#### Laboratorio #278

# PROTECCIÓN DE DATOS MEDIANTE CIFRADO

Hecho con amor por:

Ignacio Suárez - Sebastian Aguilera

Joel Umpierrez - Gonza Rondeau

Sabrina Magnani - Agustín Rodriguez







## Objetivos

Crear una clave de encriptación de AWS KMS

Instalar la CLI de AWS Encryption

Cifrar datos de texto simple y descifrarlo

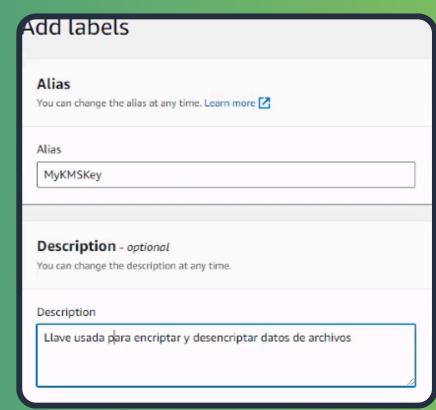
#### Tarea 1: Crear una clave de AWS KMS

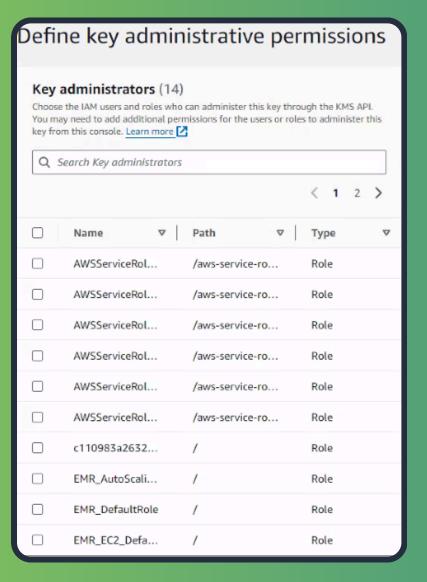
- Crear una clave de encriptación de AWS KMS
- Con AWS KMS, puede crear y administrar claves criptográficas y controlar su uso a lo largo de una amplia variedad de servicios de AWS y en sus aplicaciones.

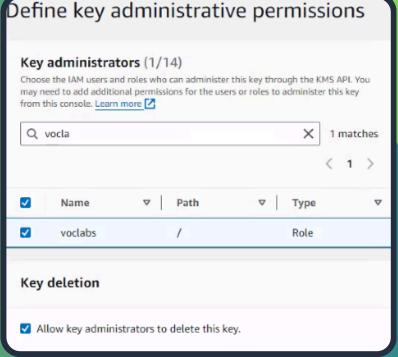
# Key Management X Service (KMS) AWS managed keys Customer managed keys Custom key stores Custom key stores Security, Identity & Compliance AWS Key Management Service

### Accedemos a AWS Key Management Service para crear y configurar una nueva clave de acceso

<ul> <li>Symmetric         A single key used for encrypting and decrypting data or generating an verifying HMAC codes     </li> </ul>	
	d
Asymmetric     A public and private key pair used for encrypting and decrypting data signing and verifying messages	or
ey usage Help me choose 🖸  • Encrypt and decrypt  Use the key only to encrypt and decrypt data.	







Define key usage permissions

Select the IAM users and roles that can use the KMS key in cryptographic operations.

▽ Path

X 1 matches

▼ Type

Role

< 1 >

Key users (1/14)

voclabs

Learn more

Q vocla



Your AWS KMS key was created with alias MyKMSKey and key ID f2a74ab5-9519-4ae9-b56f-519028337deb.

#### Finalmente copiamos el ARN de la clave creada para usarlo luego



# Tarea 2: Configurar la instancia del servidor de archivos

Configuramos las credenciales del servidor de archivos para despues poder cifrar y descifrar los datos.

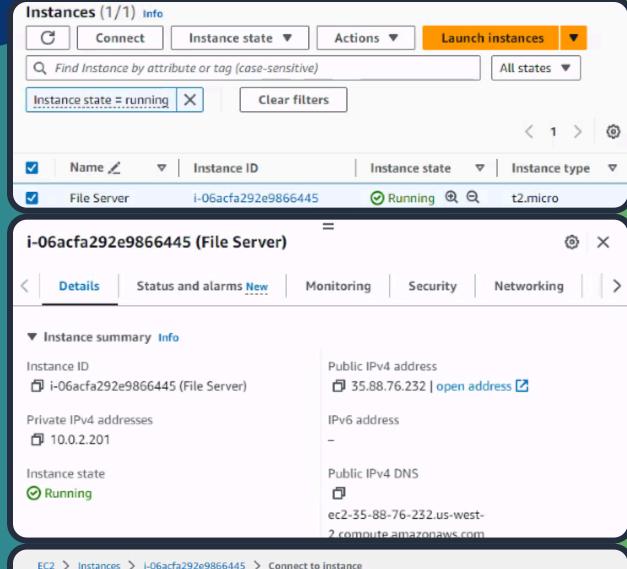
Instalamos la CLI de cifrado de AWS (aws-encrypiton-cli) y asi ejecutar los comandos.

discos compactos ~ configurar aws

vi ~/.aws/credenciales

gato ~/.aws/credentials

pip3 instala aws-encryption-sdk-cli exportar RUTA = \$RUTA :/home/ssm-user/.local/bin



En la lista de Instancias, seleccionamos nuestra instancia para Conectarnos mediante el Session Manager

```
sh-4.2$ cd ~
sh-4.2$ aws configure
AWS Access Key ID [None]: 1
AWS Secret Access Key [None]: 1
Default region name [None]: us-west-2
Default output format [None]:
```

Accedemos a editar con vim las credenciales de AWS

sh-4.2\$ vi ~/.aws/credentials

#### Borramos las credenciales anteriores y pegamos el bloque de codigo que copiamos anteriormente de Vocareum, para luego guardar el archivo con :wq

```
[default]
aws_access_key_id=ASIA2UC273IIH63EZUEC
aws_secret_access_key=nwUP2A16Wr/oMhPQIdyjKd6hYjhecKShros38vsd
aws_session_token=IQoJb3JpZ2luX2VjEEcaCXVZLXdlc3QtMiJHMEUCIQCfdjUn6UQH482+Gsl2yTSZx5hB3JocuYICJj9lcodo8
gIgO3bTPF0hf8cCeHcGDFU9GtZoLqW2Mnzt/+4UeiSFGJIqwwIIsP//////ARAAGgw3MzAzMzUyNzEONDAiDEP5dVOrnoh7SRON
+yqXAvdx9pW6Y0j6IMFPvrdFk21vX4x/VxrTrnpWLa0PXzi6HcI4jbQyj6IwICCrz2fP0Y+00iAVLZ3siucQmDi1Rpc59pvhBDVLHNb
+OMXinw6fKJYA42P6PxcNFeuMANDw6XA8AxOeT1bqTetlVlnTMPL/4eYpSsqOQRf/bcc0lagxsWO3hv5ad4Acl+AHXLZZfij0bjOIxz
4CaddnPE5WNE7g6+jwhAsqyWjycaYe7SPuy+7d8K/s /bc6I5CQCPmJ/2TTwOLyWQjXWjpOS7OfWXfFynzuUIJ0y14N3plt/181avv/
+9kI2yolbkMn3juXDaLwiXKS17rTDaYMtUN6snSMu4fuv5lAmuy5st987kYo7oSRg2kJjjCD65SyBjqdAdjpF7 XnacaY2AV879OgsO
n/D2ZIYUi4cnOHOUTC8KMSvqyGuoixm4XEIf7NQyhfoEWQdtjy4VY+AcL+HIPX5Qj5HhadN/KSVBpjTLxbK1/uVvkPkPzeLrZF1ni06
ASWJ/GoBNITK9mh2ypFyJ4wfqx KS170RyNlAqBKFH31zten8XKeW5KYjoqlidD2zORCWRdiIfz8/A9slBupCos=
```

#### Procedemos a instalar la CLI de AWS Encrpyption y establecemos la ruta de exportación

#### sh-4.2\$ pip3 install aws-encryption-sdk-cli

```
Downloading six-1.16.0-py2.py3-none-any.whl (11 kB)
Installing collected packages: wrapt, pycparser, cffi, cryptography, typing-extensions, zipp, importlib-metadata, attrs, jmespath, urllib3, six, python-dateutil, botocore, s3transfer, boto3, aws-encryption-sdk, base64io, aws-encryption-sdk-cli
WARNING: The script aws-encryption-cli is installed in '/home/ssm-user/.local/bin' which is not on PA
TH.
Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
Successfully installed attrs-23.2.0 aws-encryption-sdk-3.2.0 aws-encryption-sdk-cli-4.1.0 base64io-1.0.
3 boto3-1.33.13 botocore-1.33.13 cffi-1.15.1 cryptography-42.0.7 importlib-metadata-6.7.0 jmespath-1.0.
1 pycparser-2.21 python-dateutil-2.9.0.post0 s3transfer-0.8.2 six-1.16.0 typing-extensions-4.7.1 urllib 3-1.26.18 wrapt-1.16.0 zipp-3.15.0
sh-4.2$ export PATH=$PATH:/home/ssm-user/.local/bin
sh-4.2$
```

#### Tarea 3: Cifrar y descifrar los datos

- En esta tarea, crearemos un archivo de texto con información confidencial ficticia.
- Usaremos el cifrado para asegurar los contenidos del archivo.
- Descifraremos los datos y veremos los contenidos del archivo.

Con el comando touch crearemos tres archivos, estos son los archivos con información confidencial ficticia

```
sh-4.2$ touch secret1.txt secret2.txt secret3.txt
sh-4.2$ echo 'TOP SECRET 1!!!' > secret1.txt
```

Con *echo*, insertamos la información en el archivo "secret1.txt"

```
sh-4.2$ cat secret1.txt
TOP SECRET 1!!!
```

Podemos presenciar que nuestro archivo está en plenas condiciones para ser encriptado

```
sh-4.2$ mkdir output
sh-4.2$ keyArn=arn:aws:kms:us-west-2:730335271440:key/f2a74ab5-9519-4ae9-b56f-519028337deb
```

Crearemos un directorio "output" donde guardaremos las llaves de ARN

Usaremos el comando keyArn para guardar en una variable nuestras llaves

#### Procedemos a ejecutar el siguiente comando para encriptar nuestro mensaje confidencial mediante la clave de encriptación

Como podemos ver, el archivo está encriptado



A continuación procedemos a desencriptar el mensaje anterior para volver a recuperar nuestro mensaje confidencial.

```
sh-4.2$ cat secret1.txt.encrypted.decrypted TOP SECRET 1!!!
```

sh-4.2\$ echo \$? sh-4.2\$ ls output

0 secret1.txt.encrypted





#### Conclusiones

- Creamos correctamente claves de cifrado de AWS KMS.
- Instalamos con éxito la CLI de AWS Encryption.
- Realizamos adecuadamente el cifrado de un texto.
- Realizamos con éxito el descifrado de un texto cifrado.

# Muchas gracias!