Ubuntu Server Installation/ Setup Lab

By Michael Ambeguia

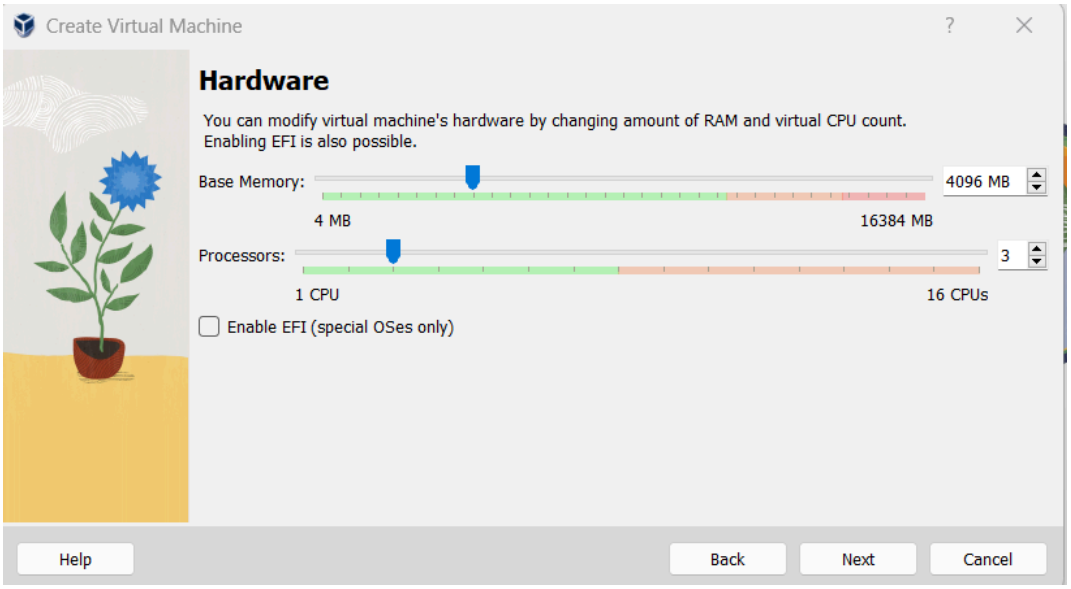
Lab Purpose: The purpose of this lab is to set up an Ubuntu Server VM. I would also like to practice user management, a couple of system hardening techniques, and other key post installation tasks. The lab will be divided into 5 sections. The first section, installation, will be a walkthrough of how I installed the Ubuntu Server VM on VirtualBox. Section #2 will go over how I created some new users on the new VM. Section #3 will demonstrate how I update the system, a crucial post installation step. Section #4 will show how I assigned a static IP address to the VM since servers are recommended to have one for convenience. Lastly, in section #5 I will demonstrate how I implemented some post installation security measures on the VM.

Sections:

Section #1 Installation

Step #1: Create the VM on VirtualBox.

Screenshots:



Create Virtual Machine

Hardware

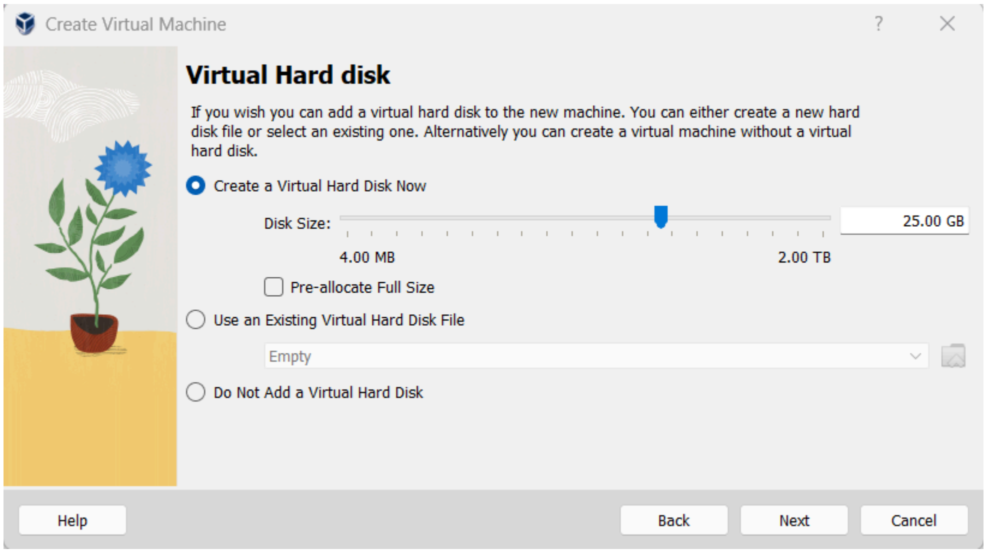
You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Base Memory: 4096 MB (4 MB – 16384 MB)

Processors: 3 (1 CPU – 16 CPUs)

□ Enable EFI (special OSes only)

I will give the VM about 4 gb of memory along with 3 cpu processors.



Create Virtual Machine

Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

● Create a Virtual Hard Disk Now

Disk Size: 25.00 GB (4.00 MB – 2.00 TB)

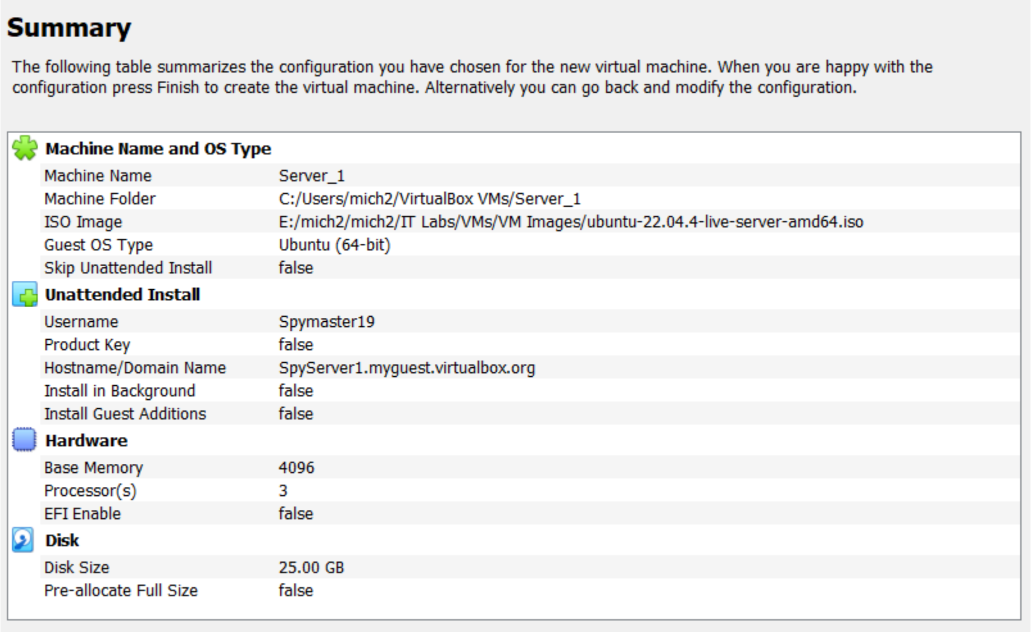
□ Pre-allocate Full Size

○ Use an Existing Virtual Hard Disk File

Empty

○ Do Not Add a Virtual Hard Disk

I also created a virtual hard disk with 25 GB of storage that is dynamically allocated.



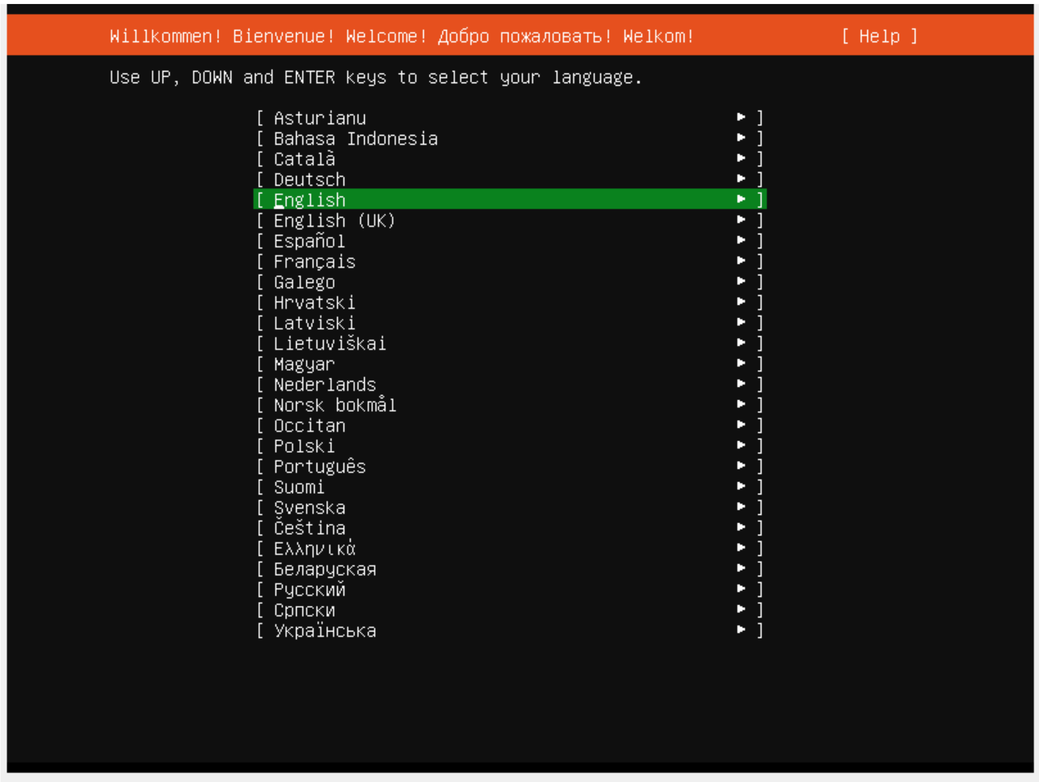
Summary

The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.

Machine Name and OS Type	
Machine Name	Server_1
Machine Folder	C:/Users/mich2/VirtualBox VMs/Server_1
ISO Image	E:/mich2/mich2/IT Labs/VMs/VM Images/ubuntu-22.04.4-live-server-amd64.iso
Guest OS Type	Ubuntu (64-bit)
Skip Unattended Install	false
Unattended Install	
Username	Spymaster19
Product Key	false
Hostname/Domain Name	SpyServer1.myguest.virtualbox.org
Install in Background	false
Install Guest Additions	false
Hardware	
Base Memory	4096
Processor(s)	3
EFI Enable	false
Disk	
Disk Size	25.00 GB
Pre-allocate Full Size	false

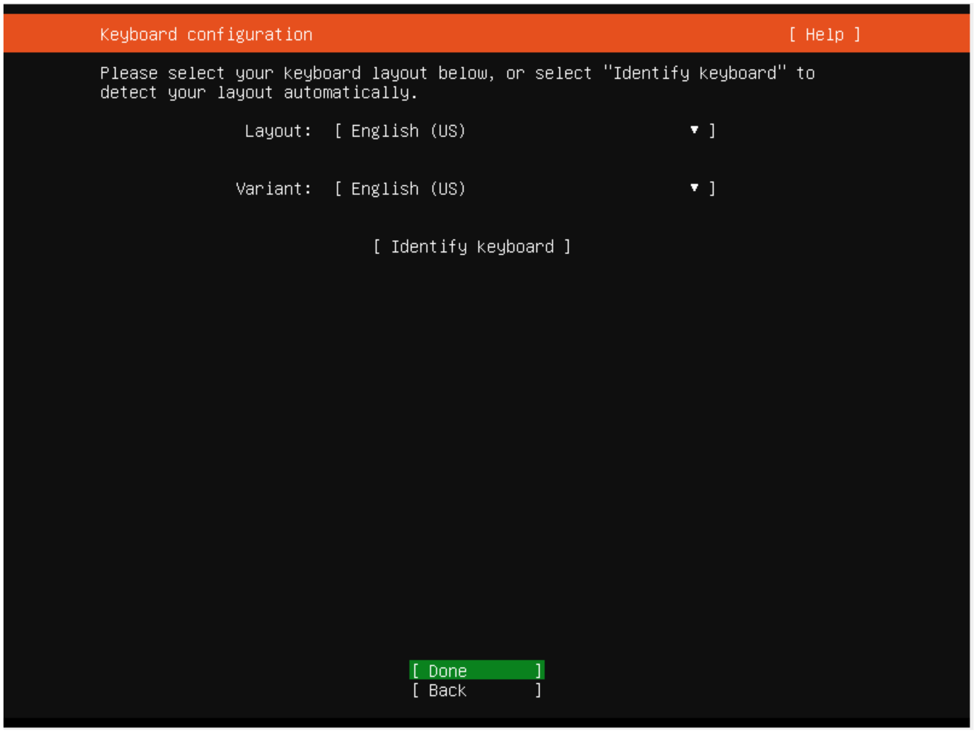
Summary of the VM that I am creating.

Now it's time to install the server once you get to this screen!



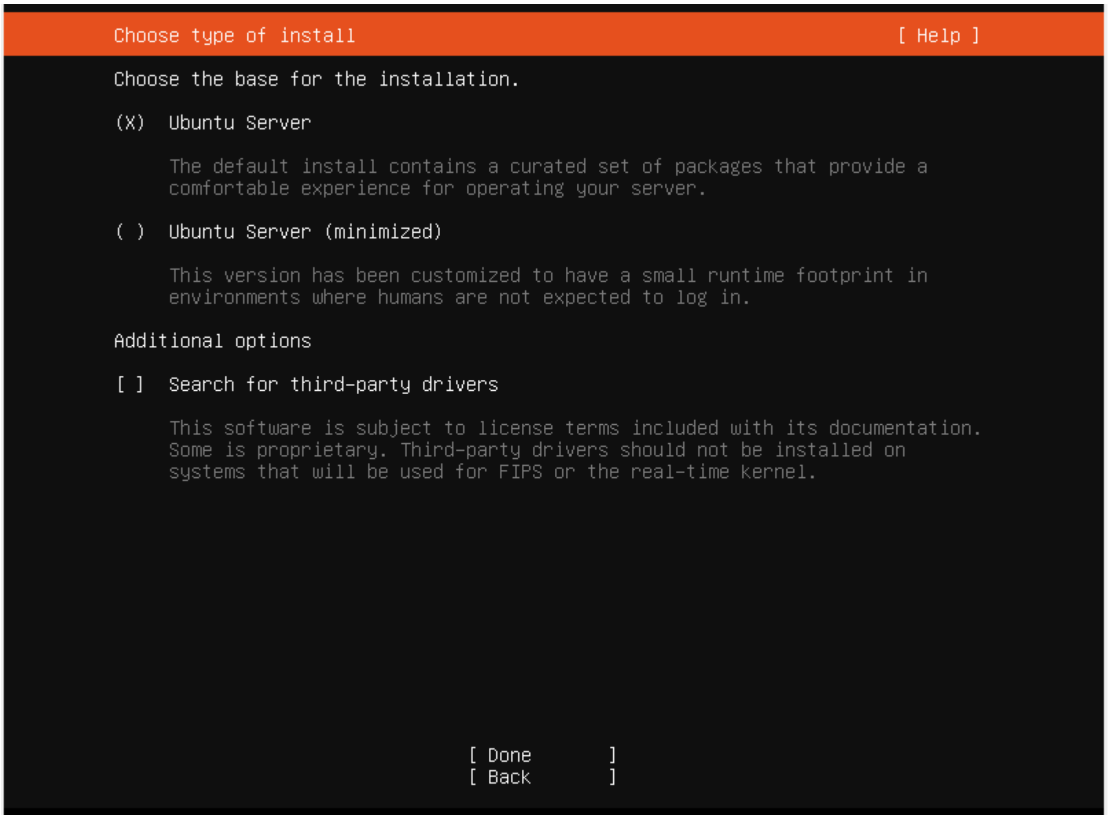
```
          Willkommen! Bienvenue! Welcome! Добро пожаловать! Welkom!              [ Help ]

          Use UP, DOWN and ENTER keys to select your language.

                         [ Asturianu                                ▸ ]
                         [ Bahasa Indonesia                         ▸ ]
                         [ Català                                   ▸ ]
                         [ Deutsch                                  ▸ ]
                         [ English                                  ▸ ]
                         [ English (UK)                             ▸ ]
                         [ Español                                  ▸ ]
                         [ Français                                 ▸ ]
                         [ Galego                                   ▸ ]
                         [ Hrvatski                                 ▸ ]
                         [ Latviski                                 ▸ ]
                         [ Lietuviškai                              ▸ ]
                         [ Magyar                                   ▸ ]
                         [ Nederlands                               ▸ ]
                         [ Norsk bokmål                             ▸ ]
                         [ Occitan                                  ▸ ]
                         [ Polski                                   ▸ ]
                         [ Português                                ▸ ]
                         [ Suomi                                    ▸ ]
                         [ Svenska                                  ▸ ]
                         [ Čeština                                  ▸ ]
                         [ Ελληνικά                                 ▸ ]
                         [ Беларуская                               ▸ ]
                         [ Русский                                  ▸ ]
                         [ Српски                                   ▸ ]
                         [ Українська                               ▸ ]
```

Choose the appropriate language. In this case, English.



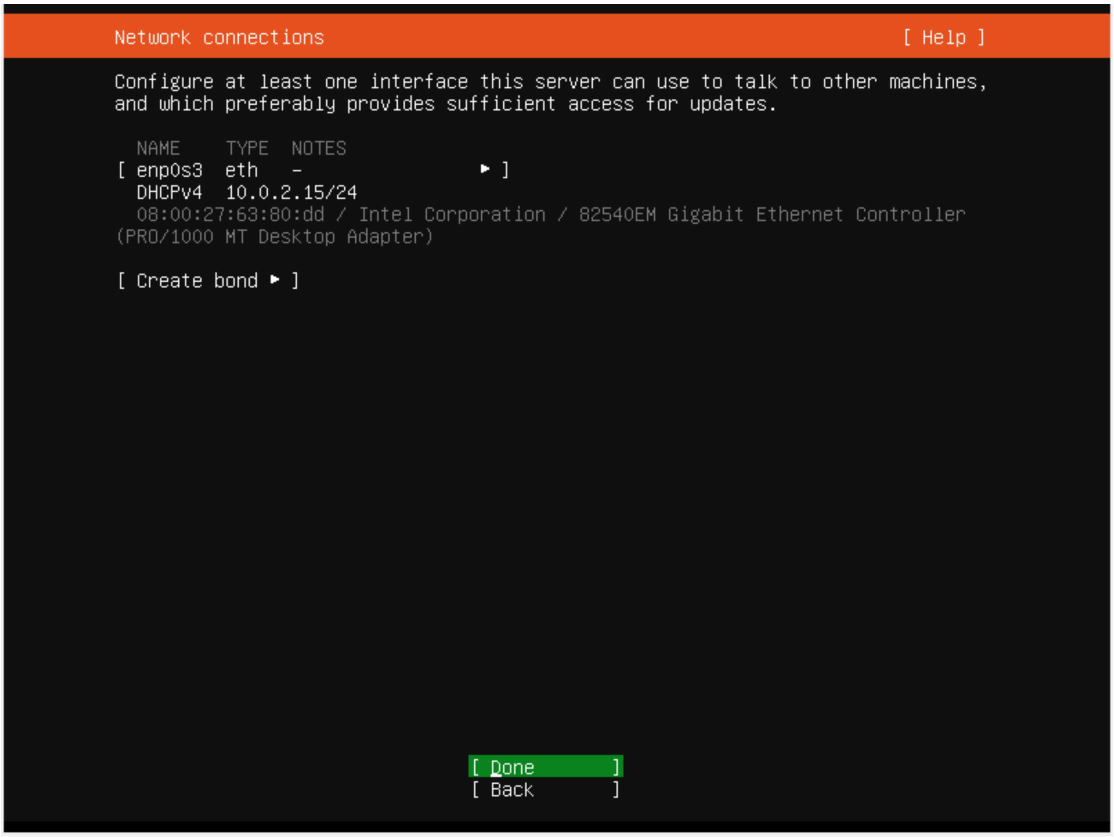
```
Keyboard configuration                                        [ Help ]

Please select your keyboard layout below, or select "Identify keyboard" to
detect your layout automatically.

          Layout:  [ English (US)                      ▼ ]

         Variant:  [ English (US)                      ▼ ]

                        [ Identify keyboard ]




                              [ Done      ]
                              [ Back      ]
```

Now choose the keyboard layout. Once you do, press enter on “Done”.



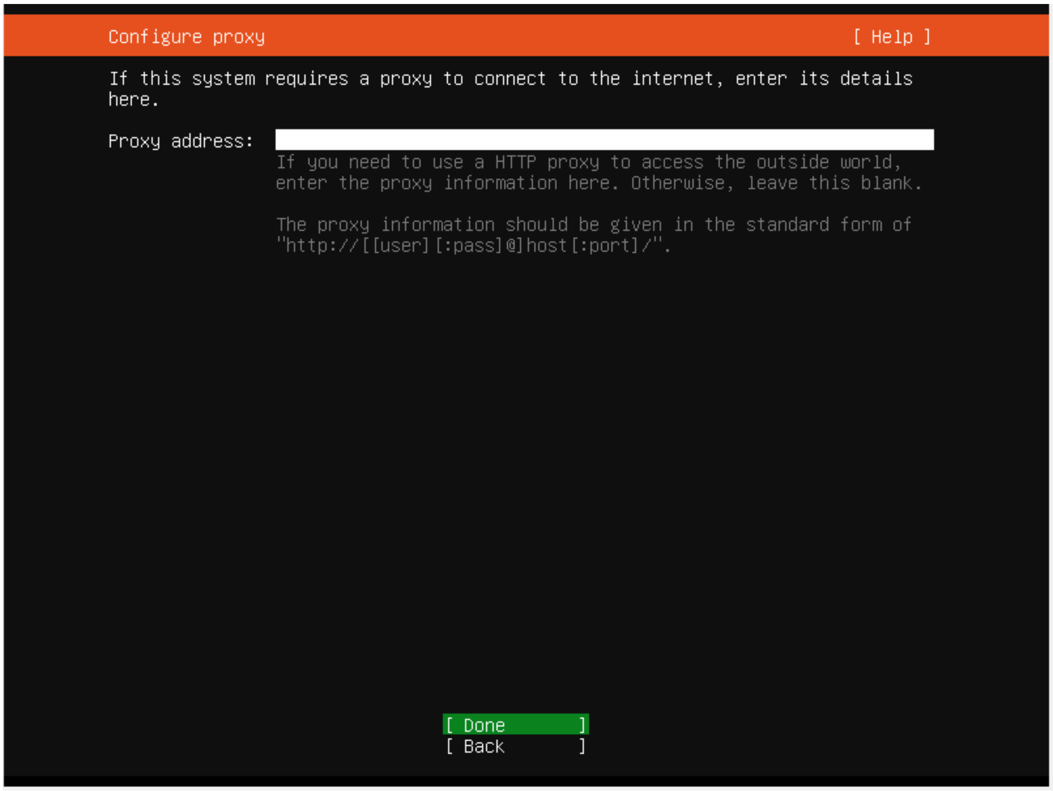
```
Choose type of install                                         [ Help ]

Choose the base for the installation.

(X)  Ubuntu Server

     The default install contains a curated set of packages that provide a
     comfortable experience for operating your server.

( )  Ubuntu Server (minimized)

     This version has been customized to have a small runtime footprint in
     environments where humans are not expected to log in.

Additional options

[ ]  Search for third-party drivers

     This software is subject to license terms included with its documentation.
     Some is proprietary. Third-party drivers should not be installed on
     systems that will be used for FIPS or the real-time kernel.




                           [ Done      ]
                           [ Back      ]
```

Now choose the type of install. I will choose Ubuntu Server.



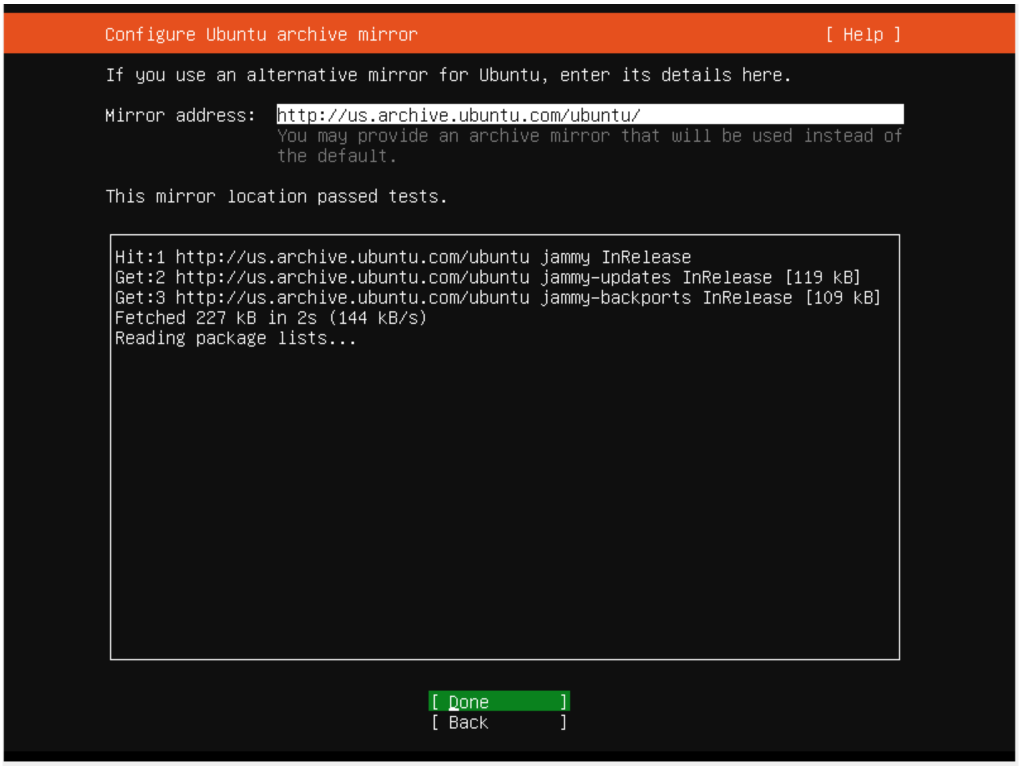
```
Network connections                                                    [ Help ]

Configure at least one interface this server can use to talk to other machines,
and which preferably provides sufficient access for updates.

  NAME     TYPE  NOTES
[ enp0s3   eth   -                ▶ ]
  DHCPv4   10.0.2.15/24
  08:00:27:63:80:dd / Intel Corporation / 82540EM Gigabit Ethernet Controller
(PRO/1000 MT Desktop Adapter)

[ Create bond ▶ ]
```

Now configure an internet interface, just choose whatever appears since that means that it has been found by the installation media for the server.



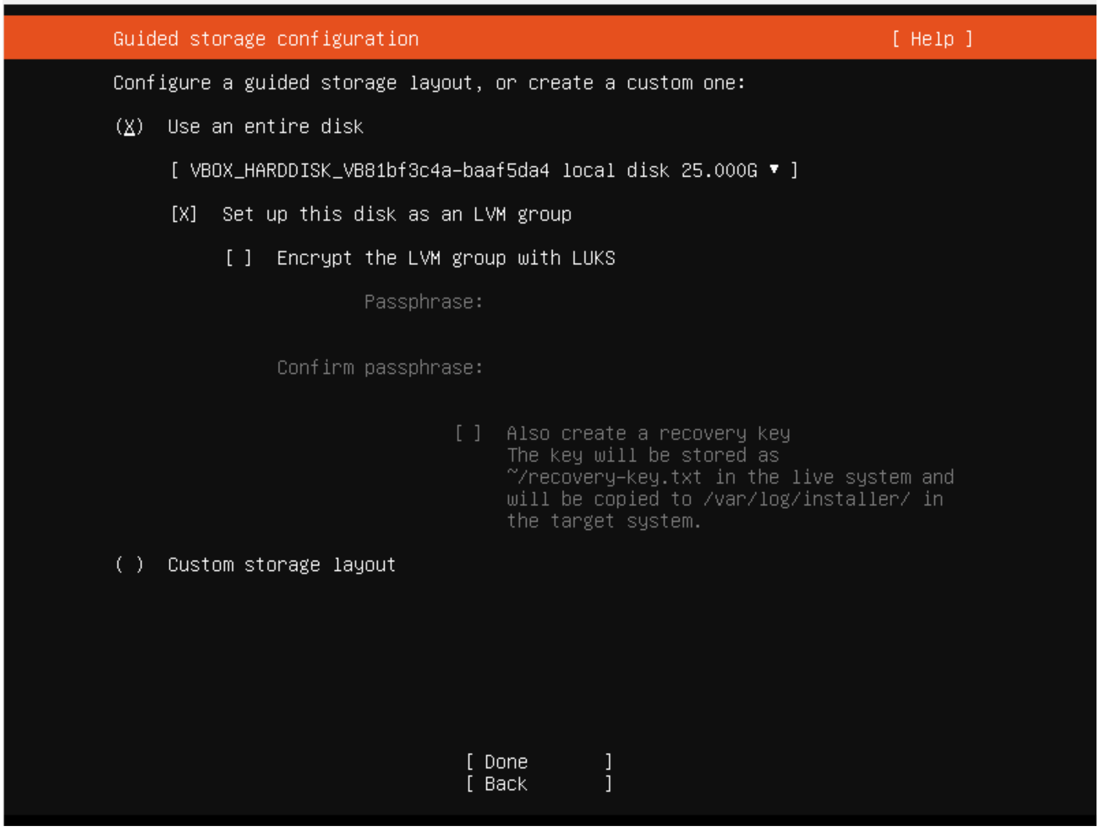
```
Configure proxy                                              [ Help ]

If this system requires a proxy to connect to the internet, enter its details
here.

Proxy address:
                If you need to use a HTTP proxy to access the outside world,
                enter the proxy information here. Otherwise, leave this blank.

                The proxy information should be given in the standard form of
                "http://[[user][:pass]@]host[:port]/".
```

The installation asks you if you need a proxy server. I don’t, so I can skip this step.



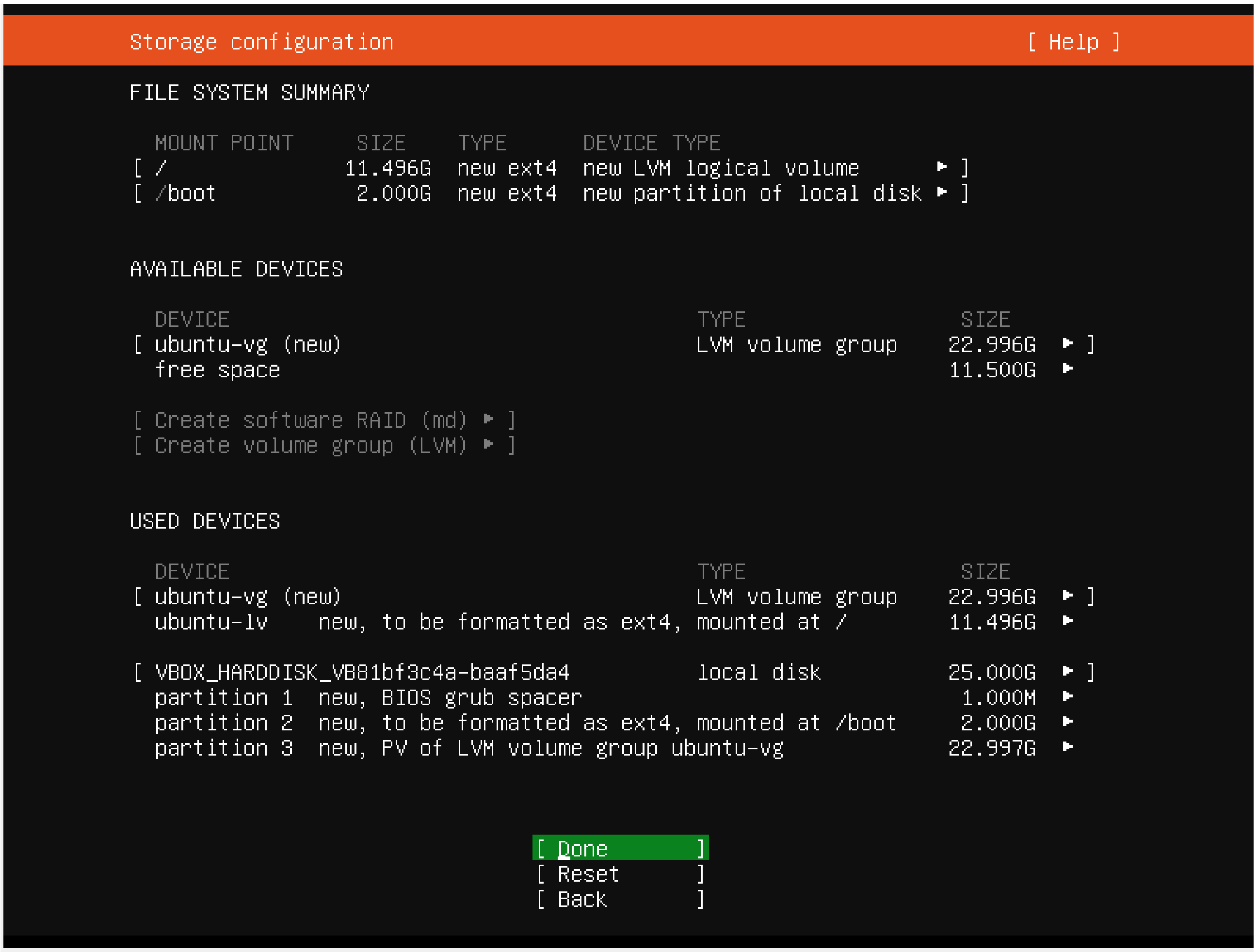
```
Configure Ubuntu archive mirror                                [ Help ]

If you use an alternative mirror for Ubuntu, enter its details here.

Mirror address: http://us.archive.ubuntu.com/ubuntu/
                You may provide an archive mirror that will be used instead of
                the default.

This mirror location passed tests.

Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease [109 kB]
Fetched 227 kB in 2s (144 kB/s)
Reading package lists...
```

Now choose the Ubuntu archive mirror/ Use the default.



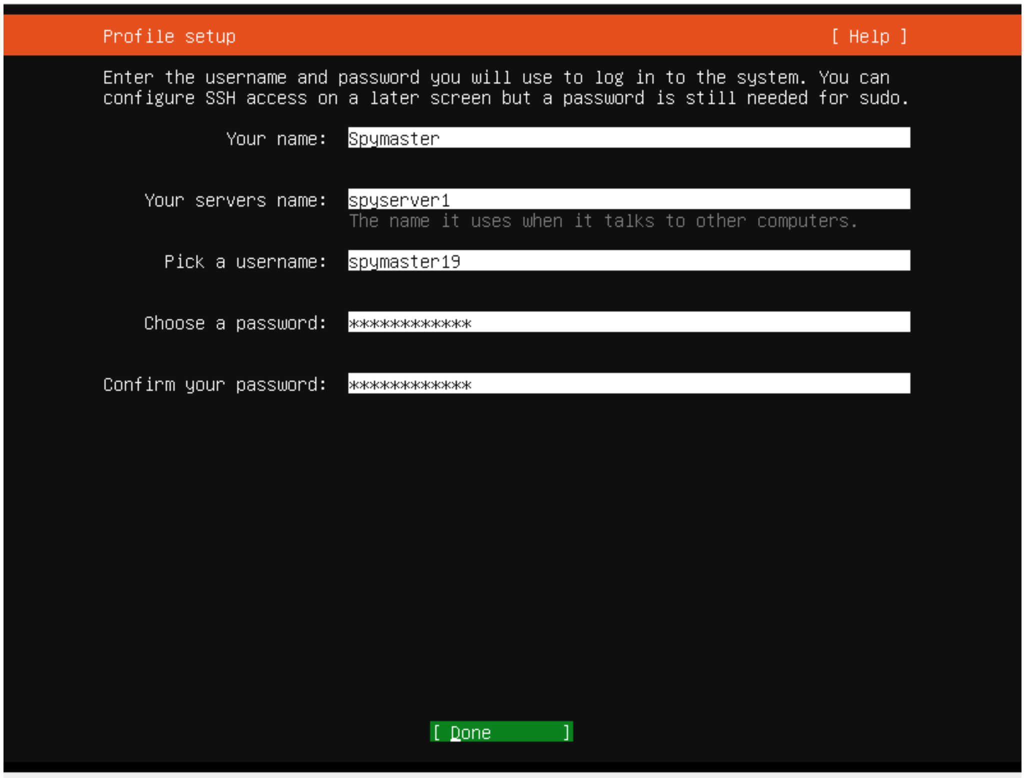
```
Guided storage configuration                                          [ Help ]

Configure a guided storage layout, or create a custom one:

(X)  Use an entire disk

     [ VBOX_HARDDISK_VB81bf3c4a-baaf5da4 local disk 25.000G ▾ ]

     [X]  Set up this disk as an LVM group

          [ ]  Encrypt the LVM group with LUKS

                         Passphrase:


                 Confirm passphrase:


                                 [ ]  Also create a recovery key
                                      The key will be stored as
                                      ~/recovery-key.txt in the live system and
                                      will be copied to /var/log/installer/ in
                                      the target system.

( )  Custom storage layout




                                  [ Done       ]
                                  [ Back       ]
```

Next up is the storage configuration. I will stick with the options given since I am okay with using my virtual disk and setting up the storage as an lvm group.



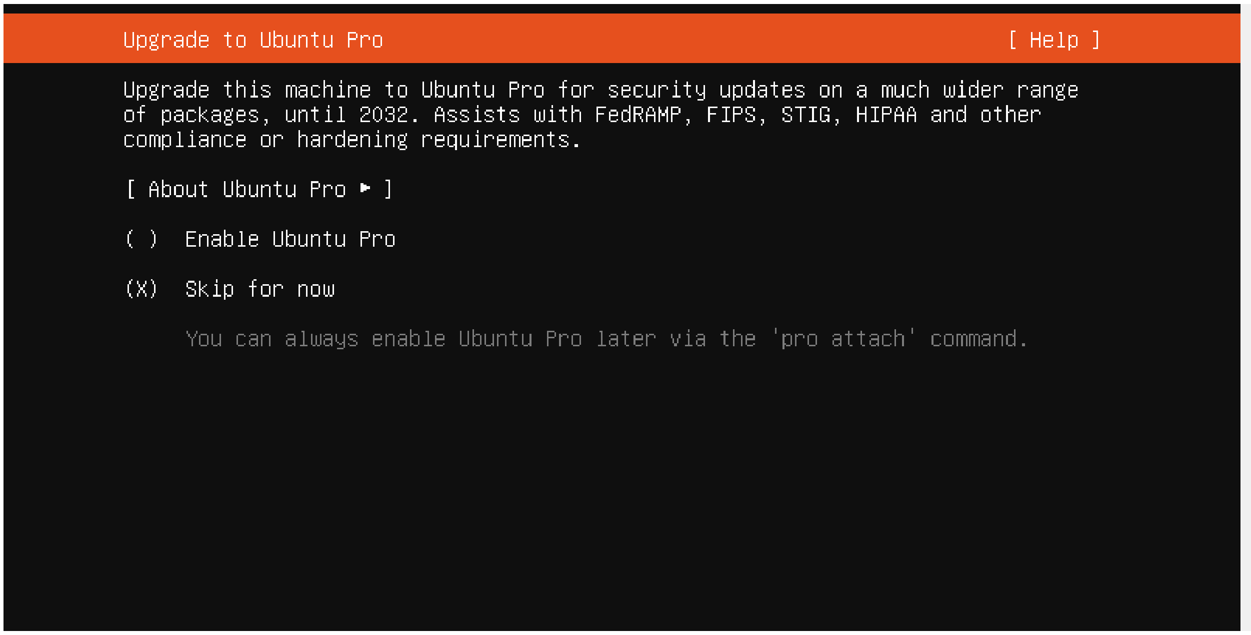
```
Storage configuration                                                [ Help ]

FILE SYSTEM SUMMARY

  MOUNT POINT     SIZE    TYPE      DEVICE TYPE
[ /             11.496G  new ext4  new LVM logical volume      ► ]
[ /boot          2.000G  new ext4  new partition of local disk ► ]


AVAILABLE DEVICES

  DEVICE                                   TYPE                SIZE
[ ubuntu-vg (new)                          LVM volume group    22.996G  ► ]
  free space                                                   11.500G  ►

[ Create software RAID (md) ► ]
[ Create volume group (LVM) ► ]


USED DEVICES

  DEVICE                                   TYPE                SIZE
[ ubuntu-vg (new)                          LVM volume group    22.996G  ► ]
  ubuntu-lv    new, to be formatted as ext4, mounted at /      11.496G  ►

[ VBOX_HARDDISK_VB81bf3c4a-baaf5da4        local disk          25.000G  ► ]
  partition 1  new, BIOS grub spacer                            1.000M  ►
  partition 2  new, to be formatted as ext4, mounted at /boot   2.000G  ►
  partition 3  new, PV of LVM volume group ubuntu-vg           22.997G  ►



                                [ Done         ]
                                [ Reset        ]
                                [ Back         ]
```

Here is a nice overview provided by the installation media to confirm the storage configuration. So I have an LV mounted on / (the root directory) and a regular disk partition mounted on /boot (where the kernel and files needed to boot the system are stored). My current LVM setup allocated 11.496G to / and I still have about 11.5 GB of free space that can be added to / if need be. The great thing about LVM is that all the storage does not have to be allocated right away and I can simply add more storage when needed if the / directory runs out of storage.



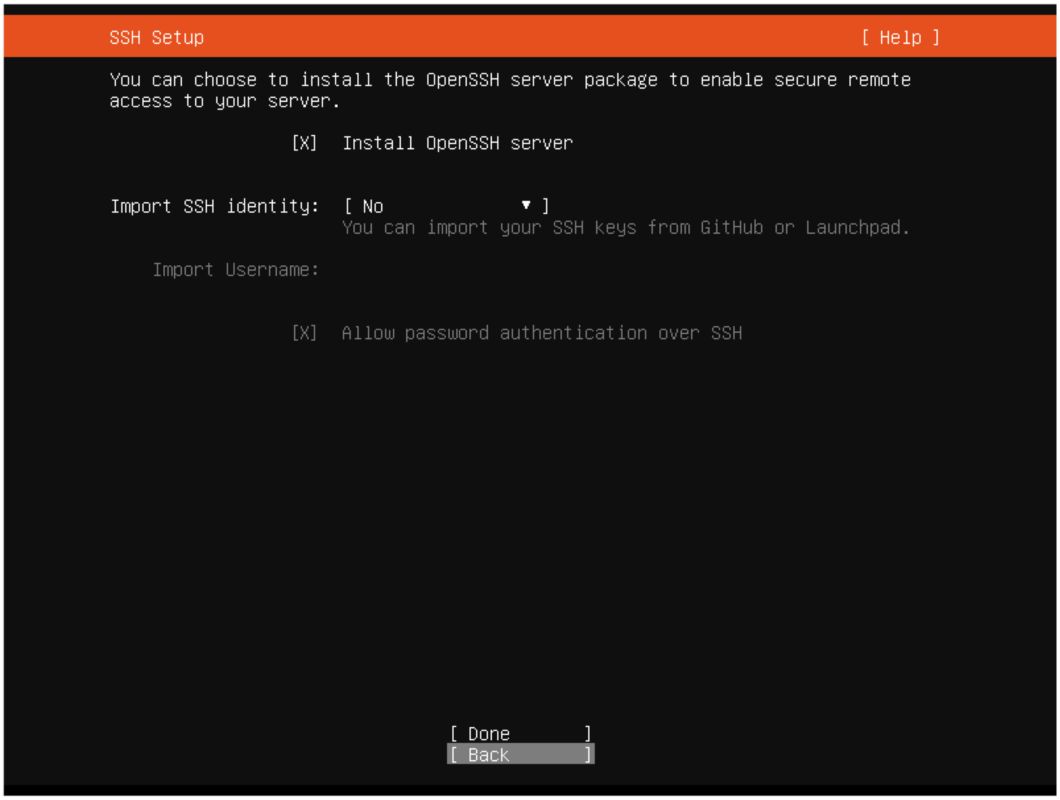
```
Profile setup                                                      [ Help ]

Enter the username and password you will use to log in to the system. You can
configure SSH access on a later screen but a password is still needed for sudo.

            Your name: Spymaster

     Your servers name: spyserver1
                        The name it uses when it talks to other computers.

      Pick a username: spymaster19

    Choose a password: *************

Confirm your password: *************

                              [ Done       ]
```

Next, set up the profile. This includes setting up the root user and their password. Make sure you create a strong password!



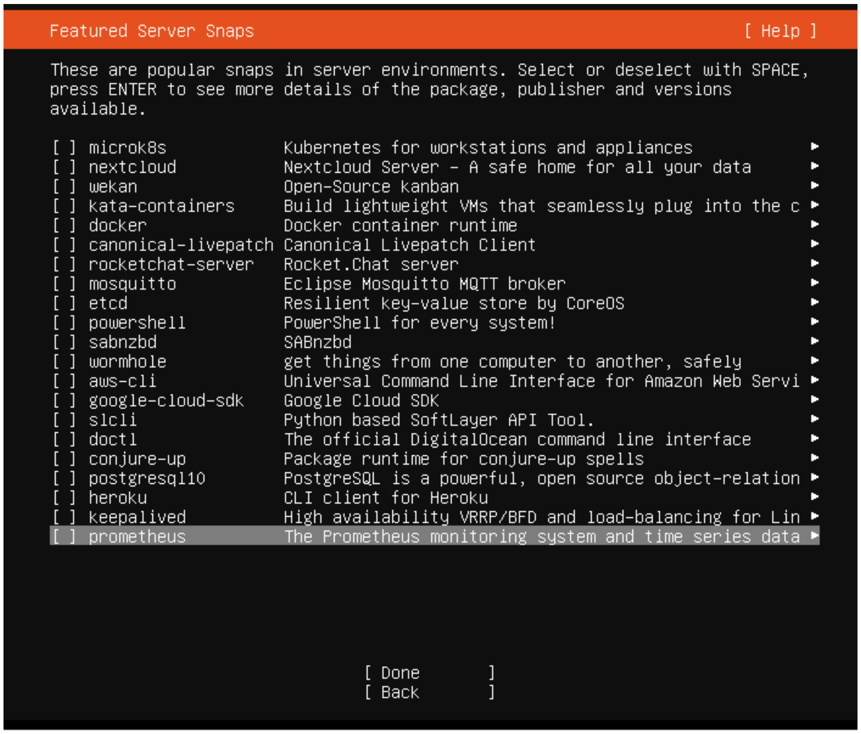
```
Upgrade to Ubuntu Pro                                          [ Help ]

Upgrade this machine to Ubuntu Pro for security updates on a much wider range
of packages, until 2032. Assists with FedRAMP, FIPS, STIG, HIPAA and other
compliance or hardening requirements.

[ About Ubuntu Pro ▶ ]

( )  Enable Ubuntu Pro

(X)  Skip for now

     You can always enable Ubuntu Pro later via the 'pro attach' command.
```

Now it asks you if you want Ubuntu Pro. You can always just enable it post-installation.



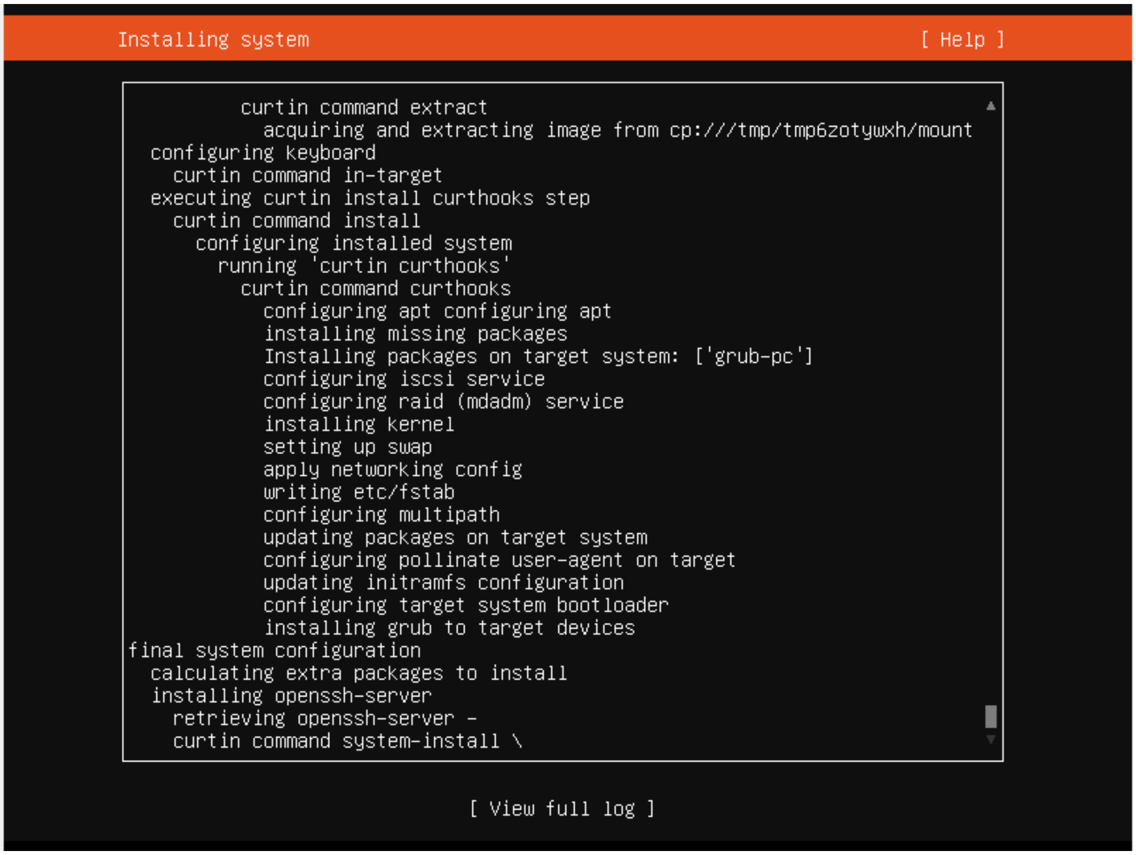
```
SSH Setup                                                       [ Help ]

You can choose to install the OpenSSH server package to enable secure remote
access to your server.

                  [X]  Install OpenSSH server

Import SSH identity:   [ No              ▼ ]
                       You can import your SSH keys from GitHub or Launchpad.

    Import Username:

                  [X]  Allow password authentication over SSH




                               [ Done       ]
                               [ Back       ]
```

The installation process will then ask you if you want to install OpenSSH Server, and yes you do since that is how you will remotely access the server.



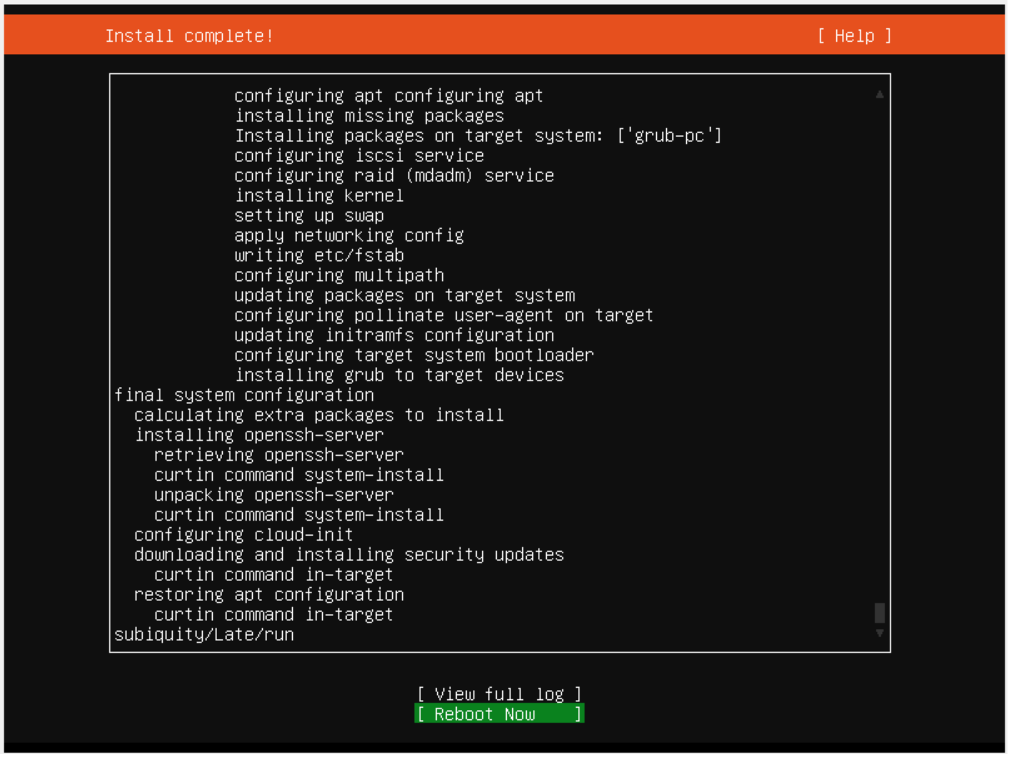
```
Featured Server Snaps                                             [ Help ]

These are popular snaps in server environments. Select or deselect with SPACE,
press ENTER to see more details of the package, publisher and versions
available.

[ ] microk8s            Kubernetes for workstations and appliances          ▶
[ ] nextcloud           Nextcloud Server - A safe home for all your data    ▶
[ ] wekan               Open-Source kanban                                  ▶
[ ] kata-containers     Build lightweight VMs that seamlessly plug into the c ▶
[ ] docker              Docker container runtime                            ▶
[ ] canonical-livepatch Canonical Livepatch Client                          ▶
[ ] rocketchat-server   Rocket.Chat server                                  ▶
[ ] mosquitto           Eclipse Mosquitto MQTT broker                       ▶
[ ] etcd                Resilient key-value store by CoreOS                 ▶
[ ] powershell          PowerShell for every system!                        ▶
[ ] sabnzbd             SABnzbd                                             ▶
[ ] wormhole            get things from one computer to another, safely     ▶
[ ] aws-cli             Universal Command Line Interface for Amazon Web Servi ▶
[ ] google-cloud-sdk    Google Cloud SDK                                    ▶
[ ] slcli               Python based SoftLayer API Tool.                    ▶
[ ] doctl               The official DigitalOcean command line interface    ▶
[ ] conjure-up          Package runtime for conjure-up spells               ▶
[ ] postgresql10        PostgreSQL is a powerful, open source object-relation ▶
[ ] heroku              CLI client for Heroku                               ▶
[ ] keepalived          High availability VRRP/BFD and load-balancing for Lin ▶
[ ] prometheus          The Prometheus monitoring system and time series data ▶



                          [ Done       ]
                          [ Back       ]
```

Other services you can install. I choose none.



```
     curtin command extract
      acquiring and extracting image from cp:///tmp/tmp6zotywxh/mount
 configuring keyboard
  curtin command in-target
 executing curtin install curthooks step
  curtin command install
   configuring installed system
    running 'curtin curthooks'
     curtin command curthooks
      configuring apt configuring apt
      installing missing packages
      Installing packages on target system: ['grub-pc']
      configuring iscsi service
      configuring raid (mdadm) service
      installing kernel
      setting up swap
      apply networking config
      writing etc/fstab
      configuring multipath
      updating packages on target system
      configuring pollinate user-agent on target
      updating initramfs configuration
      configuring target system bootloader
      installing grub to target devices
final system configuration
 calculating extra packages to install
 installing openssh-server
  retrieving openssh-server -
  curtin command system-install \
```

Now installation has begun!!



```
      configuring apt configuring apt
      installing missing packages
      Installing packages on target system: ['grub-pc']
      configuring iscsi service
      configuring raid (mdadm) service
      installing kernel
      setting up swap
      apply networking config
      writing etc/fstab
      configuring multipath
      updating packages on target system
      configuring pollinate user-agent on target
      updating initramfs configuration
      configuring target system bootloader
      installing grub to target devices
final system configuration
 calculating extra packages to install
 installing openssh-server
  retrieving openssh-server
  curtin command system-install
  unpacking openssh-server
  curtin command system-install
 configuring cloud-init
 downloading and installing security updates
  curtin command in-target
 restoring apt configuration
  curtin command in-target
subiquity/Late/run
```

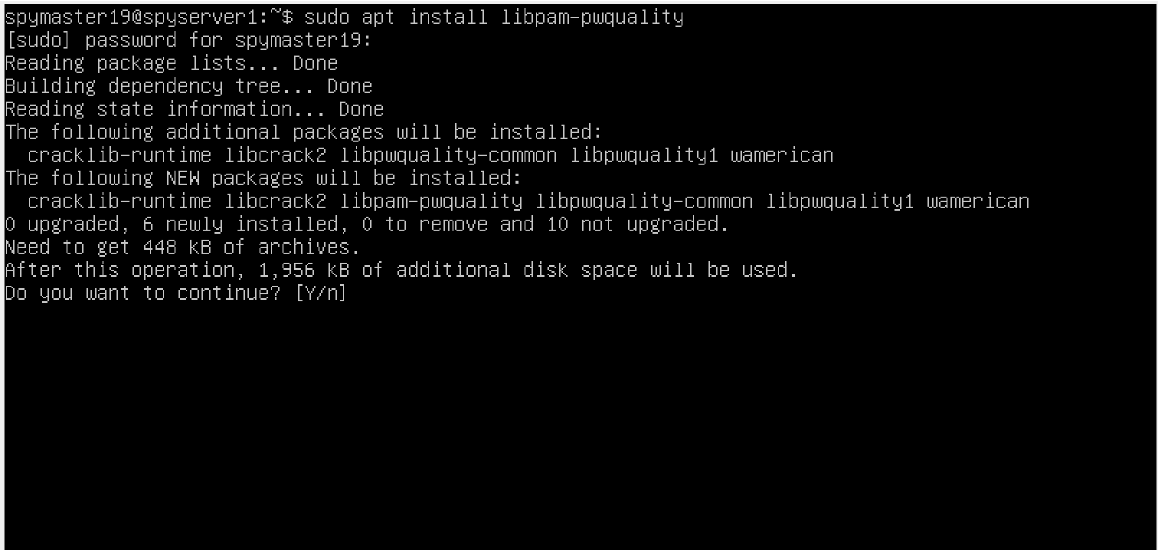
Installation is now complete! You need to reboot the system.

Section #2 User Creation

For security reasons, using the root account should be rare. The root account can do anything it wants on the Linux system. Instead, users with sudo privileges should be created. Sudo users have the ability to perform admin tasks, but they do not have full access to the system. Also, non sudo and root users should be created for daily tasks and non admin purposes.

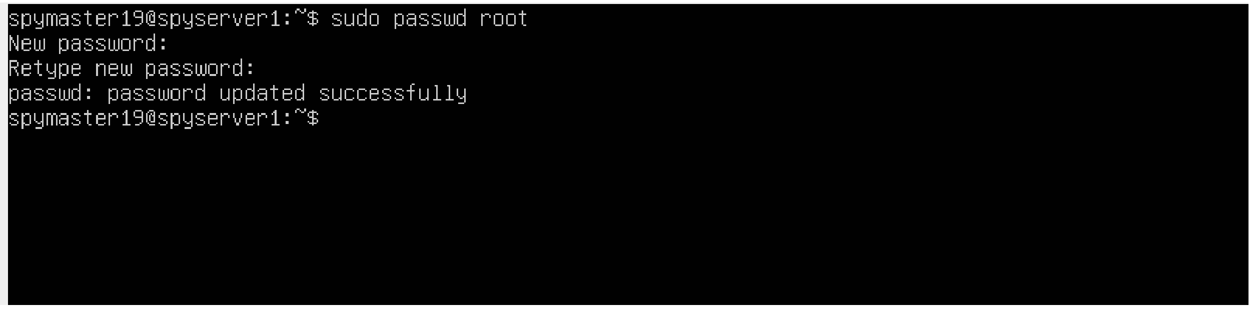
Here is how the users will be created:

1. Install libpam-pwquality to enforce strong passwords on the server. It is vital that this is installed prior to creating users since you want to ensure that all users follow your password guidelines. The only way to guarantee that the guidelines are followed is to set them before users are created.



```
spymaster19@spyserver1:~$ sudo apt install libpam-pwquality
[sudo] password for spymaster19:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  cracklib-runtime libcrack2 libpwquality-common libpwquality1 wamerican
The following NEW packages will be installed:
  cracklib-runtime libcrack2 libpam-pwquality libpwquality-common libpwquality1 wamerican
0 upgraded, 6 newly installed, 0 to remove and 10 not upgraded.
Need to get 448 kB of archives.
After this operation, 1,956 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

2. Since this is a new server, you need to create the password for the root user using sudo passwd root. Once you have a root password set, you can move onto the next step.

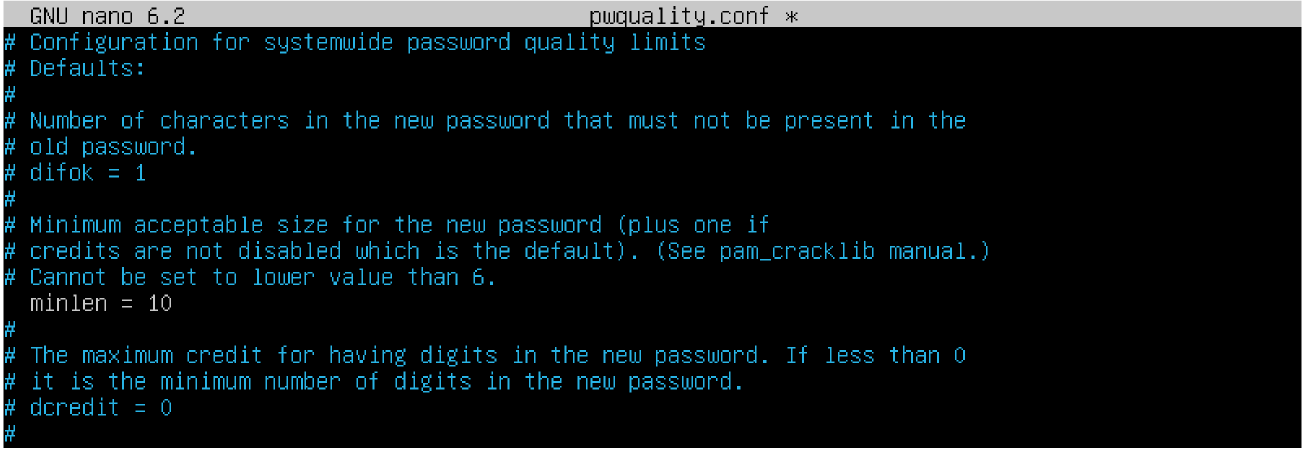


```
spymaster19@spyserver1:~$ sudo passwd root
New password:
Retype new password:
passwd: password updated successfully
spymaster19@spyserver1:~$
```

3. Now as root, update the /etc/security/pwquality.conf file. Root owns this file and that is why you need root permissions to edit it.
   - I will set the following password quality settings:

1. Minlen = 10 (so passwords must be 10 characters or longer)
2. Minclass = 4 (so upper, lowercase, numbers, and special required)
3. Dictcheck =1 (Compare passwords to ones found in password dictionary)
4. Usercheck =1 (Make sure that username is not used in password)
5. Retry = 5 (Five retries allowed for password authentication)
6. Enforce_for_root (When root password is changed, the settings apply)

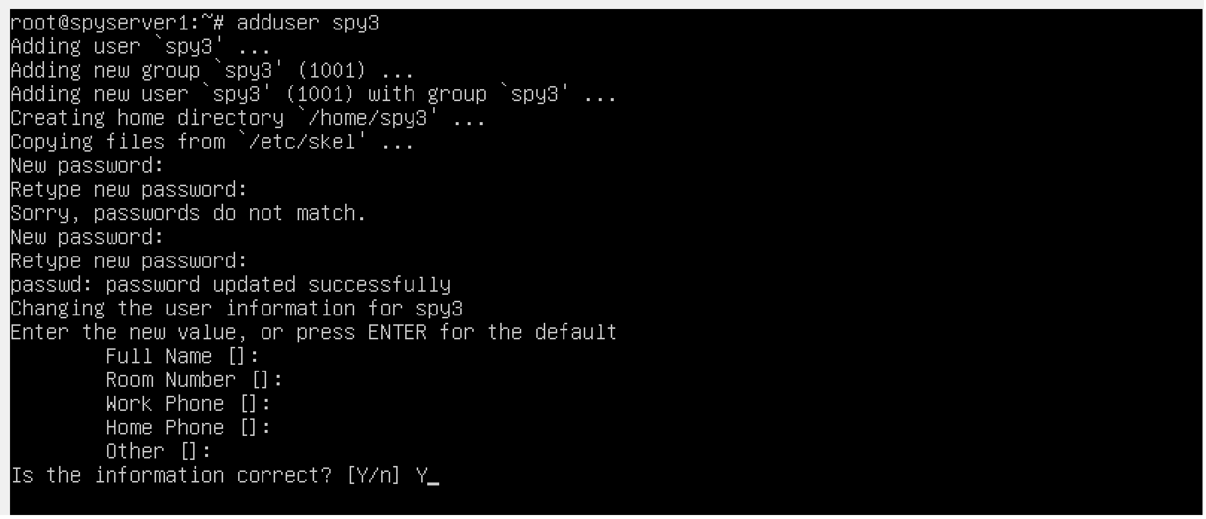
Note that in order to enable the settings you need to get rid of the # (comment)!



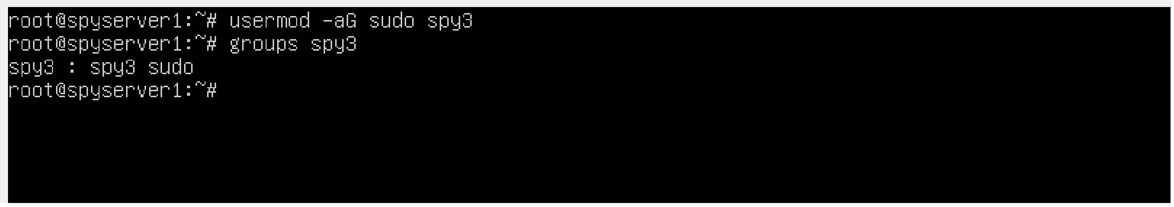
```
  GNU nano 6.2                                    pwquality.conf *
# Configuration for systemwide password quality limits
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 1
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
  minlen = 10
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
# dcredit = 0
#
```

4. Now we can create users. I created spy3 (sudo) and spyuser1 (non sudo user) using adduser.

Spy3:

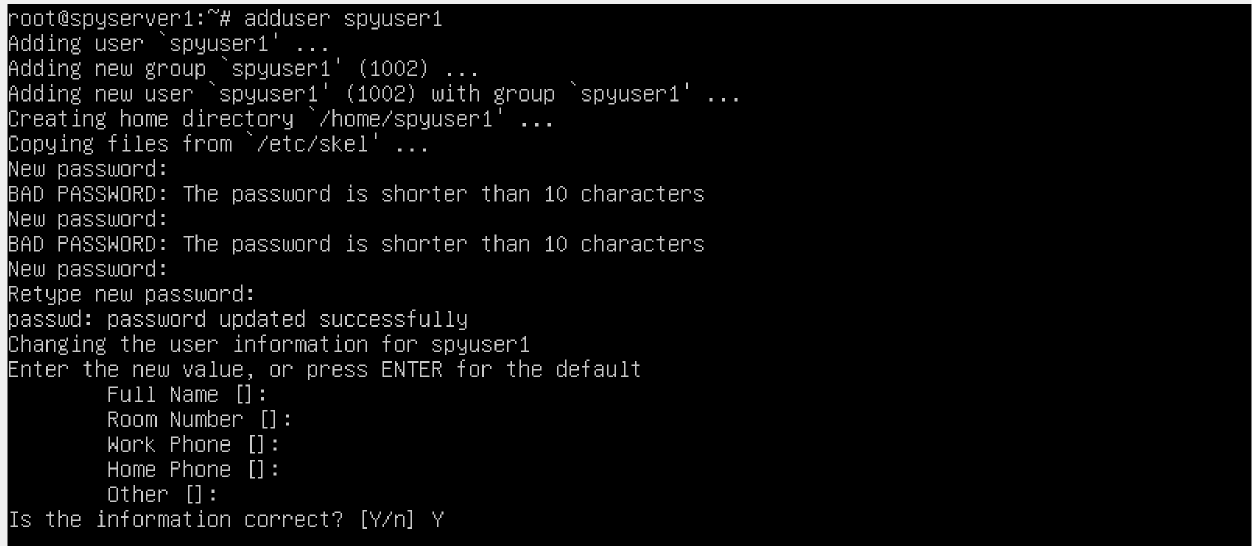


```
root@spyserver1:~# adduser spy3
Adding user `spy3' ...
Adding new group `spy3' (1001) ...
Adding new user `spy3' (1001) with group `spy3' ...
Creating home directory `/home/spy3' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for spy3
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y_
```



```
root@spyserver1:~# usermod -aG sudo spy3
root@spyserver1:~# groups spy3
spy3 : spy3 sudo
root@spyserver1:~#
```

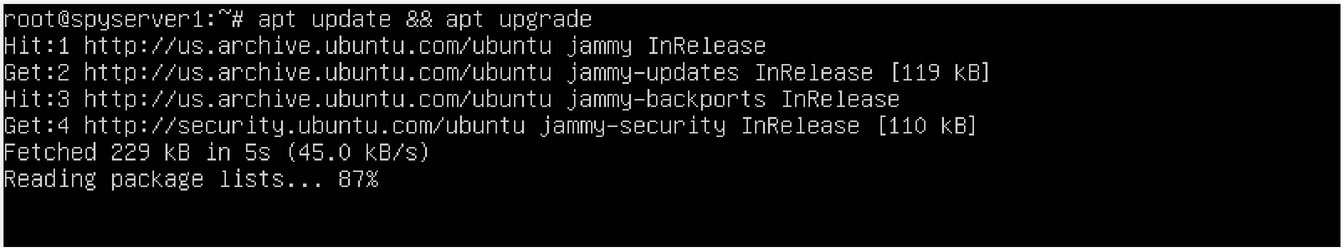
Spyuser1:



```
root@spyserver1:~# adduser spyuser1
Adding user `spyuser1' ...
Adding new group `spyuser1' (1002) ...
Adding new user `spyuser1' (1002) with group `spyuser1' ...
Creating home directory `/home/spyuser1' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 10 characters
New password:
BAD PASSWORD: The password is shorter than 10 characters
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for spyuser1
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
```

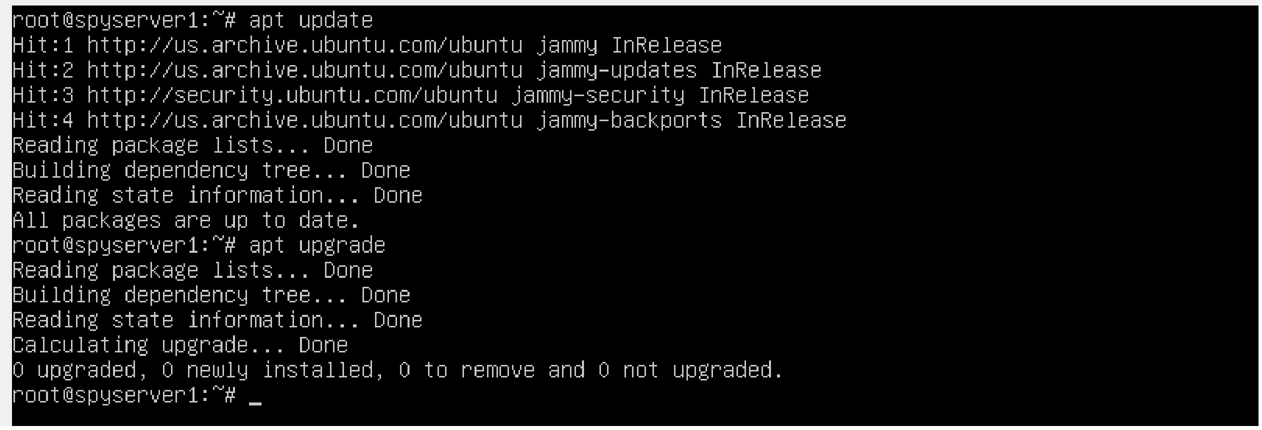
Section #3 Update the system

After installing a new Linux server, always update the system and all its packages.



```
root@spyserver1:~# apt update && apt upgrade
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Hit:3 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Fetched 229 kB in 5s (45.0 kB/s)
Reading package lists... 87%
```

First update the repository, then upgrade all the packages!

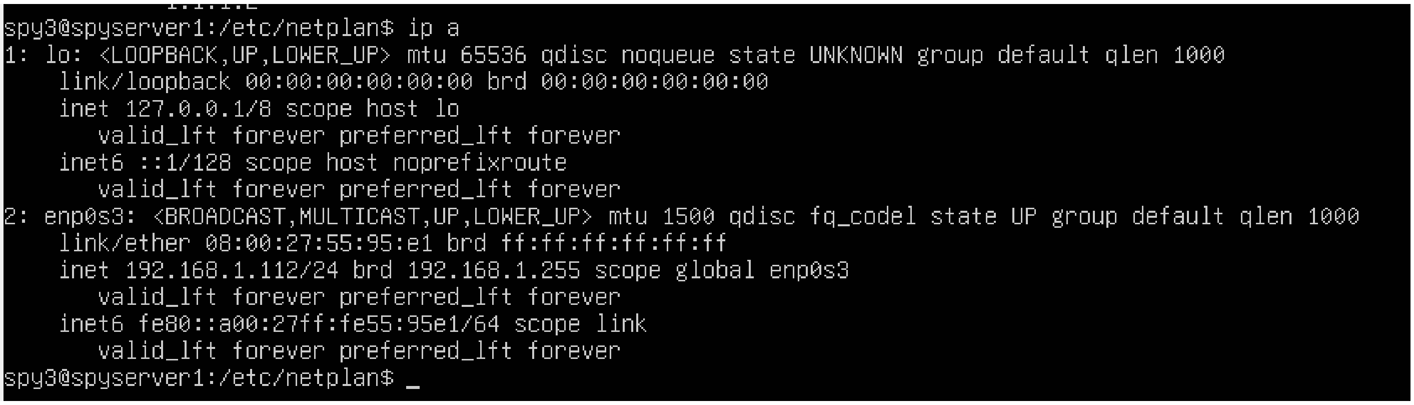


```
root@spyserver1:~# apt update
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
root@spyserver1:~# apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@spyserver1:~# _
```

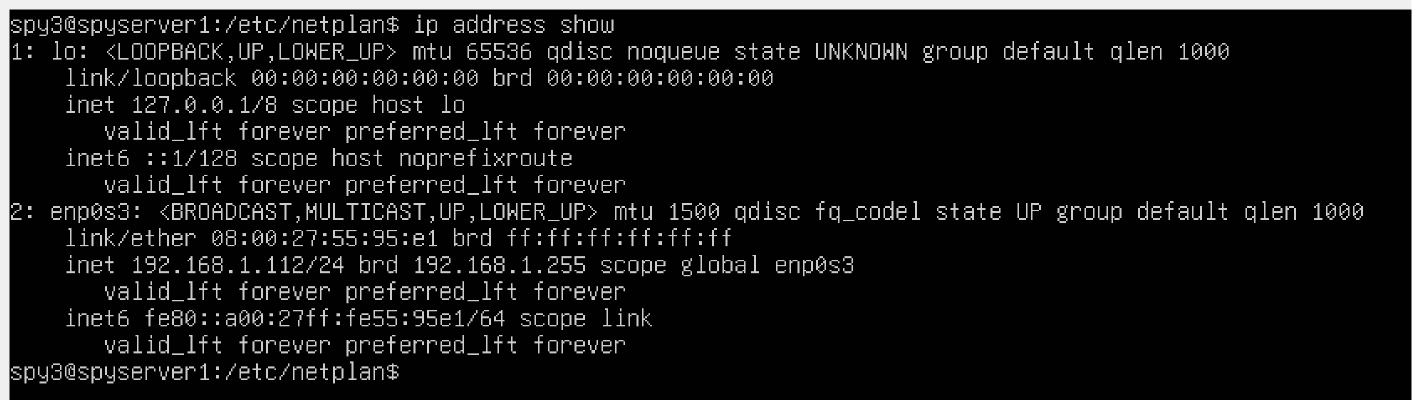
Section #4 Assigning a static IP address

It is important to have a static IP address for a server since you do not want a dynamic, changing IP address that will make it hard for requests to land on it. Having a static address ensures that the server can be accessed easily by clients.

Step #1. Identify current IP Address used for the server. You can use either ip a or ip address show to view the currently assigned IP address.

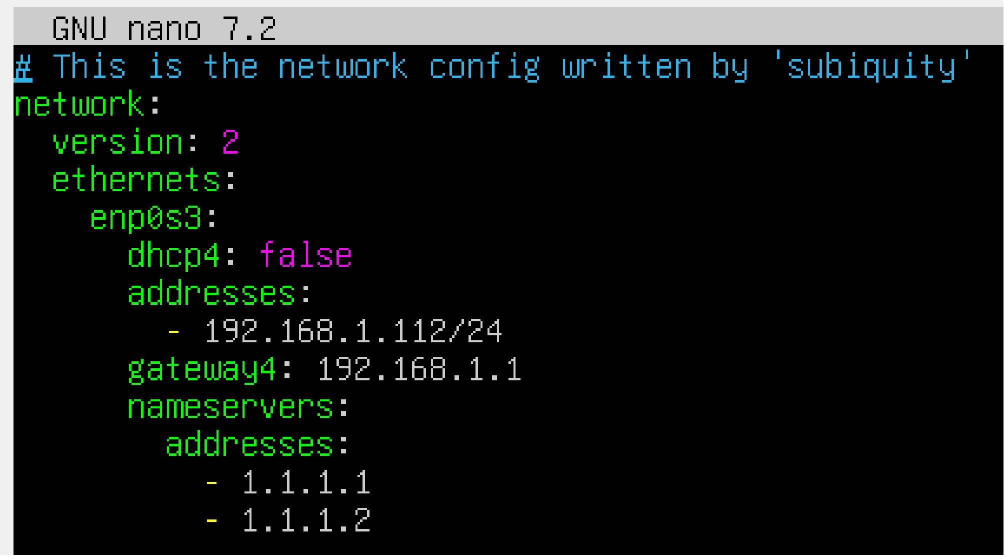


```
spy3@spyserver1:/etc/netplan$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:55:95:e1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.112/24 brd 192.168.1.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe55:95e1/64 scope link
       valid_lft forever preferred_lft forever
spy3@spyserver1:/etc/netplan$ _
```



```
spy3@spyserver1:/etc/netplan$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:55:95:e1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.112/24 brd 192.168.1.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe55:95e1/64 scope link
       valid_lft forever preferred_lft forever
spy3@spyserver1:/etc/netplan$
```

Step #2. Assign the same IP address statically. This can be accomplished by editing the configuration file under/etc/netplan/. This configuration file uses a yaml structure to configure network settings.



```
  GNU nano 7.2
# This is the network config written by 'subiquity'
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: false
      addresses:
        - 192.168.1.112/24
      gateway4: 192.168.1.1
      nameservers:
        addresses:
          - 1.1.1.1
          - 1.1.1.2
```

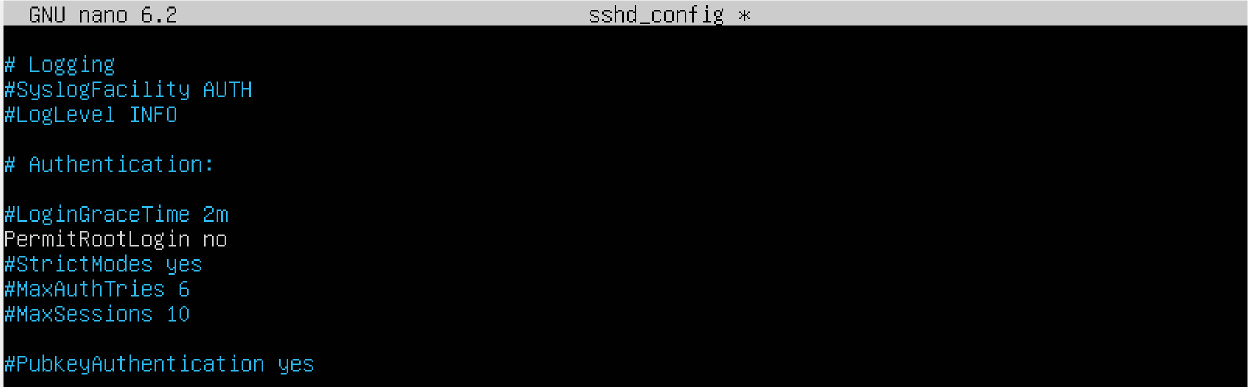
I configured the enp0s3 ethernet interface (the internet interface used by VirtualBox) to use a static ip. Note how I had to also add a gateway and nameservers. Without a gateway the server would not be able to communicate with devices outside of its own subnet. I also needed nameservers for the purpose of being able to resolve internet host names. You might wonder why an Ubuntu server which does not have a browser installed would need to resolve DNS addresses. Well the main reason is for updates since the package manager needs to resolve the hostnames of the repositories where the packages are stored.

Section #5 Implement basic post-installation security measures

1. Harden OpenSSH by editing the /etc/ssh/sshd_config configuration file.

   - Block root SSH login.

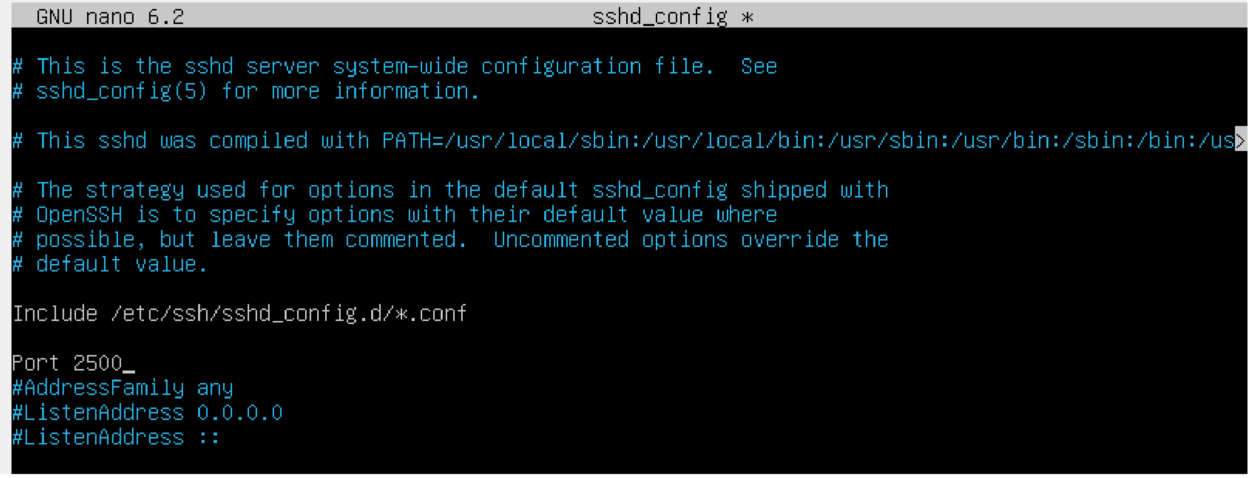
   Screenshot:



```
  GNU nano 6.2                                    sshd_config *

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes
```

   - Change the default ssh port. I changed the default ssh port value of 22 to 2500.

   Screenshot:

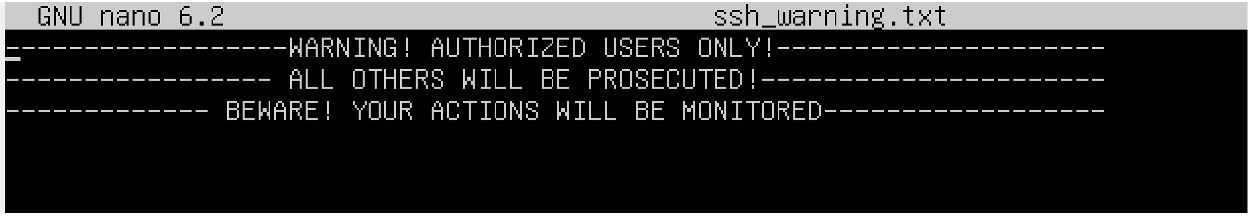


```
  GNU nano 6.2                                    sshd_config *

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/us>

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 2500_
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

   - Create an SSH login banner.

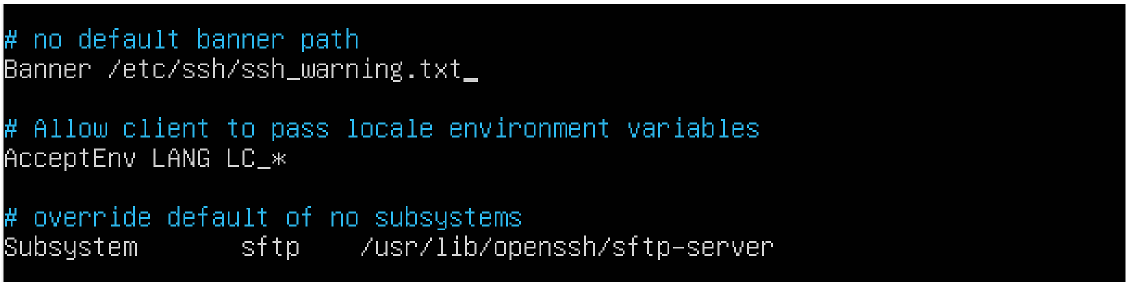
   Screenshots:

   1. In the /etc/ssh directory, create the login banner txt file.



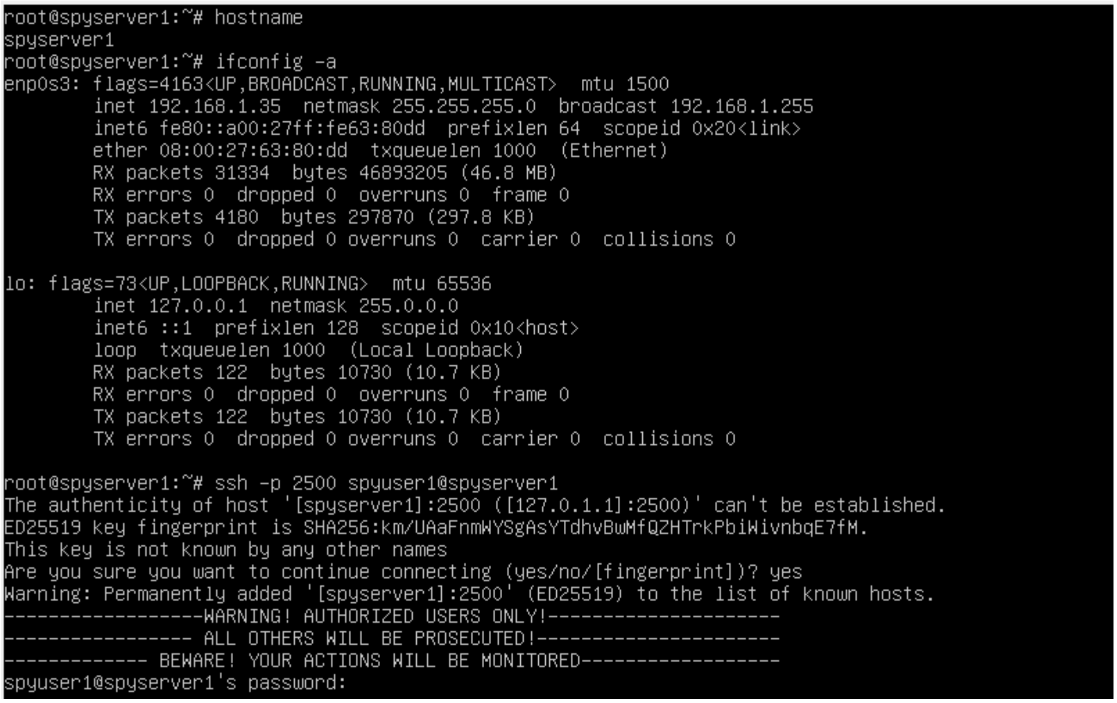
```
  GNU nano 6.2                                    ssh_warning.txt
------------------WARNING! AUTHORIZED USERS ONLY!----------------------
------------------ ALL OTHERS WILL BE PROSECUTED!-----------------------
-------------- BEWARE! YOUR ACTIONS WILL BE MONITORED-------------------
```

   2. Add the banner txt file you created to the /etc/ssh/sshd_config file.



```
# no default banner path
Banner /etc/ssh/ssh_warning.txt_

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem       sftp    /usr/lib/openssh/sftp-server
```

3. Test that the banner appears during SSH login.



```
root@spyserver1:~# hostname
spyserver1
root@spyserver1:~# ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.35  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe63:80dd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:63:80:dd  txqueuelen 1000  (Ethernet)
        RX packets 31334  bytes 46893205 (46.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4180  bytes 297870 (297.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 122  bytes 10730 (10.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 122  bytes 10730 (10.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@spyserver1:~# ssh -p 2500 spyuser1@spyserver1
The authenticity of host '[spyserver1]:2500 ([127.0.1.1]:2500)' can't be established.
ED25519 key fingerprint is SHA256:km/UAaFnmWYSgAsYTdhvBwMfQZHTrkPbiWivnbqE7fM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[spyserver1]:2500' (ED25519) to the list of known hosts.
------------------WARNING! AUTHORIZED USERS ONLY!---------------------
----------------- ALL OTHERS WILL BE PROSECUTED!----------------------
------------- BEWARE! YOUR ACTIONS WILL BE MONITORED------------------
spyuser1@spyserver1's password:
```