AWS - Lambda secure variables with KMS

This article describes how to use customer KMS (Key Management Store) to encrypt environment variables used in Lambda function.

Examples are based on Python, and describes changes in existing code to allow decrypt variables.

Step-by-step guide

Create Lambda service role with access to KMS. This role needs to be added to KMS policy and be able to save logs in cloud watch.

In Sagepay-logs AWS account this service role is named service-role/lambda-kms. Modify Lambda python code to decrypt variables from KMS

Python Lambda to add

1. Function to decrypt environment variables

   ```
   import boto3
   from base64 import b64decode

   def decryptcreds():
       global DECRYPTED_PASS
       global DECRYPTED_USR
       ENCRYPTED_PASS = os.environ['pwd']
       DECRYPTED_PASS = boto3.client('kms').decrypt(CiphertextBlob=b64decode(ENCRYPTED_PASS))
   ['Plaintext']
       ENCRYPTED_USR = os.environ['usrid']
       DECRYPTED_USR = boto3.client('kms').decrypt(CiphertextBlob=b64decode(ENCRYPTED_USR))['Plaintext']
   ```

2. find lambda handler and add decryption call. Look for the line starting with:

   ```
   def lambda_handler(event, context):
   ```

3. insert decryption function call

   ```
   decryptcreds()
   ```

4. replace existing plain text envrionment variables call

   ```
       usrid = os.environ.get('usrid')

       pwd = os.environ.get('pwd')
   ```

5. with variables decrypted from KMS by decrypt() function

   ```
       usrid = DECRYPTED_USR
       pwd = DECRYPTED_PASS
   ```

Lambda service role with access to KMS

Service role which runs lambda need to have access to KMS. Here is short CLI command to create service role lambda-kms

Example:

```
aws iam create-role --path /service-role/ --role-name lambda-kms --assume-role-policy-document
file://lambdaAssumeRolePolicyDocument.json --description 'Allows Lambda access KMS, Qualys Reports, Sumo,
and AWS services.'
```

Output

```
{


    "Role": {
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Action": "sts:AssumeRole",
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "lambda.amazonaws.com"
                    }
                }
            ]
        },
        "RoleId": "AROAJSCHGKUSR5PHCKB6Q",
        "CreateDate": "2018-12-24T12:15:41Z",
        "RoleName": "lambda-kms",
        "Path": "/service-role/",
        "Arn": "arn:aws:iam::784990508964:role/service-role/lambda-kms"
    }
}
```

lambdaAssumeRolePolicyDocument.json

Below is content of json file used to create lambda-kms service role.

```
{

            "Version": "2012-10-17",

            "Statement": [

                {

                    "Action": "sts:AssumeRole",

                    "Effect": "Allow",

                    "Principal": {

                        "Service": "lambda.amazonaws.com"

                    }

                }

            ]

   }
```

Create new role AWS CLI https://docs.aws.amazon.com/cli/latest/reference/iam/create-role.html

Related articles

- CloudWatch Logs to SumoLogic
- AWS - Lambda secure variables with KMS

- aws - OSSEC Amazon Linux