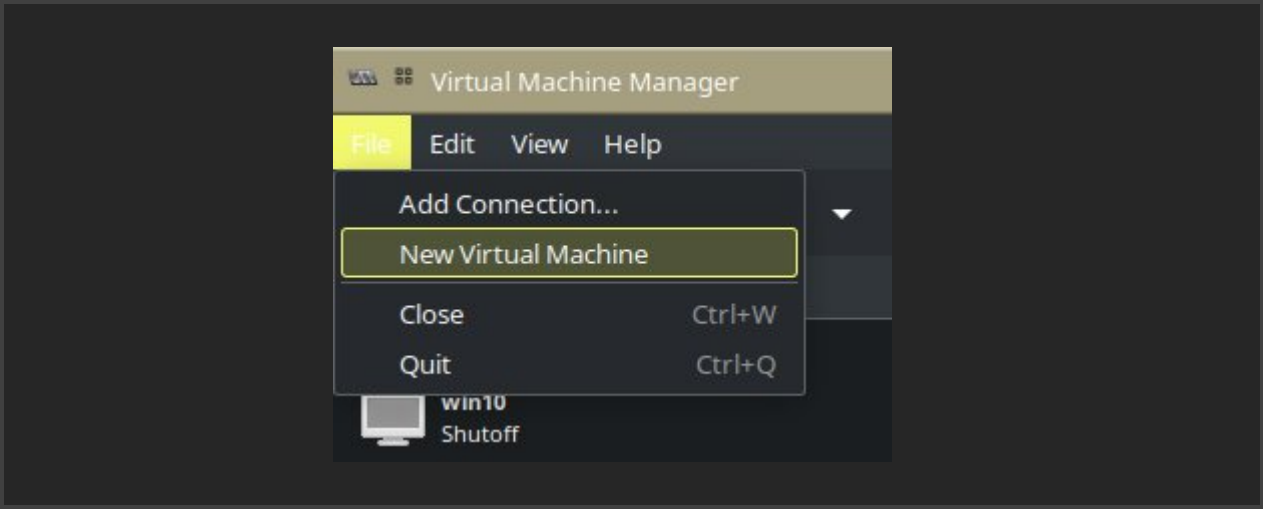
MK Mahwete

Indexer Server Setup

This documentation will take you through a step by step installation of Ubuntu Server for our Index Server to store all our log files for analyzes.

Step 1 : The first thing you will do is to open up QEMU/KVM application and create a new VM and go through all the step for setting up the server.
Here are the configuration settings for the index cluster:

- CPU: 1 core
- RAM: 1024 MB (1 GB)
- Storage: 15 GB (for storing log files)
- Network: NAT or internal network (for private communication)

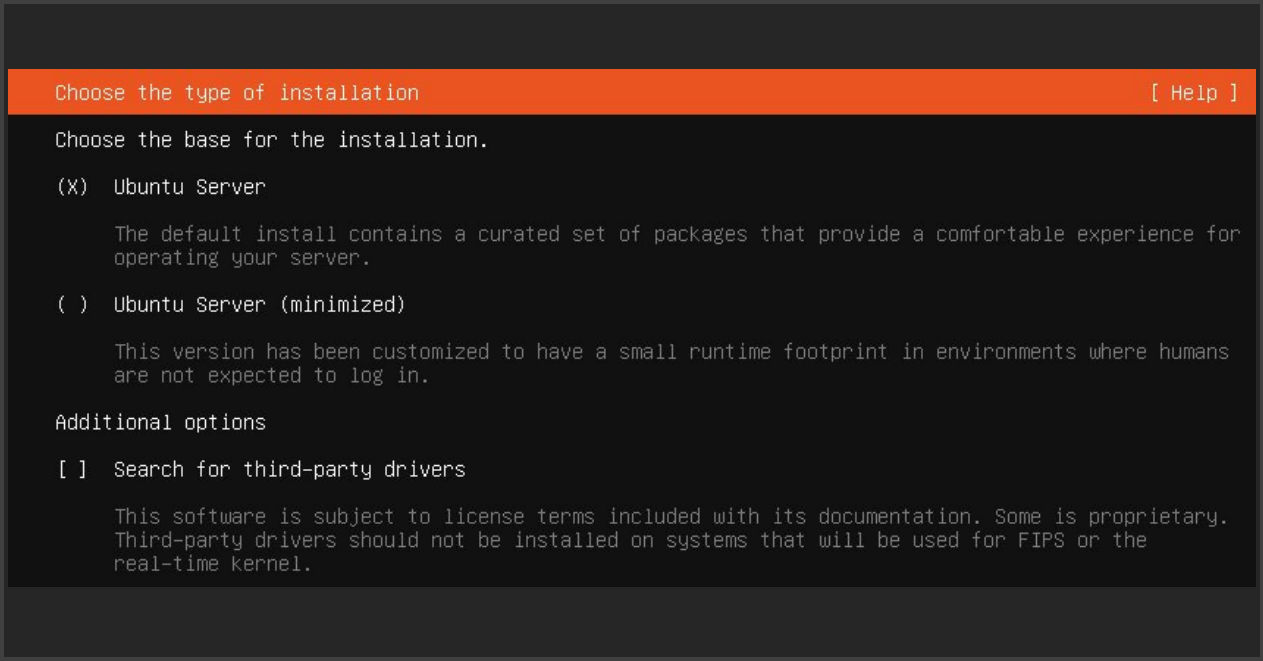


- go through the steps to select the iso image from your downloads file and create the VM with the setting above

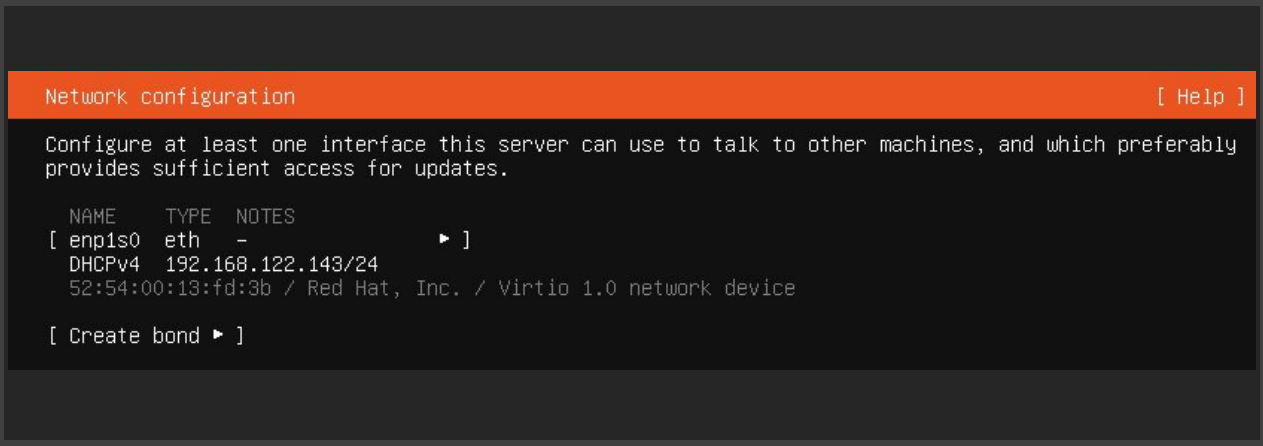
>> $ ——————————————————————————————[08 April 2025]

Step 2: Installing and configuring the server and Network (setting up IP Addresses for communication).
Now, the following steps will take you through installing and configuring the indexer server from selecting the image, networking and all the way to configuring the storage.

NOTE: it's important to pay attention while going through this phase to avoid any incorrect configuration.

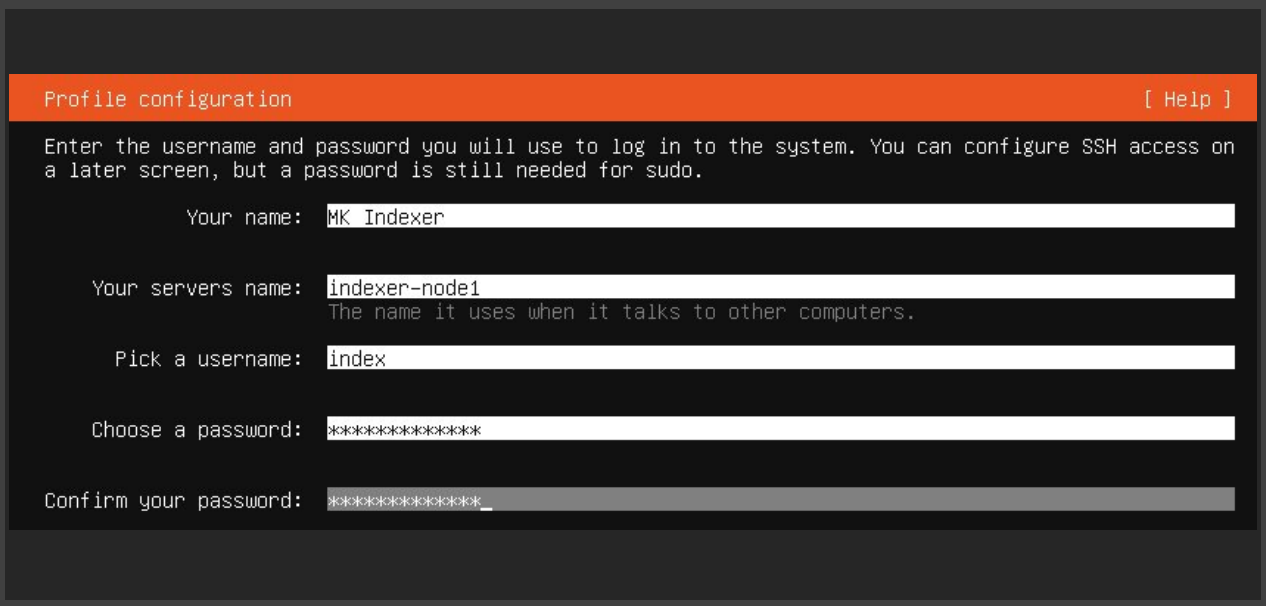


- I recommend choosing an Ubuntu server for a smooth experience



- for now I will leave everything as DHCP (I will create or edit the YAML file in the netplan directory later on for a static IP address)

- now it's time to configure and confirm your storage setup



- now it's time to setup a username and a password for the index node

NOTE: after the installation is complete, reboot our server

>> $ ——————————————————————————————————[08 April 2025]

Step 3: Updating the system and installing openssh server for remote access control.
Before doing a lot of things to the server, the most important and should be your first step is to keep our system up to date and then install openssh for remote access. Run the following command to update our system:

```
sudo apt update && sudo apt upgrade
```

- This should keep our system up to date with the latest packages

Now, the next step is to install Openssh server

```
sudo apt install openssh-server
```

>> $ ——————————————————————————————————[08 April 2025]

Step 4: Customizing the CLI and installing useful tools
To finish the installation, I will ssh into the index server in install zshell and oh-my-zsh for a better CLI look and feel. Before ssh-ing into the server, I need to get it's IP Address by running this command:

```
Ifconfig
```

- If the command output says command not found, install it with this command:

```
sudo apt install net-tools
```

```
index@indexer-node1:~$ ifconfig
enp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.122.143  netmask 255.255.255.0  broadcast 192.168.122.255
        inet6 fe80::5054:ff:fe13:fd3b  prefixlen 64  scopeid 0x20<link>
        ether 52:54:00:13:fd:3b  txqueuelen 1000  (Ethernet)
        RX packets 6274  bytes 7948927 (7.9 MB)
        RX errors 0  dropped 728  overruns 0  frame 0
        TX packets 3187  bytes 224193 (224.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- the IP Address is indicated by (look where is says): inet 192.168.122.143

NOTE: for now this is just a DHCP address and we need a Static address so we gonna set one up

>> $ ——————————————————————————————————————[08 April 2025]

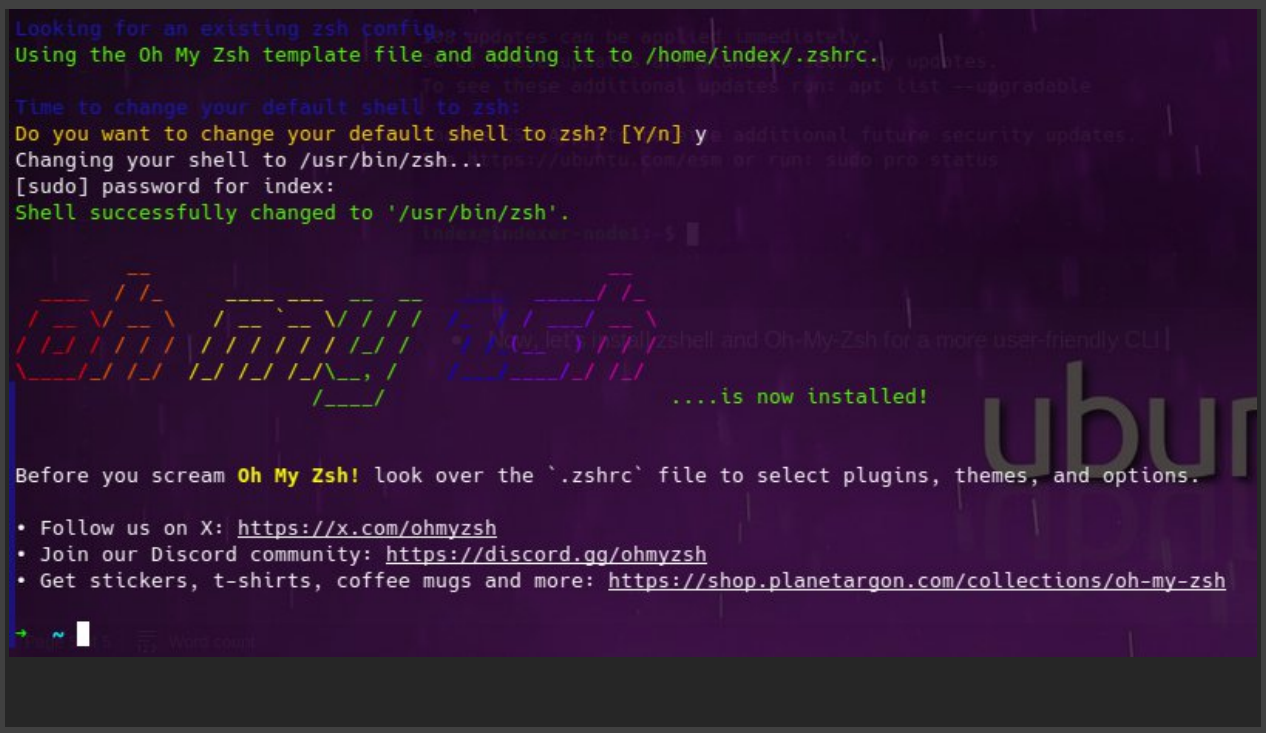
Step 5: ssh-ing into the system and finishing the installation by installing zshell and oh-my-zsh for a more better CLI took and feel.

Now that we found the our IP address. Lets ssh into the machine by using the following command.

ssh index@192.168.122.143

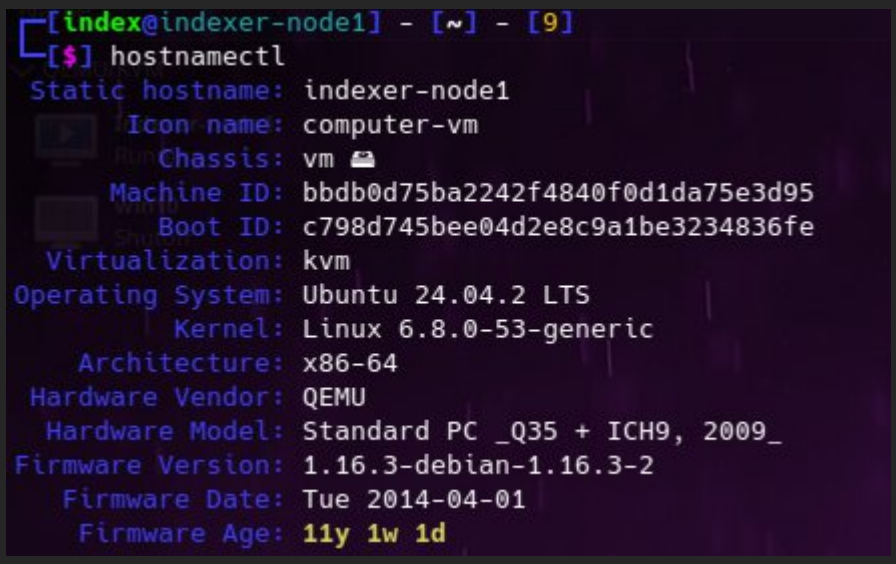
```
[02:10:18] mk-mahwete :: lenovo-s145  →  ~ » ssh index@192.168.122.143
The authenticity of host '192.168.122.143 (192.168.122.143)' can't be established.
ED25519 key fingerprint is SHA256:PIMIGQjuVUhUjS8WwvarTqDxefNtRDFwl60DKhY6DQw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.122.143' (ED25519) to the list of known hosts.
index@192.168.122.143's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-53-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Wed Apr  9 12:10:43 AM UTC 2025

  System load:  0.0               Processes:               139
  Usage of /:   33.2% of 12.94GB  Users logged in:         1
  Memory usage: 22%               IPv4 address for enp1s0: 192.168.122.143
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

108 updates can be applied immediately.
56 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


index@indexer-node1:~$
```

- Now, let’s install zshell and Oh-My-Zsh for a more user-friendly CLI
- To monitor processes we gonna install htop for a better view of our processes



- Our zshell & oh-my-zsh is now complete

The following screenshot provides with specifications for the VM



This is the end of our server setup. I will provide a step by step guide to install the .deb splunk enterprise