**AWS KMS**

AWS Key Management Service (KMS) is a fully managed service that helps you create, manage, and control encryption keys used to protect your data.

* It integrates with most AWS services (S3, EBS, RDS, Lambda, CloudTrail, etc.).
* It allows you to encrypt and decrypt data using Customer Master Keys (CMKs) or KMS keys.
* It handles key rotation, permissions, auditing, and durability automatically.

# Types of KMS Keys

In **AWS KMS**, keys are generally called **KMS keys (Customer Master Keys / CMKs)**. There are several **categories** depending on ownership, visibility, and usage.

## 1. ****AWS Owned Keys****

* **Managed entirely by AWS**.
* Not visible in your account (you don’t see them in the console).
* Used internally by AWS services to encrypt resources by default.
* Example: When you enable encryption on an S3 bucket without choosing a KMS key, AWS may use an **AWS owned key**.

## 2. ****AWS Managed Keys****

* Created, owned, and managed by AWS **for you**.
* **Visible** in your account (console/CLI).
* Named in the format:  
  aws/service-name (e.g., aws/s3, aws/ebs, aws/rds).
* Automatic key rotation every 1 year.
* Example: Encrypting an EBS volume without specifying a key → AWS uses **aws/ebs managed key**.

## 3. ****Customer Managed Keys (CMKs)****

* **Created and fully controlled by you**.
* You define:
  + Key policy (who can use/manage the key).
  + Key rotation (enable/disable).
  + Alias and description.
* You can disable or schedule deletion.
* Most flexible → recommended for **sensitive data**.
* Example: You create a CMK called my-app-key and use it in **S3, RDS, or DynamoDB**.

## 4. ****Customer Provided Keys (Imported Keys)****

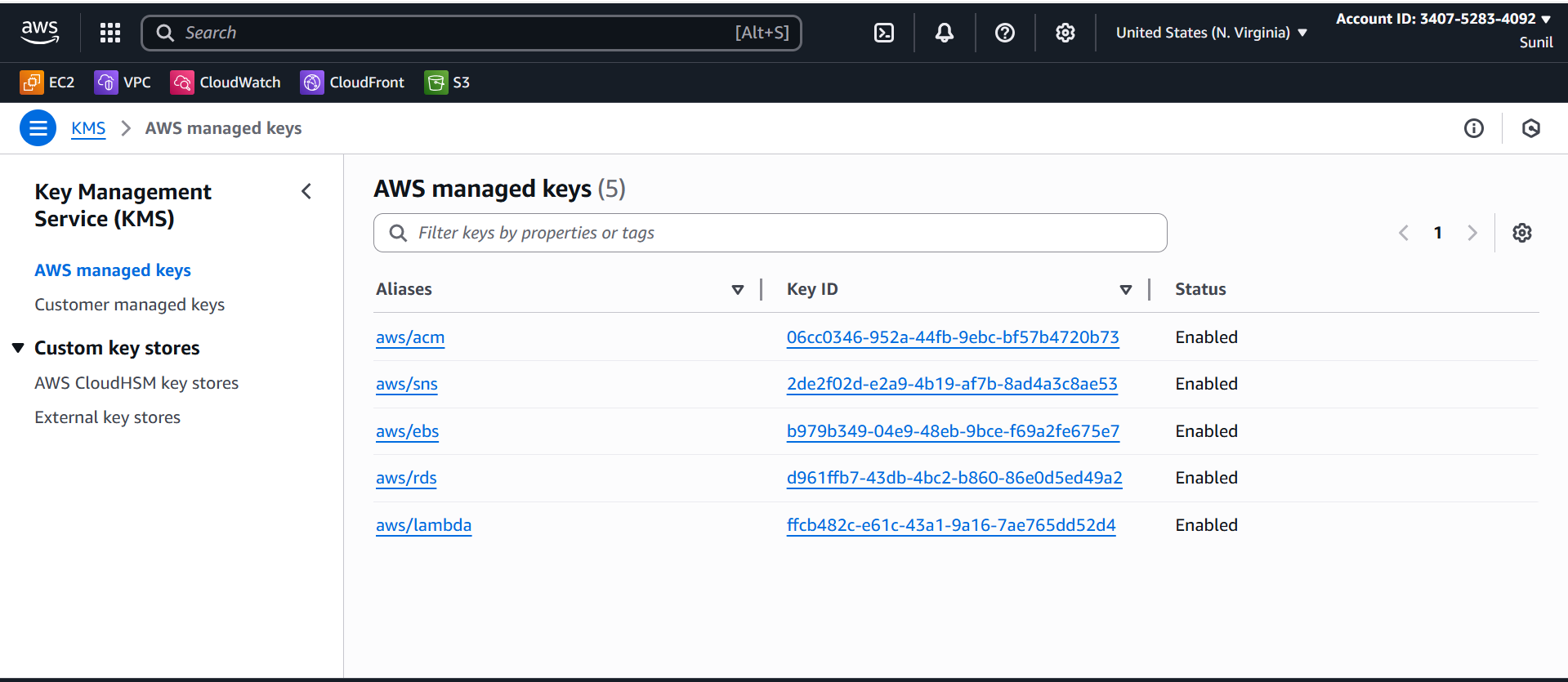
* You generate your own key material **outside AWS** (on-prem, HSM, external system).
* Import into KMS so AWS services can use it.
* Advantage: Full control over key material lifecycle.
* Limitation: No automatic key rotation by KMS (you must re-import when needed).
* Example: A bank or government org that must use **their own HSM-generated keys** but still wants AWS integration.

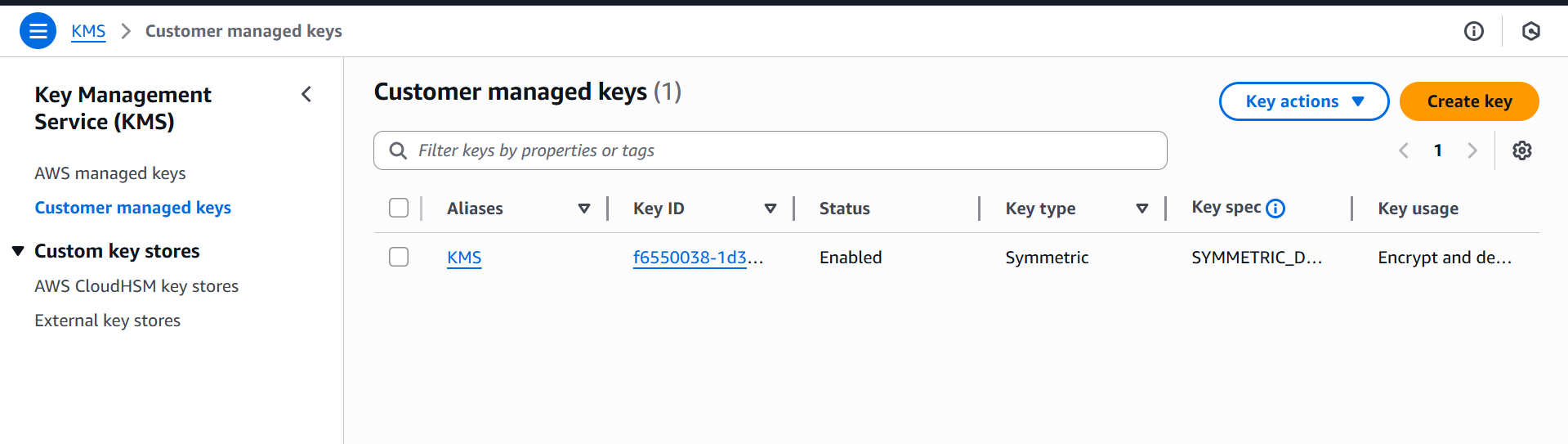
## Types of Keys in KMS

1. **AWS Managed Keys** – Automatically created by AWS services (e.g., S3, EBS).
2. **Customer Managed Keys (CMK)** – You create and manage (full control).
3. **Customer Provided Keys** – You supply your own keys (imported).
4. **AWS Owned Keys** – Completely invisible to you, just used internally by AWS.

## Example Use Cases

* Encrypting S3 objects.
* Encrypting EBS volumes and RDS databases.
* Securing secrets and API keys in **AWS Secrets Manager** or **SSM Parameter Store**.
* Encrypting application data in Lambda/DynamoDB.

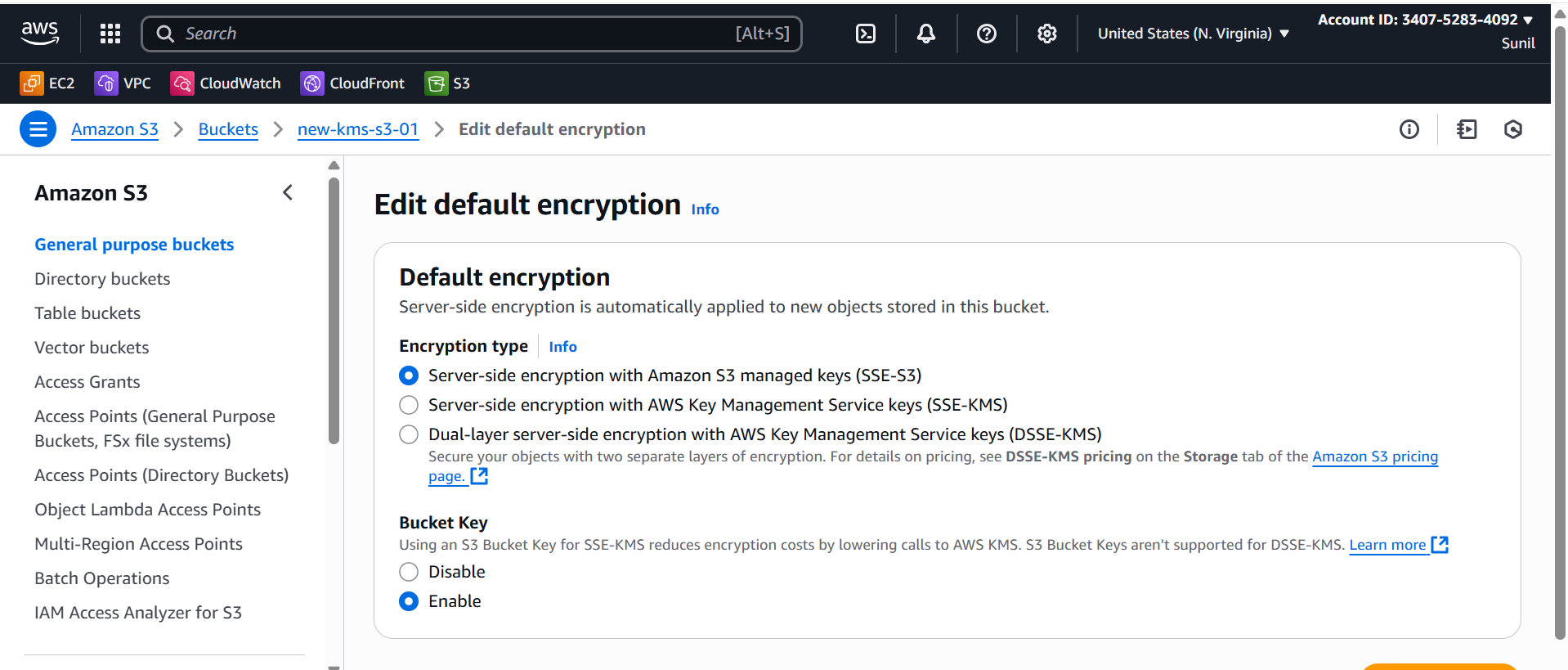




**Real-Time Examples of AWS KMS**

### 1. ****Encrypting S3 Data****

* You store sensitive files (e.g., customer financial records) in **Amazon S3**.
* Enable **Server-Side Encryption with KMS (SSE-KMS)**.
* Each object gets encrypted with a data key that is protected by your KMS key.
* Only authorized IAM roles/users can access the data.



### ****2.)EBS Volume Encryption****

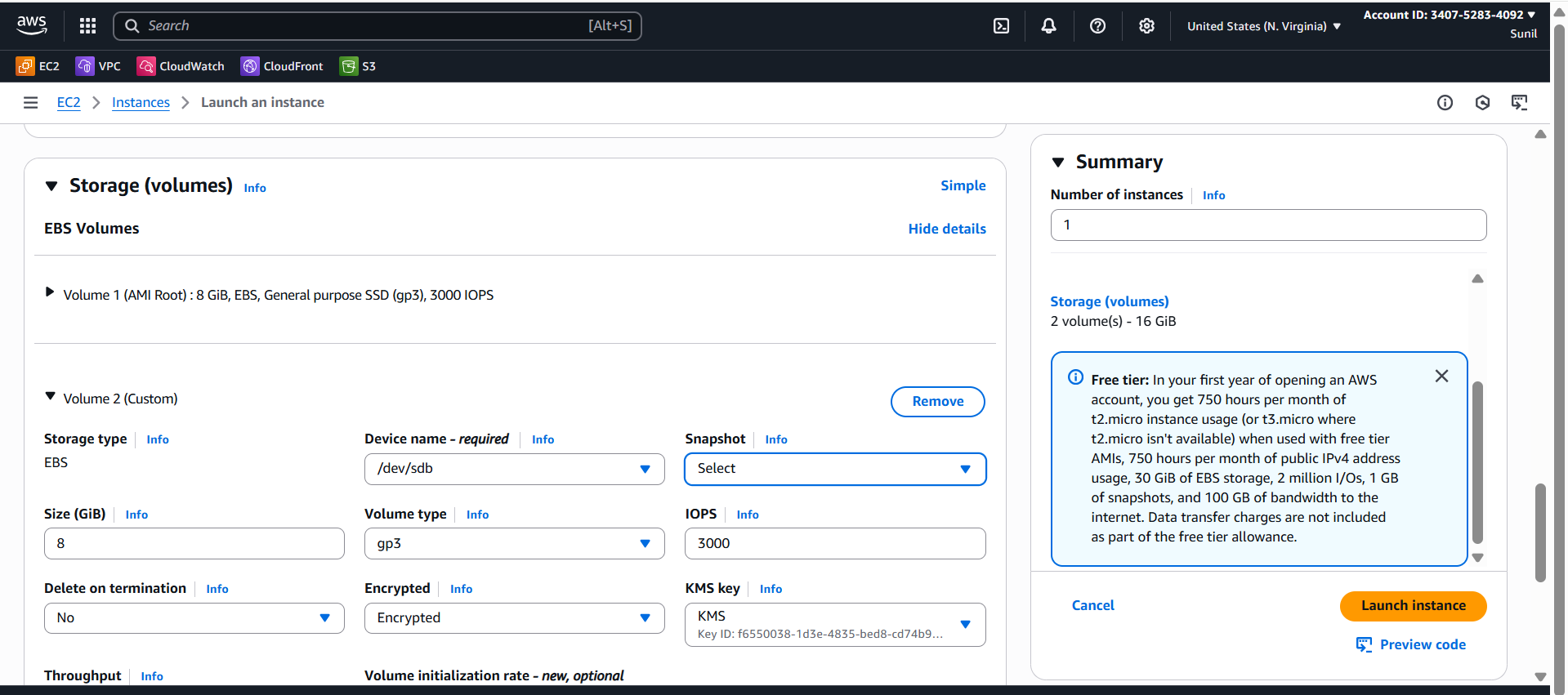
* You attach an **EBS volume** to an EC2 instance for storing logs.
* Enabling encryption ensures all logs are stored encrypted.
* If someone tries to take a snapshot and copy it, they cannot decrypt it without access to KMS.

Encrypt **while launching EC2**

When you launch an EC2 instance, you can specify that the **root volume** and any **additional EBS volumes** are encrypted.

**Steps (Console):**

1. Go to **EC2 → Launch Instance**.
2. Choose AMI, instance type, etc.
3. In **Storage** step:
   * You’ll see the root EBS volume (and you can add more).
   * Under **Encryption**, check **Encrypt this volume**.
   * Choose a **KMS key** (aws/ebs or your custom CMK).
4. Launch the instance.



### ****3.)CloudTrail Log Protection****

* CloudTrail records all AWS API calls.
* You enable encryption for logs using KMS.
* Even if logs are stored in S3, no one can read them without KMS permissions.