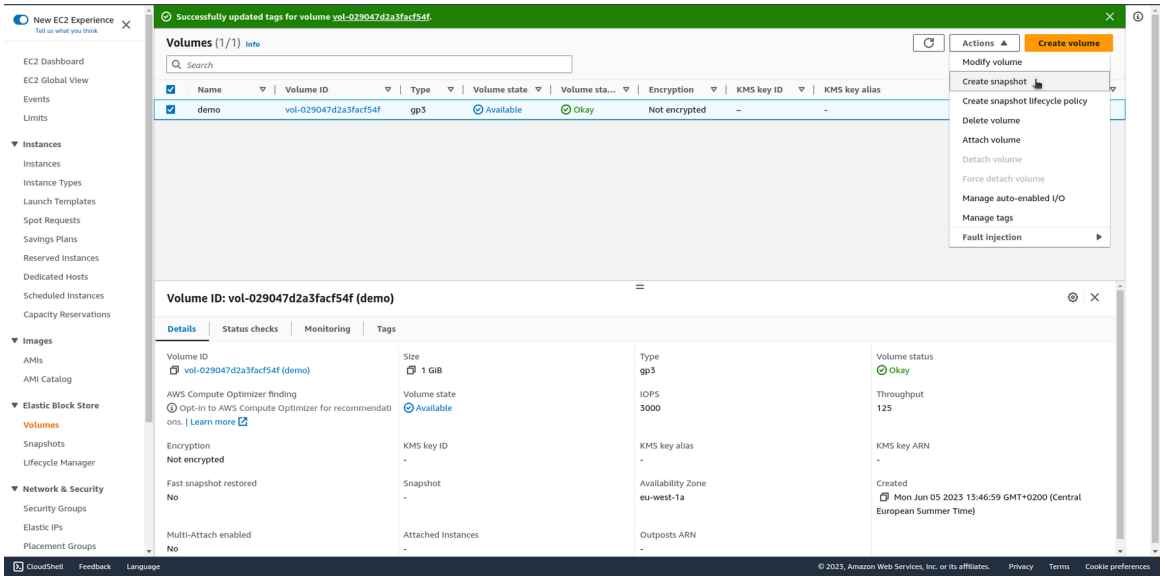
EBS ENCRYPTION

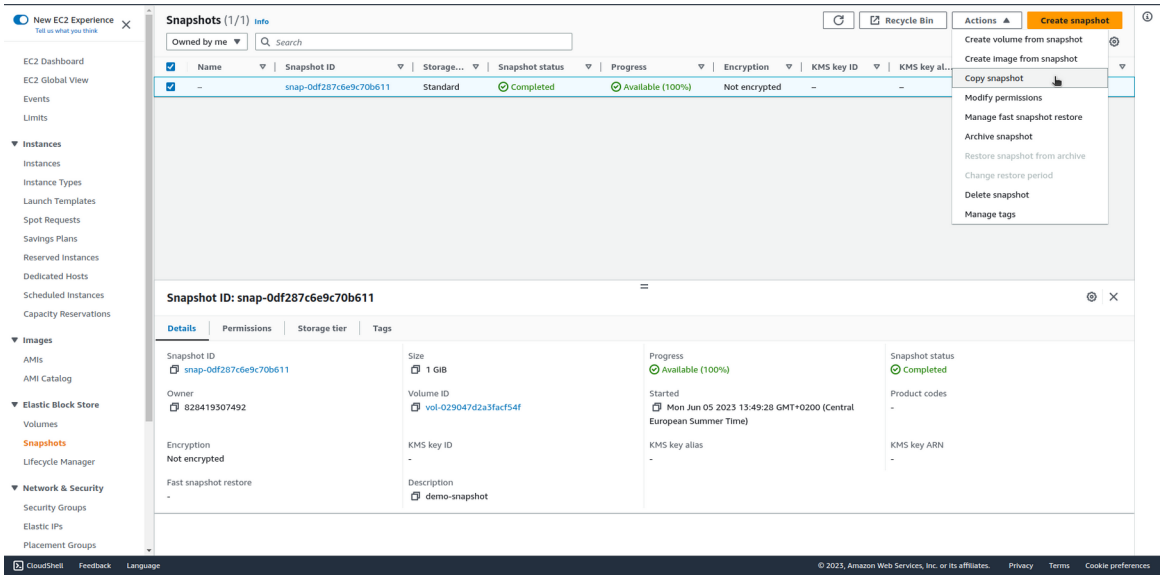
Encryption—to protect data at rest and in-flight—should be an organization's number-one priority when using any storage service. On AWS, its Elastic Block Store (EBS) service provides persistent block-level storage volumes for Amazon EC2 instances. EBS volumes can be attached to your instances and primarily used for data that is rapidly changing or that requires specific input/output operations per second, (IOPS). Because they provide persistent level storage to your instances, EBS volumes are ideally suited for retaining important data and can be used to store personally identifiable information (PII). In any environment where this is the case, it's essential that data on the volume is encrypted to protect it from malicious activity.

An existing unencrypted volume and the data it contains may not be encrypted. Instead, you'll need to follow another process, outlined below.

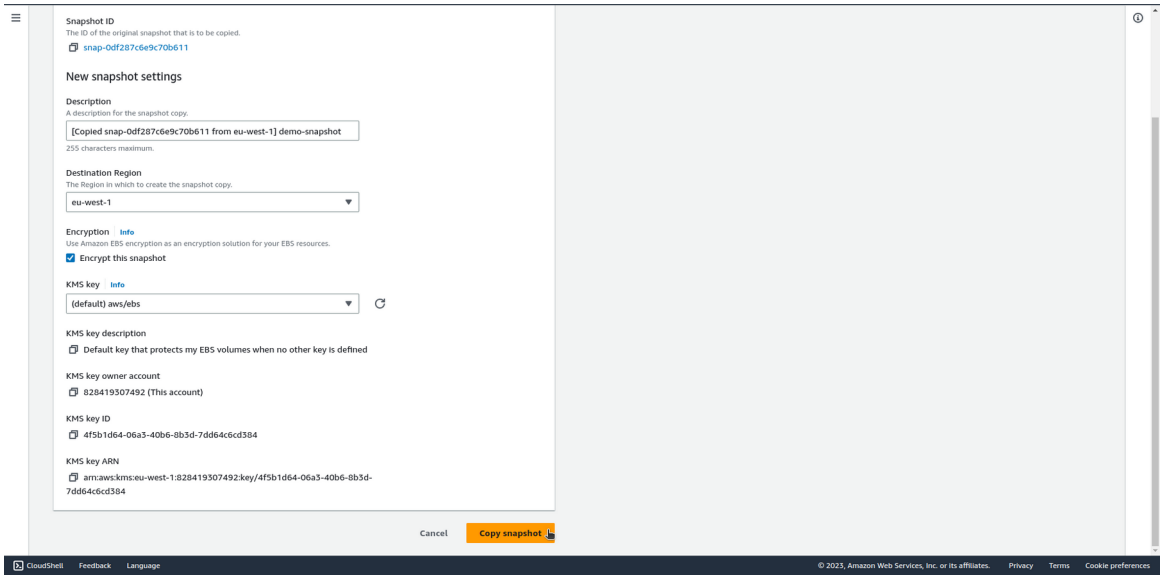
1. Select your unencrypted volume
2. Select 'Actions' – 'Create Snapshot'



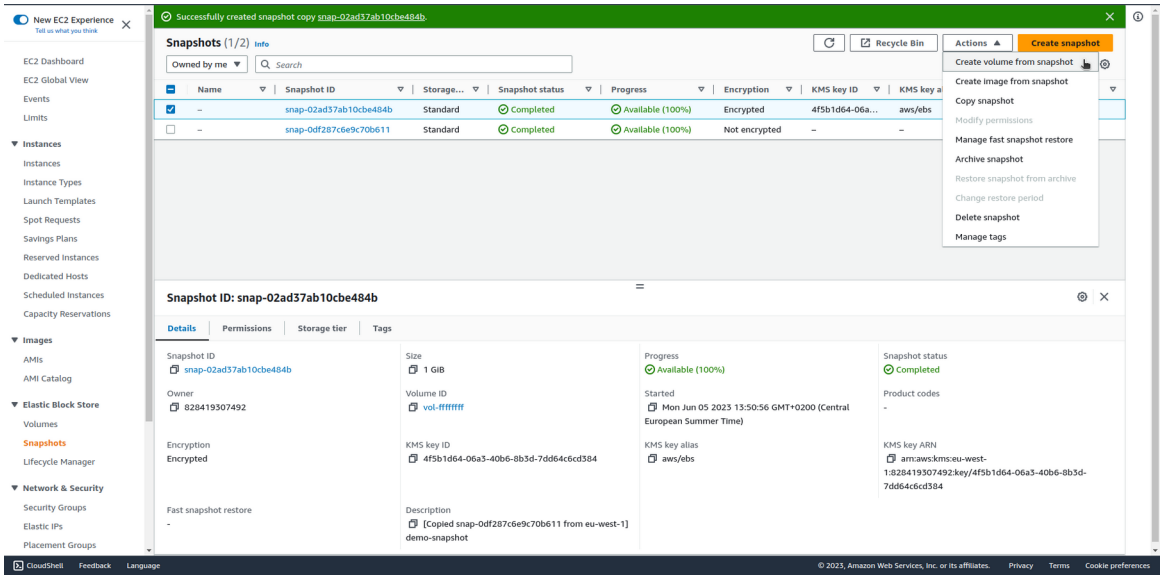
3. When the snapshot is complete, select 'Snapshots' under 'Elastic Block Store'
4. Select your newly created snapshot
5. Select 'Actions' – 'Copy'



6. Check the box for ‘Encryption’
7. Select the CMK for KMS to use as required
8. Click ‘Copy’



9. Select the newly created snapshot
10. Select ‘Actions’ – ‘Create Volume’



You will notice that the normal ‘Encryption’ option is set to ‘True.’ Because the snapshot is itself encrypted, this cannot be modified. The volume now created from this snapshot will be encrypted.