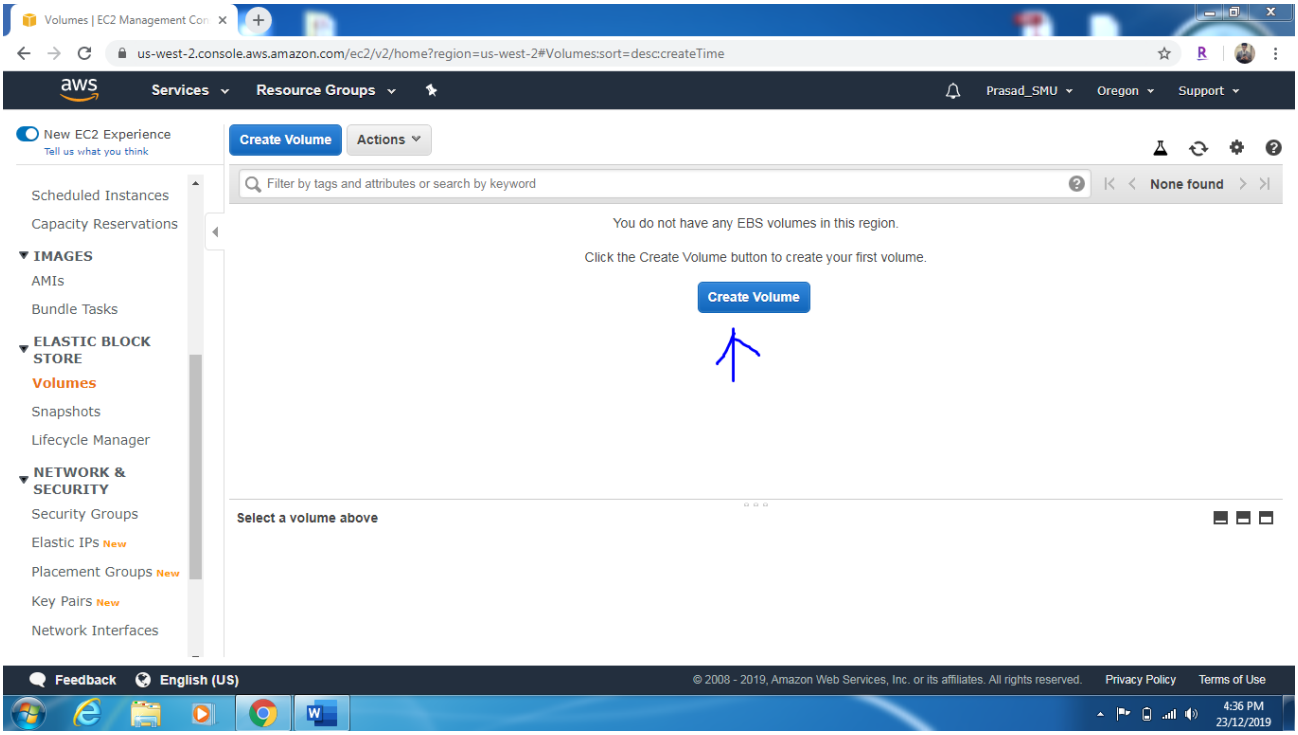
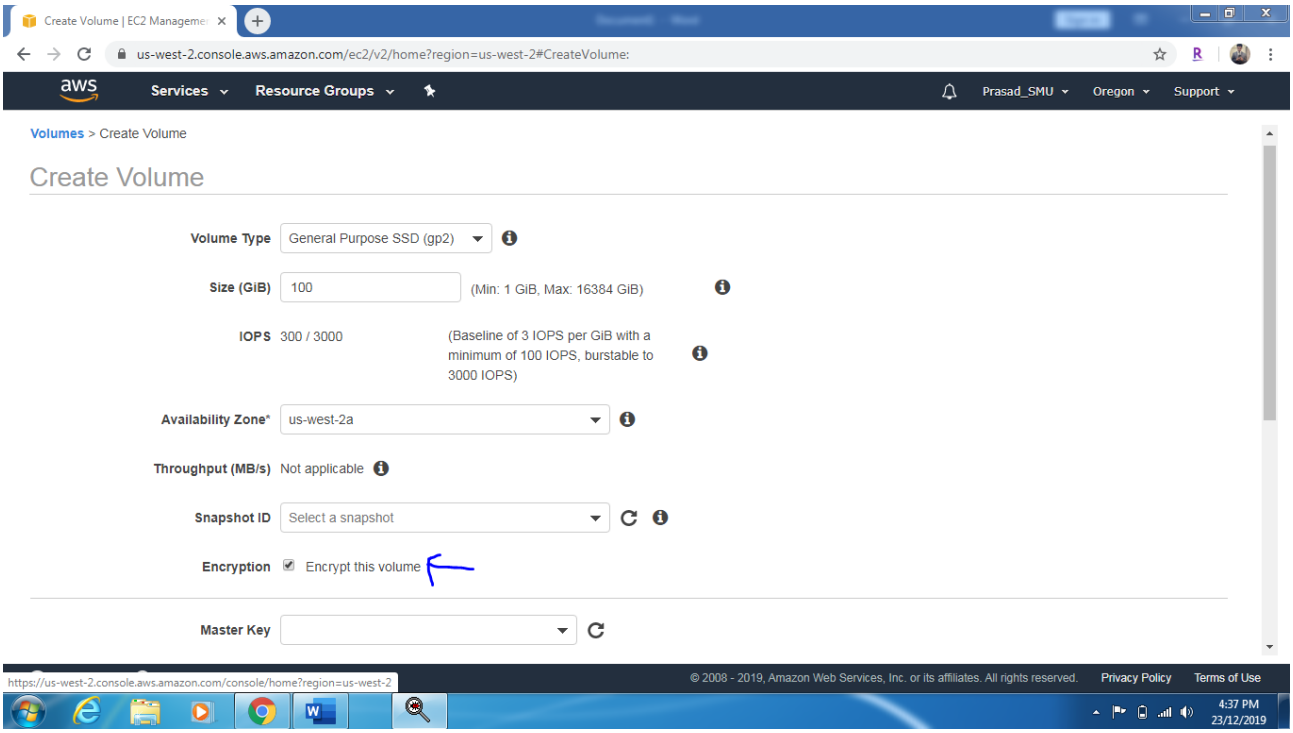
EBS Volume and Snapshot Encryption with Key Management Service (KMS)

Task 1: EBS Volume and Snapshot Encryption with Default AWS Managed Key.

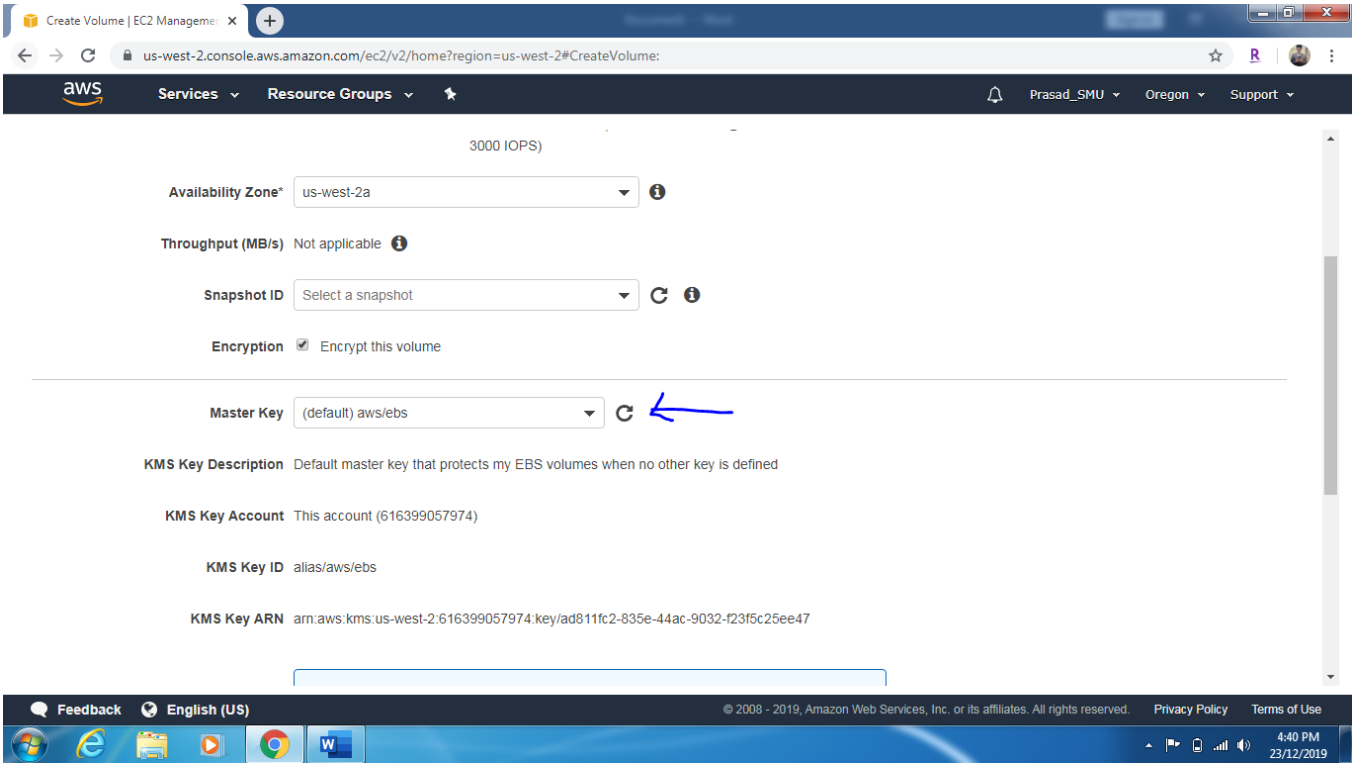
- Navigate to EC2 Service, Volumes and click on **Create Volume**.



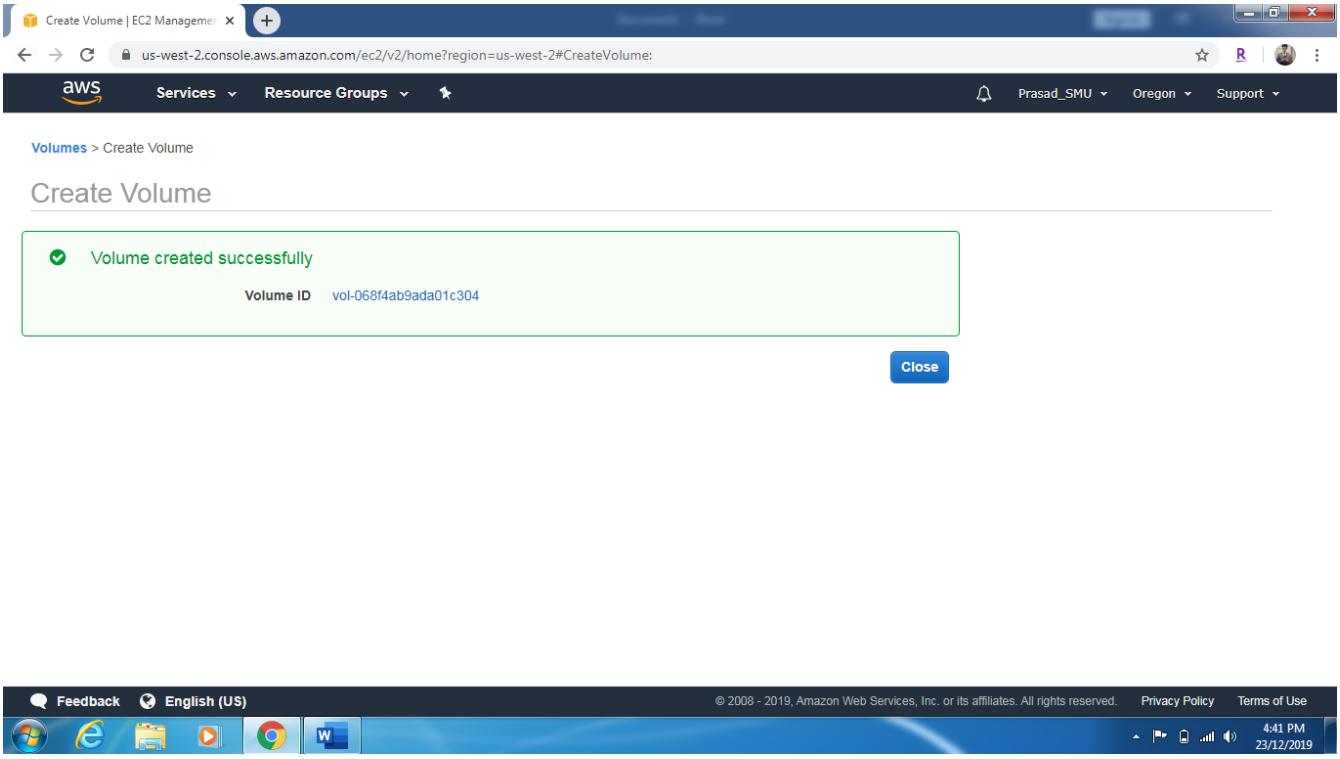
- Let's encrypt this volume by clicking on "Encrypt this volume" option.



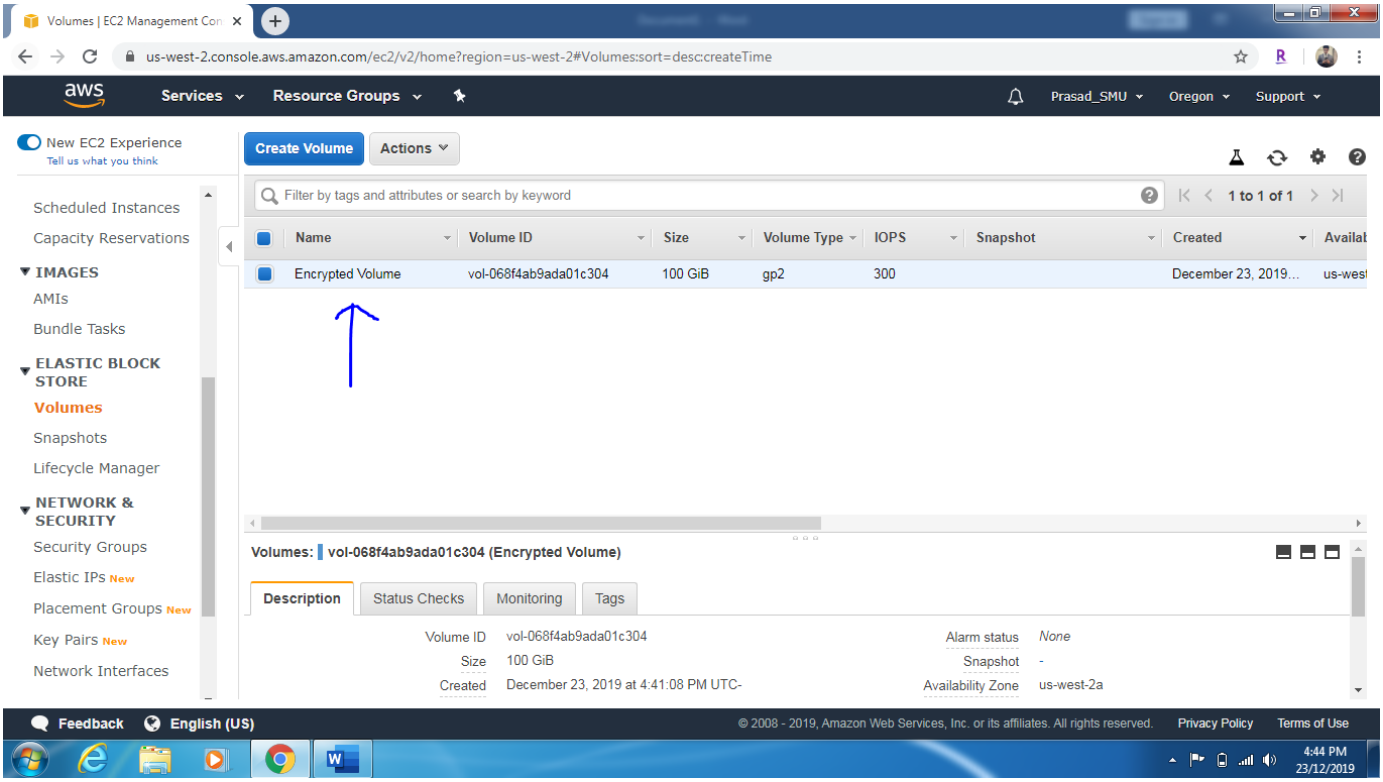
- For Encryption purpose, we are going to use the Default Master Key. (default) aws/ebs



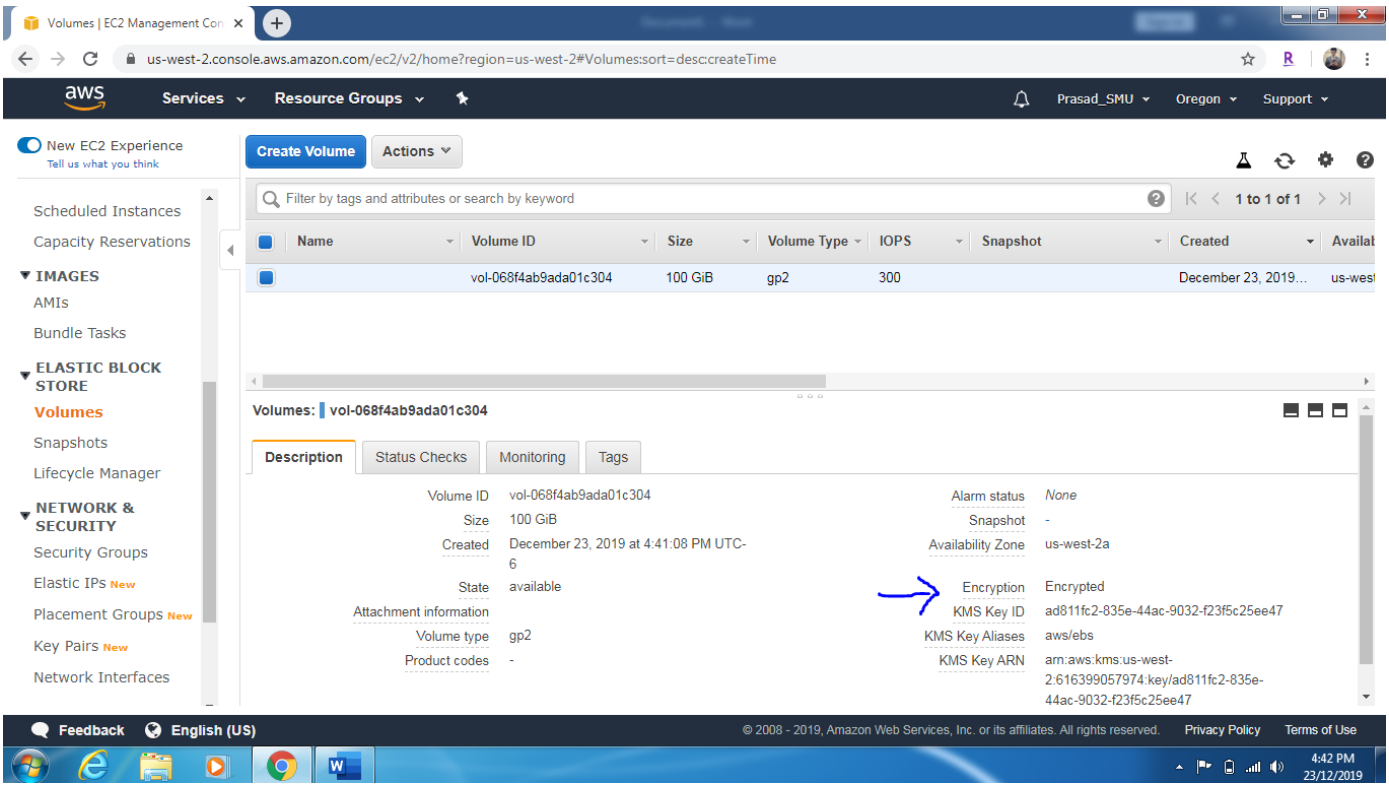
- Click on **Create Volume**. Your Volume is now fully Encrypted.



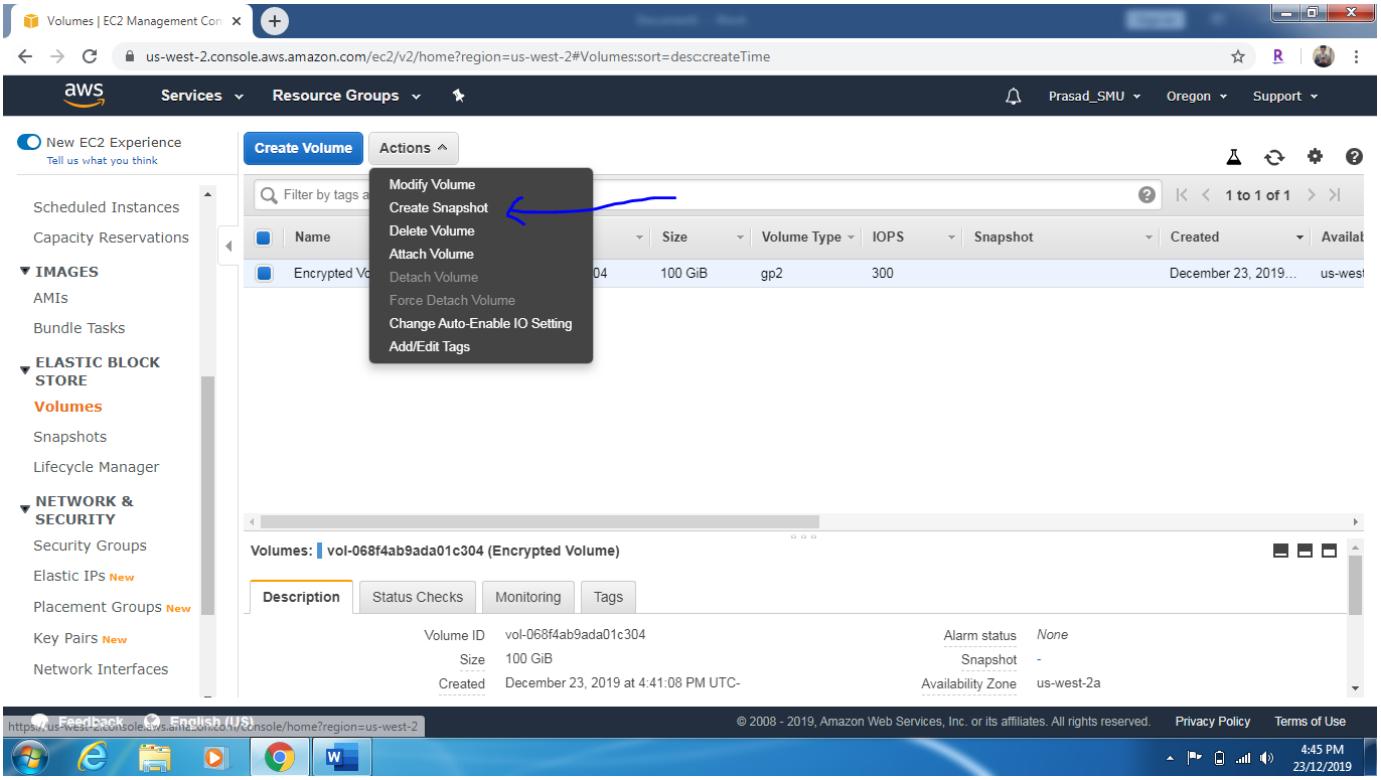
- Give the Volume name as **"Encrypted Volume".**



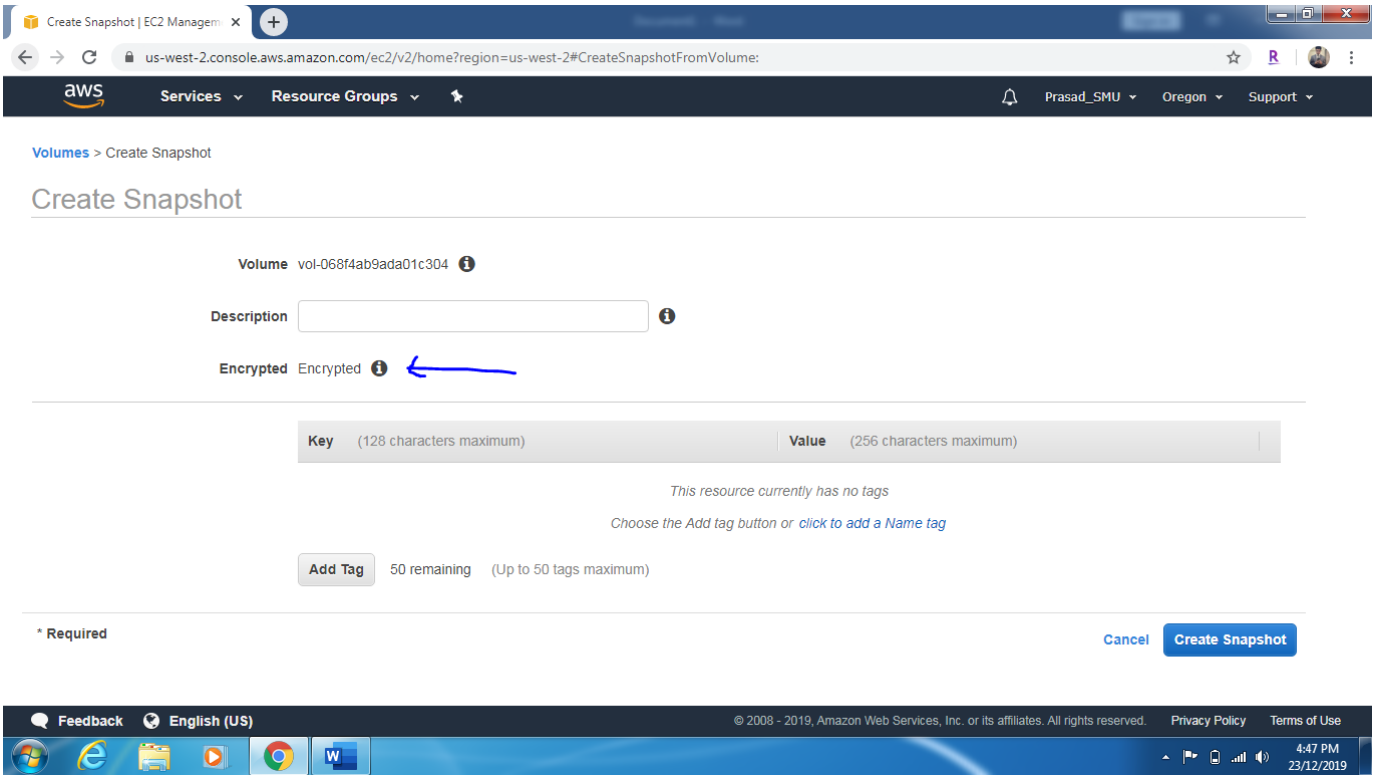
- You can verify the Volume Encryption information in the **Description**.



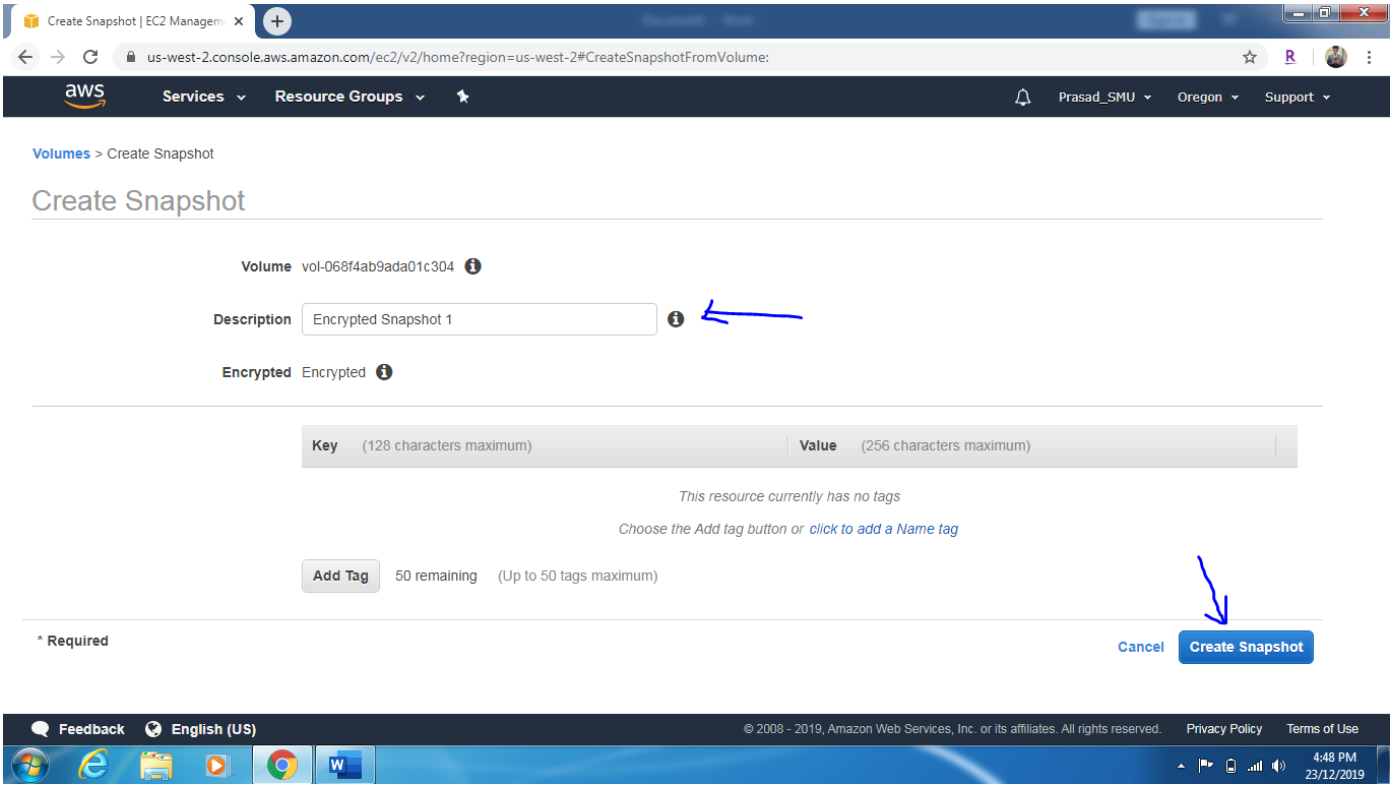
- Now go to Actions and Click on **"Create Snapshot".**

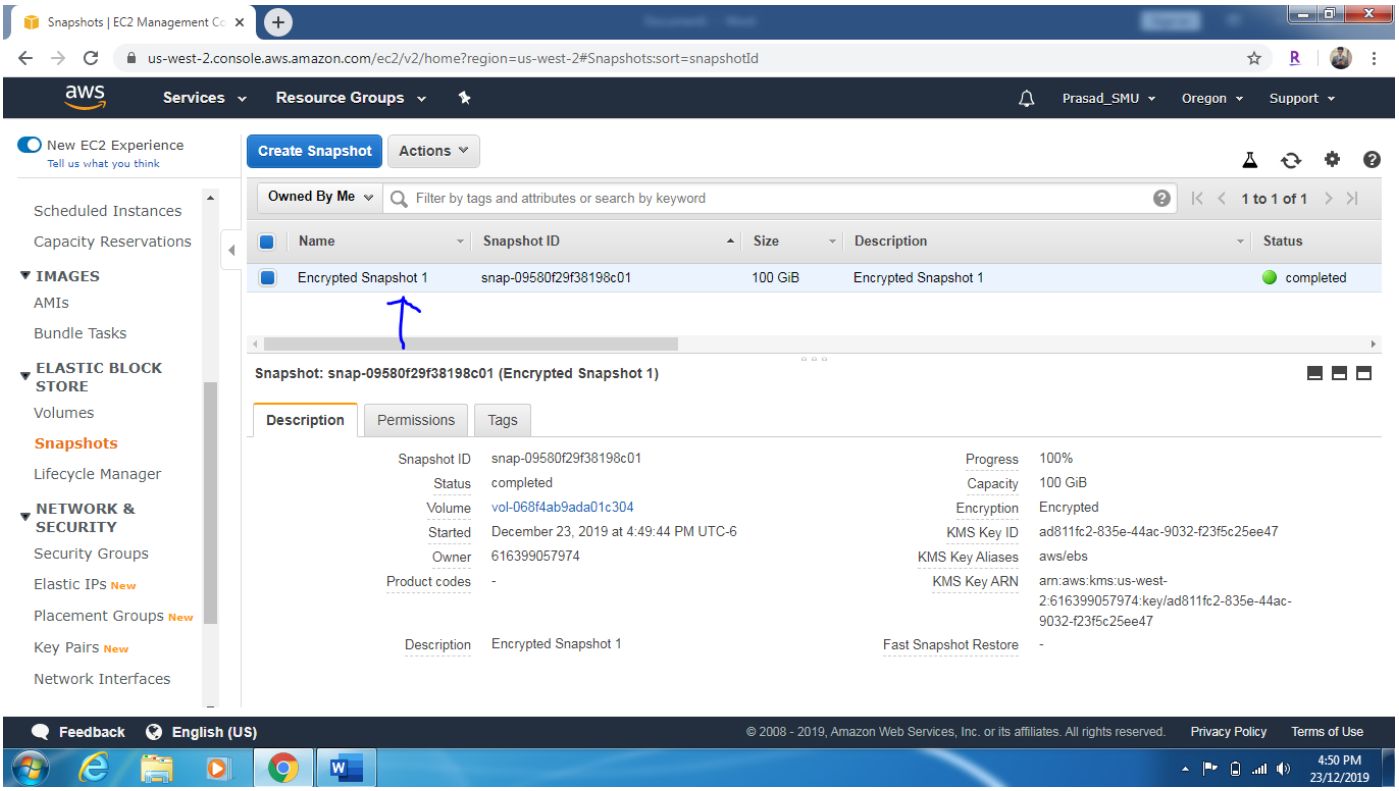


- Snapshot of an Encrypted Volume is also **Encrypted**.

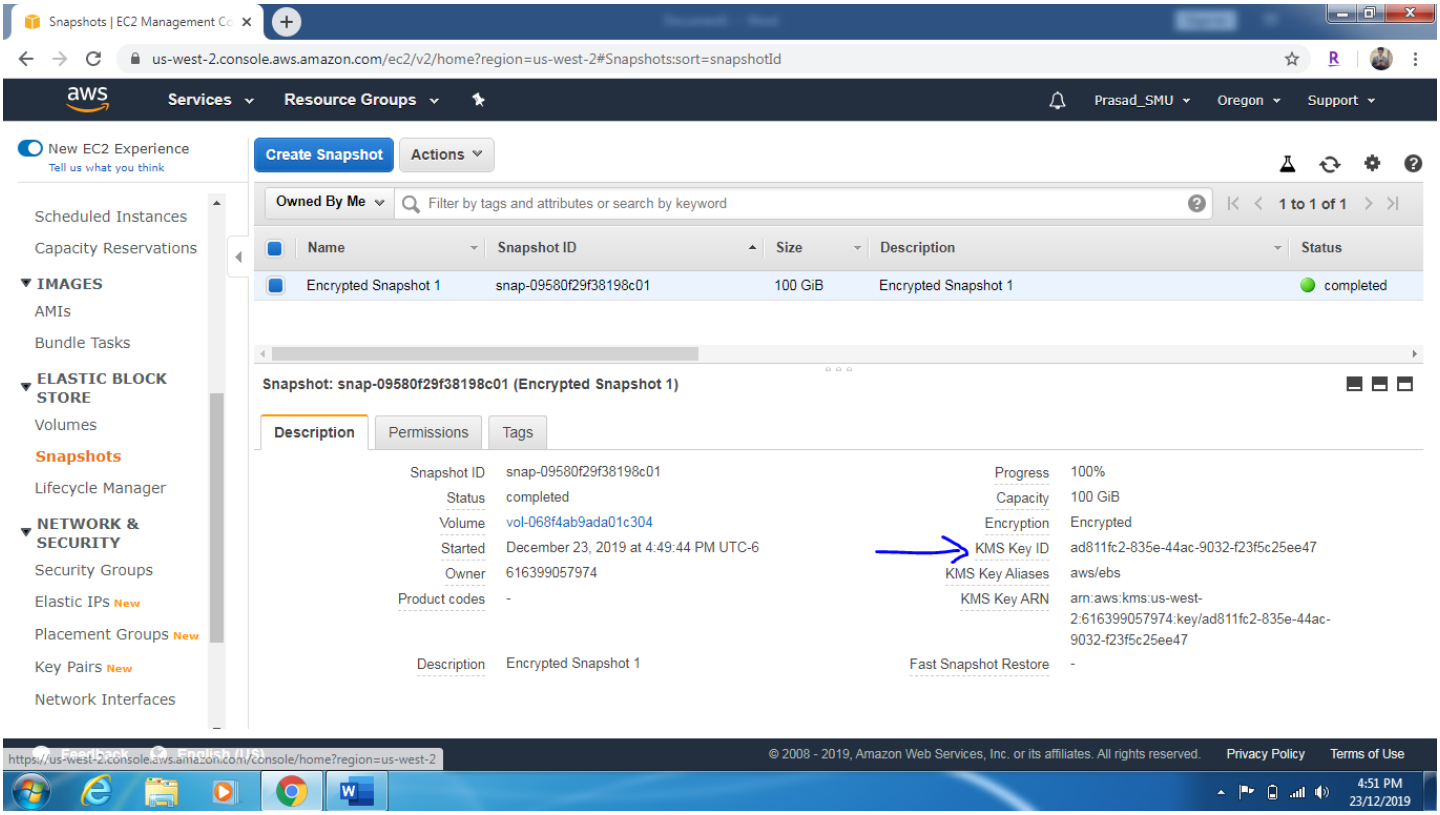


- Give the Snapshot name as **"Encrypted Snapshot 1"** and click on Create Snapshot.





- Also Verify the Encryption of the Snapshot under Description. It has been Encrypted with default AWS Managed Key which was used to Encrypt the Volume.



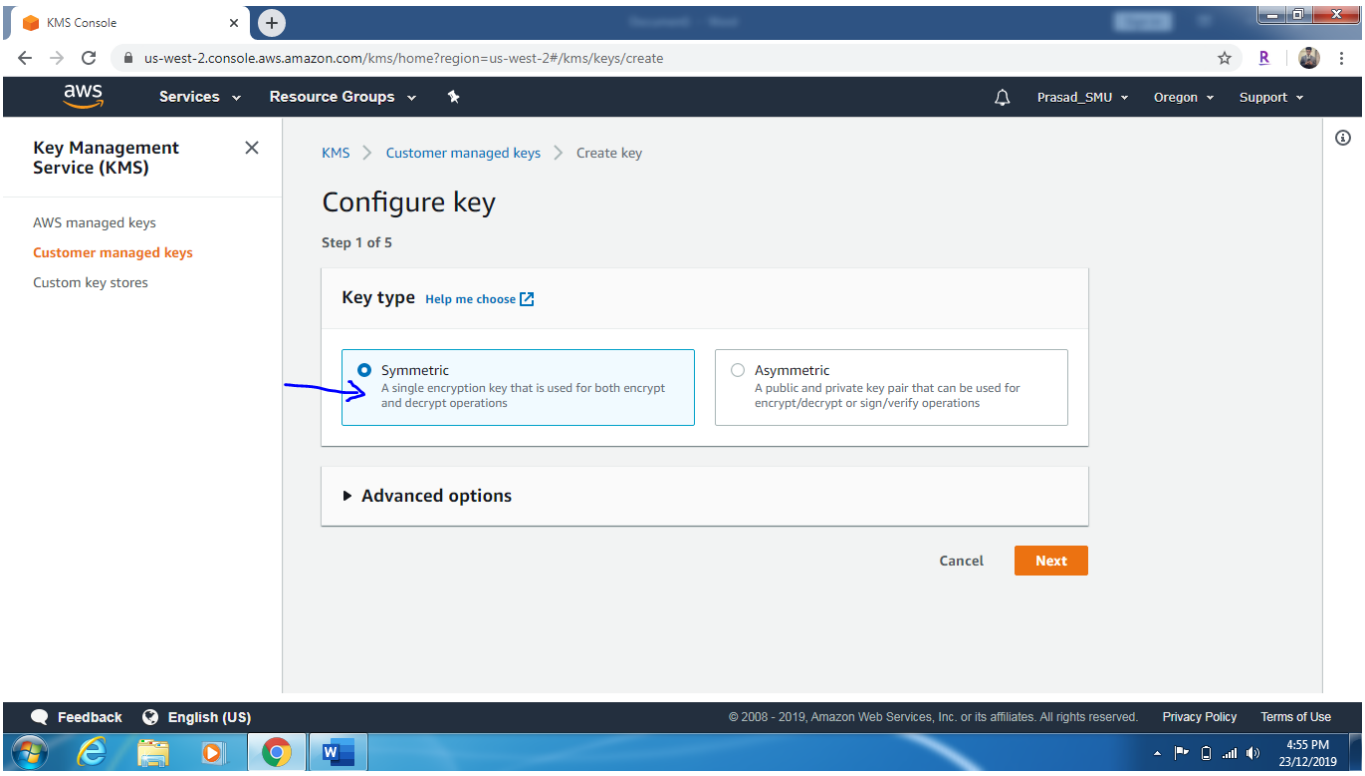
In this Task, we've learnt how to encrypt a Volume and Snapshot using default AWS Managed Key.

In the Next Task, we'll see how to encrypt a Volume and Snapshot using Customer Managed Key.

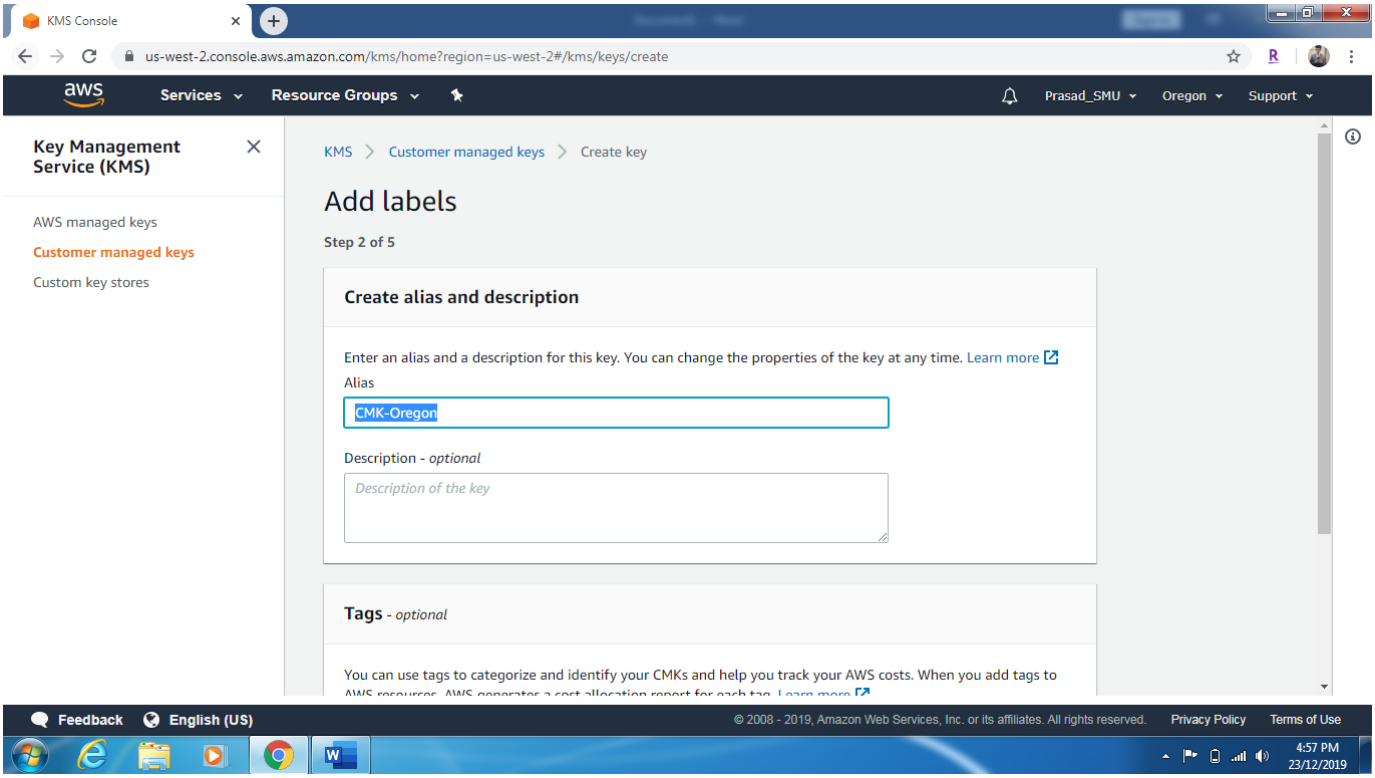
Task 2: Encrypt a Volume and Snapshot using Customer Managed Key.

- Navigate to Key Management Service (KMS) and click on **Customer Managed Key**.

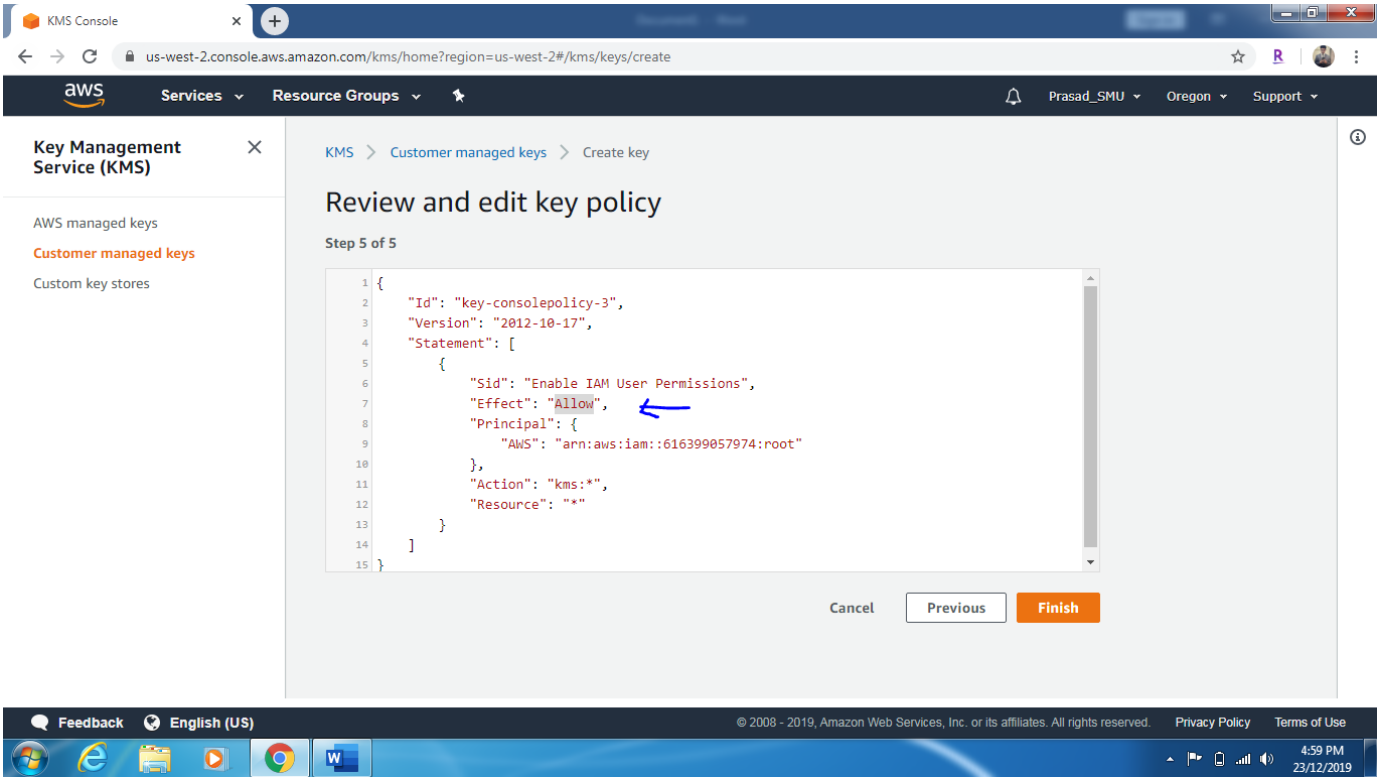
- Click on **"Create Key"** and Select Key type as **"Symmetric".**



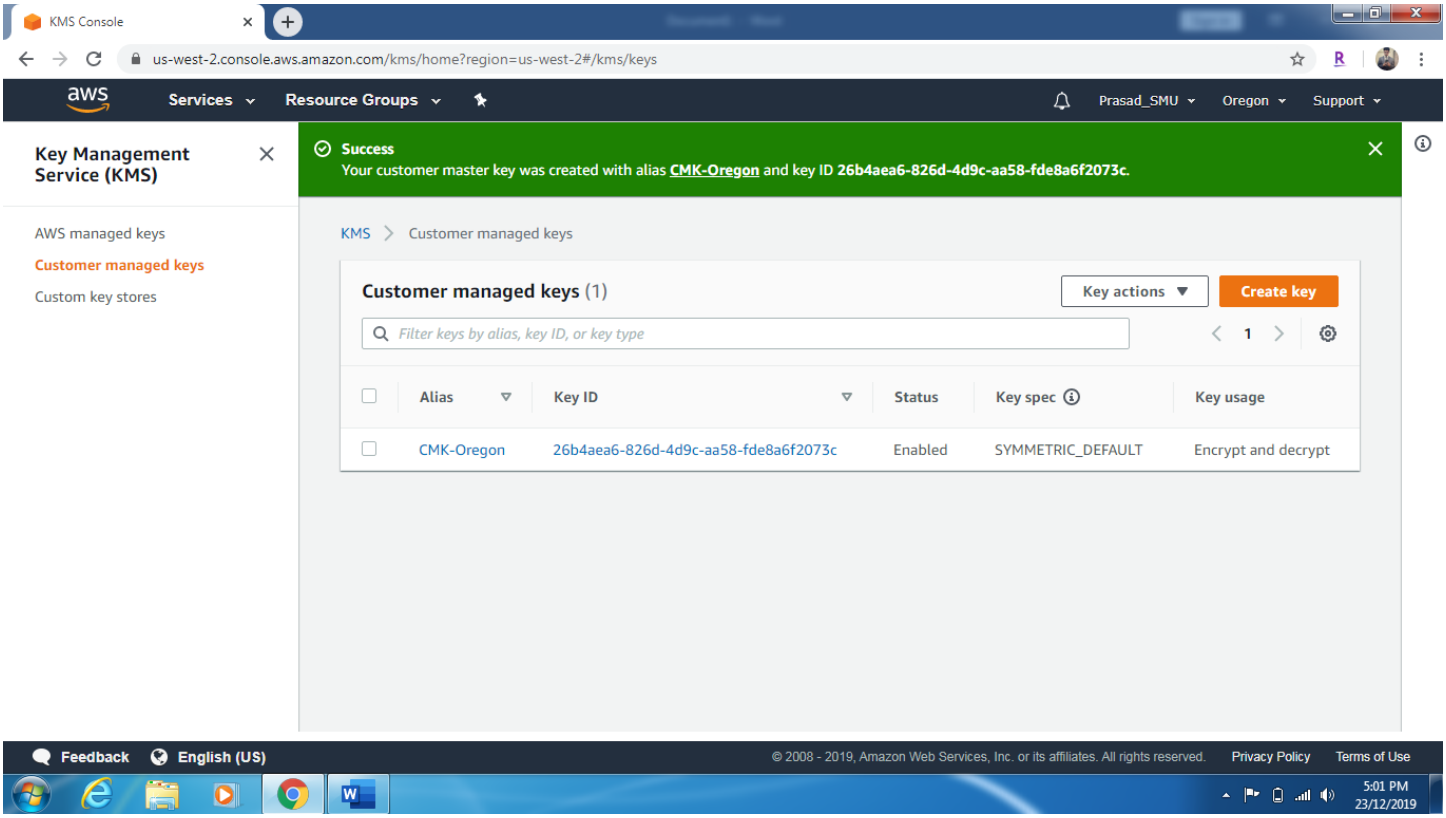
- Give Key Name as per your choice. **E.g. CMK-Oregon**



- Click Next and review the Key Policy. **Enable IAM User Permissions should be Allow**.



- Click on Finish, your Customer Managed Key has been successfully created.

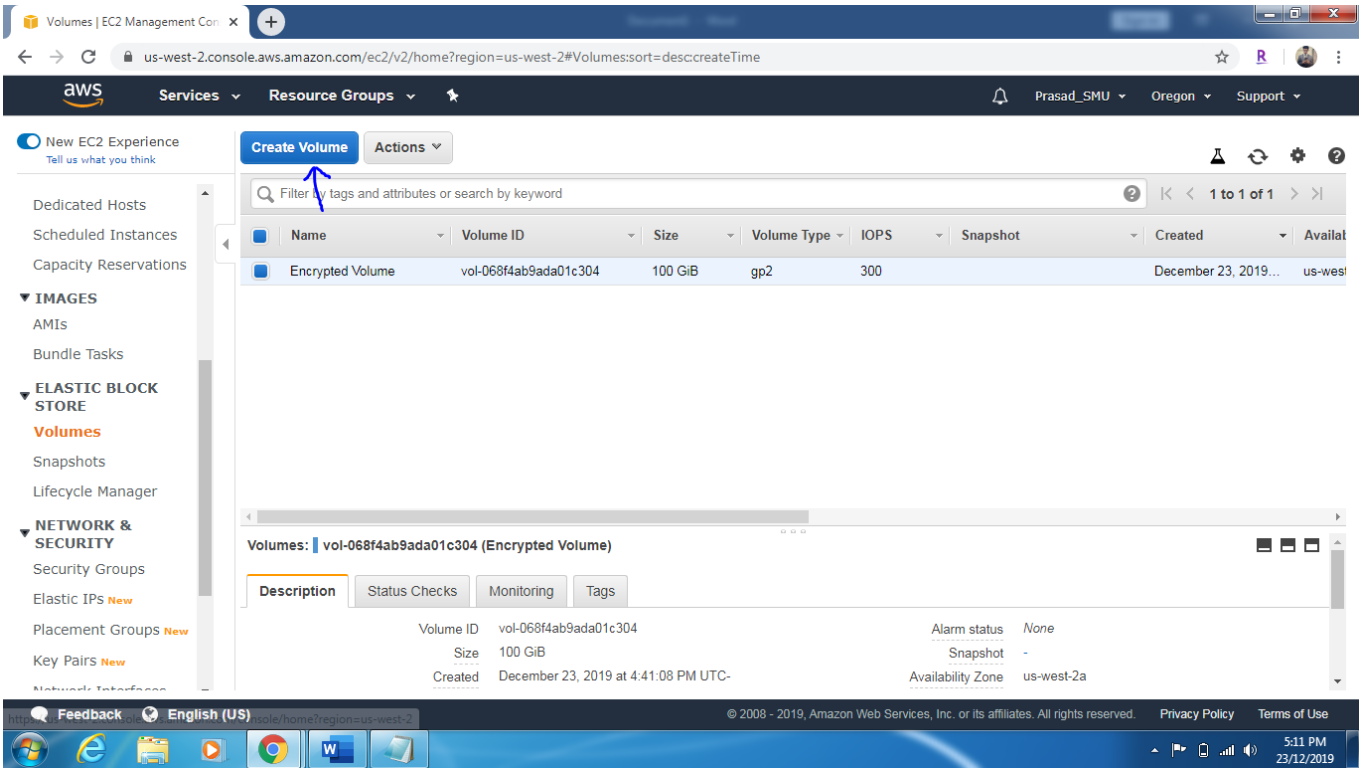


Make sure you've **TWO** different AWS Accounts in this Practical. In my case, below are my accounts.

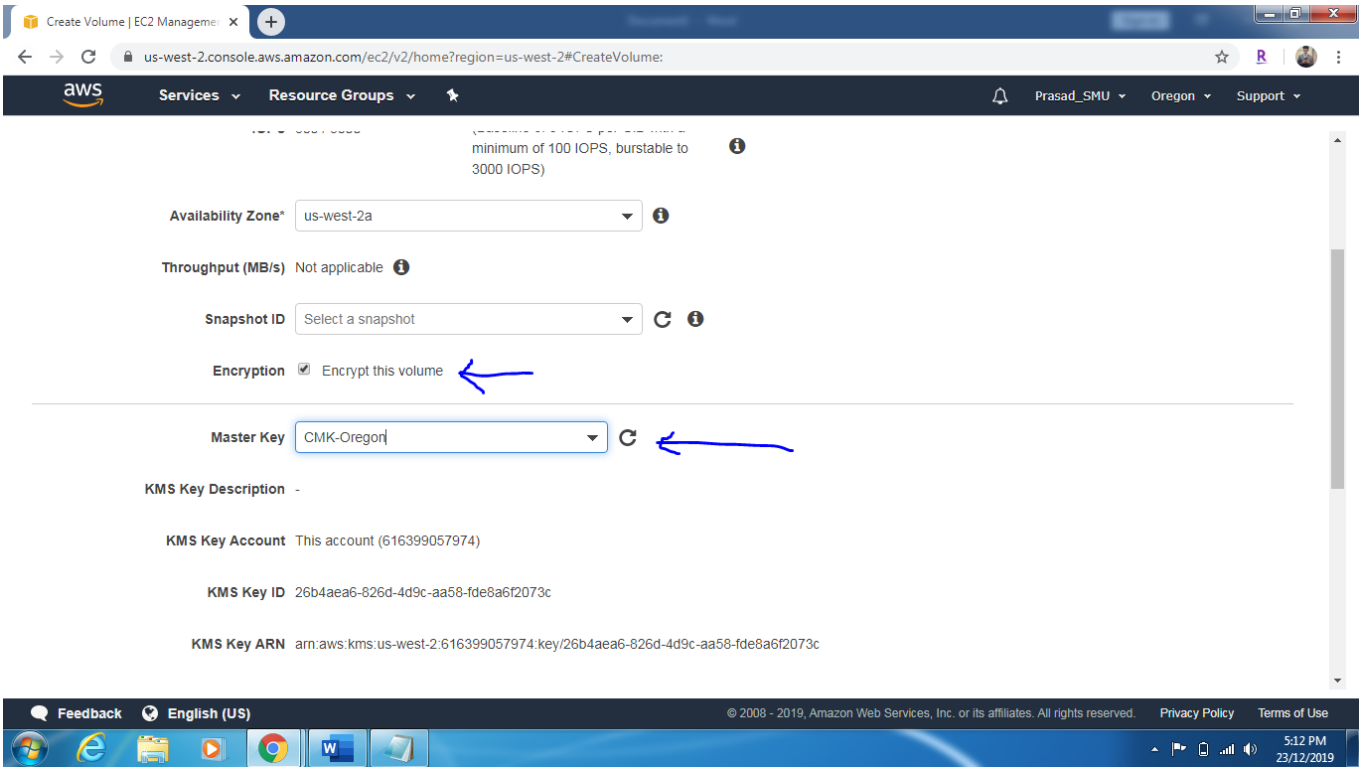
Account 1: 616399057974

Account 2: 450104983274

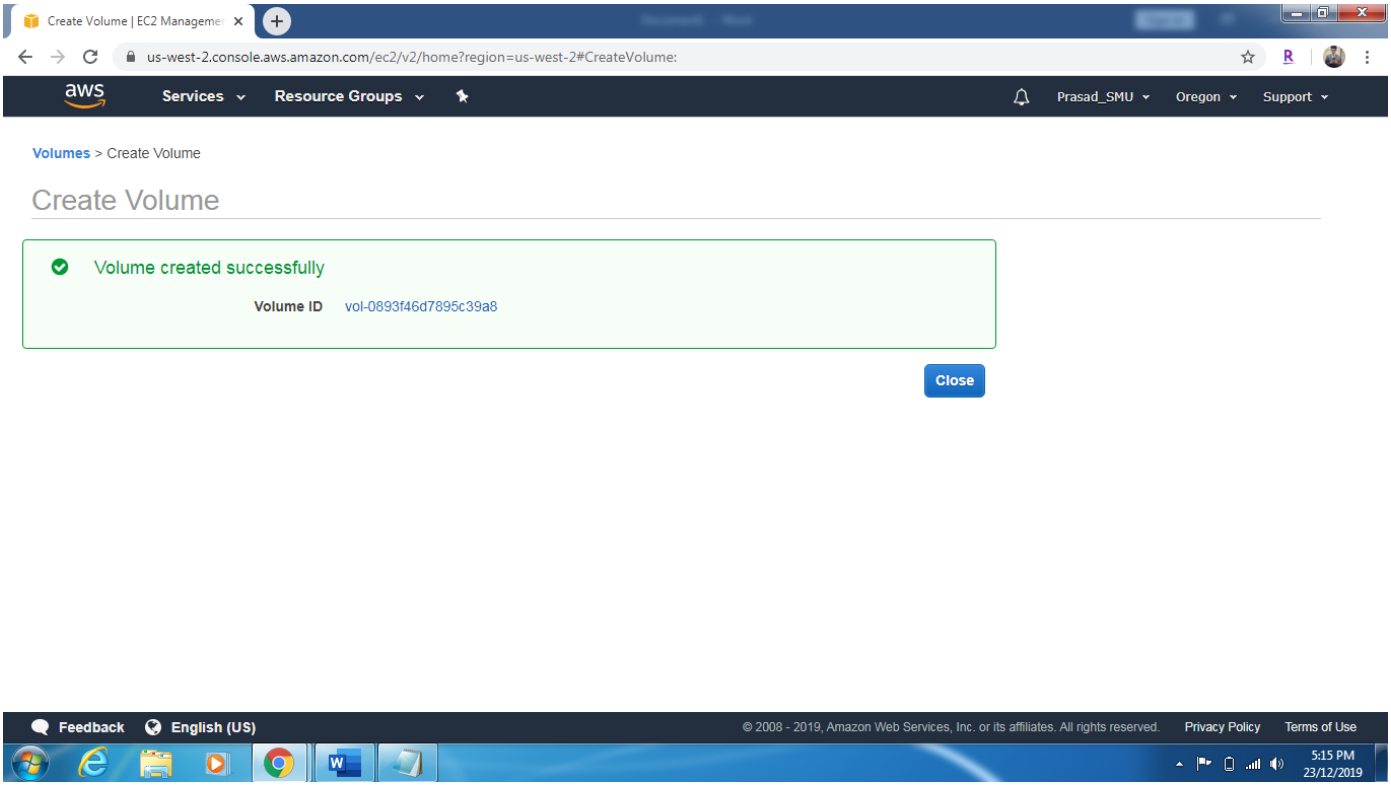
- Navigate to EC2 Service, Volume, and Click on Create Volume.



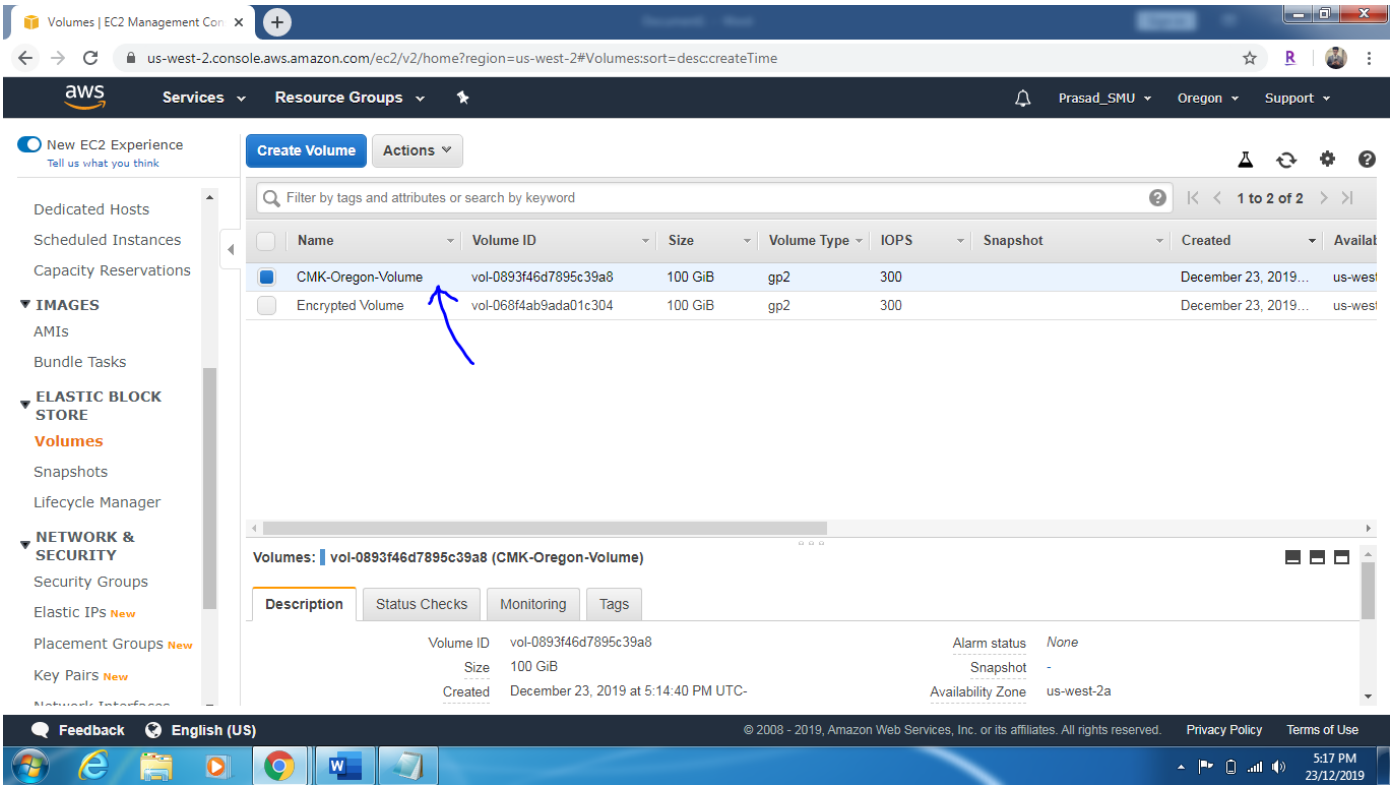
- Click on **Encrypt this volume** and select the newly created **Customer Managed Key** for Encryption and click on **Create Volume.**



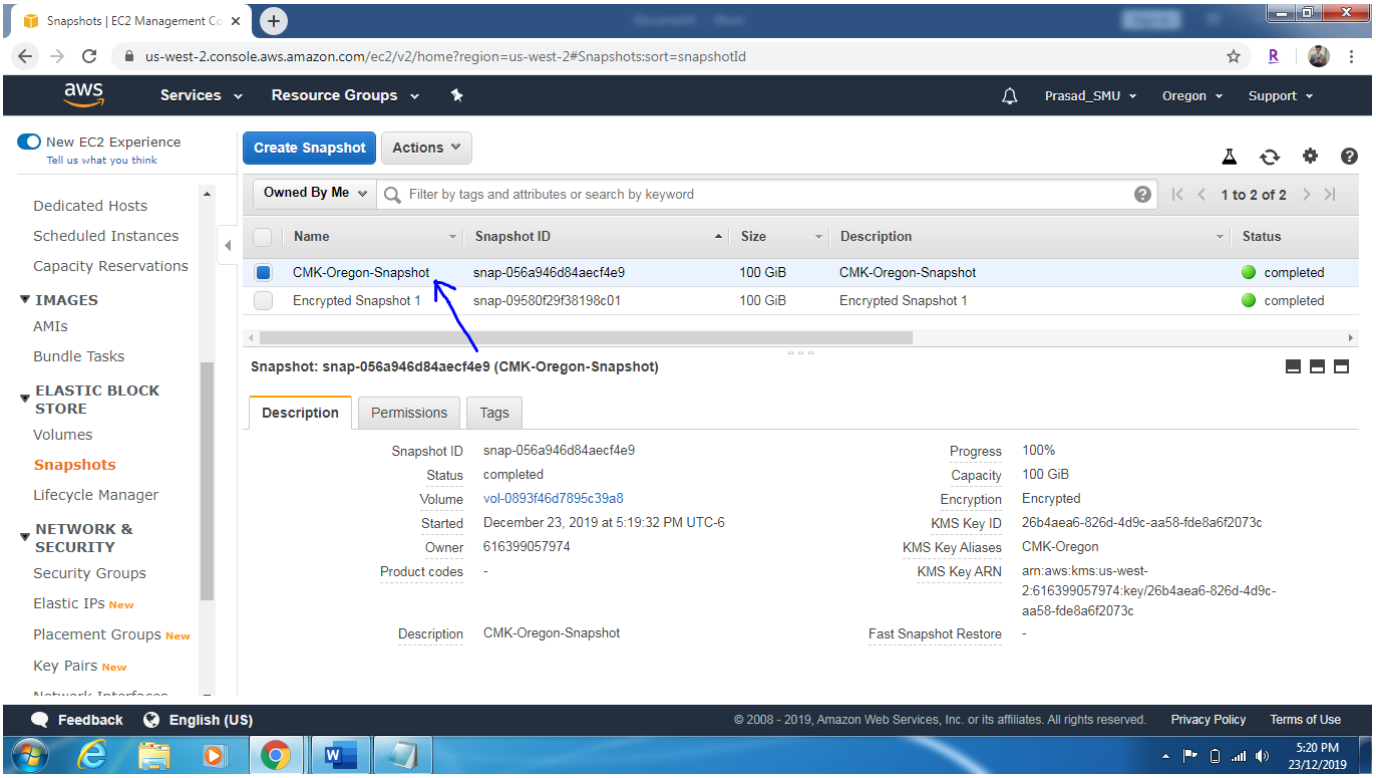
- Volume has been encrypted with Customer Managed Key.



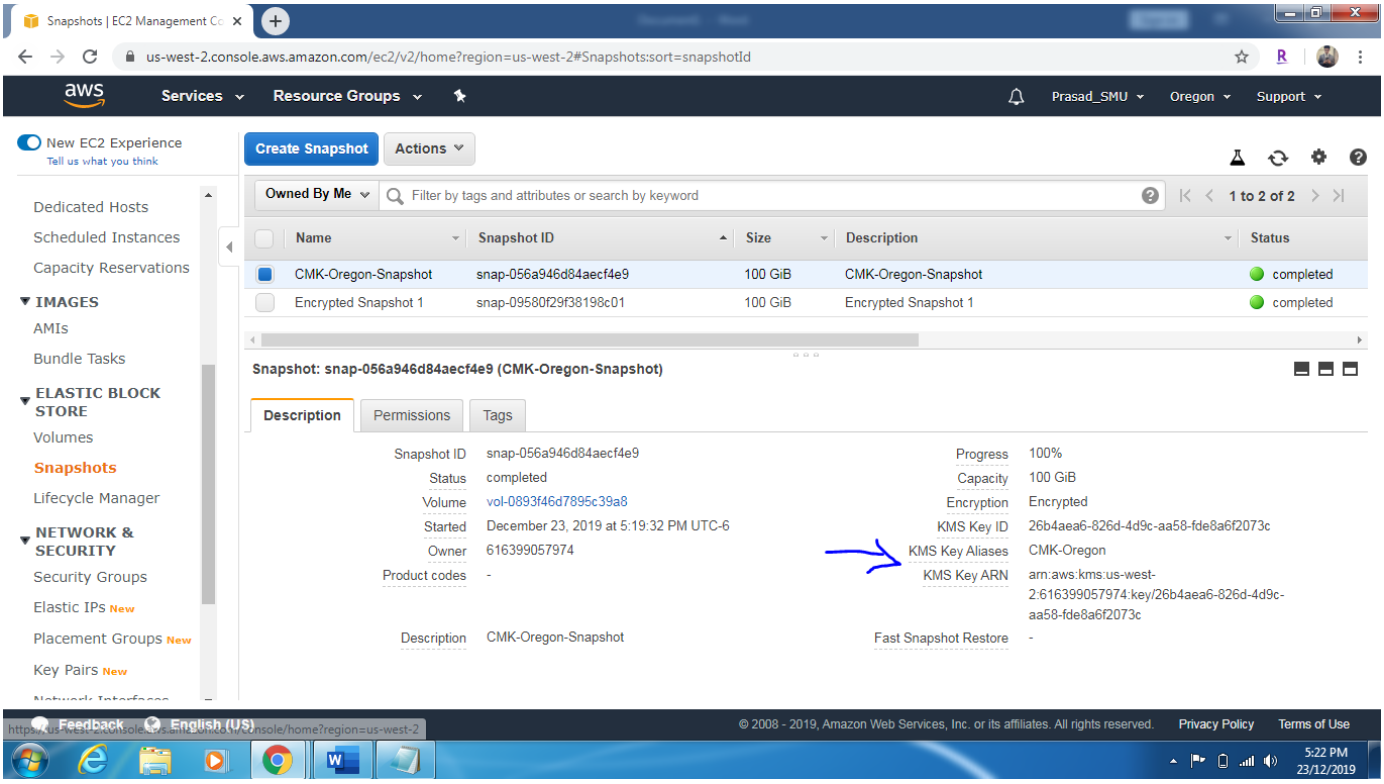
- Give Volume Name as per your choice **"CMK-Oregon-Volume".**



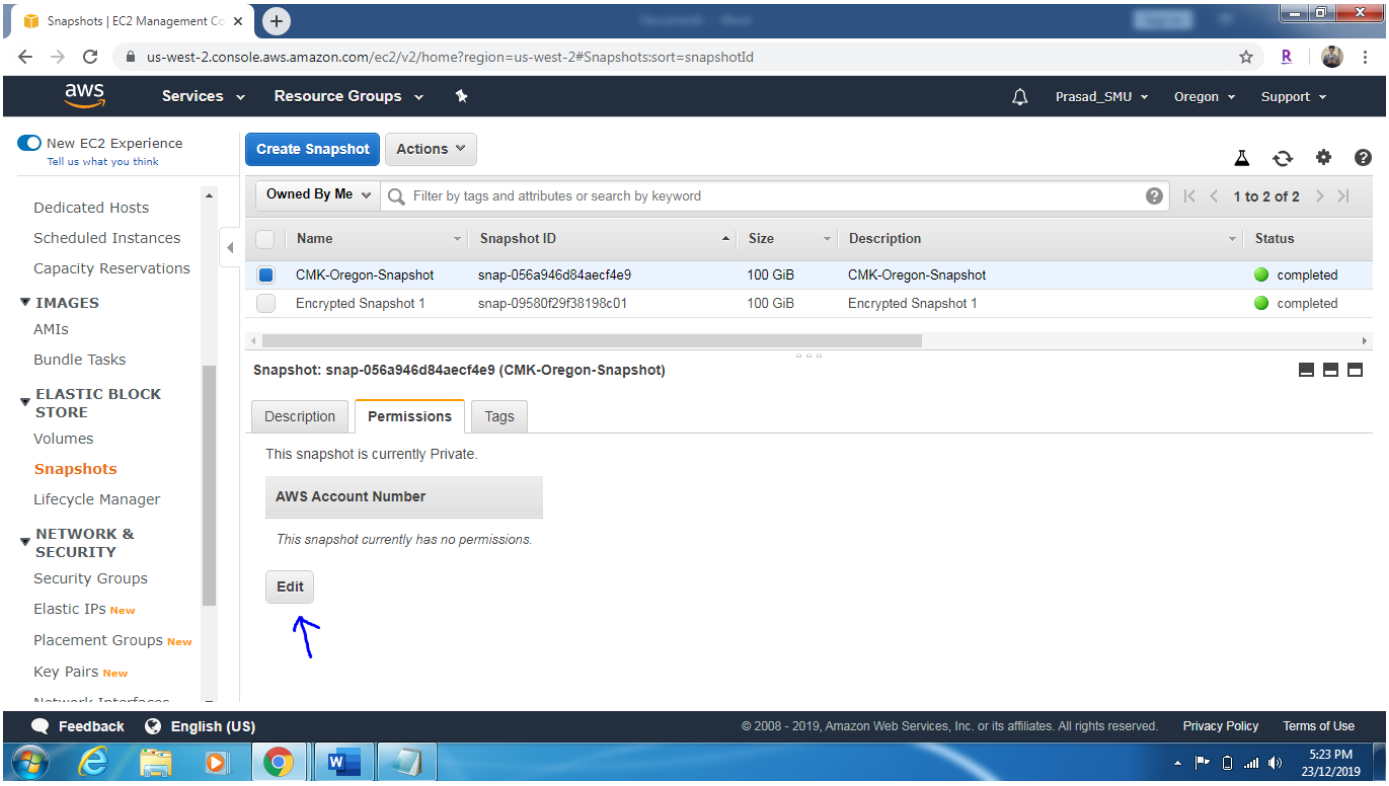
- Create a Snapshot of the Volume "CMK-Oregon-Volume" and give snapshot name as **"CMK-Oregon-Snapshot".**



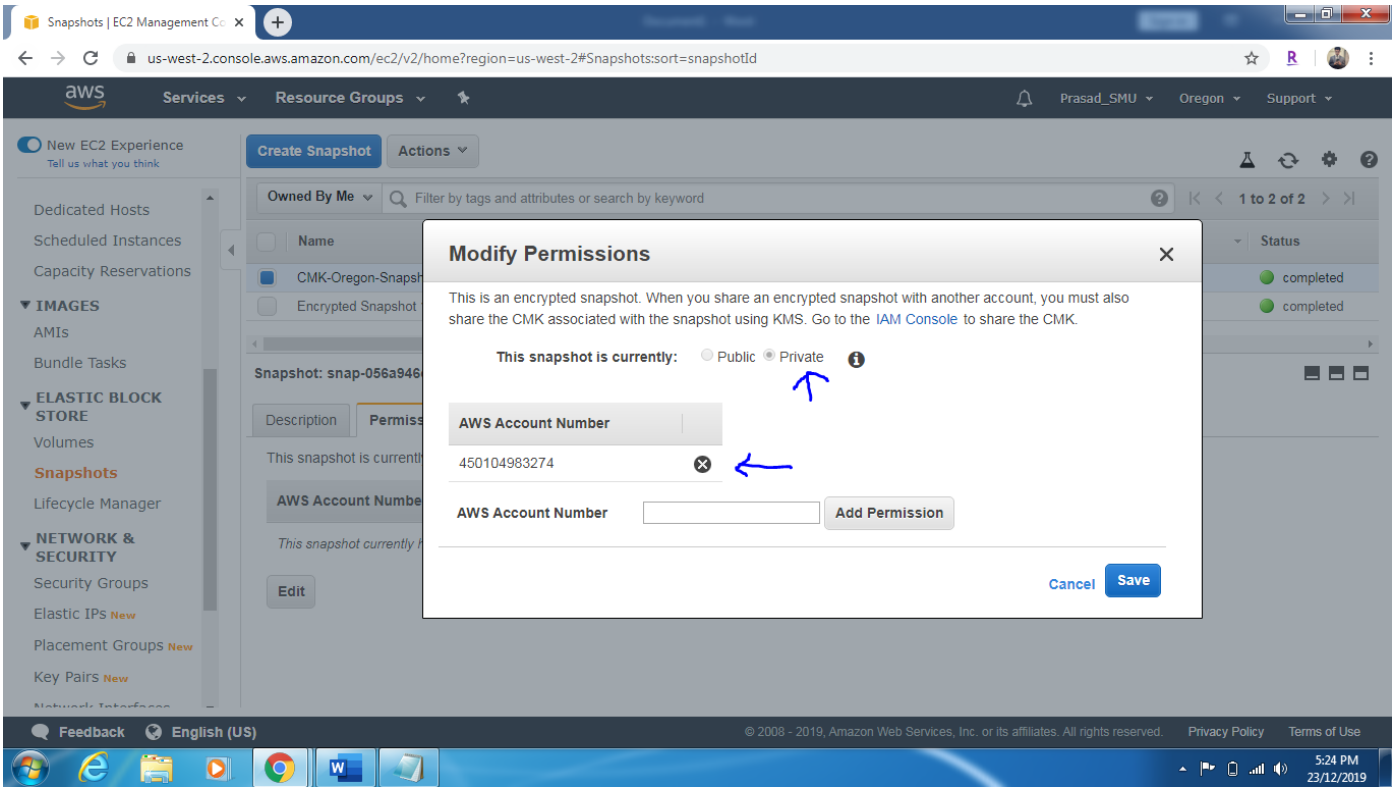
- Also, verify the Snapshot **Encryption.** Snapshot is also encrypted with newly created **Customer Managed Key**.



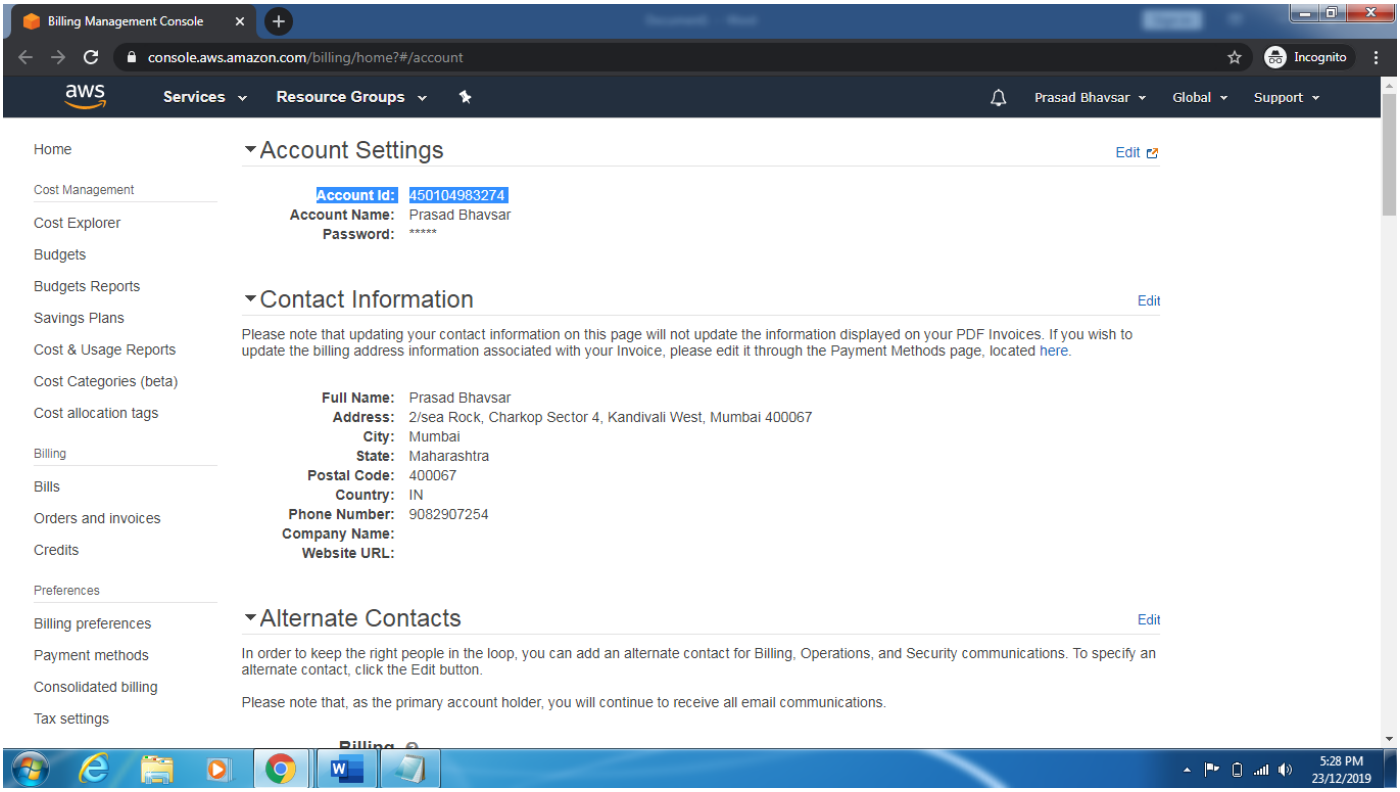
- Now click on **Snapshot Permissions** and Click on **Edit.**



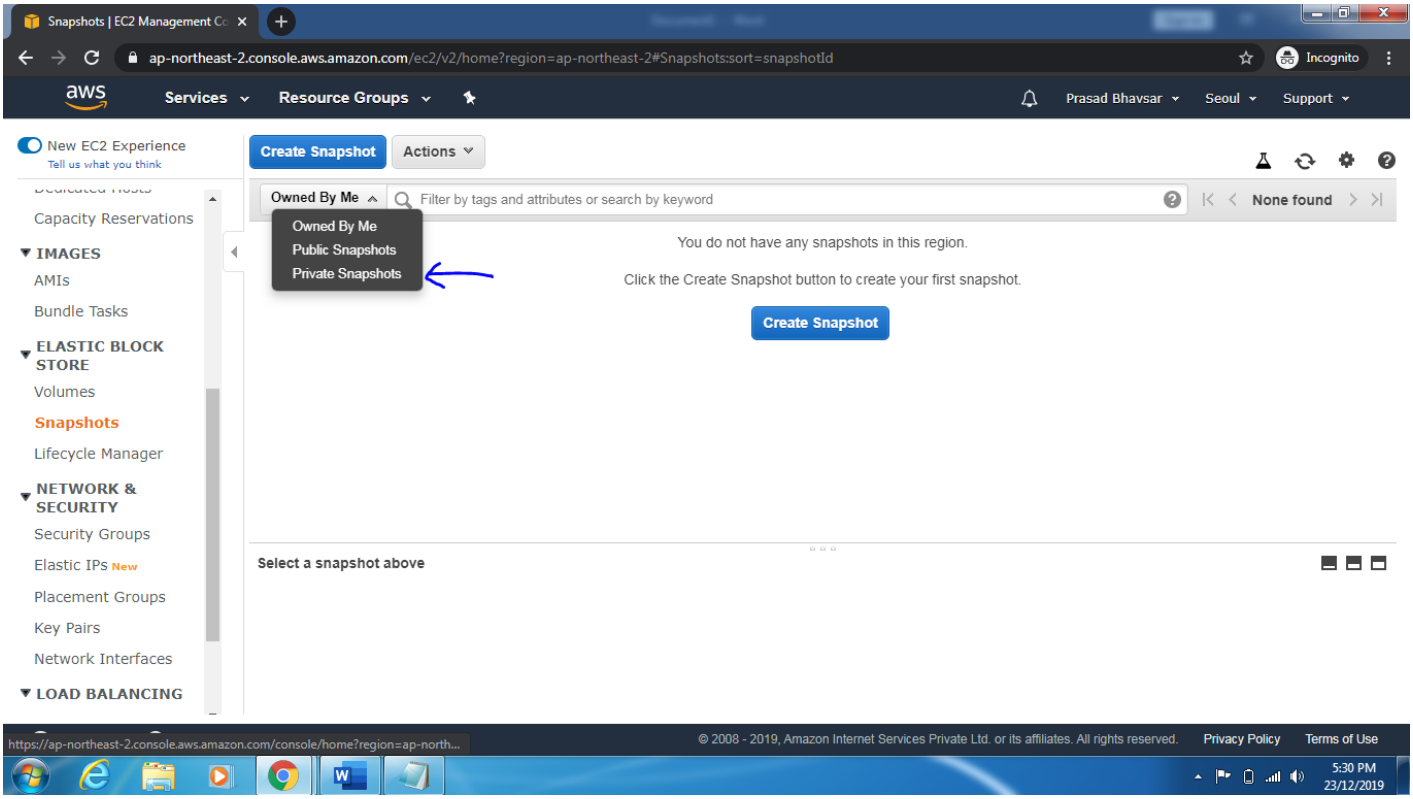
- Add another **AWS Account Number** and Keep the **Snapshot Private.**



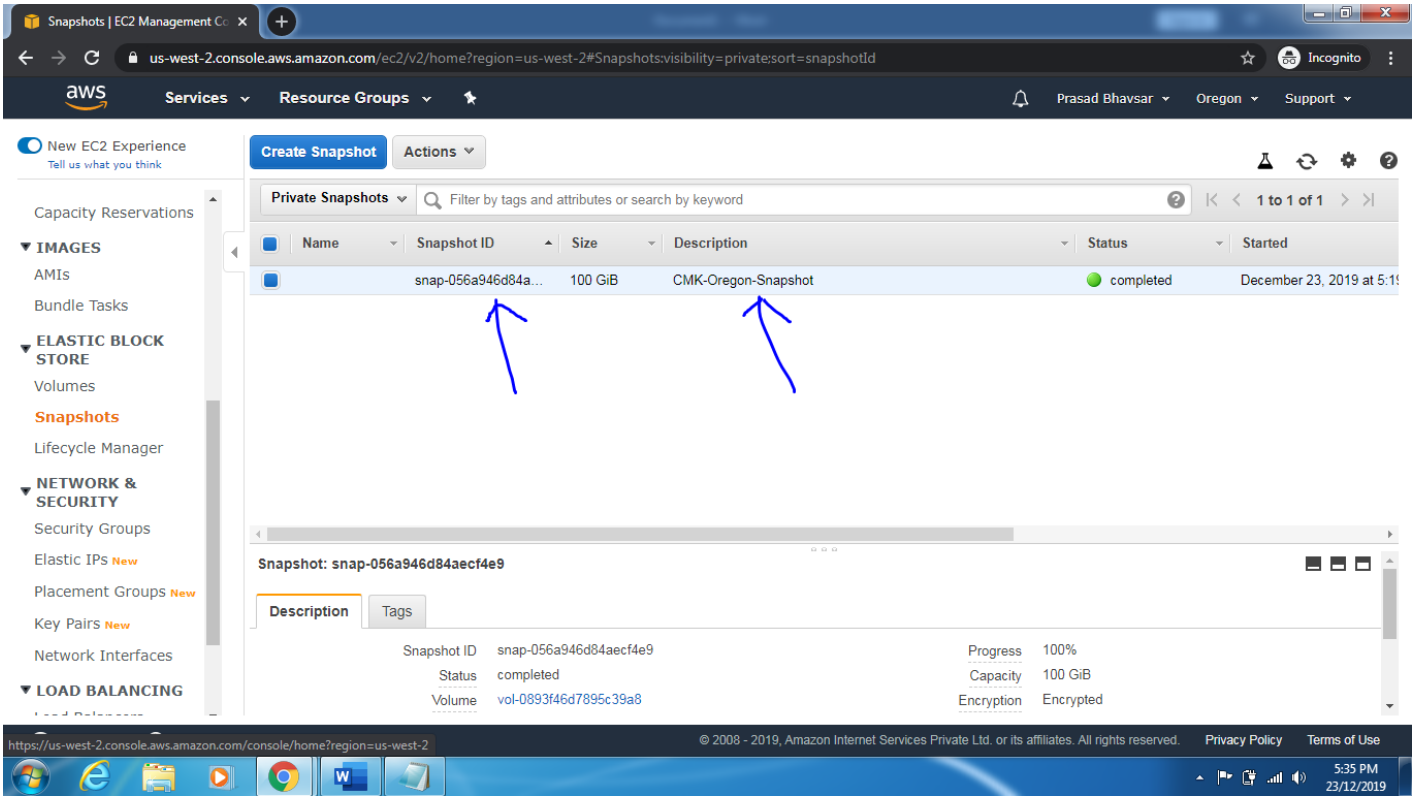
- Now login into another account (Account Id: 450104983274), make sure both the accounts are in **Same Region**.



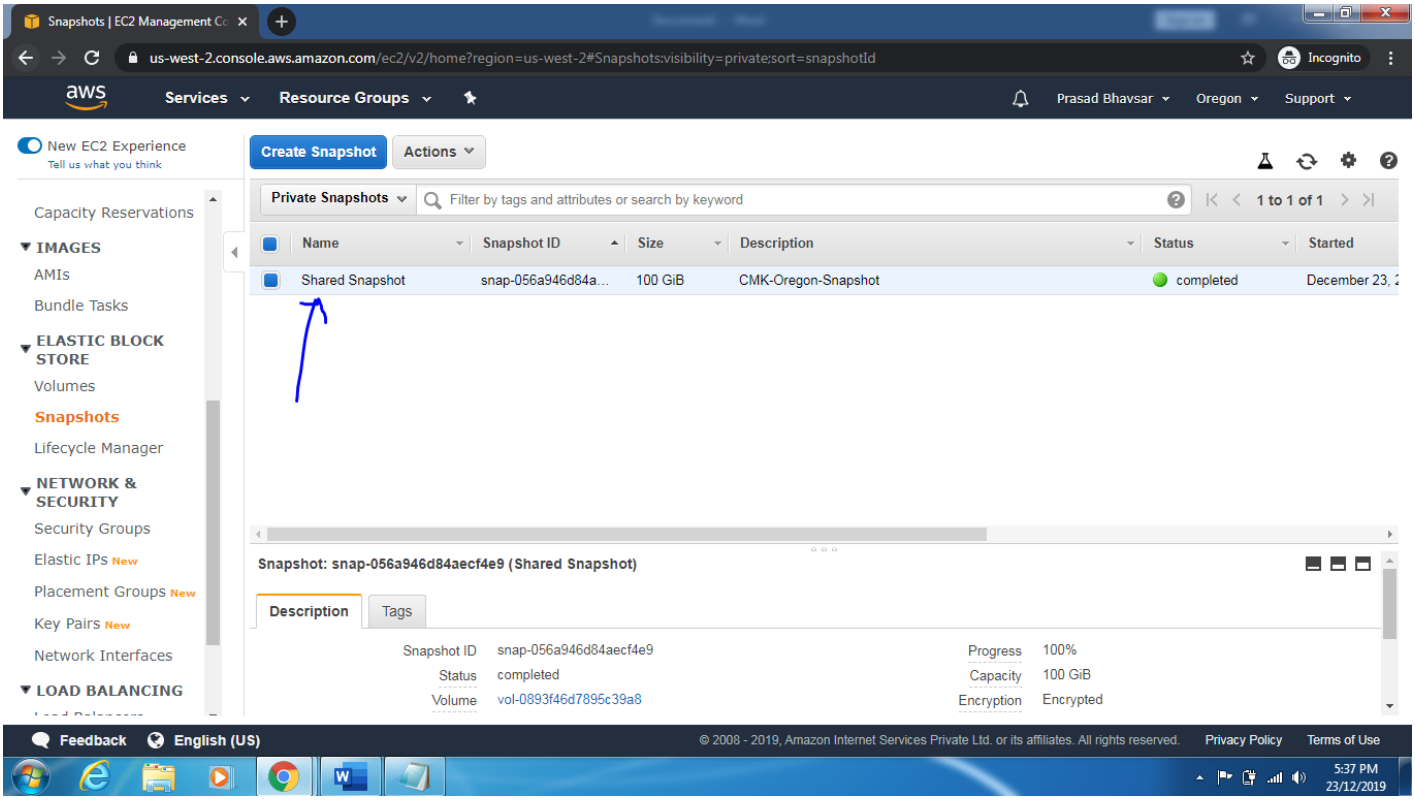
- On Another AWS Account, navigate to EC2 Service, Snapshots and click on **Private Snapshot**.



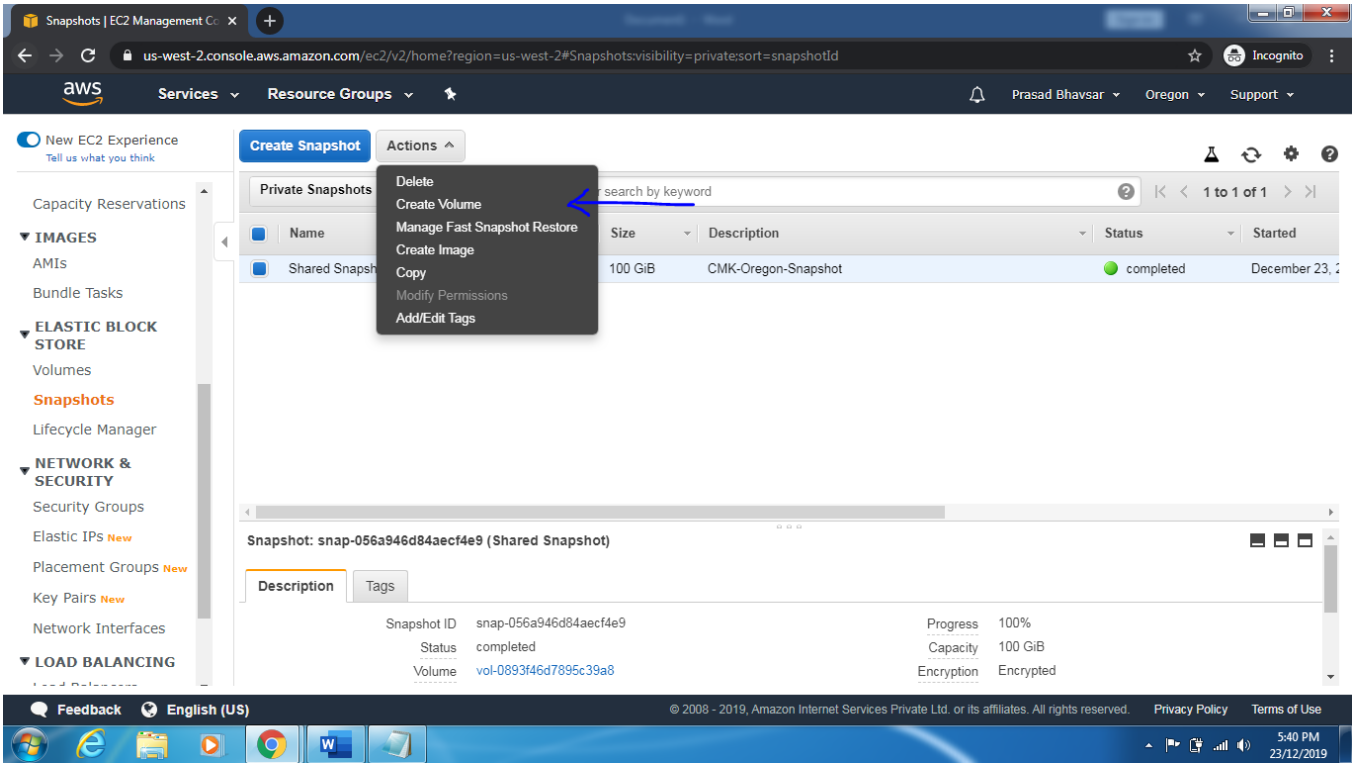
- Now you can see the **Shared Snapshot** from the first Account.



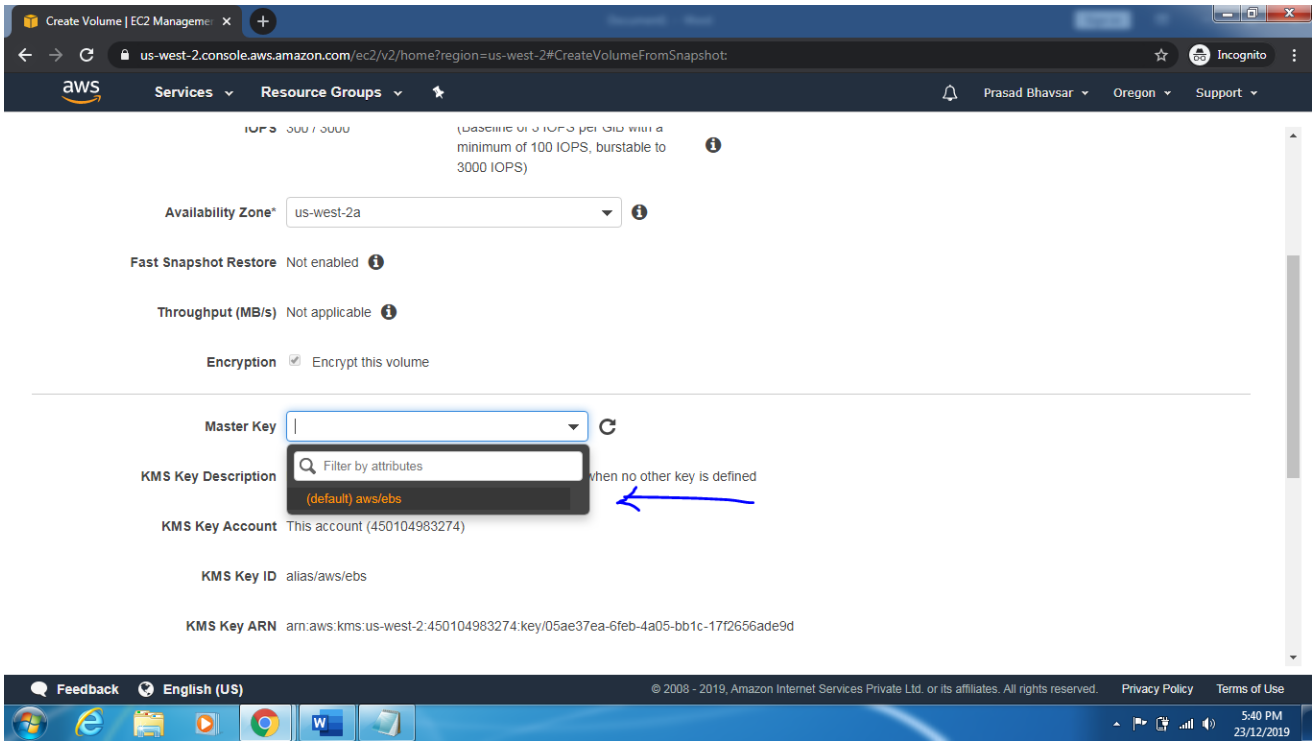
- Give the Snapshot Name as **"Shared Snapshot".**



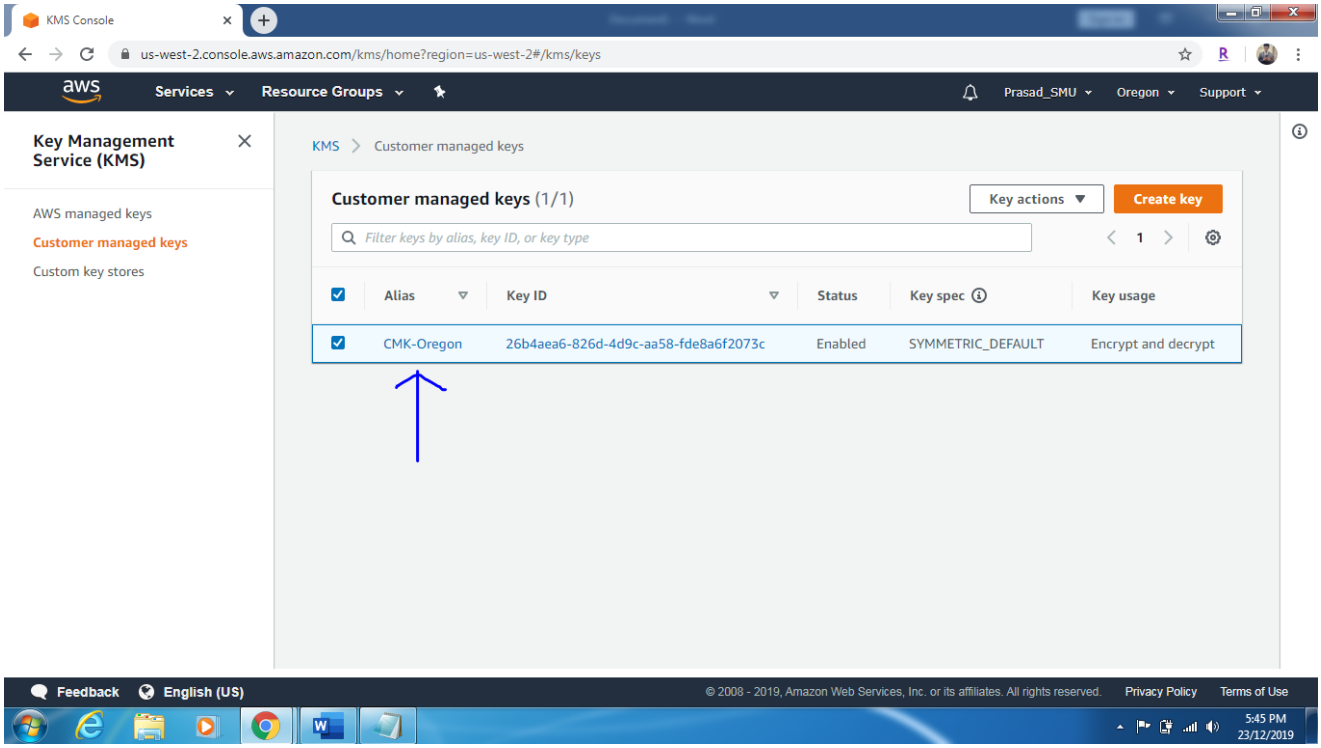
- Try to create a **New Volume** from the Shared Snapshot.



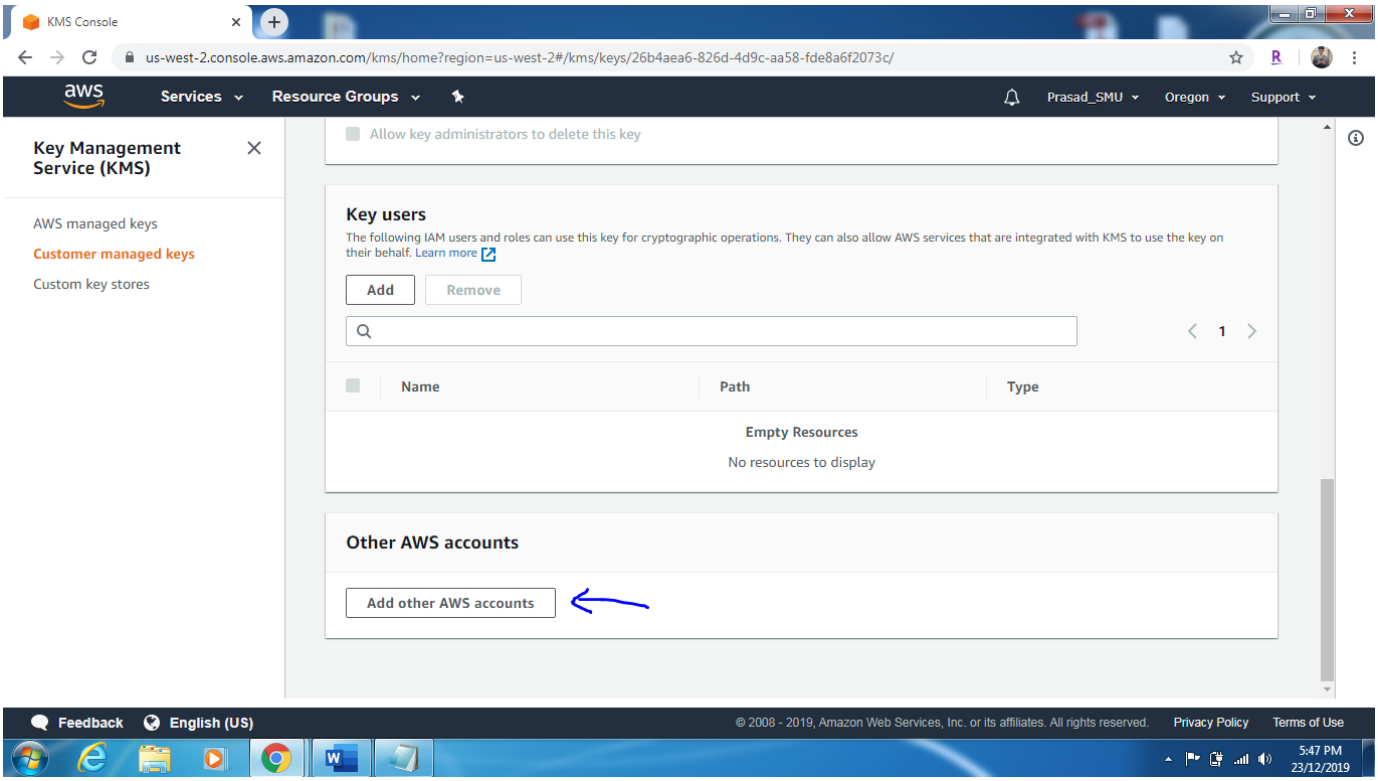
- While creating Snapshot from the Shared Snapshot, Second Account doesn't have access on **Customer Managed Key "CMK-Oregon"**. Hence even if you create a new Volume from Shared Snapshot, Volume won't be visible under EBS Volume Tab.

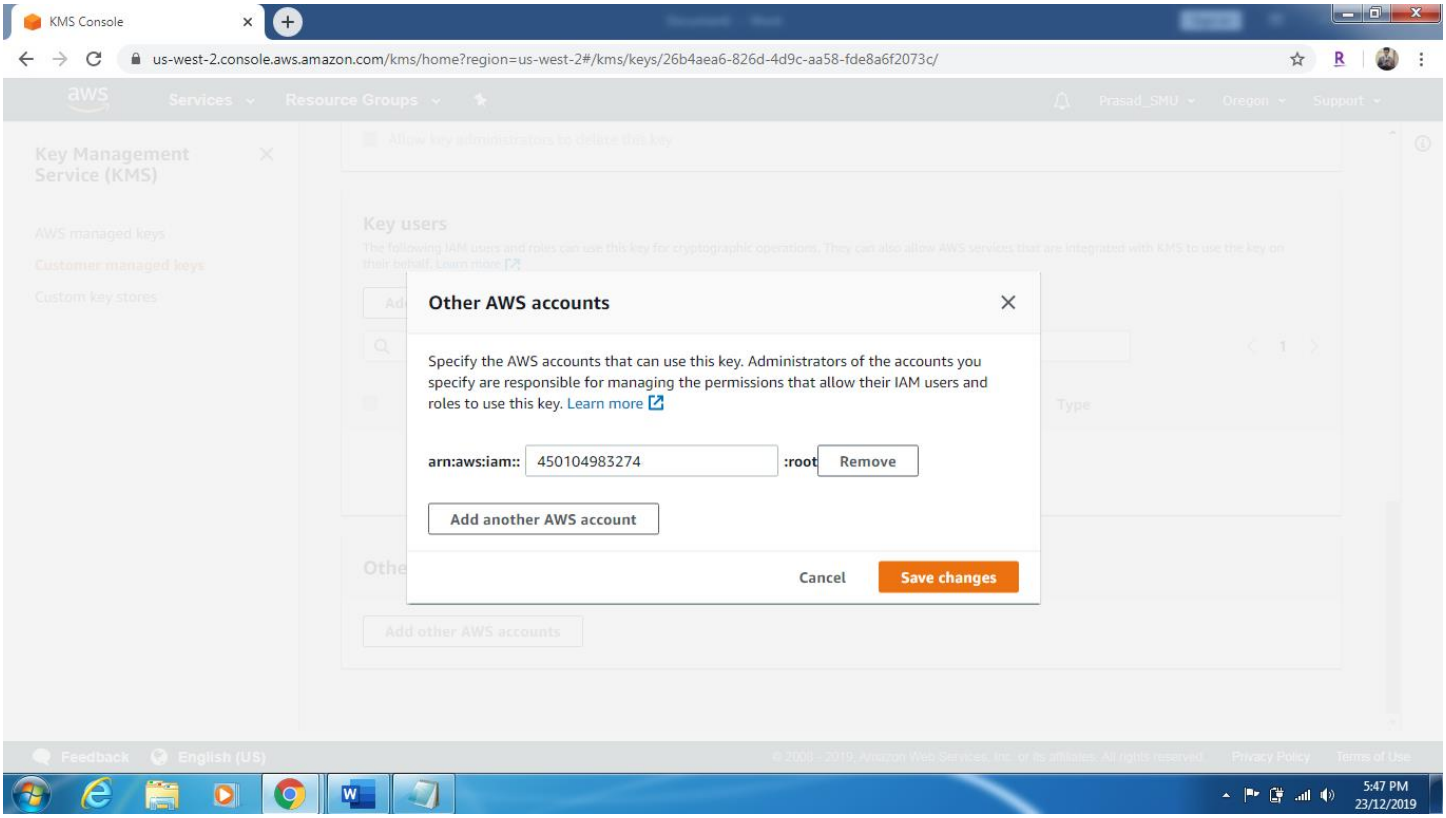


- To avoid this, go back to your First Account and Navigate to **"Key Management Service".** Select the **Customer Managed Service** that you've created.

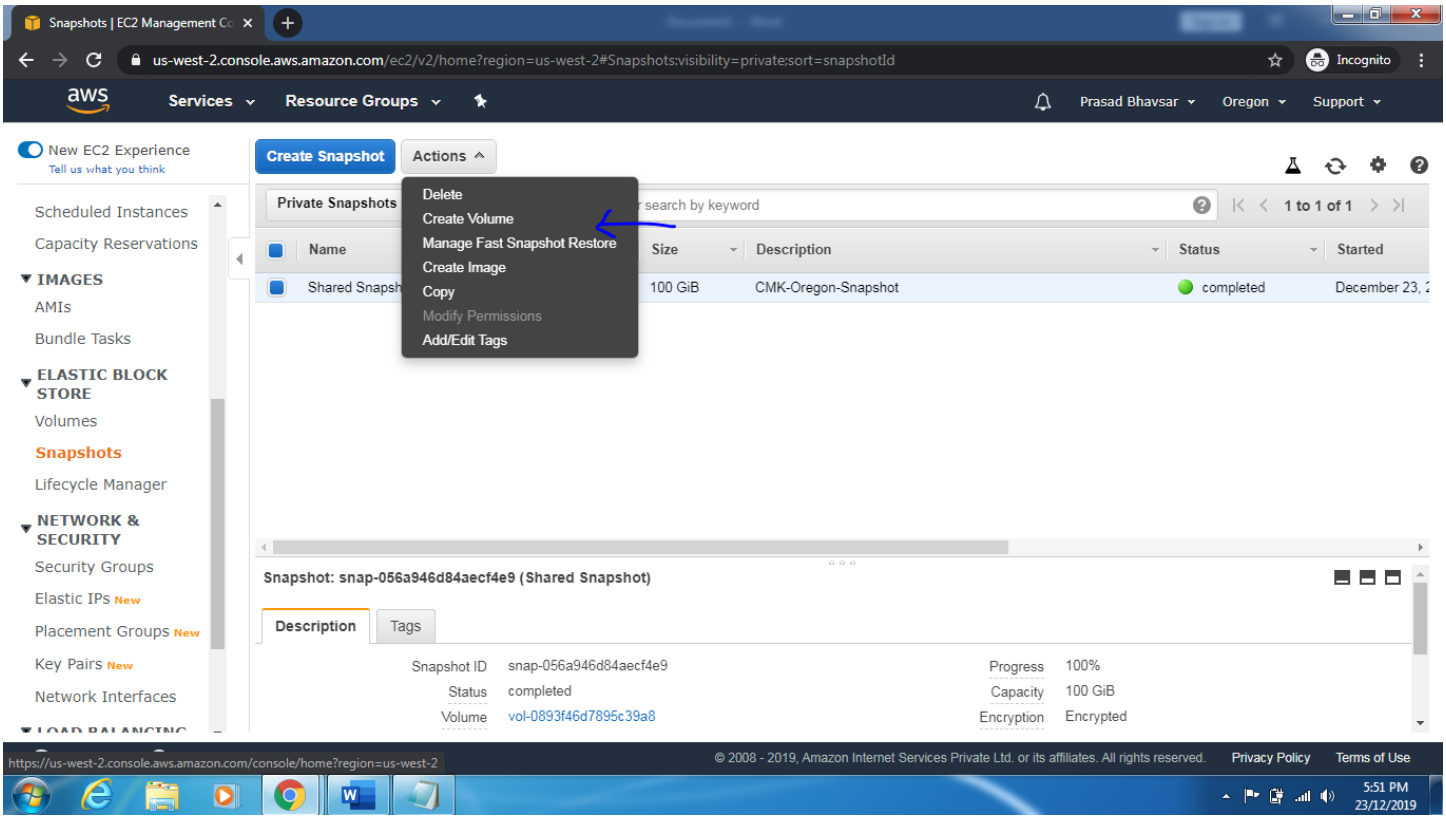


- Click on **Add other AWS Account** and put **Account ID** of the Second AWS Account.





- Now go back to Second Account and try to create new **Volume** from the Shared Snapshot.



- **New volume** has been successfully created by granting access to **Customer Managed Key**.

NOTES

- When you share a snapshot of a Volume, you're actually sharing all the data on that volume used to create a snapshot.
- You can share your unencrypted snapshot with the "AWS Community" by making it **Public** or share with a Selected AWS Account by making it **Private**.
- You cannot make your encrypted snapshot **Public**.
- You can share your encrypted snapshot with specific AWS Accounts by making it Private and by giving access to **Customer Managed Keys**. (Not default AWS Keys).

This completes the Lab on Encryption with Key Management Service (KMS).

For Questions, contact me on pbhavsar@smu.edu .