**TASK 1-MOVING AN EC2 INSTANCE TO ANOTHER REGION (MUMBAI TO SINGAPORE)**

This guide explains how I moved an Amazon EC2 instance from the Mumbai (ap-south-1) region to the Singapore (ap-southeast-1) region. The process involved creating an Amazon Machine Image (AMI) and using it to launch a new instance in the new region.

**Step 1: Create an AMI of the Existing EC2 Instance**

1. Open the **AWS EC2 Console** in the Mumbai region.
2. Find and select the instance you want to move.
3. Click **Actions > Image and templates > Create image**.
4. Give the AMI a name and description.
5. Click **Create Image** and wait for the process to finish.

**Step 2: Copy the AMI to the Singapore Region**

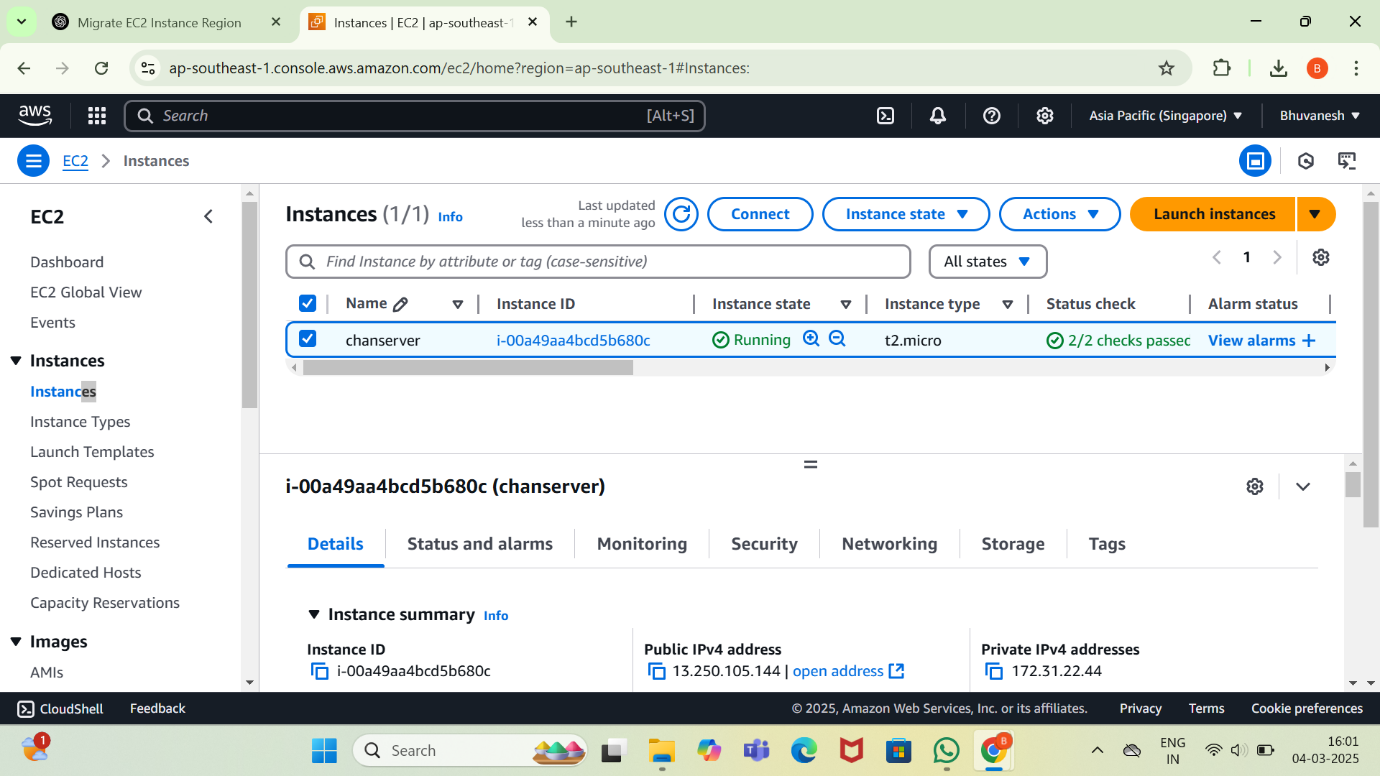
1. Go to **EC2 Dashboard > Images > AMIs**.
2. Select the AMI you just created.
3. Click **Actions > Copy AMI**.
4. Choose **Singapore (ap-southeast-1)** as the destination.
5. Click **Copy AMI** and wait for it to complete.

**Step 3: Launch a New Instance in the Singapore Region**

1. Switch to the **Singapore (ap-southeast-1)** region in the AWS console.
2. Go to **EC2 Dashboard > AMIs**.
3. Select the copied AMI and click **Launch instance from AMI**.
4. Pick an instance type (e.g., **t2.micro** for free tier).
5. Set up the network (VPC, subnet, security group as needed).
6. Create and download a new key pair.
7. Click **Launch Instance**.

**Conclusion**

The EC2 instance was successfully moved from Mumbai to Singapore. This method ensures minimal downtime and makes the migration process easy using AMIs. The new instance is now running smoothly in the Singapore region.



**TASK 2 - ENABLE AWS SYSTEMS MANAGER (SSM) FOR AN EC2 INSTANCE, FOLLOW THESE STEPS:**

**Step 1: Verify IAM Role**

Ensure your EC2 instance has an IAM role attached with the necessary permissions.

1. **Create an IAM Role for SSM** (if not already created):
   * Go to the **AWS IAM Console**.
   * Navigate to **Roles** → **Create role**.
   * Select **AWS service** → **EC2**.
   * Choose **AmazonSSMManagedInstanceCore** as the policy.
   * Name the role (e.g., SSM\_EC2\_Role) and create it.
2. **Attach the IAM Role to EC2**:
   * Open the **EC2 Console** → Select the instance.
   * Click **Actions** → **Security** → **Modify IAM Role**.
   * Select the created role (SSM\_EC2\_Role) and attach it.

**Step 2: Install the SSM Agent**

Most Amazon Linux 2 and Ubuntu AMIs have the SSM Agent pre-installed. To manually install it:

**For Amazon Linux / Amazon Linux 2 / RHEL**

sh

CopyEdit

sudo yum install -y amazon-ssm-agent

sudo systemctl enable amazon-ssm-agent

sudo systemctl start amazon-ssm-agent

**For Ubuntu/Debian**

sh

CopyEdit

sudo snap install amazon-ssm-agent --classic

sudo systemctl enable snap.amazon-ssm-agent.amazon-ssm-agent

sudo systemctl start snap.amazon-ssm-agent.amazon-ssm-agent

**For Windows**

Run the following in PowerShell:

powershell

CopyEdit

msiexec.exe /i https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/windows\_amd64/AmazonSSMAgentSetup.msi /quiet /norestart

**Step 3: Verify SSM Agent Connectivity**

Run the following command to confirm the agent is running:

sh

CopyEdit

sudo systemctl status amazon-ssm-agent

Alternatively, check from the **AWS Console**:

* Go to **AWS Systems Manager** → **Fleet Manager**.
* The instance should be listed under **Managed Instances**.

**Step 4: Connect to EC2 via Session Manager**

1. Open **AWS Systems Manager**.
2. Navigate to **Session Manager**.
3. Click **Start Session** → Select the instance.
4. Click **Start session** to access the shell.

