

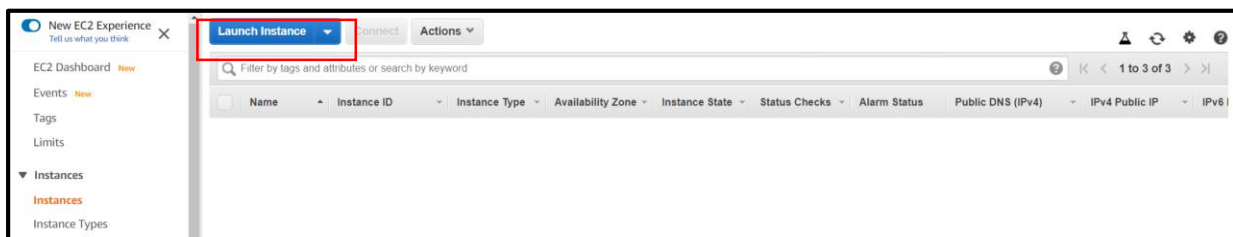
Persists EBS volume beyond the life of an EC2 instance, take snapshot & restore the EBS volume in a different region. Attach the restored EBS volume to a new EC2 instance in that region.

Objectives:

1. Learn to persist EBS Volume beyond the life of an EC2 instance.
2. Learn to replicate EBS Volume in different region and attach the same to new instance in that region. This will serve as your Disaster Recovery strategy.

Step 1: Create a Linux Instance as follows:

Click on **Instances** option in left navigation pane so as to be directed to following page. Click on **Launch Instance** button on top left.

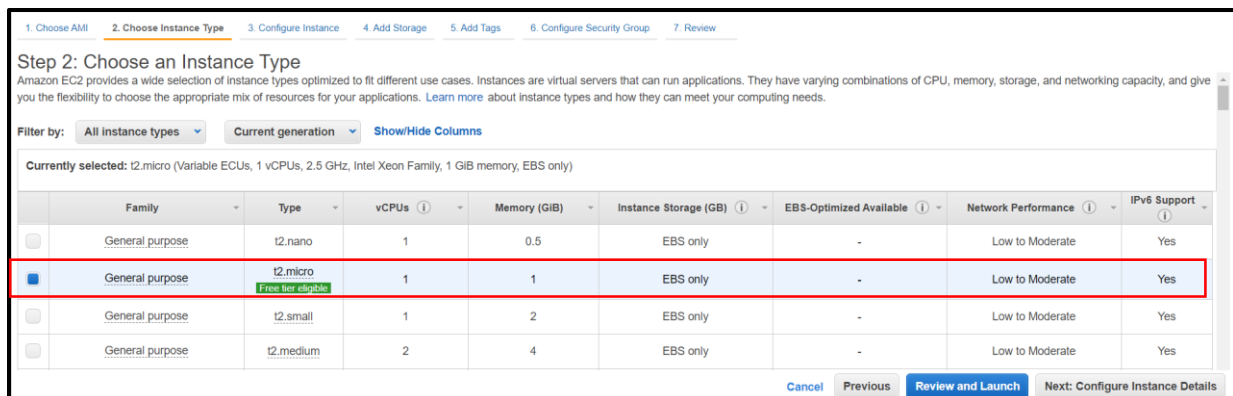


After clicking on the launch instance you will be redirected to this page. Here search/select **Amazon Linux 2 AMI**.



Choose an Instance Type over here.

- Select General purpose type **t2.micro** Instance Type.
- Click on **Next: Configure Instance Details** at the bottom right of the screen.



Cloud Plus Plus Services



Here you will Configure Instance Details.

- In the **Subnet** field select on the drop down list and **select any one** of the Subnets. It is ap-south-1a in our case.
- Note This subnet for reference afterwards.
- In the **Auto-assign Public IP** field select on the drop down list and select **Enable** option.
- **Click Next: Add Storage** at bottom right of screen.

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: ☐ Request Spot instances

Network: vpc-1a1a1a1a (default) Create new VPC

Subnet: subnet-1a1a1a1a Default in ap-south-1a 4091 IP Addresses available Create new subnet

Auto-assign Public IP: Enable

Placement group: ☐ Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory Create new directory

IAM role: None Create new IAM role

Shutdown behavior: Stop

Stop - Hibernate behavior: ☐ Enable hibernation as an additional stop behavior

Cancel Previous Review and Launch Next: Add Storage

Step 2: In the step for **Add Storage**, click on the **Add New Volume**. Let everything be default. Mention the required size of volume in GB. 50 GB in our case.

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-08d68946ad0e25c23	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	Search (case-insensit)	50	General Purpose SSD (gp2)	150 / 3000	N/A	<input type="checkbox"/>	Not Encrypted

Add New Volume

Cancel Previous Review and Launch Next: Add Tags

Click on **Next: Add Tags** button in the down right corner.

Add Tags

- Key: **Name**
- Value: **LinuxServer**

Click on the **Next: Configure Security Group** at the bottom right of the screen.
Configure Security Group

- Create a **new** security group and name it as **LinuxSG**
- In the description enter the following text:
Security Groups for Linux Servers

Cloud Plus Plus Services



- Keep the default **SSH** rule.
- Warning: Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
- While using this feature for production make sure the known IP address is entered.
- Click on **Review and Launch** button on the bottom right corner

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group
☐ Select an existing security group

Security group name:
Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Previous](#) [Review and Launch](#)

Review Instance Launch

- Here are all the details regarding your instance. Read them once and check if all the configurations are correct
- Click on the **Launch** button at the bottom right corner. This will launch your instance.

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, linuxServerSG, is open to the world.
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

AMI Details [Edit AMI](#)
Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0ebc1ac48dfd14136
Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.
Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups [Edit security groups](#)

[Cancel](#) [Previous](#) [Launch](#)

Cloud Plus Plus Services



- After you click the **Launch** button here you will be asked to select/create KEY-PAIR. Choose an existing key pair option from the drop down.
- Acknowledge the key pair and launch the instance.

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Select a key pair

☒ I acknowledge that I have access to the selected private key file (LINUX_SERVER.pem), and that without this file, I won't be able to log into my instance.

[Cancel](#) [Launch Instances](#)

Click **View Instance** button at bottom right of the screen to see your launched instance.

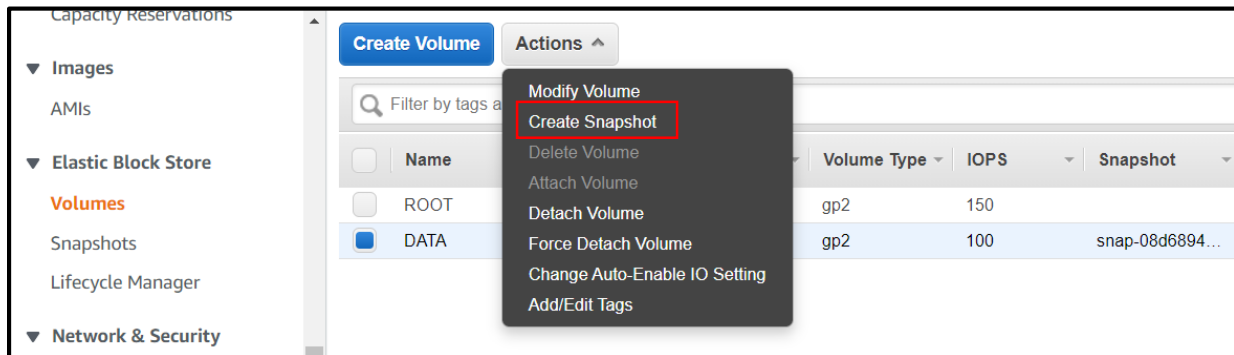
Check if the instance is running.

Step 3: In the left panel of the AWS console go into **Volumes** under **Elastic Block Store**. Here you will see our 2 volumes created (One which was added by default with the instance and the other we added extra)

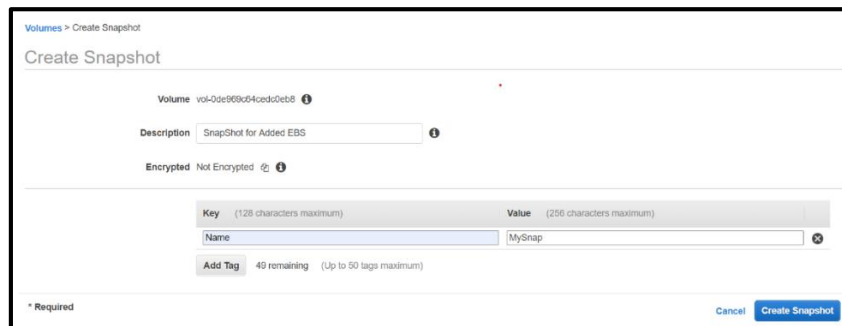
Name these two volumes as ROOT and DATA below the name category by clicking the pencil icon in the name column.

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	State	Alarm Status	Attachments
DATA	vol-09fe92d3...	50 GiB	gp2	150		September 1, 2020 ...	ap-south-1a	in-use	None	i-0d22521c...
ROOT	vol-0c103f4f...	8 GiB	gp2	100	snap-08d6894...	September 1, 2020 ...	ap-south-1a	in-use	None	i-0d22521c...

Step 4: Select the DATA volume. Go to **Actions** and click on **Create Snapshot** option.



Give details of the snapshot in the Create Snapshot pop-up window and click on **Create Snapshot**.

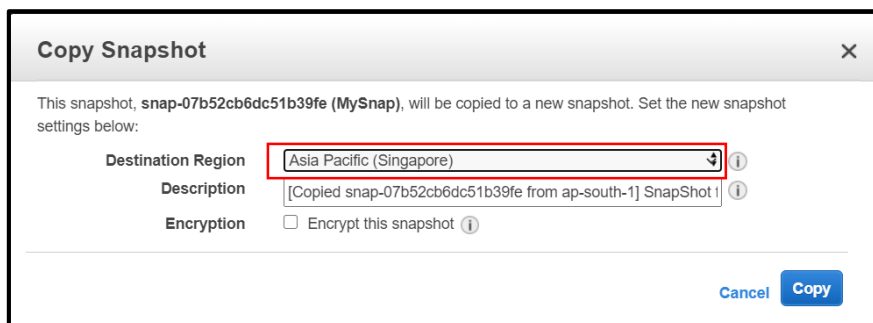


The screenshot shows the 'Create Snapshot' pop-up window. It contains the following fields and options:

- Volume:** vol-0de989d4ced0eb8
- Description:** SnapShot for Added EBS
- Encrypted:** Not Encrypted
- Key:** (128 characters maximum) - Name: MySnap
- Value:** (256 characters maximum)
- Add Tag:** 40 remaining (Up to 50 tags maximum)
- Buttons:** Cancel, Create Snapshot

Step 5: Go to **Snapshots** under **Elastic Block Store**. Select your Snapshot.

Click on **Actions** -> **Copy**. Choose a different region and click on **Copy**.



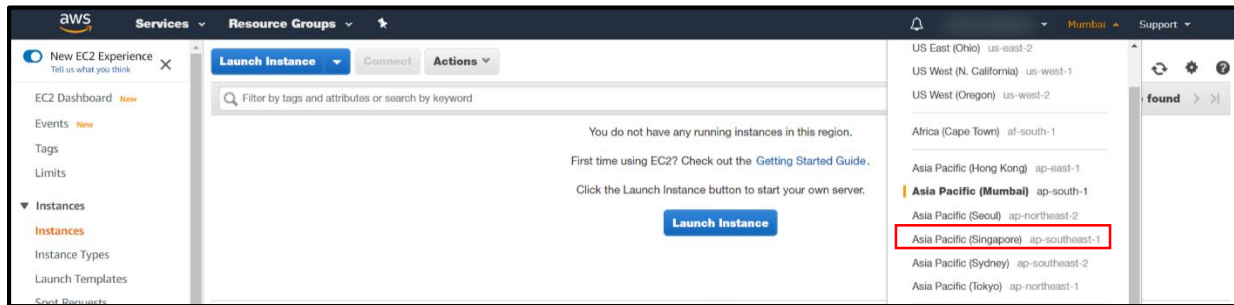
The screenshot shows the 'Copy Snapshot' pop-up window. It contains the following fields and options:

- Message:** This snapshot, snap-07b52cb6dc51b39fe (MySnap), will be copied to a new snapshot. Set the new snapshot settings below:
- Destination Region:** Asia Pacific (Singapore)
- Description:** [Copied snap-07b52cb6dc51b39fe from ap-south-1] SnapShot !
- Encryption:** ☐ Encrypt this snapshot
- Buttons:** Cancel, Copy

Cloud Plus Plus Services

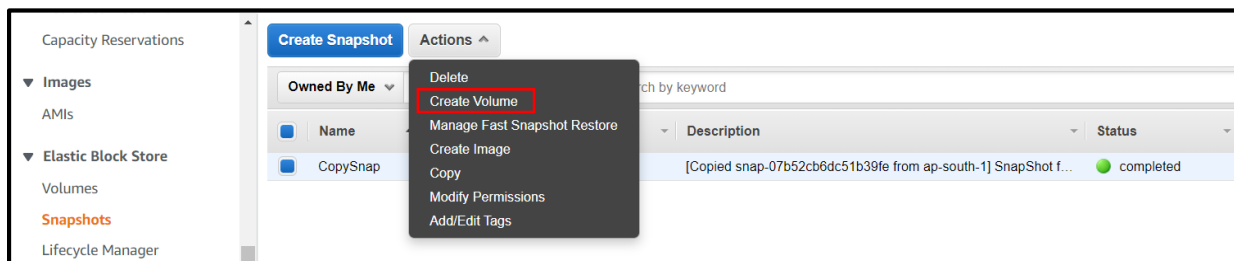


Step 6: Now go to the different region as given below. Here the selection is Singapore in our case.



Step 7: Check that the snapshot has been copied to this region.

Go to **Snapshots** under **Elastic Block Store**. Go to **Actions** -> **Create Volume**.



We choose the same subnet in which the new Instance in this region is created.

Create Volume

Snapshot ID: snap-0517764785e8e698b (MySnap)

Volume Type: General Purpose SSD (gp2)

Size (GiB): 50 (Min: 1 GiB, Max: 16384 GiB)

IOPS: 150 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)

Availability Zone*: ap-southeast-1

Fast Snapshot Restore: Not enabled

Throughput (MB/s): Not applicable

Encryption: ☐ Encrypt this volume

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

Name: DATA2

Add Tag: 49 remaining (Up to 50 tags maximum)

* Required

Cancel Create Volume

Click on **Create Volume**.

Step 8: In the same Volume Tab, we observe that the DATA2 volume is in **available** state and the root volume of new server is in **in-use** state.

Step 9: Create a Linux Instance in this region. Refer to Step 1 and Step 2 in this document. Do not create an additional volume. This instance will have the default root volume only.

Step 10: Go to Volumes. Select the DATA volume. Go to **Action** -> **Attach Volume**.

In the pop up window select your newly created instance in the **Instance** text field. Click on **Attach** button.

Thus the volume restored in a new region through copying snapshot, is now attached to an instance in that region successfully.

This new instance in new region can serve as your disaster recovery strategy.

Note: If you no longer need this instance and the volume make sure to terminate the instance and delete the volume as well as snapshots.

Was this document helpful? YES / NO

Document Created by	Version
Parag Deshpande	28-Jan-2020