait and refresh the processing dashboard to see if the files have been validated. The developer must refactor the application to immediately update the validation result on the user's dashboard without reloading the full dashboard.

What is the MOST operationally efficient solution that meets these requirements?

- A.Integrate the client with an API Gateway WebSocket API. Save the user-uploaded files with the WebSocket connection ID. Push the validation status to the connection ID when the processing is complete to initiate an update of the user interface.

B.Launch an Amazon EC2 micro instance, and set up a WebSocket server. Send the user-uploaded file and user detail to the EC2 instance after the user uploads the file. Use the WebSocket server to send updates to the user interface when the uploaded file is processed.

C.Save the user's email address along with the user-uploaded file. When the validation process is complete, send an email notification through Amazon Simple Notification Service (Amazon SNS) to the user who uploaded the file.

D.Save the user-uploaded file and user detail to Amazon DynamoDB. Use Amazon DynamoDB Streams with Amazon Simple Notification Service (Amazon SNS) push notifications to send updates to the browser to update the user interface.

**Answer: D**

**Explanation:**

Save the user-uploaded file and user detail to Amazon DynamoDB. Use Amazon DynamoDB Streams with Amazon Simple Notification Service (Amazon SNS) push notifications to send updates to the browser to update the user interface.

**Question: 252**

**CertyIQ**

A company's developer is creating an application that uses Amazon API Gateway. The company wants to ensure that only users in the Sales department can use the application. The users authenticate to the application by using federated credentials from a third-party identity provider (IdP) through Amazon Cognito. The developer has set up an attribute mapping to map an attribute that is named Department and to pass the attribute to a custom AWS Lambda authorizer.

To test the access limitation, the developer sets their department to Engineering in the IdP and attempts to log in to the application. The developer is denied access. The developer then updates their department to Sales in the IdP and attempts to log in. Again, the developer is denied access. The developer checks the logs and discovers that access is being denied because the developer's access token has a department value of Engineering.

Which of the following is a possible reason that the developer's department is still being reported as Engineering instead of Sales?

- A.Authorization caching is enabled in the custom Lambda authorizer.
- B.Authorization caching is enabled on the Amazon Cognito user pool.
- C.The IAM role for the custom Lambda authorizer does not have a Department tag.
- D.The IAM role for the Amazon Cognito user pool does not have a Department tag.

**Answer: A**

**Explanation:**

Authorization caching is enabled in the custom Lambda authorizer.

**Question: 253**

**CertyIQ**

A company has migrated an application to Amazon EC2 instances. Automatic scaling is working well for the application user interface. However, the process to deliver shipping requests to the company's warehouse staff is encountering issues. Duplicate shipping requests are arriving, and some requests are lost or arrive out of order.

The company must avoid duplicate shipping requests and must process the requests in the order that the requests arrive. Requests are never more than 250 KB in size and take 5-10 minutes to process. A developer needs to rearchitect the application to improve the reliability of the delivery and processing of the requests.

What should the developer do to meet these requirements?

A.Create an Amazon Kinesis Data Firehose delivery stream to process the requests. Create an Amazon Kinesis data stream. Modify the application to write the requests to the Kinesis data stream.

B.Create an AWS Lambda function to process the requests. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the Lambda function to the SNS topic. Modify the application to write the requests to the SNS topic.

C.Create an AWS Lambda function to process the requests. Create an Amazon Simple Queue Service (Amazon SQS) standard queue. Set the SQS queue as an event source for the Lambda function. Modify the application to write the requests to the SQS queue.

D.Create an AWS Lambda function to process the requests. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the SQS queue as an event source for the Lambda function. Modify the application to write the requests to the SQS queue.

**Answer: D**

**Explanation:**

D. Create an AWS Lambda function to process the requests. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the SQS queue as an event source for the Lambda function. Modify the application to write the requests to the SQS queue.

**CertyIQ**

A developer is creating a machine learning (ML) pipeline in AWS Step Functions that contains AWS Lambda functions. The developer has configured an Amazon Simple Queue Service (Amazon SQS) queue to deliver ML model parameters to the ML pipeline to train ML models. The developer uploads the trained models are uploaded to an Amazon S3 bucket.

The developer needs a solution that can locally test the ML pipeline without making service integration calls to Amazon SQS and Amazon S3.

Which solution will meet these requirements?

A.Use the Amazon CodeGuru Profiler to analyze the Lambda functions used in the AWS Step Functions pipeline.

B.Use the AWS Step Functions Local Docker Image to run and locally test the Lambda functions.

C.Use the AWS Serverless Application Model (AWS SAM) CLI to run and locally test the Lambda functions.

D.Use AWS Step Functions Local with mocked service integrations.

**Answer: D**

**Explanation:**

D. Use AWS Step Functions Local with mocked service integrations.

**CertyIQ**

A company runs a batch processing application by using AWS Lambda functions and Amazon API Gateway APIs with deployment stages for development, user acceptance testing, and production. A development team needs to configure the APIs in the deployment stages to connect to third-party service endpoints.

Which solution will meet this requirement?

A.Store the third-party service endpoints in Lambda layers that correspond to the stage.

B.Store the third-party service endpoints in API Gateway stage variables that correspond to the stage.

C.Encode the third-party service endpoints as query parameters in the API Gateway request URL.

D.Store the third-party service endpoint for each environment in AWS AppConfig.

**Answer: B**

**Explanation:**

Store the third-party service endpoints in API Gateway stage variables that correspond to the stage.

**Question: 256**

**CertyIQ**

A developer is building a serverless application that runs on AWS. The developer wants to create an accelerated development workflow that deploys incremental changes to AWS for testing. The developer wants to deploy the incremental changes but does not want to fully deploy the entire application to AWS for every code commit.

What should the developer do to meet these requirements?

A.Use the AWS Serverless Application Model (AWS SAM) to build the application. Use the sam sync command to deploy the incremental changes.

B.Use the AWS Serverless Application Model (AWS SAM) to build the application. Use the sam init command to deploy the incremental changes.

C.Use the AWS Cloud Development Kit (AWS CDK) to build the application. Use the cdk synth command to deploy the incremental changes.

D.Use the AWS Cloud Development Kit (AWS CDK) to build the application. Use the cdk bootstrap command to deploy the incremental changes.

**Answer: A**

**Explanation:**

Use the AWS Serverless Application Model (AWS SAM) to build the application. Use the sam sync command to deploy the incremental changes.

**Question: 257**

**CertyIQ**

A developer is building an application that will use an Amazon API Gateway API with an AWS Lambda backend. The team that will develop the frontend requires immediate access to the API endpoints to build the UI. To prepare the backend application for integration, the developer needs to set up endpoints. The endpoints need to return predefined HTTP status codes and JSON responses for the frontend team. The developer creates a method for an API resource.

Which solution will meet these requirements?

A.Set the integration type to AWS\_PROXY. Provision Lambda functions to return hardcoded JSON data.

B.Set the integration type to MOCK. Configure the method's integration request and integration response to associate a JSON responses with specific HTTP status codes.

C.Set the integration type to HTTP\_PROXY. Configure API Gateway to pass all requests to an external placeholder API, which the team will build.

D.Set the integration type to MOCK. Use a method request to define HTTP status codes. Use an integration request to define JSON responses.

**Answer: B**

**Explanation:**

Set the integration type to MOCK. Configure the method's integration request and integration response to associate a JSON responses with specific HTTP status codes.

### Question: 258

CertyIQ

A developer is migrating an application to Amazon Elastic Kubernetes Service (Amazon EKS). The developer migrates the application to Amazon Elastic Container Registry (Amazon ECR) with an EKS cluster. As part of the application migration to a new backend, the developer creates a new AWS account. The developer makes configuration changes to the application to point the application to the new AWS account and to use new backend resources. The developer successfully tests the changes within the application by deploying the pipeline.

The Docker image build and the pipeline deployment are successful, but the application is still connecting to the old backend. The developer finds that the application's configuration is still referencing the original EKS cluster and not referencing the new backend resources.

Which reason can explain why the application is not connecting to the new resources?

- A.The developer did not successfully create the new AWS account.
- B.The developer added a new tag to the Docker image.
- C.The developer did not update the Docker image tag to a new version.
- D.The developer pushed the changes to a new Docker image tag.

**Answer: C**

**Explanation:**

The developer did not update the Docker image tag to a new version.

### Question: 259

CertyIQ

A developer is creating an application that reads and writes to multiple Amazon S3 buckets. The application will be deployed to an Amazon EC2 instance. The developer wants to make secure API requests from the EC2 instances without the need to manage the security credentials for the application. The developer needs to apply the principle of least privilege.

Which solution will meet these requirements?

- A.Create an IAM user. Create access keys and secret keys for the user. Associate the user with an IAM policy that allows s3:\* permissions.
- B.Associate the EC2 instance with an IAM role that has an IAM policy that allows s3>ListBucket and s3:\*Object permissions for specific S3 buckets.
- C.Associate the EC2 instance with an IAM role that has an AmazonS3FullAccess AWS managed policy.
- D.Create a bucket policy on the S3 bucket that allows s3>ListBucket and s3:\*Object permissions to the EC2 instance.

**Answer: B**

**Explanation:**

Associate the EC2 instance with an IAM role that has an IAM policy that allows s3>ListBucket and s3:\*Object permissions for specific S3 buckets.

**Question: 260**

CertyIQ

A developer is writing an application that will retrieve sensitive data from a third-party system. The application will format the data into a PDF file. The PDF file could be more than 1 MB. The application will encrypt the data to disk by using AWS Key Management Service (AWS KMS). The application will decrypt the file when a user requests to download it. The retrieval and formatting portions of the application are complete.

The developer needs to use the GenerateDataKey API to encrypt the PDF file so that the PDF file can be decrypted later. The developer needs to use an AWS KMS symmetric customer managed key for encryption.

Which solutions will meet these requirements?

- A. Write the encrypted key from the GenerateDataKey API to disk for later use. Use the plaintext key from the GenerateDataKey API and a symmetric encryption algorithm to encrypt the file.
- B. Write the plain text key from the GenerateDataKey API to disk for later use. Use the encrypted key from the GenerateDataKey API and a symmetric encryption algorithm to encrypt the file.
- C. Write the encrypted key from the GenerateDataKey API to disk for later use. Use the plaintext key from the GenerateDataKey API to encrypt the file by using the KMS Encrypt API.
- D. Write the plain text key from the GenerateDataKey API to disk for later use. Use the encrypted key from the GenerateDataKey API to encrypt the file by using the KMS Encrypt API.

**Answer: A****Explanation:**

Write the encrypted key from the GenerateDataKey API to disk for later use. Use the plaintext key from the GenerateDataKey API and a symmetric encryption algorithm to encrypt the file.

**Question: 261**

CertyIQ

A company runs an application on Amazon EC2 instances. The EC2 instances open connections to an Amazon RDS for SQL Server database. A developer needs to store and access the credentials and wants to automatically rotate the credentials. The developer does not want to store the credentials for the database in the code.

Which solution will meet these requirements in the MOST secure way?

- A. Create an IAM role that has permissions to access the database. Attach the IAM role to the EC2 instances.
- B. Store the credentials as secrets in AWS Secrets Manager. Create an AWS Lambda function to update the secrets and the database. Retrieve the credentials from Secrets Manager as needed.
- C. Store the credentials in an encrypted text file in an Amazon S3 bucket. Configure the EC2 instance launch template to download the credentials from Amazon S3 as the instance launches. Create an AWS Lambda function to update the secrets and the database.
- D. Store the credentials in an Amazon DynamoDB table. Configure an Amazon CloudWatch Events rule to invoke an AWS Lambda function to periodically update the secrets and database.

**Answer: B****Explanation:**

Store the credentials as secrets in AWS Secrets Manager. Create an AWS Lambda function to update the secrets and the database. Retrieve the credentials from Secrets Manager as needed.

**Question: 262**

CertyIQ

A company wants to test its web application more frequently. The company deploys the application by using a

separate AWS CloudFormation stack for each environment. The company deploys the same CloudFormation template to each stack as the application progresses through the development lifecycle.

A developer needs to build in notifications for the quality assurance (QA) team. The developer wants the notifications to occur for new deployments in the final preproduction environment.

Which solution will meet these requirements?

- A.Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the QA team to the Amazon SNS topic. Update the CloudFormation stack options to point to the SNS topic in the pre-production environment.
- B.Create an AWS Lambda function that notifies the QA team. Create an Amazon EventBridge rule to invoke the Lambda function on the default event bus. Filter the events on the CloudFormation service and on the CloudFormation stack Amazon Resource Name (ARN).
- C.Create an Amazon CloudWatch alarm that monitors the metrics from CloudFormation. Filter the metrics on the stack name and the stack status. Configure the CloudWatch alarm to notify the QA team.
- D.Create an AWS Lambda function that notifies the QA team. Configure the event source mapping to receive events from CloudFormation. Specify the filtering values to limit invocations to the desired CloudFormation stack.

**Answer: A**

**Explanation:**

Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the QA team to the Amazon SNS topic. Update the CloudFormation stack options to point to the SNS topic in the pre-production environment.

**Question: 263**

**CertyIQ**

A developer manages three AWS accounts. Each account contains an Amazon RDS DB instance in a private subnet. The developer needs to define users in each database in a consistent way. The developer must ensure that the same users are created and updated later in all three accounts.

Which solution will meet these requirements with the MOST operational efficiency?

- A.Create an AWS CloudFormation template. Declare the users in the template. Attach the users to the database. Deploy the template in each account.
- B.Create an AWS CloudFormation template that contains a custom resource to create the users in the database. Deploy the template in each account.
- C.Write a script that creates the users. Deploy an Amazon EC2 instance in each account to run the script on the databases. Run the script in each account.
- D.Implement an AWS Lambda function that creates the users in the database. Provide the function with the details of all three accounts.

**Answer: B**

**Explanation:**

Create an AWS CloudFormation template that contains a custom resource to create the users in the database. Deploy the template in each account.

**Question: 264**

**CertyIQ**

A company is building a new application that runs on AWS and uses Amazon API Gateway to expose APIs. Teams

of developers are working on separate components of the application in parallel. The company wants to publish an API without an integrated backend so that teams that depend on the application backend can continue the development work before the API backend development is complete.

Which solution will meet these requirements?

- A.Create API Gateway resources and set the integration type value to MOCK. Configure the method integration request and integration response to associate a response with an HTTP status code. Create an API Gateway stage and deploy the API.
- B.Create an AWS Lambda function that returns mocked responses and various HTTP status codes. Create API Gateway resources and set the integration type value to AWS\_PROXY. Deploy the API.
- C.Create an EC2 application that returns mocked HTTP responses. Create API Gateway resources and set the integration type value to AWS. Create an API Gateway stage and deploy the API.
- D.Create API Gateway resources and set the integration type value set to HTTP\_PROXY. Add mapping templates and deploy the API. Create an AWS Lambda layer that returns various HTTP status codes. Associate the Lambda layer with the API deployment.

**Answer: A**

**Explanation:**

Create API Gateway resources and set the integration type value to MOCK. Configure the method integration request and integration response to associate a response with an HTTP status code. Create an API Gateway stage and deploy the API.

**Question: 265**

**CertyIQ**

An application that runs on AWS receives messages from an Amazon Simple Queue Service (Amazon SQS) queue and processes the messages in batches. The application sends the data to another SQS queue to be consumed by another legacy application. The legacy system can take up to 5 minutes to process some transaction data.

A developer wants to ensure that there are no out-of-order updates in the legacy system. The developer cannot alter the behavior of the legacy system.

Which solution will meet these requirements?

- A.Use an SQS FIFO queue. Configure the visibility timeout value.
- B.Use an SQS standard queue with a SendMessageBatchRequestEntry data type. Configure the DelaySeconds values.
- C.Use an SQS standard queue with a SendMessageBatchRequestEntry data type. Configure the visibility timeout value.
- D.Use an SQS FIFO queue. Configure the DelaySeconds value.

**Answer: A**

**Explanation:**

Use an SQS FIFO queue. Configure the visibility timeout value.

**Question: 266**

**CertyIQ**

A company is building a compute-intensive application that will run on a fleet of Amazon EC2 instances. The application uses attached Amazon Elastic Block Store (Amazon EBS) volumes for storing data. The Amazon EBS volumes will be created at time of initial deployment. The application will process sensitive information. All of the data must be encrypted. The solution should not impact the application's performance.

Which solution will meet these requirements?

- A.Configure the fleet of EC2 instances to use encrypted EBS volumes to store data.
- B.Configure the application to write all data to an encrypted Amazon S3 bucket.
- C.Configure a custom encryption algorithm for the application that will encrypt and decrypt all data.
- D.Configure an Amazon Machine Image (AMI) that has an encrypted root volume and store the data to ephemeral disks.

**Answer: A**

**Explanation:**

Configure the fleet of EC2 instances to use encrypted EBS volumes to store data.

### Question: 267

CertyIQ

A developer is updating the production version of an AWS Lambda function to fix a defect. The developer has tested the updated code in a test environment. The developer wants to slowly roll out the updates to a small subset of production users before rolling out the changes to all users. Only 10% of the users should be initially exposed to the new code in production.

Which solution will meet these requirements?

- A.Update the Lambda code and create a new version of the Lambda function. Create a Lambda function trigger. Configure the traffic weights in the trigger between the two Lambda function versions. Send 90% of the traffic to the production version, and send 10% of the traffic to the new version.
- B.Create a new Lambda function that uses the updated code. Create a Lambda alias for the production Lambda function. Configure the Lambda alias to send 90% of the traffic to the production Lambda function, and send 10% of the traffic to the test Lambda function.
- C.Update the Lambda code and create a new version of the Lambda function. Create a Lambda proxy integration. Configure the Lambda proxy to split traffic between the two Lambda function versions. Send 90% of the traffic to the production version, and send 10% of the traffic to the new version.
- D.Update the Lambda code and create a new version of the Lambda function. Create a Lambda function alias. Configure the traffic weights in the Lambda alias between the two Lambda function versions. Send 90% of the traffic to the production version, and send 10% of the traffic to the new version.

**Answer: D**

**Explanation:**

Update the Lambda code and create a new version of the Lambda function. Create a Lambda function alias. Configure the traffic weights in the Lambda alias between the two Lambda function versions. Send 90% of the traffic to the production version, and send 10% of the traffic to the new version.

### Question: 268

CertyIQ

A developer is creating an AWS Lambda function that consumes messages from an Amazon Simple Queue Service (Amazon SQS) standard queue. The developer notices that the Lambda function processes some messages multiple times.

How should developer resolve this issue MOST cost-effectively?

- A.Change the Amazon SQS standard queue to an Amazon SQS FIFO queue by using the Amazon SQS message deduplication ID.

- B.Set up a dead-letter queue.
- C.Set the maximum concurrency limit of the AWS Lambda function to 1.
- D.Change the message processing to use Amazon Kinesis Data Streams instead of Amazon SQS.

**Answer: A**

**Explanation:**

Change the Amazon SQS standard queue to an Amazon SQS FIFO queue by using the Amazon SQS message deduplication ID.

**CertyIQ**

**Question: 269**

A developer is optimizing an AWS Lambda function and wants to test the changes in production on a small percentage of all traffic. The Lambda function serves requests to a REST API in Amazon API Gateway. The developer needs to deploy their changes and perform a test in production without changing the API Gateway URL.

Which solution will meet these requirements?

- A.Define a function version for the currently deployed production Lambda function. Update the API Gateway endpoint to reference the new Lambda function version. Upload and publish the optimized Lambda function code. On the production API Gateway stage, define a canary release and set the percentage of traffic to direct to the canary release. Update the API Gateway endpoint to use the \$LATEST version of the Lambda function. Publish the API to the canary stage.
- B.Define a function version for the currently deployed production Lambda function. Update the API Gateway endpoint to reference the new Lambda function version. Upload and publish the optimized Lambda function code. Update the API Gateway endpoint to use the \$LATEST version of the Lambda function. Deploy a new API Gateway stage.
- C.Define an alias on the \$LATEST version of the Lambda function. Update the API Gateway endpoint to reference the new Lambda function alias. Upload and publish the optimized Lambda function code. On the production API Gateway stage, define a canary release and set the percentage of traffic to direct to the canary release. Update the API Gateway endpoint to use the \$LATEST version of the Lambda function. Publish to the canary stage.
- D.Define a function version for the currently deployed production Lambda function. Update the API Gateway endpoint to reference the new Lambda function version. Upload and publish the optimized Lambda function code. Update the API Gateway endpoint to use the \$LATEST version of the Lambda function. Deploy the API to the production API Gateway stage.

**Answer: C**

**Explanation:**

Define an alias on the \$LATEST version of the Lambda function. Update the API Gateway endpoint to reference the new Lambda function alias. Upload and publish the optimized Lambda function code. On the production API Gateway stage, define a canary release and set the percentage of traffic to direct to the canary release. Update the API Gateway endpoint to use the \$LATEST version of the Lambda function. Publish to the canary stage.

**CertyIQ**

**Question: 270**

A company notices that credentials that the company uses to connect to an external software as a service (SaaS) vendor are stored in a configuration file as plaintext.

The developer needs to secure the API credentials and enforce automatic credentials rotation on a quarterly basis.

Which solution will meet these requirements MOST securely?

- A.Use AWS Key Management Service (AWS KMS) to encrypt the configuration file. Decrypt the configuration file when users make API calls to the SaaS vendor. Enable rotation.
- B.Retrieve temporary credentials from AWS Security Token Service (AWS STS) every 15 minutes. Use the temporary credentials when users make API calls to the SaaS vendor.
- C.Store the credentials in AWS Secrets Manager and enable rotation. Configure the API to have Secrets Manager access.
- D.Store the credentials in AWS Systems Manager Parameter Store and enable rotation. Retrieve the credentials when users make API calls to the SaaS vendor.

**Answer: C**

**Explanation:**

Store the credentials in AWS Secrets Manager and enable rotation. Configure the API to have Secrets Manager access.

### Question: 271

CertyIQ

A company has an application that is hosted on Amazon EC2 instances. The application stores objects in an Amazon S3 bucket and allows users to download objects from the S3 bucket. A developer turns on S3 Block Public Access for the S3 bucket. After this change, users report errors when they attempt to download objects. The developer needs to implement a solution so that only users who are signed in to the application can access objects in the S3 bucket.

Which combination of steps will meet these requirements in the MOST secure way? (Choose two.)

- A.Create an EC2 instance profile and role with an appropriate policy. Associate the role with the EC2 instances.
- B.Create an IAM user with an appropriate policy. Store the access key ID and secret access key on the EC2 instances.
- C.Modify the application to use the S3 GeneratePresignedUrl API call.
- D.Modify the application to use the S3 GetObject API call and to return the object handle to the user.
- E.Modify the application to delegate requests to the S3 bucket.

**Answer: AC**

**Explanation:**

- A.Create an EC2 instance profile and role with an appropriate policy. Associate the role with the EC2 instances.
- C.Modify the application to use the S3 GeneratePresignedUrl API call.

### Question: 272

CertyIQ

An Amazon Simple Queue Service (Amazon SQS) queue serves as an event source for an AWS Lambda function. In the SQS queue, each item corresponds to a video file that the Lambda function must convert to a smaller resolution. The Lambda function is timing out on longer video files, but the Lambda function's timeout is already configured to its maximum value.

What should a developer do to avoid the timeouts without additional code changes?

- A.Increase the memory configuration of the Lambda function.

- B.Increase the visibility timeout on the SQS queue.
- C.Increase the instance size of the host that runs the Lambda function.
- D.Use multi-threading for the conversion.

**Answer: A**

**Explanation:**

Increase the memory configuration of the Lambda function.

**CertyIQ**

**Question: 273**

A company is building an application on AWS. The application's backend includes an Amazon API Gateway REST API. The company's frontend application developers cannot continue work until the backend API is ready for integration. The company needs a solution that will allow the frontend application developers to continue their work.

Which solution will meet these requirements in the MOST operationally efficient way?

- A.Configure mock integrations for API Gateway API methods.
- B.Integrate a Lambda function with API Gateway and return a mocked response.
- C.Add new API endpoints to the API Gateway stage and returns a mocked response.
- D.Configure a proxy resource for API Gateway API methods.

**Answer: A**

**Explanation:**

A. Configure mock integrations for API Gateway API methods.

Mock integrations in Amazon API Gateway allow you to return a fixed response without sending the request further to the backend. This approach enables frontend developers to work with a predetermined response structure and data, facilitating parallel development without waiting for the backend services to be fully implemented. This solution does not require additional code changes or the deployment of placeholder backend services, making it operationally efficient and straightforward to implement for temporary use during the development phase.

**CertyIQ**

**Question: 274**

A company is preparing to migrate an application to the company's first AWS environment. Before this migration, a developer is creating a proof-of-concept application to validate a model for building and deploying container-based applications on AWS.

Which combination of steps should the developer take to deploy the containerized proof-of-concept application with the LEAST operational effort? (Choose two.)

- A.Package the application into a .zip file by using a command line tool. Upload the package to Amazon S3.
- B.Package the application into a container image by using the Docker CLI. Upload the image to Amazon Elastic Container Registry (Amazon ECR).
- C.Deploy the application to an Amazon EC2 instance by using AWS CodeDeploy.
- D.Deploy the application to Amazon Elastic Kubernetes Service (Amazon EKS) on AWS Fargate.
- E.Deploy the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.

**Answer: BE**

**Explanation:**

B.Package the application into a container image by using the Docker CLI. Upload the image to Amazon Elastic Container Registry (Amazon ECR).

E.Deploy the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.

**CertyIQ**

A developer supports an application that accesses data in an Amazon DynamoDB table. One of the item attributes is expirationDate in the timestamp format. The application uses this attribute to find items, archive them, and remove them from the table based on the timestamp value.

The application will be decommissioned soon, and the developer must find another way to implement this functionality. The developer needs a solution that will require the least amount of code to write.

Which solution will meet these requirements?

A.Enable TTL on the expirationDate attribute in the table. Create a DynamoDB stream. Create an AWS Lambda function to process the deleted items. Create a DynamoDB trigger for the Lambda function.

B.Create two AWS Lambda functions: one to delete the items and one to process the items. Create a DynamoDB stream. Use the DeleteItem API operation to delete the items based on the expirationDate attribute. Use the GetRecords API operation to get the items from the DynamoDB stream and process them.

C.Create two AWS Lambda functions: one to delete the items and one to process the items. Create an Amazon EventBridge scheduled rule to invoke the Lambda functions. Use the DeleteItem API operation to delete the items based on the expirationDate attribute. Use the GetRecords API operation to get the items from the DynamoDB table and process them.

D.Enable TTL on the expirationDate attribute in the table. Specify an Amazon Simple Queue Service (Amazon SQS) dead-letter queue as the target to delete the items. Create an AWS Lambda function to process the items.

**Answer: A**

**Explanation:**

Enable TTL on the expirationDate attribute in the table. Create a DynamoDB stream. Create an AWS Lambda function to process the deleted items. Create a DynamoDB trigger for the Lambda function.

**CertyIQ**

**Question: 276**

A developer needs to implement a custom machine learning (ML) library in an application. The size of the library is 15 GB. The size of the library is increasing. The application uses AWS Lambda functions. All the Lambda functions must have access to the library.

Which solution will meet these requirements?

A.Save the library in Lambda layers. Attach the layers to all Lambda functions.

B.Save the library in Amazon S3. Download the library from Amazon S3 inside the Lambda function.

C.Save the library as a Lambda container image. Redeploy the Lambda functions with the new image.

D.Save the library in an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system in all the Lambda functions.

**Answer: D**

**Explanation:**

Save the library in an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system in all the Lambda functions.

**CertyIQ**

**Question: 277**

A developer is designing a serverless application for a game in which users register and log in through a web browser. The application makes requests on behalf of users to a set of AWS Lambda functions that run behind an Amazon API Gateway HTTP API.

The developer needs to implement a solution to register and log in users on the application's sign-in page. The solution must minimize operational overhead and must minimize ongoing management of user identities.

Which solution will meet these requirements?

- A.Create Amazon Cognito user pools for external social identity providers. Configure IAM roles for the identity pools.
- B.Program the sign-in page to create users' IAM groups with the IAM roles attached to the groups.
- C.Create an Amazon RDS for SQL Server DB instance to store the users and manage the permissions to the backend resources in AWS.
- D.Configure the sign-in page to register and store the users and their passwords in an Amazon DynamoDB table with an attached IAM policy.

**Answer: A**

**Explanation:**

Create Amazon Cognito user pools for external social identity providers. Configure IAM roles for the identity pools.

**CertyIQ**

**Question: 278**

A company has a web application that is hosted on Amazon EC2 instances. The EC2 instances are configured to stream logs to Amazon CloudWatch Logs. The company needs to receive an Amazon Simple Notification Service (Amazon SNS) notification when the number of application error messages exceeds a defined threshold within a 5-minute period.

Which solution will meet these requirements?

- A.Rewrite the application code to stream application logs to Amazon SNS. Configure an SNS topic to send a notification when the number of errors exceeds the defined threshold within a 5-minute period.
- B.Configure a subscription filter on the CloudWatch Logs log group. Configure the filter to send an SNS notification when the number of errors exceeds the defined threshold within a 5-minute period.
- C.Install and configure the Amazon Inspector agent on the EC2 instances to monitor for errors. Configure Amazon Inspector to send an SNS notification when the number of errors exceeds the defined threshold within a 5-minute period.
- D.Create a CloudWatch metric filter to match the application error pattern in the log data. Set up a CloudWatch alarm based on the new custom metric. Configure the alarm to send an SNS notification when the number of errors exceeds the defined threshold within a 5-minute period.

**Answer: D**

**Explanation:**

Create a Cloud Watch metric filter to match the application error pattern in the log data. Set up a Cloud Watch alarm based on the new custom metric. Configure the alarm to send an SNS notification when the number of errors exceeds the defined threshold within a 5-minute period.

**Question: 279****CertyIQ**

A photo sharing application uses Amazon S3 to store image files. All user images are manually audited for inappropriate content by a third-party company. The audits are completed 1-24 hours after user upload and the results are written to an Amazon DynamoDB table, which uses the S3 object key as a primary key. The database items can be queried by using a REST API created by the third-party company.

An application developer needs to implement an automated process to tag all S3 objects with the results of the content audit.

What should the developer do to meet these requirements in the MOST operationally efficient way?

- A.Create an AWS Lambda function to run in response to the s3:ObjectCreated event type. Write the S3 key to an Amazon Simple Queue Service (Amazon SQS) queue with a visibility timeout of 24 hours. Create and configure a second Lambda function to read items from the queue. Retrieve the results for each item from the DynamoDB table. Tag each S3 object accordingly.
- B.Create an AWS Lambda function to run in response to the s3:ObjectCreated event type. Integrate the function into an AWS Step Functions standard workflow. Define an AWS Step Functions Wait state and set the value to 24 hours. Create and configure a second Lambda function to retrieve the audit results and tag the S3 objects accordingly after the Wait state is over.
- C.Create an AWS Lambda function to load all untagged S3 objects. Retrieve the results for each item from the REST API and tag each S3 object accordingly. Create and configure an Amazon EventBridge rule to run at regular intervals. Set the Lambda function as a target for the EventBridge rule.
- D.Launch an Amazon EC2 instance. Deploy a script to the EC2 instance to use the external database results to tag the S3 objects accordingly. Configure a crontab file to run the script at regular intervals.

**Answer: C****Explanation:**

Create an AWS Lambda function to load all untagged S3 objects. Retrieve the results for each item from the REST API and tag each S3 object accordingly. Create and configure an Amazon Event Bridge rule to run at regular intervals. Set the Lambda function as a target for the Event Bridge rule.

**Question: 280****CertyIQ**

A company has built an AWS Lambda function to convert large image files into output files that can be used in a third-party viewer application. The company recently added a new module to the function to improve the output of the generated files. However, the new module has increased the bundle size and has increased the time that is needed to deploy changes to the function code.

How can a developer increase the speed of the Lambda function deployment?

- A.Use AWS CodeDeploy to deploy the function code.
- B.Use Lambda layers to package and load dependencies.
- C.Increase the memory size of the function.
- D.Use Amazon S3 to host the function dependencies.

**Answer: B****Explanation:**

B. Use Lambda layers to package and load dependencies.

Lambda layers are a way to manage your function's dependencies separately, reducing the size of the deployment package that needs to be uploaded when the function's code changes. By moving the large module or other dependencies to a Lambda layer, only changes to the function's own code need to be uploaded during deployment, which can significantly speed up the deployment process. This approach allows for more efficient management of libraries and dependencies, making deployments quicker and more streamlined without altering the function's memory size, which would not directly impact deployment speed, or relying on external services like Amazon S3 or AWS CodeDeploy in a way that doesn't specifically address deployment speed for large dependencies.

**Question: 281****CertyIQ**

A developer creates a static website for their department. The developer deploys the static assets for the website to an Amazon S3 bucket and serves the assets with Amazon CloudFront. The developer uses origin access control (OAC) on the CloudFront distribution to access the S3 bucket.

The developer notices users can access the root URL and specific pages but cannot access directories without specifying a file name. For example, /products/index.html works, but /products/ returns an error. The developer needs to enable accessing directories without specifying a file name without exposing the S3 bucket publicly.

Which solution will meet these requirements?

- A.Update the CloudFront distribution's settings to index.html as the default root object is set.
- B.Update the Amazon S3 bucket settings and enable static website hosting. Specify index.html as the Index document. Update the S3 bucket policy to enable access. Update the CloudFront distribution's origin to use the S3 website endpoint.
- C.Create a CloudFront function that examines the request URL and appends index.html when directories are being accessed. Add the function as a viewer request CloudFront function to the CloudFront distribution's behavior.
- D.Create a custom error response on the CloudFront distribution with the HTTP error code set to the HTTP 404 Not Found response code and the response page path to /index.html. Set the HTTP response code to the HTTP 200 OK response code.

**Answer: C****Explanation:**

Create a CloudFront function that examines the request URL and appends index.html when directories are being accessed. Add the function as a viewer request CloudFront function to the CloudFront distribution's behavior.

**Question: 282****CertyIQ**

A developer is testing a RESTful application that is deployed by using Amazon API Gateway and AWS Lambda. When the developer tests the user login by using credentials that are not valid, the developer receives an HTTP 405: METHOD\_NOT\_ALLOWED error. The developer has verified that the test is sending the correct request for the resource.

Which HTTP error should the application return in response to the request?

- A.HTTP 401
- B.HTTP 404
- C.HTTP 503
- D.HTTP 505

**Answer: A**

**Explanation:**

Correct answer is A:HTTP 401.

**CertyIQ**

**Question: 283**

A developer must use multi-factor authentication (MFA) to access data in an Amazon S3 bucket that is in another AWS account.

Which AWS Security Token Service (AWS STS) API operation should the developer use with the MFA information to meet this requirement?

- A.AssumeRoleWithWebIdentity
- B.GetFederationToken
- C.AssumeRoleWithSAML
- D.AssumeRole

**Answer: D**

**Explanation:**

Correct answer is D:AssumeRole.

**CertyIQ**

**Question: 284**

A developer designed an application on an Amazon EC2 instance. The application makes API requests to objects in an Amazon S3 bucket.

Which combination of steps will ensure that the application makes the API requests in the MOST secure manner? (Choose two.)

- A.Create an IAM user that has permissions to the S3 bucket. Add the user to an IAM group.
- B.Create an IAM role that has permissions to the S3 bucket.
- C.Add the IAM role to an instance profile. Attach the instance profile to the EC2 instance.
- D.Create an IAM role that has permissions to the S3 bucket. Assign the role to an IAM group.
- E.Store the credentials of the IAM user in the environment variables on the EC2 instance.

**Answer: BC**

**Explanation:**

B.Create an IAM role that has permissions to the S3 bucket.

C.Add the IAM role to an instance profile. Attach the instance profile to the EC2 instance.

**Question: 285**

CertyIQ

An AWS Lambda function requires read access to an Amazon S3 bucket and requires read/write access to an Amazon DynamoDB table. The correct IAM policy already exists.

What is the MOST secure way to grant the Lambda function access to the S3 bucket and the DynamoDB table?

- A.Attach the existing IAM policy to the Lambda function.
- B.Create an IAM role for the Lambda function. Attach the existing IAM policy to the role. Attach the role to the Lambda function.
- C.Create an IAM user with programmatic access. Attach the existing IAM policy to the user. Add the user access key ID and secret access key as environment variables in the Lambda function.
- D.Add the AWS account root user access key ID and secret access key as encrypted environment variables in the Lambda function.

**Answer: B****Explanation:**

Create an IAM role for the Lambda function. Attach the existing IAM policy to the role. Attach the role to the Lambda function.

**Question: 286**

CertyIQ

A developer is using AWS Step Functions to automate a workflow. The workflow defines each step as an AWS Lambda function task. The developer notices that runs of the Step Functions state machine fail in the GetResource task with either an `IllegalArgumentException` error or a `TooManyRequestsException` error.

The developer wants the state machine to stop running when the state machine encounters an `IllegalArgumentException` error. The state machine needs to retry the GetResource task one additional time after 10 seconds if the state machine encounters a `TooManyRequestsException` error. If the second attempt fails, the developer wants the state machine to stop running.

How can the developer implement the Lambda retry functionality without adding unnecessary complexity to the state machine?

- A.Add a Delay task after the GetResource task. Add a catcher to the GetResource task. Configure the catcher with an error type of `TooManyRequestsException`. Configure the next step to be the Delay task. Configure the Delay task to wait for an interval of 10 seconds. Configure the next step to be the GetResource task.
- B.Add a catcher to the GetResource task. Configure the catcher with an error type of `TooManyRequestsException`, an interval of 10 seconds, and a maximum attempts value of 1. Configure the next step to be the GetResource task.
- C.Add a retrier to the GetResource task. Configure the retrier with an error type of `TooManyRequestsException`, an interval of 10 seconds, and a maximum attempts value of 1.
- D.Duplicate the GetResource task. Rename the new GetResource task to TryAgain. Add a catcher to the original GetResource task. Configure the catcher with an error type of `TooManyRequestsException`. Configure the next step to be TryAgain.

**Answer: C****Explanation:**

Add a retrier to the GetResource task. Configure the retrier with an error type of `TooManyRequestsException`, an interval of 10 seconds, and a maximum attempts value of 1.

**Question: 287**

CertyIQ

A developer is creating a serverless application that uses an AWS Lambda function. The developer will use AWS CloudFormation to deploy the application. The application will write logs to Amazon CloudWatch Logs. The developer has created a log group in a CloudFormation template for the application to use. The developer needs to modify the CloudFormation template to make the name of the log group available to the application at runtime.

Which solution will meet this requirement?

- A.Use the AWS::Include transform in CloudFormation to provide the log group's name to the application.
- B.Pass the log group's name to the application in the user data section of the CloudFormation template.
- C.Use the CloudFormation template's Mappings section to specify the log group's name for the application.
- D.Pass the log group's Amazon Resource Name (ARN) as an environment variable to the Lambda function.

**Answer: D****Explanation:**

Pass the log group's Amazon Resource Name (ARN) as an environment variable to the Lambda function.

**Question: 288**

CertyIQ

A developer is creating an Amazon DynamoDB table by using the AWS CLI. The DynamoDB table must use server-side encryption with an AWS owned encryption key.

How should the developer create the DynamoDB table to meet these requirements?

- A.Create an AWS Key Management Service (AWS KMS) customer managed key. Provide the key's Amazon Resource Name (ARN) in the KMSMasterKeyId parameter during creation of the DynamoDB table.
- B.Create an AWS Key Management Service (AWS KMS) AWS managed key. Provide the key's Amazon Resource Name (ARN) in the KMSMasterKeyId parameter during creation of the DynamoDB table.
- C.Create an AWS owned key. Provide the key's Amazon Resource Name (ARN) in the KMSMasterKeyId parameter during creation of the DynamoDB table.
- D.Create the DynamoDB table with the default encryption options.

**Answer: D****Explanation:**

Create the DynamoDB table with the default encryption options.

**Question: 289**

CertyIQ

A company has an application that runs across multiple AWS Regions. The application is experiencing performance issues at irregular intervals. A developer must use AWS X-Ray to implement distributed tracing for the application to troubleshoot the root cause of the performance issues.

What should the developer do to meet this requirement?

- A.Use the X-Ray console to add annotations for AWS services and user-defined services.
- B.Use Region annotation that X-Ray adds automatically for AWS services. Add Region annotation for user-defined services.
- C.Use the X-Ray daemon to add annotations for AWS services and user-defined services.
- D.Use Region annotation that X-Ray adds automatically for user-defined services. Configure X-Ray to add

Region annotation for AWS services.

**Answer: B**

**Explanation:**

Use Region annotation that X-Ray adds automatically for AWS services. Add Region annotation for user-defined services.

**CertyIQ**

**Question: 290**

A company runs an application on AWS. The application uses an AWS Lambda function that is configured with an Amazon Simple Queue Service (Amazon SQS) queue called high priority queue as the event source. A developer is updating the Lambda function with another SQS queue called low priority queue as the event source. The Lambda function must always read up to 10 simultaneous messages from the high priority queue before processing messages from low priority queue. The Lambda function must be limited to 100 simultaneous invocations.

Which solution will meet these requirements?

- A. Set the event source mapping batch size to 10 for the high priority queue and to 90 for the low priority queue.
- B. Set the delivery delay to 0 seconds for the high priority queue and to 10 seconds for the low priority queue.
- C. Set the event source mapping maximum concurrency to 10 for the high priority queue and to 90 for the low priority queue.
- D. Set the event source mapping batch window to 10 for the high priority queue and to 90 for the low priority queue.

**Answer: C**

**Explanation:**

Set the event source mapping maximum concurrency to 10 for the high priority queue and to 90 for the low priority queue.

**CertyIQ**

**Question: 291**

A data visualization company wants to strengthen the security of its core applications. The applications are deployed on AWS across its development, staging, pre-production, and production environments. The company needs to encrypt all of its stored sensitive credentials. The sensitive credentials need to be automatically rotated. A version of the sensitive credentials need to be stored for each environment.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. Configure AWS Secrets Manager versions to store different copies of the same credentials across multiple environments.
- B. Create a new parameter version in AWS Systems Manager Parameter Store for each environment. Store the environment-specific credentials in the parameter version.
- C. Configure the environment variables in the application code. Use different names for each environment type.
- D. Configure AWS Secrets Manager to create a new secret for each environment type. Store the environment-specific credentials in the secret.

**Answer: D**

**Explanation:**

D. Configure AWS Secrets Manager to create a new secret for each environment type. Store the environment-specific credentials in the secret.

AWS Secrets Manager supports the encryption of secrets (including sensitive credentials) and allows for automatic rotation of these secrets. By creating a new secret for each environment (development, staging, pre-production, and production), you can manage and access the environment-specific credentials securely. This approach facilitates operational efficiency by leveraging AWS Secrets Manager's built-in capabilities for encryption and rotation, without the need for manual intervention or complex configurations. Secrets Manager also provides a straightforward way to retrieve the correct version of the credentials for each specific environment, simplifying the management of sensitive data across different stages of application deployment.

### Question: 292

CertyIQ

A developer is investigating an issue in part of a company's application. In the application, messages are sent to an Amazon Simple Queue Service (Amazon SQS) queue. The AWS Lambda function polls messages from the SQS queue and sends email messages by using Amazon Simple Email Service (Amazon SES). Users have been receiving duplicate email messages during periods of high traffic.

Which reasons could explain the duplicate email messages? (Choose two.)

- A.Standard SQS queues support at-least-once message delivery.
- B.Standard SQS queues support exactly-once processing, so the duplicate email messages are because of user error.
- C.Amazon SES has the DomainKeys Identified Mail (DKIM) authentication incorrectly configured.
- D.The SQS queue's visibility timeout is lower than or the same as the Lambda function's timeout.
- E.The Amazon SES bounce rate metric is too high.

### Answer: AD

#### Explanation:

- A.Standard SQS queues support at-least-once message delivery.
- D.The SQS queue's visibility timeout is lower than or the same as the Lambda function's timeout.

### Question: 293

CertyIQ

A developer is deploying a company's application to Amazon EC2 instances. The application generates gigabytes of data files each day. The files are rarely accessed, but the files must be available to the application's users within minutes of a request during the first year of storage. The company must retain the files for 7 years.

How can the developer implement the application to meet these requirements MOST cost-effectively?

- A.Store the files in an Amazon S3 bucket. Use the S3 Glacier Instant Retrieval storage class. Create an S3 Lifecycle policy to transition the files to the S3 Glacier Deep Archive storage class after 1 year.
- B.Store the files in an Amazon S3 bucket. Use the S3 Standard storage class. Create an S3 Lifecycle policy to transition the files to the S3 Glacier Flexible Retrieval storage class after 1 year.
- C.Store the files on an Amazon Elastic Block Store (Amazon EBS) volume. Use Amazon Data Lifecycle Manager (Amazon DLM) to create snapshots of the EBS volumes and to store those snapshots in Amazon S3.
- D.Store the files on an Amazon Elastic File System (Amazon EFS) mount. Configure EFS lifecycle management to transition the files to the EFS Standard- Infrequent Access (Standard-IA) storage class after 1 year.

**Answer: A**

**Explanation:**

Store the files in an Amazon S3 bucket. Use the S3 Glacier Instant Retrieval storage class. Create an S3 Lifecycle policy to transition the files to the S3 Glacier Deep Archive storage class after 1 year.

CertyIQ

**Question: 294**

A company's developer has deployed an application in AWS by using AWS CloudFormation. The CloudFormation stack includes parameters in AWS Systems Manager Parameter Store that the application uses as configuration settings. The application can modify the parameter values.

When the developer updated the stack to create additional resources with tags, the developer noted that the parameter values were reset and that the values ignored the latest changes made by the application. The developer needs to change the way the company deploys the CloudFormation stack. The developer also needs to avoid resetting the parameter values outside the stack.

Which solution will meet these requirements with the LEAST development effort?

- A.Modify the CloudFormation stack to set the deletion policy to Retain for the Parameter Store parameters.
- B.Create an Amazon DynamoDB table as a resource in the CloudFormation stack to hold configuration data for the application. Migrate the parameters that the application is modifying from Parameter Store to the DynamoDB table.
- C.Create an Amazon RDS DB instance as a resource in the CloudFormation stack. Create a table in the database for parameter configuration. Migrate the parameters that the application is modifying from Parameter Store to the configuration table.
- D.Modify the CloudFormation stack policy to deny updates on Parameter Store parameters.

**Answer: D**

**Explanation:**

Modify the CloudFormation stack policy to deny updates on Parameter Store parameters.

CertyIQ

**Question: 295**

A company has a social media application that receives large amounts of traffic. User posts and interactions are continuously updated in an Amazon RDS database. The data changes frequently, and the data types can be complex. The application must serve read requests with minimal latency.

The application's current architecture struggles to deliver these rapid data updates efficiently. The company needs a solution to improve the application's performance.

Which solution will meet these requirements?

- A.Use Amazon DynamoDB Accelerator (DAX) in front of the RDS database to provide a caching layer for the high volume of rapidly changing data.
- B.Set up Amazon S3 Transfer Acceleration on the RDS database to enhance the speed of data transfer from the databases to the application.
- C.Add an Amazon CloudFront distribution in front of the RDS database to provide a caching layer for the high volume of rapidly changing data.
- D.Create an Amazon ElastiCache for Redis cluster. Update the application code to use a write-through caching strategy and read the data from Redis.

**Answer: D**

**Explanation:**

Create an Amazon ElastiCache for Redis cluster. Update the application code to use a write-through caching strategy and read the data from Redis.

**CertyIQ**

**Question: 296**

A developer created an AWS Lambda function that performs a series of operations that involve multiple AWS services. The function's duration time is higher than normal. To determine the cause of the issue, the developer must investigate traffic between the services without changing the function code.

Which solution will meet these requirements?

- A.Enable AWS X-Ray active tracing in the Lambda function. Review the logs in X-Ray.
- B.Configure AWS CloudTrail. View the trail logs that are associated with the Lambda function.
- C.Review the AWS Config logs in Amazon CloudWatch.
- D.Review the Amazon CloudWatch logs that are associated with the Lambda function.

**Answer: A**

**Explanation:**

A. Enable AWS X-Ray active tracing in the Lambda function. Review the logs in X-Ray.X-Ray provides insights into the duration and performance of each component, helping you identify the root cause of performance issues without modifying the function code.

**CertyIQ**

**Question: 297**

A company has on-premises data centers that run an image processing service. The service consists of containerized applications that run on Kubernetes clusters. All the applications have access to the same NFS share for files and data storage.

The company is running out of NFS capacity in the data centers and needs to migrate to AWS as soon as possible. The Kubernetes clusters must be highly available on AWS.

Which combination of actions will meet these requirements? (Choose two.)

- A.Transfer the information that is in the NFS share to an Amazon Elastic Block Store (Amazon EBS) volume. Upload the container images to Amazon Elastic Container Registry (Amazon ECR).
- B.Transfer the information that is in the NFS share to an Amazon Elastic File System (Amazon EFS) volume. Upload the container images to Amazon Elastic Container Registry (Amazon ECR).
- C.Create an Amazon Elastic Container Service (Amazon ECS) cluster to run the applications. Configure each node of the cluster to mount the Amazon Elastic Block Store (Amazon EBS) volume at the required path for the container images.
- D.Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster to run the applications. Configure each node of the cluster to mount the Amazon Elastic Block Store (Amazon EBS) volume at the required path for the container images.
- E.Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster to run the applications. Configure each node of the cluster to mount the Amazon Elastic File System (Amazon EFS) volume at the required path for the container images.

**Answer: BE**

**Explanation:**

- B.Transfer the information that is in the NFS share to an Amazon Elastic File System (Amazon EFS) volume. Upload the container images to Amazon Elastic Container Registry (Amazon ECR).
- E.Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster to run the applications. Configure each node of the cluster to mount the Amazon Elastic File System (Amazon EFS) volume at the required path for the container images.

**CertyIQ****Question: 298**

A company has an analytics application that uses an AWS Lambda function to process transaction data asynchronously. A developer notices that asynchronous invocations of the Lambda function sometimes fail. When failed Lambda function invocations occur, the developer wants to invoke a second Lambda function to handle errors and log details.

Which solution will meet these requirements?

- A.Configure a Lambda function destination with a failure condition. Specify Lambda function as the destination type. Specify the error-handling Lambda function's Amazon Resource Name (ARN) as the resource.
- B.Enable AWS X-Ray active tracing on the initial Lambda function. Configure X-Ray to capture stack traces of the failed invocations. Invoke the error-handling Lambda function by including the stack traces in the event object.
- C.Configure a Lambda function trigger with a failure condition. Specify Lambda function as the destination type. Specify the error-handling Lambda function's Amazon Resource Name (ARN) as the resource.
- D.Create a status check alarm on the initial Lambda function. Configure the alarm to invoke the error-handling Lambda function when the alarm is initiated. Ensure that the alarm passes the stack trace in the event object.

**Answer: A****Explanation:**

Configure a Lambda function destination with a failure condition. Specify Lambda function as the destination type. Specify the error-handling Lambda function's Amazon Resource Name (ARN) as the resource.

**CertyIQ****Question: 299**

A company introduced a new feature that should be accessible to only a specific group of premium customers. A developer needs the ability to turn the feature on and off in response to performance and feedback. The developer needs a solution to validate and deploy these configurations quickly without causing any disruptions.

What should the developer do to meet these requirements?

- A.Use AWS AppConfig to manage the feature configuration and to validate and deploy changes. Use feature flags to turn the feature on and off.
- B.Use AWS Secrets Manager to securely manage and validate the feature configurations. Enable lifecycle rules to turn the feature on and off.
- C.Use AWS Config to manage the feature configuration and validation. Set up AWS Config rules to turn the feature on and off based on predefined conditions.
- D.Use AWS Systems Manager Parameter Store to store and validate the configuration settings for the feature. Enable lifecycle rules to turn the feature on and off.

**Answer: A**

**Explanation:**

Use AWS AppConfig to manage the feature configuration and to validate and deploy changes. Use feature flags to turn the feature on and off.

**Question: 300****CertyIQ**

A developer needs approval from a product owner before the developer can deploy code for an application to production. The developer uses AWS CodePipeline to deploy the application. The developer configures an Amazon Simple Notification Service (Amazon SNS) topic to send notifications to the product owner.

Which solution is the MOST operationally efficient way for the developer to receive approval from the product owner?

- A.Add a new stage to CodePipeline before the production deployment. Add a manual approval action to the new stage. Add a new notification rule in the pipeline settings. Specify manual approval as the event that initiates the notification. Specify the SNS topic's Amazon Resource Name (ARN) to notify the product owner.
- B.Develop an AWS Step Functions state machine that sends a notification to the product owner and accepts an approval. Add a new stage to CodePipeline before the production deployment. Add the state machine as a Step Functions action to the new stage.
- C.Add a manual approval action to the existing production deployment stage in CodePipeline. Specify the SNS topic's Amazon Resource Name (ARN) while configuring the new manual approval action.
- D.Edit the settings in CodePipeline. Create a new notification rule. Specify manual approval as the event that initiates the notification. Create a new notification target. Specify the SNS topic to notify the product owner. Save the notification rule.

**Answer: A****Explanation:**

Add a new stage to CodePipeline before the production deployment. Add a manual approval action to the new stage. Add a new notification rule in the pipeline settings. Specify manual approval as the event that initiates the notification. Specify the SNS topic's Amazon Resource Name (ARN) to notify the product owner.

**Question: 301****CertyIQ**

A developer is building a serverless application on AWS for a workflow that processes high volumes of data. In the workflow, an AWS Step Functions state machine invokes several AWS Lambda functions.

One of the Lambda functions occasionally fails because of timeout errors during periods of high demand. The developer must ensure that the workflow automatically retries the failed function invocation if a timeout error occurs.

Which solution will meet this requirement?

- A.Add a Retry field in the Step Functions state machine definition. Configure the state machine with the maximum number of retry attempts and the timeout error type to retry on.
- B.Add a Timeout field in the Step Functions state machine definition. Configure the state machine with the maximum number of retry attempts.
- C.Add a Fail state to the Step Functions state machine definition. Configure the state machine with the maximum number of retry attempts.
- D.Update the Step Functions state machine to pass the invocation request to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe a Lambda function to the SNS topic. Configure the Lambda function with the maximum number of retry attempts for a timeout error type.

**Answer: A**

**Explanation:**

Add a Retry field in the Step Functions state machine definition. Configure the state machine with the maximum number of retry attempts and the timeout error type to retry on.

**CertyIQ**

**Question: 302**

A company runs a serverless application on AWS. The application includes an AWS Lambda function. The Lambda function processes data and stores the data in an Amazon RDS for PostgreSQL database. A developer created a user credentials in the database for the application.

The developer needs to use AWS Secrets Manager to manage the user credentials. The password must to be rotated on a regular basis. The solution needs to ensure that there is high availability and no downtime for the application during secret rotation.

What should the developer do to meet these requirements?

- A.Configure managed rotation with the single user rotation strategy.
- B.Configure managed rotation with the alternating users rotation strategy.
- C.Configure automatic rotation with the single user rotation strategy.
- D.Configure automatic rotation with the alternating users rotation strategy.

**Answer: D**

**Explanation:**

Configure automatic rotation with the alternating users rotation strategy.

**CertyIQ**

**Question: 303**

A company runs an application on AWS. The application consists of a static website that is hosted on Amazon S3. The application includes Amazon API Gateway APIs that invoke AWS Lambda functions. During a period of high traffic on the application, application users reported that the application was slow at irregular intervals. There were no failed requests.

A developer needs to find the slow executions across all the Lambda functions.

Which solution will meet these requirements?

- A.Perform a query across all the Lambda function log groups by using Amazon CloudWatch Logs Insights. Filter on type of report and sort descending by Lambda function execution duration.
- B.Enable AWS CloudTrail Insights on the account where the Lambda functions are running. After CloudTrail Insights has finished processing, review CloudTrail Insights to find the anomalous functions.
- C.Enable AWS X-Ray for all the Lambda functions. Configure an X-Ray insight on a new group that includes all the Lambda functions. After the X-Ray insight has finished processing, review the X-Ray logs.
- D.Set up AWS Glue to crawl through the logs in Amazon CloudWatch Logs for the Lambda functions. Configure an AWS Glue job to transform the logs into a structured format and to output the logs into Amazon S3. Use the Amazon CloudWatch dashboard to visualize the slowest functions based on the duration.

**Answer: C**

**Explanation:**

Enable AWS X-Ray for all the Lambda functions. Configure an X-Ray insight on a new group that includes all the Lambda functions. After the X-Ray insight has finished processing, review the X-Ray logs.

### Question: 304

CertyIQ

A company is building a serverless application on AWS. The application uses Amazon API Gateway and AWS Lambda. The company wants to deploy the application to its development, test, and production environments.

Which solution will meet these requirements with the LEAST development effort?

- A.Use API Gateway stage variables and create Lambda aliases to reference environment-specific resources.
- B.Use Amazon Elastic Container Service (Amazon ECS) to deploy the application to the environments.
- C.Duplicate the code for each environment. Deploy the code to a separate API Gateway stage.
- D.Use AWS Elastic Beanstalk to deploy the application to the environments.

**Answer: A**

**Explanation:**

Use API Gateway stage variables and create Lambda aliases to reference environment-specific resources.

### Question: 305

CertyIQ

A developer uses AWS CloudFormation to deploy an Amazon API Gateway API and an AWS Step Functions state machine. The state machine must reference the API Gateway API after the CloudFormation template is deployed. The developer needs a solution that uses the state machine to reference the API Gateway endpoint.

Which solution will meet these requirements MOST cost-effectively?

- A.Configure the CloudFormation template to reference the API endpoint in the DefinitionSubstitutions property for the AWS::StepFunctions::StateMachine resource.
- B.Configure the CloudFormation template to store the API endpoint in an environment variable for the AWS::StepFunctions::StateMachine resource. Configure the state machine to reference the environment variable.
- C.Configure the CloudFormation template to store the API endpoint in a standard AWS::SecretsManager::Secret resource. Configure the state machine to reference the resource.
- D.Configure the CloudFormation template to store the API endpoint in a standard AWS::AppConfig::ConfigurationProfile resource. Configure the state machine to reference the resource.

**Answer: A**

**Explanation:**

Configure the CloudFormation template to reference the API endpoint in the DefinitionSubstitutions property for the AWS::StepFunctions::StateMachine resource.

### Question: 306

CertyIQ

A developer is building an application on AWS. The application includes an AWS Lambda function that processes messages from an Amazon Simple Queue Service (Amazon SQS) queue.

The Lambda function sometimes fails or times out. The developer needs to figure out why the Lambda function

fails to process some messages.

Which solution will meet these requirements with the LEAST operational overhead?

- A.Increase the maximum timeout of the Lambda function to 15 minutes. Check the AWS CloudTrail event history for error details.
- B.Increase the visibility timeout of the SQS queue. Check logs in Amazon CloudWatch Logs for error details.
- C.Create a dead-letter queue. Configure the Lambda function to send the failed messages to the dead-letter queue.
- D.Create an Amazon DynamoDB table. Update the Lambda function to send the failed messages to the DynamoDB table.

**Answer: C**

**Explanation:**

Create a dead-letter queue. Configure the Lambda function to send the failed messages to the dead-letter queue.

**Question: 307**

**CertyIQ**

A developer needs to deploy an application in three AWS Regions by using AWS CloudFormation. Each Region will use an AWS Elastic Beanstalk environment with an Application Load Balancer (ALB). The developer wants to use AWS Certificate Manager (ACM) to deploy SSL certificates to each ALB.

Which solution will meet these requirements?

- A.Create a certificate in ACM in any one of the Regions. Import the certificate into the ALB that is in each Region.
- B.Create a global certificate in ACM. Update the CloudFormation template to deploy the global certificate to each ALB.
- C.Create a certificate in ACM in each Region. Import the certificate into the ALB for each Region.
- D.Create a certificate in ACM in the us-east-1 Region. Update the CloudFormation template to deploy the certificate to each ALB.

**Answer: C**

**Explanation:**

Create a certificate in ACM in each Region. Import the certificate into the ALB for each Region.

**Question: 308**

**CertyIQ**

A company needs to deploy all its cloud resources by using AWS CloudFormation templates. A developer must create an Amazon Simple Notification Service (Amazon SNS) automatic notification to help enforce this rule. The developer creates an SNS topic and subscribes the email address of the company's security team to the SNS topic.

The security team must receive a notification immediately if an IAM role is created without the use of CloudFormation.

Which solution will meet this requirement?

- A.Create an AWS Lambda function to filter events from CloudTrail if a role was created without CloudFormation. Configure the Lambda function to publish to the SNS topic. Create an Amazon EventBridge

schedule to invoke the Lambda function every 15 minutes.

B.Create an AWS Fargate task in Amazon Elastic Container Service (Amazon ECS) to filter events from CloudTrail if a role was created without CloudFormation. Configure the Fargate task to publish to the SNS topic. Create an Amazon EventBridge schedule to run the Fargate task every 15 minutes.

C.Launch an Amazon EC2 instance that includes a script to filter events from CloudTrail if a role was created without CloudFormation. Configure the script to publish to the SNS topic. Create a cron job to run the script on the EC2 instance every 15 minutes.

D.Create an Amazon EventBridge rule to filter events from CloudTrail if a role was created without CloudFormation. Specify the SNS topic as the target of the EventBridge rule.

**Answer: D**

**Explanation:**

Create an Amazon EventBridge rule to filter events from CloudTrail if a role was created without CloudFormation. Specify the SNS topic as the target of the EventBridge rule.

**CertyIQ**

A company is adopting serverless computing for some of its new services. A development team needs to create a serverless infrastructure by using AWS Serverless Application Model (AWS SAM). All infrastructure must be deployed by using AWS CloudFormation templates.

What should the development team do to meet these requirements?

- A.Add a Resources section to the CloudFormation templates that contains AWS::Lambda::Function resources.
- B.Add a Mappings section to the CloudFormation templates that contains AWS::Serverless::Function and AWS::Serverless::API.
- C.Add a Transform section to the CloudFormation templates. Use the AWS SAM syntax to define the resources.
- D.Add a Parameters section to the CloudFormation templates that specifies the relevant AWS SAM Globals section.

**Answer: C**

**Explanation:**

Add a Transform section to the CloudFormation templates. Use the AWS SAM syntax to define the resources.

**CertyIQ**

**Question: 310**

A developer is building an application that invokes AWS Lambda functions asynchronously to process events. The developer notices that a Lambda function fails to process some events at random times. The developer needs to investigate the failed events and capture the events that the Lambda function fails to process.

Which solution will meet these requirements?

- A.Add an Amazon EventBridge rule for the Lambda function. Configure the EventBridge rule to react to failed events and to store the events in an Amazon DynamoDB table.
- B.Configure the Lambda function with a dead-letter queue based in Amazon Kinesis. Update the Lambda function's execution role with the required permissions.
- C.Configure the Lambda function with an Amazon Simple Queue Service (Amazon SQS) dead-letter queue. Update the Lambda function's execution role with the required permissions.
- D.Configure the Lambda function with an Amazon Simple Queue Service (Amazon SQS) FIFO dead-letter queue. Update the Lambda function's execution role with the required permissions.

**Answer: C****Explanation:**

Configure the Lambda function with an Amazon Simple Queue Service (Amazon SQS) dead-letter queue.

Update the Lambda function's execution role with the required permissions.

**CertyIQ****Question: 311**

A company has built a serverless application for its ecommerce website. The application includes a REST API in Amazon API Gateway that invokes an AWS Lambda function. The Lambda function processes data and stores the data in Amazon DynamoDB table. The Lambda function calls a third-party stock application API to process the order. After the ordered is processed, the Lambda function returns an HTTP 200 status code with no body to the client.

During peak usage when the API calls exceeds a certain threshold, the third-party stock application sometimes fails to process the data and responds with error messages. The company needs a solution that will not overwhelm the third-party stock application.

Which solution will meet these requirements?

- A.Configure the REST API in API Gateway to write the requests directly into DynamoDB. Configure a DynamoDB intrinsic function to perform the transformation. Set up a DynamoDB stream to call the third-party stock application API with each new row. Delete the Lambda function.
- B.Configure the REST API in API Gateway to write the requests directly into an Amazon Simple Queue Service (Amazon SQS) queue. Configure the Lambda function with a reserved concurrency equal to the third-party stock application's threshold. Set Lambda function to process the messages from the SQS queue.
- C.Configure the REST API in API Gateway to write the requests directly into an Amazon Simple Notification Service (Amazon SNS) topic. Configure the Lambda function with a provisioned concurrency equal to the third-party stock application's threshold. Set the Lambda function to process the messages from the SNS topic.
- D.Configure the REST API in API Gateway to write the requests directly into Amazon Athena. Configure the transformation of the data by using SQL with multiple query result locations set up to point to the DynamoDB table and the third-party stock fulfilment application API. Delete the Lambda function.

**Answer: B****Explanation:**

Configure the REST API in API Gateway to write the requests directly into an Amazon Simple Queue Service (Amazon SQS) queue. Configure the Lambda function with a reserved concurrency equal to the third-party stock application's threshold. Set Lambda function to process the messages from the SQS queue.

**CertyIQ****Question: 312**

A company hosts its application on AWS. The application runs on an Amazon Elastic Container Service (Amazon ECS) cluster that uses AWS Fargate. The cluster runs behind an Application Load Balancer. The application stores data in an Amazon Aurora database. A developer encrypts and manages database credentials inside the application.

The company wants to use a more secure credential storage method and implement periodic credential rotation.

Which solution will meet these requirements with the LEAST operational overhead?

- A.Migrate the secret credentials to Amazon RDS parameter groups. Encrypt the parameter by using an AWS Key Management Service (AWS KMS) key. Turn on secret rotation. Use IAM policies and roles to grant AWS KMS permissions to access Amazon RDS.

B.Migrate the credentials to AWS Systems Manager Parameter Store. Encrypt the parameter by using an AWS Key Management Service (AWS KMS) key. Turn on secret rotation. Use IAM policies and roles to grant Amazon ECS Fargate permissions to access to AWS Secrets Manager.

C.Migrate the credentials to ECS Fargate environment variables. Encrypt the credentials by using an AWS Key Management Service (AWS KMS) key. Turn on secret rotation. Use IAM policies and roles to grant Amazon ECS Fargate permissions to access to AWS Secrets Manager.

D.Migrate the credentials to AWS Secrets Manager. Encrypt the credentials by using an AWS Key Management Service (AWS KMS) key. Turn on secret rotation. Use IAM policies and roles to grant Amazon ECS Fargate permissions to access to AWS Secrets Manager by using keys.

**Answer: D**

**Explanation:**

Migrate the credentials to AWS Secrets Manager. Encrypt the credentials by using an AWS Key Management Service (AWS KMS) key. Turn on secret rotation. Use IAM policies and roles to grant Amazon ECS Fargate permissions to access to AWS Secrets Manager by using keys.

**Question: 313**

**CertyIQ**

A company has a mobile app. The app includes an Amazon API Gateway REST API that invokes AWS Lambda functions. The Lambda functions process data from the app.

The company needs to test updated Lambda functions that have new features. The company must conduct these tests with a subset of users before deployment. The tests must not affect other users of the app.

Which solution will meet these requirements with the LEAST amount of operational effort?

A.Create a new version of each Lambda function with a weighted alias. Configure a weight value for each version of the Lambda function. Update the new weighted alias Amazon Resource Name (ARN) in the REST API.

B.Create a new REST API in API Gateway. Set up a Lambda proxy integration to connect to multiple Lambda functions. Enable canary settings on the deployment stage. Specify a smaller percentage of API traffic to go to the new version of the Lambda function.

C.Create a new version of each Lambda function. Integrate a predefined canary deployment in AWS CodeDeploy to slowly shift the traffic to the new versions automatically.

D.Create a new REST API in API Gateway. Set up a Lambda non-proxy integration to connect to multiple Lambda functions. Specify the necessary parameters and properties in API Gateway. Enable canary settings on the deployment stage. Specify a smaller percentage of API traffic to go to the new version of the Lambda function.

**Answer: B**

**Explanation:**

Create a new REST API in API Gateway. Set up a Lambda proxy integration to connect to multiple Lambda functions. Enable canary settings on the deployment stage. Specify a smaller percentage of API traffic to go to the new version of the Lambda function.

**Question: 314**

**CertyIQ**

A developer works for a company that only has a single pre-production AWS account with an AWS CloudFormation AWS Serverless Application Model (AWS SAM) stack. The developer made changes to an existing AWS Lambda function specified in the AWS SAM template and additional Amazon Simple Notification service (Amazon SNS) topics.

The developer wants to do a one-time deploy of the changes to test if the changes are working. The developer does not want to impact the existing pre-production application that is currently being used by other team members as part of the release pipeline.

Which solution will meet these requirements?

- A.Use the AWS SAM CLI to package and deploy the SAM application to the pre-production AWS account. Specify the debug parameter.
- B.Use the AWS SAM CLI to package and create a change set against the pre-production AWS account. Execute the change set in a new AWS account designated for a development environment.
- C.Use the AWS SAM CLI to package and deploy the SAM application to a new AWS account designated for a development environment.
- D.Update the CloudFormation stack in the pre-production account. Add a separate stage that points to a new AWS account designated for a development environment.

**Answer: C**

**Explanation:**

Use the AWS SAM CLI to package and deploy the SAM application to a new AWS account designated for a development environment.

### Question: 315

CertyIQ

A company built an online event platform. For each event, the company organizes quizzes and generates leaderboards that are based on the quiz scores. The company stores the leaderboard data in Amazon DynamoDB and retains the data for 30 days after an event is complete. The company then uses a scheduled job to delete the old leaderboard data.

The DynamoDB table is configured with a fixed write capacity. During the months when many events occur, the DynamoDB write API requests are throttled when the scheduled delete job runs.

A developer must create a long-term solution that deletes the old leaderboard data and optimizes write throughput.

Which solution meets these requirements?

- A.Configure a TTL attribute for the leaderboard data.
- B.Use DynamoDB Streams to schedule and delete the leaderboard data.
- C.Use AWS Step Functions to schedule and delete the leaderboard data.
- D.Set a higher write capacity when the scheduled delete job runs.

**Answer: A**

**Explanation:**

Configure a TTL attribute for the leaderboard data.

### Question: 316

CertyIQ

A company uses an AWS Lambda function that reads messages from an Amazon Simple Queue Service (Amazon SQS) standard queue. The Lambda function makes an HTTP call to a third-party API for each message. The company wants to ensure that the Lambda function does not overwhelm the third-party API with more than two concurrent requests.

Which solution will meet these requirements?

- A.Configure a provisioned concurrency of two on the Lambda function.
- B.Configure a batch size of two on the Amazon SQS event source mapping for the Lambda function.
- C.Configure Lambda event filtering to process two messages from Amazon SQS at every invocations.
- D.Configure a maximum concurrency of two on the Amazon SQS event source mapping for the Lambda function.

**Answer: D**

**Explanation:**

Configure a maximum concurrency of two on the Amazon SQS event source mapping for the Lambda function.

### Question: 317

**CertyIQ**

A company is using Amazon API Gateway to develop an API for its application on AWS. A developer needs to test and generate API responses. Other teams are required to test the API immediately.

What should the developer do to meet these requirements?

- A.Set up a mock integration request in API Gateway. Configure the method's integration request and integration response to associate a response with a given status code.
- B.Set up the request validators in the API's OpenAPI definition file. Import the OpenAPI definitions into API Gateway to test the API.
- C.Set up a gateway response for the API in API Gateway. Configure response headers with hardcoded HTTP status codes and responses.
- D.Set up a request parameter-based Lambda authorizer to control access to the API. Configure the Lambda function with the necessary mapping template.

**Answer: A**

**Explanation:**

Set up a mock integration request in API Gateway. Configure the method's integration request and integration response to associate a response with a given status code.

### Question: 318

**CertyIQ**

A company is releasing a new feature. Users can request early access to the new feature by using an application form. The company expects a surge of requests when the application form becomes available. Each request will be stored as an item in an Amazon DynamoDB table.

Each item will contain the user's username, the submission date, and a validation status of UNVALIDATED, VALID, or NOT VALID. Each item also will contain the user's rating of the process on a scale of 1 to 5.

Each user can submit one request. For the DynamoDB table, the developer must choose a partition key that will give the workload well-distributed records across partitions.

Which DynamoDB attribute will meet these requirements?

- A.Username
- B.Submission date
- C.Validation status

D.Rating of the process on a scale of 1 to 5

**Answer: A**

**Explanation:**

Correct answer is A:Username.

**CertyIQ**

**Question: 319**

A developer is creating a publicly accessible enterprise website consisting of only static assets. The developer is hosting the website in Amazon S3 and serving the website to users through an Amazon CloudFront distribution. The users of this application must not be able to access the application content directly from an S3 bucket. All content must be served through the Amazon CloudFront distribution.

Which solution will meet these requirements?

- A.Create a new origin access control (OAC) in CloudFront. Configure the CloudFront distribution's origin to use the new OAC. Update the S3 bucket policy to allow CloudFront OAC with read and write access to access Amazon S3 as the origin.
- B.Update the S3 bucket settings. Enable the block all public access setting in Amazon S3. Configure the CloudFront distribution's with Amazon S3 as the origin. Update the S3 bucket policy to allow CloudFront write access.
- C.Update the S3 bucket's static website settings. Enable static website hosting and specifying index and error documents. Update the CloudFront origin to use the S3 bucket's website endpoint.
- D.Update the CloudFront distribution's origin to send a custom header. Update the S3 bucket policy with a condition by using the aws:RequestTag/tag-key key. Configure the tag-key as the custom header name, and the value being matched is the header's value.

**Answer: A**

**Explanation:**

Create a new origin access control (OAC) in CloudFront. Configure the CloudFront distribution's origin to use the new OAC. Update the S3 bucket policy to allow CloudFront OAC with read and write access to access Amazon S3 as the origin.

**CertyIQ**

**Question: 320**

A developer built an application that calls an external API to obtain data, processes the data, and saves the result to Amazon S3. The developer built a container image with all of the necessary dependencies to run the application as a container.

The application runs locally and requires minimal CPU and RAM resources. The developer has created an Amazon ECS cluster. The developer needs to run the application hourly in Amazon Elastic Container Service (Amazon ECS).

Which solution will meet these requirements with the LEAST amount of infrastructure management overhead?

- A.Add a capacity provider to manage instances.
- B.Add an Amazon EC2 instance that runs the application.
- C.Define a task definition with an AWS Fargate launch type.
- D.Create an Amazon ECS cluster and add the managed node groups feature to run the application.

**Answer: C**

**Explanation:**

Define a task definition with an AWS Fargate launch type.

**CertyIQ****Question: 321**

A company runs its website on AWS. The company posts daily polls on its website and publishes the poll results next day. The website stores user responses in an Amazon DynamoDB table. After the poll results are published, the company does not need to keep the user responses.

A developer needs to implement a solution that will automatically remove old user responses from the DynamoDB table. The developer adds a new expiration\_date attribute to the DynamoDB table. The developer plans to use the expiration\_date attribute for the automation.

Which solution will meet these requirements with the LEAST development effort?

- A.Create an AWS Lambda function to delete old user responses based on the expiration\_date attribute. Create an Amazon EventBridge schedule to run the Lambda function daily.
- B.Create an AWS Fargate task in Amazon Elastic Container Service (Amazon ECS) to delete old user responses based on the expiration\_date attribute. Create an Amazon EventBridge schedule to run the Fargate task daily.
- C.Create an AWS Glue job to delete old user responses based on the expiration\_date attribute. Create an AWS Glue trigger schedule to run the job daily.
- D.Enable TTL on the DynamoDB table and specify the expiration\_date attribute. Expire old user responses by using DynamoDB TTL.

**Answer: A****Explanation:**

Create an AWS Lambda function to delete old user responses based on the expiration\_date attribute. Create an Amazon EventBridge schedule to run the Lambda function daily.

**CertyIQ****Question: 322**

A developer is creating a simple proof-of-concept demo by using AWS CloudFormation and AWS Lambda functions. The demo will use a CloudFormation template to deploy an existing Lambda function. The Lambda function uses deployment packages and dependencies stored in Amazon S3. The developer defined an AWS::Lambda::Function resource in a CloudFormation template. The developer needs to add the S3 bucket to the CloudFormation template.

What should the developer do to meet these requirements with the LEAST development effort?

- A.Add the function code in the CloudFormation template inline as the code property.
- B.Add the function code in the CloudFormation template as the ZipFile property.
- C.Find the S3 key for the Lambda function. Add the S3 key as the ZipFile property in the CloudFormation template.
- D.Add the relevant key and bucket to the S3Bucket and S3Key properties in the CloudFormation template.

**Answer: D****Explanation:**

Add the relevant key and bucket to the S3Bucket and S3Key properties in the CloudFormation template..

**Question: 323**

CertyIQ

A developer is building a microservices-based application by using Python on AWS and several AWS services. The developer must use AWS X-Ray. The developer views the service map by using the console to view the service dependencies. During testing, the developer notices that some services are missing from the service map.

What can the developer do to ensure that all services appear in the X-Ray service map?

- A.Modify the X-Ray Python agent configuration in each service to increase the sampling rate.
- B.Instrument the application by using the X-Ray SDK for Python. Install the X-Ray SDK for all the services that the application uses.
- C.Enable X-Ray data aggregation in Amazon CloudWatch Logs for all the services that the application uses.
- D.Increase the X-Ray service map timeout value in the X-Ray console.

**Answer: B****Explanation:**

Instrument the application by using the X-Ray SDK for Python. Install the X-Ray SDK for all the services that the application uses.

**Question: 324**

CertyIQ

A developer is building a containerized application on AWS. The application communicates with a third-party service by using API keys. The developer needs a secure way to store the API keys and pass the API keys to the containerized application.

Which solutions will meet these requirements? (Choose two.)

- A.Store the API keys as a SecureString parameter in AWS Systems Manager Parameter Store. Grant the application access to retrieve the value from Parameter Store.
- B.Store the API keys in AWS CloudFormation templates by using base64 encoding. Pass the API keys to the application through container definition environment variables.
- C.Add a new AWS CloudFormation parameter to the CloudFormation template. Pass the API keys to the application by using the container definition environment variables.
- D.Embed the API keys in the application. Build the container image on-premises. Upload the container image to Amazon Elastic Container Registry (Amazon ECR).
- E.Store the API keys as a SecretString parameter in AWS Secrets Manager. Grant the application access to retrieve the value from Secrets Manager.

**Answer: AE****Explanation:**

A.Store the API keys as a SecureString parameter in AWS Systems Manager Parameter Store. Grant the application access to retrieve the value from Parameter Store.

E.Store the API keys as a SecretString parameter in AWS Secrets Manager. Grant the application access to retrieve the value from Secrets Manager.

**Question: 325**

CertyIQ

A company runs an application on AWS. The application stores data in an Amazon DynamoDB table. Some queries

are taking a long time to run. These slow queries involve an attribute that is not the table's partition key or sort key.

The amount of data that the application stores in the DynamoDB table is expected to increase significantly. A developer must increase the performance of the queries.

Which solution will meet these requirements?

- A.Increase the page size for each request by setting the Limit parameter to be higher than the default value. Configure the application to retry any request that exceeds the provisioned throughput.
- B.Create a global secondary index (GSI). Set query attribute to be the partition key of the index.
- C.Perform a parallel scan operation by issuing individual scan requests. In the parameters, specify the segment for the scan requests and the total number of segments for the parallel scan.
- D.Turn on read capacity auto scaling for the DynamoDB table. Increase the maximum read capacity units (RCUs).

**Answer: B**

**Explanation:**

Create a global secondary index (GSI). Set query attribute to be the partition key of the index.

### Question: 326

CertyIQ

A company runs a payment application on Amazon EC2 instances behind an Application Load Balance. The EC2 instances run in an Auto Scaling group across multiple Availability Zones. The application needs to retrieve application secrets during the application startup and export the secrets as environment variables. These secrets must be encrypted at rest and need to be rotated every month.

Which solution will meet these requirements with the LEAST development effort?

- A.Save the secrets in a text file and store the text file in Amazon S3. Provision a customer managed key. Use the key for secret encryption in Amazon S3. Read the contents of the text file and read the export as environment variables. Configure S3 Object Lambda to rotate the text file every month.
- B.Save the secrets as strings in AWS Systems Manager Parameter Store and use the default AWS Key Management Service (AWS KMS) key. Configure an Amazon EC2 user data script to retrieve the secrets during the startup and export as environment variables. Configure an AWS Lambda function to rotate the secrets in Parameter Store every month.
- C.Save the secrets as base64 encoded environment variables in the application properties. Retrieve the secrets during the application startup. Reference the secrets in the application code. Write a script to rotate the secrets saved as environment variables.
- D.Store the secrets in AWS Secrets Manager. Provision a new customer master key. Use the key to encrypt the secrets. Enable automatic rotation. Configure an Amazon EC2 user data script to programmatically retrieve the secrets during the startup and export as environment variables.

**Answer: D**

**Explanation:**

Store the secrets in AWS Secrets Manager. Provision a new customer master key. Use the key to encrypt the secrets. Enable automatic rotation. Configure an Amazon EC2 user data script to programmatically retrieve the secrets during the startup and export as environment variables.

### Question: 327

CertyIQ

A company is using Amazon API Gateway to invoke a new AWS Lambda function. The company has Lambda

function versions in its PROD and DEV environments. In each environment, there is a Lambda function alias pointing to the corresponding Lambda function version. API Gateway has one stage that is configured to point at the PROD alias.

The company wants to configure API Gateway to enable the PROD and DEV Lambda function versions to be simultaneously and distinctly available.

Which solution will meet these requirements?

- A. Enable a Lambda authorizer for the Lambda function alias in API Gateway. Republish PROD and create a new stage for DEV. Create API Gateway stage variables for the PROD and DEV stages. Point each stage variable to the PROD Lambda authorizer to the DEV Lambda authorizer.
- B. Set up a gateway response in API Gateway for the Lambda function alias. Republish PROD and create a new stage for DEV. Create gateway responses in API Gateway for PROD and DEV Lambda aliases.
- C. Use an environment variable for the Lambda function alias in API Gateway. Republish PROD and create a new stage for development. Create API gateway environment variables for PROD and DEV stages. Point each stage variable to the PROD Lambda function alias to the DEV Lambda function alias.
- D. Use an API Gateway stage variable to configure the Lambda function alias. Republish PROD and create a new stage for development. Create API Gateway stage variables for PROD and DEV stages. Point each stage variable to the PROD Lambda function alias and to the DEV Lambda function alias.

**Answer: D**

**Explanation:**

Use an API Gateway stage variable to configure the Lambda function alias. Republish PROD and create a new stage for development. Create API Gateway stage variables for PROD and DEV stages. Point each stage variable to the PROD Lambda function alias and to the DEV Lambda function alias.

**Question: 328**

**CertyIQ**

A developer is working on an ecommerce platform that communicates with several third-party payment processing APIs. The third-party payment services do not provide a test environment.

The developer needs to validate the ecommerce platform's integration with the third-party payment processing APIs. The developer must test the API integration code without invoking the third-party payment processing APIs.

Which solution will meet these requirements?

- A. Set up an Amazon API Gateway REST API with a gateway response configured for status code 200. Add response templates that contain sample responses captured from the real third-party API.
- B. Set up an AWS AppSync GraphQL API with a data source configured for each third-party API. Specify an integration type of Mock. Configure integration responses by using sample responses captured from the real third-party API.
- C. Create an AWS Lambda function for each third-party API. Embed responses captured from the real third-party API. Configure Amazon Route 53 Resolver with an inbound endpoint for each Lambda function's Amazon Resource Name (ARN).
- D. Set up an Amazon API Gateway REST API for each third-party API. Specify an integration request type of Mock. Configure integration responses by using sample responses captured from the real third-party API.

**Answer: D**

**Explanation:**

Set up an Amazon API Gateway REST API for each third-party API. Specify an integration request type of Mock. Configure integration responses by using sample responses captured from the real third-party API.

**Question: 329**

CertyIQ

A developer is storing many objects in a single Amazon S3 bucket. The developer needs to optimize the S3 bucket for high request rates.

How should the developer store the objects to meet this requirement?

- A.Store the objects by using S3 Intelligent-Tiering.
- B.Store the objects at the root of the S3 bucket.
- C.Store the objects by using object key names distributed across multiple prefixes.
- D.Store each object with an object tag named "prefix" that contains a unique value.

**Answer: C****Explanation:**

Store the objects by using object key names distributed across multiple prefixes.

**Question: 330**

CertyIQ

A company deploys a new application to AWS. The company is streaming application logs to Amazon CloudWatch Logs. The company's development team must receive notification by email when the word "ERROR" appears in any log lines. A developer sets up an Amazon Simple Notification Service (Amazon SNS) topic and subscribes the development team to the topic.

What should the developer do next to meet the requirements?

- A.Select the appropriate log group. Create a CloudWatch metric filter with "ERROR" as the search term. Create an alarm on this metric that notifies the SNS topic when the metric is 1 or higher.
- B.In CloudWatch Logs Insights, select the appropriate log group. Create a metric query to search for the term "ERROR" in the logs. Create an alarm on this metric that notifies the SNS topic when the metric is 1 or higher.
- C.Select the appropriate log group. Create an SNS subscription filter with "ERROR" as the filter pattern. Select the SNS topic as the destination.
- D.Create a CloudWatch alarm that includes "ERROR" as a filter pattern, a log group dimension that defines the appropriate log group, and a destination that notifies the SNS topic.

**Answer: A****Explanation:**

Select the appropriate log group. Create a CloudWatch metric filter with "ERROR" as the search term. Create an alarm on this metric that notifies the SNS topic when the metric is 1 or higher.

**Question: 331**

CertyIQ

A company uses Amazon Simple Queue Service (Amazon SQS) to decouple its microservices architecture. Some messages in an SQS queue contain sensitive information. A developer must implement a solution that encrypts all the data at rest.

Which solution will meet this requirement?

- A.Enable server-side encryption for the SQS queue by using an SQS managed encryption key (SSE-SQS).
- B.Use the aws:SecureTransport condition in the queue policy to ensure that only HTTPS (TLS) is used for all

requests to the SQS queue.

C.Use AWS Certificate Manager (ACM) to generate an SSL/TLS certificate. Reference the certificate when messages are sent to the queue.

D.Set a message attribute in the SQS SendMessage request for messages that are sent to the queue. Set the Name to ENCRYPT. Set the Value to TRUE.

**Answer: A**

**Explanation:**

Reference:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-server-side-encryption.html>

**CertyIQ**

**Question: 332**

A company recently deployed a new serverless user portal. Users have reported that part of the portal is slow. The initial analysis found a single Amazon API Gateway endpoint that is responsible for the performance issues. The endpoint integrates with an AWS Lambda function. However, the Lambda function interacts with other APIs and AWS services.

How can a developer find the source of the increased response time by using operational best practices?

A.Update the Lambda function by adding logging statements with high-precision timestamps before and after each external request. Deploy the updated Lambda function. After accumulating enough usage data, examine the Amazon CloudWatch logs for the Lambda function to determine the likely sources for the increased response time.

B.Instrument the Lambda function with the AWS X-Ray SDK. Add HTTP and HTTPS interceptors and SDK client handlers. Deploy the updated Lambda function. Turn on X-Ray tracing. After accumulating enough usage data, use the X-Ray service map to examine the average response times to determine the likely sources.

C.Review the Lambda function's Amazon CloudWatch metrics by using the metrics explorer. Apply anomaly detection to the Duration metric and the Throttles metric. Review the anomalies to determine the likely sources.

D.Use Amazon CloudWatch Synthetics to create a new canary. Turn on AWS X-Ray tracing on the canary. Configure the canary to scan the user portal. After accumulating enough usage data, use the CloudWatch Synthetics canary dashboard to view the metrics from the canary.

**Answer: D**

**Explanation:**

Reference:

[https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch\\_Synthetics\\_Canaries.html](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Synthetics_Canaries.html)

**CertyIQ**

**Question: 333**

A developer is building an event-driven application by using AWS Lambda and Amazon EventBridge. The Lambda function needs to push events to an EventBridge event bus. The developer uses an SDK to run the PutEvents EventBridge action and specifies no credentials in the code. After deploying the Lambda function, the developer notices that the function is failing and there are AccessDeniedException errors in the logs.

How should the developer resolve this issue?

A.Configure a VPC peering connection between the Lambda function and EventBridge.

- B.Modify their AWS credentials to include permissions for the PutEvents EventBridge action.
- C.Modify the Lambda function execution role to include permissions for the PutEvents EventBridge action.
- D.Add a resource-based policy to the Lambda function to include permissions for the PutEvents EventBridge action.

**Answer: D**

**Explanation:**

Reference:

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-event-bus-perms.html>

**CertyIQ**

**Question: 334**

A company's application has an AWS Lambda function that processes messages from IoT devices. The company wants to monitor the Lambda function to ensure that the Lambda function is meeting its required service level agreement (SLA).

A developer must implement a solution to determine the application's throughput in near real time. The throughput must be based on the number of messages that the Lambda function receives and processes in a given time period. The Lambda function performs initialization and post-processing steps that must not factor into the throughput measurement.

What should the developer do to meet these requirements?

- A.Use the Lambda function's ConcurrentExecutions metric in Amazon CloudWatch to measure the throughput.
- B.Modify the application to log the calculated throughput to Amazon CloudWatch Logs. Use Amazon EventBridge to invoke a separate Lambda function to process the logs on a schedule.
- C.Modify the application to publish custom Amazon CloudWatch metrics when the Lambda function receives and processes each message. Use the metrics to calculate the throughput.
- D.Use the Lambda function's Invocations metric and Duration metric to calculate the throughput in Amazon CloudWatch.

**Answer: A**

**Explanation:**

Reference:

<https://aws.amazon.com/blogs/compute/understanding-aws-lambda-scaling-and-throughput/>

**CertyIQ**

**Question: 335**

A developer is using an AWS CodePipeline pipeline to provide continuous integration and continuous delivery (CI/CD) support for a Java application. The developer needs to update the pipeline to support the introduction of a new application dependency .jar file. The pipeline must start a build when a new version of the .jar file becomes available.

Which solution will meet these requirements?

- A.Create an Amazon S3 bucket to store the dependency .jar file. Publish the dependency .jar file to the S3 bucket. Use an Amazon Simple Notification Service (Amazon SNS) notification to start a CodePipeline pipeline build.
- B.Create an Amazon Elastic Container Registry (Amazon ECR) private repository. Publish the dependency .jar

file to the repository. Use an ECR source action to start a CodePipeline pipeline build.

C.Create an Amazon Elastic Container Registry (Amazon ECR) private repository. Publish the dependency .jar file to the repository. Use an Amazon Simple Notification Service (Amazon SNS) notification to start a CodePipeline pipeline build.

D.Create an AWS CodeArtifact repository. Publish the dependency .jar file to the repository. Use an Amazon EventBridge rule to start a CodePipeline pipeline build.

**Answer: D**

**Explanation:**

Create an AWS CodeArtifact repository. Publish the dependency .jar file to the repository. Use an Amazon EventBridge rule to start a CodePipeline pipeline build.

**Question: 336**

**CertyIQ**

A company with multiple branch locations has an analytics and reporting application. Each branch office pushes a sales report to a shared Amazon S3 bucket at a predefined time each day. The company has developed an AWS Lambda function that analyzes the reports from all branch offices in a single pass. The Lambda function stores the results in a database.

The company needs to start the analysis once each day at a specific time.

Which solution will meet these requirements MOST cost-effectively?

A.Configure an S3 event notification to invoke the Lambda function when a branch office uploads a sales report.

B.Create an AWS Step Functions state machine that invokes the Lambda function once each day at the predefined time.

C.Configure the Lambda function to run continuously and to begin analysis only at the predefined time each day.

D.Create an Amazon EventBridge scheduled rule that invokes the Lambda function once each day at the predefined time.

**Answer: A**

**Explanation:**

Configure an S3 event notification to invoke the Lambda function when a branch office uploads a sales report.

**Question: 337**

**CertyIQ**

A developer has an application that asynchronously invokes an AWS Lambda function. The developer wants to store messages that resulted in failed invocations of the Lambda function so that the application can retry the call later.

What should the developer do to accomplish this goal with the LEAST operational overhead?

A.Set up Amazon CloudWatch Logs log groups to filter and store the messages in an Amazon S3 bucket. Import the messages in Lambda. Run the Lambda function again.

B.Configure Amazon EventBridge to send the messages to Amazon Simple Notification Service (Amazon SNS) to initiate the Lambda function again.

C.Implement a dead-letter queue for discarded messages. Set the dead-letter queue as an event source for the Lambda function.

D.Send Amazon EventBridge events to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the

Lambda function to pull messages from the SQS queue. Run the Lambda function again.

**Answer: C**

**Explanation:**

Implement a dead-letter queue for discarded messages. Set the dead-letter queue as an event source for the Lambda function.

**Question: 338**

CertyIQ

A company is using AWS CloudFormation templates to deploy AWS resources. The company needs to update one of its AWS CloudFormation stacks.

What can the company do to find out how the changes will impact the resources that are running?

- A.Investigate the change sets.
- B.Investigate the stack policies.
- C.Investigate the Metadata section.
- D.Investigate the Resources section.

**Answer: A**

**Explanation:**

Correct answer is A:Investigate the change sets.

**Question: 339**

CertyIQ

A company stores all personally identifiable information (PII) in an Amazon DynamoDB table named PII in Account A. Developers are working on an application that is running on Amazon EC2 instances in Account B. The application in Account B requires access to the PII table.

An administrator in Account A creates an IAM role named AccessPII that has permission to access the PII table. The administrator also creates a trust policy that specifies Account B as a principal that can assume the role.

Which combination of steps should the developers take in Account B to allow their application to access the PII table? (Choose two.)

- A.Allow the EC2 IAM role the permission to assume the AccessPII role.
- B.Allow the EC2 IAM role the permission to access the PII table.
- C.Include the AWS API in the application code logic to obtain temporary credentials from the EC2 IAM role to access the PII table.
- D.Include the AssumeRole API operation in the application code logic to obtain temporary credentials to access the PII table.
- E.Include the GetSessionToken API operation in the application code logic to obtain temporary credentials to access the PII table.

**Answer: BD**

**Explanation:**

- B.Allow the EC2 IAM role the permission to access the PII table.

D.Include the AssumeRole API operation in the application code logic to obtain temporary credentials to access the PII table.

### Question: 340

CertyIQ

A gaming website gives users the ability to trade game items with each other on the platform. The platform requires both users' records to be updated and persisted in one transaction. If any update fails, the transaction must roll back.

Which AWS solutions can provide the transactional capability that is required for this feature? (Choose two.)

- A.Amazon DynamoDB with operations made with the ConsistentRead parameter set to true
- B.Amazon ElastiCache for Memcached with operations made within a transaction block
- C.Amazon DynamoDB with reads and writes made by using Transact\* operations
- D.Amazon Aurora MySQL with operations made within a transaction block
- E.Amazon Athena with operations made within a transaction block

**Answer: CD**

**Explanation:**

- C.Amazon DynamoDB with reads and writes made by using Transact\* operations.
- D.Amazon Aurora MySQL with operations made within a transaction block.

### Question: 341

CertyIQ

A developer is deploying an application in the AWS Cloud by using AWS CloudFormation. The application will connect to an existing Amazon RDS database. The hostname of the RDS database is stored in AWS Systems Manager Parameter Store as a plaintext value. The developer needs to incorporate the database hostname into the CloudFormation template to initialize the application when the stack is created.

How should the developer reference the parameter that contains the database hostname?

- A.Use the ssm dynamic reference.
- B.Use the Ref intrinsic function.
- C.Use the Fn::ImportValue intrinsic function.
- D.Use the ssm-secure dynamic reference.

**Answer: A**

**Explanation:**

Use the ssm dynamic reference.

### Question: 342

CertyIQ

A company uses an AWS Lambda function to call a third-party service. The third-party service has a limit of requests each minute. If the number of requests exceeds the limit, the third-party service returns rate-limiting errors.

A developer needs to configure the Lambda function to avoid receiving rate limiting errors from the third-party

service.

Which solution will meet these requirements?

- A.Set the reserved concurrency on the Lambda function to match the number of concurrent requests that the third-party service allows.
- B.Decrease the memory that is allocated to the Lambda function.
- C.Set the provisioned concurrency on the Lambda function to match the number of concurrent requests that the third-party service allows.
- D.Increase the timeout value that is specified on the Lambda function.

**Answer: A**

**Explanation:**

Set the reserved concurrency on the Lambda function to match the number of concurrent requests that the third-party service allows.

**Question: 343**

**CertyIQ**

A developer is building a new containerized application by using AWS Copilot. The developer uses the AWS Copilot command line interface (CLI) to deploy the application during development. The developer committed the application code to a new AWS CodeCommit repository. The developer must create an automated deployment process before releasing the new application to production.

What should the developer do to meet these requirements in the MOST operationally efficient way?

- A.Create a buildspec file that invokes the AWS Copilot CLI commands to build and deploy the application. Use the AWS Copilot CLI to create an AWS CodePipeline that uses the CodeCommit repository in the source stage and AWS CodeBuild in the build stage.
- B.Use the AWS Serverless Application Model (AWS SAM) CLI to bootstrap and initialize an AWS CodePipeline configuration. Use the CodeCommit repository as the source. Invoke the AWS Copilot CLI to build and deploy the application.
- C.Use the AWS Copilot CLI to define the AWS Copilot pipeline and to deploy the AWS CodePipeline. Select CodeCommit as the source for the AWS CodePipeline.
- D.Define an AWS CloudFormation template for an AWS CodePipeline with CodeCommit as the source. Configure the template as an AWS Copilot CLI add-on. Use the AWS Copilot CLI to deploy the application.

**Answer: C**

**Explanation:**

Use the AWS Copilot CLI to define the AWS Copilot pipeline and to deploy the AWS CodePipeline. Select CodeCommit as the source for the AWS CodePipeline.

**Question: 344**

**CertyIQ**

A developer is creating a new application for a pet store. The application will manage customer rewards points. The developer will use Amazon DynamoDB to store the data for the application. The developer needs to optimize query performance and limit partition overload before actual performance analysis.

Which option should the developer use for a partition key to meet these requirements?

- A.A randomly generated universally unique identifier (UUID)
- B.The customer's full name

C.The date when the customer signed up for the rewards program

D.The name of the customer's pet

**Answer: A**

**Explanation:**

A randomly generated universally unique identifier (UUID).

**CertyIQ**

A developer uses AWS IAM Identity Center (AWS Single Sign-On) to interact with the AWS CLI and AWS SDKs on a local workstation. API calls to AWS services were working when the SSO access was first configured. However, the developer is now receiving Access Denied errors. The developer has not changed any configuration files or scripts that were previously working on the workstation.

What is the MOST likely cause of the developer's access issue?

A.The access permissions to the developer's AWS CLI binary file have changed.

B.The permission set that is assumed by IAM Identity Center does not have the necessary permissions to complete the API call.

C.The credentials from the IAM Identity Center federated role have expired.

D.The developer is attempting to make API calls to the incorrect AWS account.

**Answer: C**

**Explanation:**

The credentials from the IAM Identity Center federated role have expired.

**CertyIQ**

A company is building a serverless application. The application uses an API key to authenticate with a third-party application. The company wants to store the external API key as a part of an AWS Lambda configuration. The company needs to have full control over the AWS Key Management Service (AWS KMS) keys that will encrypt the API key and should be visible only to authorized entities.

Which solution will meet these requirements?

A.Store the API key in AWS Systems Manager Parameter Store as a string parameter. Use the default AWS KMS key that AWS provides to encrypt the API key.

B.Store the API key in AWS Lambda environment variables. Create an AWS KMS customer managed key to encrypt the API key.

C.Store the API key in the code repository. Use an AWS managed key to encrypt the code repository.

D.Store the API key as an Amazon DynamoDB table record. Use an AWS managed key to encrypt the API key.

**Answer: B**

**Explanation:**

Store the API key in AWS Lambda environment variables. Create an AWS KMS customer managed key to encrypt the API key.

**Question: 347****CertyIQ**

A developer is writing an application to analyze the traffic to a fleet of Amazon EC2 instances. The EC2 instances run behind a public Application Load Balancer (ALB). An HTTP server runs on each of the EC2 instances, logging all requests to a log file.

The developer wants to capture the client public IP addresses. The developer analyzes the log files and notices only the IP address of the ALB.

What must the developer do to capture the client public IP addresses in the log file?

- A.Add a Host header to the HTTP server log configuration file.
- B.Install the Amazon CloudWatch Logs agent on each EC2 instance. Configure the agent to write to the log file.
- C.Install the AWS X-Ray daemon on each EC2 instance. Configure the daemon to write to the log file.
- D.Add an X-Forwarded-For header to the HTTP server log configuration file.

**Answer: D****Explanation:**

D. Add an X-Forwarded-For header to the HTTP server log configuration file. The 'X-Forwarded-For' header is used to capture the original client IP address when requests are routed through a load balancer like the ALB.

**Question: 348****CertyIQ**

A company is developing a serverless application by using AWS Lambda functions. One of the Lambda functions needs to access an Amazon RDS DB instance. The DB instance is in a private subnet inside a VPC.

The company creates a role that includes the necessary permissions to access the DB instance. The company then assigns the role to the Lambda function. A developer must take additional action to give the Lambda function access to the DB instance.

What should the developer do to meet these requirements?

- A.Assign a public IP address to the DB instance. Modify the security group of the DB instance to allow inbound traffic from the IP address of the Lambda function.
- B.Set up an AWS Direct Connect connection between the Lambda function and the DB instance.
- C.Configure an Amazon CloudFront distribution to create a secure connection between the Lambda function and the DB instance.
- D.Configure the Lambda function to connect to the private subnets in the VPC. Add security group rules to allow traffic to the DB instance from the Lambda function.

**Answer: D****Explanation:**

Configure the Lambda function to connect to the private subnets in the VPC. Add security group rules to allow traffic to the DB instance from the Lambda function.

**Question: 349****CertyIQ**

A developer needs temporary access to resources in a second account.

What is the MOST secure way to achieve this?

- A.Use the Amazon Cognito user pools to get short-lived credentials for the second account.
- B.Create a dedicated IAM access key for the second account, and send it by mail.
- C.Create a cross-account access role, and use sts:AssumeRole API to get short-lived credentials.
- D.Establish trust, and add an SSH key for the second account to the IAM user.

**Answer: C**

**Explanation:**

Create a cross-account access role, and use sts:AssumeRole API to get short-lived credentials.

### Question: 350

**CertyIQ**

A company wants to migrate applications from its on-premises servers to AWS. As a first step, the company is modifying and migrating a non-critical application to a single Amazon EC2 instance. The application will store information in an Amazon S3 bucket. The company needs to follow security best practices when deploying the application on AWS.

Which approach should the company take to allow the application to interact with Amazon S3?

- A.Create an IAM role that has administrative access to AWS. Attach the role to the EC2 instance.
- B.Create an IAM user. Attach the AdministratorAccess policy. Copy the generated access key and secret key. Within the application code, use the access key and secret key along with the AWS SDK to communicate with Amazon S3.
- C.Create an IAM role that has the necessary access to Amazon S3. Attach the role to the EC2 instance.
- D.Create an IAM user. Attach a policy that provides the necessary access to Amazon S3. Copy the generated access key and secret key. Within the application code, use the access key and secret key along with the AWS SDK to communicate with Amazon S3.

**Answer: C**

**Explanation:**

Create an IAM role that has the necessary access to Amazon S3. Attach the role to the EC2 instance.

### Question: 351

**CertyIQ**

A company has an internal website that contains sensitive data. The company wants to make the website public. The company must ensure that only employees who authenticate through the company's OpenID Connect (OIDC) identity provider (IdP) can access the website. A developer needs to implement authentication without editing the website.

Which combination of steps will meet these requirements? (Choose two.)

- A.Create a public Network Load Balancer.
- B.Create a public Application Load Balancer.
- C.Configure a listener for the load balancer that listens on HTTPS port 443. Add a default authenticate action providing the OIDC IdP configuration.
- D.Configure a listener for the load balancer that listens on HTTP port 80. Add a default authenticate action providing the OIDC IdP configuration.
- E.Configure a listener for the load balancer that listens on HTTPS port 443. Add a default AWS Lambda action providing an Amazon Resource Name (ARN) to a Lambda authentication function.

**Answer: BC**

**Explanation:**

- B.Create a public Application Load Balancer.
- C.Configure a listener for the load balancer that listens on HTTPS port 443. Add a default authenticate action providing the OIDC IdP configuration.

**CertyIQ**

**Question: 352**

A developer is working on a web application that requires selective activation of specific features. The developer wants to keep the features hidden from end users until the features are ready for public access.

Which solution will meet these requirements?

- A.Create a feature flag configuration profile in AWS AppSync. Store the feature flag values in the configuration profile. Activate and deactivate feature flags as needed.
- B.Store prerelease data in an Amazon DynamoDB table. Enable Amazon DynamoDB Streams in the table. Toggle between hidden and visible states by using DynamoDB Streams.
- C.Create a feature flag configuration profile in AWS AppConfig. Store the feature flag values in the configuration profile. Activate and deactivate feature flags as needed.
- D.Store prerelease data in AWS Amplify DataStore. Toggle between hidden and visible states by using Amplify DataStore cloud synchronization.

**Answer: C**

**Explanation:**

Create a feature flag configuration profile in AWS AppConfig. Store the feature flag values in the configuration profile. Activate and deactivate feature flags as needed.

**CertyIQ**

**Question: 353**

A developer at a company writes an AWS CloudFormation template. The template refers to subnets that were created by a separate AWS CloudFormation template that the company's network team wrote. When the developer attempts to launch the stack for the first time, the launch fails.

Which template coding mistakes could have caused this failure? (Choose two.)

- A.The developer's template does not use the Ref intrinsic function to refer to the subnets.
- B.The developer's template does not use the ImportValue intrinsic function to refer to the subnets.
- C.The Mappings section of the developer's template does not refer to the subnets.
- D.The network team's template does not export the subnets in the Outputs section.
- E.The network team's template does not export the subnets in the Mappings section.

**Answer: BD**

**Explanation:**

- B.The developer's template does not use the ImportValue intrinsic function to refer to the subnets.
- D.The network team's template does not export the subnets in the Outputs section.

**Question: 354****CertyIQ**

A developer is running an application on an Amazon EC2 instance. When the application tries to read an Amazon S3 bucket, the application fails. The developer notices that the associated IAM role is missing the S3 read permission. The developer needs to give the application the ability to read the S3 bucket.

Which solution will meet this requirement with the LEAST application disruption?

- A.Add the permission to the role. Terminate the existing EC2 instance. Launch a new EC2 instance.
- B.Add the permission to the role so that the change will take effect automatically.
- C.Add the permission to the role. Hibernate and restart the existing EC2 instance.
- D.Add the permission to the S3 bucket. Restart the EC2 instance.

**Answer: B****Explanation:**

Add the permission to the role so that the change will take effect automatically.

**Question: 355****CertyIQ**

A developer is writing a web application that is deployed on Amazon EC2 instances behind an internet-facing Application Load Balancer (ALB). The developer must add an Amazon CloudFront distribution in front of the ALB. The developer also must ensure that customer data from outside the VPC is encrypted in transit.

Which combination of CloudFront configuration settings should the developer use to meet these requirements? (Choose two.)

- A.Restrict viewer access by using signed URLs.
- B.Set the Origin Protocol Policy setting to Match Viewer.
- C.Enable field-level encryption.
- D.Enable automatic object compression.
- E.Set the Viewer Protocol Policy setting to Redirect HTTP to HTTPS.

**Answer: BE****Explanation:**

- B.Set the Origin Protocol Policy setting to Match Viewer.
- E.Set the Viewer Protocol Policy setting to Redirect HTTP to HTTPS.

**Question: 356****CertyIQ**

A developer is implementing an AWS Lambda function that will be invoked when an object is uploaded to Amazon S3. The developer wants to test the Lambda function in a local development machine before publishing the function to a production AWS account.

Which solution will meet these requirements with the LEAST operational overhead?

- A.Upload an object to Amazon S3 by using the aws s3api put-object CLI command. Wait for the local Lambda invocation from the S3 event.

B.Create a sample JSON text file for a put object S3 event. Invoke the Lambda function locally. Use the aws lambda invoke CLI command with the JSON file and Lambda function name as arguments.

C.Use the sam local start-lambda CLI command to start Lambda. Use the sam local generate-event s3 put CLI command to create the Lambda test JSON file. Use the sam local invoke CLI command with the JSON file as the argument to invoke the Lambda function.

D.Create a JSON string for the put object S3 event. In the AWS Management Console, use the JSON string to create a test event for the local Lambda function. Perform the test.

**Answer: C**

**Explanation:**

Use the sam local start-lambda CLI command to start Lambda. Use the sam local generate-event s3 put CLI command to create the Lambda test JSON file. Use the sam local invoke CLI command with the JSON file as the argument to invoke the Lambda function.

**Question: 357**

**CertyIQ**

A developer is publishing critical log data to a log group in Amazon CloudWatch Logs. The log group was created 2 months ago. The developer must encrypt the log data by using an AWS Key Management Service (AWS KMS) key so that future data can be encrypted to comply with the company's security policy.

Which solution will meet this requirement with the LEAST effort?

- A.Use the AWS Encryption SDK for encryption and decryption of the data before writing to the log group.
- B.Use the AWS KMS console to associate the KMS key with the log group.
- C.Use the AWS CLI aws logs create-log-group command, and specify the key Amazon Resource Name (ARN).
- D.Use the AWS CLI aws logs associate-kms-key command, and specify the key Amazon Resource Name (ARN).

**Answer: D**

**Explanation:**

Use the AWS CLI aws logs associate-kms-key command, and specify the key Amazon Resource Name (ARN).

# Thank you

Thank you for being so interested in the premium exam material.

I'm glad to hear that you found it informative and helpful.

If you have any feedback or thoughts on the bumps, I would love to hear them.  
Your insights can help me improve our writing and better understand our readers.

## Best of Luck

You have worked hard to get to this point, and you are well-prepared for the exam  
Keep your head up, stay positive, and go show that exam what you're made of!

[Feedback](#)

[More Papers](#)



Future is Secured  
100% Pass Guarantee



24/7 Customer Support  
Mail us - [certyiqofficial@gmail.com](mailto:certyiqofficial@gmail.com)



Free Updates  
Lifetime Free Updates!

Total: **357 Questions**

Link: <https://certyiq.com/papers?provider=amazon&exam=aws-certified-developer-associate>

dva-c02