Contents

[**Giai đoạn 3: Bảo mật tài nguyên AWS bằng cách sử dụng AWS KMS** 3](#_Toc202378005)

[**Nhiệm vụ 3.1: Tạo khóa do khách hàng quản lý và cấu hình luân chuyển khóa** 3](#_Toc202378006)

[**Bước 1: Truy cập KMS trong AWS Console** 3](#_Toc202378007)

[**Bước 2: Tạo Customer Managed Key** 3](#_Toc202378008)

[**Bước 3: Chọn type key** 3](#_Toc202378009)

[**Bước 4: Add label** 3](#_Toc202378010)

[**Bước 5: Cấu hình quyền truy cập khóa** 4](#_Toc202378011)

[**Bước 6: Xác nhận và tạo khóa** 4](#_Toc202378012)

[**Bước 7: Bật xoay vòng khóa (Key rotation)** 5](#_Toc202378013)

[**Nhiệm vụ 3.2: Cập nhật chính sách khóa AWS KMS và phân tích chính sách IAM** 6](#_Toc202378014)

[**Bước 1: Mở AWS Management Console.** 6](#_Toc202378015)

[**Bước 2: Vào AWS Key Management Service (KMS).** 6](#_Toc202378016)

[**Bước 3: Tìm và chọn khóa MyKMSKey.** 6](#_Toc202378017)

[**Bước 4: Vào tab "Key policy"** 6](#_Toc202378018)

[**Bước 5: Tìm phần có "Sid": "Allow use of the key".** 6](#_Toc202378019)

[**Bước 6: Chỉnh phần Principal** 6](#_Toc202378020)

[**Bước 7: Nhấn Save changes**. 9](#_Toc202378021)

[**Nhiệm vụ 3.3: Sử dụng AWS KMS để mã hóa dữ liệu trong Amazon S3** 9](#_Toc202378022)

[**Bước 1: Cập nhật mã hóa SSE-KMS cho bucket data-bucket** 9](#_Toc202378023)

[**Bước 2: Tạo file loan-data.csv trên máy tính** 10](#_Toc202378024)

[**Bước 3: Đăng nhập với IAM user sofia (trong cửa sổ ẩn danh)** 10](#_Toc202378025)

[**Bước 4: Phân tích mã hóa của object loan-data.csv** 12](#_Toc202378026)

[**Bước 5: Kiểm tra quyền truy cập với user sofia** 12](#_Toc202378027)

[**Bước 6: Kiểm tra quyền truy cập với user paulo** 13](#_Toc202378028)

[**Nhiệm vụ 3.4: Sử dụng AWS KMS để mã hóa ổ đĩa gốc của phiên bản EC2** 13](#_Toc202378029)

[**Bước 1: Tạo EC2 instance mới** 13](#_Toc202378030)

[**Bước 2: Cấu hình cơ bản** 13](#_Toc202378031)

[**Bước 3: Cấu hình mạng** 14](#_Toc202378032)

[**Bước 4: Cấu hình ổ đĩa (storage)** 15](#_Toc202378033)

[**Bước 5: Advanced details** 16](#_Toc202378034)

[**Bước 6: Khởi chạy Instance** 16](#_Toc202378035)

[**Bước 7: Xác minh mã hóa ổ đĩa** 17](#_Toc202378036)

[**Nhiệm vụ 3.5: Sử dụng mã hóa phong bì AWS KMS để mã hóa dữ liệu tại chỗ** 17](#_Toc202378037)

[**Bước 1: Kết nối với WebServer2** 17](#_Toc202378038)

[**Bước 2: Tạo file cần mã hóa** 17](#_Toc202378039)

[**Bước 3: Kiểm tra quyền truy cập AWS KMS** 17](#_Toc202378040)

[**Bước 4: Tạo Data Key từ KMS Key** 18](#_Toc202378041)

[**Bước 5: Lưu khóa mã hóa (CiphertextBlob) ra file** 18](#_Toc202378042)

[**Bước 6: Giải mã để lấy khóa dữ liệu gốc (Plaintext)** 18](#_Toc202378043)

[**Bước 7: Mã hóa dữ liệu** 19](#_Toc202378044)

[**Bước 8: Xóa file gốc chưa mã hóa** 19](#_Toc202378045)

[**Bước 9: Giải mã file đã mã hóa** 19](#_Toc202378046)

[**Nhiệm vụ 3.6: Sử dụng AWS KMS để mã hóa bí mật Secrets Manager** 19](#_Toc202378047)

[**Bước 1: Tạo secret trong Secrets Manager** 19](#_Toc202378048)

[**Bước 2: Truy xuất bí mật bằng AWS CLI** 20](#_Toc202378049)

# **Giai đoạn 3: Bảo mật tài nguyên AWS bằng cách sử dụng AWS KMS**

Bộ phận pháp lý tại AnyCompany Financial đã nhận được thông báo từ Tổng công ty Bảo hiểm Tiền gửi Liên bang Hoa Kỳ (FDIC) rằng công ty cần mã hóa thông tin nhạy cảm, chẳng hạn như PII, số thẻ tín dụng và số an sinh xã hội. Bộ phận pháp lý đã liên hệ với người quản lý của bạn, giám đốc CNTT và họ giao cho bạn nhiệm vụ triển khai mã hóa và mã hóa để đáp ứng các tiêu chuẩn tuân thủ quy định.

Cụ thể, công ty muốn thực hiện những điều sau:

Triển khai cơ chế để tạo và quản lý khóa do khách hàng quản lý AWS KMS.

Sử dụng giải pháp khóa được quản lý để mã hóa dữ liệu được lưu trữ trong Amazon S3 và trên ổ đĩa gốc EBS của phiên bản EC2.

Sử dụng khóa do khách hàng quản lý để mã hóa các bí mật được lưu trữ trong Secrets Manager.

Đến cuối giai đoạn này, bạn sẽ tạo được kiến ​​trúc được hiển thị trong sơ đồ sau.

## **Nhiệm vụ 3.1: Tạo khóa do khách hàng quản lý và cấu hình luân chuyển khóa**

### **Bước 1: Truy cập KMS trong AWS Console**

1. Đăng nhập vào [AWS Management Console](https://console.aws.amazon.com).
2. Ở thanh tìm kiếm trên đầu, gõ **KMS** rồi chọn **Key Management Service**.

### **Bước 2: Tạo Customer Managed Key**

1. Trong menu bên trái, chọn **Customer managed keys**.
2. Bấm **Create key**.

### **Bước 3: Chọn type key**

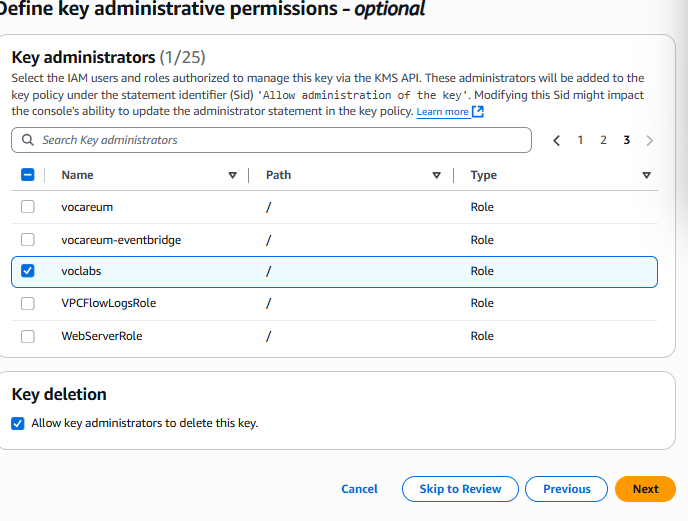
1. Chọn **Symmetric** (khóa đối xứng – dùng cho mã hóa và giải mã).
2. Chọn **Encrypt and decrypt**.
3. Bấm **Next**.

### **Bước 4: Add label**

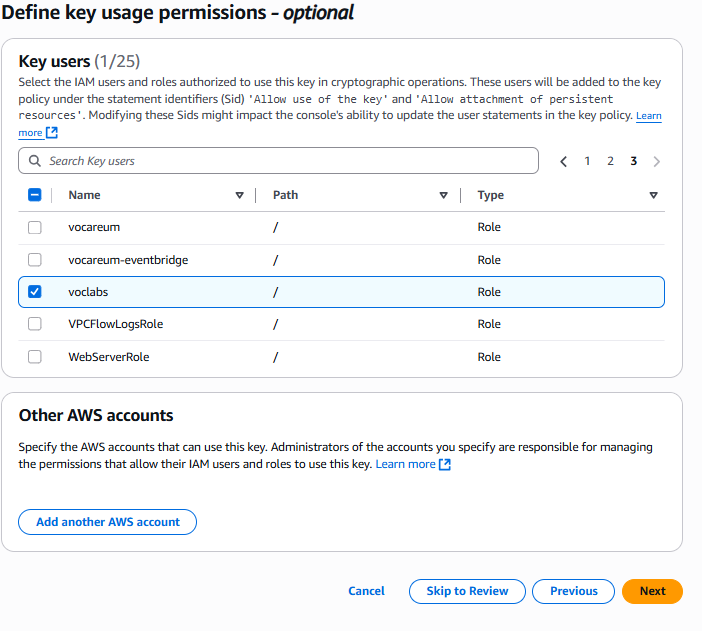
1. Trong phần **Alias**, nhập ***MyKMSKey***
2. Mô tả (Description): bạn có thể để trống hoặc nhập gì đó tùy thích.
3. Bấm **Next**.

### **Bước 5: Cấu hình quyền truy cập khóa**

1. **Key administrators**: Bấm **Add** và chọn vai trò **voclabs**.



1. **Key users**: Bấm **Add** và chọn **voclabs** **(lần nữa)**.



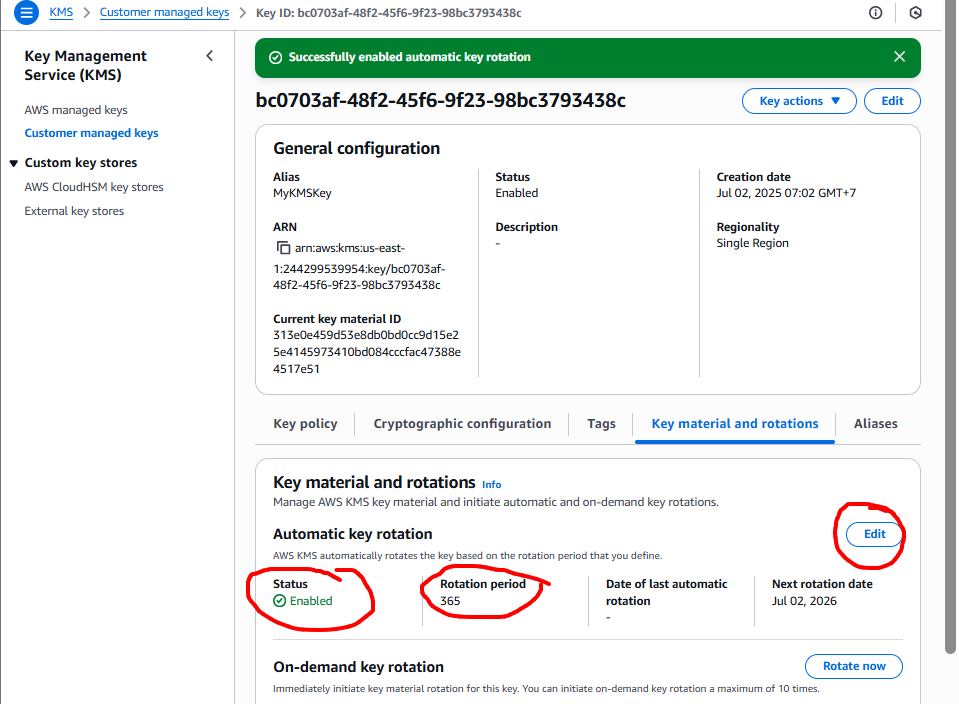
1. Các phần khác giữ nguyên mặc định.
2. Bấm **Next**.

### **Bước 6: Xác nhận và tạo khóa**

1. Kiểm tra lại thông tin.
2. Bấm **Finish** hoặc **Create key**.

### **Bước 7: Bật xoay vòng khóa (Key rotation)**

1. Sau khi tạo xong, bạn sẽ thấy danh sách khóa. Tìm đến khóa có alias là **MyKMSKey**.
2. Click vào tên khóa đó để vào trang chi tiết.
3. Ở phần **Key rotation**, bật tùy chọn **Enable automatic key rotation**.



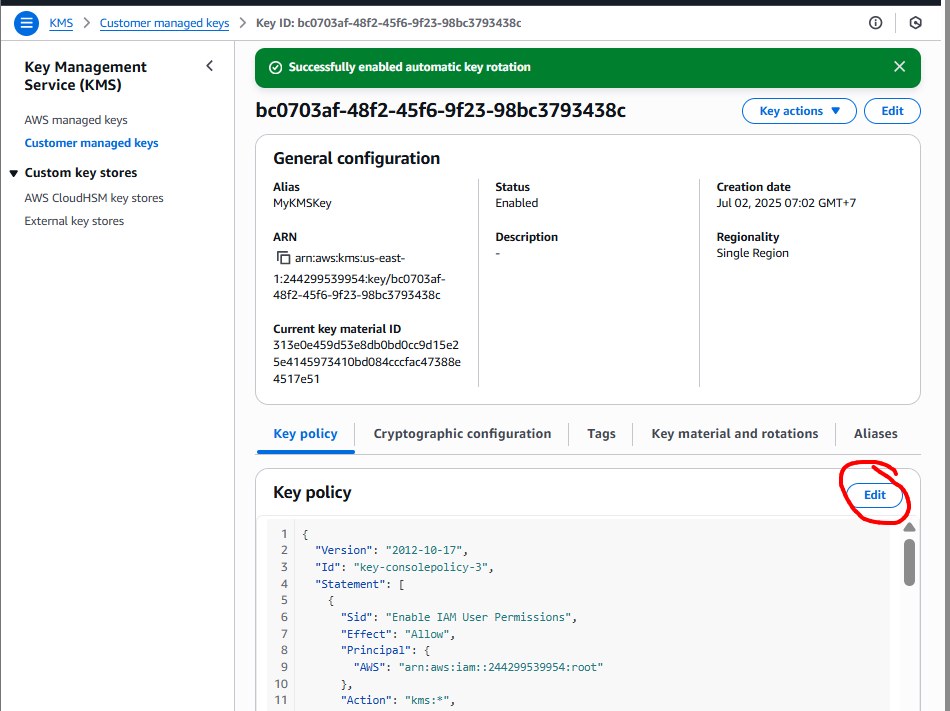
## **Nhiệm vụ 3.2: Cập nhật chính sách khóa AWS KMS và phân tích chính sách IAM**

### **Bước 1: Mở AWS Management Console.**

### **Bước 2: Vào AWS Key Management Service (KMS).**

### **Bước 3: Tìm và chọn khóa MyKMSKey.**

### **Bước 4: Vào tab "Key policy"**



### **Bước 5: Tìm phần có "Sid": "Allow use of the key".**

### **Bước 6: Chỉnh phần Principal**

Trong phần "Principal": {}, chỉnh sửa dòng "AWS" thành như sau (thay ACCOUNT-NUMBER bằng số tài khoản thực tế của bạn):

***"AWS": [***

***"arn:aws:iam::ACCOUNT-NUMBER:role/voclabs",***

***"arn:aws:iam::ACCOUNT-NUMBER:user/sofia"***

***]***

**Code hoàn chỉnh ví dụ nhưu với id của tôi**

***{***

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

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

***"Statement": [***

***{***

***"Sid": "Enable IAM User Permissions",***

***"Effect": "Allow",***

***"Principal": {***

***"AWS": "arn:aws:iam::244299539954:root"***

***},***

***"Action": "kms:\*",***

***"Resource": "\*"***

***},***

***{***

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

***"Effect": "Allow",***

***"Principal": {***

***"AWS": "arn:aws:iam::244299539954:role/voclabs"***

***},***

***"Action": [***

***"kms:Create\*",***

***"kms:Describe\*",***

***"kms:Enable\*",***

***"kms:List\*",***

***"kms:Put\*",***

***"kms:Update\*",***

***"kms:Revoke\*",***

***"kms:Disable\*",***

***"kms:Get\*",***

***"kms:Delete\*",***

***"kms:TagResource",***

***"kms:UntagResource",***

***"kms:ScheduleKeyDeletion",***

***"kms:CancelKeyDeletion",***

***"kms:RotateKeyOnDemand"***

***],***

***"Resource": "\*"***

***},***

***{***

***"Sid": "Allow use of the key",***

***"Effect": "Allow",***

***"Principal": {***

***"AWS": [***

***"arn:aws:iam::244299539954:role/voclabs",***

***"arn:aws:iam::244299539954:user/sofia"***

***]***

***},***

***"Action": [***

***"kms:Encrypt",***

***"kms:Decrypt",***

***"kms:ReEncrypt\*",***

***"kms:GenerateDataKey\*",***

***"kms:DescribeKey"***

***],***

***"Resource": "\*"***

***},***

***{***

***"Sid": "Allow attachment of persistent resources",***

***"Effect": "Allow",***

***"Principal": {***

***"AWS": "arn:aws:iam::244299539954:role/voclabs"***

***},***

***"Action": [***

***"kms:CreateGrant",***

***"kms:ListGrants",***

***"kms:RevokeGrant"***

***],***

***"Resource": "\*",***

***"Condition": {***

***"Bool": {***

***"kms:GrantIsForAWSResource": "true"***

***}***

***}***

***}***

***]***

***}***

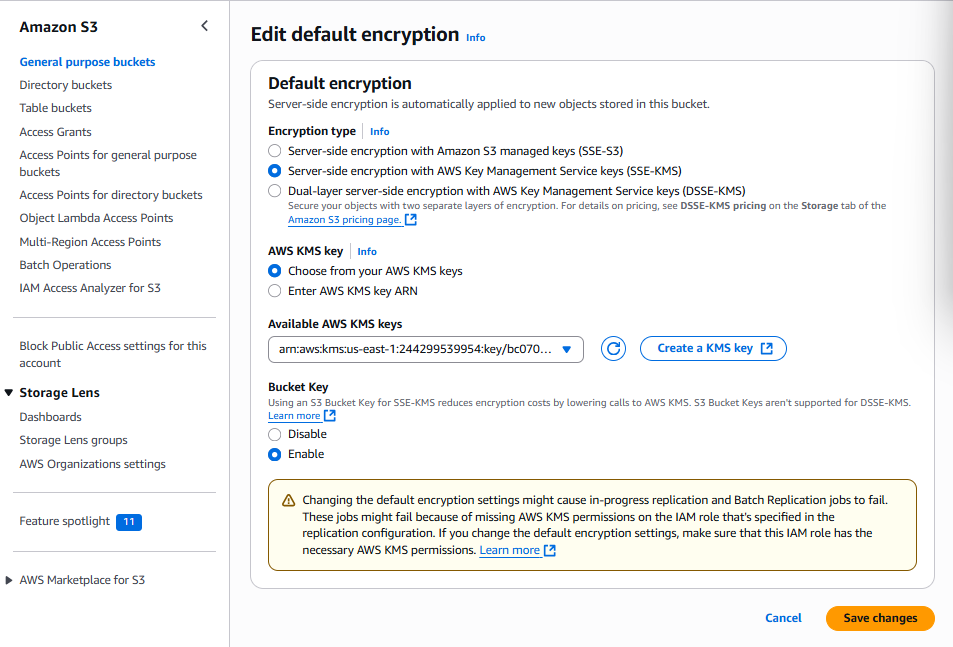
✅ Lưu ý: Giữ nguyên các phần khác của policy. Bạn chỉ **chỉnh sửa mảng AWS Principal**.

### **Bước 7: Nhấn Save changes**.

## **Nhiệm vụ 3.3: Sử dụng AWS KMS để mã hóa dữ liệu trong Amazon S3**

### **Bước 1: Cập nhật mã hóa SSE-KMS cho bucket data-bucket**

1. Vào AWS Management Console với user voclabs (hoặc role tương đương có quyền quản trị).
2. Truy cập **S3** → chọn bucket **data-bucket**. Đã tạo ở bước task 1.1
3. Chọn tab **Properties**.
4. Cuộn xuống phần **Default encryption**.-> **Edit**
5. Bật tuỳ chọn:
   * **Enable** encryption
   * Chọn **AWS Key Management Service key (SSE-KMS)**
   * Chọn key KMS mà bạn đã tạo ở Task 3.1



1. Bấm **Save changes**.

### **Bước 2: Tạo file loan-data.csv trên máy tính**

Dùng notepad

***date,description,amount,principal,interest***

***2023-01-14,payment,1000.00,845.52,154.48***

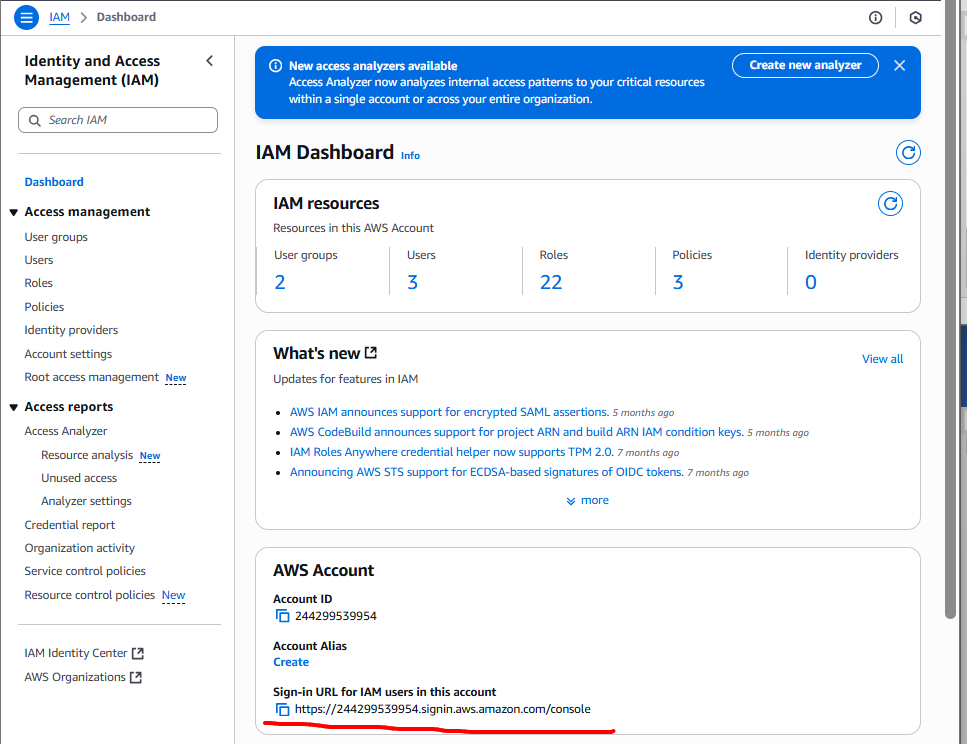
***2022-12-22,payment,1021.52,742.80,278.72***

***2022-11-15,payment,1000.00,855.27,144.73***

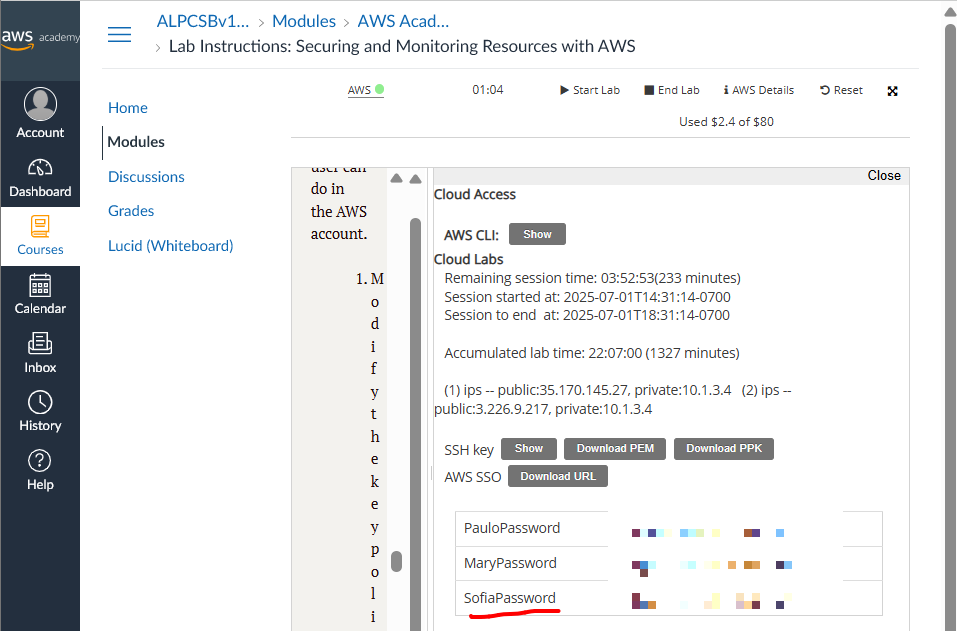
Lưu file lại.

### **Bước 3: Đăng nhập với IAM user sofia (trong cửa sổ ẩn danh)**

1. Mở trình duyệt **Incognito / Private**.
2. Truy cập vào liên kết IAM sign-in mà bạn có được từ mục **AWS Details**.



1. Đăng nhập bằng IAM user sofia (password trong phần hướng dẫn bài lab).

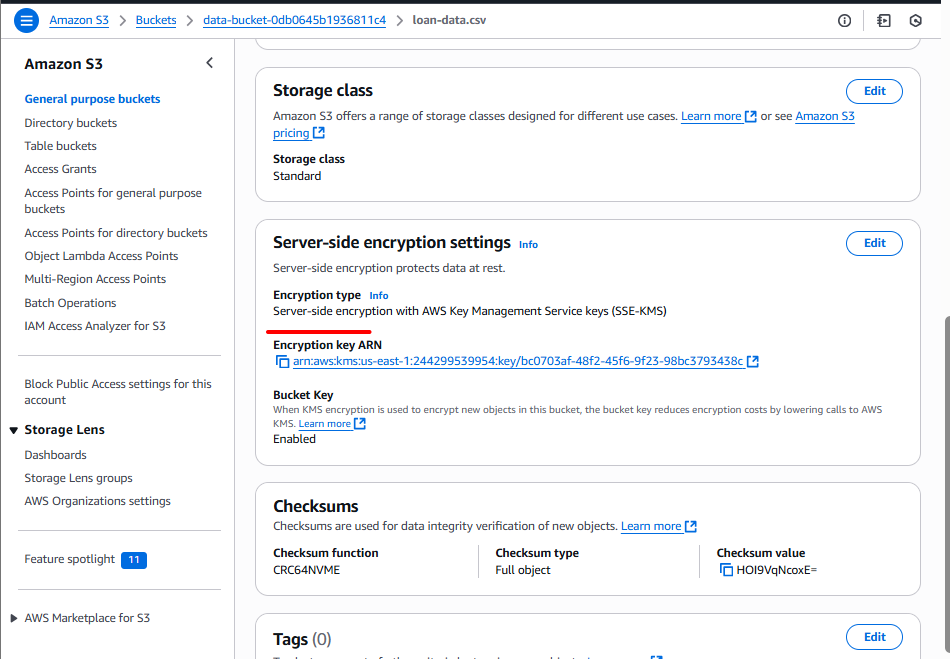


1. Vào S3 → tìm đến bucket **data-bucket** → **upload** file loan-data.csv.
2. Kiểm tra lại: upload thành công nghĩa là sofia có quyền sử dụng bucket **và** key KMS.

### **Bước 4: Phân tích mã hóa của object loan-data.csv**

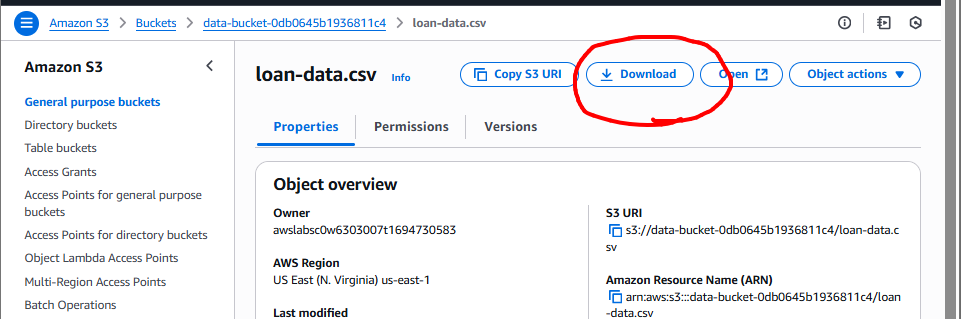
* Sau khi upload, click vào file loan-data.csv.
* Tìm phần **Encryption**.
* Xác nhận có dòng:

Encryption: **SSE-KMS**



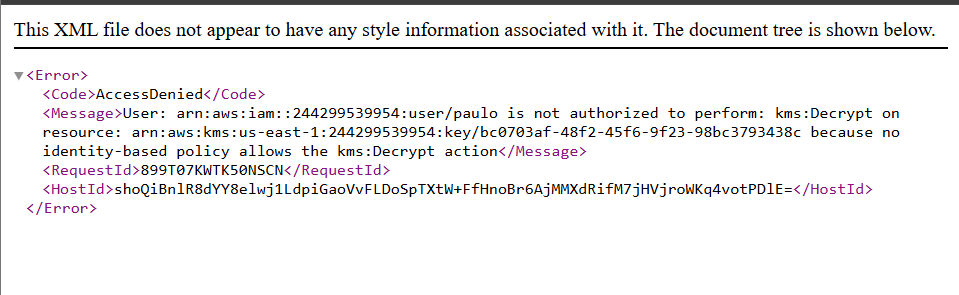
### **Bước 5: Kiểm tra quyền truy cập với user sofia**

* Trong khi vẫn đăng nhập bằng sofia, thử mở hoặc download file loan-data.csv.
* Bạn sẽ **truy cập thành công**.



### **Bước 6: Kiểm tra quyền truy cập với user paulo**

1. **Đăng xuất sofia** khỏi cửa sổ ẩn danh.
2. Đăng nhập lại bằng IAM user paulo.
3. Vào S3 → vào bucket data-bucket → thử mở hoặc tải file loan-data.csv.
4. Lần này, bạn sẽ **thất bại** (Access Denied) vì paulo không có quyền truy cập KMS key.



**📘 Giải thích phân tích cuối cùng**

**Sofia có quyền:**

* Vì bucket policy cho phép upload object
* IAM policy cho phép dùng S3 và KMS
* KMS key policy cho phép sofia dùng key mã hóa → Do đó upload + xem file được

❌ **Paulo bị từ chối:**

* IAM policy + S3 policy có thể cho phép đọc file
* Nhưng không có quyền dùng KMS key (không có trong key policy)  
  → Không thể giải mã nội dung → Không xem được file

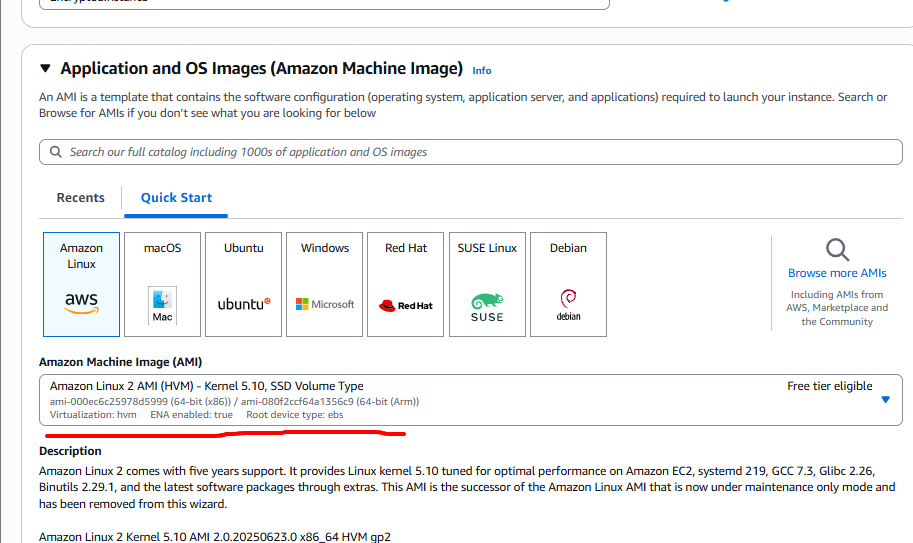
## **Nhiệm vụ 3.4: Sử dụng AWS KMS để mã hóa ổ đĩa gốc của phiên bản EC2**

### **Bước 1: Tạo EC2 instance mới**

1. Truy cập **EC2 Console** tại: <https://console.aws.amazon.com/ec2/>
2. Chọn **Launch Instance** (Khởi chạy instance)

### **Bước 2: Cấu hình cơ bản**

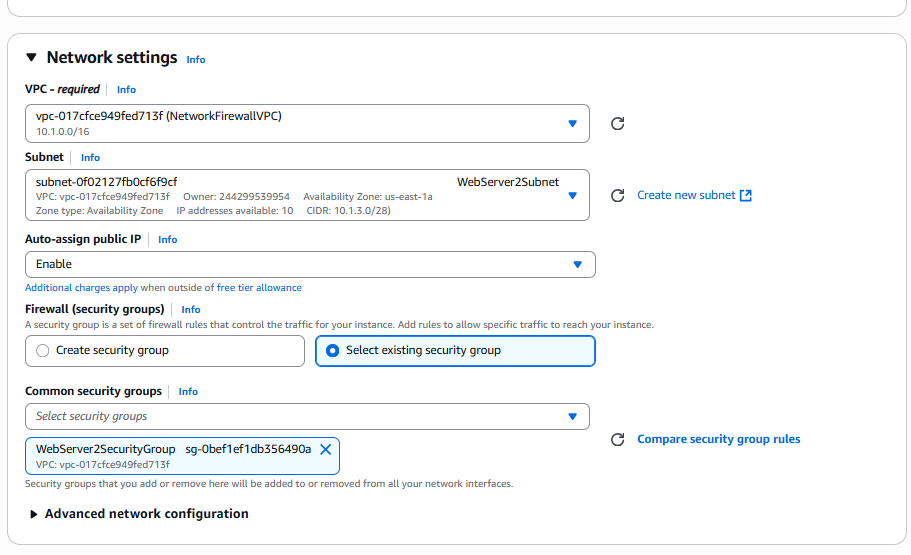
* **Name**: EncryptedInstance
* **Application and OS Images (AMI)**:
  + Chọn **Amazon Linux 2 AMI**  
    ⚠️ *Không chọn Amazon Linux 2023*



* **Instance type**: t2.micro (được miễn phí trong Free Tier)
* **Key pair (login)**:
  + Chọn **vockey**

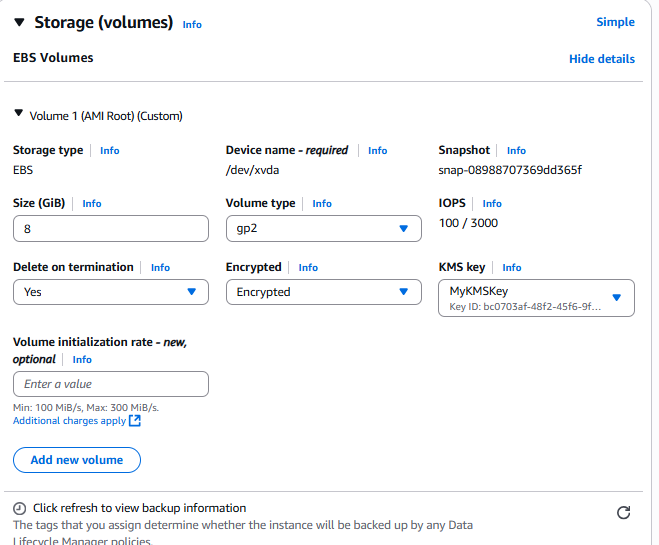
### **Bước 3: Cấu hình mạng**

* Chọn **Network: NetworkFirewallVPC**
* **Subnet**: chọn WebServerSubnet2
* **Firewall (security group)**: Chọn **WebServer2SecurityGroup**



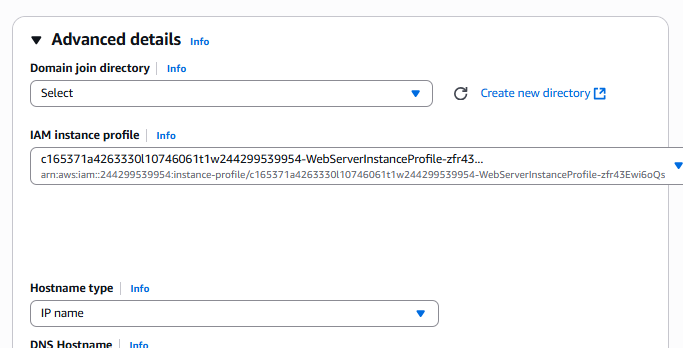
### **Bước 4: Cấu hình ổ đĩa (storage)**

1. Tìm phần **Configure storage** (Cấu hình bộ nhớ)
2. Chọn **Advanced** (Nâng cao)
3. Trong **Root volume**:
   * Đảm bảo là EBS
   * **Tích chọn "Encrypt this volume"**
   * Trong phần **KMS key**, chọn: **MyKMSKey** (Khóa bạn đã tạo ở Task 3.1)



### **Bước 5: Advanced details**

* Mở phần **Advanced details**
* Trong mục **IAM instance profile**, chọn:  
  → **WebServerInstanceProfile**



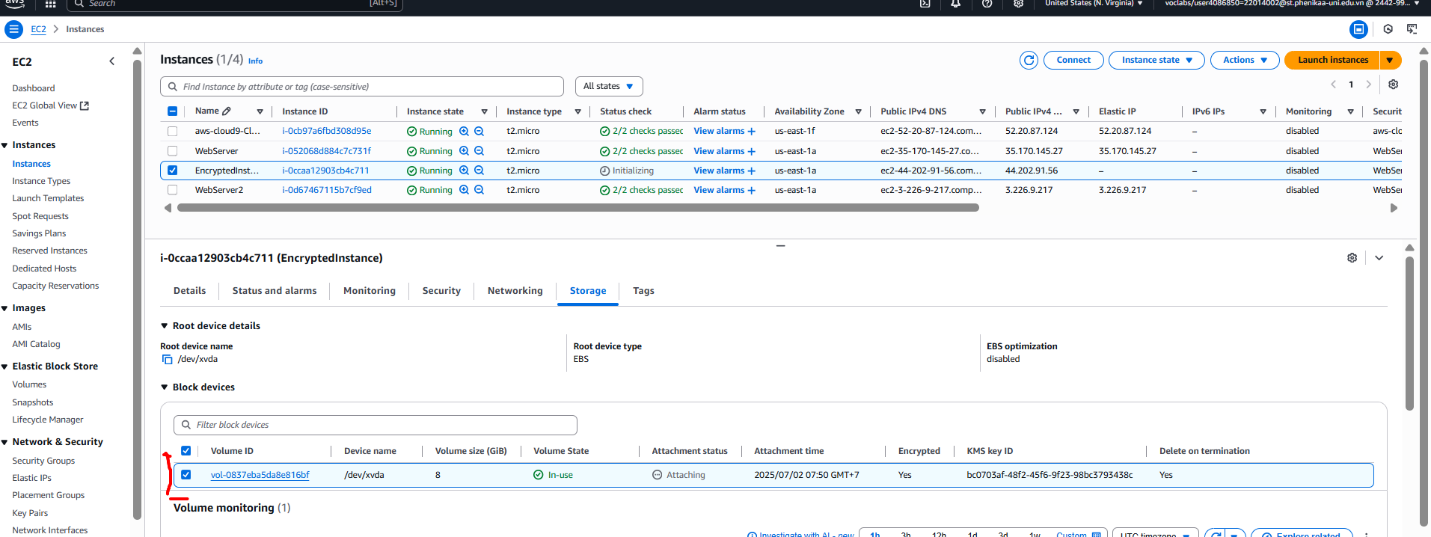
### **Bước 6: Khởi chạy Instance**

* Kiểm tra lại toàn bộ cấu hình
* Nhấn **Launch Instance**

### **Bước 7: Xác minh mã hóa ổ đĩa**

1. Trong EC2 Console, chọn instance mới có tên là **EncryptedInstance**
2. Chuyển sang tab **Storage**
3. Kiểm tra:
   * Volume type: gp2/gp3
   * **Encrypted: Yes**
   * **KMS key: alias/MyKMSKey**

Nó sẽ giống với ảnh minh họa trong hướng dẫn như sau:



## **Nhiệm vụ 3.5: Sử dụng mã hóa phong bì AWS KMS để mã hóa dữ liệu tại chỗ**

### **Bước 1: Kết nối với WebServer2**

Dùng **EC2 Instance Connect** để kết nối với EC2 instance có tên **WebServer2** đã được tạo từ Phase 2.

### **Bước 2: Tạo file cần mã hóa**

Chạy các lệnh sau trong terminal của WebServer2:

***echo "Let's encrypt these file contents. Sensitive data here." > data\_unencrypted.txt***

***cat data\_unencrypted.txt***

✅ Kết quả: Tạo file data\_unencrypted.txt chứa dữ liệu văn bản cần mã hóa.

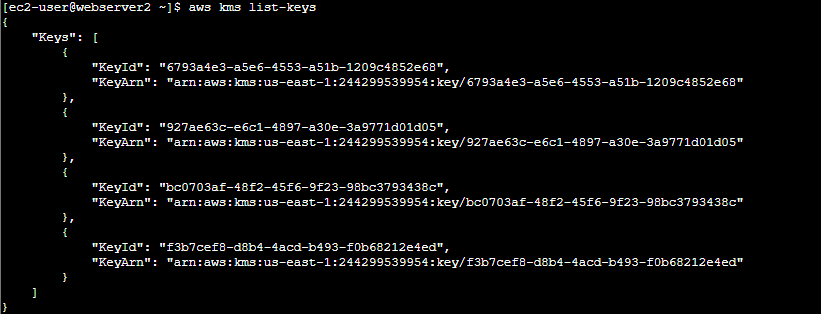
### **Bước 3: Kiểm tra quyền truy cập AWS KMS**

Chạy:

***aws kms list-keys***

✅ Nếu thấy danh sách các khóa xuất hiện → Bạn đã kết nối và có quyền dùng AWS KMS.

❌ Nếu không có phản hồi → Kiểm tra lại **Network Firewall** có cho phép truy cập port **443** chưa (HTTPS).



### **Bước 4: Tạo Data Key từ KMS Key**

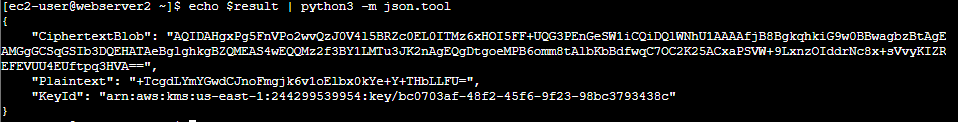
Chạy:

***result=$(aws kms generate-data-key --key-id alias/MyKMSKey --key-spec AES\_256)***

***echo $result | python3 -m json.tool***

✅ Phân tích:

* Plaintext: là khóa dữ liệu **chưa mã hóa**.
* CiphertextBlob: là khóa dữ liệu **đã mã hóa bằng KMS Key**. Bạn sẽ lưu phần này để sử dụng lại sau.



### **Bước 5: Lưu khóa mã hóa (CiphertextBlob) ra file**

Chạy:

***dk\_cipher=$(echo $result | jq '.CiphertextBlob' | cut -d '"' -f2)***

***echo $dk\_cipher***

***echo $dk\_cipher | base64 --decode > data\_key\_ciphertext***

### **Bước 6: Giải mã để lấy khóa dữ liệu gốc (Plaintext)**

Chạy:

***aws kms decrypt --ciphertext-blob fileb://./data\_key\_ciphertext --query Plaintext --output text | base64 --decode > data\_key\_plaintext\_encrypted***

✅ File data\_key\_plaintext\_encrypted chứa **khóa dữ liệu dạng gốc**, dùng để mã hóa/giải mã file.

### **Bước 7: Mã hóa dữ liệu**

Dùng OpenSSL để mã hóa file gốc:

***openssl enc -aes-256-cbc -salt -pbkdf2 -in data\_unencrypted.txt -out data\_encrypted -pass file:data\_key\_plaintext\_encrypted***

Kiểm tra:

***cat data\_encrypted***

✅ Kết quả là dữ liệu đã mã hóa (không đọc được).

### **Bước 8: Xóa file gốc chưa mã hóa**

***rm data\_unencrypted.txt***

### **Bước 9: Giải mã file đã mã hóa**

***openssl enc -d -aes-256-cbc -pbkdf2 -in data\_encrypted -out data\_decrypted.txt -pass file:./data\_key\_plaintext\_encrypted***

Xem nội dung:

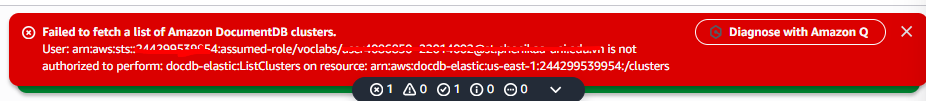
***cat data\_decrypted.txt***

✅ Kết quả: Bạn sẽ thấy lại nội dung gốc "Let's encrypt these file contents. Sensitive data here.".

## **Nhiệm vụ 3.6: Sử dụng AWS KMS để mã hóa bí mật Secrets Manager**

### **Bước 1: Tạo secret trong Secrets Manager**

1. Vào **AWS Console** → **Secrets Manager**.
2. Nhấn **“Store a new secret”**.
3. Chọn **Other type of secret** (không phải database hay API key).
4. Trong phần key-value:
   * **Key:** secret
   * **Value:** my secret data
5. Chọn **encryption key** là **MyKMSKey** (KMS key bạn đã tạo ở task 3.1).
6. Đặt tên cho secret: mysecret
7. Hoàn tất các bước còn lại và nhấn **“Store”**.



Note : Nếu xuất hiện thì cứ tiếp tục làm vì nó sẽ không ảnh hưởng gì !

### **Bước 2: Truy xuất bí mật bằng AWS CLI**

**🔗 Kết nối với WebServer2 EC2 instance:**

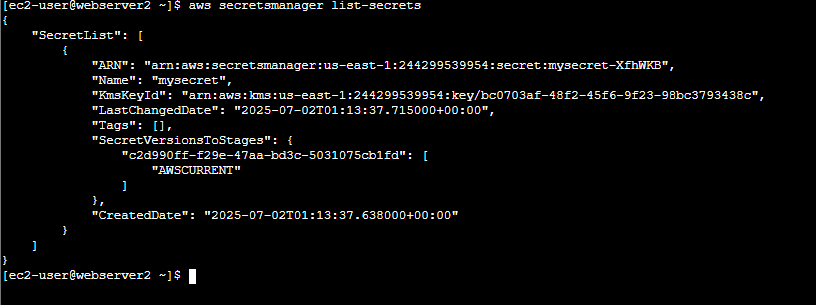
* Vào EC2 → WebServer2 → Nhấn **“Connect”** → Chọn **EC2 Instance Connect** → **Connect**.

**🧑‍💻 Thực hiện các lệnh CLI sau:**

**✅ 1. Liệt kê tất cả secrets:**

***aws secretsmanager list-secrets***

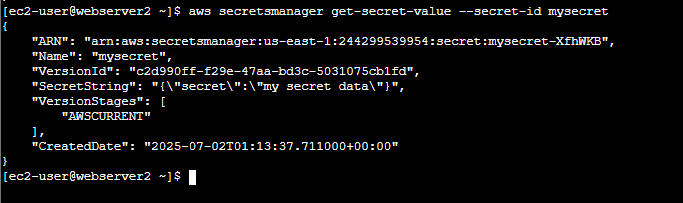
📌 Tìm trong danh sách dòng có "Name": "mysecret".



**✅ 2. Lấy giá trị bí mật:**

***aws secretsmanager get-secret-value --secret-id mysecret***

➡️ **Kết quả mẫu sẽ giống như sau:**



📌 Bạn sẽ thấy rõ cặp key-value secret: my secret data.