**Simulacro examen AWS Netec**

email = [External] Fw: Exámenes de Preparación

Link: <https://www.net4skills-certificaciones.netecdigital.com/examenes-de-preparacion>  
Your username: [zarbio.ordonez@tcs.com](mailto:zarbio.ordonez@tcs.com)  
Your password: N3t3c

**Cada pregunta vale 2.5%**

A screenshot of a computer

Description automatically generated

* 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. (Correcta)**

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.

Explanation: The requirement of maximizing resiliency rules out One Zone. Standard recover is within 12 hours, which fits the requirement of within 24 hours.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/restoring-objects-retrieval-options.html>

Resiliency: recover quickly

**S3 Standard-IA**: for infrequently accessed data

**S3 Glacier Deep Archive with standard retrieval**: 24-hour access requirement

**S3 Glacier Deep Archive with bulk retrieval**: Can take up to 48 hours

* A company uses an AWS CloudFormation template to deploy and manage its AWS infrastructure. The CloudFormation template creates Amazon VPC security groups and Amazon EC2 security groups.

A manager finds out that some engineers modified the security groups of a few EC2 instances for testing purposes. A developer needs to determine what modifications occurred.

Which solution will meet this requirement?

A. Add a Conditions section statement in the source YAML file of the template. Run the CloudFormation stack.

**B. Perform a drift detection operation on the CloudFormation stack. (Correcta)**

C. Execute a change set for the CloudFormation stack.

D. Use Amazon Detective to detect the modifications.

Explanation:

**Drift Detection** identifies any changes (**drift**), such as modifications to security groups

* A developer needs to store files in an Amazon S3 bucket for a company's application. Each S3 object can have multiple versions. The objects must be permanently removed 1 year after object creation.

The developer creates an S3 bucket that has versioning enabled.

What should the developer do next to meet the data retention requirements?

**A. Create an S3 Lifecycle rule on the S3 bucket. Configure the rule to expire current versions of objects and permanently delete noncurrent versions 1 year after object creation. (Correcta)**

B. Create an event notification for all object creation events in the S3 bucket. Configure the event notification to invoke an AWS Lambda function. Program the Lambda function to check the object creation date and to delete the object if the object is older than 1 year.

C. Create an event notification for all object removal events in the S3 bucket. Configure the event

notification to invoke an AWS Lambda function. Program the Lambda function to check the object

creation date and to delete the object if the object is older than 1 year.

D. Create an S3 Lifecycle rule on the S3 bucket. Configure the rule to delete expired object delete

markers and permanently delete noncurrent versions 1 year after object creation.

* 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. (Correcta)**

C. Enable field-level encryption.

D. Enable automatic object compression.

**E. Set the Viewer Protocol Policy setting to Redirect HTTP to HTTPS. (Correcta)**

Explanation: <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-cloudfront-to-custom-origin.html>

CloudFront ↔ Viewer communication is secure (via **HTTPS** enforced by the Viewer Protocol Policy).

CloudFront ↔ ALB communication is secure (via the Origin Protocol Policy set to **Match Viewer**).

* 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:DeleleItem

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 (Correcta)**

Explanation: dynamodb:GetItem: This permission allows the Lambda function to retrieve an item

from DynamoDB. 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.

* 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. (Correcta)**

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. (Correcta)**

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.

Explanation:

Option A is correct because an Amazon EventBridge 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.

Capture S3 events (criteria .csv).

Option C is correct because the existing Lambda function can be updated with an EventBridge trigger. The trigger type should be set to EventBridge, and the Amazon EventBridge rule created in step A should be selected.

Add the EventBridge Rule as a Trigger for the Lambda Function

* 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. (Correcta)**

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.

Explanation:

**Authorization caching in API Gateway Lambda authorizers** is the most likely cause of outdated attribute values being used for access control.

**Cognito** does **not** have an authorization **caching** mechanism that directly impacts Lambda authorizers in API Gateway.

* 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. (Correcta)**

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.

* 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. (Correcta)**

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.

Explanation: You need to use environment variables.

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

* A developer needs to use a code template to create an automated deployment of an application onto Amazon EC2 instances. The template must be configured to repeat deployment, installation, and updates of resources for the application. The template must be able to create identical environments and roll back to previous versions.

Which solution will meet these requirements?

A. Use AWS Amplify for automatic deployment templates. Use a traffic-splitting deployment to copy

any deployments. Modify any resources created by Amplify, if necessary.

B. Use AWS CodeBuild for automatic deployment. Upload the required AppSpec file template. Save

the appspec.yml file in the root directory folder of the revision. Specify the deployment group that

includes the EC2 instances for the deployment.

**C. Use AWS CloudFormation to create an infrastructure template in JSON format to deploy the EC2 instances. Use CloudFormation helper scripts to install the necessary software and to start the application. Call the scripts directly from the template. (Correcta)**

D. Use AWS AppSync to deploy the application. Upload the template as a GraphQL schema.

Specify the EC2 instances for deployment of the application. Use resolvers as a version control mechanism and to make any updates to the deployments.

* 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. (Correcta)**

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. (Correcta)**

* A Developer has been asked to make changes to the source code of an AWS Lambda function. The function is managed using an AWS CloudFormation template. The template is configured to load the source code from an Amazon S3 bucket. The Developer manually created a .ZIP file deployment package containing the changes and put the file into the correct location on Amazon S3.

When the function is invoked, the code changes have not been applied.

What step is required to update the function with the changes?

A. Delete the .ZIP file on S3, and re-upload by using a different object key name.

**B. Update the CloudFormation stack with the correct values for the function code properties**

**S3Bucket, S3Key, or S3ObjectVersion. (Correcta)**

C. Ensure that the function source code is base64-encoded before uploading the deployment package to S3.

D. Modify the execution role of the Lambda function to allow S3 access permission to the deployment package .ZIP file.

Explanation: Changes to a deployment package in Amazon S3 are not detected automatically during stack updates. To update the function code, change the object key or version in the template.

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-propertieslambda-function-code.html>

The **CloudFormation stack** must be updated with the new object key (**S3Key**) or the S3 bucket (**S3Bucket**), or you may need to update the object version (**S3ObjectVersion**) if versioning is enabled on the S3 bucket.

**CloudFormation** will then **redeploy** the **Lambda** function with the new .ZIP file that was uploaded to S3.

* A developer is creating a new batch application that will run on an Amazon EC2 instance. The application requires read access to an Amazon S3 bucket. The developer needs to follow security best practices to grant S3 read access to the application.

Which solution meets these requirements?

**A. Add the permissions to an IAM policy. Attach the policy to a role. Attach the role to the EC2**

**instance profile. (Correcta)**

B. Add the permissions inline to an IAM group. Attach the group to the EC2 instance profile.

C. Add the permissions to an IAM policy. Attach the policy to a user. Attach the user to the EC2 instance profile.

D. Add the permissions to an IAM policy. Use IAM web identity federation to access the S3 bucket with the policy.

Explanation:

Permissions -> policy -> role -> EC2 instance profile

* A developer needs to freeze changes to an AWS CodeCommit repository before a production release. The developer will work on new features while a quality assurance (QA) team tests the release.

The QA testing and all bug fixes must take place in isolation from the **main branch**.

After the release, the developer must integrate all bug fixes into the main branch.

Which solution will meet these requirements?

**A. Create a release branch from the latest Git commit that will be in the release. Apply fixes to the**

**release branch. Continue developing new features, and merge the features into the main branch.**

**Merge the release branch into the main branch after the release. (Correcta)**

B. Create a Git tag on the latest Git commit that will be in the release. Continue developing new

features, and merge the features into the main branch. Apply fixes to the main branch. Update

the Git tag for the release to be on the latest commit on the main branch.

C. Create a release branch from the latest Git commit that will be in the release. Apply fixes to the

release branch. Continue developing new features, and merge the features into the main branch.

Rebase the main branch onto the release branch after the release.

D. Create a Git tag on the latest Git commit that will be in the release. Continue developing new features, and merge the features into the main branch. Apply the Git commits for fixes to the Git tag for the release.

Explanation: Create a release branch from the latest Git commit that will be in the release. Apply fixes to the release branch. Continue developing new features, and merge the features into the main branch. Merge the release branch into the main branch after the release.

* 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. (Correcta)**

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.

Explanation: <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.

In AWS Lambda:

1. Obtain the request identifier from the context.awsRequestId field (not from the event object).

2. Write logs to standard output by using console.log(), as AWS Lambda automatically collects and sends logs from standard output (stdout) to Amazon CloudWatch Logs.

* 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. (Correcta)**

Explanation:

In Amazon API Gateway, you can deploy different versions of your API by creating **stages**. Each stage represents a different **environment** (e.g., development, testing, production). By deploying multiple stages with unique endpoints, you can isolate different versions of the API.

Additionally, you can use stage variables to pass contextual information (such as versioning details) to the Lambda functions. This allows you to easily control which version of your Lambda function is executed based on the stage of the API being called.

* A company has a web application that is hosted on AWS. The application is behind an Amazon CloudFront distribution. A developer needs a dashboard to monitor error rates and anomalies of the CloudFront distribution as **frequently** as possible.

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

A. Stream the CloudFront distribution logs to an Amazon S3 bucket. Detect anomalies and error

rates by using Amazon Athena.

**B. Enable real-time logs on the CloudFront distribution. Create a data stream in Amazon Kinesis**

**Data Streams. (Correcta)**

**C. Set up Amazon Kinesis Data Streams to send the logs to Amazon OpenSearch Service by using**

**an AWS Lambda function. Make a dashboard in OpenSearch Dashboards. (Correcta)**

D. Stream the CloudFront distribution logs to Amazon Kinesis Data Firehose.

E. Set up Amazon Kinesis Data Firehose to send the logs to AWS CloudTrail. Create CloudTrail

metrics, alarms, and dashboards.

Explanation:

To monitor the error rates and anomalies in real-time for the CloudFront distribution, the best approach involves using real-time logs from CloudFront, streaming them to **Kinesis Data Streams**, and then using **Amazon OpenSearch Service** (formerly known as Elasticsearch Service) to create a dashboard for visualization.

* 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. (Correcta)**

**C. Configure a listener for the load balancer that listens on HTTPS port 443. Add a default**

**authenticate action providing the OIDC IdP configuration. (Correcta)**

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.

* A set of APIs are exposed to customers using the Amazon API Gateway. These APIs have caching enabled on the API Gateway. Customers have asked for an option to invalidate this cache for each of the APIs.

What action can be taken to allow API customers to invalidate the API Cache?

A. Ask customers to use AWS credentials to call the InvalidateCache API.

B. Ask customers to invoke an AWS API endpoint which invalidates the cache.

**C. Ask customers to pass an HTTP header called Cache-Control:max-age=0. (Correcta)**

D. Ask customers to add a query string parameter called "INVALIDATE\_CACHE" when making an API call.

Explanation: <https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-caching.html> Invalidate an API Gateway Cache Entry. A client of your API can invalidate an existing cache entry and reload it from the integration endpoint for individual requests. The client must send a request that contains the Cache-Control: max-age=0 header. The client receives the response directly from the integration endpoint instead of the cache, provided that the client is authorized to do so. This replaces the existing cache entry with the new response, which is fetched from the integration endpoint. To grant permission for a client, attach a policy of the following format to an IAM execution role for the user.

* A developer is using AWS CodeDeploy to deploy an application running on Amazon EC2. The developer wants to change the file permissions for a specific deployment file.

Which lifecycle event should a developer use to meet this requirement?

**A. AfterInstall. (Correcta)**

B. DownloadBundle.

C. BeforeInstall.

D. ValidateService.

Explanation: You can use the AfterInstall deployment lifecycle event for tasks such as configuring your application or changing file permissions. <https://aws.amazon.com/es/codedeploy/faqs/>

* 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. (Correcta)**

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.

Explanation:

The AWS Serverless Application Model (AWS SAM) simplifies the development and deployment of serverless applications.

sam sync:

Deploy incremental changes to the AWS environment.

Avoid a full application deployment for every change.

Accelerate the feedback loop for testing.

* A company uses an AWS Lambda function to transfer files from an Amazon S3 bucket to the company's SFTP server. The Lambda function connects to the SFTP server by using credentials such as username and password. The company uses Lambda environment variables to store these credentials.

A developer needs to implement encrypted username and password credentials.

Which solution will meet these requirements?

A. Remove the user credentials from the Lambda environment. Implement IAM database

authentication.

**B. Move the user credentials from Lambda environment variables to AWS Systems Manager**

**Parameter Store. (Correcta)**

C. Move the user credentials from Lambda environment variables to AWS Key Management Service

(AWS KMS).

D. Move the user credentials from the Lambda environment to an encrypted .txt file. Store the file in

an S3 bucket.

Explanation:

AWS KMS is a key management service, not a storage solution for credentials.

For managing credentials securely in AWS Lambda, you can use either:

1. AWS Systems Manager Parameter Store (Secure String): Ideal for small-scale needs.

2. AWS Secrets Manager: A more advanced solution for rotating, retrieving, and managing secrets.

* A company has an ecommerce web application that uses an on-premises MySQL database as a data store. The company migrates the on-premises MySQL database to Amazon RDS for MySQL.

A developer needs to configure the application's access to the RDS for MySQL database. The developer's solution must **not use long term credentials**.

Which solution will meet these requirements?

A. Enable IAM database authentication on the RDS for MySQL DB instance. Create an IAM role that

has the minimum required permissions. Assign the role to the application.

**B. Store the MySQL credentials as secrets in AWS Secrets Manager. Create an IAM role that has**

**the minimum required permissions to retrieve the secrets. Assign the role to the application. (Correcta)**

C. Configure the MySQL credentials as environment variables that are available at runtime for the

application.

D. Store the MySQL credentials as SecureString parameters in AWS Systems Manager Parameter Store. Create an IAM role that has the minimum required permissions to retrieve the parameters. Assign the role to the application.

Explanation:

Option A: IAM database authentication eliminates the need for long-term credentials.

Option B: AWS Secrets Manager securely manages credentials, it still involves storing long-term credentials (MySQL username and password) in encrypted form.

* 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. (Correcta)**

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.

* 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. (Correcta)**

B. Decrease the timeout of the Lambda function.

**C. Increase the memory that is allocated to the Lambda function. (Correcta)**

D. Decrease the number of shards of the Kinesis data stream.

E. Increase the timeout of the Lambda function.

Explanation: <https://aws.amazon.com/premiumsupport/knowledge-center/lambda-iterator-age/>

* 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. (Correcta)**

Explanation: 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.

* 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. (Correcta)**

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.

* 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. (Correcta)**

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.

* A company hosts its application in the us-west-1 Region. The company wants to add redundancy in the us-east-1 Region.

The application secrets are stored in AWS Secrets Manager in us-west-1. A developer needs to replicate the secrets to us-east-1.

Which solution will meet this requirement?

**A. Configure secret replication for each secret. Add us-east-1 as a replication Region. Choose an AWS Key Management Service (AWS KMS) key in us-east-1 to encrypt the replicated secrets. (Correcta)**

B. Create a new secret in us-east-1 for each secret. Configure secret replication in us-east-1. Set the source to be the corresponding secret in us-west-1. Choose an AWS Key Management Service (AWS KMS) key in us-west-1 to encrypt the replicated secrets.

C. Create a replication rule for each secret. Set us-east-1 as the destination Region. Configure the rule to run during secret rotation. Choose an AWS Key Management Service (AWS KMS) key in us-east-1 to encrypt the replicated secrets.

D. Create a Secrets Manager lifecycle rule to replicate each secret to a new Amazon S3 bucket in us-west-1. Configure an S3 replication rule to replicate the secrets to us-east-1.

Explanation:

**AWS Secrets Manager** natively supports secret **replication** across **Regions**.

**secret rotation** do **not** exist as a feature in **Secrets Manager**.

* 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. (Correcta)**

D. AWS Directory Service.

Explanation: You can't register using Identity Pool. It lets you authenticate with provided identification pools.

* 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. (Correcta)**

* 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. (Correcta)**

D. Create one API Gateway and one Lambda function, and use a REST parameter to identify the environment.

* 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. (Su respuesta)(Correcta)**

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.

* 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. (Correcta)**

D. Run Amazon Inspector agents and then analyze performance.

Explanation: 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.

* 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. (Su respuesta)(Correcta)**

D. Create a certificate in ACM in the us-east-1 Region. Update the CloudFormation template to deploy the certificate to each ALB.

Explanation: <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html>

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

DELETE\_FAILED (The following resource(s) failed to delete:

[ASGInstanceRole12345678].)

Which action should the developer take to resolve this error?

A. Contact AWS Support to report an issue with the Auto Scaling Groups (ASG) service.

B. Add a DependsOn attribute to the ASGInstanceRole12345678 resource in the CloudFormation template. Then delete the stack.

**C. Modify the CloudFormation template to retain the ASGInstanceRole12345678 resource. Then**

**manually delete the resource after deployment. (Correcta)**

D. Add a force parameter when calling CloudFormation with the role-arn of ASGInstanceRole12345678.

* 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. (Correcta)**

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.

Explanation: It's not secure to store API keys in git repository. Hence storing it in secret manager is a most secure to way to handle this scenario.

* A company that has large online business uses an Amazon DynamoDB table to store sales data. The company enabled Amazon DynamoDB Streams on the table. The transaction status of each sale is stored in a TransactionStatus attribute in the table. The value of the TransactionStatus attribute must be either failed, pending, or completed.

The company wants to be notified of failed sales where the Price attribute is above a specific threshold. A developer needs to set up notification for the failed sales.

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

A. Create an event source mapping between DynamoDB Streams and an AWS Lambda function.

Use Lambda event filtering to trigger the Lambda function only if sales fail when the price is above the specified threshold. Configure the Lambda function to publish the data to an Amazon Simple Notification Service (Amazon SNS) topic.

B. Create an event source mapping between DynamoDB Streams and an AWS Lambda function.

Configure the Lambda function handler code to publish to an Amazon Simple Notification Service (Amazon SNS) topic if sales fail when price is above the specified threshold.

**C. Create an event source mapping between DynamoDB Streams and an Amazon Simple Notification Service (Amazon SNS) topic. Use event filtering to publish to the SNS topic if sales fail when the price is above the specified threshold. (Correcta)**

D. Create an Amazon CloudWatch alarm to monitor the DynamoDB Streams sales data. Configure the alarm to publish to an Amazon Simple Notification Service (Amazon SNS) topic if sales fail due when price is above the specified threshold.

* 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. (Correcta)**

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.

Explanation: 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.

* 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. (Correcta)**

* 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. (Correcta)**

B. Amazon Elastic File System (Amazon EFS).

C. Amazon Elastic Block Store (Amazon EBS).

D. Amazon S3.

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>

* A company runs an ecommerce application on AWS. The application stores data in an Amazon Aurora database.

A developer is adding a caching layer to the application. The caching strategy must ensure that the application always uses the **most recent value for each data item**.

Which caching strategy will meet these requirements?

**A. Implement a TTL strategy for every item that is saved in the cache. (Correcta)**

B. Implement a write-through strategy for every item that is created and updated.

C. Implement a lazy loading strategy for every item that is loaded.

D. Option 4

Explanation:

Option B. Implement a write-through strategy for every item that is created and updated: the cache always has the most recent and consistent values because updates are propagated to both the cache and the database simultaneously.

Option A (TTL strategy): incorrect, Time-to-Live can help ensure freshness by expiring items after a certain time, it does not guarantee the cache always contains the most recent value. There may be stale data between TTL expirations.

* 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. Connect 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. (Correcta)**

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.

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

* 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. (Correcta)**

Explanation: The best caching strategy for populating real-time dashboards using Amazon ElastiCache 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.

* 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. (Correcta)**

**B. One of the earlier stages in the pipeline failed and the pipeline has terminated. (Correcta)**

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.

* 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. (Correcta)**

C. Configure Amazon Simple Workflow Service to process any direct unprocessed events.

D. Configure AWS Config to process any direct unprocessed events.

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.

* 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. (Correcta)**

**D. Amazon Aurora MySQL with operations made within a transaction block. (Correcta)**

E. Amazon Athena with operations made within a transaction block.

Explanation: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/transaction-apis.html>

* 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. (Correcta)**

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.

Explanation:

**no out-of-order updates** means that message **ordering** must be preserved. SQS FIFO (First-In-First-Out) queues.

visibility timeout ensures that a message is not processed by multiple consumers simultaneously.

* 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. (Correcta)**

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.

* 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. (Correcta)**

D. Configure reserved concurrency for each Lambda function by setting the ReservedConcurrentExecutions parameter to 10.

Explanation: **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.

* 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. (Correcta)**

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.

* 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. (Correcta)**

C. CacheMissCount.

**D. Latency. (Correcta)**

E. Count.

Explanation: The issue is caused by **timeout**. So the developer needs to know the latency information.

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

<https://repost.aws/knowledge-center/api-gateway-rest-api-504-errors>

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

* 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. (Correcta)**

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.

* 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. (Correcta)**

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.

* 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. (Correcta)**

**D. Set the deployment preference type to Canary10Percent30Minutes. Use hooks to test the deployment. (Correcta)**

E. Set the deployment preference type to Linear10PercentEvery10Minutes. Use hooks to test the deployment.

Explanation:

Option C. Enable gradual deployments through AWS SAM templates: Using AWS SAM templates, you can configure gradual deployment strategies such as canary deployments or linear deployments.

Option D. Set the deployment preference type to Canary10Percent30Minutes. Use hooks to test the deployment.

canary deployment allows you to direct a small portion (in this case, 10%) of the traffic to the updated version of the Lambda function for a specific time period (30 minutes).

Hooks can be used to run tests or checks during the deployment process.

* 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. Correcta)**

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. (Correcta)**

E. Increase the provisioned write capacity of the DynamoDB tables that the operation accesses.

Explanation:

For B: "If DynamoDB returns any unprocessed items, you should retry the batch operation on those items. However, we strongly recommend that you use an **exponential backoff** algorithm. If you retry the batch operation immediately, the underlying read or write requests can still fail due to throttling on the individual tables".

For D: "The most likely cause of a failed read or a failed write is throttling. For BatchGetItem, one or more of the tables in the batch request does not have enough provisioned read capacity to support the operation." Extracted from Error Handling Documentation: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Programming.Errors.html#BatchOperations>

* 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. (Correcta)**

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.

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

* 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. (Correcta)**

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.

Explanation: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/using-presigned-url.html>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html>

* 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. (Correcta)**

D. AWS CloudTrail logs.

* A development team set up a pipeline to launch a test environment. The developers want to automate tests for their application. The team created an AWS CodePipeline stage to deploy the application to a test environment in batches using AWS Elastic Beanstalk. A later CodePipeline stage contains a single action that uses AWS CodeBuild to run numerous automated Selenium-based tests on the deployed application. The team must speed up the pipeline without removing any of the individual tests.

Which set of actions will MOST effectively speed up application deployment and testing?

**A. Set up an all-at-once deployment in Elastic Beanstalk. Run tests in parallel with multiple CodeBuild actions. (Correcta)**

B. Set up a rolling update in Elastic Beanstalk. Run tests in serial with a single CodeBuild action.

C. Set up an immutable update in Elastic Beanstalk. Run tests in serial with a single CodeBuild action.

D. Set up a traffic-splitting deployment in Elastic Beanstalk. Run tests in parallel with multiple CodeBuild actions

.

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

**All at once**: The **quickest** deployment method. Suitable if you can accept a short loss of service, and if quick deployments are important to you. With this method, Elastic Beanstalk deploys the new application version to each instance. Then, the web proxy or application server might need to restart. As a result, your application might be unavailable to users (or have low availability) for a short time.

* A developer is writing an application, which stores data in an Amazon DynamoDB table. The developer wants to query the DynamoDB table by using the partition key and a different sort key value. The developer needs the latest data with all recent write operations.

How should the developer write the DynamoDB query?

A. Add a local secondary index (LSI) during table creation. Query the LSI by using eventually consistent reads.

**B. Add a local secondary index (LSI) during table creation. Query the LSI by using strongly consistent reads. (Correcta)**

C. Add a global secondary index (GSI) during table creation. Query the GSI by using eventually consistent reads.

D. Add a global secondary index (GSI) during table creation. Query the GSI by using strongly consistent reads.

Explanation:

Local Secondary Index (**LSI**): querying with same partition key but a different sort key. Supports **strongly consistent reads** (retrieves the most-up-to-date data).

Global Secondary Index (**GSI**): querying with a different partition key. Supports eventually consistent reads (**not return the latest data**)

* 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 tile 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. (Correcta)**

Explanation:

EventBridge rules can directly filter specific events (CreateRole) from AWS CloudTrail logs. You can configure a rule to look for IAM role creation events and check if they lack attributes indicating they were created by AWS CloudFormation.

* 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. (Correcta)**

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.

Explanation: Under the "Test" tab there's an option. (Shareable) This event is available to IAM users within the same account who have permissions to access and use shareable events.

<https://docs.aws.amazon.com/lambda/latest/dg/testing-functions.html#creating-shareable-events>

* A company uses AWS X-Ray to monitor a serverless application. The components of the application have different request rates. The user interactions and transactions are important to trace, but they are low in volume. The background processes such as application health checks, polling, and connection maintenance generate high volumes of read-only requests.

Currently, the default X-Ray sampling rules are universal for all requests. Only the first request per second and some additional requests are recorded. This setup is not helping the company review the requests based on service or request type.

A developer must configure rules to trace requests based on service or request properties. The developer must trace the user interactions and transactions without wasting effort recording minor background tasks.

Which solution will meet these requirements?

A. Disable sampling for high-volume read-only requests. Sample at a lower rate for all requests that

handle user interactions or transactions.

B. Disable sampling and trace all requests for requests that handle user interactions or transactions.

Sample high-volume read-only requests at a higher rate.

**C. Disable sampling and trace all requests for requests that handle user interactions or transactions. Sample high-volume read-only requests at a lower rate. (Correcta)**

D. Disable sampling for high-volume read-only requests. Sample at a higher rate for all requests that handle user interactions or transactions.

* 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. (Correcta)**

C. Increase the memory size of the function.

D. Use Amazon S3 to host the function dependencies.

* 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. (Correcta)**

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.

* 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 he 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. (Correcta)**

Explanation: NAT Gateway is for when we want Lambda to access the public when it is in a private VPC. <https://docs.aws.amazon.com/lambda/latest/dg/foundation-networking.html>

* 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. (Correcta)**

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.

Explanation: "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>

* 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. (Correcta)**

Explanation: This solution ensures that users can access only their own files in a secure manner.

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

* 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. (Correcta)**

D. Add a layer to the Lambda function. Select the S3 bucket as the source.

Explanation: 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.

* 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. (Correcta)**

D. Create one Amazon Simple Notification Service (Amazon SNS) topic. Subscribe all partners to the SNS topic.

Explanation: <https://docs.aws.amazon.com/sns/latest/dg/sns-message-filtering.html>

* 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. (Correcta)**

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).

* 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. (Correcta)**

D. Establish trust, and add an SSH key for the second account to the IAM user.

* 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. (Correcta)**

D. Use an AWS CodeCommit repository to host the dependencies in a centralized location.

* 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. (Correcta)**

* 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. (Correcta)**

D. Amazon DynamoDB.

Explanation: Lambda automatically integrates with CloudWatch Logs and pushes all logs from your code to a CloudWatch Logs group associated with a Lambda function <https://docs.aws.amazon.com/prescriptive-guidance/latest/implementing-logging-monitoring-cloudwatch/lambda-logging-metrics.html>

* A developer is trying to get data from an Amazon DynamoDB table called demoman table. The developer configured the AWS CLI to use a specific IAM user's credentials and ran the following command:

aws dynamodb get-item --table-name demoman-table --key '{"id": {"N":"1993"}}'

The command returned errors and no rows were returned.

What is the MOST likely cause of these issues?

A. The command is incorrect; it should be rewritten to use put-item with a string argument.

B. The developer needs to log a ticket with AWS Support to enable access to the demoman-table.

C. Amazon DynamoDB cannot be accessed from the AWS CLI and needs to be called via the REST API.

**D. The IAM user needs an associated policy with read access to demoman-table. (Correcta)**

Explanation: The command is correct and the demoman table exists. The most likely issue is that the IAM user does not have a policy associated with read access to the demoman table. To resolve the issue, the developer must add a policy to the IAM user that grants read access to the demoman table.

* 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. (Correcta)**

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.

Explanation: 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.

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

* 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. (Correcta)**

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.

Explanation: 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>

* 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. (Correcta)**

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.

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

* 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). (Correcta)**

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.

* 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. (Correcta)**

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.

* A company used AWS to develop an application for customers. The application includes an Amazon API Gateway API that invokes AWS Lambda functions. The Lambda functions process data and store the data in Amazon DynamoDB tables. The company must monitor the entire application to identify potential bottlenecks in the architecture that can negatively affect customers.

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

**A. Instrument the application with AWS X-Ray. Inspect the service map to identify errors and issues. (Correcta)**

B. Configure Lambda exceptions and additional logging to Amazon CloudWatch. Use CloudWatch Logs Insights to query the logs.

C. Configure API Gateway to log responses to Amazon CloudWatch. Create a metric filter for the TooManyRequestsException error message.

D. Use Amazon CloudWatch metrics for the DynamoDB tables to identify all the ProvisionedThroughputExceededException error messages.

* 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. (Correcta)**

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.

Explanation: <https://docs.aws.amazon.com/apigateway/latest/developerguide/set-up-lambda-integration-async.html>

* A developer has written a distributed application that uses microservices. The microservices are running on Amazon EC2 instances. Because of message volume, the developer is unable to match log output from each microservice to a specific transaction. The developer needs to analyze the message flow to debug the application.

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

**A. Download the AWS X-Ray daemon. Install the daemon on an EC2 instance. Ensure that the EC2 instance allows UDP traffic on port 2000. (Correcta)**

B. Configure an interface VPC endpoint to allow traffic to reach the global AWS X-Ray daemon on TCP port 2000.

C. Enable AWS X-Ray. Configure Amazon CloudWatch to push logs to X-Ray.

**D. Add the AWS X-Ray software development kit (SDK) to the microservices. Use X-Ray to trace requests that each microservice makes. (Correcta)**

E. Set up Amazon CloudWatch metric streams to collect streaming data from the microservices.

* 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. (Correcta)**

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. Fall the stack**

**synthesis if any violations are present. (Correcta)**

Explanation:

Option B: Use the **CDK assertions module** for unit testing.

Option E: Use the **CDK Aspects class** to enforce security rules.

* 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. (Correcta)**

C. 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.

D. Create a bucket policy on the S3 bucket that allows s3:ListBucket and s3:\*Object permissions to the EC2 instance.

* 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 Cl/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. (Correcta)**

D. Use the aws lambda invoke command with a test event during the CIICD process.

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 behavior of the function based on its interactions with the test queue. This approach isolates the function's behavior from the rest of the system, which is a key principle of unit testing.

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

* 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. (Correcta)**

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.

Explanation: CloudWatch Logs can use filter expressions. For example, find a specific IP inside of a log Or count occurrences of "ERROR" in your logs - Metric filters can be used to trigger CloudWatch alarms.

* 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. (Correcta)**

* 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 writethrough caching strategy and read the data from Redis. (Correcta)**

Explanation: <https://docs.aws.amazon.com/whitepapers/latest/database-caching-strategies-using-redis/caching-patterns.html>

* 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. (Correcta)**

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.

Explanation:

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

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/es/blogs/security/use-amazon-inspector-to-manage-your-build-and-deploy-pipelines-for-containerized-applications/>

* 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. (Correcta)**

D. Store prerelease data in AWS Amplify DataStore. Toggle between hidden and visible states by using Amplify DataStore cloud synchronization.

Explanation: <https://aws.amazon.com/blogs/mt/using-aws-appconfig-feature-flags/>

* 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. (Su respuesta)(Correcta)**

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.

Explanation: This will allow the developer to implement a fallback mechanism by using another Lambda function that resizes the profile picture with the least development effort.

* 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. (Correcta)**

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.

* 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. (Correcta)**

D. The developer is attempting to make API calls to the incorrect AWS account.

Explanation: <https://docs.aws.amazon.com/IAM/latest/UserGuide/security-creds.html>

* 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 accidently 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. (Correcta)**

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.

* 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. (Correcta)**

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.

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

* 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. (Correcta)**

D. AWS Cloud9.

* 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. (Correcta)**

C. BeforeInstall -> ApplicationStop -> ValidateService -> ApplicationStart.

D. ApplicationStop -> BeforeInstall -> ValidateService -> ApplicationStart.

Explanation: <https://docs.aws.amazon.com/codedeploy/latest/userguide/reference-appspec-file-structure-hooks.html#reference-appspec-file-structure-hooks-run-order> Section: Run Order of Hooks in a Deployment.

* 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". (Correcta)**

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".

Explanation: <https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-policy-for-config-rule/>

**aws:SecureTransport: “false”** : checks for **non-HTTPS** traffic and **denies** it. Only **HTTPS** requests are **allowed**, enforcing encryption in transit.

* 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. (Correcta)**

D. Configure maximum concurrency on the SQS event source based on the third-party service's documented rate limits.

Explanation: Provisioned concurrency will not solve the problem as the number of instances can increase till it reaches the max number of unreserved limit (this is not reserved concurrency).

* 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. (Correcta)**

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.

Explanation: <https://docs.aws.amazon.com/apigateway/latest/developerguide/set-up-stages.html>

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

* 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. (Correcta)**

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. (Correcta)**

E. Add the signature to an HTTP header that is named WWW-Authenticate.

* 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. (Correcta)**

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.

Explanation: <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>

* 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. (Correcta)**

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

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

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

B. The updateAuthorizer method must be called to update the API's authorizer to include the newly

created API key.

C. The importApiKeys method must be called to import all newly created API keys into the current

stage of the API.

**D. The createUsagePlanKey method must be called to associate the newly created API key with the correct usage plan. (Correcta)**

* A developer needs to modify an application architecture to meet new functional requirements. Application data is stored in Amazon DynamoDB and processed for analysis in a nightly batch. The system analysts do not want to wait until the next day to view the processed data and have asked to have it available in near-real time.

Which application architecture pattern would enable the data to be processed as it is received

**A. Event driven. (Correcta)**

B. Client-server driven.

C. Fan-out driven.

D. Schedule driven.

* 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. (Correcta)**

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.

* 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). (Correcta)**

C. Server-side encryption with customer-provided keys (SSE-C).

D. Server-side encryption with self-managed keys.

Explanation: **KMS** provides **audit** functionalities.

* 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. (Correcta)**

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.

Explanation: <https://docs.aws.amazon.com/AmazonS3/latest/API/API_ListBuckets.html>

* 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. (Correcta)**

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.

* 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.** 

**(Correcta)**

B.



C.



D.



* 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. (Correcta)**

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.

Explanation: 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/>

* 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. (Correcta)**

D. Amazon DynamoDB Accelerator (DAX).

* 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. (Correcta)**

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.

Explanation: <https://aws.amazon.com/s3/storage-classes/>

* A developer uses an AWS Lambda function in an application to edit users' uploaded photos. The developer needs to update the Lambda function code and needs to test the updates.

For testing, the developer must divide the user traffic between the original version of the Lambda function and the new version of the Lambda function.

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

**A. Publish a version of the original Lambda function. Make the necessary changes to the Lambda code. Publish a new version of the Lambda function. (Correcta)**

B. Use AWS CodeBuild to detect updates to the Lambda function. Configure CodeBuild to incrementally shift traffic from the original version of the Lambda function to the new version of the Lambda function.

C. Update the original version of the Lambda function to add a function URL. Make the necessary changes to the Lambda code. Publish another function URL for the updated Lambda code.

**D. Create an alias that points to the original version of the Lambda function. Configure the alias to be a weighted alias that also includes the new version of the Lambda function. Divide traffic between the two versions. (Correcta)**

E. Create an alias that points to the original function URL. Configure the alias to be a weighted alias that also includes the additional function URL. Divide traffic between the two function URLs.

Explanation:

**alias** simplifies **traffic** shifting. Function URLs do not support weighted traffic shifting

* A developer has an application that uses WebSocket APIs in Amazon API Gateway. The developer wants to use an **API Gateway Lambda authorizer** to control access to the application.

The developer needs to add credential caching and reduce repeated usage of secret keys and authorization tokens on every request.

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

**A. Use a token-based Lambda authorizer. (Correcta)**

B. Use a request parameter-based Lambda authorizer.

**C. Configure an integration request mapping template to reference the context map from the APIGateway Lambda authorizer. (Correcta)**

D. Configure an integration request mapping template to reference the identity API key value from the API Gateway Lambda authorizer.

E. Use VPC endpoint policies for the WebSocket APIs.

Explanation:

Option A: token-based Lambda authorizer to validate credentials (tokens or API keys) passed in requests. Support **credential caching** (reducing the need to revalidate the token on every request).

Option C: **Context map** in API Gateway Lambda authorizers contains **metadata** from the authorization process (user ID, roles, or custom claims).

* A Developer has been asked to build a real-time dashboard web application to visualize the key prefixes and storage size of objects in Amazon S3 buckets. Amazon DynamoDB will be used to store the Amazon S3 metadata.

What is the optimal and MOST cost-effective design to ensure that the real-time dashboard is kept up to date with the state of the objects in the Amazon S3 buckets?

A. Use an Amazon CloudWatch event backed by an AWS Lambda function. Issue an Amazon S3 API call to get a list of all Amazon S3 objects and persist the metadata within DynamoDB. Have the web application poll the DynamoDB table to reflect this change.

**B. Use Amazon S3 Event Notification backed by a Lambda function to persist the metadata into DynamoDB. Have the web application poll the DynamoDB table to reflect this change. (Correcta)**

C. Run a cron job within an Amazon EC2 instance to list all objects within Amazon S3 and persist the metadata into DynamoDB. Have the web application poll the DynamoDB table to reflect this change.

D. Create a new Amazon EMR cluster to get all the metadata about Amazon S3 objects; persist the metadata into DynamoDB. Have the web application poll the DynamoDB table to reflect this change.

Explanation: Cloudwatch notifications are at best every minute at extra cost. Lambda off an S3

notification will provide real-time data and lambda is the most cost effective processing method.

Option B: **Real-Time Updates**: **Amazon S3** **Event Notifications** can be configured to trigger an AWS Lambda function when specific events occur in an S3 bucket, such as object creation or deletion.

Option A: CloudWatch Events introduces unnecessary overhead and is **not real-time**.

* 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. (Correcta)**

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.

Explanation:

**AWS SAM CLI** (Serverless Application Model Command Line Interface) provides tools specifically for **local** **testing** of AWS Lambda functions.

* A developer manages an application that writes customer orders to an Amazon DynamoDB table. The orders use customer\_id as the partition key, order\_id as the sort key, and order\_date as an attribute. A new access pattern requires accessing data by order\_date and order\_id. The developer needs to implement a new AWS Lambda function to support the new access pattern.

How should the developer support the new access pattern in the MOST operationally efficient way?

A. Add a new local secondary index (LSI) to the DynamoDB table that specifies order\_date as the partition key and order\_id as the sort key. Write the new Lambda function to query the new LSI index.

B. Write the new Lambda function to scan the DynamoDB table. In the Lambda function, write a method to retrieve and combine results by order\_date and order\_id.

**C. Add a new global secondary index (GSI) to the DynamoDB table that specifies order\_date as the partition key and order\_id as the sort key. Write the new Lambda function to query the new GSI index. (Correcta)**

D. Enable DynamoDB Streams on the table. Choose the new and old images information to write to the DynamoDB stream. Write the new Lambda function to query the DynamoDB stream.

Explanation:

**Global Secondary Index (GSI)**: create query pattern by new partition key and sort key. Can be added to **existing** **tables**.

**Local Secondary Index (LSI):** cannot be added after table creation, must be defined at the time of table creation.

* 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. (Correcta)**

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.

Explanation: <https://aws.amazon.com/blogs/networking-and-content-delivery/implementing-default-directory-indexes-in-amazon-s3-backed-amazon-cloudfront-origins-using-cloudfront-functions/>

CloudFront Functions for customizing URL behavior.

* 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. (Correcta)**

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. (Correcta)**

* 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. (Correcta)**

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.

* 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. (Correcta)**

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.

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**: for storing and retrieving non-sensitive configuration data (API URL) across environments (development, testing, production).

**AWS Secrets Manager**: for storing and managing sensitive information (authentication credentials).

* 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. (Correcta)**

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.

Explanation: **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

* 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. (Correcta)**

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.

Explanation: You can use the Embedded Metrics format to embed custom metrics alongside detailed log event data. CloudWatch automatically extracts the custom metrics so you can visualize and alarm on them, for real-time incident detection. <https://docs.aws.amazon.com/lambda/latest/operatorguide/custom-metrics.html>

* 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. (Correcta)**

**B. Modify the application to use the AWS SDKs for DynamoDB. (Correcta)**

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.

Explanation: Your request rate is too high. The AWS SDKs for DynamoDB automatically retry requests that receive this exception. Your request is eventually successful, unless your retry queue is too large to finish. Reduce the frequency of requests using Error Retries and Exponential Backoff.

* 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. (Correcta)**

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 ISet the variation to Variation A.

Explanation: Overrides let you pre-define the variation for selected users. to always receive the editable variation. <https://aws.amazon.com/es/blogs/aws/cloudwatch-evidently/>

* 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). (Correcta)**

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. (Correcta)**

Explanation: <https://docs.aws.amazon.com/efs/latest/ug/efs-onpremises.html>

* An open-source map application gathers data from several geolocation APIs. The application's source code repository is public and can be used by anyone, but the geolocation APIs must not be directly accessible.

A developer must implement a solution to prevent the credentials that are used to access the APIs from becoming public. The solution also must ensure that the application still functions properly.

Which solution will meet these requirements MOST cost-effectively?

A. Store the credentials in AWS Secrets Manager. Retrieve the credentials by using the GetSecretValue API operation.

B. Store the credentials in AWS Key Management Service (AWS KMS). Retrieve the credentials by using the GetPublicKey API operation.

C. Store the credentials in AWS Security Token Service (AWS STS). Retrieve the credentials by using the GetCallerldentity API operation.

**D. Store the credentials in AWS Systems Manager Parameter Store. Retrieve the credentials by using the GetParameter API operation. (Correcta)**

Explanation: Secrets Manager: It is paid. The storage cost is $0.40 per secret per month and API interactions cost is $0.05 per 10,000 API calls. Parameter Store: For Standard parameters, No additional charge for storage and standard throughput. For higher throughput, API interactions cost is $0.05 per 10,000 API calls. For Advanced parameters, storage cost is $0.05 per advanced parameter per month and API interactions cost is $0.05 per 10,000 API calls. <https://aws.amazon.com/es/systems-manager/pricing/>

* 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. (Correcta)**

D. Add a test phase to the aws-exports.js file for the application.

Explanation: You can run end-to-end (E2E) tests in the test phase of your Amplify app to catch regressions before pushing code to production. The test phase can be configured in the build specification YML. <https://docs.aws.amazon.com/amplify/latest/userguide/running-tests.html>

* 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. (Correcta)**

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.

Explanation: Setting the integration type to MOCK allows you to create mock responses without having a backend implementation. With this approach, you can easily provide predefined JSON responses for specific HTTP status codes, allowing the frontend team to work on UI development with realistic data. Configuring the method's integration request and integration response in API Gateway allows you to define the expected request and response formats, including associating JSON responses with specific HTTP status codes.

* 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. (Correcta)**

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.

* 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. (Correcta)**

Explanation: <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/parameters-section-structure.html> Parameters: InstanceTypeParameter: Type: String Default: t2.micro AllowedValues: - t2.micro - m1.small - m1.large Description: Enter t2.micro, m1.small, or m1.large. Default is t2.micro.

* 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. (Correcta)**

C. Provides better error handling.

D. Creates a new SDK instance for each invocation.

Explanation: 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.

* 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. (Correcta)**

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.

Explanation: <https://docs.aws.amazon.com/lambda/latest/dg/invocation-async.html#invocation-dlq>

* 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. (Correcta)**

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.

* 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. (Correcta)**

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.

Explanation: Lambda@Edge is a good fit for the following scenarios: Functions that take several milliseconds or more to complete. Functions that require adjustable CPU or memory. Functions that depend on third-party libraries (including the AWS SDK, for integration with other AWS services).

* 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. Correcta)**

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.

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.

* 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. (Correcta)**

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.

* 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. (Correcta)**

* 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. (Correcta)**

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.

Explanation: <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

* 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. (Correcta)**

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.

* 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. (Correcta)**

**E. Store the application's static content in Amazon S3. (Correcta)**

Explanation:

Option (D), creating an Amazon CloudFront distribution to cache static content, is the most recommended solution. CloudFront 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.

* 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. (Correcta)**

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.

* A company uses the AWS SDK for JavaScript in the Browser to build a web application and then hosts the application on Amazon S3. The company wants the application to support 10,000 users concurrently. The company selects Amazon DynamoDB to store user preferences in a table.

There is a requirement to uniquely identify users at any scale.

Which solution will meet these requirements?

A. Create a user cookie. Attach an IAM role to the S3 bucket that hosts the application.

B. Deploy an Amazon CloudFront distribution with an origin access identity (OAI) to access the S3 bucket.

**C. Configure and use Amazon Cognito. Access DynamoDB with the authenticated users. (Correcta)**

D. Create an IAM user for each user. Use fine-grained access control on the DynamoDB table to control access.

Explanation: This will allow the application to support 10,000 users concurrently and will provide a unique identifier for each user. By using Amazon Cognito, the company can authenticate users and then access DynamoDB with the authenticated users to store their preferences in a table.

This approach will allow the company to control access to the DynamoDB table and to scale to any number of users. Creating a user cookie or deploying an Amazon CloudFront distribution with an OAI would not solve the problem because these solutions do not provide a way to uniquely identify users or control access to DynamoDB. Creating an IAM user for each user and using fine-grained access control on the DynamoDB table would not be practical or scalable because it would require the company to manage and maintain a large number of IAM users. When dealing with user profiles in serverless applications we often turn to Cognito for managing their credentials while the app itself will store user entities.

<https://www.sorenandersen.com/manage-user-profile-data-between-cognito-and-dynamodb/>

* 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. (Correcta)**

* 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. (Correcta)**

* An AWS Lambda function is invoked asynchronously to process events. Occasionally, the Lambda function falls to process events. A developer needs to collect and analyze these failed events to fix the issue.

What should the developer do to meet these requirements with the LEAST development effort?

A. Add logging statements for all events in the Lambda function. Filter AWS CloudTrail logs for errors.

B. Configure the Lambda function to start an AWS Step Functions workflow with retries for failed events.

**C. Add a dead-letter queue to send messages to an Amazon Simple Queue Service (Amazon SQS) standard queue. (Correcta)**

D. Add a dead-letter queue to send messages to an Amazon Simple Notification Service (Amazon SNS) FIFO topic.

* 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. (Correcta)**

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.

Explanation:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-concepts.html>

<https://awscli.amazonaws.com/v2/documentation/api/2.1.30/reference/cloudformation/create-stack-set.html>

* 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. (Correcta)**

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.

* A developer creates an AWS Lambda function that is written in Java. During testing, the Lambda function does not work how the developer expected. The developer wants to use tracing capabilities to troubleshoot the problem.

Which AWS service should the developer use to accomplish this goal?

A. AWS Trusted Advisor.

B. Amazon CloudWatch.

**C. AWS X-Ray. (Correcta)**

D. AWS CloudTrail.

* A developer has a continuous integration and continuous delivery (CI/CD) pipeline that uses AWS CodeArtifact and AWS CodeBuild. The build artifacts are between 0.5 GB and 1.5 GB in size. The builds happen frequently and retrieve many dependencies from CodeArtifact each time.

The builds have been slow because of the time it takes to transfer dependencies.

The developer needs to improve build performance by reducing the number of dependencies that are retrieved for each build.

Which solution will meet this requirement?

A. Specify an Amazon S3 cache in CodeBuild. Add the S3 cache folder path to the buildspec.yaml file for the build project.

B. Specify a local cache in CodeBuild. Add the CodeArtifact repository name to the buildspec.yaml file for the build project.

**C. Specify a local cache in CodeBuild. Add the cache folder path to the buildspec.yaml file for the build project. (Correcta)**

D. Retrieve the buildspec.yaml file directly from CodeArtifact. Add the CodeArtifact repository name to the buildspec.yaml file for the build project.

Explanation: Using a local cache in CodeBuild allows you to cache dependencies locally on the build host, which can significantly reduce the time it takes to retrieve dependencies during subsequent builds.

* 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. (Correcta)**

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.

* 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. (Correcta)**

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. (Correcta)**

E. Include the GetSessionToken API operation in the application code logic to obtain temporary credentials to access the PII table.

* 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. (Correcta)**

D. Create an Amazon Simple Notification Service (Amazon SNS) topic that has a subscription to the Lambda function with a 600-second timer.

Explanation: Amazon EventBridge can be used to run Lambda functions on a regular schedule. You can set a cron or rate expression to define the schedule.

* 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. (Correcta)**

D. Add the lambda:GetFunctionConcurrency action to the execution role.

**E. Request a service quota change for increased concurrency. (Correcta)**

* 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. (Correcta)**

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.

* 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. (Correcta)**

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.

Explanation: 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.

* 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. (Correcta)**

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.

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

* 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 BatchGetltem 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. (Correcta)**

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 BatchGetltem 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.

Explanation: BatchGetItem can return one or multiple items from one or more tables.

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

* 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. (Correcta)**

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. (Correcta)**

E. Allow all users to access the sample content by default. Create a role for authenticated users that allows access to the other content.

Explanation:

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.

* 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. (Correcta)**

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.

Explanation: Amazon ElastiCache for Memcached is a scalable, multithreaded caching solution that can be used to offload heavy read traffic from Amazon RDS instances. ElastiCache for Memcached is easy to configure and manage, making it a low-effort solution to meet technical lead requirements.

* 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. (Correcta)**

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.

Explanation: By adding a second cache behavior 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 behavior's settings remain unchanged, and private content remains secure because it still requires signed cookies for access. If you create additional cache behaviors, the default cache behavior is always the last to be processed.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html#DownloadDistValuesCacheBehavior>

* 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). (Correcta)**

D. AWS Cloud Development Kit (AWS CDK).

Explanation: The AWS Serverless Application Model(SAM) is an open-source framework for building serverless applications. It provides shorthand syntax to express functions, APIs, databases, and event source mappings. With just a few lines per resource, you can define the application you want and model it using YAML. <https://aws.amazon.com/es/serverless/sam/>

* 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. (Correcta)**

Explanation:

<https://aws.amazon.com/blogs/infrastructure-and-automation/deploying-aws-lambda-functions-using-aws-cloudformation-the-portable-way/>

* A developer built an application by using multiple AWS Lambda functions. The Lambda functions must access dynamic configuration data at runtime. The data is maintained as a 6 KB JSON document in AWS AppConfig. The configuration data needs to be updated without requiring the redeployment of the application.

The developer needs a solution that will give the Lambda functions access to the dynamic configuration data.

What should the developer do to meet these requirements with the LEAST development effort?

A. Migrate the document from AWS AppConfig to a Lambda environment variable. Read the document at the runtime.

**B. Configure the AWS AppConfig Agent Lambda extension. Access the dynamic configuration data by calling the extension on a local host. (Correcta)**

C. Use the AWS X-Ray SDK to call the AWS AppConfig APIs. Retrieve the configuration file at runtime.

D. Migrate the configuration file to a Lambda deployment package. Read the file from the file system at runtime.

* 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. (Correcta)**

D. Convert the API Gateway type from REST API to HTTP API.

* 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:



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

**A. Implement retries with exponential backoff. (Correcta)**

B. Use a PutRecord API instead of PutRecords.

**C. Reduce the frequency and/or size of the requests. (Correcta)**

D. Use Amazon SNS instead of Kinesis.

E. Reduce the number of KCL consumers.

Explanation: ProvisionedThroughputExceededException: 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.

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

* A company has multiple Amazon VPC endpoints in the same VPC. A developer needs to configure an Amazon S3 bucket policy so users can access an S3 bucket only by using these VPC endpoints.

Which solution will meet these requirements?

A. Create multiple S3 bucket polices by using each VPC endpoint ID that have the aws:SourceVpce value in the StringNotEquals condition.

B. Create a single S3 bucket policy that has the aws:SourceVpc value and in the StringNotEquals condition to use VPC ID.

C. Create a single S3 bucket policy that has the aws:SourceVpce value and in the StringNotEquals condition to use vpce\*.

**D. Create a single S3 bucket policy that has multiple aws:sourceVpce value in the StringNotEquals condition. Repeat for all the VPC endpoint IDs. (Correcta)**

* 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-EXAMPLEBUCKET. 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?

1. **(Correcta)**



B.



C.



D.



* 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. (Correcta)**

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 massage to the chat.

Explanation: <https://repost.aws/es/knowledge-center/secrets-manager-share-between-accounts/>

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

* 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. (Correcta)**

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.

* 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. (Correcta)**

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.

Explanation: 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.

* 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. (Correcta)**

D. The DynamoDB table is not running in the same Availability Zone as the Lambda function.

Explanation: The Lambda function needs to have the appropriate IAM permissions to write to the

DynamoDB table. If the function does not have these permissions, it will fail when it attempts to

write to the table. <https://aws.amazon.com/es/blogs/security/how-to-create-an-aws-iam-policy-to-grant-aws-lambda-access-to-an-amazon-dynamodb-table/>

* 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. (Correcta)**

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.

* 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. (Correcta)**

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

* 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. (Correcta)**

* A company launched an online portal to announce a new product that the company will release in 6 months. The portal requests that users enter an email address to receive communications about the product. The company needs to create a REST API that will store the email addresses in Amazon DynamoDB.

A developer has created an AWS Lambda function that can store the email addresses. The developer will deploy the Lambda function by using the AWS Serverless Application Model (AWS SAM). The developer must provide access to the Lambda function over HTTP.

Which solutions will meet these requirements with the LEAST additional configuration? (Choose two.)

**A. Expose the Lambda function by using function URLs. (Correcta)**

B. Expose the Lambda function by using a Gateway Load Balancer.

C. Expose the Lambda function by using a Network Load Balancer.

D. Expose the Lambda function by using AWS Global Accelerator.

**E. Expose the Lambda function by using Amazon API Gateway. (Correcta)**

* A company has a web application that contains an Amazon API Gateway REST API. A developer has created an AWS CloudFormation template for the initial deployment of the application. The developer has deployed the application successfully as part of an AWS CodePipeline continuous integration and continuous delivery (CI/CD) process. All resources and methods are available through the deployed stage endpoint.

The CloudFormation template contains the following resource types:

AWS::ApiGateway::RestApi

AWS::ApiGateway::Resource

AWS::ApiGateway::Method

AWS::ApiGateway::Stage

AWS::ApiGateway::Deployment

The developer adds a new resource to the REST API with additional methods and redeploys the template. CloudFormation reports that the deployment is successful and that the stack is in the UPDATE\_COMPLETE state. However, calls to all new methods are returning 404 (Not Found) errors.

What should the developer do to make the new methods available?

A. Specify the disable-rollback option during the update-stack operation.

B. Unset the CloudFormation stack failure options.

**C. Add an AWS CodeBuild stage to CodePipeline to run the aws apigateway create-deployment AWS CLI command. (Correcta)**

D. Add an action to CodePipeline to run the aws cloudfront create-invalidation AWS CLI command.

* 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. (Correcta)**

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.

* 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. (Correcta)**

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.

* 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. (Correcta)**

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.

Explanation: This will allow the company to deploy the application to the us-west-1 Region using

the same custom AMI that is used in the us-east-1 Region.

* 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. (Correcta)**

B. Write data to Amazon Elastic Block Store.

C. Write data to Amazon EC2 Instance Store.

D. Write data to the root filesystem.

Explanation: By storing session data in ElastiCache, you ensure that regardless of which EC2 instance handles a given request, the session data can be consistently and rapidly accessed.

* 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. (Correcta)**

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.

Explanation: You can use Amazon Elasticache for Redis Sorted Sets to easily implement a dashboard that keeps a list of sorted data by their rank.

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

<https://aws.amazon.com/es/elasticache/redis-vs-memcached/>

* 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. (Correcta)**

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. (Correcta)**

E. The network team’s template does not export the subnets in the Mappings section.

Explanation:

When referencing resources from another stack, the **exporting stack** must declare those resources in the **Outputs** section with the **Export** key, and the importing stack must use the **ImportValue** function to access them.

Option B: If subnets were created in another CloudFormation **stack**, the developer's template must use the **ImportValue** intrinsic function to reference the exported values (subnet IDs) from the network team's stack.

Option D**:** For the **ImportValue** function to work, the network team's stack must explicitly export the subnet IDs in its Outputs section. If the subnet IDs are not exported, they cannot be referenced by other templates.

Option A: Ref to reference resources within the same stack.

Option C: Mapping section for static configuration values, not for dynamically referencing resources created in another stack.

A screenshot of a computer

Description automatically generated

* A developer is working on an app for a company that uses an Amazon DynamoDB table named Orders to store customer orders. The table uses OrderID as the partition key and there is no sort key. The table contains more than 100,000 records. The develop needs to a add a functionality that will retrieve all Orders records that contain an OrderSource attribute with the MobileApp value.

Which solution will improve the user experience in the MOST efficient way?

1. Perform a Scan operation on the Orders table. Provide a QueryFilter condition to filter to only the items where the OrderSource attribute is equal to the MobileApp value.
2. Create a local secondary index (LSI) with OrderSource as the partition key. Perform a Query operation by using MobileApp as the key.
3. Create a global secondary index (GSI) with OrderSource as the sort key. Perform a Query operation by using MobileApp as the key.
4. **Create a global secondary index (GSI) with OrderSource as the partition key. Perform a Query operation by using MobileApp as the key.**

Explanation:

A **Global Secondary Index (GSI)** allows you to create a different partition key and sort key for a DynamoDB table. In this case, using **OrderSource** as the **partition key** in a GSI enables efficient querying for all records with **OrderSource** = **MobileApp**.

* A company has an application that uses an AWS Lambda function to process data. A developer must implement encryption in transit for all sensitive configuration data, such as API keys, that is stored in the application. The developer creates an AWS Key Management Service (AWS KMS) customer managed key.

What should the developer do next to meet the encryption requirement?

A. Create parameters of the String type in AWS Systems Manager Parameter Store. For each parameter, specify the KMS key ID to encrypt the parameter in transit. Reference the GetParameter API call in the Lambda environment variables.

B. Create secrets in AWS Secrets Manager by using the customer managed KMS key. Create a new Lambda function and set up a Lambda layer. Configure the Lambda layer to retrieve the values from Secrets Manager.

C. Create objects in Amazon S3 for each sensitive data field. Specify the customer managed KMS key to encrypt the object. Configure the Lambda function to retrieve the objects from Amazon S3 during processing.

**D. Create encrypted Lambda environment variables. Specify the customer managed KMS key to encrypt the variables. Enable encryption helpers for encryption in transit. Grant permission to the Lambda function’s execution role to access the KMS key. (Correcta)**

Explanation:

Option A: String no cifra, KMS realiza el cifrado

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

* A developer is building an ecommerce application. When there is a sale event, the application needs to concurrently call three third-party systems to record the sale. The developer wrote three AWS Lambda functions. There is one Lambda function for each third-party system, which contains integration logic.

These Lambda functions are all independent. The developer need to design the application so each Lambda function will run regardless of others’ success or failure.

Which solution will meet these requirements?

A. Publish the sale event from the application to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the three Lambda functions to poll the queue.

**B. Publish the sale event from the application to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the three Lambda functions to be triggered by the SNS topic. (Correcta)**

C. Publish the sale event from the application to an Application Load Balance (ALB). Add the three Lambda functions as ALB targets.

D. Publish the sale event from the application to an AWS Step Functions state machine. Move the logic from the three Lambda functions into the Step Functions state machine.

Explanation:

Option B: SNS is a fan-out pattern where a single event can trigger multiple consumers independently. No es encolado como SQS, se envía independiente.

* 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 roles so that the change will take effect automatically. (Correcta)**

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.

* 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).**

* A developer manages a website that distributes its content by using Amazon CloudFront. The website's static artifacts are stored in an Amazon S3 bucket.

The developer deploys some changes and can see the new artifacts in the S3 bucket. However, the changes do not appear on the webpage that the CloudFront distribution delivers.

How should the developer resolve this issue?

**A. Configure S3 Object Lock to update to the latest version of the files every time an S3 object is updated. (Correcta)**

B. Configure the S3 bucket to clear all old objects from the bucket before new artifacts are uploaded.

C. Set CloudFront to invalidate the cache after the artifacts have been deployed to Amazon S3.

D. Set CloudFront to modify the distribution origin after the artifacts have been deployed to Amazon S3.

* 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. (Correcta)**

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.

* 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. (Correcta)**

D. Amazon CodeGuru.

Explanation: AWS CodeCommit - A fully-managed source control service that hosts secure Git-based repositories. CodeCommit makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem. This solution uses CodeCommit to create a repository to store the application and deployment codes. <https://aws.amazon.com/es/blogs/devops/complete-ci-cd-with-aws-codecommit-aws-codebuild-aws-codedeploy-and-aws-codepipeline/>

* 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 UserData 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. (Correcta)**

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. (Correcta)**

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 UserData script.

Explanation: <https://docs.aws.amazon.com/codedeploy/latest/userguide/integrations-aws-auto-scaling.html>

* 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. (Correcta)**

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.

Explanation: 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 presigned object URL will be valid for a limited period of time and can only be used by the paid subscriber who requested the download.

* 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. (Correcta)**

D. Use an AWS Batch job that is submitted to an AWS Batch job queue.

* A developer is creating AWS CloudFormation templates to manage an application's deployment in Amazon Elastic Container Service (Amazon ECS) through AWS CodeDeploy. The developer wants to automatically deploy new versions of the application to a percentage of users before the new version becomes available for all users.

How should the developer manage the deployment of the new version?

**A. Modify the CloudFormation template to include a Transform section and the AWS::CodeDeploy::BlueGreen hook. (Correcta)**

B. Deploy the new version in a new CloudFormation stack. After testing is complete, update the application's DNS records for the new stack.

C. Run CloudFormation stack updates on the application stack to deploy new application versions when they are available.

D. Create a nested stack for the new version. Include a Transform section and the AWS::CodeDeploy::BlueGreen hook.

* 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". (Correcta)**

C. Set the Origin's HTTP Port to 443.

**D. Set the Viewer Protocol Policy to "HTTPS Only" or "Redirect HTTP to HTTPS". (Correcta)**

E. Enable the CloudFront option Restrict Viewer Access.

Explanation:

B: Setting the Origin Protocol Policy to "HTTPS Only" ensures that CloudFront always uses HTTPS to connect to the origin, which is the web application in this scenario.

D: Setting the Viewer Protocol Policy to "HTTPS Only" ensures that CloudFront will only serve requests over HTTPS. Setting it to "Redirect HTTP to HTTPS" ensures that any HTTP request from viewers is redirected to HTTPS.

* 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. (Correcta)**

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.

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.

* 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. (Correcta)**

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>.

* 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. (Correcta)**

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.

Explanation: If you add annotations with the X-Ray SDK, you can also filter based on the presence of an annotation key or the value of a key. <https://docs.aws.amazon.com/xray/latest/devguide/xray-console-filters.html>

* 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. (Correcta)**

D. Create an Amazon Elastic File System (Amazon EFS) file system to store all the custom libraries.

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.

* 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:



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. (Correcta)**

D. Create a trust relationship between the role and dynamodb.amazonaws.com.

Explanation: <https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-roles/>

* 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. (Correcta)**

* 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. (Correcta)**

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.

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

* 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. (Correcta)**

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.

* 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. (Correcta)**

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.

* 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. (Correcta)**

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.

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.

* 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. (Correcta)**

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.

* 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. (Correcta)**

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.

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

* 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. (Correcta)**

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.

* 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 Xray 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. (Correcta)**

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.

Explanation: To run the X-Ray daemon locally, on-premises, or on other AWS services, download it, run it, and then give it permission to upload segment documents to X-Ray. <https://docs.aws.amazon.com/xray/latest/devguide/xray-daemon.html>