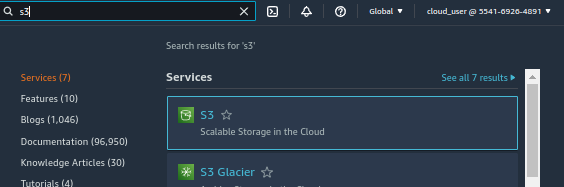
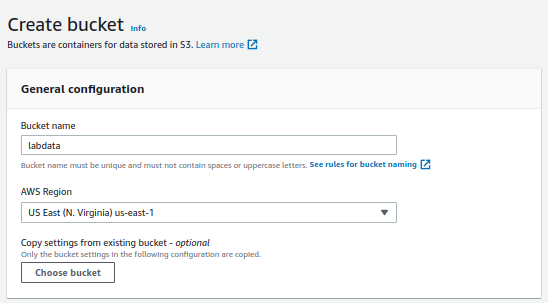
### **Configure Two S3 Buckets**

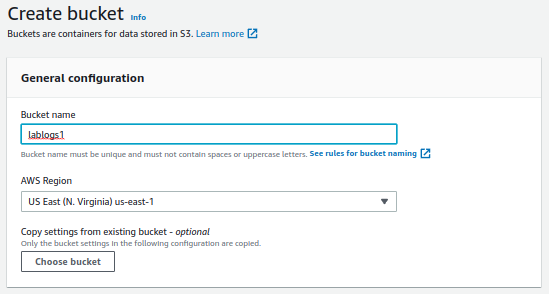
1. In the search bar at the top, enter "S3".
2. Select **S3** in the search results dropdown.

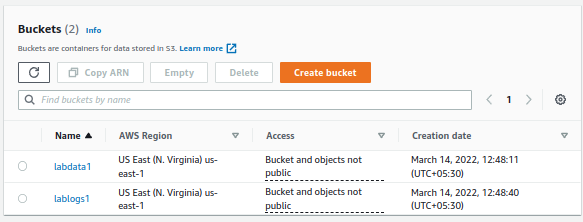


1. Select **Create Bucket**.
2. Under *Bucket name*, enter "labdata" at the beginning of your bucket name.
3. **Note**: Remember, bucket names must be unique



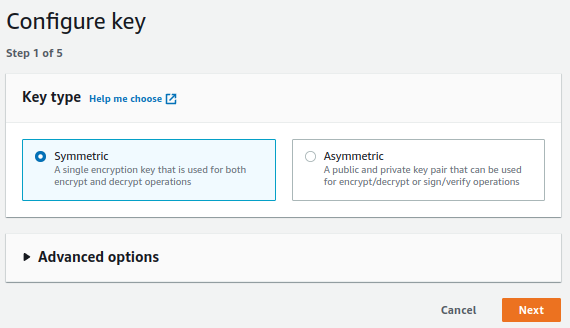
1. Click **Create bucket**.
2. Select **Create Bucket** once again.
3. Under *Bucket name*, enter "lablogs" at the beginning of your bucket name.
4. Click **Create bucket**.



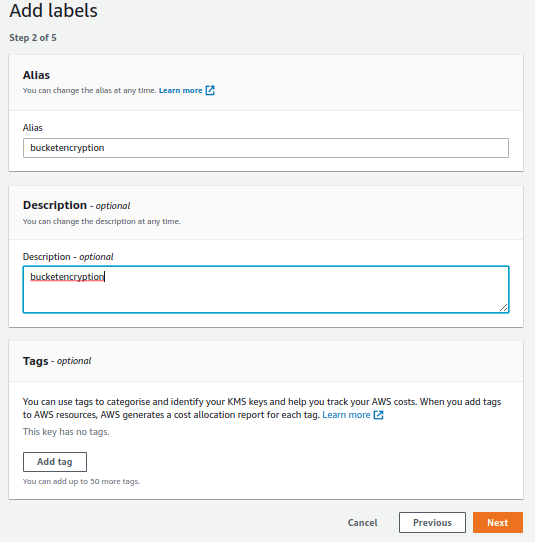


### **Configure KMS Encryption for the Labdata Bucket**

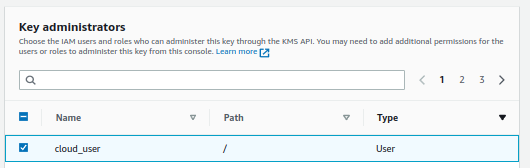
1. In the search bar at the top, enter "KMS".
2. Open **Key Management Service** from the search results dropdown in a new tab.
3. Navigate to the new tab (the KMS Console), and select **Create a key**.
4. Ensure **Symmetric** is selected, and leave settings as default.
5. Click **Next**.



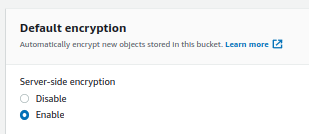
1. Under *Alias*, enter "bucketencrypt".
2. Under *Description*, enter "bucketencrypt".
3. Click **Next**.



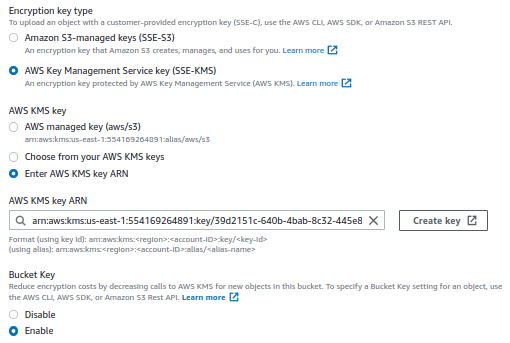
1. Under *Key administrators*, select **cloud\_user**.
2. Click **Next**.



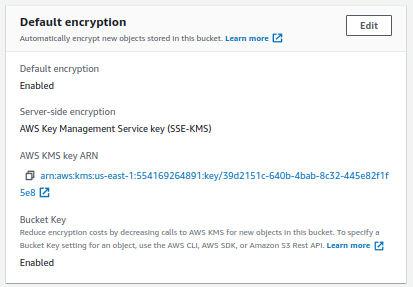
1. Under *Define key usage permissions*, select **cloud\_user**.
2. Click **Next**.
3. Click **Finish**.
4. Navigate back to the S3 Management Console tab.
5. Select the **labdata** bucket.
6. Navigate to the *Properties* tab.
7. Scroll down to *Default encryption* and select **Edit**.
8. Under *Server-side encryption*, select **Enable**.



1. Under *Encryption key type*, select **AWS Key Management Service key (SSE-KMS)**.
   * Under *AWS KMS key*, select **Choose from your AWS KMS keys**.
   * Under the *AWS KMS key* dropdown menu, select the **bucketencrypt** key.
2. Under *Bucket Key*, select **Enable**.

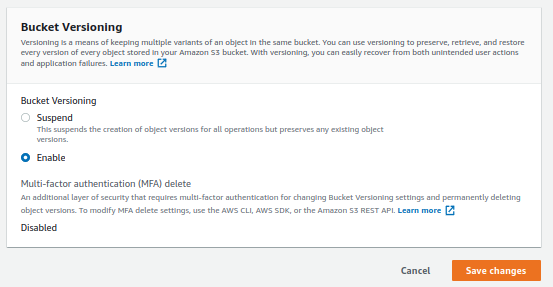


1. Select **Save changes**.

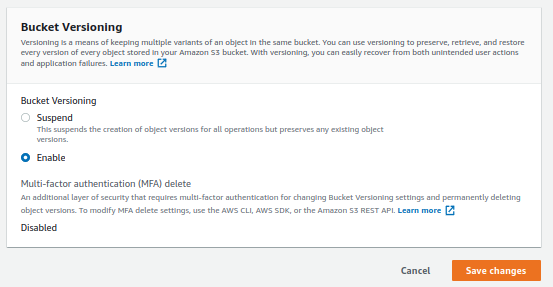


### **Configure Protection for Accidental Deletion of Data for Both Buckets**

1. Navigate back to the S3 Management Console tab.
2. Select the **labdata** bucket.
3. Navigate to the *Properties* tab.
4. Under *Bucket Versioning*, select **Edit**.
5. Under *Bucket Versioning*, select **Enable**.
6. Click **Save changes**.



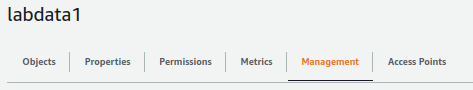
1. Navigate back to the S3 Management Console and select the **lablogs** bucket.
2. Navigate to the *Properties* tab.
3. Under *Bucket Versioning*, select **Edit**.
4. Under *Bucket Versioning*, select **Enable**.
5. Click **Save changes**.



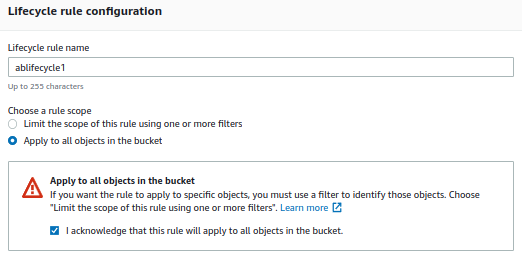
### **Configure Lifecycle Configuration for Both Buckets**

Configure Lifecycle policies for the S3 buckets. Below are the requirements identified by our fictional company.

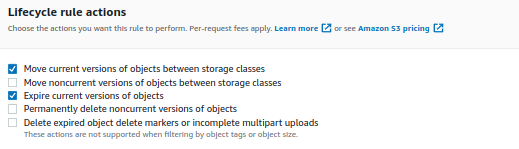
1. Select the **labdata** bucket.
2. Select the *Management* tab.



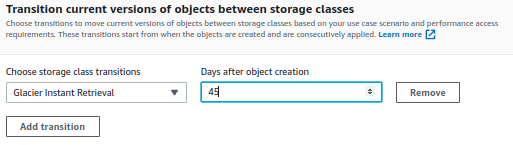
1. Under *Lifecycle rules*, select **Create lifecycle rule**.
2. Under *Lifecycle rule configuration*, set the following values:
   * *Lifecycle rule name*: enter "lablifecycle"
   * *Choose a rule scope*: select **This rule applies to *all* objects in the bucket** (make sure to select the checkbox next to the warning)



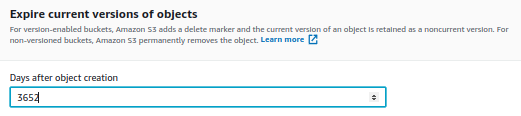
* + *Lifecycle rule actions*: select both **Transition *current* versions of objects between storage classes** and **expire *current* versions of objects**

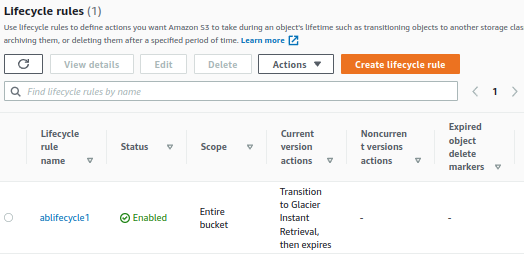


* + *Transition current versions of objects between storage classes*:
    - *Storage class transitions*: **Glacier**
    - *Days after object creation*: enter "45" (make sure to select the checkbox next to the warning)



* + *Expire current versions of objects*:
    - *Number of days after object creation*: enter "3652"





1. Select **Create rule**.
2. Navigate back to the S3 Management Console tab.
3. Select the **lablogs** bucket.
4. Select the *Management* tab.
5. Under *Lifecycle rules*, select **Create lifecycle rule**.
6. Under *Lifecycle rule configuration*, set the exact same values that you set for the labdata bucket.
7. Select **Create rule**.

