Free Questions for DVA-C02 by vceexamstest

Shared by Sparks on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

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

Options:

A) Hardcode the credentials that are required to access the S3 objects in the application code. Use the credentials to access me required S3 objects.

B) Create a secret access key and access key ID with permission to access the S3 bucket. Store the key and key ID in AWS Secrets Manager. Configure the application to retrieve the Secrets Manager secret and use the credentials to access me S3 objects.

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

D) Create a secret access key and access key ID with permission to access the S3 bucket Store the key and key ID as environment variables m Lambda. Use the environment variables to access the required S3 objects.

Answer:

C

Explanation:

This solution will meet the requirements by creating a Lambda function execution role, which is an IAM role that grants permissions to a Lambda function to access AWS resources such as Amazon S3 objects. The developer can attach a policy to the role that grants access to specific objects in the S3 bucket that are required by the application, following the principle of least privilege. Option A is not optimal because it will hardcode the credentials that are required to access S3 objects in the application code, which is insecure and difficult to maintain. Option B is not optimal because it will create a secret access key and access key ID with permission to access the S3 bucket, which will introduce additional security risks and complexity for storing and managing credentials. Option D is not optimal because it will store the secret access key and access key ID as environment variables in Lambda, which is also insecure and difficult to maintain.

Question 2

Question Type: MultipleChoice

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

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

Options:

A) Hardcode the credentials that are required to access the S3 objects in the application code. Use the credentials to access me required S3 objects.

B) Create a secret access key and access key ID with permission to access the S3 bucket. Store the key and key ID in AWS Secrets Manager. Configure the application to retrieve the Secrets Manager secret and use the credentials to access me S3 objects.

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

D) Create a secret access key and access key ID with permission to access the S3 bucket Store the key and key ID as environment variables m Lambda. Use the environment variables to access the required S3 objects.

Answer:

C

Explanation:

This solution will meet the requirements by creating a Lambda function execution role, which is an IAM role that grants permissions to a Lambda function to access AWS resources such as Amazon S3 objects. The developer can attach a policy to the role that grants access to specific objects in the S3 bucket that are required by the application, following the principle of least privilege. Option A is not optimal because it will hardcode the credentials that are required to access S3 objects in the application code, which is insecure and difficult to maintain. Option B is not optimal because it will create a secret access key and access key ID with permission to access the S3 bucket, which will introduce additional security risks and complexity for storing and managing credentials. Option D is not optimal because it will store the secret access key and access key ID as environment variables in Lambda, which is also insecure and difficult to maintain.