I just got some requests from students that their VMs cannot access with “connection denied” error. The problems are mostly because of their VMs being hacked. So, this is a good time for you to practice and make sure your mini cluster safe to block all of the attacks to your VMs from the Internet.

There is a very easy way to secure the VMs just by restricting the access from allowing all the IPs to access the cluster to just allowing the subnet (your three VMs and the client which is often your laptop to access the cluster)

For doing this, there are three steps (all the steps need to be done on all the VMs):

1. Make sure the ssh can access from all the IPs

$ sudo ufw allow 22

2. Make sure the IPs from all the VMs can connect to each other:

$ sudo ufw allow from <VM01_IP>

$ sudo ufw allow from <VM02_IP>

$ sudo ufw allow from <VM03_IP>

If you want to use the webapp of Hadoop to check the status on your own laptop, you need to add the IP of your laptop to the allow list (if the IP address is dynamic, you need to add this every time your IP is changed)

$ sudo ufw allow from <YOUR_LAPTOP_IP>

3. Enable the ubuntu fire wall and check the status:

$ sudo ufw enable

$ sudo ufw status

The output should like:

```
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
Anywhere                   ALLOW       <VM01_IP>
9000                       ALLOW       Anywhere
Anywhere                   ALLOW       <VM02_IP>
Anywhere                   ALLOW       <VM03_IP>
Anywhere                   ALLOW       < YOUR_LAPTOP_IP>
22 (v6)                    ALLOW       Anywhere (v6)
9000 (v6)                  ALLOW       Anywhere (v6)
```