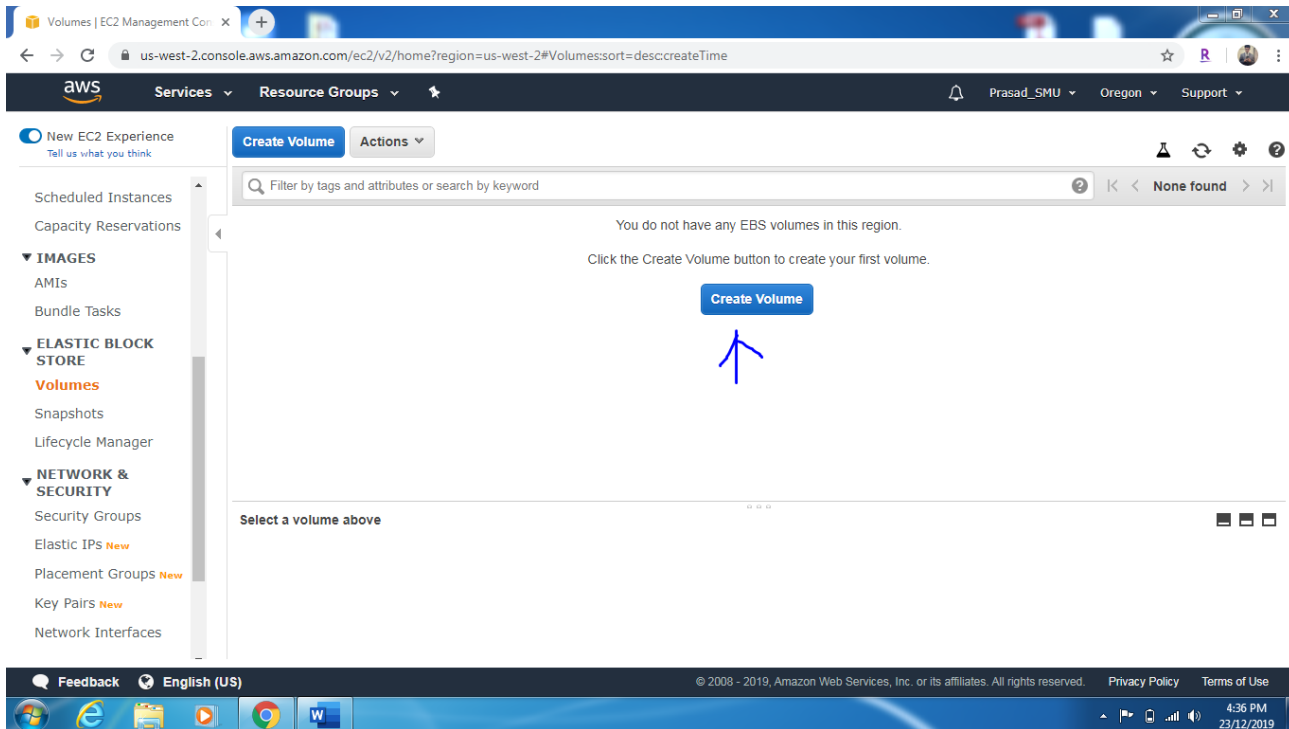


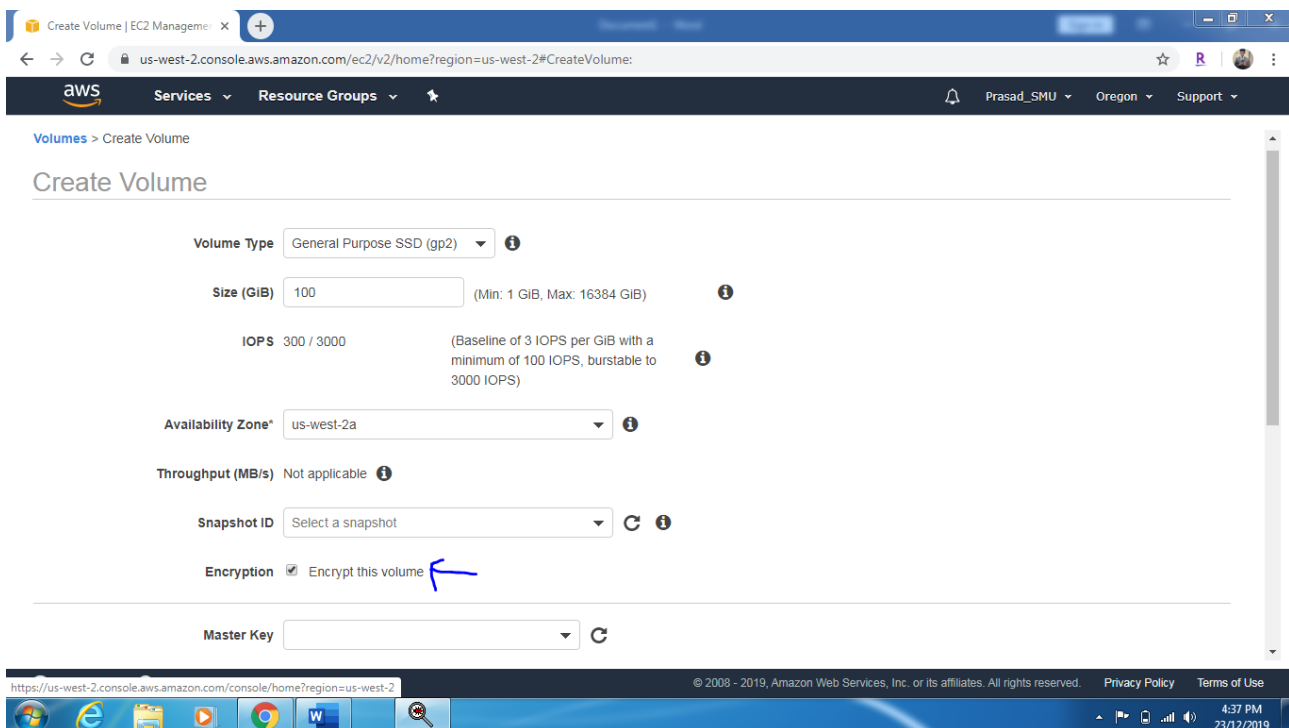
EBS Volume and Snapshot Encryption with Key Management Service (KMS)

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

The screenshot shows the AWS Management Console 'Create Volume' page. The 'Availability Zone' is set to 'us-west-2a'. 'Throughput (MB/s)' is 'Not applicable'. 'Snapshot ID' is 'Select a snapshot'. Under 'Encryption', the checkbox 'Encrypt this volume' is checked. The 'Master Key' dropdown is set to '(default) aws/ebs', with a blue arrow pointing to the refresh icon. Below this, the 'KMS Key Description' is 'Default master key that protects my EBS volumes when no other key is defined', the 'KMS Key Account' is 'This account (616399057974)', the 'KMS Key ID' is 'alias/aws/ebs', and the 'KMS Key ARN' is 'arn:aws:kms:us-west-2:616399057974:key/ad811fc2-835e-44ac-9032-f23f5c25ee47'. The bottom of the console shows a Windows taskbar with the time 4:40 PM on 23/12/2019.

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

The screenshot shows the AWS Management Console 'Create Volume' page after successful creation. A green message box states 'Volume created successfully' with the 'Volume ID' 'vol-068f4ab9ada01c304'. A 'Close' button is visible. The bottom of the console shows a Windows taskbar with the time 4:41 PM on 23/12/2019.

- Give the Volume name as “Encrypted Volume”.

The screenshot shows the AWS Management Console interface. In the left-hand navigation pane, the 'ELASTIC BLOCK STORE' section is expanded, and 'Volumes' is selected. The main content area displays a table of volumes. A blue arrow points to the volume named 'Encrypted Volume'.

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone
Encrypted Volume	vol-068f4ab9ada01c304	100 GiB	gp2	300	-	December 23, 2019...	us-west-2a

Below the table, the 'Description' tab is selected for the volume 'vol-068f4ab9ada01c304 (Encrypted Volume)'. The details shown are:

- Volume ID: vol-068f4ab9ada01c304
- Size: 100 GiB
- Created: December 23, 2019 at 4:41:08 PM UTC-
- Alarm status: None
- Snapshot: -
- Availability Zone: us-west-2a

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

This screenshot shows the 'Description' tab for the volume 'vol-068f4ab9ada01c304'. A blue arrow points to the 'Encryption' section, which indicates that the volume is encrypted.

Property	Value
Volume ID	vol-068f4ab9ada01c304
Size	100 GiB
Created	December 23, 2019 at 4:41:08 PM UTC-6
State	available
Attachment information	
Volume type	gp2
Product codes	-
Alarm status	None
Snapshot	-
Availability Zone	us-west-2a
Encryption	Encrypted
KMS Key ID	ad811fc2-835e-44ac-9032-f23f5c25ee47
KMS Key Aliases	aws/ebs
KMS Key ARN	arn:aws:kms:us-west-2:616399057974:key/ad811fc2-835e-44ac-9032-f23f5c25ee47

➤ Now go to Actions and Click on “Create Snapshot”.

The screenshot shows the AWS Management Console interface. On the left, the navigation pane includes sections for 'IMAGES' (AMIs, Bundle Tasks) and 'ELASTIC BLOCK STORE' (Volumes, Snapshots, Lifecycle Manager). The 'Volumes' section is selected. The main content area displays a table of volumes. A context menu is open over a volume, with the 'Create Snapshot' option highlighted by a blue arrow. Below the table, the details for the selected volume 'vol-068f4ab9ada01c304 (Encrypted Volume)' are shown, including its ID, size (100 GiB), type (gp2), IOPS (300), and creation time (December 23, 2019 at 4:41:08 PM UTC).

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

The screenshot shows the 'Create Snapshot' page in the AWS Management Console. The 'Volume' field is set to 'vol-068f4ab9ada01c304'. The 'Description' field is empty. The 'Encrypted' checkbox is checked, indicated by a blue arrow. Below this, there are fields for 'Key' and 'Value' for tagging. At the bottom, there is a section for adding tags, with a note that the resource currently has no tags. The 'Create Snapshot' button is visible at the bottom right.

- Give the Snapshot name as “Encrypted Snapshot 1” and click on Create Snapshot.

Create Snapshot | EC2 Management Console

us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#CreateSnapshotFromVolume:

Volumes > Create Snapshot

Create Snapshot

Volume vol-068f4ab9ada01c304 ⓘ

Description Encrypted Snapshot 1 ⓘ

Encrypted Encrypted ⓘ

Key (128 characters maximum) Value (256 characters maximum)

This resource currently has no tags

Choose the Add tag button or click to add a Name tag

Add Tag 50 remaining (Up to 50 tags maximum)

* Required

Cancel Create Snapshot

Feedback English (US) © 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use 4:48 PM 23/12/2019

Snapshots | EC2 Management Console

us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Snapshots:sort=snapshotId

New EC2 Experience Tell us what you think

Scheduled Instances Capacity Reservations

IMAGES AMIs Bundle Tasks

ELASTIC BLOCK STORE Volumes Snapshots Lifecycle Manager

NETWORK & SECURITY Security Groups Elastic IPs New Placement Groups New Key Pairs New Network Interfaces

Create Snapshot Actions

Owned By Me Filter by tags and attributes or search by keyword

Name	Snapshot ID	Size	Description	Status
Encrypted Snapshot 1	snap-09580f29f38198c01	100 GiB	Encrypted Snapshot 1	completed

Snapshot: snap-09580f29f38198c01 (Encrypted Snapshot 1)

Description Permissions Tags

Snapshot ID	snap-09580f29f38198c01	Progress	100%
Status	completed	Capacity	100 GiB
Volume	vol-068f4ab9ada01c304	Encryption	Encrypted
Started	December 23, 2019 at 4:49:44 PM UTC-6	KMS Key ID	ad811fc2-835e-44ac-9032-f23f5c25ee47
Owner	616399057974	KMS Key Aliases	aws/ebs
Product codes	-	KMS Key ARN	arn:aws:kms:us-west-2:616399057974:key/ad811fc2-835e-44ac-9032-f23f5c25ee47
Description	Encrypted Snapshot 1	Fast Snapshot Restore	-

Feedback English (US) © 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use 4:50 PM 23/12/2019

- 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.

The screenshot shows the AWS Management Console interface. On the left, the navigation menu includes 'New EC2 Experience', 'Scheduled Instances', 'Capacity Reservations', 'IMAGES', 'ELASTIC BLOCK STORE', and 'NETWORK & SECURITY'. The 'Snapshots' section under 'ELASTIC BLOCK STORE' is highlighted. The main content area shows a table of snapshots with one entry: 'Encrypted Snapshot 1' with ID 'snap-09580f29f38198c01' and size '100 GiB'. Below the table, the details for 'Snapshot: snap-09580f29f38198c01 (Encrypted Snapshot 1)' are displayed. The 'Description' tab is active, showing metadata such as 'Snapshot ID', 'Status' (completed), 'Volume' (vol-068f4ab9ada01c304), 'Started' (December 23, 2019 at 4:49:44 PM UTC-6), 'Owner' (616399057974), and 'Product codes'. The 'Permissions' tab is also visible, showing 'Progress' (100%), 'Capacity' (100 GiB), 'Encryption' (Encrypted), 'KMS Key ID' (ad811fc2-835e-44ac-9032-f23f5c25ee47), 'KMS Key Aliases' (aws/ebs), 'KMS Key ARN' (arn:aws:kms:us-west-2:616399057974:key/ad811fc2-835e-44ac-9032-f23f5c25ee47), and 'Fast Snapshot Restore' (-). A blue arrow points to the 'KMS Key ID' field.

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

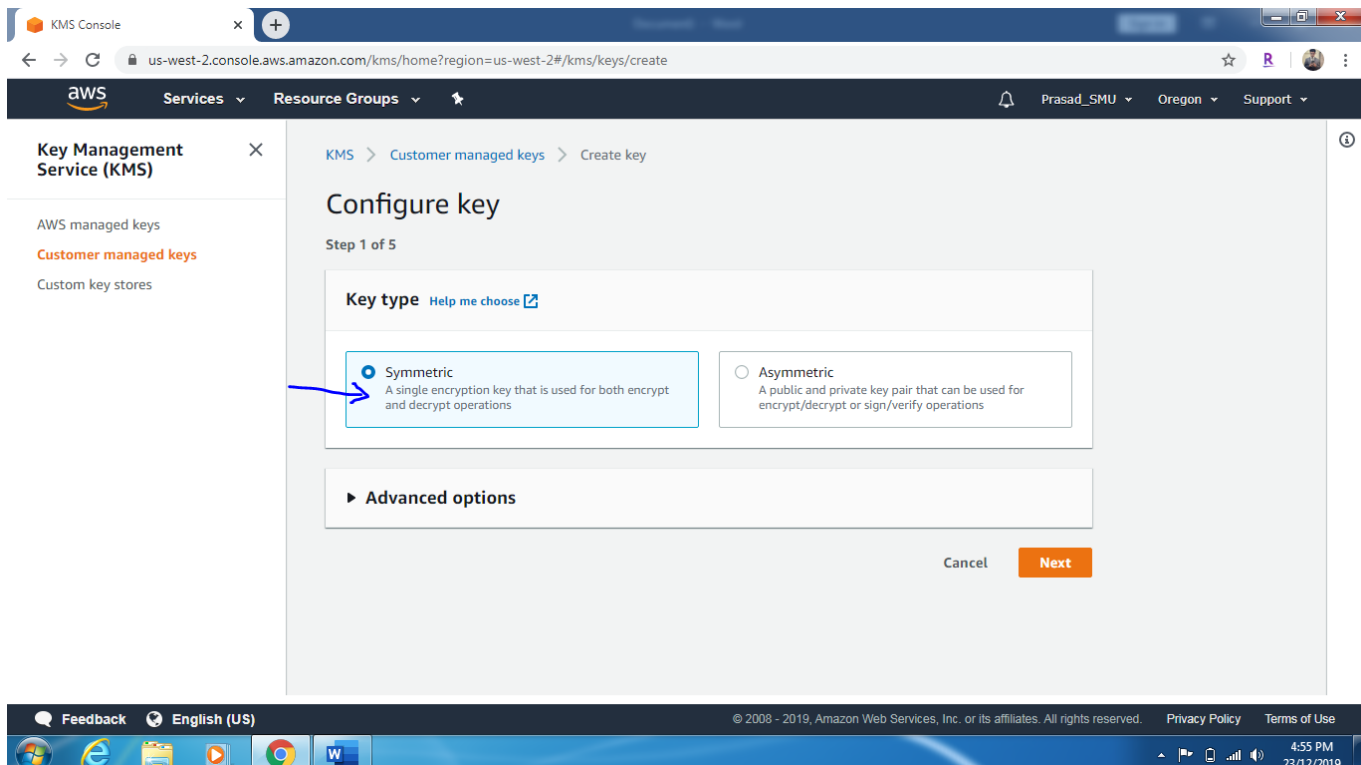
In the Next Task, we'll see how to encrypt a Volume and Snapshot using Customer Managed Key.

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

The screenshot shows the AWS KMS Console interface. The left sidebar displays 'Key Management Service (KMS)' with options for 'AWS managed keys', 'Customer managed keys' (selected), and 'Custom key stores'. The main content area is titled 'Add labels' and is 'Step 2 of 5'. It contains a section 'Create alias and description' with a text input field for 'Alias' containing 'CMK-Oregon' and an optional 'Description' field. Below this is a 'Tags - optional' section. The bottom of the console shows a Windows taskbar with various application icons and a system clock indicating 4:57 PM on 23/12/2019.

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

The screenshot shows the 'Review and edit key policy' step, which is 'Step 5 of 5'. It displays a JSON policy document in a text editor. The policy includes a statement with 'Effect': 'Allow', which is highlighted by a blue arrow. The policy is for the root user of the AWS account. At the bottom of the console, there are 'Cancel', 'Previous', and 'Finish' buttons. The Windows taskbar at the bottom shows the system clock as 4:59 PM on 23/12/2019.

```
1 {
2   "Id": "key-consolepolicy-3",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "Enable IAM User Permissions",
7       "Effect": "Allow",
8       "Principal": {
9         "AWS": "arn:aws:iam::616399057974:root"
10      },
11       "Action": "kms:*",
12       "Resource": "*"
13     }
14   ]
15 }
```


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

The screenshot shows the AWS KMS console interface. A green success banner at the top states: "Success Your customer master key was created with alias **CMK-Oregon** and key ID **26b4aea6-826d-4d9c-aa58-fde8a6f2073c**." Below this, the "Customer managed keys" section displays a table with one key.

	Alias	Key ID	Status	Key spec	Key usage
<input type="checkbox"/>	CMK-Oregon	26b4aea6-826d-4d9c-aa58-fde8a6f2073c	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt

The bottom of the screenshot shows the Windows taskbar with the time 5:01 PM on 23/12/2019.

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

Account 1: 616399057974

Account 2: 450104983274

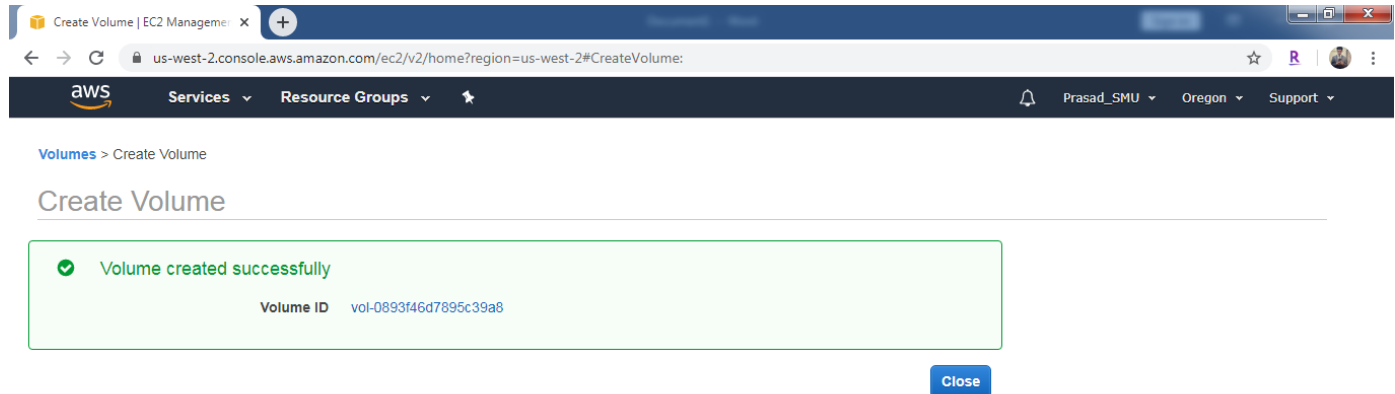
- Navigate to EC2 Service, Volume, and Click on Create Volume.

The screenshot shows the AWS Management Console for the 'us-west-2' region. The 'Create Volume' button is highlighted with a blue arrow. The console displays a table of existing volumes, including one named 'Encrypted Volume' with a size of 100 GiB and a type of gp2. The left sidebar shows the navigation menu with 'Volumes' selected under 'ELASTIC BLOCK STORE'.

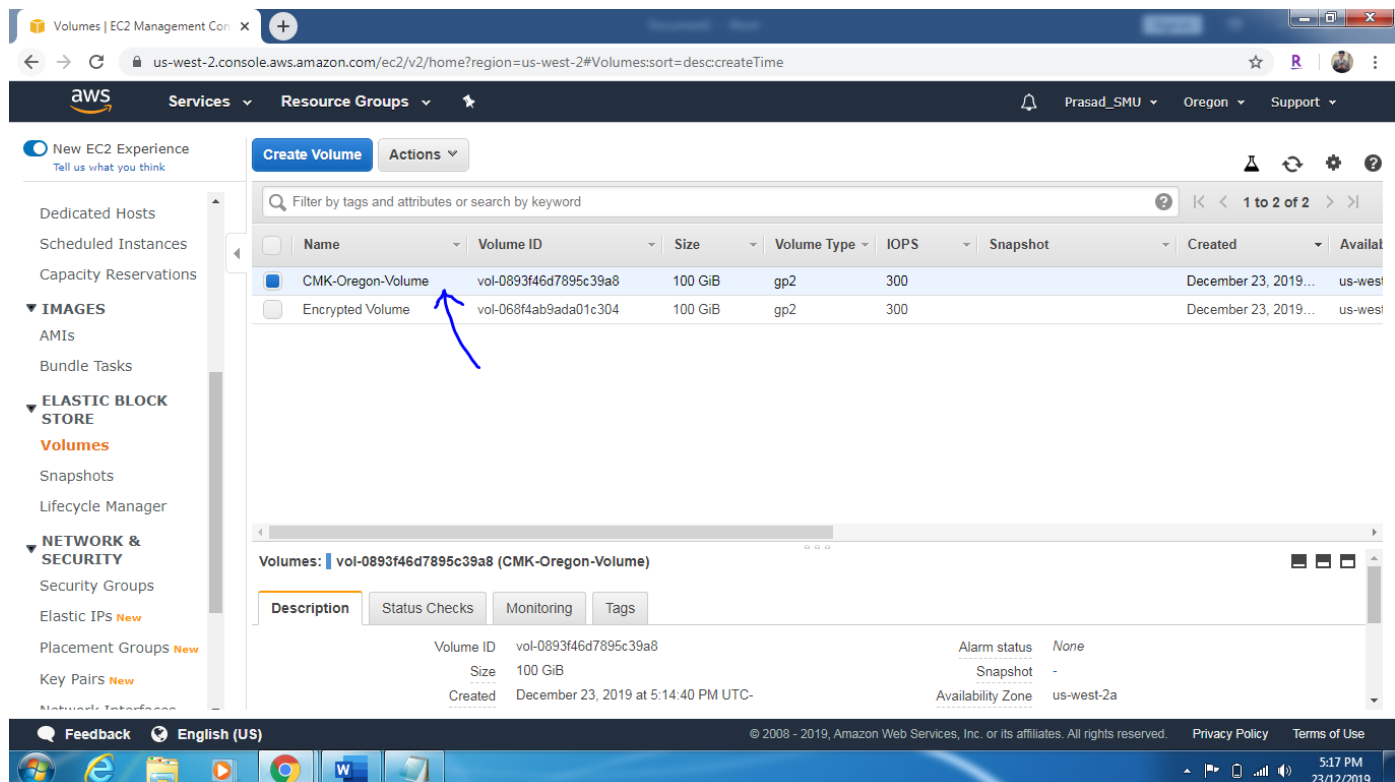
- Click on **Encrypt this volume** and select the newly created **Customer Managed Key** for Encryption and click on **Create Volume**.

The screenshot shows the 'Create Volume' wizard in the AWS Management Console. The 'Encryption' checkbox is checked, and the 'Master Key' dropdown is set to 'CMK-Oregon'. A blue arrow points to the 'Encrypt this volume' checkbox, and another blue arrow points to the 'Master Key' dropdown. The 'Availability Zone' is set to 'us-west-2a'. The 'Throughput (MB/s)' is 'Not applicable'. The 'Snapshot ID' is 'Select a snapshot'. The 'KMS Key Description' is empty. The 'KMS Key Account' is 'This account (616399057974)'. The 'KMS Key ID' is '26b4aea6-826d-4d9c-aa58-fde8a6f2073c'. The 'KMS Key ARN' is 'arn:aws:kms:us-west-2:616399057974:key/26b4aea6-826d-4d9c-aa58-fde8a6f2073c'.

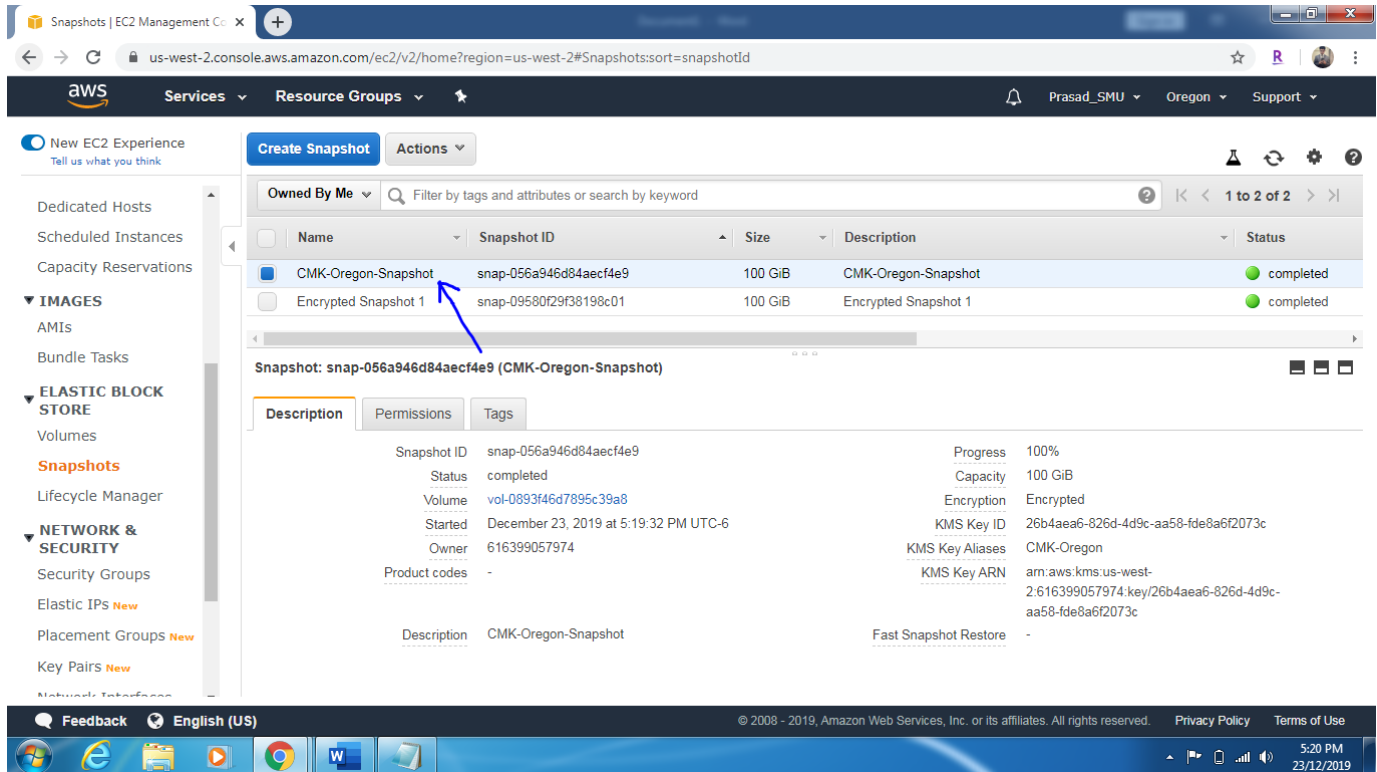
- Volume has been encrypted with Customer Managed Key.



- 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”.



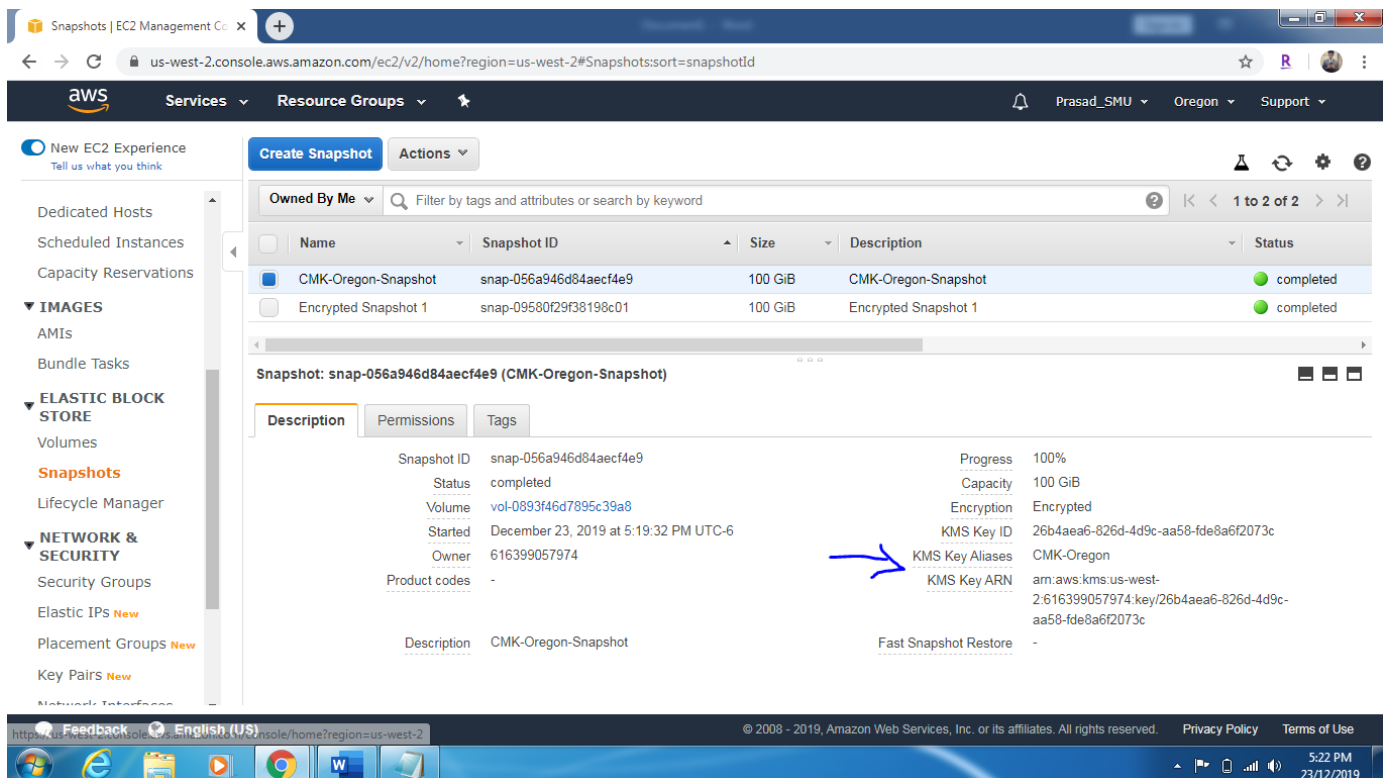
The screenshot shows the AWS Management Console for the 'us-west-2' region. The 'Snapshots' page is displayed, showing a list of snapshots. The 'CMK-Oregon-Snapshot' is highlighted, and its details are shown below the table. A blue arrow points to the 'CMK-Oregon-Snapshot' entry in the table.

Name	Snapshot ID	Size	Description	Status
CMK-Oregon-Snapshot	snap-056a946d84aecf4e9	100 GiB	CMK-Oregon-Snapshot	completed
Encrypted Snapshot 1	snap-09580f29f38198c01	100 GiB	Encrypted Snapshot 1	completed

Snapshot: snap-056a946d84aecf4e9 (CMK-Oregon-Snapshot)

Description		Permissions		Tags	
Snapshot ID	snap-056a946d84aecf4e9	Progress	100%		
Status	completed	Capacity	100 GiB		
Volume	vol-0893f46d7895c39a8	Encryption	Encrypted		
Started	December 23, 2019 at 5:19:32 PM UTC-6	KMS Key ID	26b4aea6-826d-4d9c-aa58-fde8a6f2073c		
Owner	616399057974	KMS Key Aliases	CMK-Oregon		
Product codes	-	KMS Key ARN	arn:aws:kms:us-west-2:616399057974:key/26b4aea6-826d-4d9c-aa58-fde8a6f2073c		
Description	CMK-Oregon-Snapshot	Fast Snapshot Restore	-		

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



The screenshot shows the AWS Management Console for the 'us-west-2' region. The 'Snapshots' page is displayed, showing a list of snapshots. The 'CMK-Oregon-Snapshot' is highlighted, and its details are shown below the table. A blue arrow points to the 'KMS Key Aliases' field in the snapshot details, which shows 'CMK-Oregon'.

Name	Snapshot ID	Size	Description	Status
CMK-Oregon-Snapshot	snap-056a946d84aecf4e9	100 GiB	CMK-Oregon-Snapshot	completed
Encrypted Snapshot 1	snap-09580f29f38198c01	100 GiB	Encrypted Snapshot 1	completed

Snapshot: snap-056a946d84aecf4e9 (CMK-Oregon-Snapshot)

Description		Permissions		Tags	
Snapshot ID	snap-056a946d84aecf4e9	Progress	100%		
Status	completed	Capacity	100 GiB		
Volume	vol-0893f46d7895c39a8	Encryption	Encrypted		
Started	December 23, 2019 at 5:19:32 PM UTC-6	KMS Key ID	26b4aea6-826d-4d9c-aa58-fde8a6f2073c		
Owner	616399057974	KMS Key Aliases	CMK-Oregon		
Product codes	-	KMS Key ARN	arn:aws:kms:us-west-2:616399057974:key/26b4aea6-826d-4d9c-aa58-fde8a6f2073c		
Description	CMK-Oregon-Snapshot	Fast Snapshot Restore	-		

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

The screenshot shows the AWS Management Console interface. On the left sidebar, the 'Snapshots' link is highlighted. The main content area displays the 'Permissions' tab for a specific snapshot. The 'Edit' button is located at the bottom left of the permissions section and is pointed to by a blue arrow.

Name	Snapshot ID	Size	Description	Status
CMK-Oregon-Snapshot	snap-056a946d84aecf4e9	100 GiB	CMK-Oregon-Snapshot	completed
Encrypted Snapshot 1	snap-09580f29f38198c01	100 GiB	Encrypted Snapshot 1	completed

Snapshot: snap-056a946d84aecf4e9 (CMK-Oregon-Snapshot)

Description Permissions Tags

This snapshot is currently Private.

AWS Account Number

This snapshot currently has no permissions.

Edit

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

The screenshot shows the 'Modify Permissions' dialog box in the AWS Management Console. The 'Private' radio button is selected. A new AWS Account Number is being added to the list. The 'Add Permission' button is highlighted with a blue arrow.

Modify Permissions

This is an encrypted snapshot. When you share an encrypted snapshot with another account, you must also share the CMK associated with the snapshot using KMS. Go to the [IAM Console](#) to share the CMK.

This snapshot is currently: ☐ Public ☒ Private

AWS Account Number

450104983274

AWS Account Number

Add Permission

Cancel Save

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

The screenshot shows the AWS Billing Management Console for Account Id: 450104983274. The page is titled "Account Settings" and includes sections for "Contact Information" and "Alternate Contacts".

Account Settings

- Account Id: 450104983274
- Account Name: Prasad Bhavsar
- Password: *****

Contact Information

Please note that updating your contact information on this page will not update the information displayed on your PDF Invoices. If you wish to update the billing address information associated with your Invoice, please edit it through the Payment Methods page, located [here](#).

Full Name: Prasad Bhavsar
Address: 2/sea Rock, Charkop Sector 4, Kandivali West, Mumbai 400067
City: Mumbai
State: Maharashtra
Postal Code: 400067
Country: IN
Phone Number: 9082907254
Company Name:
Website URL:

Alternate Contacts

In order to keep the right people in the loop, you can add an alternate contact for Billing, Operations, and Security communications. To specify an alternate contact, click the Edit button.

Please note that, as the primary account holder, you will continue to receive all email communications.

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

The screenshot shows the AWS Snapshots console for the ap-northeast-2 region. The "Private Snapshots" tab is selected, and a "Create Snapshot" button is visible. The page displays a message: "You do not have any snapshots in this region. Click the Create Snapshot button to create your first snapshot."

Create Snapshot

Owned By Me

Public Snapshots

Private Snapshots

Create Snapshot

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

The screenshot shows the AWS Management Console for the 'us-west-2' region. The left sidebar contains navigation links for Capacity Reservations, IMAGES (AMI, Bundle Tasks), ELASTIC BLOCK STORE (Volumes, Snapshots, Lifecycle Manager), NETWORK & SECURITY (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), and LOAD BALANCING. The main content area is titled 'Private Snapshots' and includes a search bar and a table of snapshots. A single snapshot is listed with the following details:

Name	Snapshot ID	Size	Description	Status	Started
	snap-056a946d84a...	100 GiB	CMK-Oregon-Snapshot	completed	December 23, 2019 at 5:19

Below the table, the details for the selected snapshot 'snap-056a946d84aef4e9' are shown:

Description		Tags	
Snapshot ID	snap-056a946d84aef4e9	Progress	100%
Status	completed	Capacity	100 GiB
Volume	vol-0893f46d7895c39a8	Encryption	Encrypted

Two blue arrows point to the 'Snapshot ID' and 'Description' columns of the snapshot table.

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

The screenshot shows the AWS Management Console for the 'us-west-2' region, similar to the previous one. The left sidebar is the same. The main content area is titled 'Private Snapshots' and shows a table with one snapshot. A blue arrow points to the 'Name' column of this snapshot, which is 'Shared Snapshot'.

Name	Snapshot ID	Size	Description	Status	Started
Shared Snapshot	snap-056a946d84a...	100 GiB	CMK-Oregon-Snapshot	completed	December 23, 2019 at 5:19

Below the table, the details for the selected snapshot 'snap-056a946d84aef4e9 (Shared Snapshot)' are shown:

Description		Tags	
Snapshot ID	snap-056a946d84aef4e9	Progress	100%
Status	completed	Capacity	100 GiB
Volume	vol-0893f46d7895c39a8	Encryption	Encrypted

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

The screenshot shows the AWS Management Console for the 'us-west-2' region. The 'Create Snapshot' dropdown menu is open, showing options: Delete, Create Volume, Manage Fast Snapshot Restore, Create Image, Copy, Modify Permissions, and Add/Edit Tags. A blue arrow points to the 'Create Volume' option. Below the menu, a table lists snapshots:

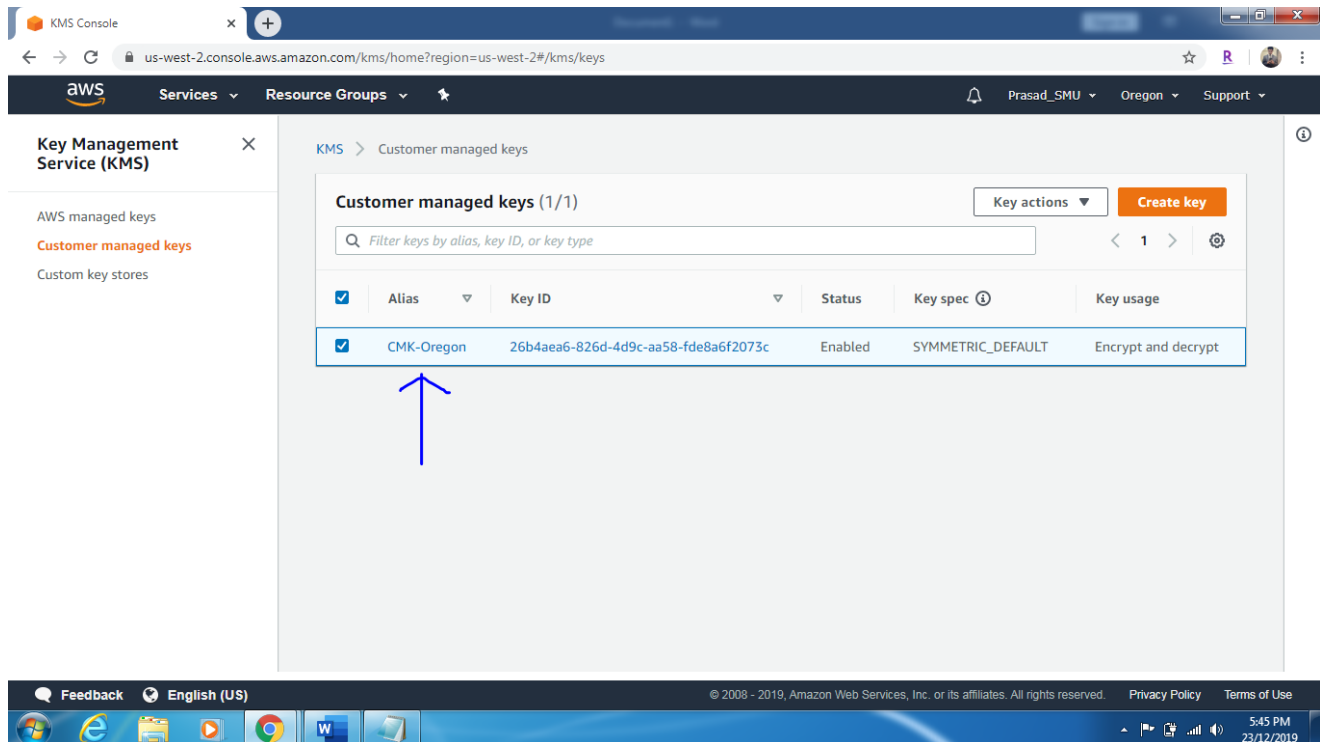
Name	Size	Description	Status	Started
Shared Snapshot	100 GiB	CMK-Oregon-Snapshot	completed	December 23, 2019

Below the table, the details for the snapshot 'snap-056a946d84aecf4e9 (Shared Snapshot)' are shown. The 'Description' tab is active, displaying the Snapshot ID, Status (completed), Volume (vol-0893f46d7895c39a8), Progress (100%), Capacity (100 GiB), and Encryption (Encrypted).

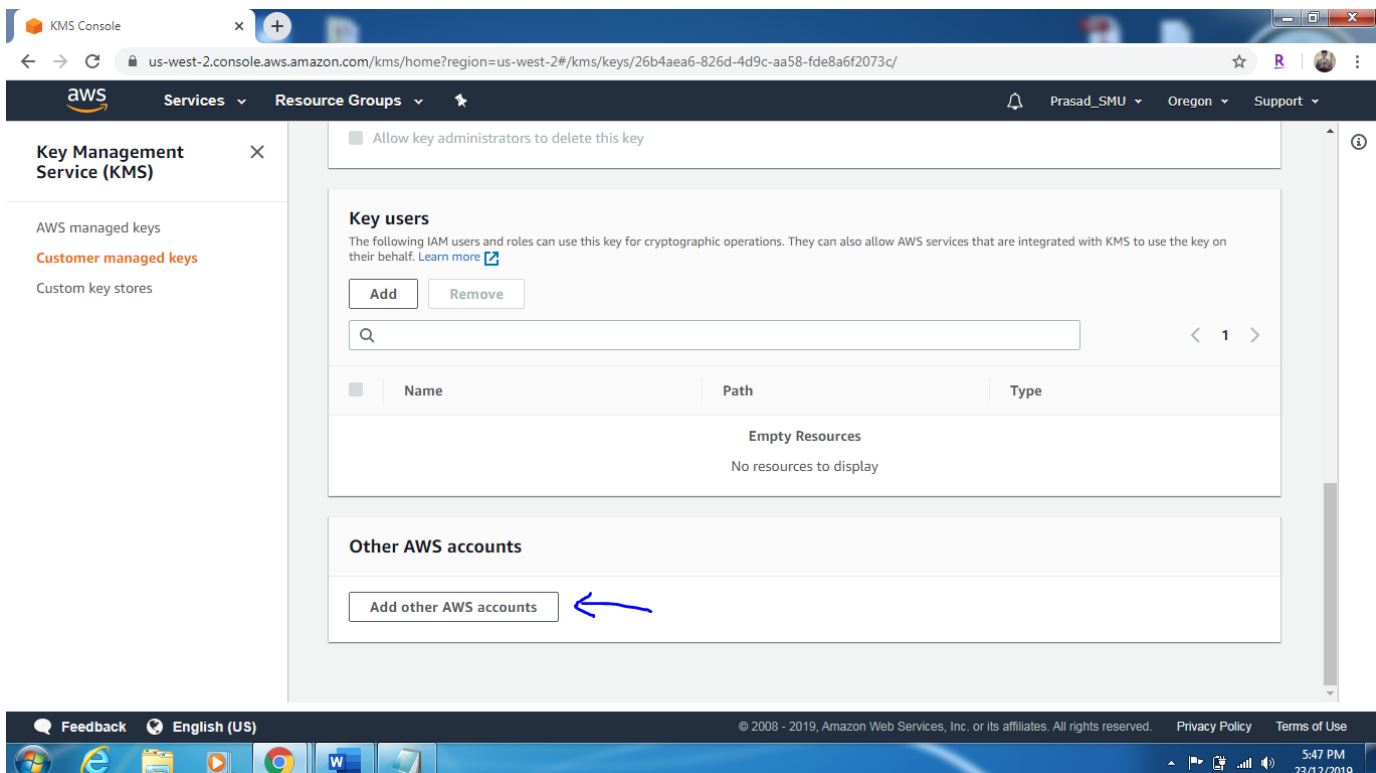
- While creating Snapshot from the Shared Snapshot, Second Account doesn't have access on **Customer Managed Key "CMK-Oregon"**. Hence even if you create a new Volume from Shared Snapshot, Volume won't be visible under EBS Volume Tab.

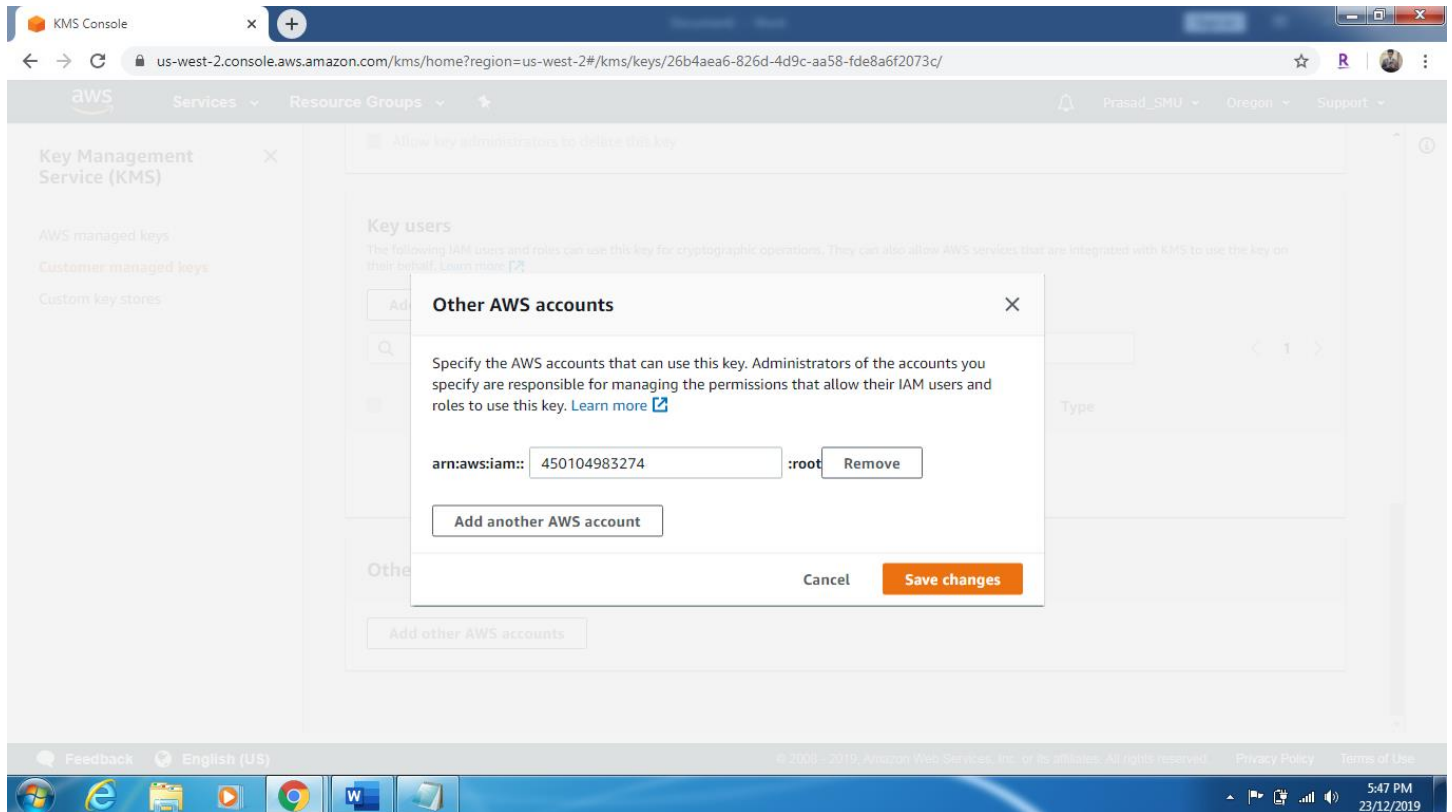
The screenshot shows the 'Create Volume' form in the AWS Management Console. The 'Availability Zone' is set to 'us-west-2a'. The 'Fast Snapshot Restore' is 'Not enabled'. The 'Throughput (MB/s)' is 'Not applicable'. The 'Encryption' checkbox is checked, with the label 'Encrypt this volume'. The 'Master Key' dropdown menu is open, showing a search bar and a list of keys. A blue arrow points to the '(default) aws/ebs' option. The 'KMS Key Description' is '(default) aws/ebs'. The 'KMS Key Account' is 'This account (450104983274)'. The 'KMS Key ID' is 'alias/aws/ebs'. The 'KMS Key ARN' is 'arn:aws:kms:us-west-2:450104983274:key/05ae37ea-6feb-4a05-bb1c-17f2656ade9d'.

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

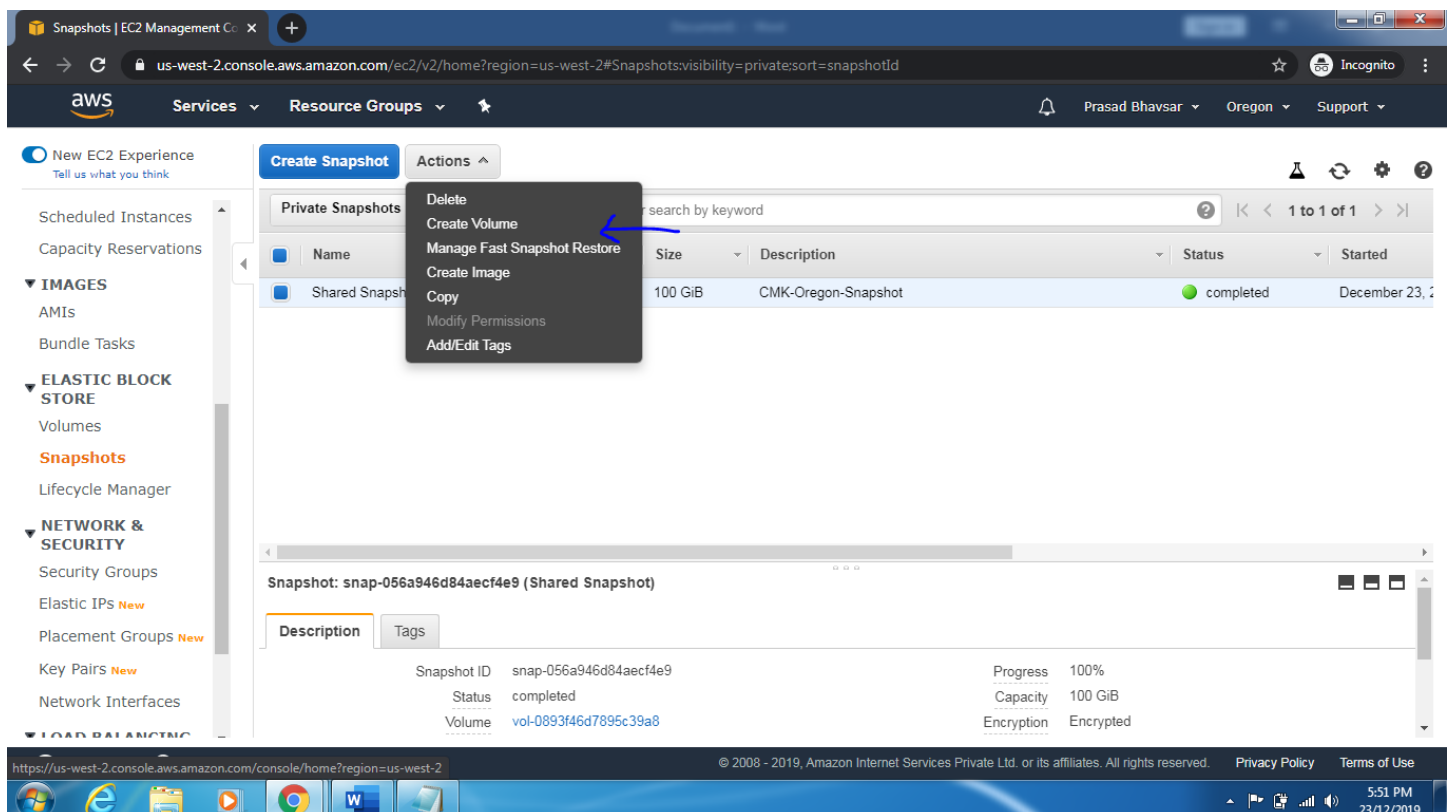


- Click on **Add other AWS Account** and put **Account ID** of the Second AWS Account.





➤ 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 .