Security: Create a Vault and Encryption Key and Perform Encryption/Decryption of Data

Lab 19-1 Practices

Get Started

Overview

OCI Vault is a cloud native service that allows customers to securely store and manage their master encryption keys and configuration information. The OCI Vault service supports several key encryption algorithms such as the Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and the Elliptic Curve Digital Signature Algorithm (ECDSA).

This lab enables you to encrypt or decrypt sensitive information (such as credit card details, salary information, and so on) by using the master encryption key stored in OCI Vault.

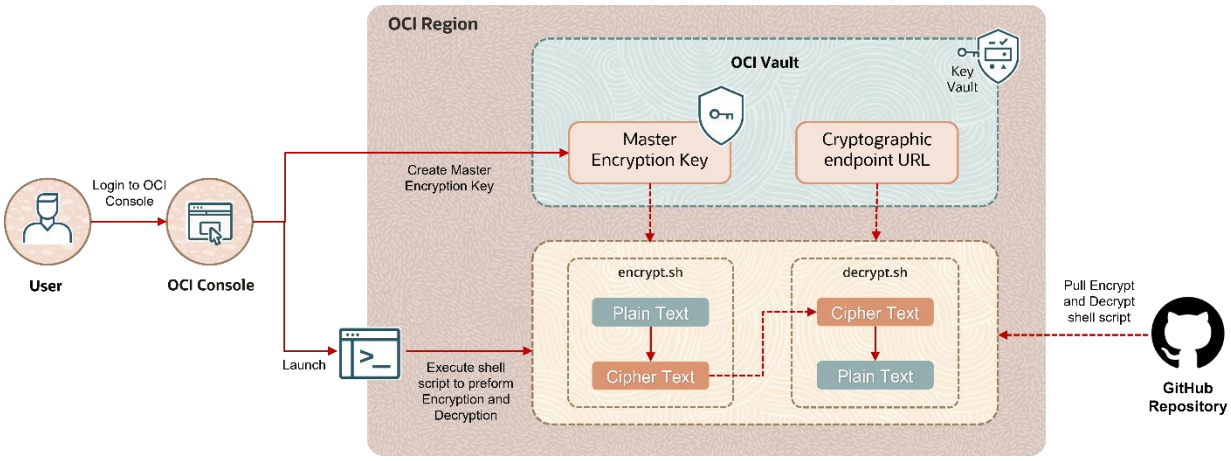
In this lab, you'll:

a. Create a Vault and a master encryption key

b. Perform basic encryption and decryption by using the master encryption key

Prerequisites

- URL of a precreated encryption script located at a predetermined location git
- URL of a precreated decryption script located at a predetermined location git



Create a Vault and a Master Encryption Key

You'll create a Vault and a master encryption key required to perform cryptographic operations.

Tasks

1. Log in to the Oracle Cloud Infrastructure (OCI) console.
2. From the Main Menu, select **Identity & Security,** and then click **Vault**.
3. Click **Create Vault.**
4. In the Create Vault dialog box, provide the following details:
    a. **Create in Compartment:** Select your <*compartment_name*>
    b. **Name:** ARCHITECT-ASS-VAULT
    c. **Do not check the** "Make it a virtual private vault" option.
5. Click **Create Vault.**

   It will take about a minute to create the vault. The vault will go through the **Creating** state to the **Active** state.
6. Select **ARCHITECT-ASS-VAULT** from the list of vaults in the root compartment.
7. Locate the **Cryptographic Endpoint** URL on the Vault Information tab. Copy the URL to your clipboard and save it somewhere to use later during encryption process.
    a. Example: https://xxxxxx-crypto.kms.eu-frankfurt-1.oraclecloud.com
8. From the left navigation pane under **Resources**, click **Master Encryption Keys**, and then click **Create Key**.
9. In the Create Key dialog box, enter the following values for your key:
    a. **Create in Compartment:** <Select your *compartment*>
    b. **Protection Mode:** HSM
    c. **Name:** FRA-AA-LAB19-VK-01
    d. Leave everything else to default values and click **Create Key**. It will take about a minute to create the master encryption key. The keys will go through the **Creating** state to the **Enabled** state.
10. Select your compartment from the **Compartment** drop-down list in the left column under List Scope. To the right, you will see the key that you created. Click your Master Encrypted Key.
11. On the Key Details page, locate the OCID value on the Key Information tab. Click the **Copy** link located to the right of the OCID value. Save the OCID value somewhere to use later during the encryption process.

    Sample: ocid1.key.oc1.xxx.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Perform Encryption

You will now run the provided shell script, which will take as input the OCI Vault cryptographic endpoint, the OCID of the master encryption key you created, and plain text to encrypt. The provided shell script invokes `oci kms crypto encrypt` to perform data encryption.

Tasks

1. Click the **Cloud Shell** icon in the Console header to launch your Cloud Shell.
   a. Go to your home directory.
      ```
      $ cd ~
      ```
   b. Get the shell script to encrypt the plain text.
      ```
      $ wget https://raw.githubusercontent.com/ou-developers/oci-vaultoperations/main/ocivault-encrypt.sh
      ```
   c. Make the downloaded shell script executable.
      ```
      $ chmod +x ocivault-encrypt.sh
      ```
   d. Run the shell script.
      ```
      $ ./ocivault-encrypt.sh
      ```

   Note: This command will execute the downloaded interactive script, which will prompt you for the following values. When prompted, locate, and enter the values that you saved in the previous section.
2. Provide the required parameters as input.
   a. **`Please enter the OCI Vault Cryptographic Endpoint URL`**

      < *OCI Vault Cryptographic Endpoint URL*>

      Example: https://xxxxxx-crypto.kms.eu-frankfurt-1.oraclecloud.com
   b. **`Please enter your Master Encryption Key OCID`**

      < *Master Encryption Key OCID*>

      Example: ocid1.key.oc1.xxx.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

c. **Please enter the text you wish to encrypt**

<Plain text to be encrypted>

Example: HelloWorld

3. The Shell script will invoke `oci kms crypto encrypt` and perform a cryptographic operation. The following is a sample output of the script:

```
Please enter the OCI Vault Cryptographic Endpoint URL
https://xxxx-crypto.kms.eu-frankfurt-1.oraclecloud.com
Please enter your Master Encryption Key OCID
ocid1.key.oc1.xxx.xxxxxxxxxxxxxxxxxxxxxxxxx
Please enter the text you wish to encrypt
HelloWorld
{
"data": {
    "ciphertext":
"QRu3Y6UBExxxxxaSCNyAKuhqRsxxxxxuk/shqzs4iimhWgyyAA==",
    "encryption-algorithm": "AES_256_GCM",
    "key-id": "ocid1.key.oc1.xxx.xxxxxxxxxxbbbbbbbbbxxxx",
    "key-version-id": "ocid1.keyversion.oc1.xxx.aaaabbbbb"
  }
}
---------- Encrypted Text ----------
QYcEncB2aSYnAC7QkpXd589LxN8XdddFWJzHyFg2gTKCaCcht97rAAAA==
```

4. Copy and save the **Encrypted Text** somewhere to use later during the decryption process.

Perform Decryption

You will now run the provided shell script, which will take as input the OCI Vault cryptographic endpoint, the OCID of the master encryption key you created, and the encrypted text to decrypt. The provided shell script invokes `oci kms crypto decrypt` to perform data decryption.

Tasks

1. Click the **Cloud Shell** icon in the Console header to launch your Cloud Shell.
   a. Go to your home directory.
      ```
      $ cd ~
      ```
   b. Get the shell script to decrypt the encrypted text.
      ```
      $ wget https://raw.githubusercontent.com/ou-developers/oci-vaultoperations/main/ocivault-decrypt.sh
      ```
   c. Make the downloaded shell script executable.
      ```
      $ chmod +x ocivault-decrypt.sh
      ```
   d. Run the shell script.
      ```
      $ ./ocivault-decrypt.sh
      ```
2. Provide the required parameters as input.
   a. **Please enter the OCI Vault Cryptographic Endpoint URL**

      < *OCI Vault Cryptographic Endpoint URL*>

      Example: https://xxxxxx-crypto.kms.eu-frankfurt-1.oraclecloud.com
   b. **Please enter your Master Encryption Key OCID**

      < *Master Encryption Key OCID*>

      Example: ocid1.key.oc1.xxx.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

      ```
      ocid1.key.oc1.xxx.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
      ```
   c. **Please enter the Encrypted Text (Generated Above)**

      ```
      <Encrypted_Text_from_above_step>
      Example:
      QYcEncB2aSYnAC7QkpXd589LxN8XdddFWJzHyFg2gTKCaCcht97rAAAA==
      ```
3. The Shell script will invoke `oci kms crypto decrypt` and perform a cryptographic operation. The following is a sample output of the script:

   ```
   Please enter the OCI Vault Cryptographic Endpoint URL
   https://xxxx-crypto.kms.eu-frankfurt-1.oraclecloud.com
   Please enter your Master Encryption Key OCID
   ocid1.key.oc1.xxx.xxxxxxxxxxxxxxxxxxxxxxxxx
   Please enter the Encrypted Text (Generated Above)
   QYcEncB2aSYnAC7QkpXd589LxN8XdddFWJzHyFg2gTKCaCcht97rAAAA==

   {
   "data": {
   ```

```
          ....
    "key-id": "ocid1.key.oc1.xxx.xxxxxxxxxxbbbbbbbbbxxxx",
    "key-version-id": "ocid1.keyversion.oc1.xxx.aaaabbbbb"
     "plaintext": "ampqanNzc3NzCg==",
"plaintext-checksum": "2060560141"
  }
}
---------- Plain Text ----------
HelloWorld
--------------------------------
```