

# Lab 278

---

**PROTECCIÓN DE DATOS USANDO CIFRADO.**

Creadores: Fernanda Urman, Felipe Barceló, Sony Etcheverry,  
Agustín Esteche, Juan Sansberro.



# Objetivos

- **CREAR UNA CLAVE DE CIFRADO DE AWS KMS.**
- **INSTALAR LA CLI DE CIFRADO DE AWS.**
- **CIFRAR TEXTO PLANO.**
- **DESCIFRAR EL TEXTO CIFRADO.**

# Tarea 1:

CREAR UNA CLAVE DE AWS KMS

# CREAR UNA CLAVE DE AWS KMS

## Configure key

### Key type [Help me choose](#)

☒ Symmetric  
A single key used for encrypting and decrypting data or generating and verifying HMAC codes

☐ Asymmetric  
A public and private key pair used for encrypting and decrypting data or signing and verifying messages

### Key usage [Help me choose](#)

☒ Encrypt and decrypt  
Use the key only to encrypt and decrypt data.

☐ Generate and verify MAC  
Use the key only to generate and verify hash-based message authentication codes (HMAC).

En la parte de  
aquí  
seleccionamos  
el tipo de llave

Abajo  
seleccionamos  
el uso de la  
clave

Al darle  
siguiente  
configuramos  
el alias y la  
descripción

### Alias

You can change the alias at any time. [Learn more](#)

Alias

MyKMSKey

### Description - optional

You can change the description at any time.

Description

Key used to encrypt and decrypt data files.

### Tags - optional

You can use tags to categorize and identify your KMS keys and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each tag. [Learn more](#)

This key has no tags.

Add tag

You can add up to 50 more tags.

# CREAR UNA CLAVE DE AWS KMS

## Define key administrative permissions

### Key administrators (1/14)

Choose the IAM users and roles who can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this console. [Learn more](#)

Q voclab X 1 matches

< 1 >

<input checked="" type="checkbox"/>	Name	Path	Type
<input checked="" type="checkbox"/>	voclabs	/	Role

### Key deletion

☒ Allow key administrators to delete this key.

Al dar siguiente  
podremos  
administrar los  
permisos de la  
clave.

En este caso  
seleccionamos  
voclab

En la siguiente  
página  
definimos los  
usos de la  
clave. Aquí  
también  
seleccionamos  
voclabs

## Define key usage permissions

### Key users (1/14)

Select the IAM users and roles that can use the KMS key in cryptographic operations. [Learn more](#)

Q vocl X 1 matches

< 1 >

<input checked="" type="checkbox"/>	Name	Path	Type
<input checked="" type="checkbox"/>	voclabs	/	Role

Key users selection voclabs is selected

### Other AWS accounts

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. [Learn more](#)

Add another AWS account

# CREAR UNA CLAVE DE AWS KMS

En esta parte se ve en más detalle la información de la llave

Key configuration

Key type

Symmetric

Key spec

SYMMETRIC\_DEFAULT

Key usage

Encrypt and decrypt

Origin

AWS KMS

Regionality

Single-Region key

You cannot change the key configuration after the key is created.

Alias and description

Alias

MyKMSKey

Description

Key used to encrypt and decrypt data files.

Tags

Key	Value
No data	
No tags to display	

Key policy

To change this policy, return to previous steps or edit the text here.

1

{

2

"Id": "key-consolepolicy-3",

3

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

4

"Statement": [

5

{

6

"Sid": "Enable IAM User Permissions"

7

,"

8

"Effect": "Allow",

9

"Principal": {

10

"AWS": "arn:aws:iam::992382449614:root"

11

},

12

"Action": "kms:\*",

13

"Resource": "\*"

14

},

15

{

16

"Sid": "Allow access for Key Administrators",

17

"Effect": "Allow",

18

"Principal": {

19

"AWS": "arn:aws:iam::992382449614:role/voclabs"

20

},

"Action": [

# Tarea 2:

CONFIGURAR LA INSTANCIA DE SERVIDOR DE ARCHIVO

# CONFIGURAR LA INSTANCIA DE SERVIDOR DE ARCHIVO

Instances (1/1) <a href="#">Info</a>					<a href="#">Refresh</a>	<a href="#">Connect</a>	Instance state ▾	
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/>					All states ▾			
<input checked="" type="checkbox"/>	Name <a href="#">✎</a> ▾	Instance ID	Instance state ▾	Instance type ▾	Status check			
<input checked="" type="checkbox"/>	File Server	i-0bc1d1feefc5a	Running	t2.micro	2/2 checks passed			

Seleccionamos la instancia FileServer y nos conectamos a la misma

```
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]:
sh-4.2$
```

Nos conectamos a Session Manager, allí cambiaremos de directorio principal y crearemos un archivo de credenciales de AWS. Luego lo ajustaremos.

```
[Fault]
access_key_id=ASIA6ODU2O7HKW5G24GW
secret_access_key=KZfUZ+zAtf2w8ZaQS1eXZWpQPeOy6GF6QAnRp7vM
session_token=IQoJb3JpZ21uX2VjEEcaCXVzLXdlc3QtMiJIMEYCIQDqpcY1+mC4OWbxgZ103tD/+uGuuA8Ms0AXE9HkVdN45gIhAMCGIJinEsY90ZQQcHmEMW
4UcvpnHSrVsoXcIGKroCCLD////////wEQABoMOTkyMzgyNDQ5NjE0Igz58OhBhwEbXYzgXP8qjgJRzTeWvYTGng6ulUNfaDmO+wlXi+hEu6w7EYWsrubaN7ezZ
0JA79atJEODKyRrW7d4EAckj+LLOSXqO6pcsEnWKRxvXUjp26XhqPUCnYFDQHT3NsdmcXNw6v17AA2B1TdlM2/QERoonaWIfD81ggy6JXWtsznreo9VOOhhvoDT5
NlrNkbtuaQummRn8xMcGQs+vGvQTADYIPMGfUy224XOVk42ugnfhmO/22knTefdBEEAis2DFC2285g+elBiB6JG5BpkgkXQzeDKWW53oaGq2p19jQkVIZJv9D341I
W7BURgqp6ukuzL3jOzC5/xh1eCxSx2Oc6ee1Rng0HYgeeMwu/6UsgY6nAHHwU5UULnZ/NANbYpnPw6rv+rhNIRF9W1iQDZG/YUBntfqx1dSYVMd9HsRuYk3Q2GCIA
fdTxWz3XhLbAG7VhRnx9g4x+u+9kVHe/IgwWUOLyM1yO5Pr5XhS59qiZMdfnF1ViUpagzd2Zf1UXE66CeNxH4SGUBCwOO7LWFXLcl0NkSFEU45za/1P+8mYqtIlc3
```



# CONFIGURAR LA INSTANCIA DE SERVIDOR DE ARCHIVO

```
sh-4.2$ cat ~/.aws/credentials
[default]
aws_access_key_id=ASIA6ODU2O7HKW5G24GW
aws_secret_access_key=KZfUZ+zAtf2w8ZaQSleXZWpQPeOy6GF6QAnRp7vM
aws_session_token=IQoJb3JpZ2luX2VjEEcaCXVzLXdlc3QtMiJIMEYCIQDqpcY1+mC4OWbxgZ103tD/+uGuuA8Ms0AXE9HkVdN45gIhAMCGIJinEsY90ZQQcHmEMW2iQ
sOAMUcvpnHSrVsoXcIGKroCCLD////////wEQABoMOTkyMzgyNDQ5NjE0Igz58OhBhwEbXYzgXP8qjgJRzTeWvYTGng6ulUNfaDmO+wlXi+hEu6w7EYWsruBaN7ezZCdT
8ZS0JA79atJEODKyRrW7d4EAckj+LLOSXqO6pcsEnWKRxvXUjp26XhqPUCnYFDQHT3NsdmcXNw6v17AA2B1TdlM2/QERoonaWIfD81ggy6JXWtsznreo9VOOhhvoDT5Zir
d5iNlrNkbtuaQummRn8xMcGQs+vGvQTADYIPMGfUy224XOVk42ugnfhmO/22knTefdBEEAiS2DFC2285g+elBiB6JG5BpkgkXQzeDKWW53oaGq2p19jQkVIZJv9D341INMg
ZyMW7BURgqp6ukuzL3jOzC5/xhleCxSx2Oc6ee1Rng0HYgeeMwu/6UsgY6nAHHwU5UULnZ/NANbYpnPw6rv+rhNIRF9W1iQDZG/YUBntfqlsYVMD9HsRuYk3QZGCia+7o
lN6FdTxWz3XhLbAG7VhRnx9g4x+u+9kVHe/IgwWUOLyMlyO5Pr5XhS59qiZMdfnF1ViUpagzd2Zf1UXE66CeNxH4SGUBCwOO7LWFXLcl0NkSFEU45za/1P+8mYqtIlc36Nw
82iGdXI=
sh-4.2$ pip3 install aws-encryption-sdk-cli
```

Para poder ver el contenido actualizado del archivo usamos el comando ***cat ~/.aws/credentials***

```
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-1.3
3.13 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 urllib3-1.26.18 wrapt-1.16.0 zipp-3.15.0
sh-4.2$ export PATH=$PATH:/home/ssm-user/.local/bin
```

Y para instalar la CLI de AWS Encryption y establecer su ruta usamos el comando ***pip3 install aws-encryption-sdk-cli***

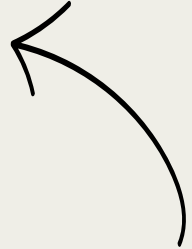
# Tarea 3:

## CIFRAR Y DESCIFRAR DATOS

# CIFRAR Y DESCIFRAR DATOS


---

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



Con el comando ***touch*** creamos esos 3 archivos  
Y luego con ***echo*** muestra que el archivo esta encriptado al ver su contenido

```
sh-4.2$ mkdir output
sh-4.2$ keyArn=(arn:aws:kms:us-west-2:992382449614:key/43b8929e-5523-4849-86e3-4bebd2ec42b4)
```





Crearemos un directorio llamado ***output*** con *mkdir output*.  
Con ***nano***, ingresamos ***keyArn=(ARN de KMS)*** para definir la clave de acceso a recursos de AWS Key Management Service que se usará para el cifrado.

# CIFRAR Y DESCIFRAR DATOS

---

```
sh-4.2$ aws-encryption-cli --encrypt \  
> --input secret1.txt \  
> --wrapping-keys key=$keyArn \  
> --metadata-output ~/metadata \  
> --encryption-context purpose=test \  
> --commitment-policy require-encrypt-require-decrypt \  
> --output ~/output/.  
sh-4.2$
```

Luego para encriptar el archivo **secret1.txt** ingresamos el código de la imagen de la izquierda.



```
sh-4.2$ echo $?  
0  
sh-4.2$ ls output  
secret1.txt.encrypted  
sh-4.2$
```


Y ahora usaremos el comando **echo \$?** para poder determinar si el comando funciona.

Luego para ver la ubicación del archivo que ciframos utilizamos el comando **ls output**.

# CIFRAR Y DESCIFRAR DATOS

---

Visualizamos los contenidos del archivo encriptado colocando los comandos ***cd output*** y ***cat secret1.txt.encrypted***.



```
sh-4.2$ cd output
sh-4.2$ cat secret1.txt.encrypted
aws-crypto-public-keyDAogJ08btp7+6WFgCfl8ITULwIFguWX9caTm9ixxWU802firBmfDS1PaD832B0Vpqw==purposetestaws-kmsKarn:aws:kms
0o0m0hst`He.0382449614:key/43b8929e-5523-4849-86e3-4bebd2ec42b4x(5-d8[EwZ9x3]>](([[]>0|*H
F[];Ga7I<y_
g[]L[][xI[]w[]1[4^[]A[]nv[]]"[]t[]BU[]2N[]w]/[]([[]WA6[]nz5[]5[]kg$[]hy[]u[]T3
&
nd[] []g0e1[]^g[]K[]i[]5/[]k[] []}[]zF[]owd[]l[]Mp[]q9j[]K4[]b[] []#.x([]b)[]=[]sPHsh-4.2$
```

# CIFRAR Y DESCIFRAR DATOS

---

```
sh-4.2$ aws-encryption-cli --decrypt \  
> --input secret1.txt.encrypted \  
> --wrapping-keys key=$keyArn \  
> --commitment-policy require-encrypt-require-decrypt \  
> --encryption-context purpose=test \  
> --metadata-output ~/metadata \  
> --max-encrypted-data-keys 1 \  
> --buffer \  
> --output .  
sh-4.2$
```

Desencryptamos el archivo  
colocando el comando en pantalla.

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

Luego vemos su nueva ubicación, notando  
que el archivo  
***secret1.txt.encrypted.decrypted*** contiene el  
contenido descifrado del archivo  
***secret1.txt.encrypted***.

Vemos el contenido del archivo encriptado ***secret1.txt*** usando  
el comando ***cat***.

# ¡Muchas gracias!

---