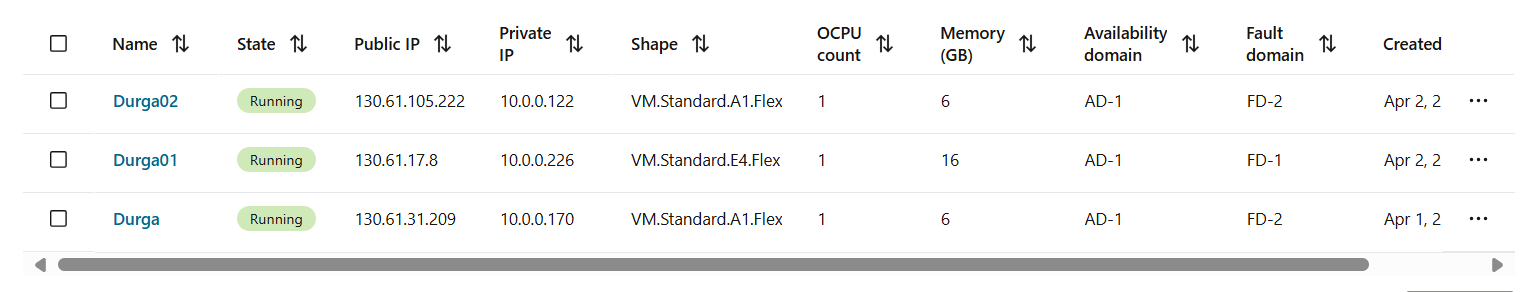
**One Year Accomplishments In Accenture**

1. **Creating a Network File System ( NFS) In One server and Sharing it with the two clients**
2. **Attaching a Block volume to the instance and Partitioning that disk by using LVM process, creating file systems for partitions and mounting them on different mount points.**
3. **Troubleshooting the issues by using console connection to enter into single user mode if server is refusing the key , if you are unable to login to server due to changes made in sudoers file , if you forgot the root password you can change it.**
4. **Synchronizing the clients time with the servers time by using the chronyd service**
5. **Creating a metric-based autoscaling for instance pool created by instance configuration , attaching a load balancer to pool.**
6. **Creating a Network File System ( NFS) In One server and Sharing it with the two clients**

Step -1 : Goto OCI Console and create 3 Virtual Machines (Durga, Durga01, Durga02) within the same VCN and Subnet (Public).



Step-2 : Login to one server by using putty , In my case , I am logging in to Durga01. I will consider this as my nfs server. Login as a root user.

A screen shot of a computer

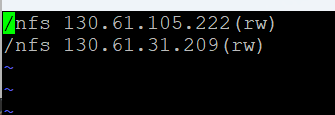
AI-generated content may be incorrect.

Step-3 : Check whether nfs-utils package is installed or not by using below command shown in picture. If not, you can install it by using # dnf install nfs-utils.



Step -4 : After installing the nfs-utils , we have to edit the exports file and add the clients which we want to share.





/nfs : directory I want to share with clients

130.61.105.222, 130.61.31.209 : Ip addresses of clients (Durga02, Durga)

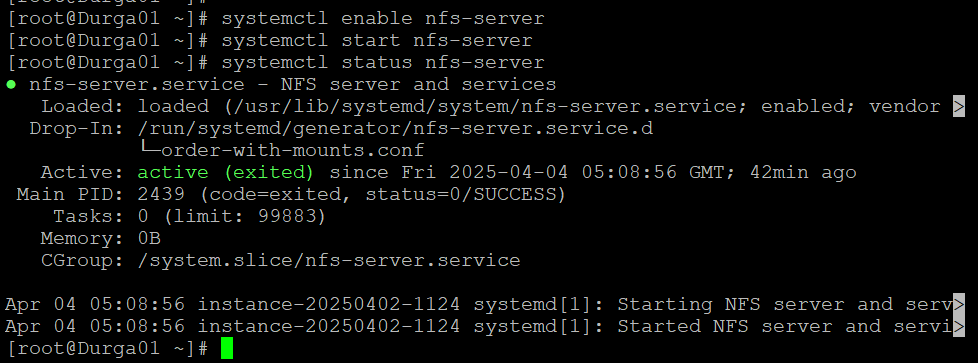
rw: permissions to clients for accessing files (read, write)

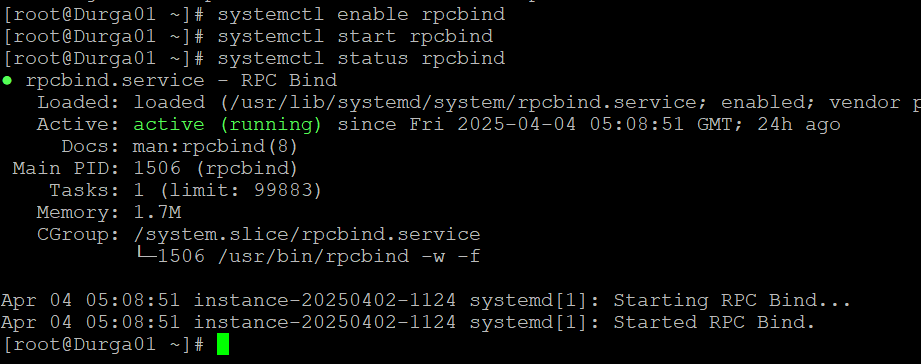
Step-5 : After editing the file , run below command to apply changes to the file.

A group of symbols on a black background

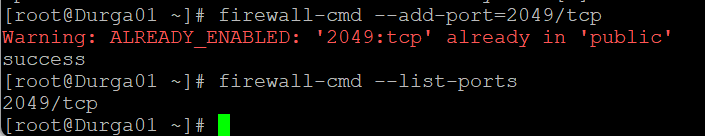
AI-generated content may be incorrect.

Step-6 : Now , Start the services related to NFS and check the status. (nfs-server, rpcbind)

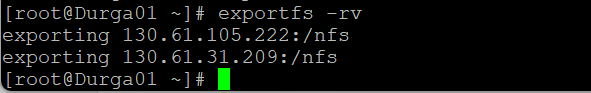




Step-7: Now add the port for nfs (2049) in the firewall



Step -8 : now export the nfs share to allow the clients to connect to this server

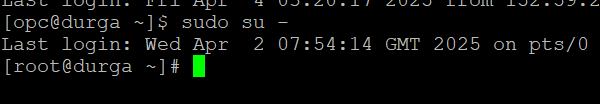


Step-9 : Go to the console , navigate to the security list of your subnet and add the ingress rule for allowing the traffic for port 2049 as shown below

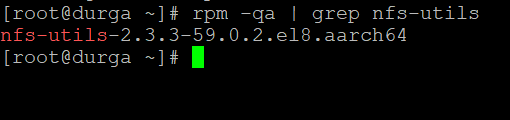
A screenshot of a computer

AI-generated content may be incorrect.

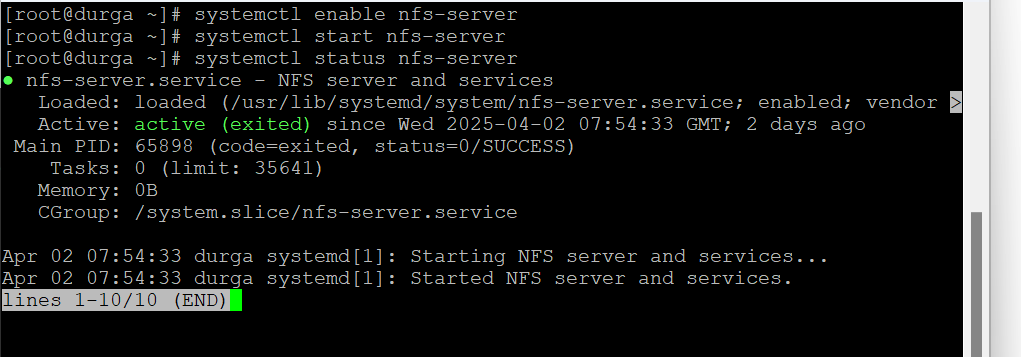
Step-10 : Login to the one of the two clients (Durga, Durga02) by using the putty . Login as a root user. In this case , I logged in to Durga.

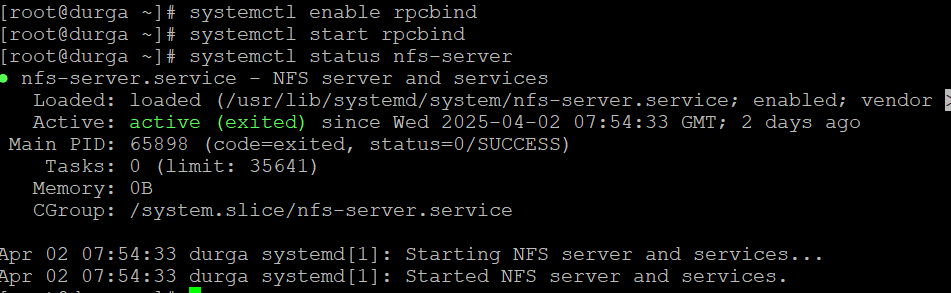


Step-11 : Check whether nfs-utils package is installed or not by using below command shown in picture. If not, you can install it by using # dnf install nfs-utils.

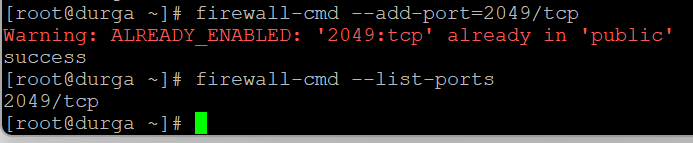


Step-12 : Start the services related to nfs and check the status(nfs-server, rpcbind).

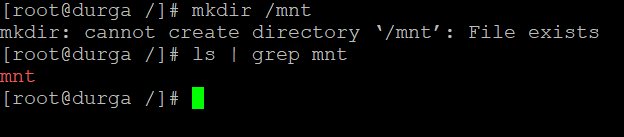




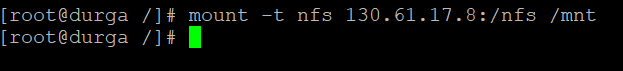
Step-12 : Now add the port for nfs (2049) in the firewall



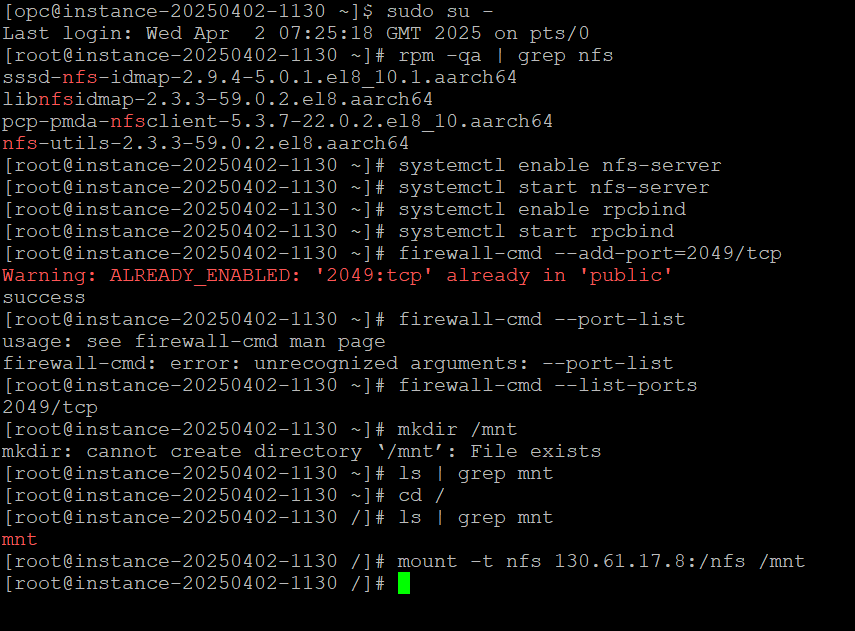
Step -13: Now create a directory for mounting the nfs share as shown below:



Step -14: mount the nfs shared directory with the directory you created as shown below:



Step-15 : Login to the other client and do the same process as we do for Durga.



Nfs has been configured successfully and now we will test it by creating the files in both clients and check whether they are being created in server or not .

Server : Durga01

Client1 : Durga – creating durga file by using the touch

Client2 : Durga02 – creating durga02 file by using the touch.

These two file must be created in the server as well as clients also as we are using nfs.

To verify mount is successful or not , you can check it by using df -h command also.

EX :

A black background with white numbers

AI-generated content may be incorrect.

A black screen with white text

AI-generated content may be incorrect.

A black background with white text

AI-generated content may be incorrect.

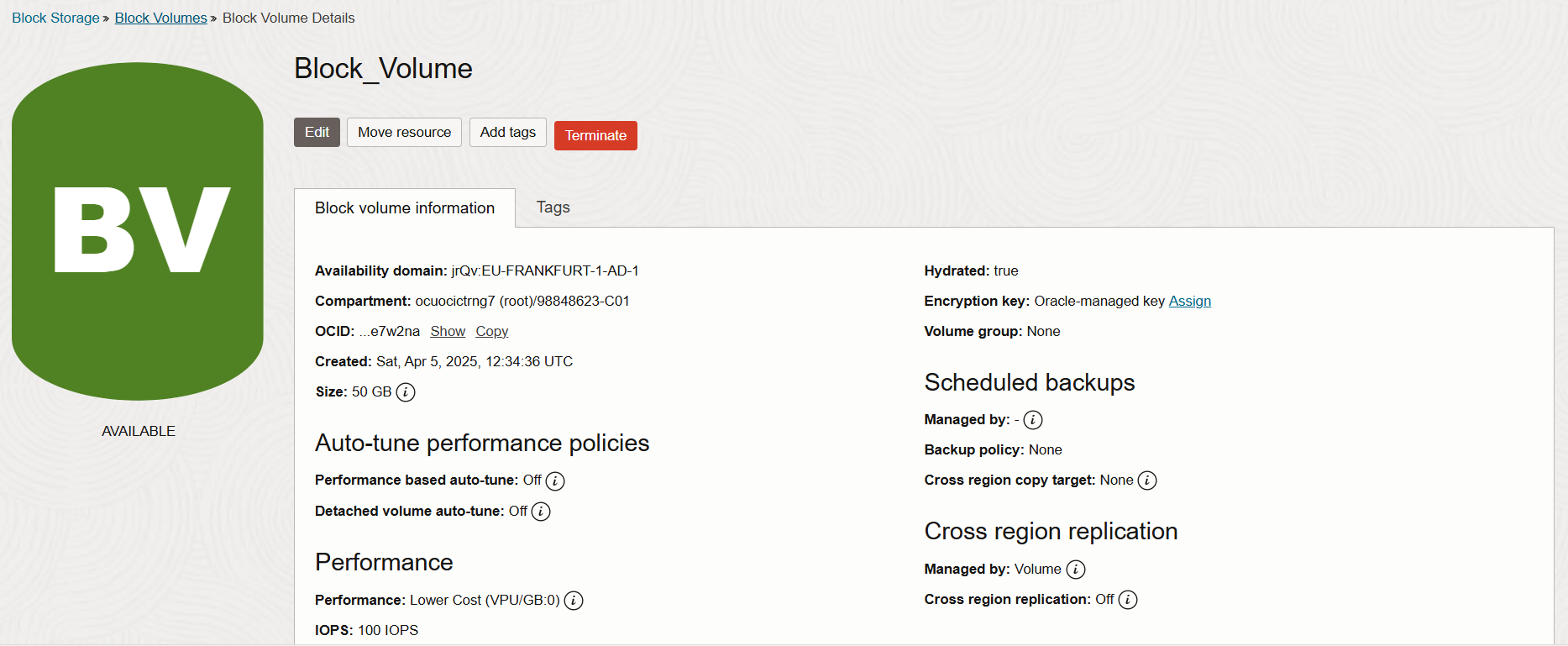
1. **Attaching a Block volume to the instance and Partitioning that disk by using LVM process, creating file systems for partitions and mounting them on different mount points and extending the LVs with attaching new disks.**

Step-1 : Create an instance with the name Durga

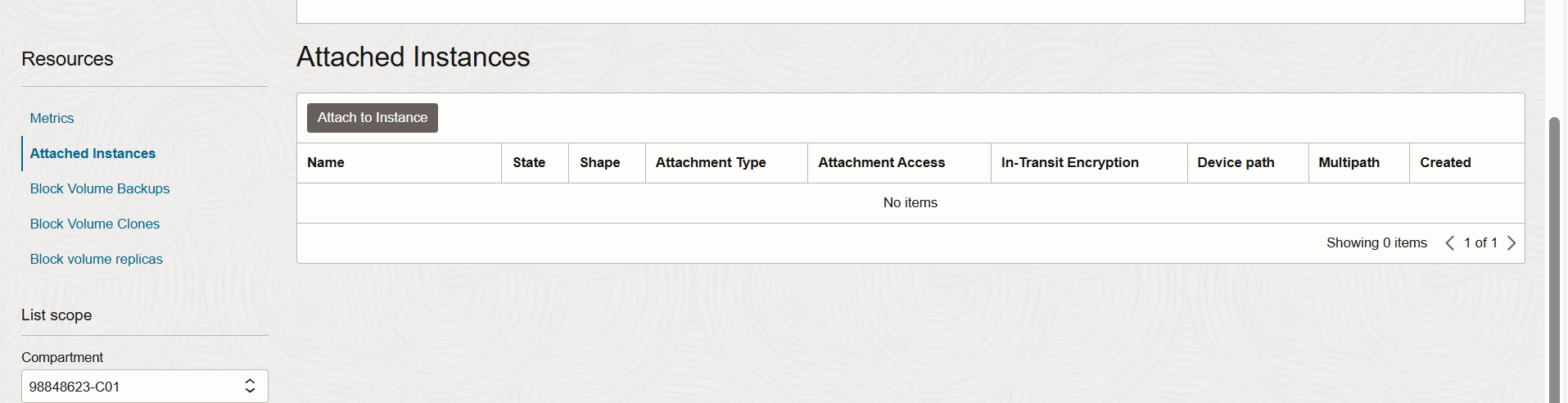
A screenshot of a computer

AI-generated content may be incorrect.

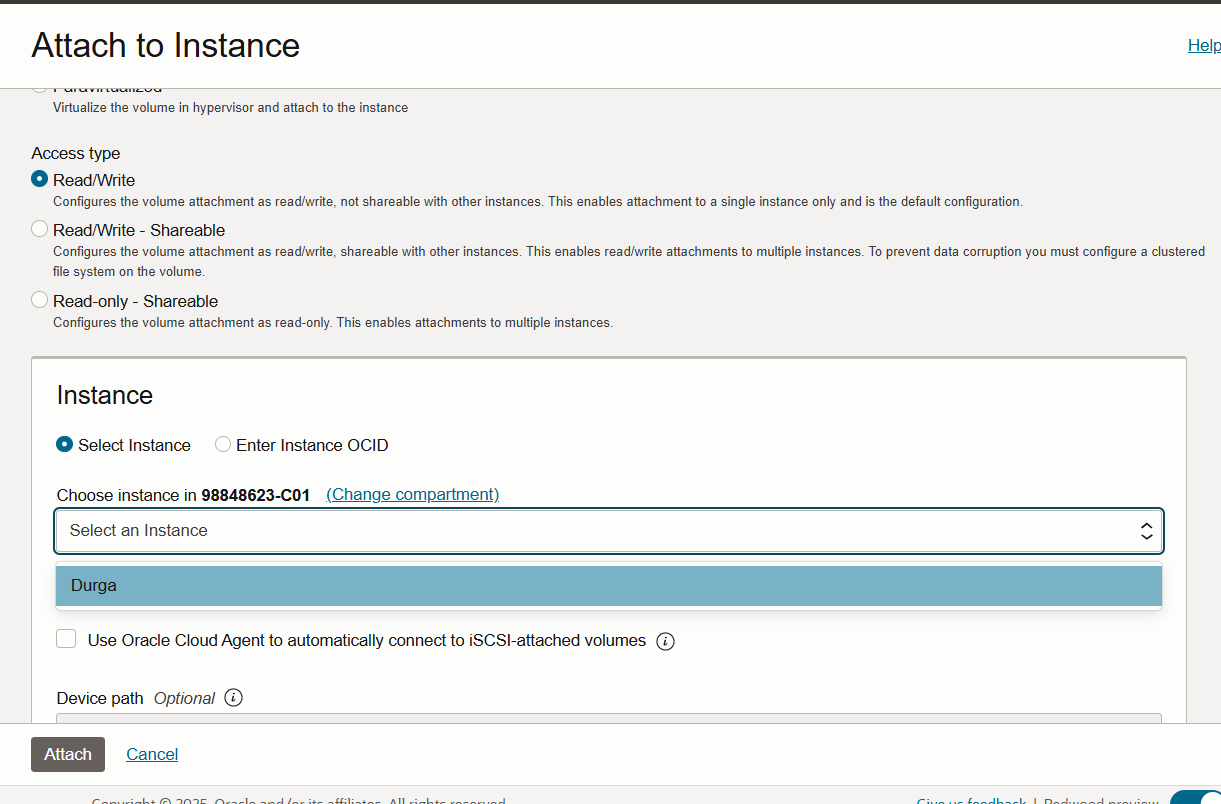
Step-2: create a block volume with a size of 50 GB within the same availability domain.

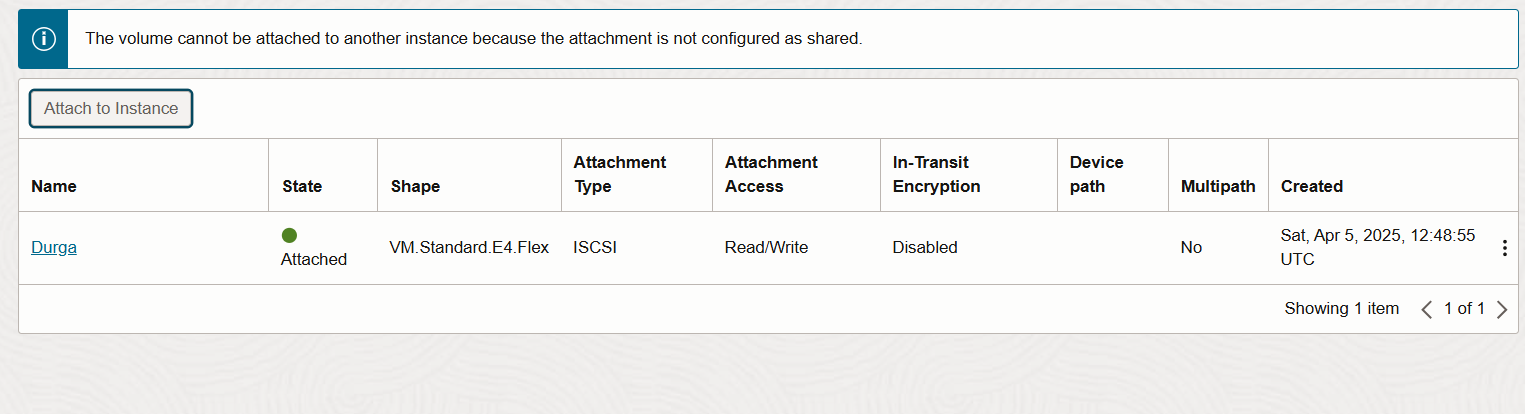


Step-3 : Goto Block Volumes in the console and click on the block volume you created and scroll down you will see attached instances option click on that.



Step-4 : Select Access type as Read/Write and select the instance you want to attach , in our case Durga. Click on Attach





Step-5 : After attaching the volume to the instance , you can login to the instance by using putty and search for the volume as below. Then you will find out the newly added volume sdb here.

A screen shot of a computer

AI-generated content may be incorrect.

Step-6 : Now you can do partitioning to the disk , here I want to create two partitions of 25 GB , and change the partition type to Linux LVM after creating the partition.

A screenshot of a computer program

AI-generated content may be incorrect.

A computer screen shot of a black screen

AI-generated content may be incorrect.

Step-7 : Print the partition table once after creating the partitions.

A computer screen with numbers and letters

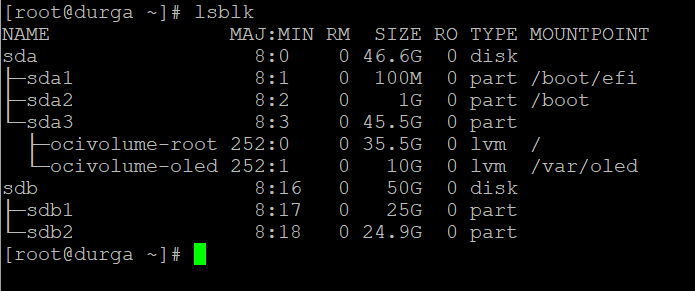
AI-generated content may be incorrect.

Step-8 : Write the changes to the partition table .

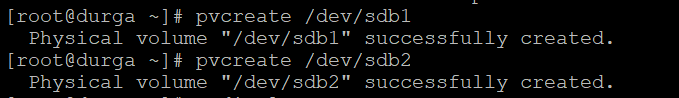
A black background with white text

AI-generated content may be incorrect.

Step-9 : Check whether partitions created or not.



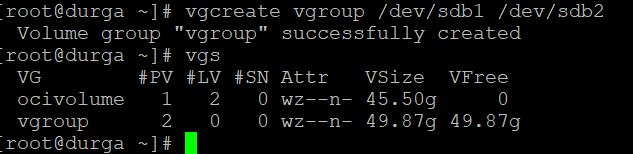
Step-10 : Now create two physical volumes for the both partitions.



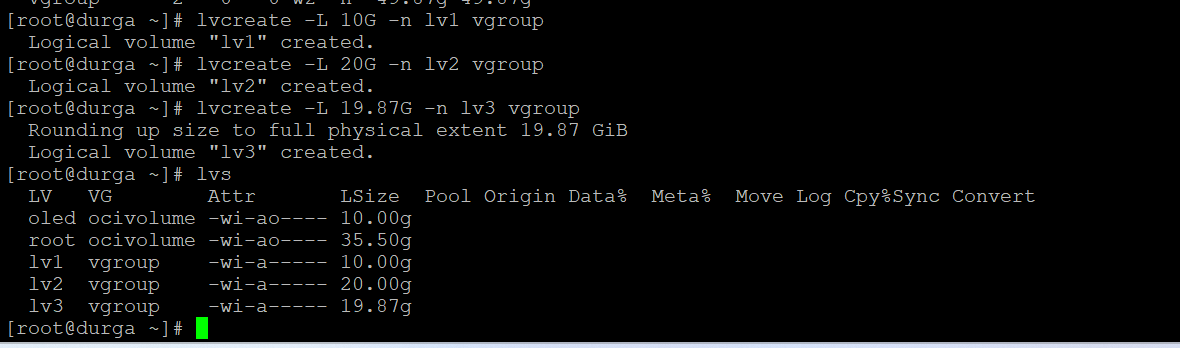
A black background with white text

AI-generated content may be incorrect.

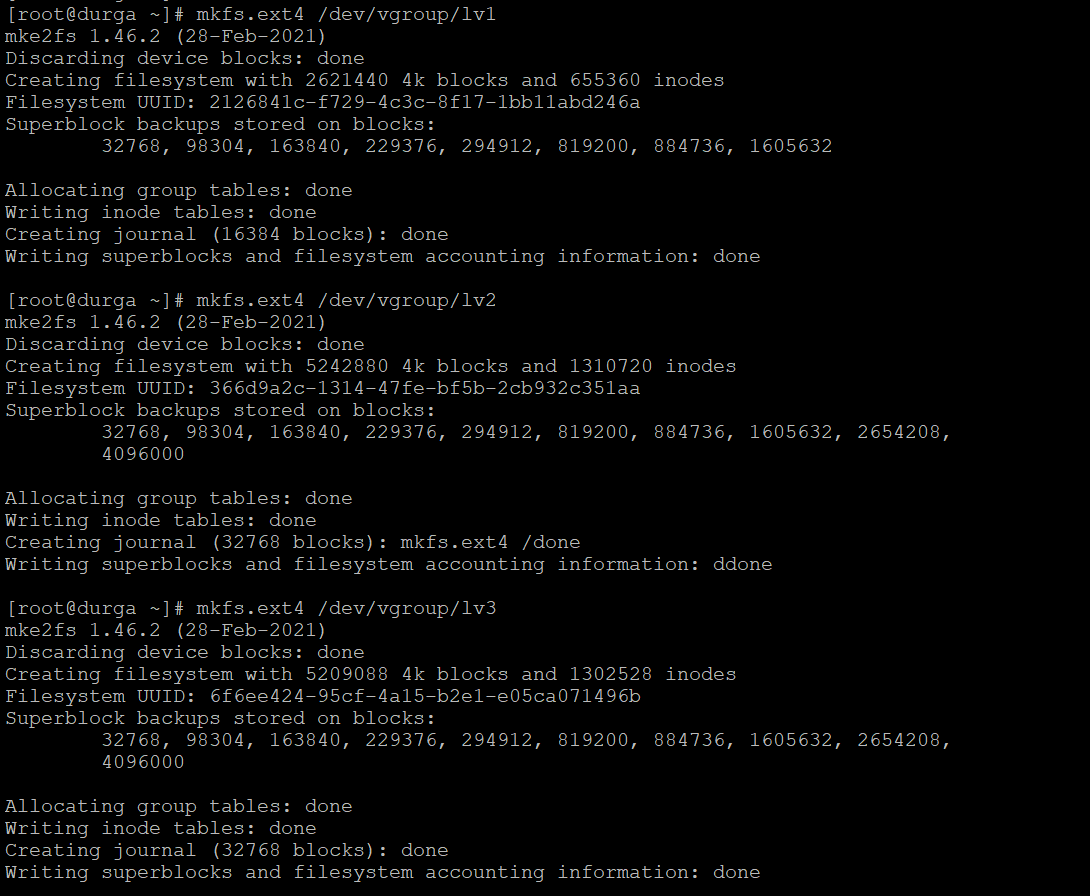
Step-11 : Now create a volume group by adding the both physical volumes to volume group. In this case, ‘vgroup’ is volume group.



Step-12 : Now Create three logical volumes of size 10GB, 20GB, 20GB by using the volume group (vgroup we created earlier of 50GB).



Step -13 : Now apply a filesystem for each logical volume. In this case , I am applying ext4 filesystem.

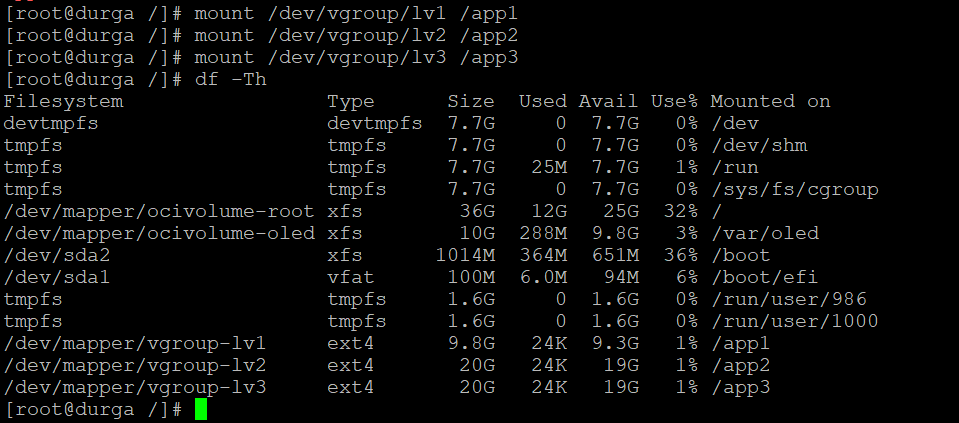


Step-14 : Now create three mount points for mounting the logical volumes we created. I am creating /app1, /app2, /app3.

A screenshot of a computer program

AI-generated content may be incorrect.

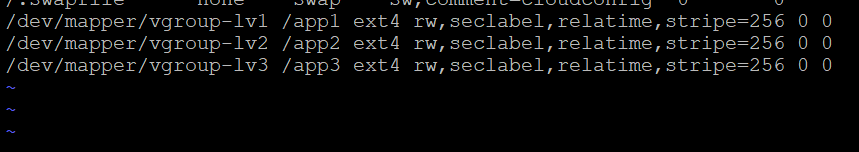
Step-15 : Now mount the LVs on the mount points you created.



Step -16 : If you want to make these mount points persistent after reboot, then you can add them in the end of the /etc/fstab file.

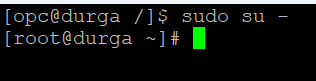
A green rectangle with white text

AI-generated content may be incorrect.

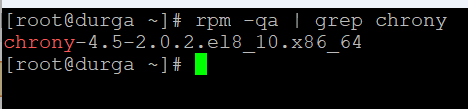


1. **Synchronizing the clients time with the servers time by using the chronyd service**

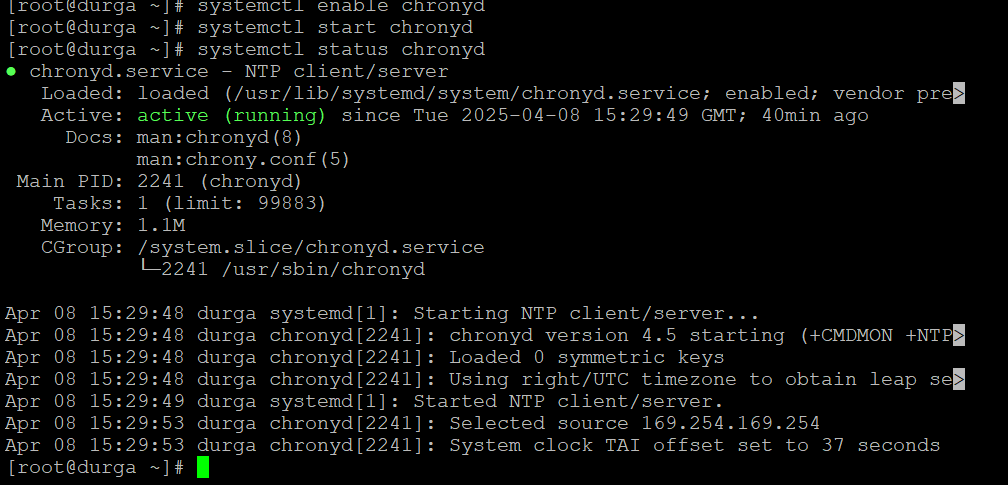
Step-1 : Login to the instance(durga) by using putty and login as a root user. Consider this as a server.



Step-2 : Check whether the chrony package is installed or not . If not , install it by using this command ‘dnf install chrony’



Step-3 : Now , you have to enable and start the chronyd service as shown below and check status.



Step-4 : Find the location of chrony.conf file and open it by using vi editor

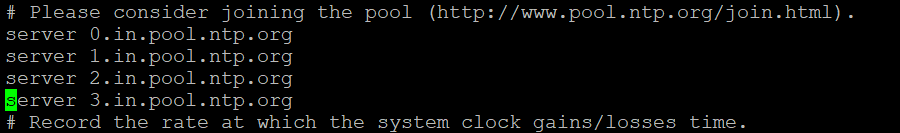
A screenshot of a computer screen

AI-generated content may be incorrect.

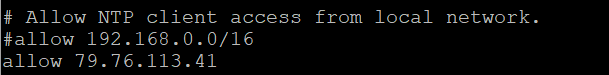


Step-5 : Edit the chrony.conf file and add the lines shown below in the chrony.conf file. We are adding the pool zone of india in the chrony.conf file.

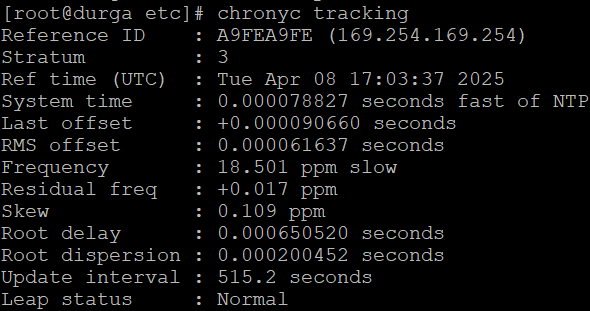




Step -6 : Allow the client , In our case Durga01(79.76.113.41) which you need the to synchronize the time with.



Step-7 : To check if the server is running correctly , use below command , it will show synchronization status of NTP. As it is still connecting to older server (169.254.169.254) , you need to restart the chronyd service.

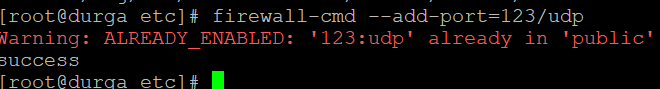




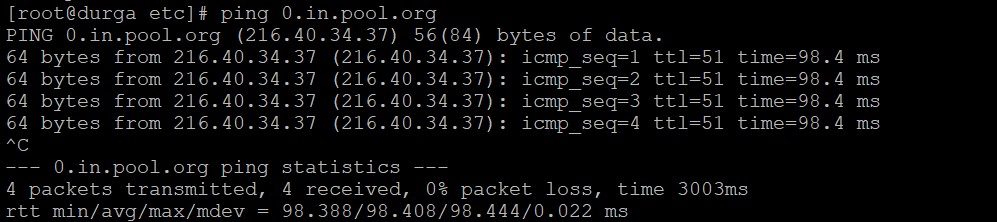
Step -8 : It is still shows the not synchronized in leap status that means server we added did not synced yet.



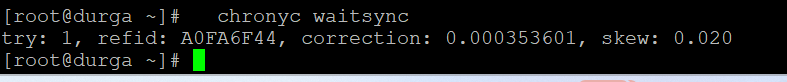
Step-9: Add the port number 123 to the firewall, using below command



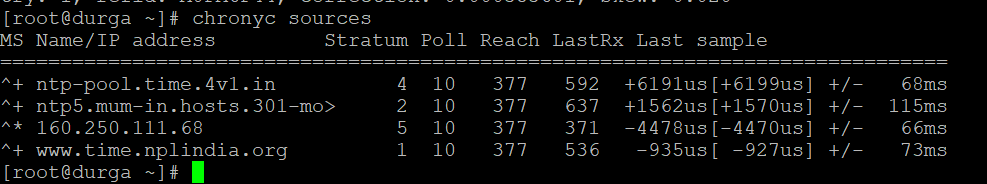
Step-10 : Try to ping the one of the server in the pool , whether it is working or not. It is working in our case as packet loss is 0%.



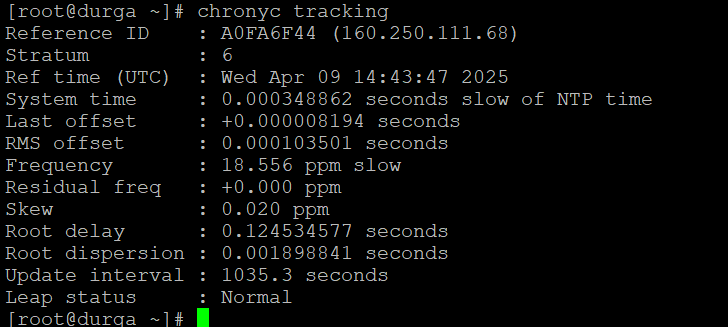
Step-11 : Synchronize the time by using the ‘chronyc waitsync’ command.



Step-12 : Now , check which source the server is synchronized with , ^\* means our server is synchronized with that server for the time.



Step-13 : Now check the leap status is normal or not and our server is synchronized with which server by using below command.



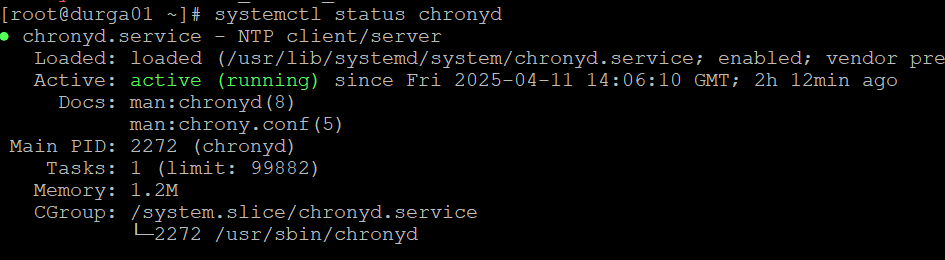
Server configuration is completed.

Step-14 : Login to the Client server as root user

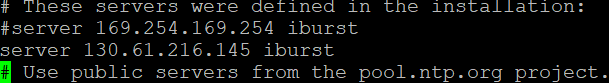
A number symbols on a black background

AI-generated content may be incorrect.

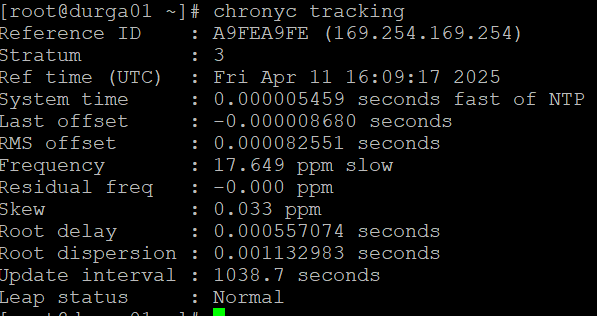
Step-15 : Check whether the chronyd service is running or not.



Step-16 : edit the /etc/chrony.conf file and add the server durga entry in the file as below



Step-17 : To check if the server is running correctly , use below command , it will show synchronization status of NTP. As it is still connecting to older server (169.254.169.254) , you need to restart the chronyd service.

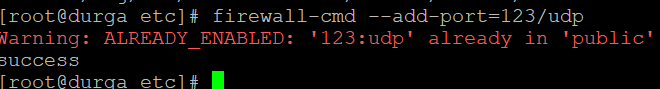




Step-18 : : It is still shows the not synchronized in leap status that means server we added did not synced yet.



Step-19: Add the port number 123 to the firewall, using below command



Step -20 : Try to synchronize the time with the server by using waitsync command. As we can see below , it is not syncing.

A screen shot of a computer

AI-generated content may be incorrect.

Step-21 : Now try to check whether you can ping the server or not. Now we can see below that client is not able to ping the server.

A black screen with numbers and text

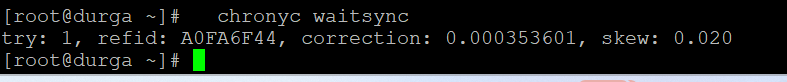
AI-generated content may be incorrect.

Step-22 : Now add the ICMP rule in the security list to be able to ping the server.

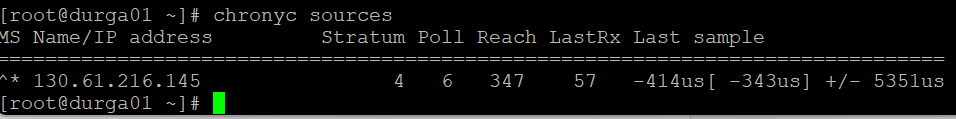
A close up of a computer screen

AI-generated content may be incorrect.

Step-23 : Synchronize the time by using the ‘chronyc waitsync’ command.



Step-24 : Now , check which source the server is synchronized with , ^\* means our server is synchronized with that server for the time.



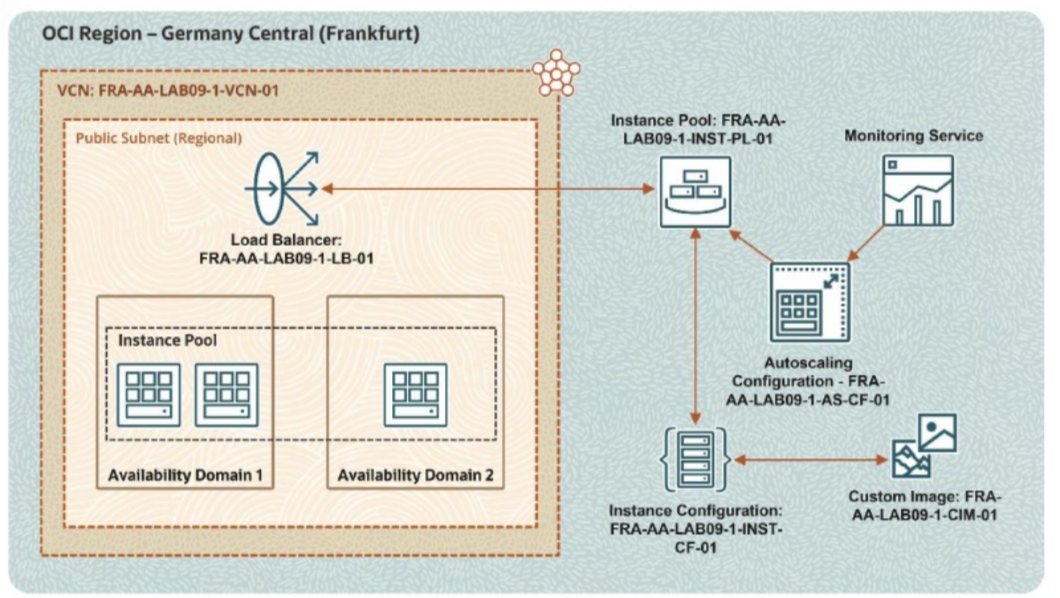
Step-25 : Now check the leap status is normal or not and our server is synchronized with which server by using below command.

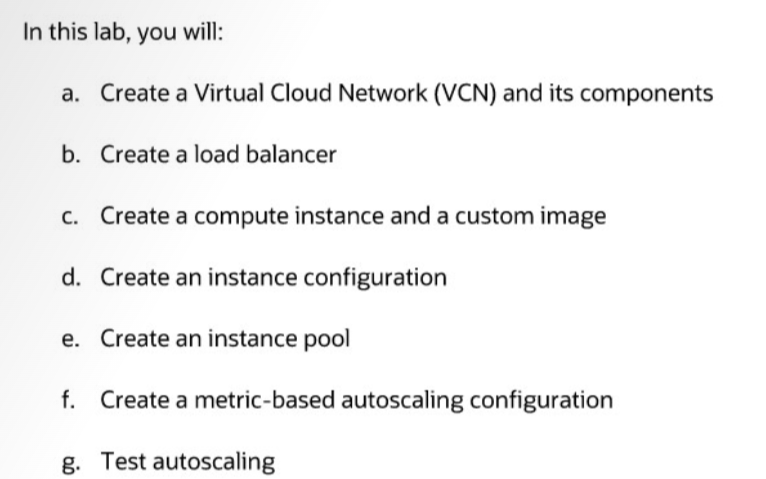
A screenshot of a computer

AI-generated content may be incorrect.

Time synchronization for client with the server is completed.

1. **Creating a metric-based autoscaling for instance pool created by instance configuration , attaching a load balancer to pool.**

****

****

Step-1 : In this first step we will create a VCN, a Subnet, An Internet Gateway and add it to route table, add an ingress rule in security list for port 80 – http.

Create a Virtual Cloud Network and Its Components

In this practice, you will create a Virtual Cloud Network (VCN), subnet, and Internet gateway,

and add route rules in the route table.

Tasks

1. Sign in to your Oracle Cloud Infrastructure (OCI) Console.

2. From the navigation menu, under Networking, select Virtual Cloud Networks.

3. Click Create VCN.

4. In the Create a Virtual Cloud Network dialog box, populate the following information:

• Name: FRA-AA-LAB09-1-VCN-01

• Create In Compartment: <your compartment>

• IPv4 CIDR Blocks: 10.0.0.0/16

5. Keep all the other options default and click Create VCN.

Note: You can see that the VCN is created successfully.

6. Click FRA-AA-LAB09-1-VCN-01 to view the details and click Create Subnet.

7. In the Create Subnet dialog box, populate the following information:

• Name: FRA-AA-LAB09-1-SNET-01

• Create In Compartment: <your compartment>

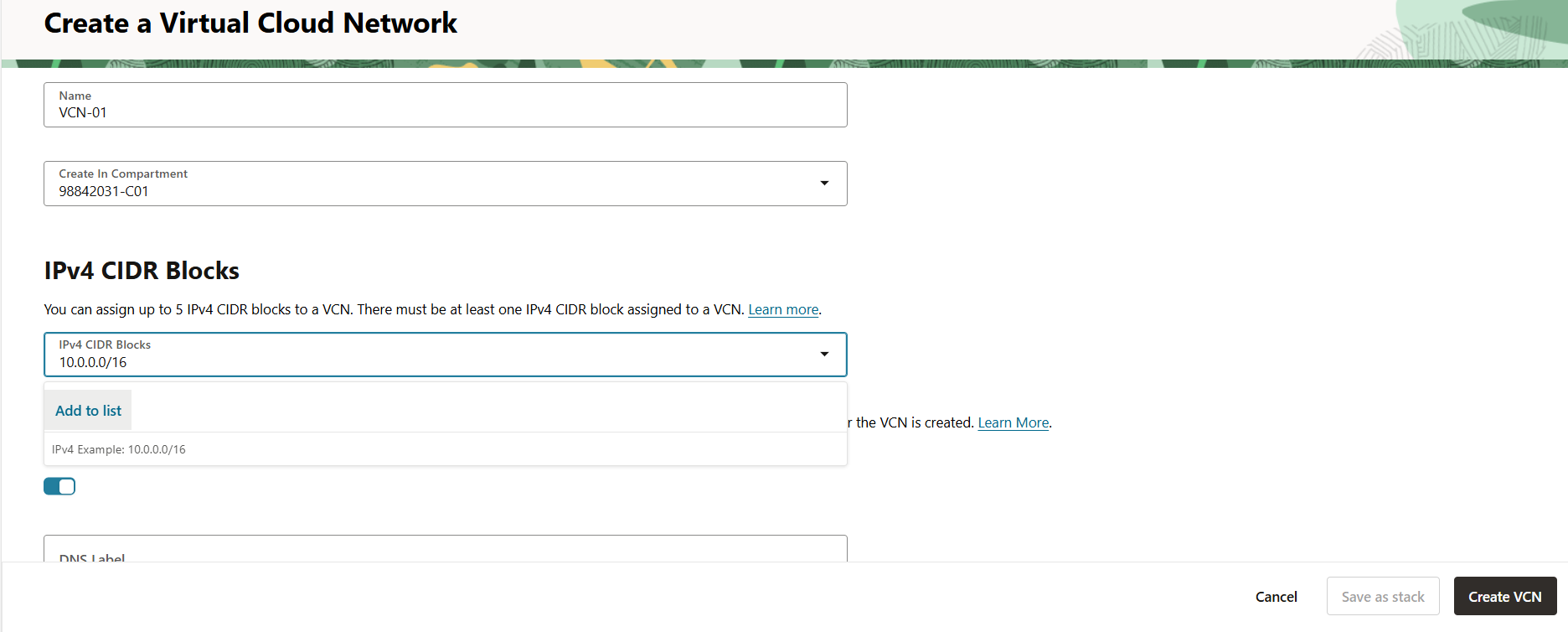
• Subnet Type: Regional

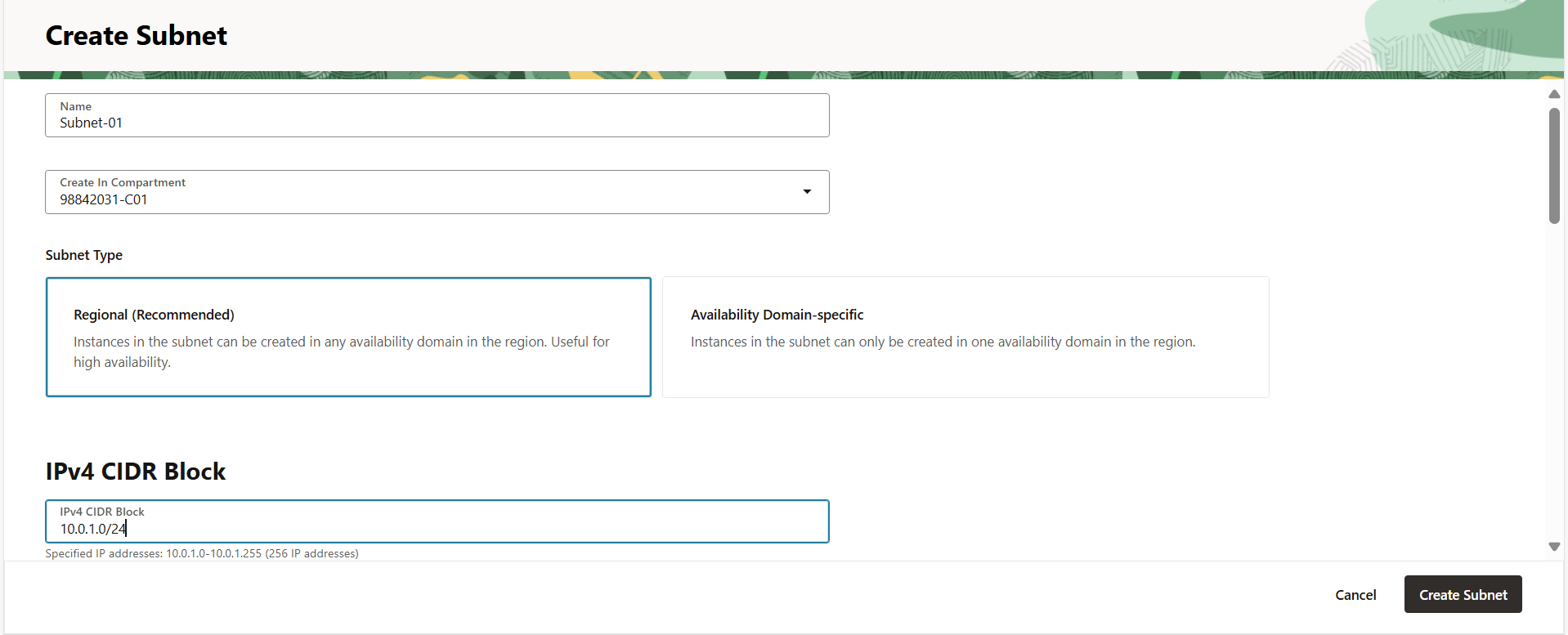
• IPv4 CIDR Blocks: 10.0.1.0/24

• Subnet Access: Public Subnet

8. Keep all the other options default and click Create Subnet.

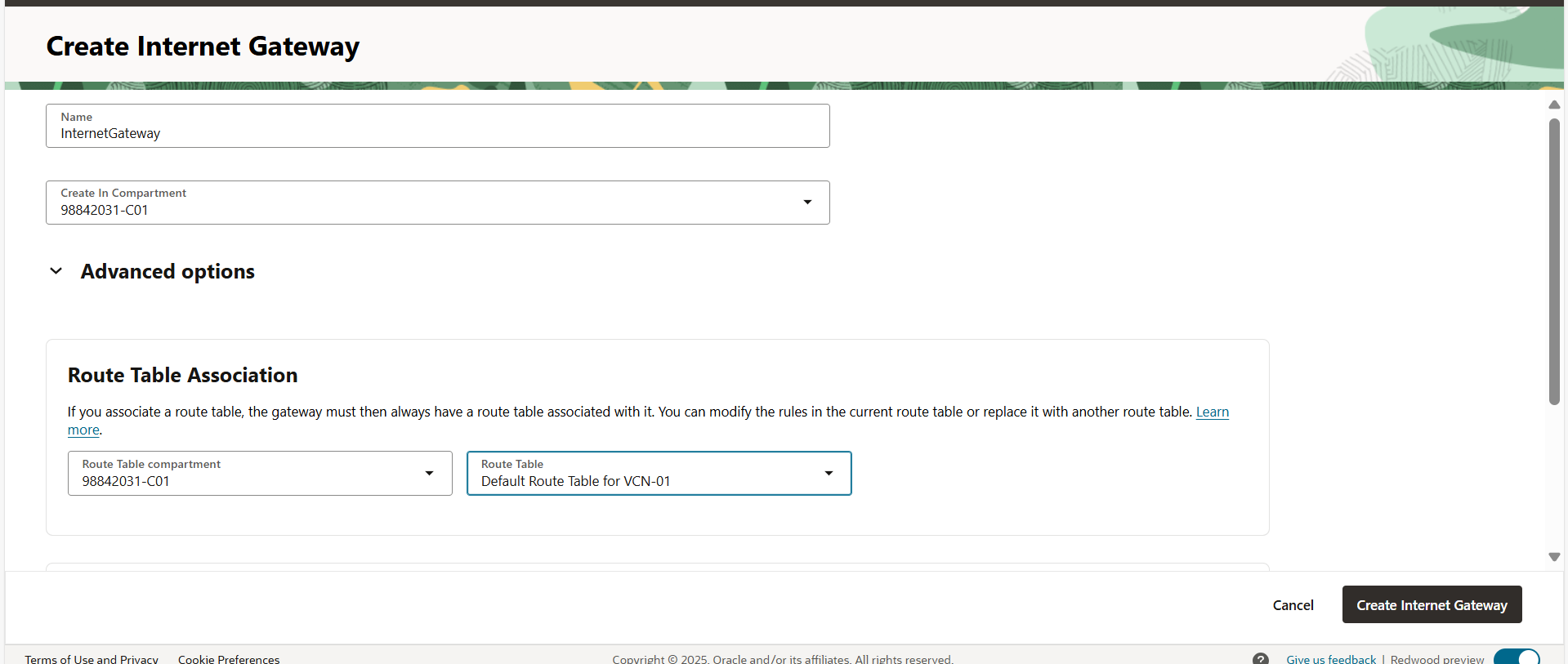
9. Under Resources in the left navigation panel, click Internet Gateways.

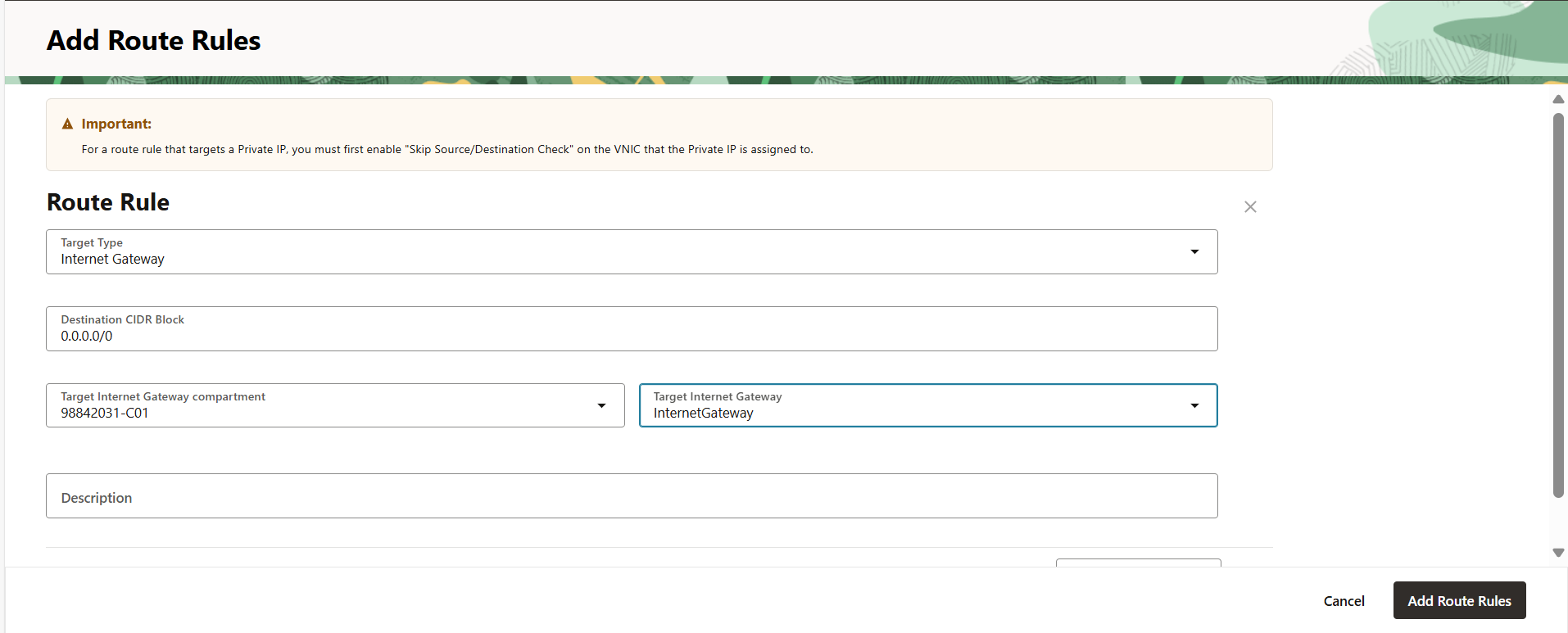


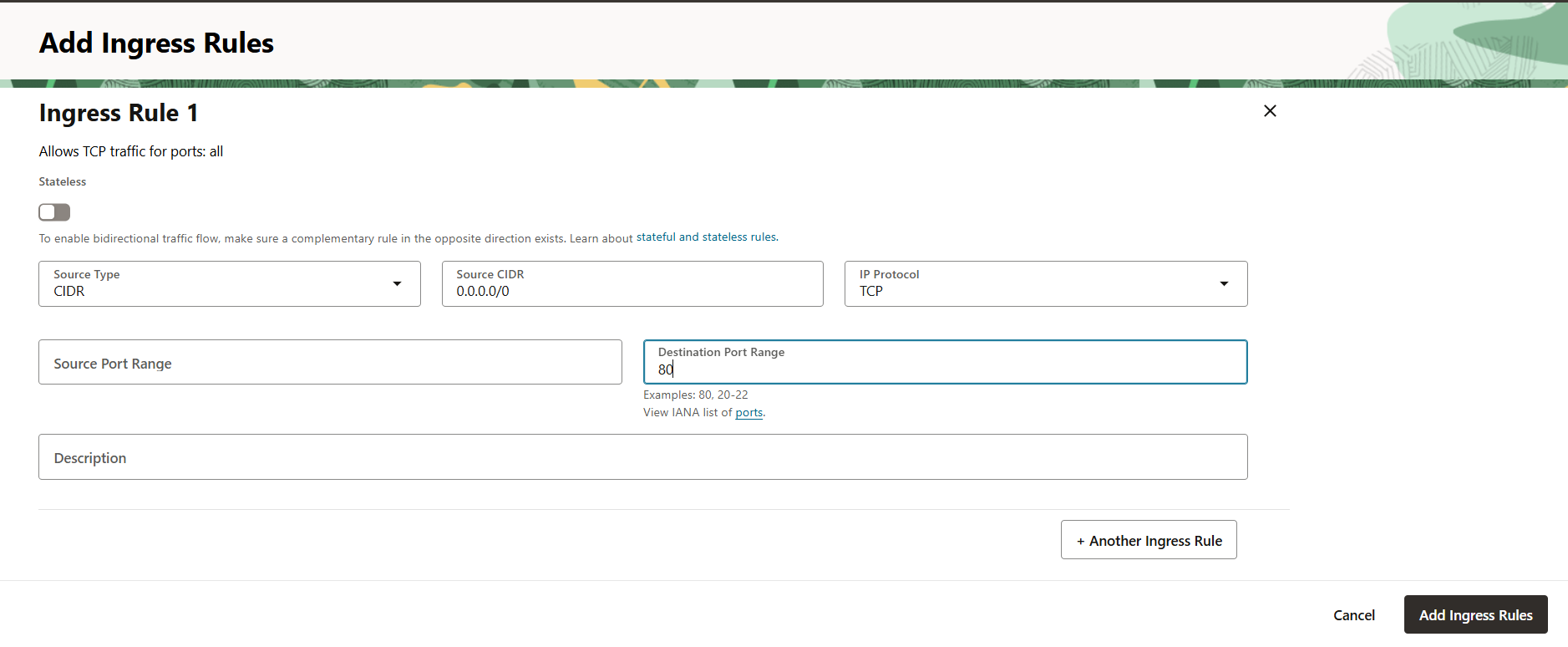


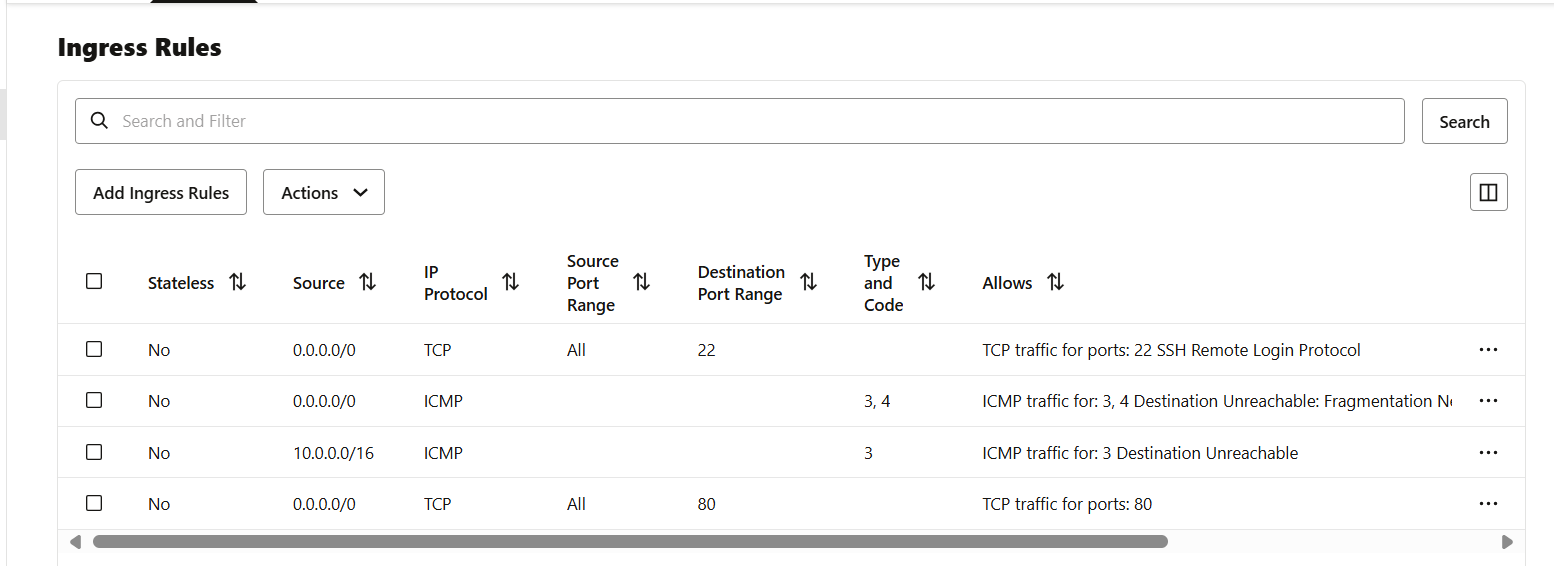
A screenshot of a computer

AI-generated content may be incorrect.

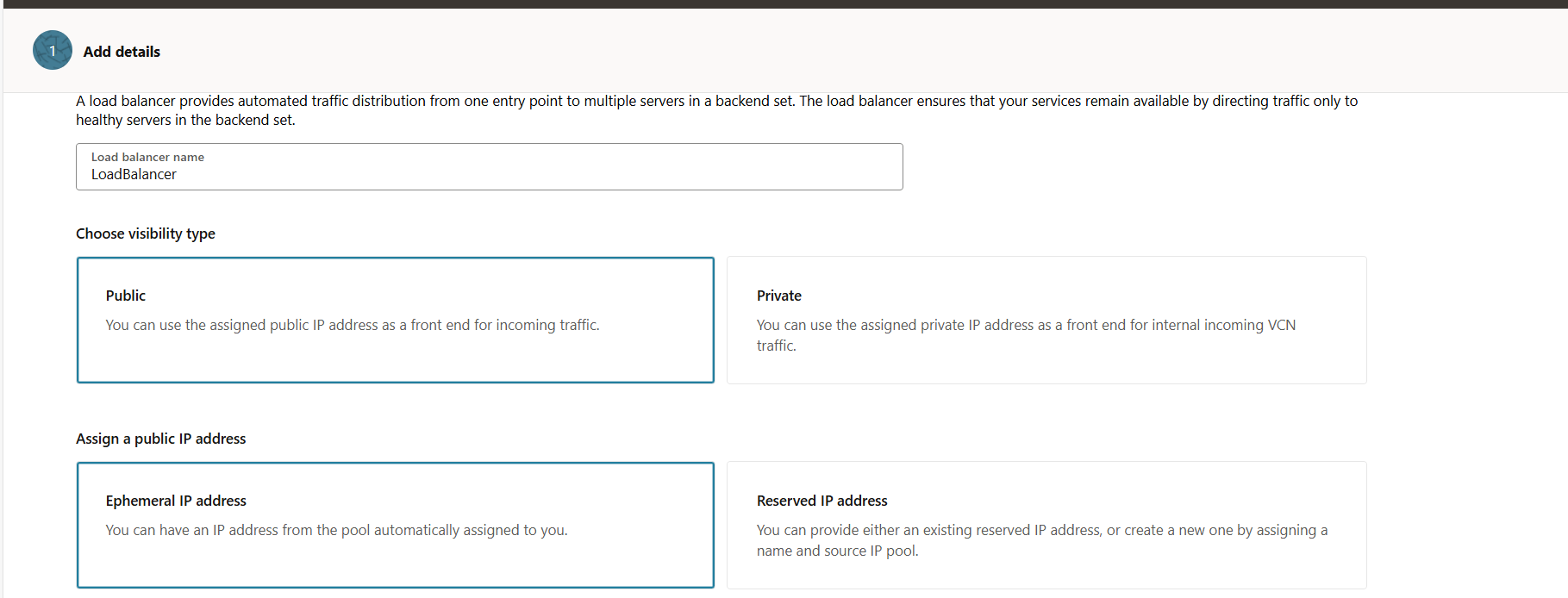






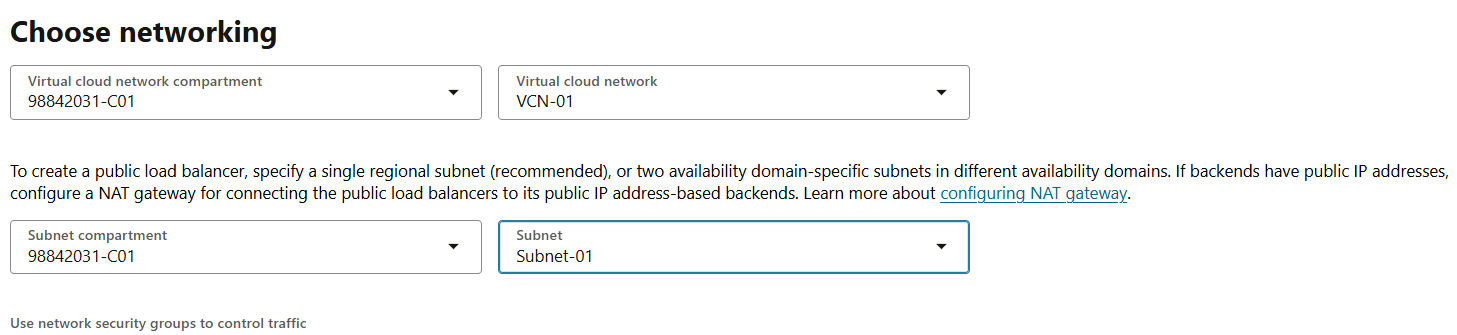


Step-2 : Creating a load balancer without attaching any backend instances as we will create instance pool and will attach it to LB.



A screenshot of a computer

AI-generated content may be incorrect.



A screenshot of a computer

AI-generated content may be incorrect.

A white background with black and white clouds

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A close up of a text

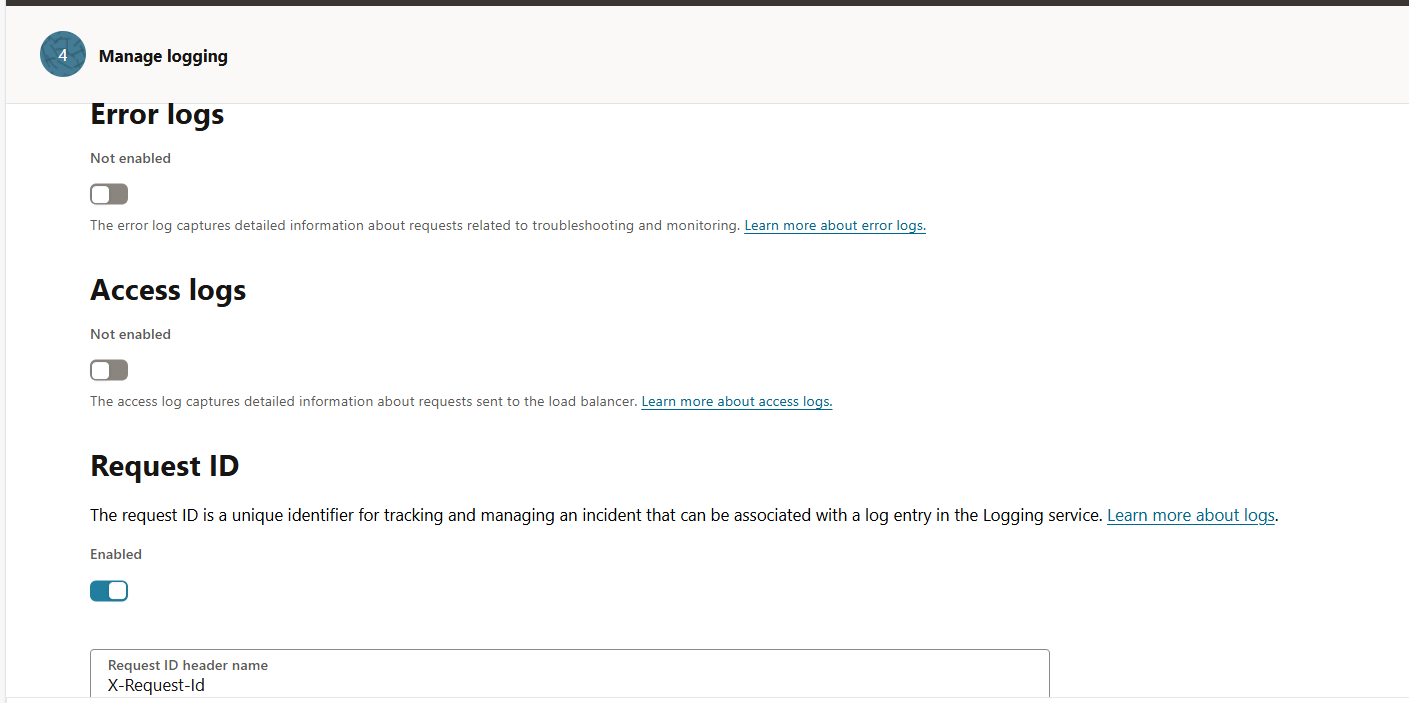
AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

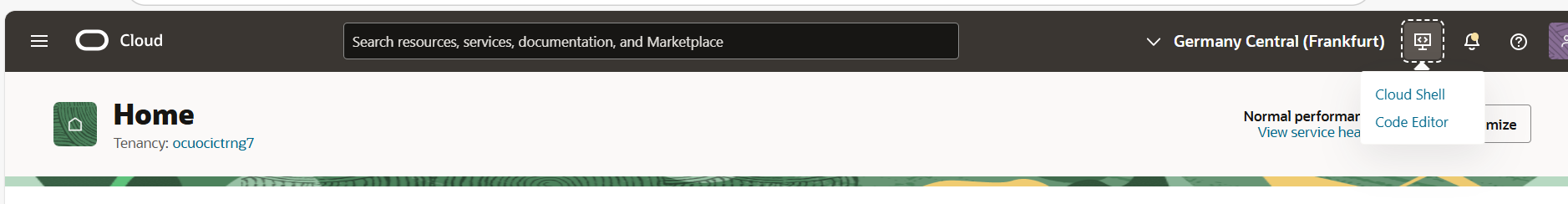
A screenshot of a computer

AI-generated content may be incorrect.



Step-3 : Creating a compute instance and custom image

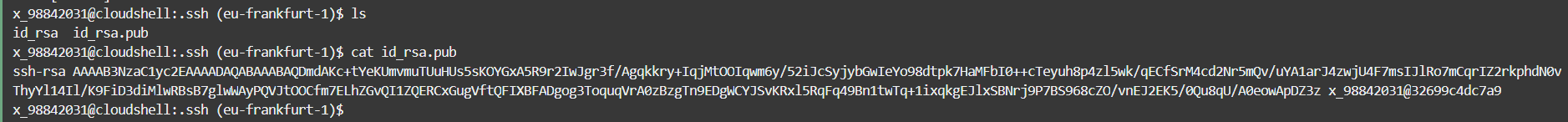
3.1 : Launch cloud shell



3.2: Create an ssh key pair using ssh-keygen command



3.3 Copy the public key for pasting it while creating instance.



3.4: Create an instance and while creating paste the public key copied.

Click Create instance and populate the following information:

• Name: FRA-AA-LAB09-1-VM-01

• Create in compartment: <your compartment>

• Availability Domain: AD 1 .

Click Show advanced options and select On-demand capacity under Capacity type.

• Image: Oracle Linux 8

• Shape: Select VM.Standard.A1.Flex (1 OCPU, 6GB Memory) [Shape series: Ampere]

• Primary Network: Select existing virtual cloud network.

• Virtual cloud network in <your compartment>: FRA-AA-LAB09-1-VCN-01

• Subnet: Select existing subnet.

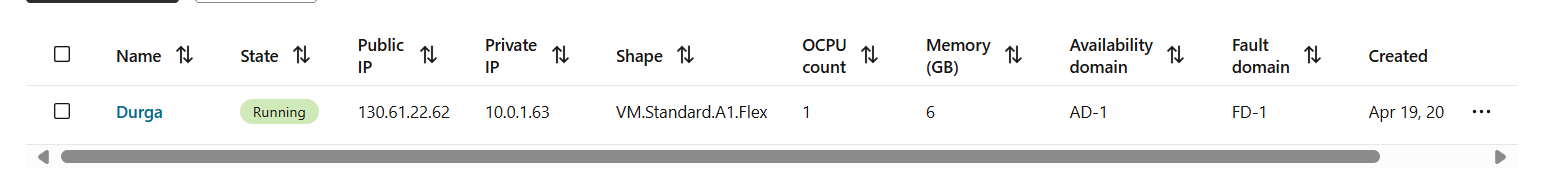
• Subnet in <your compartment>: FRA-AA-LAB09-1-SNET-01 (regional)

• Public IP address: Assign a public IPv4 address.

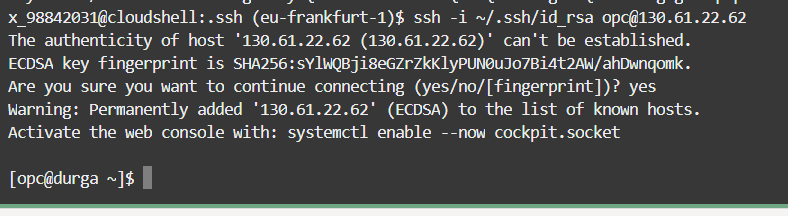
• Add SSH keys: Paste public keys.

• SSH Keys: <contents of the public key> (which is copied in Step 5 of this practice)

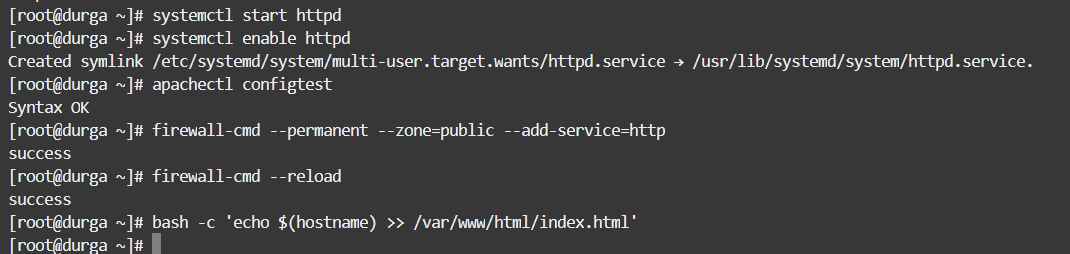
8. Keep the Boot Volume default and click Create



3.5: Open cloud shell and login to the instance , install apache server, start the service and edit data in index.html file.







3.6 Creating the custom image,

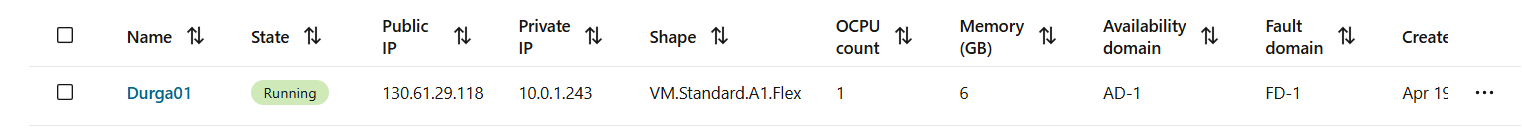
A screenshot of a computer

AI-generated content may be incorrect.

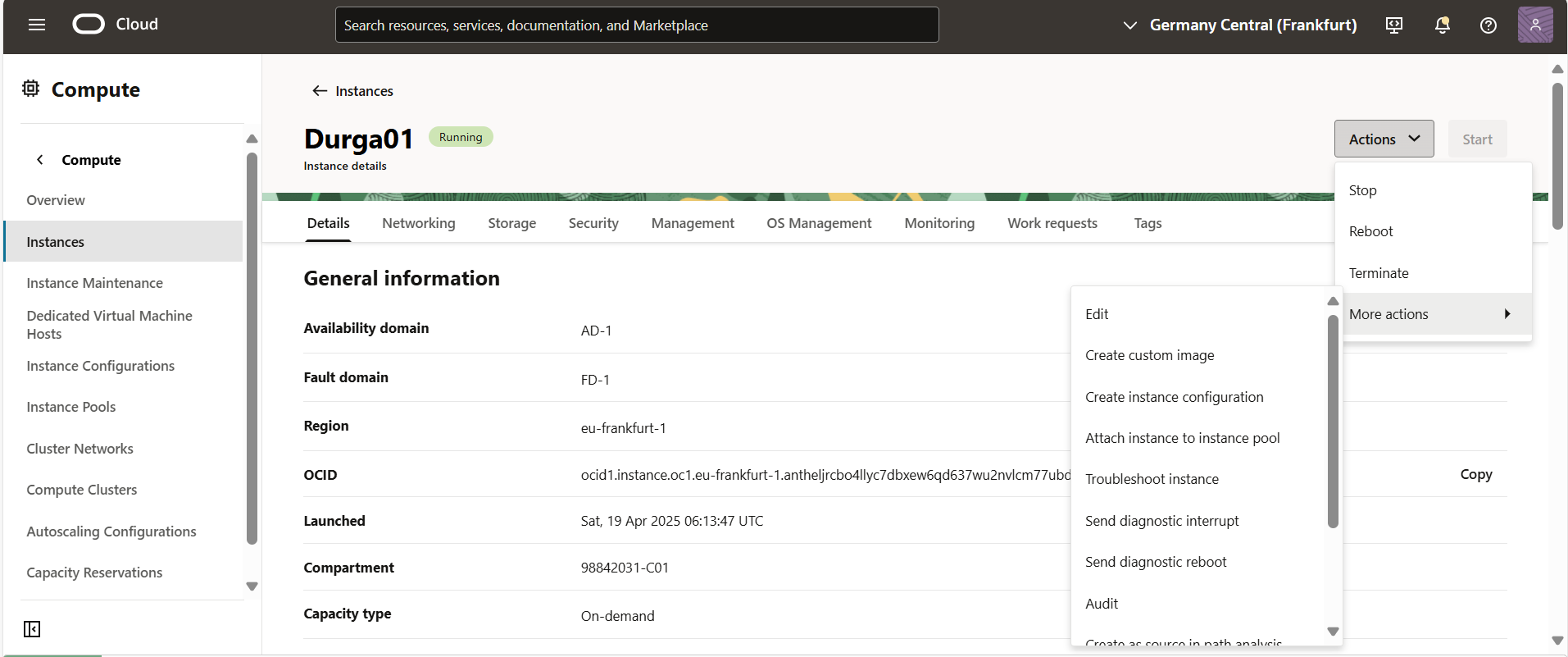
A screenshot of a computer

AI-generated content may be incorrect.

3.7: create an instance by using the custom image



Step-4: Creating an instance configuration by using the instance we created above.



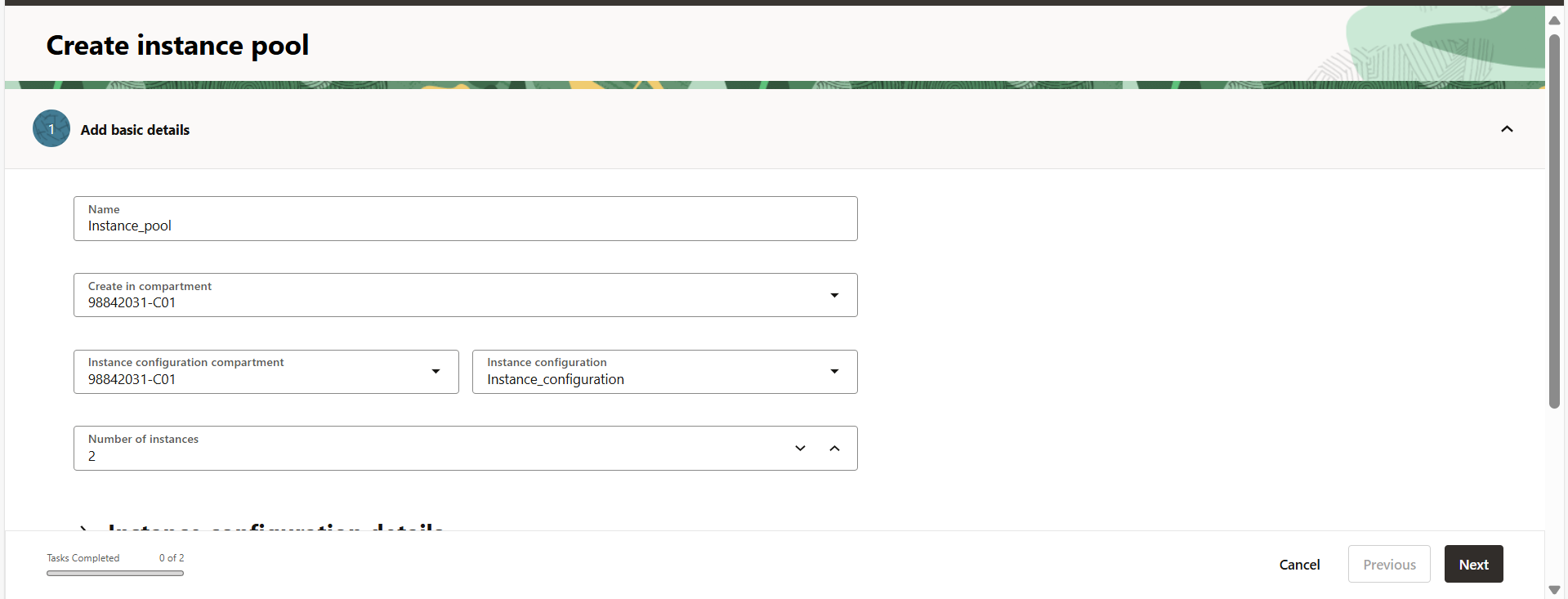
A screenshot of a computer

AI-generated content may be incorrect.

**A white background with black and blue text

AI-generated content may be incorrect.**

Step-5 : Creating the instance pool by using the instance configuration and attaching the load balancer to it.



A screenshot of a computer

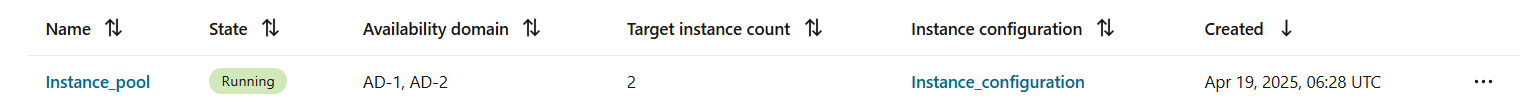
AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

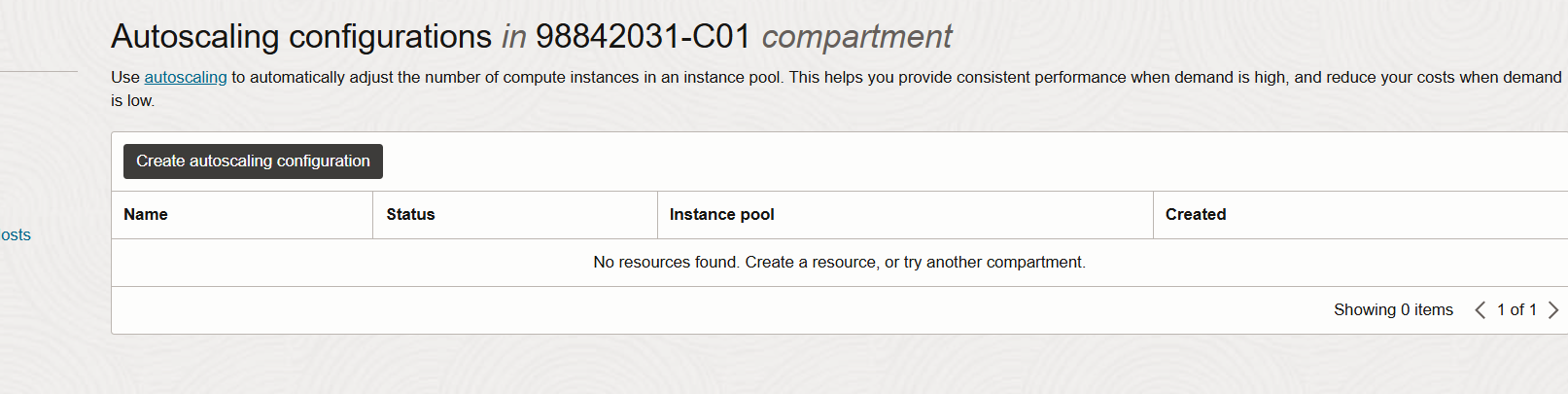
A screenshot of a computer

AI-generated content may be incorrect.



Step-6 : Creating the autoscaling configuration.

A screenshot of a computer

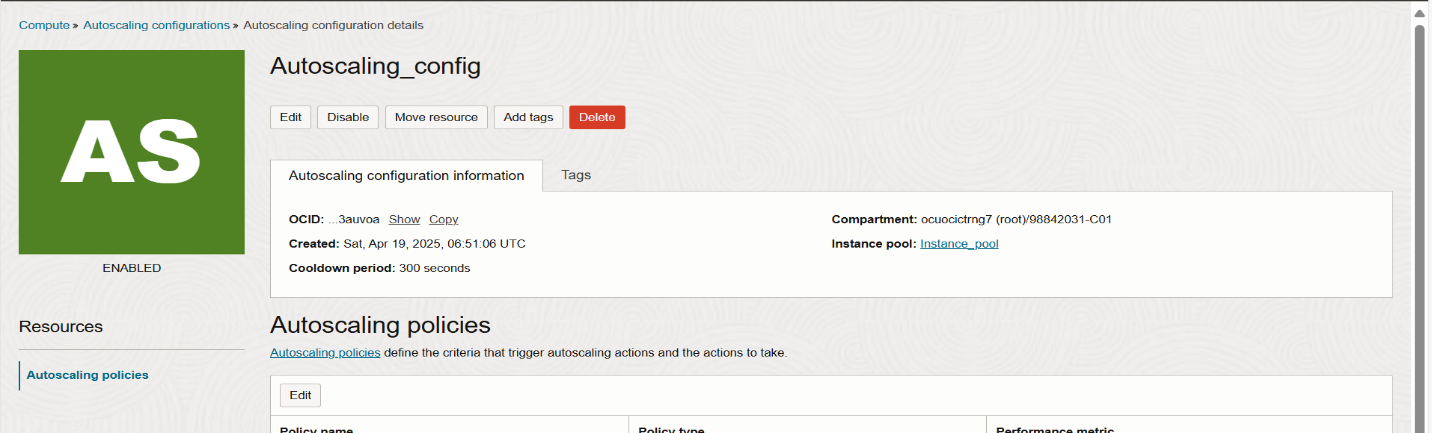
AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

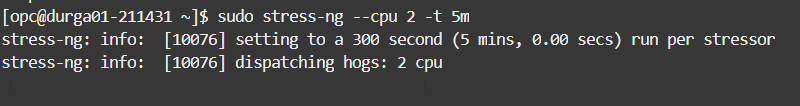


Step-7: Testing the autoscaling configuration is working or not. Connect to the instance in the instance pool by using the cloud shell and increase cpu threshold beyond 70 by using the stress command and watch it for few minutes it will add the new instance to the pool







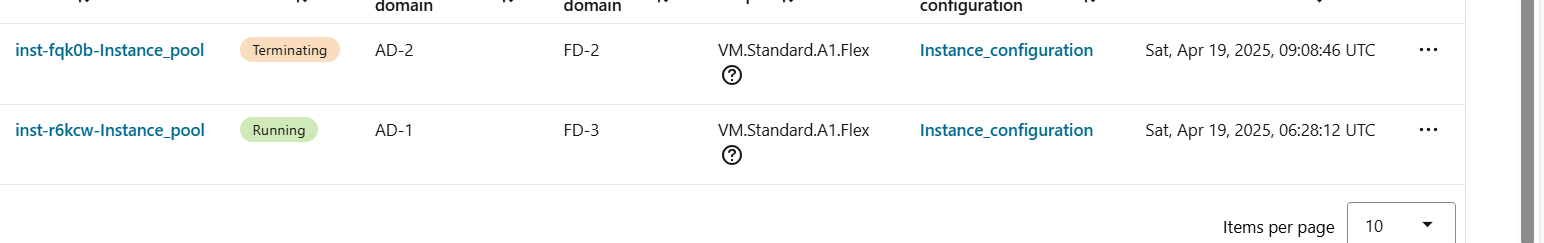


A screenshot of a phone

AI-generated content may be incorrect.

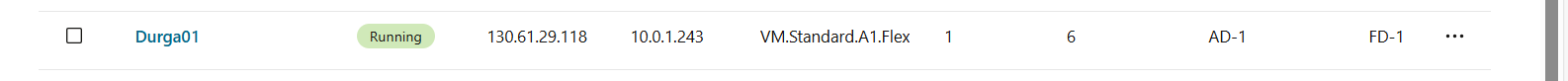
At first there is one instance in the pool now it became two

Now cpu threshold is reduced below 20 , so its automatically terminating an instance in the pool.



**Troubleshooting the issues by using console connection to enter into single user mode if server is refusing the key , if you are unable to login to server due to changes made in sudoers file , if you forgot the root password you can change it.**

Step-01 : Create an instance



Step-2 : GO inside the instance , Goto connections and click on Launch cloud shell connection

A close-up of a mail

AI-generated content may be incorrect.

Step-3 : Reboot the instance and open the cloud shell under the instance.

A screenshot of a computer

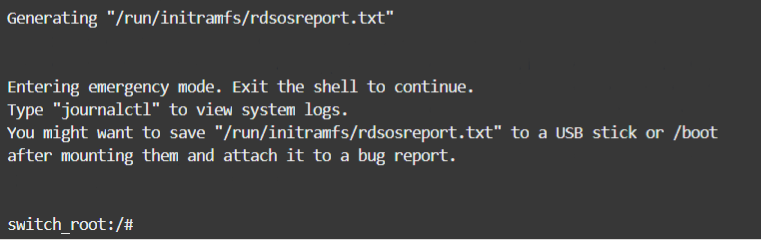
AI-generated content may be incorrect.

Step-4 : While system is booting , interrupt the boot process by clicking ‘Esc’ button and then you get to see grub menu , click ‘e’ button after the selecting the kernel you want to boot , then you get to see the below screenshot , so ‘add the ‘rd.break’ at the end of the line which is starting with ‘linux’ word and press ‘Ctrl + x’ .

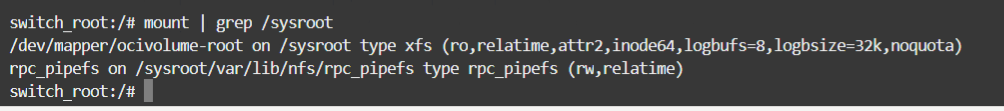
A black screen with white text

AI-generated content may be incorrect.

Step-5 : you will get to see like this , which the system is rebooted into single user mode.

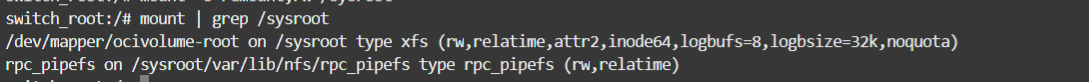


Step-6 : Now find the in which partition root file system is mounted .

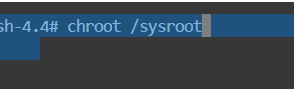


Step-7 : Remount the root file system with read-write mode.





Step-8 : changing root directory to the /sysroot.



Step-9: Now you can change the password for the root if you forgot , or you can troubleshoot any other issues like if you want to modify the sudoers file. Now to change the password for the root.

