* **What is the difference between PVM and HVM?**

**Ans:**

HVM guests are fully virtualized. It means that the VMs running on top of their hypervisors are not aware that they are sharing processing time with other clients on the same hardware. The host should have the capability to emulate underlying hardware for each of its guest machines. This virtualization type provides the ability to run an operating system directly on top of a virtual machine without any modification — as if it were run on the bare-metal hardware. The advantage of this is that HVMs can use hardware extensions which provide very fast access to underlying hardware on the host system.

Paravirtualization, on the other hand, is a lighter form of virtualization. This technique is fast, and provides near native speed in comparison to full virtualization. With Paravirtualization, the guest operating system requires some modification before everything can work. These modifications allow the hypervisor to export a modified version of the underlying hardware to the VMs, allowing them near-native performance. All PV machines running on a hypervisor are basically modified operating systems like Solaris or various Linux distributions.

This is in contrast to HVM, which requires no modifications to the guest OS and the host OS is completely unaware of the virtualization. This may add to the performance penalty because it places an extra burden on the hypervisor.

* **Consider a scenario, you have just launched EC2 instances and you are unable to ssh into it, what all things will you check to troubleshoot this.**

**Ans:**

**Does it have a public IP address?**

Either create an Elastic IP address and attach it to the instance *or* terminate the instance and create a new one (making sure to “enable” public IP address during the creation process). Check the connection again.

**Does the security group have inbound allow rules for HTTPS and/or SSH?**

Add an allow rule for HTTP and/or SHH (depending on which you need). Check the connection again.

**Does the HTTP and/or SSH all for traffic from all sources (0.0.0.0/0)?**

Edit the source to be 0.0.0.0/0 for each protocol. Check the connection again.

**Does the subnets route table have a route to the Internet Gateway?**

Edit the route table to add a route to the IGW Destination = 0.0.0.0/0 and Target = (the Internet Gateway ID)

**Does the Network Access Control List protecting the subnet have inbound allow rules for HTTPS and/or SSH?**

Add an allow rule for HTTP and/or SHH (depending on which you need). Check the connection again.

**Does the Network Access Control List protecting the subnet have outbound allow rules set for all traffic?**

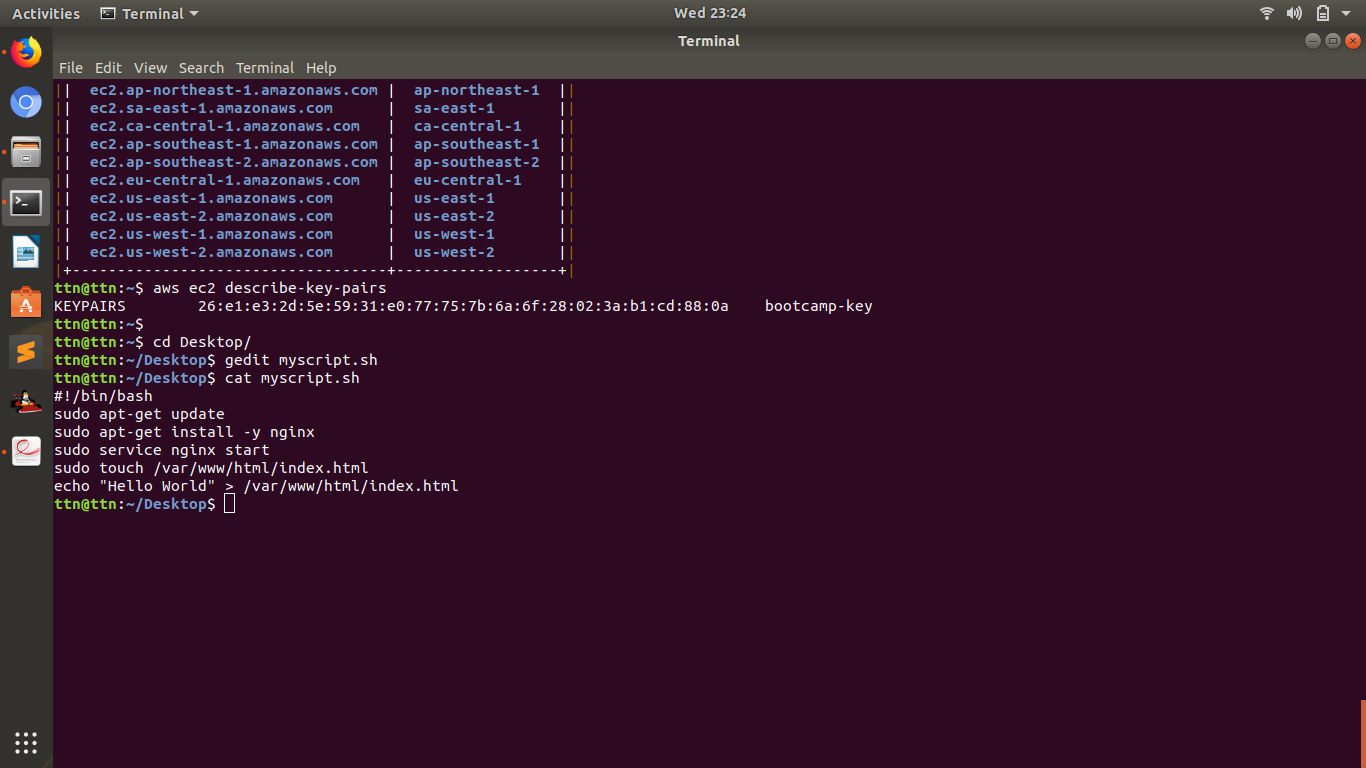
Edit the outbound rules to allow for all traffic from all sources (0.0.0.0/0). Check the connection again.

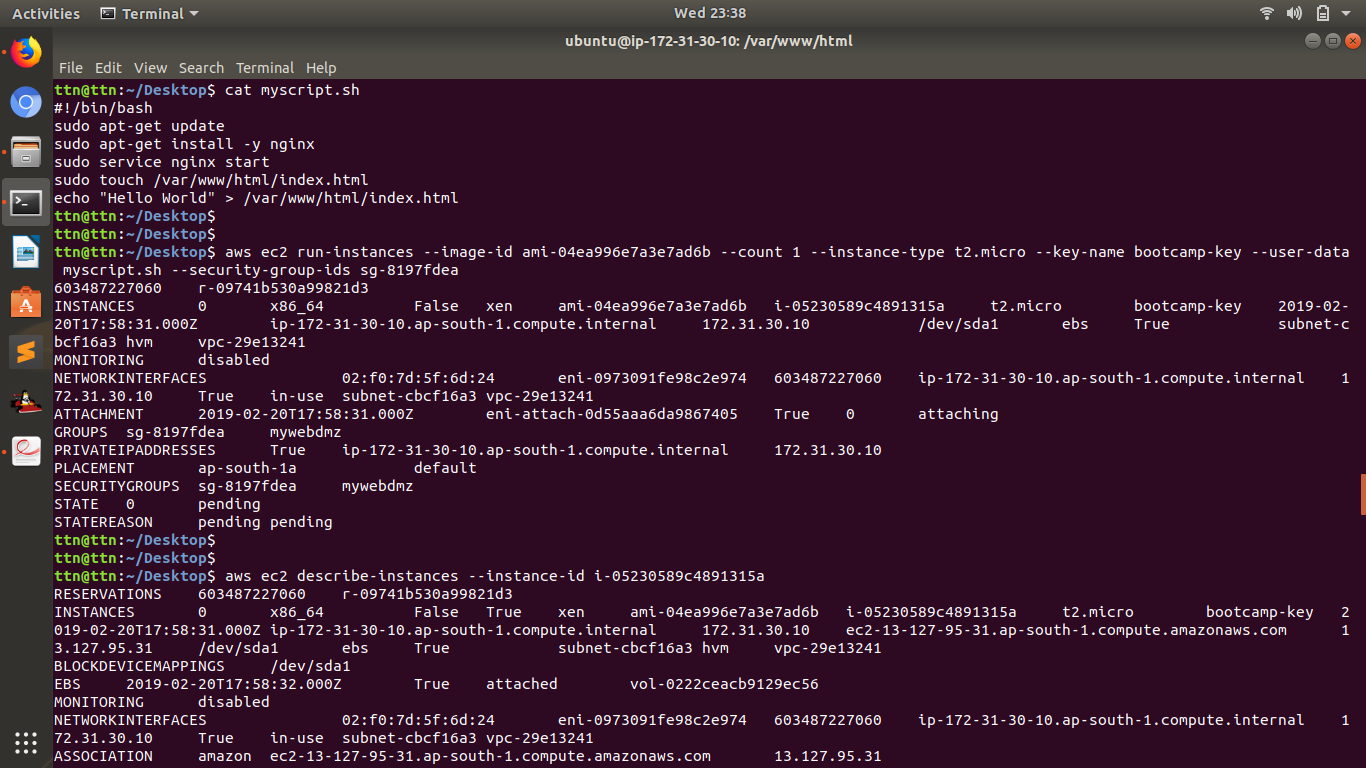
**Is there an internet gateway attached to the VPC in which the EC2 instance has been provisioned in?**

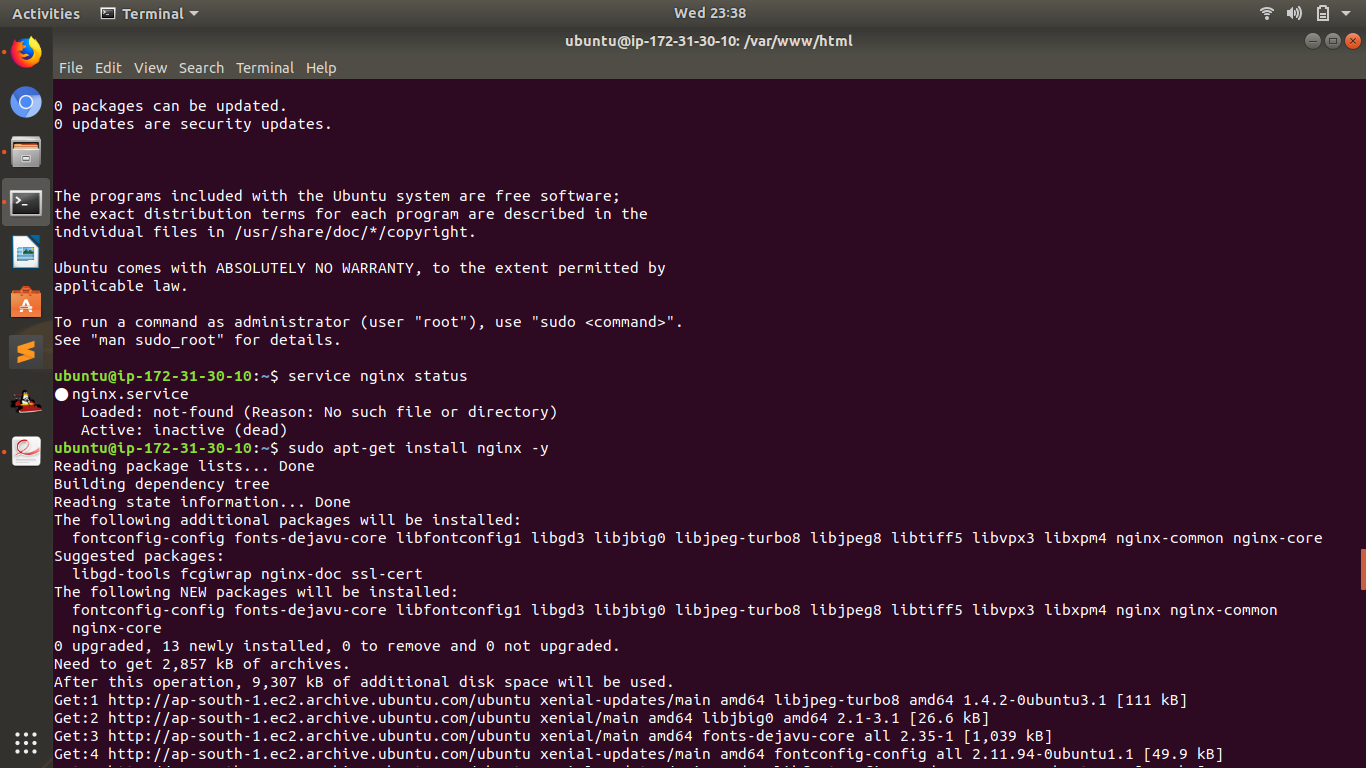
Create and IGW and attached it to the VPC. The move back to “the subnet” section.

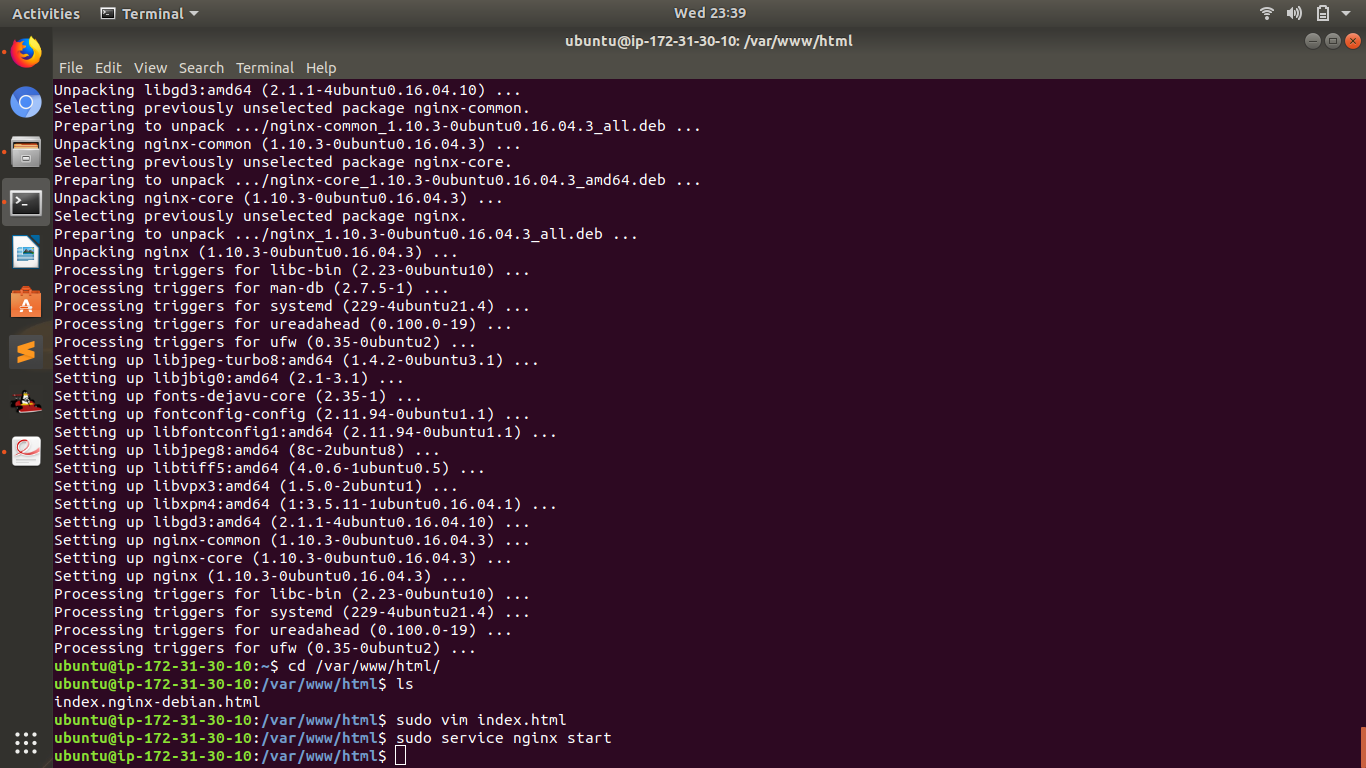
* **Launch EC2 instances with user-data (install Nginx and print hello world on the default page), using AWS CLI**

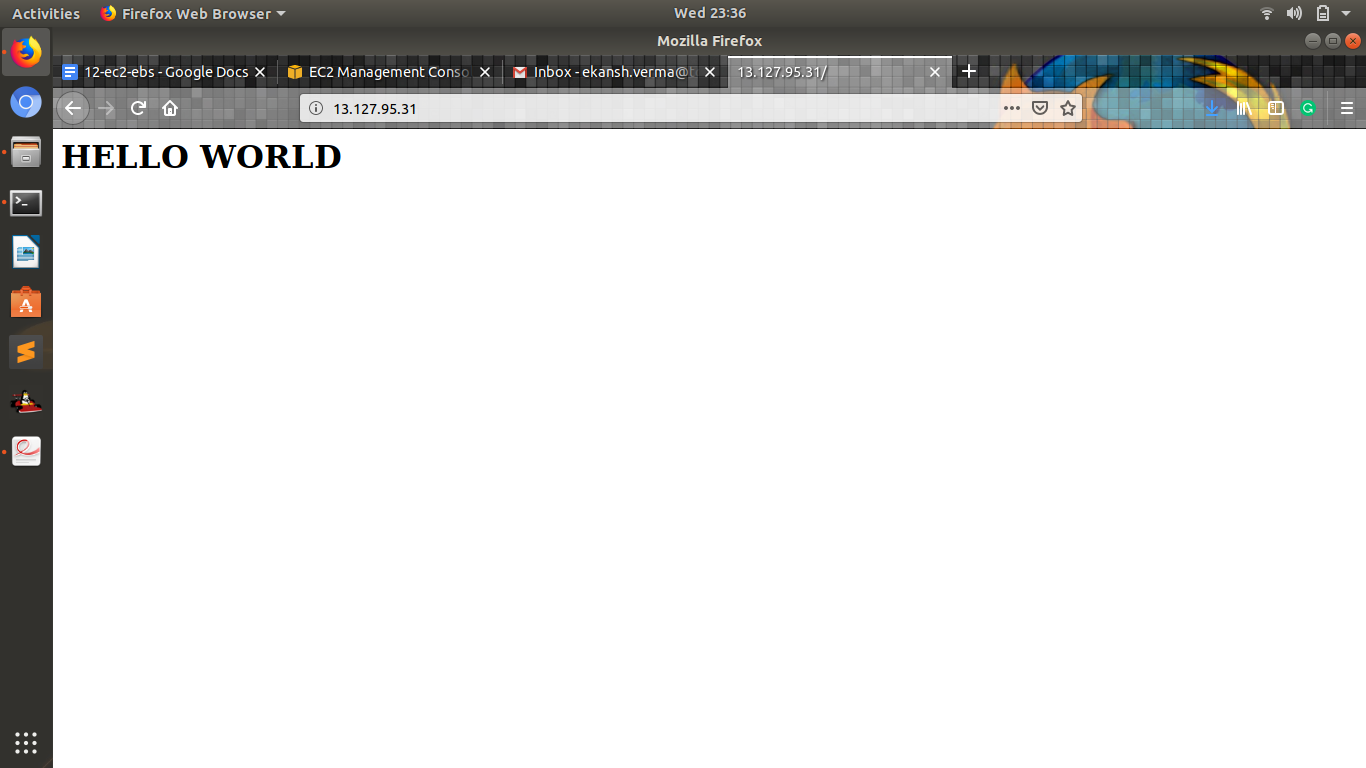
**Ans:**



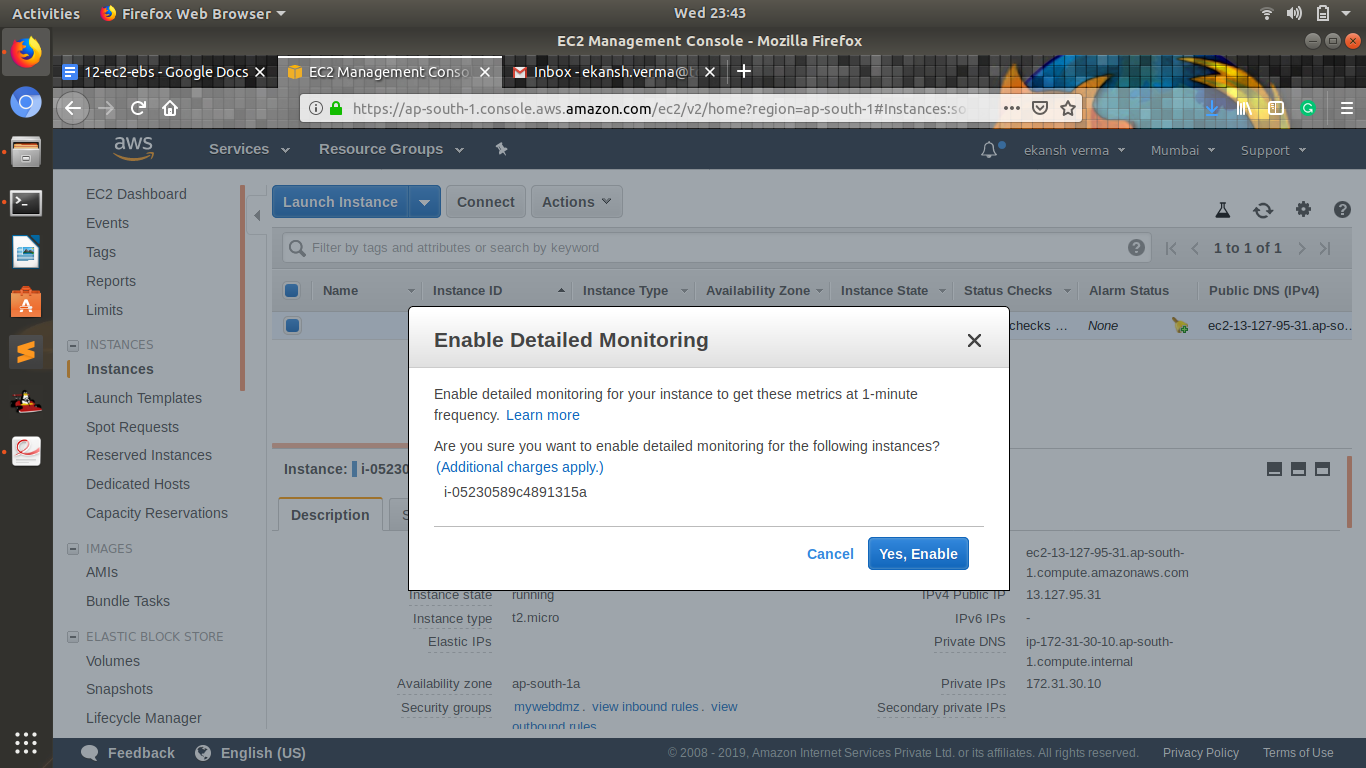


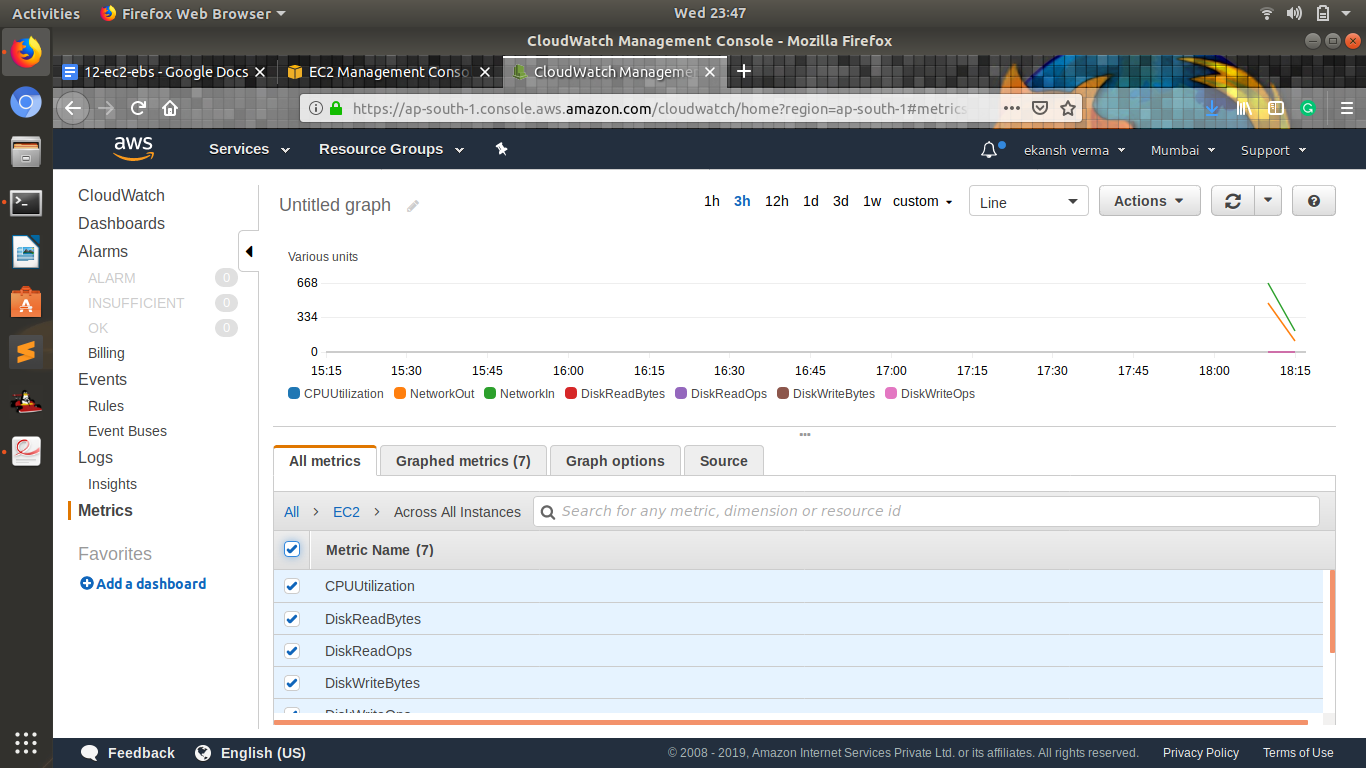




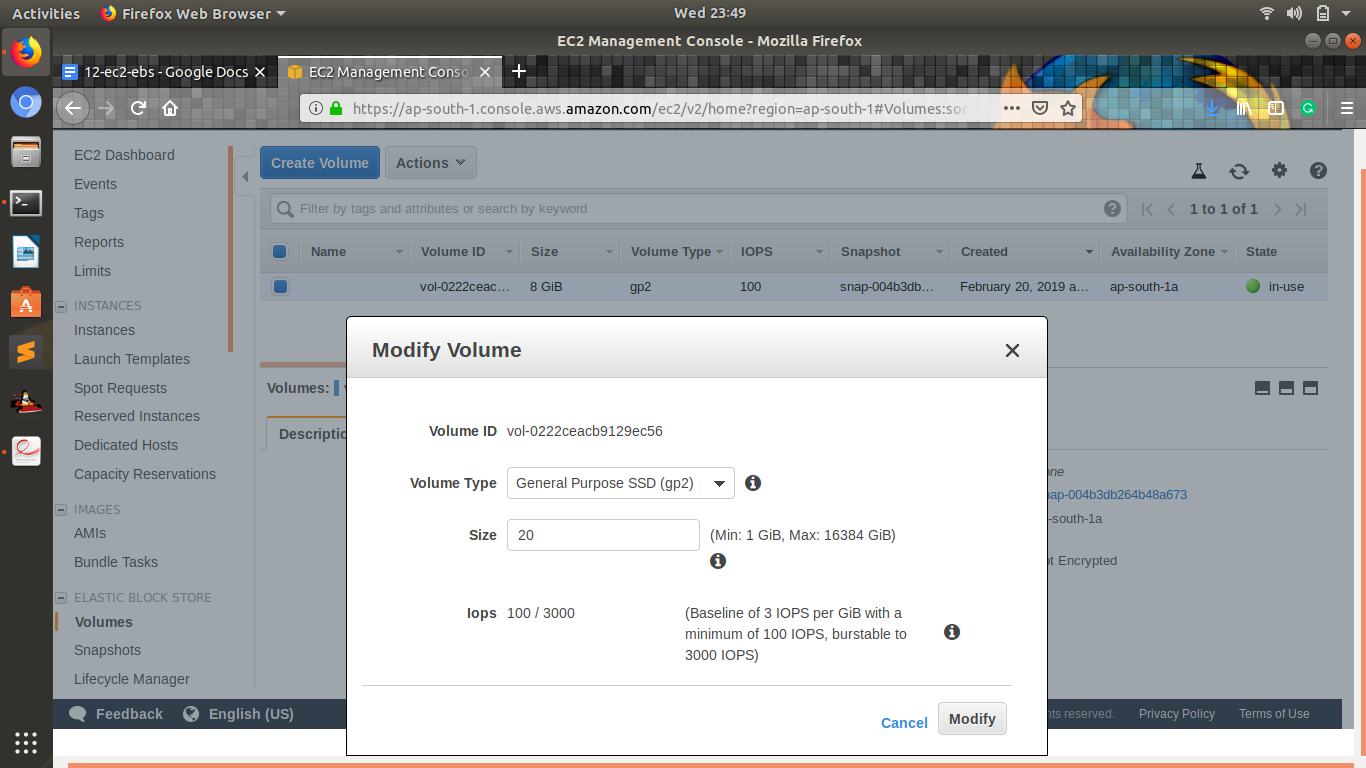


* **Add memory metrics for the instance in the cloud watch**





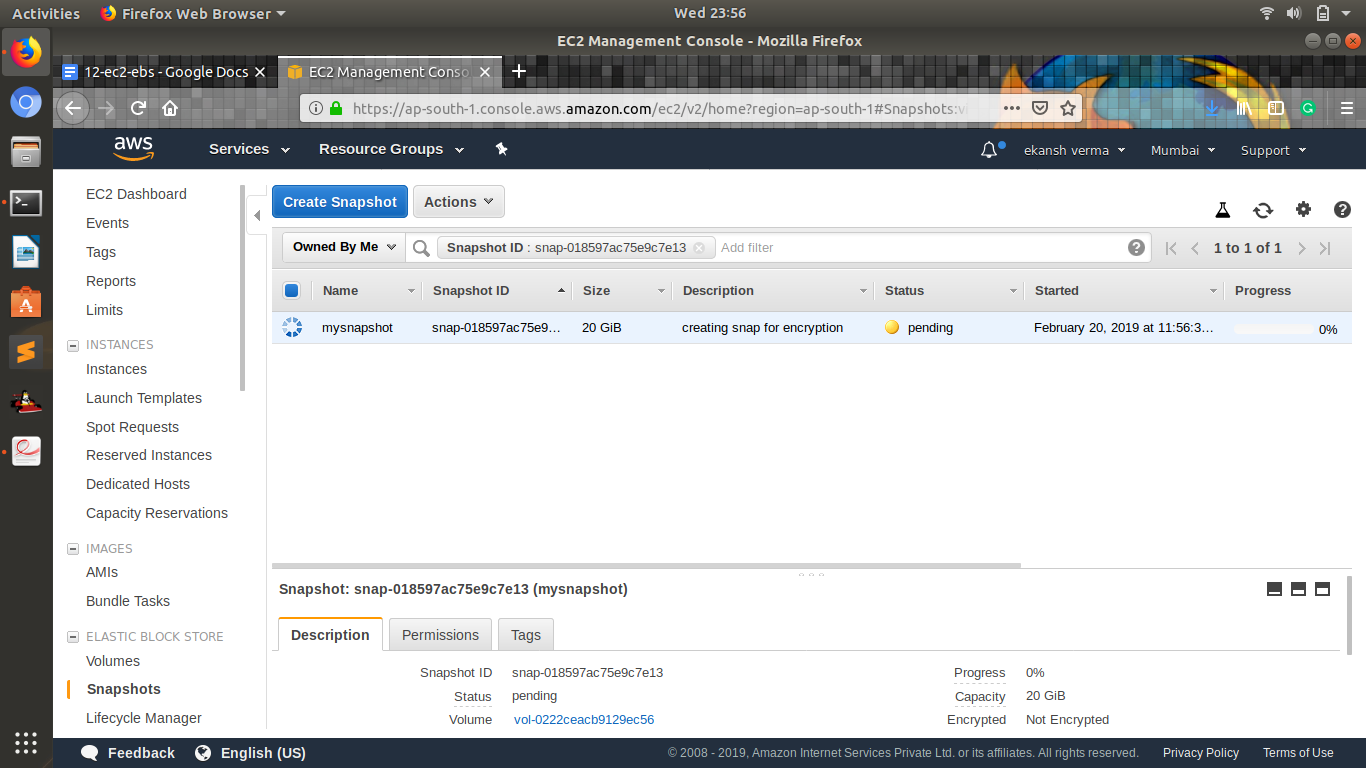
* **Increase EBS volume size from 8 GB to 20 GB without rebooting the server on the instance created above**



* **Convert EBS disk to encrypted EBS disk on the instance created above**

1. Select your unencrypted volume

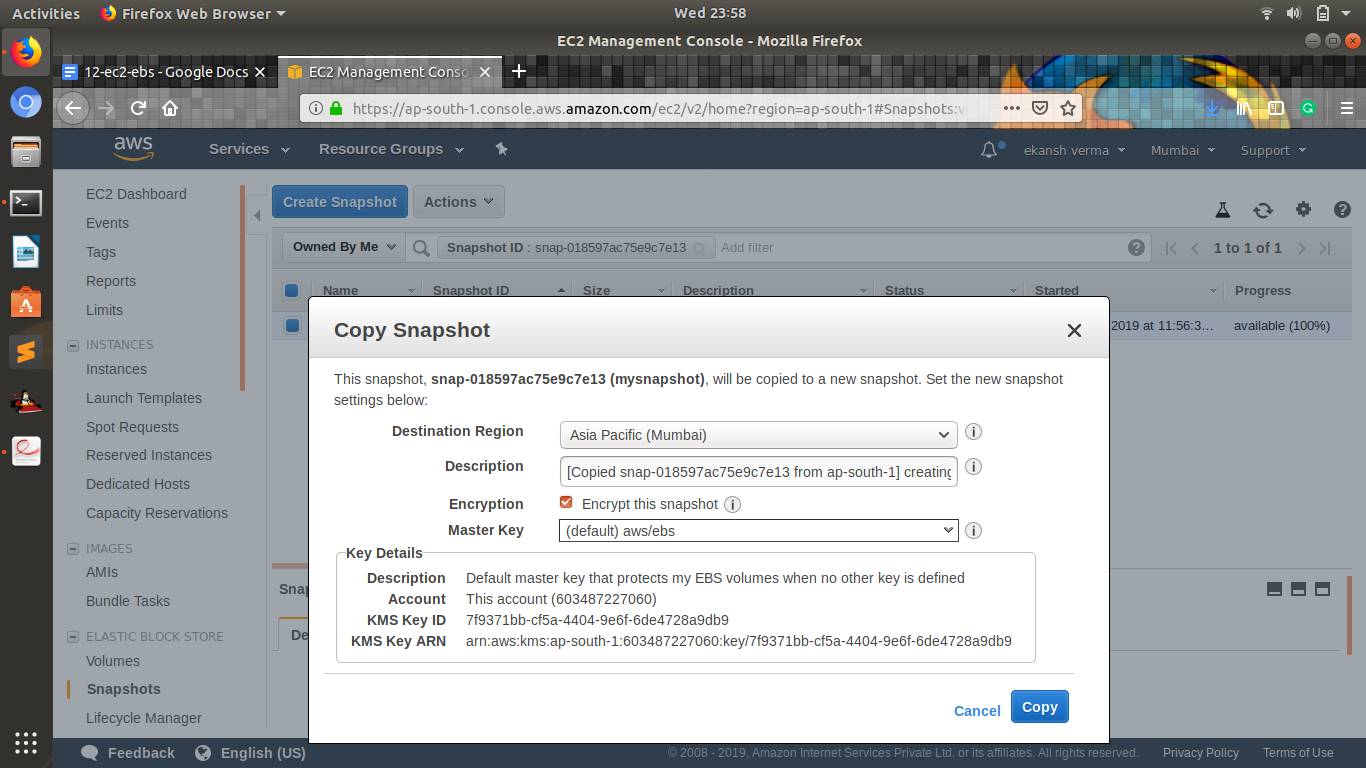
2. Select ‘Actions’ – ‘Create Snapshot’



3. When the snapshot is complete, select ‘Snapshots’ under ‘Elastic Block Store’ Select your newly created snapshot

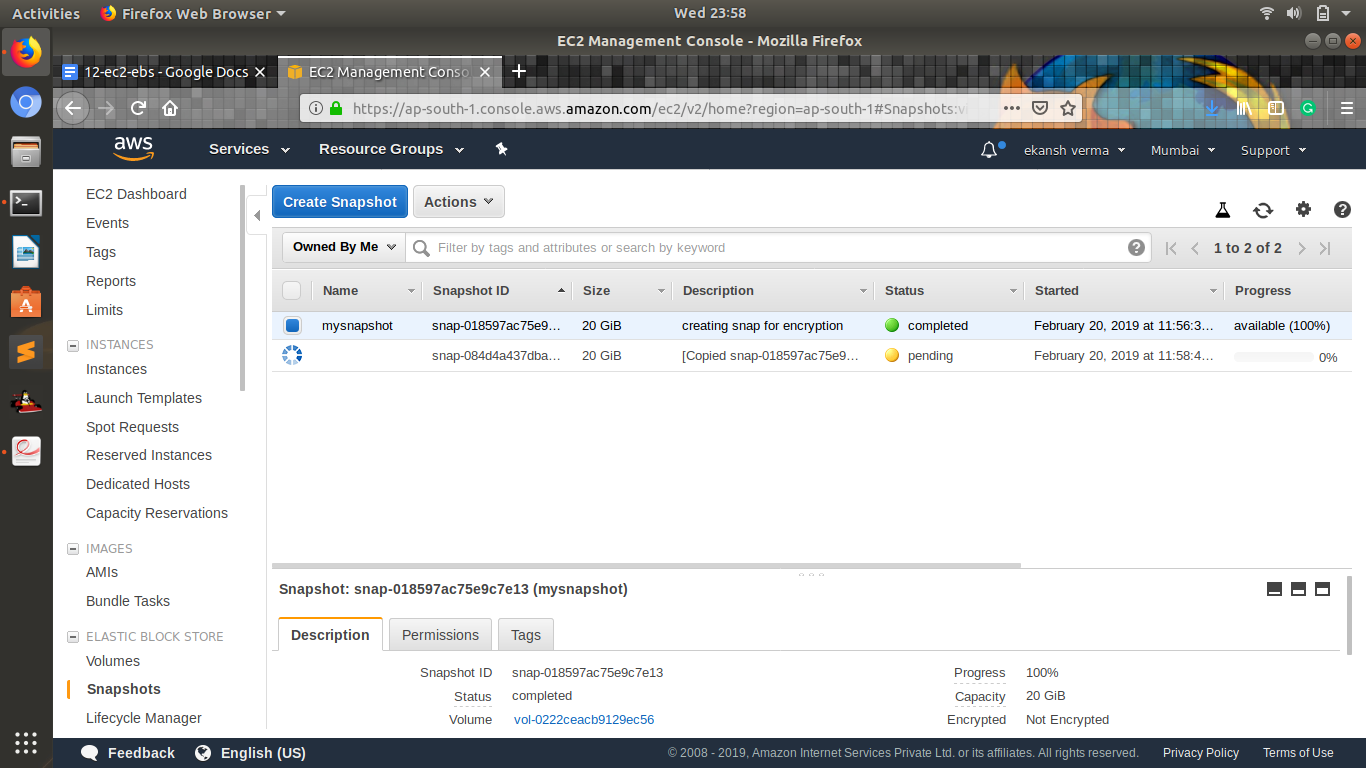
4. Select ‘Actions’ – ‘Copy’

5. Check the box for ‘Encryption’



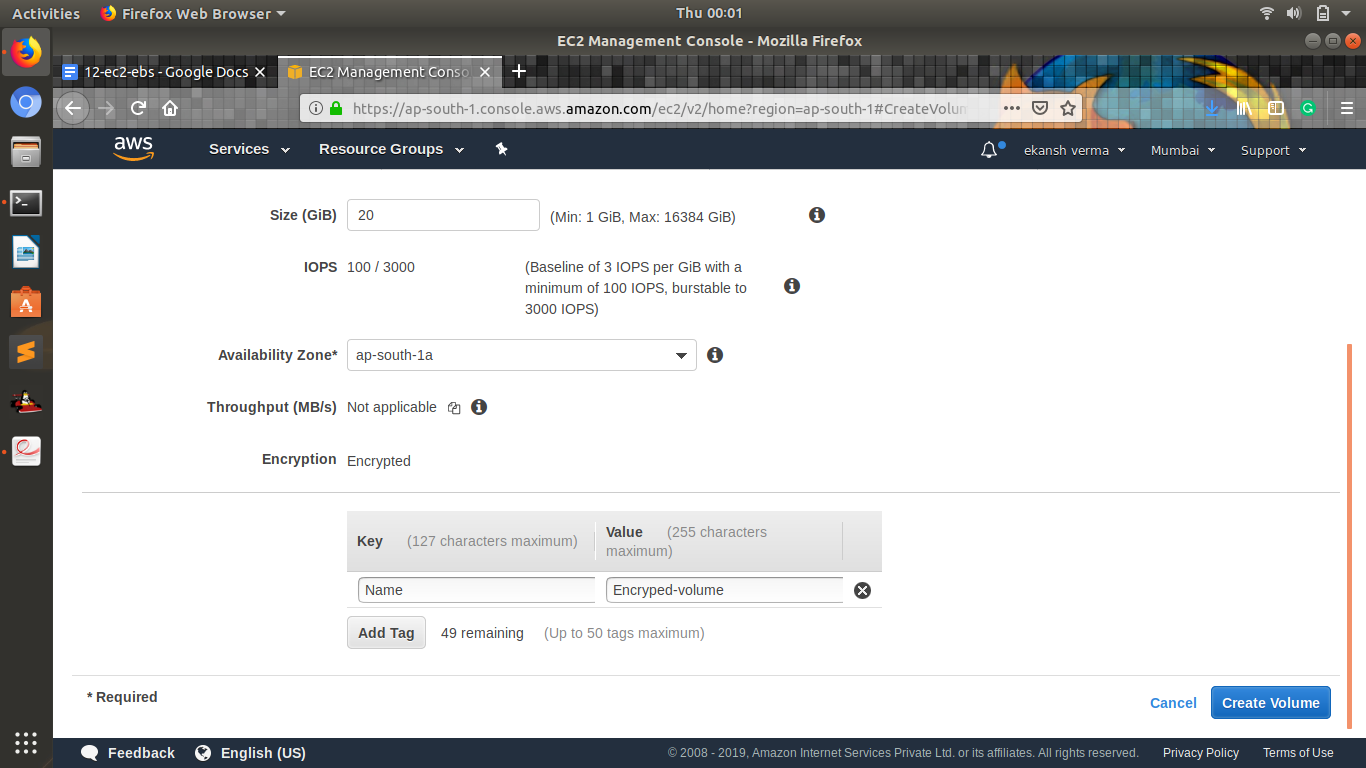
6. Select the CMK for KMS to use as required

7. Click ‘Copy’

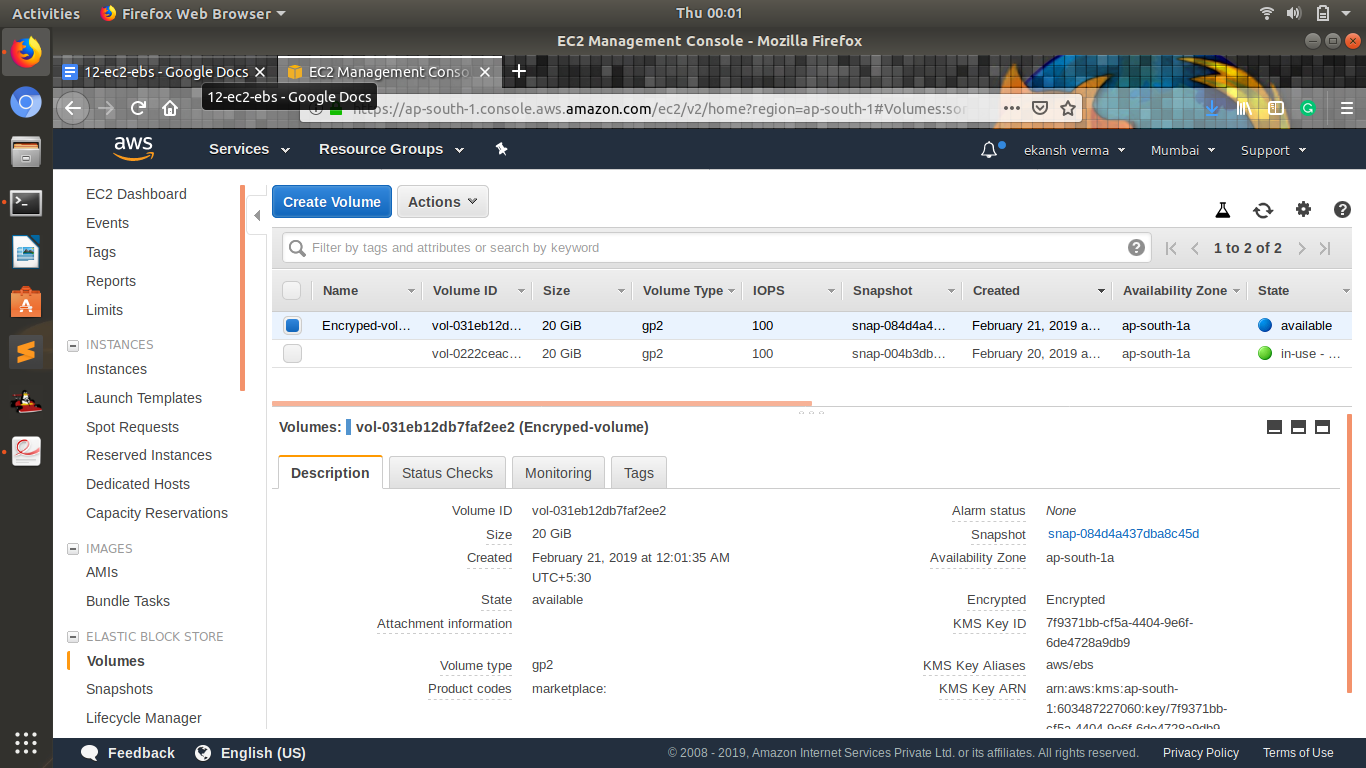


8. Select the newly created snapshot

9. Select ‘Actions’ – ‘Create Volume’



10. 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



* **You have lost the private key for one of the servers, how will you recover ssh access to the server.**

1. Detach the volume from the ec2 instance.
2. Launch a new instance and attach this volume to this new instance.
3. Create new private key of this instance.
4. SSH to this instance.