Suppervised by Pr. TADIST KHAWLA

FINAL PROJECT : ENTERPRISE NETWORK

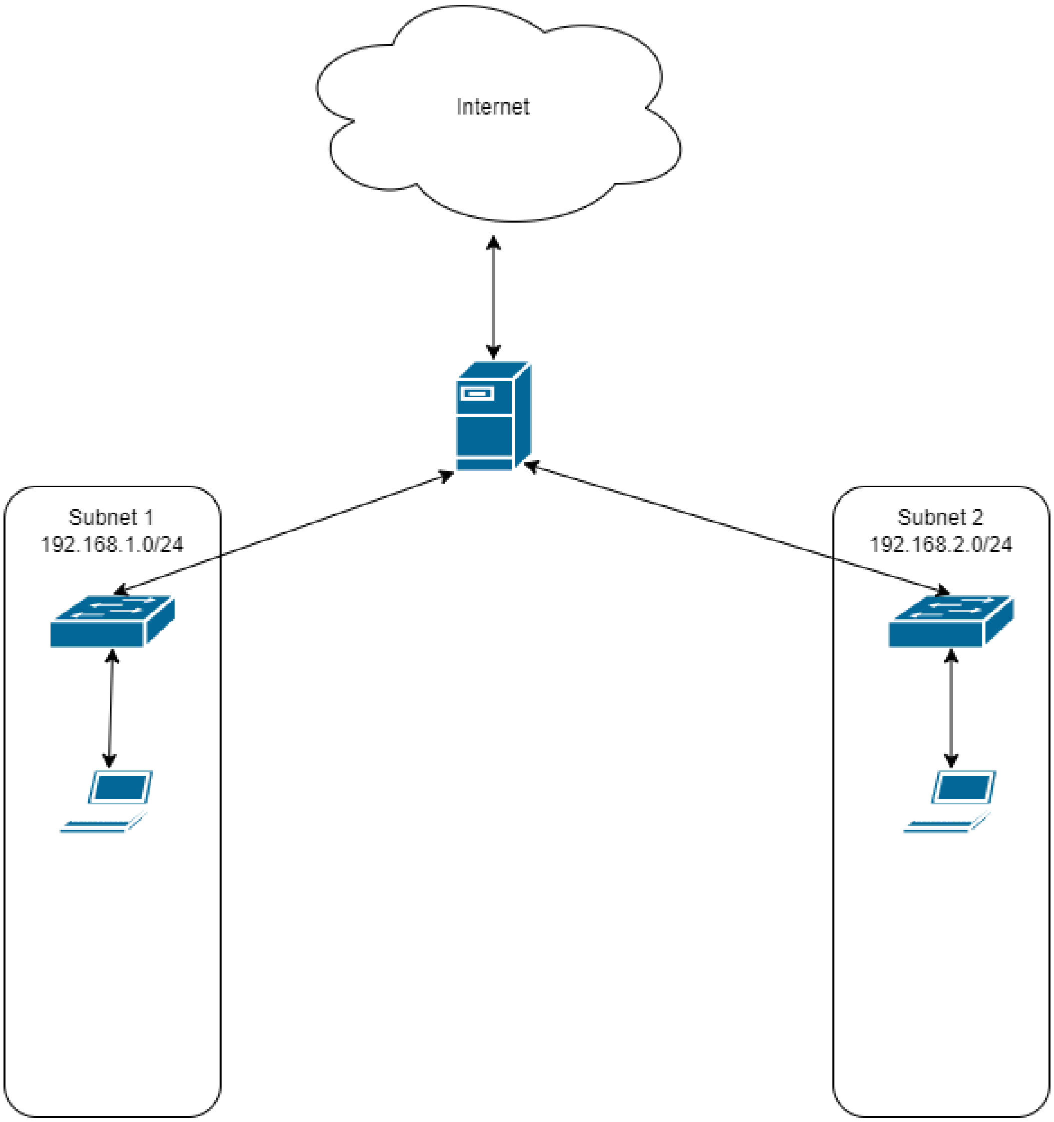
Belmessid Anas

Contents

Network Topology

There is a main server connected to the Internet and two subnets. The server will be hosting following services

- DHCP for both Subnet 1 and Subnet 2
- DNS Server
- FTP Server (For subnet 1 only)
- HTTP Server
- Email Exchange
- LDAP

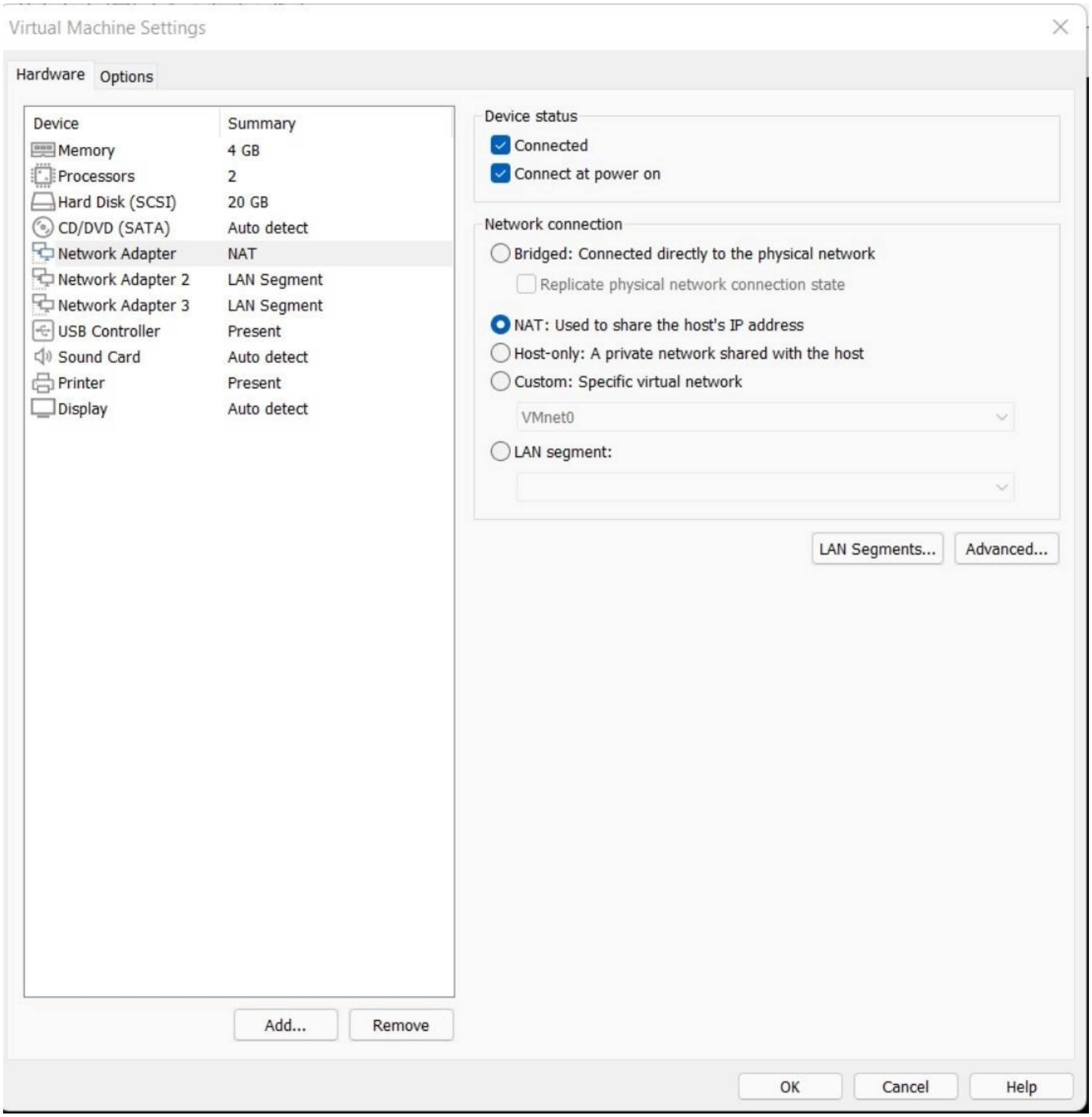


Enterprise Network Implementation

1. Environment Setup

We will use 3 Ubuntu based VMs to simulate above mentioned network topology and implement the network services.

First VM will act as a server for both subnets “subnet 1” and “subnet 2”. It is assigned 3 Network Interface Card (NIC). First is connected to the Internet, second is connected to an Internal Network titled “Subnet 1” and third is connected to “Subnet 2”.



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	4 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Auto detect
Network Adapter	NAT
Network Adapter 2	LAN Segment
Network Adapter 3	LAN Segment
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

● NAT: Used to share the host's IP address

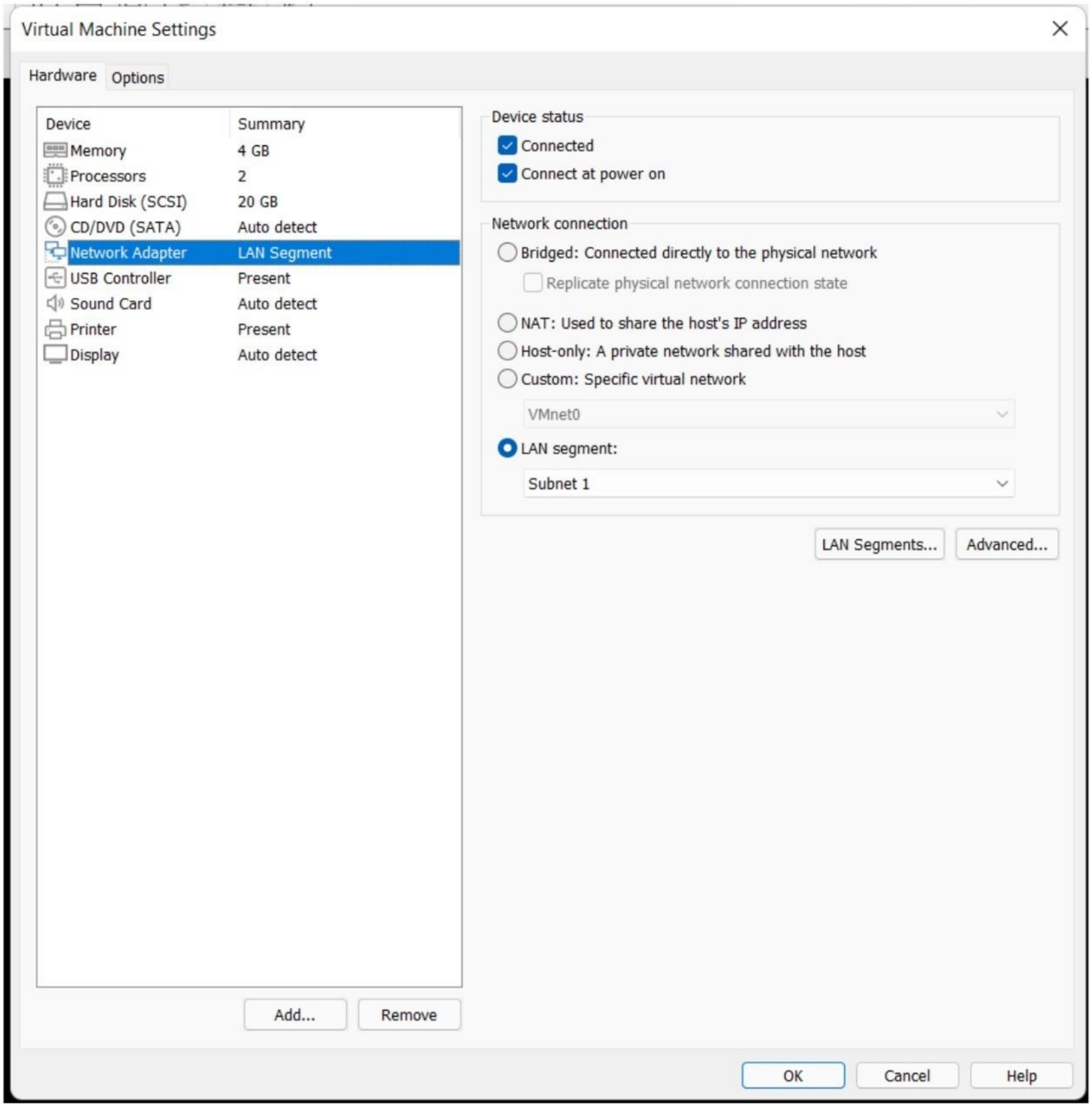
○ Host-only: A private network shared with the host

○ Custom: Specific virtual network

VMnet0

○ LAN segment:

Similarly a second VM is assigned only one Network Interface Card (NIC) and is connected to "Subnet 1" LAN segment.



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	4 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Auto detect
Network Adapter	LAN Segment
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

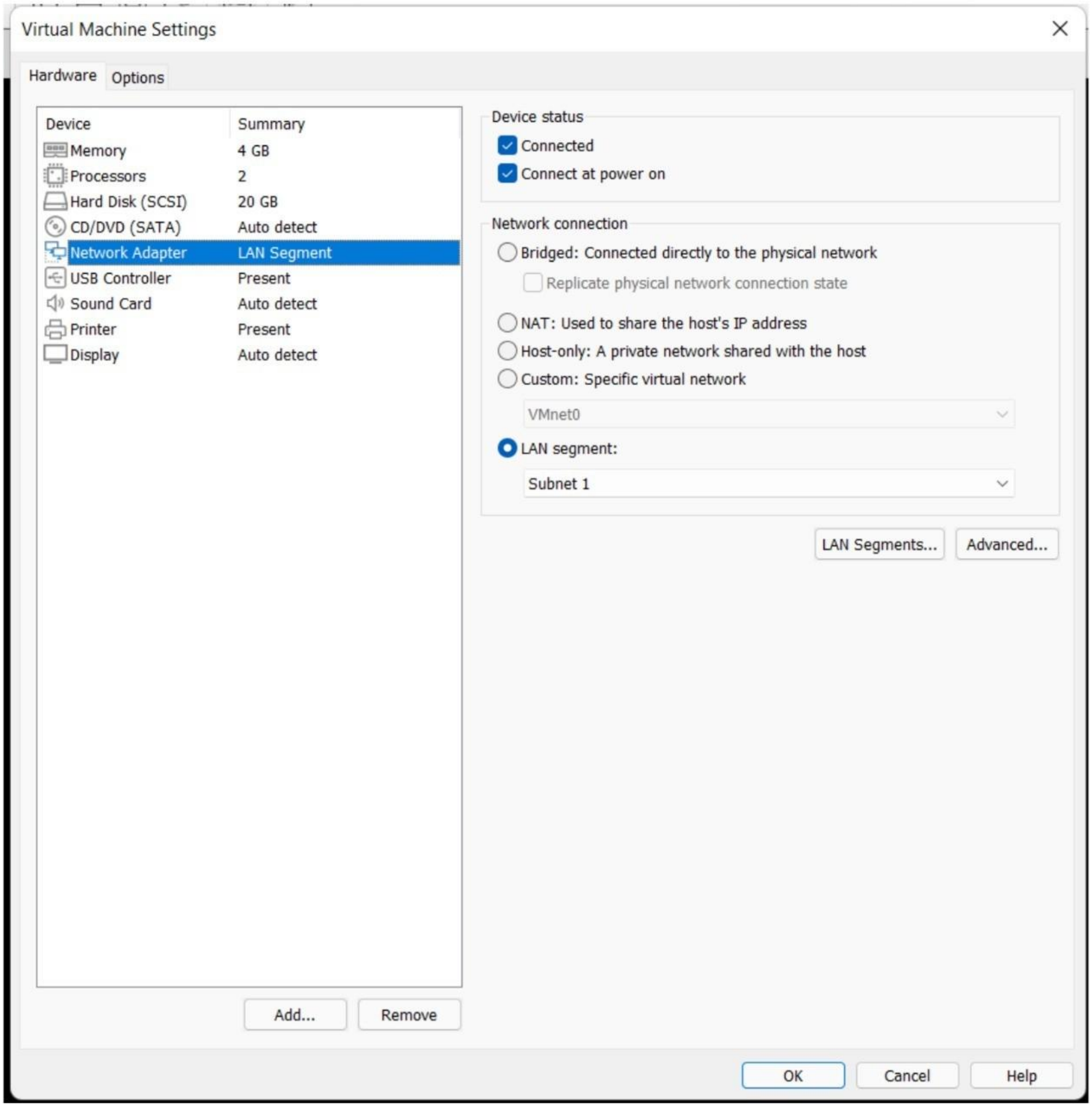
○ Custom: Specific virtual network

VMnet0

● LAN segment:

Subnet 1

And 3rd VM is connected to "Subnet 2" LAN segment.



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	4 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Auto detect
Network Adapter	LAN Segment
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

○ Custom: Specific virtual network

VMnet0

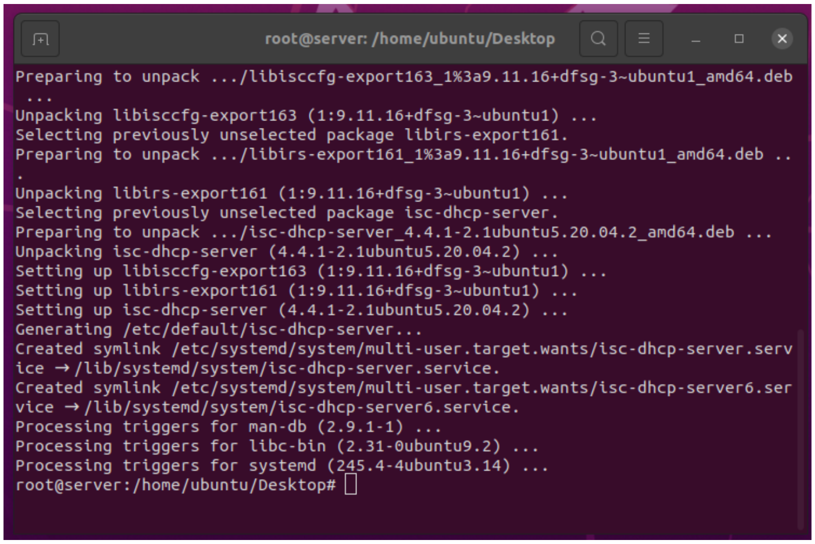
● LAN segment:

Subnet 1

2. Configure DHCP for both subnets.

We will need to install DHCP server program to serve IPs to the hosts over the subnets. Following is the command to install DHCP server

```
# apt -y install isc-dhcp-server
```



```
Preparing to unpack .../libisccfg-export163_1%3a9.11.16+dfsg-3~ubuntu1_amd64.deb
 ...
Unpacking libisccfg-export163 (1:9.11.16+dfsg-3~ubuntu1) ...
Selecting previously unselected package libirs-export161.
Preparing to unpack .../libirs-export161_1%3a9.11.16+dfsg-3~ubuntu1_amd64.deb ..
.
Unpacking libirs-export161 (1:9.11.16+dfsg-3~ubuntu1) ...
Selecting previously unselected package isc-dhcp-server.
Preparing to unpack .../isc-dhcp-server_4.4.1-2.1ubuntu5.20.04.2_amd64.deb ...
Unpacking isc-dhcp-server (4.4.1-2.1ubuntu5.20.04.2) ...
Setting up libisccfg-export163 (1:9.11.16+dfsg-3~ubuntu1) ...
Setting up libirs-export161 (1:9.11.16+dfsg-3~ubuntu1) ...
Setting up isc-dhcp-server (4.4.1-2.1ubuntu5.20.04.2) ...
Generating /etc/default/isc-dhcp-server...
Created symlink /etc/systemd/system/multi-user.target.wants/isc-dhcp-server.serv
ice → /lib/systemd/system/isc-dhcp-server.service.
Created symlink /etc/systemd/system/multi-user.target.wants/isc-dhcp-server6.ser
vice → /lib/systemd/system/isc-dhcp-server6.service.
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
Processing triggers for systemd (245.4-4ubuntu3.14) ...
root@server:/home/ubuntu/Desktop# 
```

isc-dhcp-server is successfully installed. Next we need to edit the configuration file to define two IP Addresses ranges for the subnets.

We need to assign static IP addresses to both interfaces of the server for DHCP sever to work.

We will specify interfaces for the DHCP server in /etc/default/isc-dhcp-server configuration file

```
INTERFACESv4="eth0 enp0s3"
```

Next we need to specify DHCP IP ranges in /var/lib/dhcp/dhcpd.leases

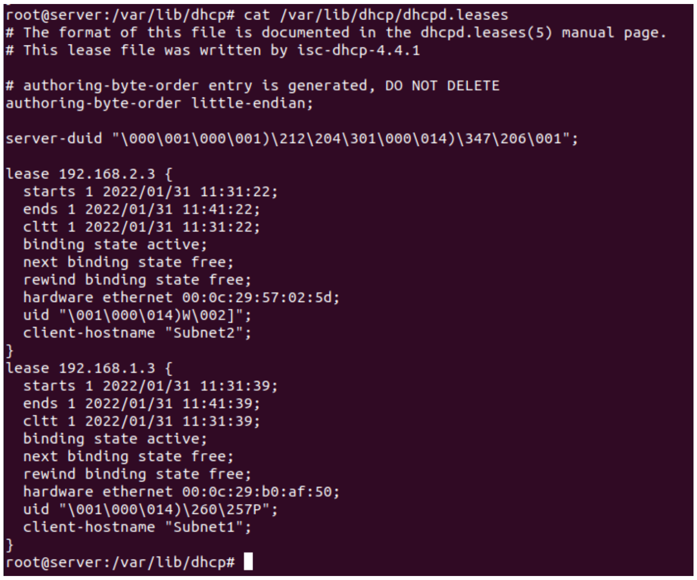
```
subnet 192.168.1.0 netmask 255.255.255.0 {
        option subnet-mask 255.255.255.0;
        option routers 192.168.1.1;
        range 192.168.1.2 192.168.1.10;
}
subnet 192.168.2.0 netmask 255.255.255.0 {
        option subnet-mask 255.255.255.0;
        option routers 192.168.2.1;
        range 192.168.2.2 192.168.2.10;
}
```

Restart the DHCP server for the changes to take effect

```
systemctl restart isc-dhcp-server
```

Next we can see the lease file to see if DHCP server is assigning the IP Addresses

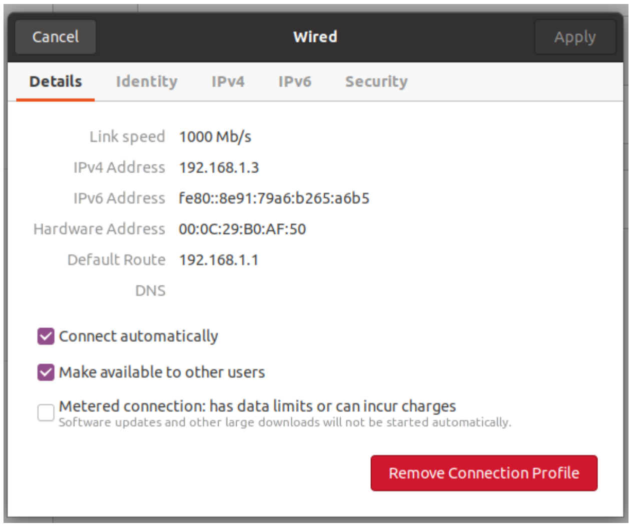
```
#cat /var/lib/dhcp/dhcpd.leases
```



```
root@server:/var/lib/dhcp# cat /var/lib/dhcp/dhcpd.leases
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.4.1

# authoring-byte-order entry is generated, DO NOT DELETE
authoring-byte-order little-endian;

server-duid "\000\001\000\001)\212\204\301\000\014)\347\206\001";

lease 192.168.2.3 {
  starts 1 2022/01/31 11:31:22;
  ends 1 2022/01/31 11:41:22;
  cltt 1 2022/01/31 11:31:22;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 00:0c:29:57:02:5d;
  uid "\001\000\014)W\002]";
  client-hostname "Subnet2";
}
lease 192.168.1.3 {
  starts 1 2022/01/31 11:31:39;
  ends 1 2022/01/31 11:41:39;
  cltt 1 2022/01/31 11:31:39;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 00:0c:29:b0:af:50;
  uid "\001\000\014)\260\257P";
  client-hostname "Subnet1";
}
root@server:/var/lib/dhcp# 
```

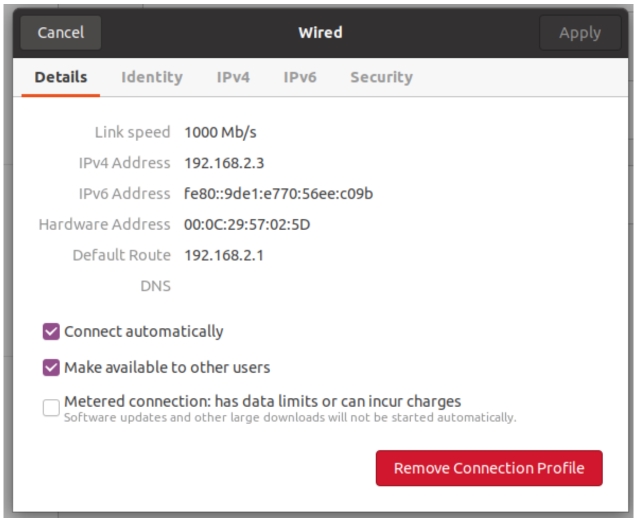
We see that 192.168.2.3 and 192.168.1.3 are assigned successfully.

Next we can verify from the clients in “Subnet 1” and “Subnet 2”.



Link speed 1000 Mb/s
IPv4 Address 192.168.1.3
IPv6 Address fe80::8e91:79a6:b265:a6b5
Hardware Address 00:0C:29:B0:AF:50
Default Route 192.168.1.1
DNS

☑ Connect automatically
☑ Make available to other users
□ Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.



Link speed 1000 Mb/s
IPv4 Address 192.168.2.3
IPv6 Address fe80::9de1:e770:56ee:c09b
Hardware Address 00:0C:29:57:02:5D
Default Route 192.168.2.1
DNS

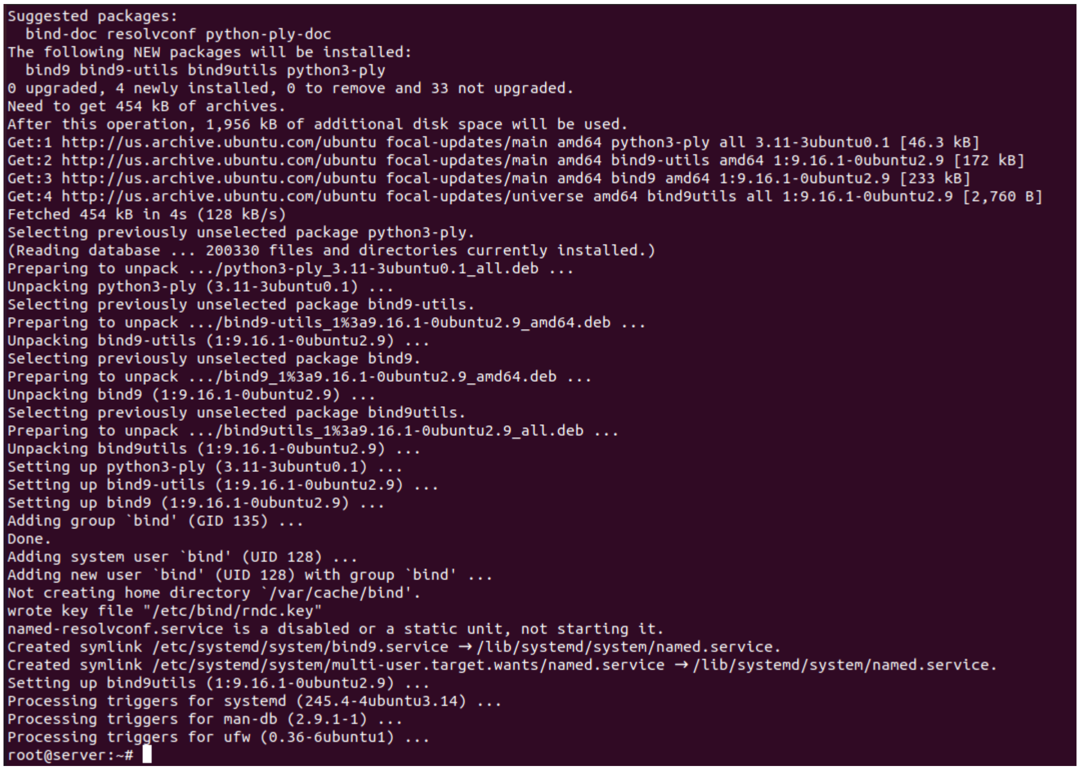
☑ Connect automatically
☑ Make available to other users
□ Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.

3. Configure DNS Server

DNS stands for Domain Name System. DNS is a hierarchical distributed system that is used to translate a domain name to IP address over Internet or in private networks. A computer connected to the Internet can only communicate with the IP Addresses but it is almost impossible for humans to remember IP Addresses for all the servers available on Internet. DNS solves this problem by providing Domain name to IP address translation service. Bind is highly used DNS server package available in Linux systems.

We need to install DNS Server service

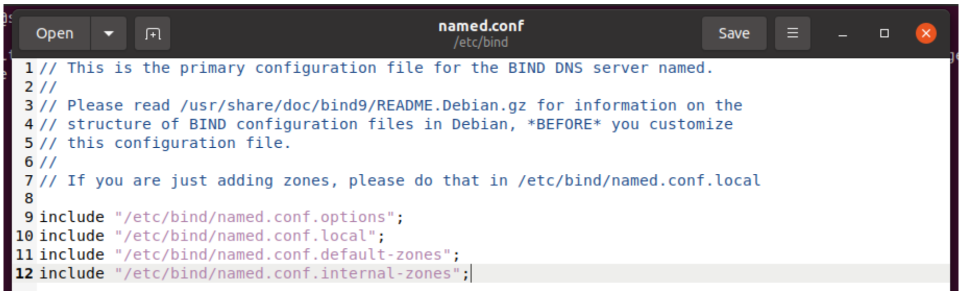
```
# apt -y install bind9 bind9utils
```



```
Suggested packages:
  bind-doc resolvconf python-ply-doc
The following NEW packages will be installed:
  bind9 bind9-utils bind9utils python3-ply
0 upgraded, 4 newly installed, 0 to remove and 33 not upgraded.
Need to get 454 kB of archives.
After this operation, 1,956 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 python3-ply all 3.11-3ubuntu0.1 [46.3 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 bind9-utils amd64 1:9.16.1-0ubuntu2.9 [172 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 bind9 amd64 1:9.16.1-0ubuntu2.9 [233 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal-updates/universe amd64 bind9utils all 1:9.16.1-0ubuntu2.9 [2,760 B]
Fetched 454 kB in 4s (128 kB/s)
Selecting previously unselected package python3-ply.
(Reading database ... 200330 files and directories currently installed.)
Preparing to unpack .../python3-ply_3.11-3ubuntu0.1_all.deb ...
Unpacking python3-ply (3.11-3ubuntu0.1) ...
Selecting previously unselected package bind9-utils.
Preparing to unpack .../bind9-utils_1%3a9.16.1-0ubuntu2.9_amd64.deb ...
Unpacking bind9-utils (1:9.16.1-0ubuntu2.9) ...
Selecting previously unselected package bind9.
Preparing to unpack .../bind9_1%3a9.16.1-0ubuntu2.9_amd64.deb ...
Unpacking bind9 (1:9.16.1-0ubuntu2.9) ...
Selecting previously unselected package bind9utils.
Preparing to unpack .../bind9utils_1%3a9.16.1-0ubuntu2.9_all.deb ...
Unpacking bind9utils (1:9.16.1-0ubuntu2.9) ...
Setting up python3-ply (3.11-3ubuntu0.1) ...
Setting up bind9-utils (1:9.16.1-0ubuntu2.9) ...
Setting up bind9 (1:9.16.1-0ubuntu2.9) ...
Adding group `bind' (GID 135) ...
Done.
Adding system user `bind' (UID 128) ...
Adding new user `bind' (UID 128) with group `bind' ...
Not creating home directory `/var/cache/bind'.
wrote key file "/etc/bind/rndc.key"
named-resolvconf.service is a disabled or a static unit, not starting it.
Created symlink /etc/systemd/system/bind9.service → /lib/systemd/system/named.service.
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /lib/systemd/system/named.service.
Setting up bind9utils (1:9.16.1-0ubuntu2.9) ...
Processing triggers for systemd (245.4-4ubuntu3.14) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for ufw (0.36-6ubuntu1) ...
root@server:~#
```

Next we need to configure /etc/bind/named.conf to allow internal network to access Bind service.

Add following line in configuration file
include "/etc/bind/named.conf.internal-zones";



```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
include "/etc/bind/named.conf.internal-zones";
```

Forwarders 1.1.1.1 and 8.8.8.8

Forwarders are the DNS servers which are contacted by the local DNS server to resolve a domain name for which the local DNS servers don't have any records. Here we are using 1.1.1.1 and 8.8.8.8 as forwarders.

Next edit /etc/bind/named.conf.options to add an ACL entry for 192.168.1.0/24 and 192.168.2.0/24 networks.

Set ACL(Access Control List) entry for local network

```
acl internal-network {

       192.168.1.0/24; 192.168.2.0/24;

};

forwarders {

        1.1.1.1; 8.8.8.8;

};

allow-query { localhost; internal-network; };

recursion yes;
```

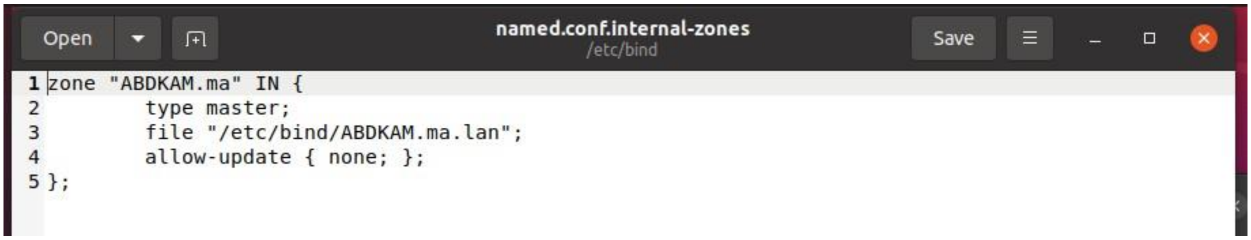
Zone

Every domain in the DNS server is stored at server in form of a zone file. A zone file stores information about a start of authority (SOA). Normally a domain name is also a start of the authority. It is part of domain for which local DNS sever is authoritative name server. It means that the local server has all records locally available for that specific domain and does not need to contact forwarders for the name resolution.

/etc/bind/named.conf.internal-zones file contains all internal zones. We need to define a local file where the details of DNS records are stored and Zone name. In following configurations we are defining **forward zone** that is used to translate domain name to IP address.

Edit /etc/bind/named.conf.internal-zones to add a zone

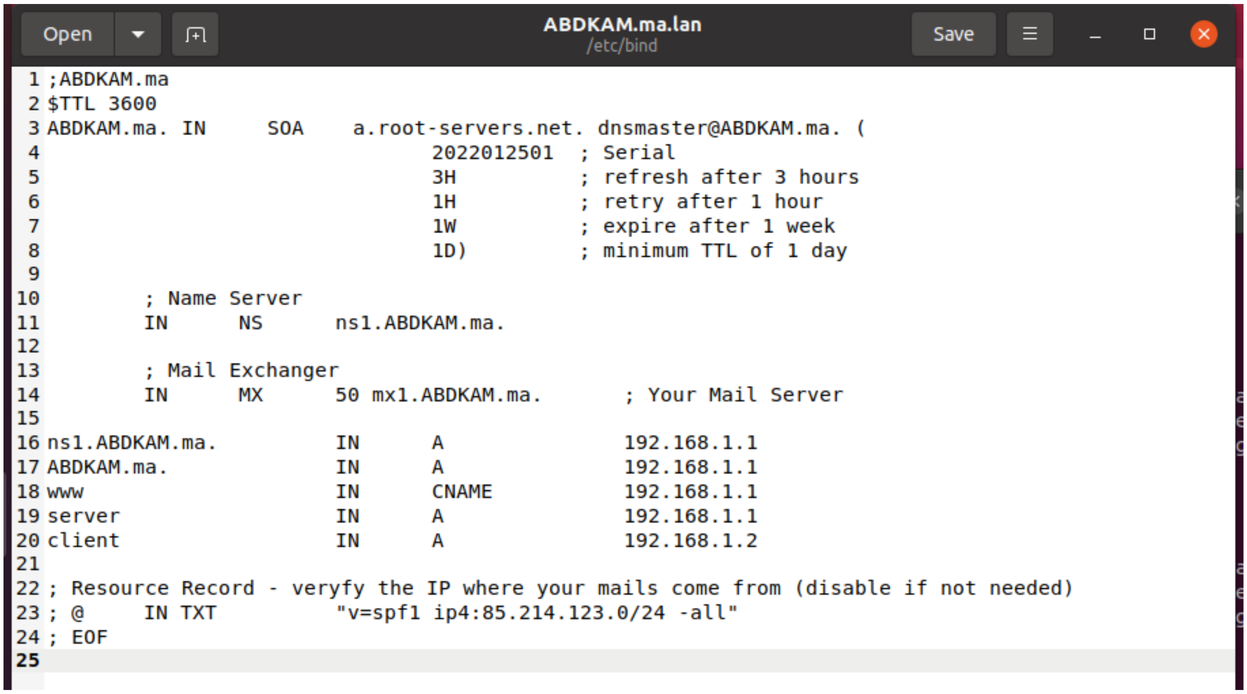
```
zone "ABDKAM.ma" IN {
        type master;
        file "/etc/bind/ABDKAM.ma.lan";
        allow-update { none; };
};
```



```
zone "ABDKAM.ma" IN {
        type master;
        file "/etc/bind/ABDKAM.ma.lan";
        allow-update { none; };
};
```

Next we need to create /etc/bind/ABDKAM.ma.lan to define zone entries

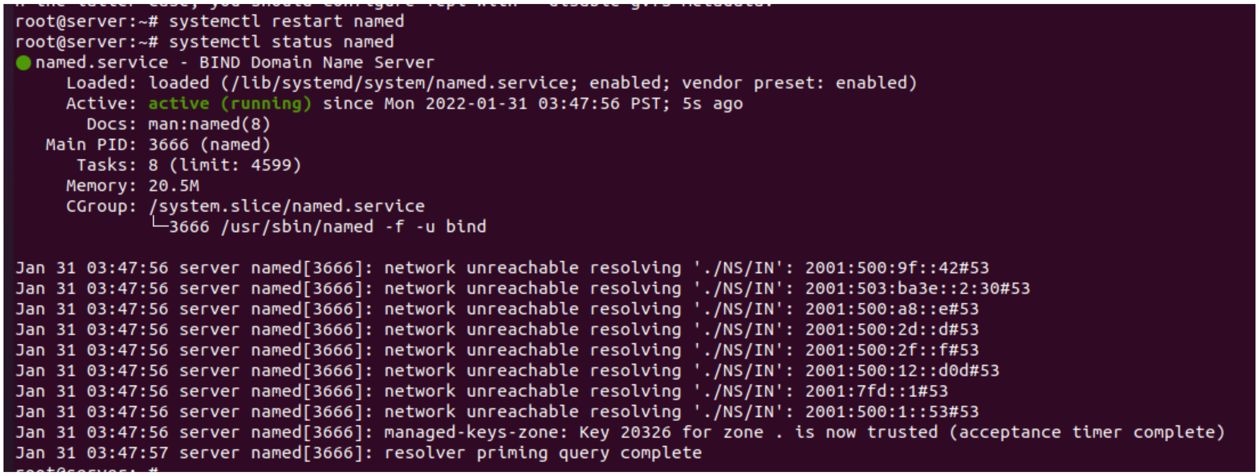
```
;ABDKAM.ma
$TTL 3600
ABDKAM.ma. IN     SOA    a.root-servers.net. dnsmaster@ABDKAM.ma. (
                          2022012501  ; Serial
                          3H          ; refresh after 3 hours
                          1H          ; retry after 1 hour
                          1W          ; expire after 1 week
                          1D)         ; minimum TTL of 1 day

      ; Name Server
      IN     NS     ns1.ABDKAM.ma.

      ; Mail Exchanger
      IN     MX     50 mx1.ABDKAM.ma.   ; Your Mail Server

ns1.ABDKAM.ma.      IN     A             192.168.1.1
ABDKAM.ma.          IN     A             192.168.1.1
www                 IN     CNAME         192.168.1.1
server              IN     A             192.168.1.1
client              IN     A             192.168.1.2

; Resource Record - verify the IP where your mails come from (disable if not needed)
; @    IN TXT       "v=spf1 ip4:85.214.123.0/24 -all"
; EOF
```



```
;ABDKAM.ma
$TTL 3600
ABDKAM.ma. IN     SOA    a.root-servers.net. dnsmaster@ABDKAM.ma. (
                                2022012501  ; Serial
                                3H          ; refresh after 3 hours
                                1H          ; retry after 1 hour
                                1W          ; expire after 1 week
                                1D)         ; minimum TTL of 1 day

        ; Name Server
        IN      NS      ns1.ABDKAM.ma.

        ; Mail Exchanger
        IN      MX      50 mx1.ABDKAM.ma.       ; Your Mail Server

ns1.ABDKAM.ma.          IN      A               192.168.1.1
ABDKAM.ma.              IN      A               192.168.1.1
www                     IN      CNAME           192.168.1.1
server                  IN      A               192.168.1.1
client                  IN      A               192.168.1.2

; Resource Record - veryfy the IP where your mails come from (disable if not needed)
; @     IN TXT          "v=spf1 ip4:85.214.123.0/24 -all"
; EOF
```

Next we need to restart DNS server and see if it's working

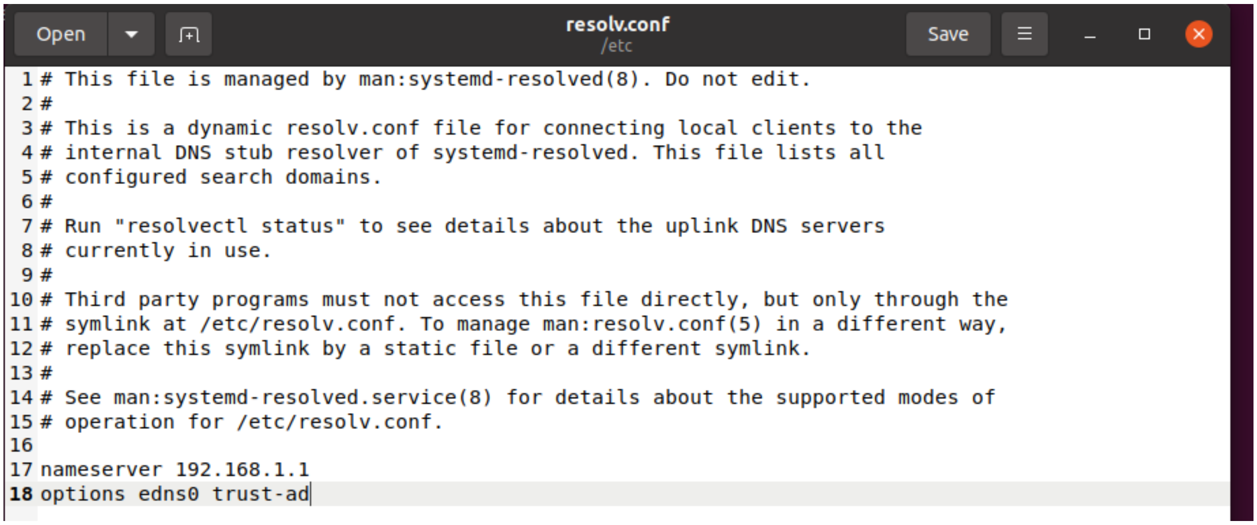
```
# systemctl restart named

# systemctl status named
```



```
root@server:~# systemctl restart named
root@server:~# systemctl status named
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2022-01-31 03:47:56 PST; 5s ago
       Docs: man:named(8)
   Main PID: 3666 (named)
      Tasks: 8 (limit: 4599)
     Memory: 20.5M
     CGroup: /system.slice/named.service
             └─3666 /usr/sbin/named -f -u bind

Jan 31 03:47:56 server named[3666]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
Jan 31 03:47:56 server named[3666]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
Jan 31 03:47:56 server named[3666]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
Jan 31 03:47:56 server named[3666]: network unreachable resolving './NS/IN': 2001:500:2d::d#53
Jan 31 03:47:56 server named[3666]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
Jan 31 03:47:56 server named[3666]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
Jan 31 03:47:56 server named[3666]: network unreachable resolving './NS/IN': 2001:7fd::1#53
Jan 31 03:47:56 server named[3666]: network unreachable resolving './NS/IN': 2001:500:1::53#53
Jan 31 03:47:56 server named[3666]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
Jan 31 03:47:57 server named[3666]: resolver priming query complete
```

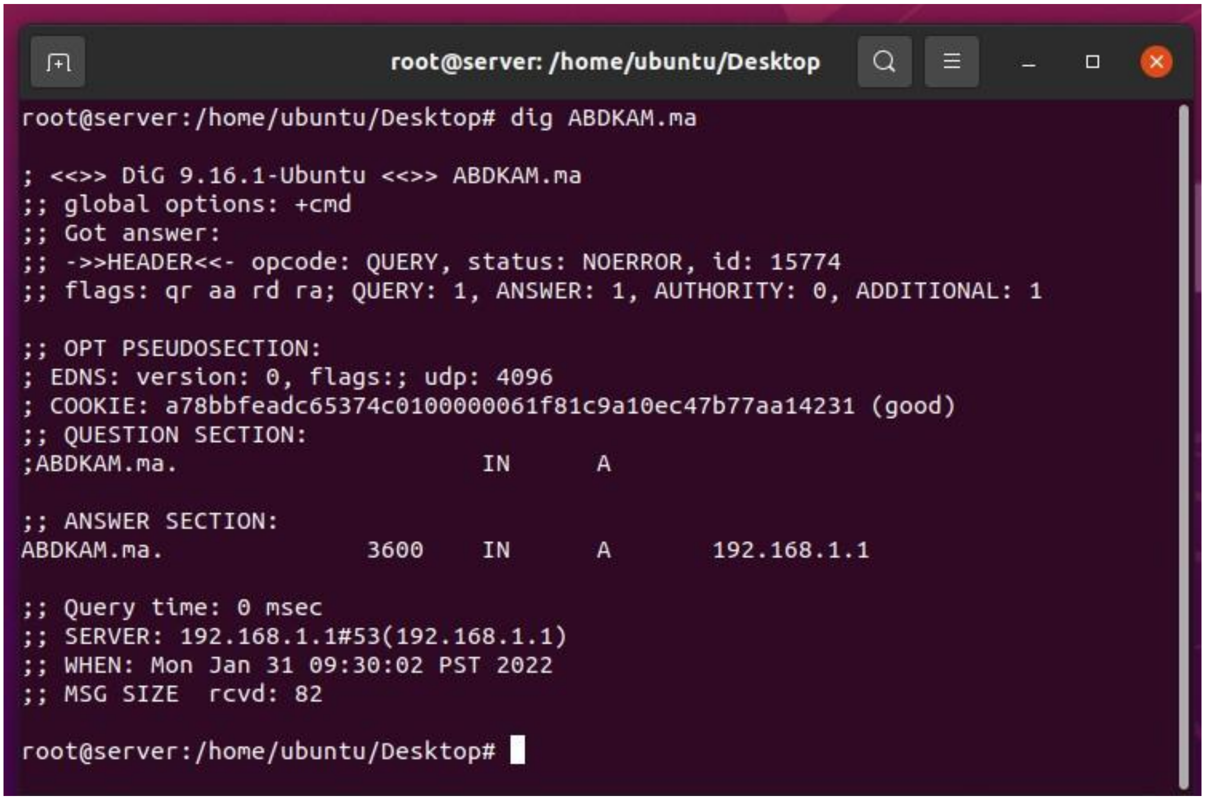
Server is running.

To test the DNS server we will change local DNS resolver to 192.168.1.1 by editing /etc/resolv.conf file



```
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 192.168.1.1
options edns0 trust-ad
```

Next we dig ABDKAM.ma and we see that A record is there with IP Address 192.168.1.1

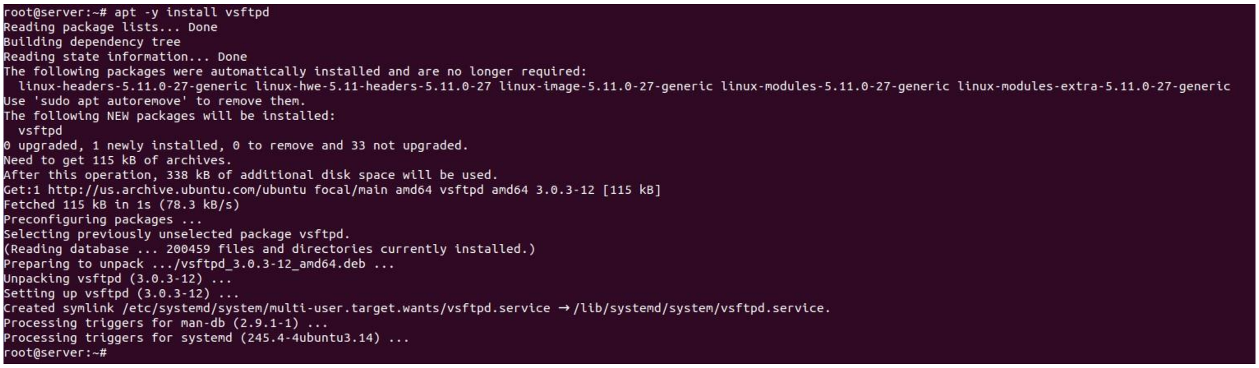


```
root@server:/home/ubuntu/Desktop# dig ABDKAM.ma

; <<>> DiG 9.16.1-Ubuntu <<>> ABDKAM.ma
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15774
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a78bbfeadc65374c0100000061f81c9a10ec47b77aa14231 (good)
;; QUESTION SECTION:
;ABDKAM.ma.                     IN      A

;; ANSWER SECTION:
ABDKAM.ma.              3600    IN      A       192.168.1.1

;; Query time: 0 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Jan 31 09:30:02 PST 2022
;; MSG SIZE  rcvd: 82

root@server:/home/ubuntu/Desktop# 
```

4. Configure FTP Server (For subnet 1 only)

We will use vsftpd as FTP server software. To install vsftpd, command is

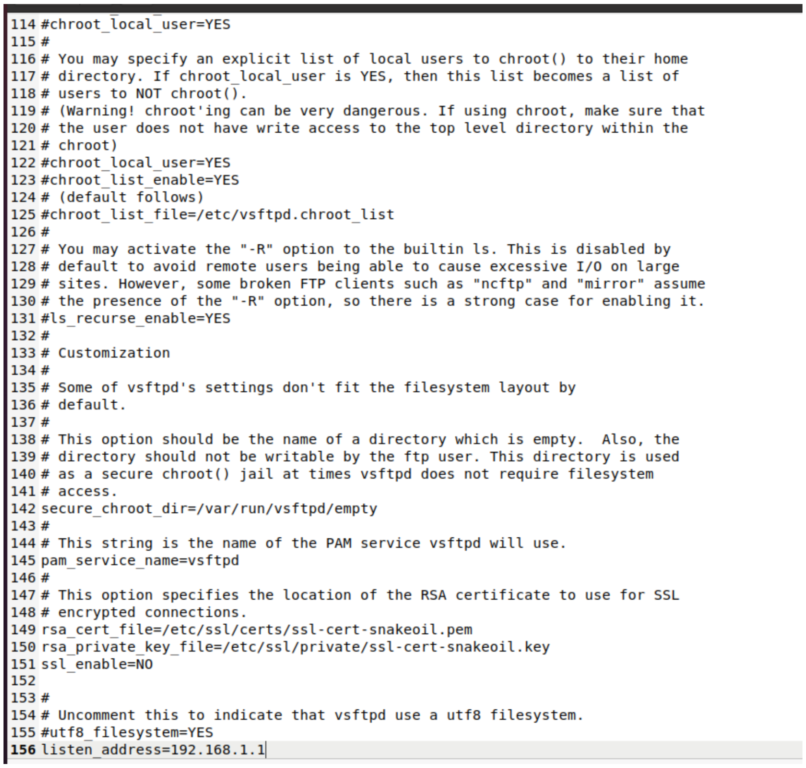
```
#apt -y install vsftpd
```



```
root@server:~# apt -y install vsftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-5.11.0-27-generic linux-hwe-5.11-headers-5.11.0-27 linux-image-5.11.0-27-generic linux-modules-5.11.0-27-generic linux-modules-extra-5.11.0-27-generic
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 33 not upgraded.
Need to get 115 kB of archives.
After this operation, 338 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 vsftpd amd64 3.0.3-12 [115 kB]
Fetched 115 kB in 1s (78.3 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 200459 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-12_amd64.deb ...
Unpacking vsftpd (3.0.3-12) ...
Setting up vsftpd (3.0.3-12) ...
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /lib/systemd/system/vsftpd.service.
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for systemd (245.4-4ubuntu3.14) ...
root@server:~#
```

FTP server is installed correctly. Now we need to configure it.

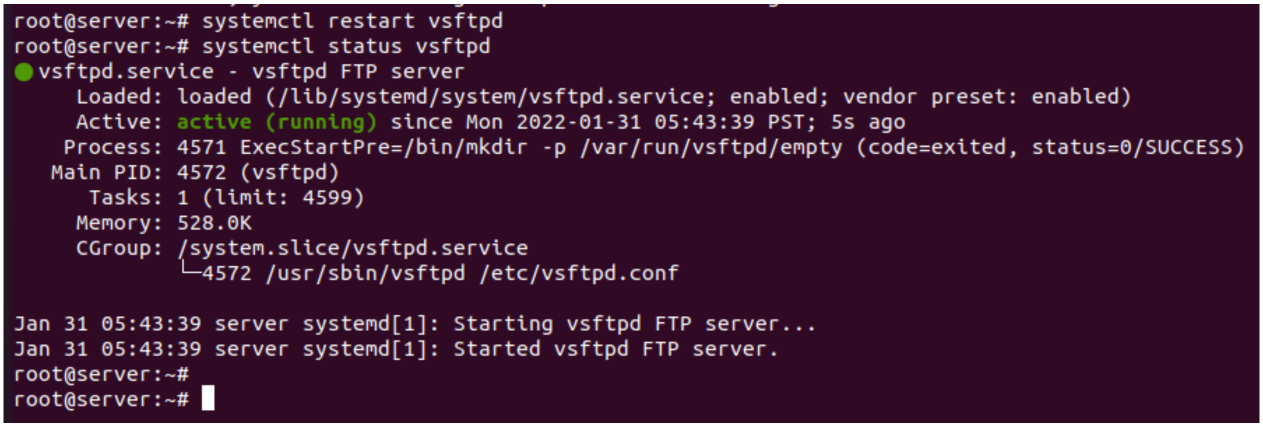
We need to change listen_address to 192.168.1.1 so that the FTP server is only accessible in this subnet.



```
#chroot_local_user=YES
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
#chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# Customization
#
# Some of vsftpd's settings don't fit the filesystem layout by
# default.
#
# This option should be the name of a directory which is empty.  Also, the
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO

#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES
listen_address=192.168.1.1
```

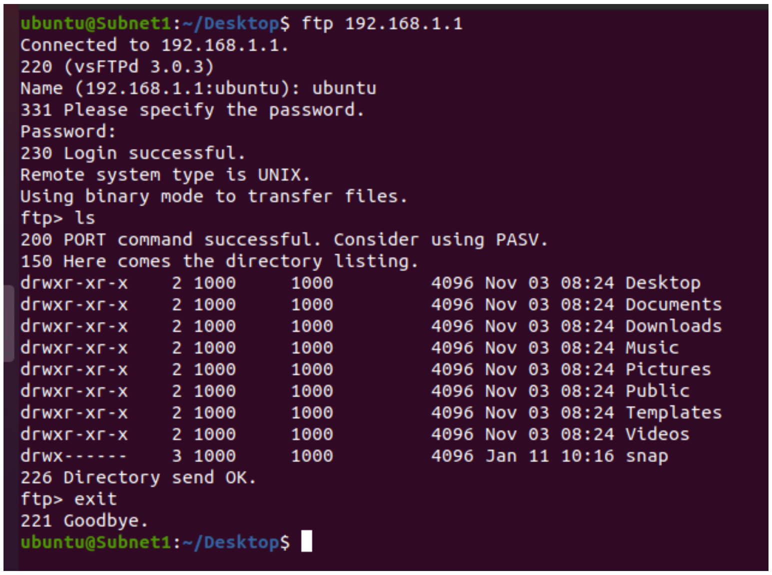
Next we restart the FTP server

```
#systemctl restart vsftpd
```



```
root@server:~# systemctl restart vsftpd
root@server:~# systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2022-01-31 05:43:39 PST; 5s ago
    Process: 4571 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 4572 (vsftpd)
      Tasks: 1 (limit: 4599)
     Memory: 528.0K
     CGroup: /system.slice/vsftpd.service
             └─4572 /usr/sbin/vsftpd /etc/vsftpd.conf

Jan 31 05:43:39 server systemd[1]: Starting vsftpd FTP server...
Jan 31 05:43:39 server systemd[1]: Started vsftpd FTP server.
root@server:~#
root@server:~#
```

Next we verify the service from Subnet 1



```
ubuntu@Subnet1:~/Desktop$ ftp 192.168.1.1
Connected to 192.168.1.1.
220 (vsFTPd 3.0.3)
Name (192.168.1.1:ubuntu): ubuntu
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 1000     1000         4096 Nov 03 08:24 Desktop
drwxr-xr-x    2 1000     1000         4096 Nov 03 08:24 Documents
drwxr-xr-x    2 1000     1000         4096 Nov 03 08:24 Downloads
drwxr-xr-x    2 1000     1000         4096 Nov 03 08:24 Music
drwxr-xr-x    2 1000     1000         4096 Nov 03 08:24 Pictures
drwxr-xr-x    2 1000     1000         4096 Nov 03 08:24 Public
drwxr-xr-x    2 1000     1000         4096 Nov 03 08:24 Templates
drwxr-xr-x    2 1000     1000         4096 Nov 03 08:24 Videos
drwx------    3 1000     1000         4096 Jan 11 10:16 snap
226 Directory send OK.
ftp> exit
221 Goodbye.
ubuntu@Subnet1:~/Desktop$
```

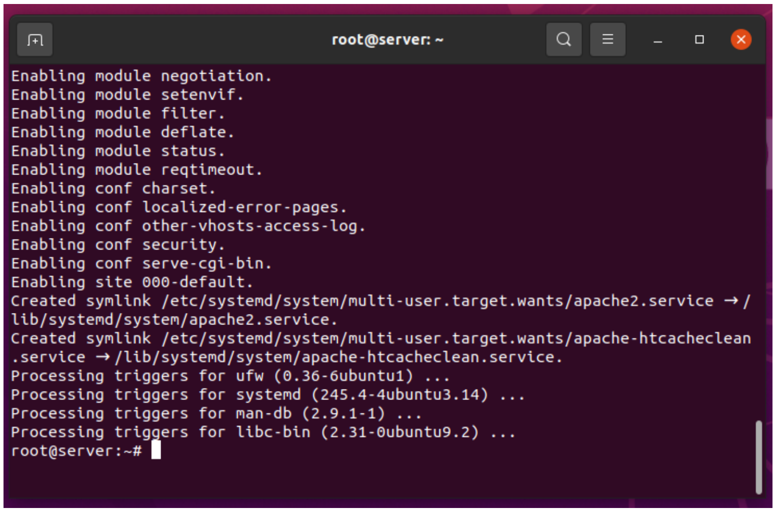
It works!

5. Configure HTTP Server

A web server is used to serve web pages to clients. Apache is a very commonly used web server. We will install and configure Apache as web server.

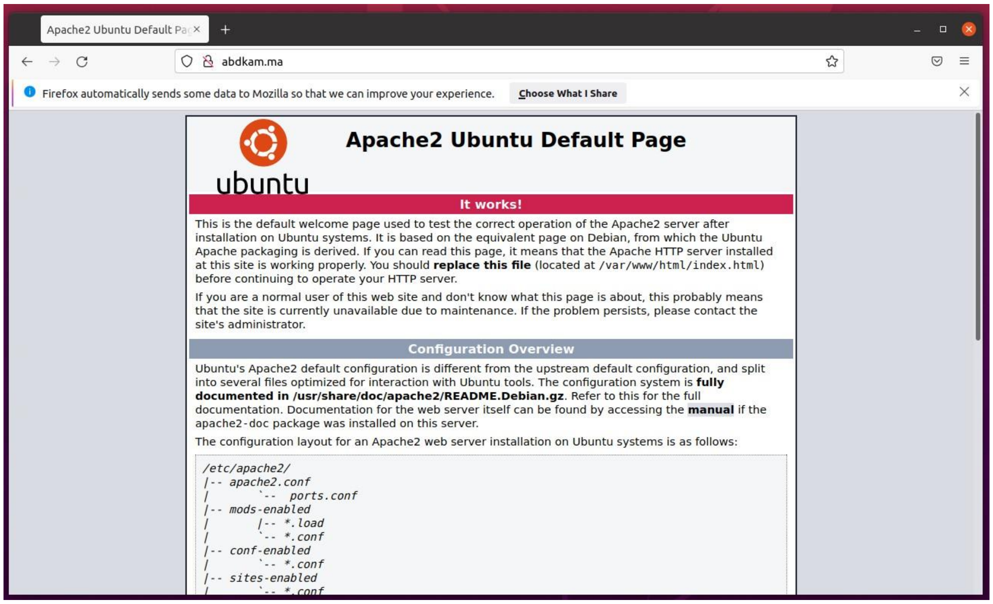
Install HTTPD

```
#apt -y install apache2
```



```
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service →/
lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean
.service →/lib/systemd/system/apache-htcacheclean.service.
Processing triggers for ufw (0.36-6ubuntu1) ...
Processing triggers for systemd (245.4-4ubuntu3.14) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
root@server:~#
```

Next we test if server is running successfully.


Apache2 Ubuntu Default Pa
abdkam.ma
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
ubuntu

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

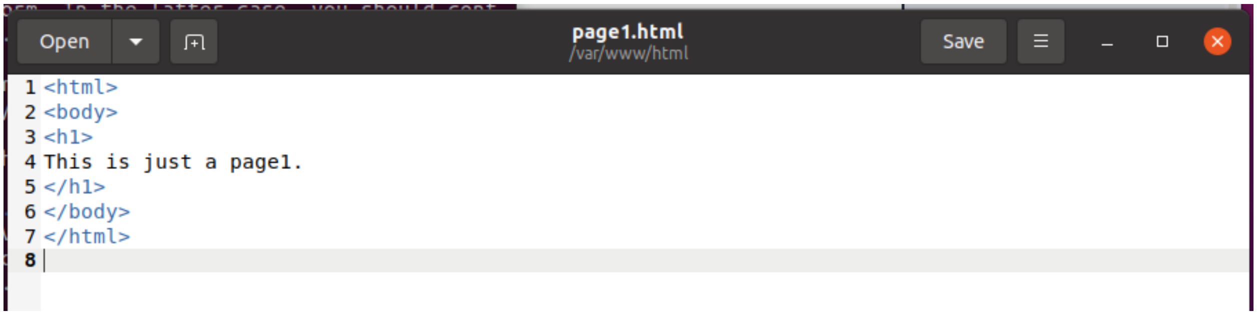
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

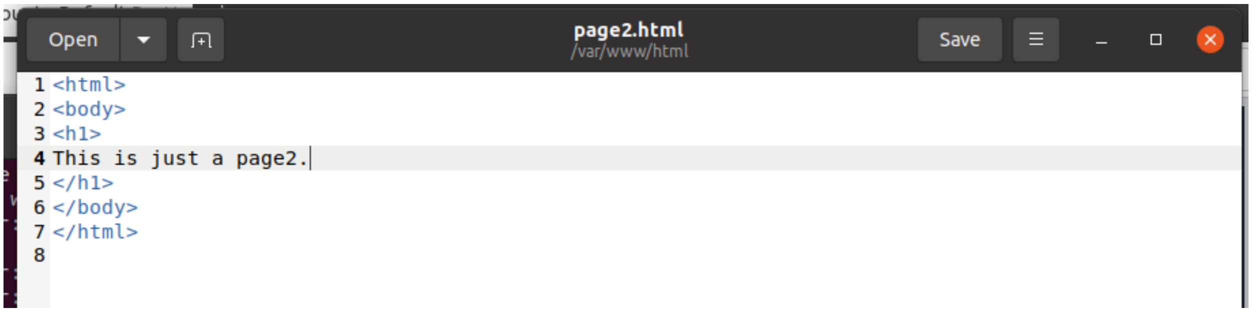
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

We will create two pages in /var/www/html/ as page1.html and page2.html

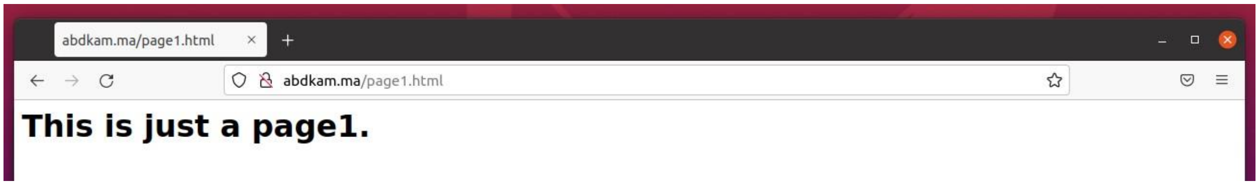


```
<html>
<body>
<h1>
This is just a page1.
</h1>
</body>
</html>

```

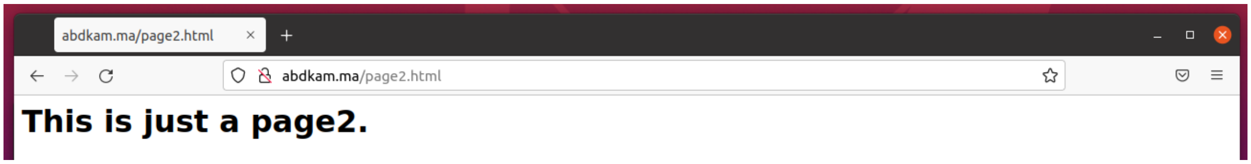


```
<html>
<body>
<h1>
This is just a page2.
</h1>
</body>
</html>

```

Pages are working fine.



This is just a page1.

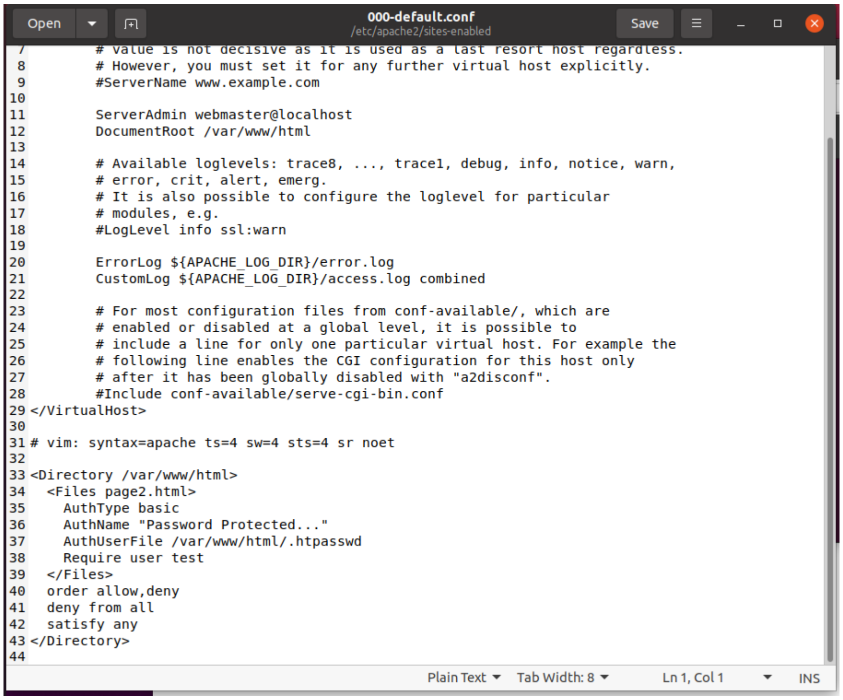


This is just a page2.

Next we will put password protection on page2.

We need to edit /etc/apache2/sites-enabled/000-default.conf and add authentication directives at the end of file

```
<Directory /var/www/html>
  <Files page2.html>
    AuthType basic
    AuthName "Password Protected..."
    AuthUserFile /var/www/html/.htpasswd
    Require user test
  </Files>
  order allow,deny
  deny from all
  satisfy any
</Directory>
```



```
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

<Directory /var/www/html>
  <Files page2.html>
    AuthType basic
    AuthName "Password Protected..."
    AuthUserFile /var/www/html/.htpasswd
    Require user test
  </Files>
  order allow,deny
  deny from all
  satisfy any
</Directory>

```

We will need to create /var/www/html/.htpasswd file which contains usernames and password of authenticated users. For example

```
test:$2y$10$Tw4P6yxCFWbfpuOYYP5ZDefOAvLG6P9jXmTkI2OE3LfhHcmnh9n5K
```

Password is not “test” but its Hashed value.

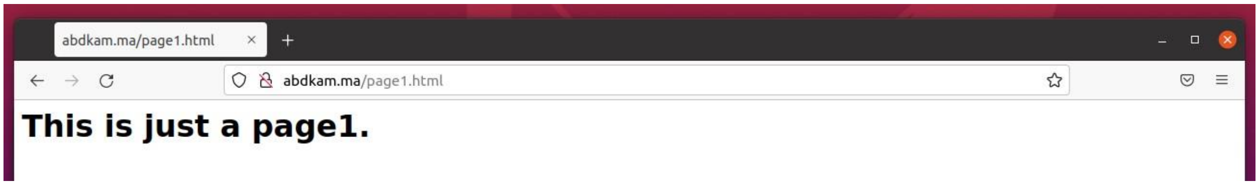
Next We need to enable rewrite Apache module

```
#a2enmod rewrite
```

And finally restart the Apache2 service.

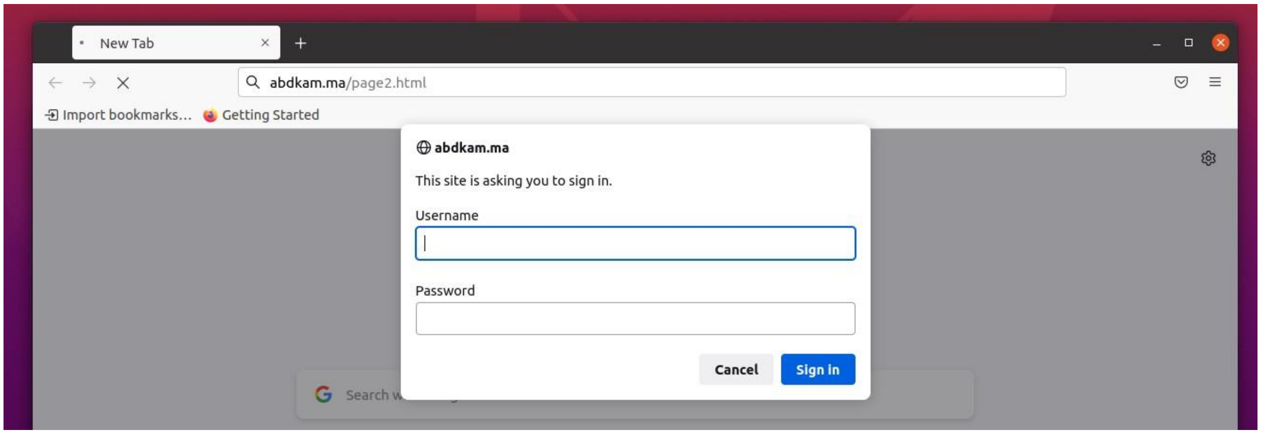
```
#systemctl restart apache2
```

Now we can test the pages. Page1 is accessible without password.



This is just a page1.

But page2 asks for the password



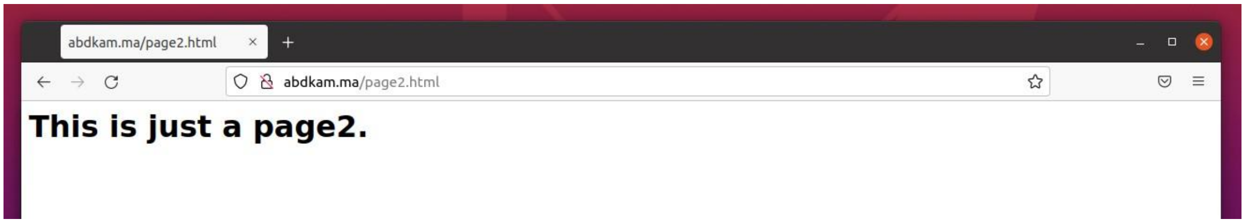
abdkam.ma

This site is asking you to sign in.

Username

Password

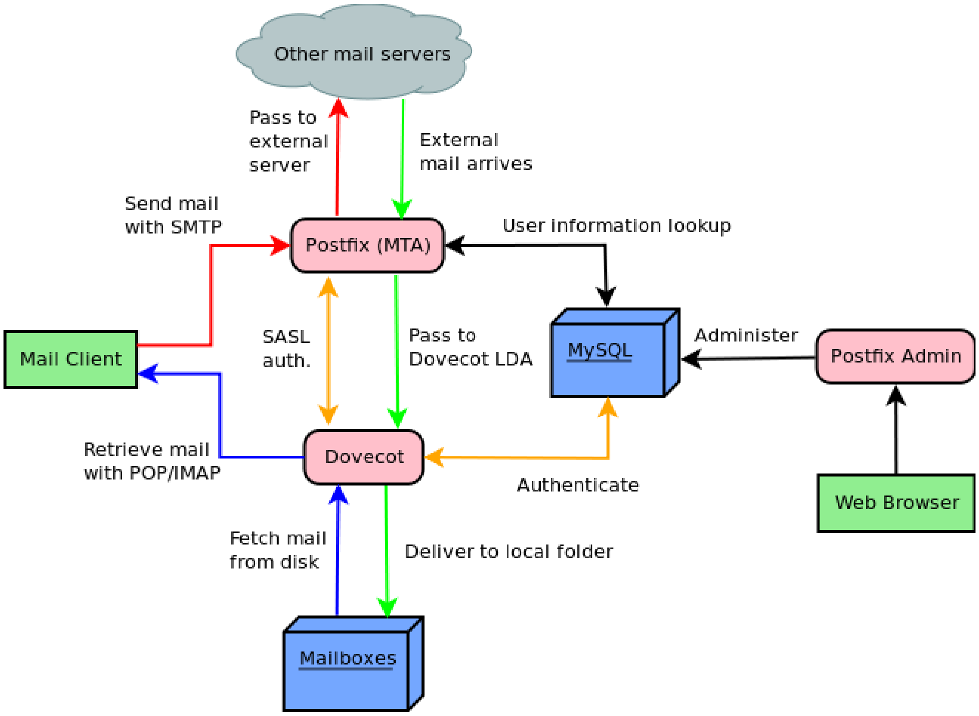
If it is entered correctly the page is displayed.



This is just a page2.

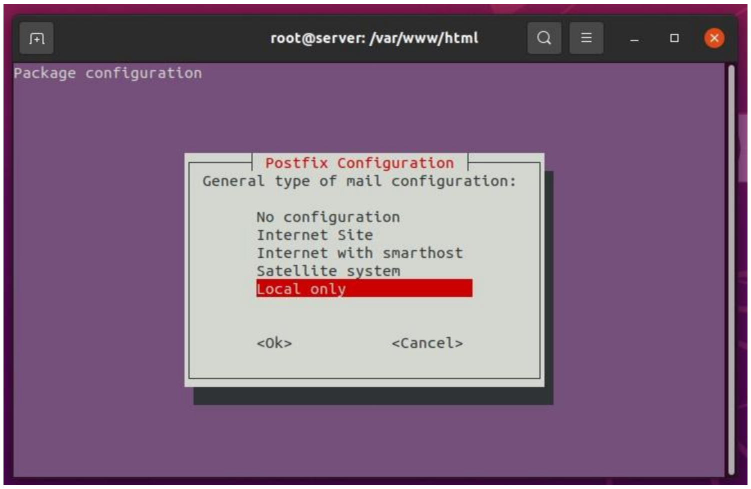
6. Configure Email Server

This diagram shows eco system of an email server. How different components work together to deliver and receive the emails.

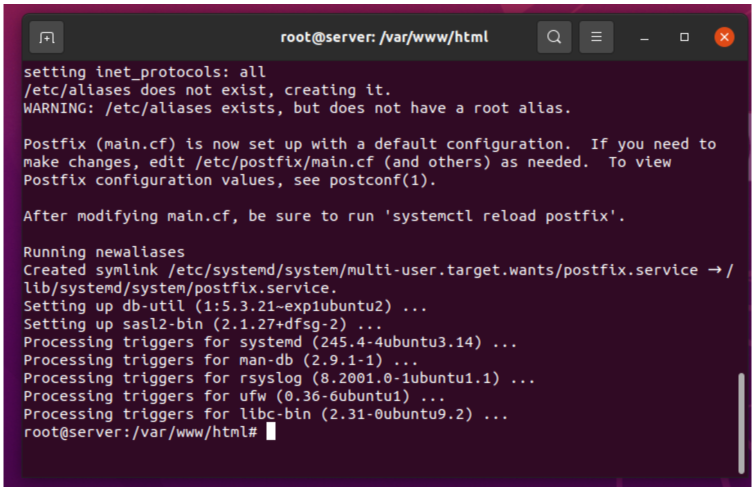


We will configure Postfix as SMTP server.

```
#apt -y install postfix sasl2-bin
```



```
Package configuration

Postfix Configuration
General type of mail configuration:

        No configuration
        Internet Site
        Internet with smarthost
        Satellite system
        Local only

        <Ok>              <Cancel>
```



```
setting inet_protocols: all
/etc/aliases does not exist, creating it.
WARNING: /etc/aliases exists, but does not have a root alias.

Postfix (main.cf) is now set up with a default configuration.  If you need to
make changes, edit /etc/postfix/main.cf (and others) as needed.  To view
Postfix configuration values, see postconf(1).

After modifying main.cf, be sure to run 'systemctl reload postfix'.

Running newaliases
Created symlink /etc/systemd/system/multi-user.target.wants/postfix.service →/
lib/systemd/system/postfix.service.
Setting up db-util (1:5.3.21~exp1ubuntu2) ...
Setting up sasl2-bin (2.1.27+dfsg-2) ...
Processing triggers for systemd (245.4-4ubuntu3.14) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for rsyslog (8.2001.0-1ubuntu1.1) ...
Processing triggers for ufw (0.36-6ubuntu1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
root@server:/var/www/html#
```

Postfix is installed successfully. Next we need to edit the configuration file. We will copy a sample configuration file and edit it according to our requirements.

```
#cp /usr/share/postfix/main.cf.dist /etc/postfix/main.cf
```

Next we edit /etc/postfix/main.cf as

```
mail_owner = postfix
myhostname = ABDKAM.ma
mydomain = ABDKAM.ma
myorigin = $mydomain
inet_interfaces = all
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
local_recipient_maps = unix:passwd.byname  $alias_maps
mynetworks_style = subnet
mynetworks = 192.168.1.0/24, 192.168.2.0/24
alias_maps = hash:/etc/aliases
```

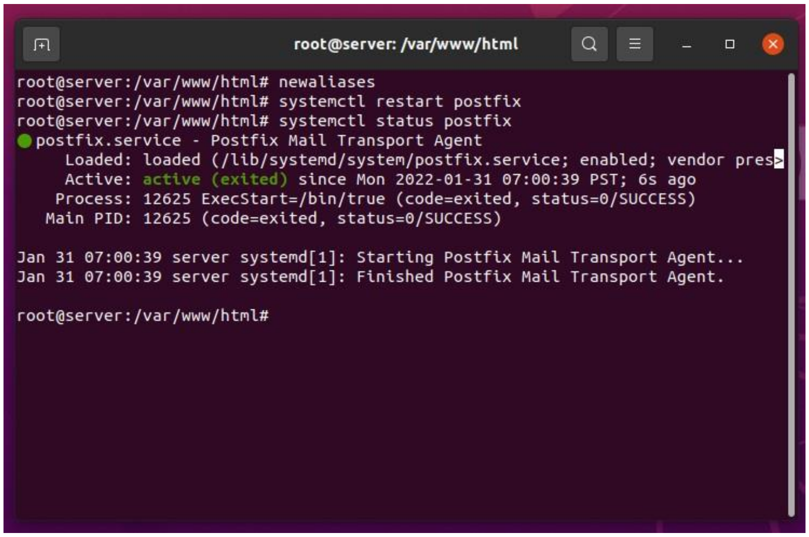
```
alias_database = hash:/etc/aliases
home_mailbox = Maildir/
smtpd_banner = $myhostname ESMTP
sendmail_path = /usr/sbin/postfix
newaliases_path = /usr/bin/newaliases
mailq_path = /usr/bin/mailq
setgid_group = postdrop
#html_directory =
#manpage_directory =
#sample_directory =
#readme_directory =
inet_protocols = ipv4
message_size_limit = 10485760
mailbox_size_limit = 1073741824
# SMTP-Auth settings
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain = $myhostname
smtpd_recipient_restrictions = permit_mynetworks, permit_auth_destination,
permit_sasl_authenticated, reject
```

Next we need to update SMTP aliases

```
#newaliases
```

And finally restart the Postfix service

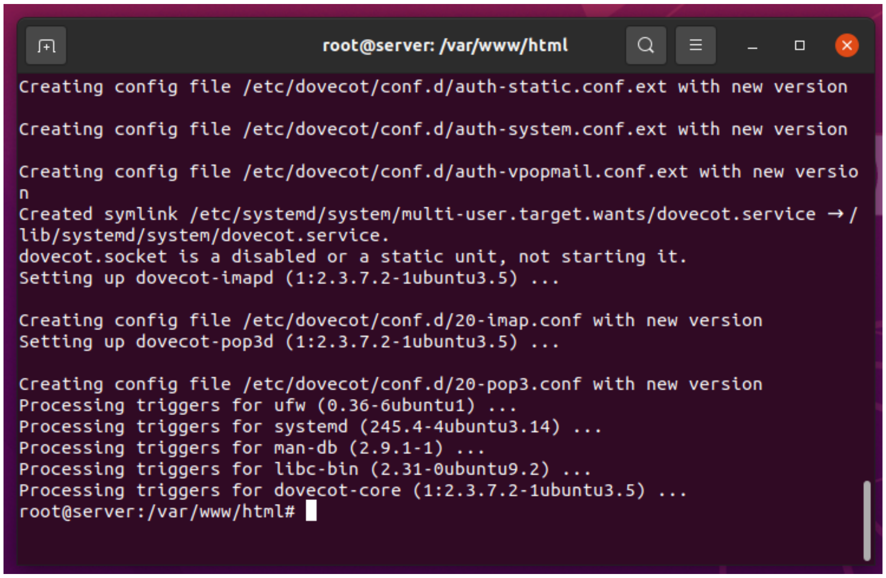
```
#systemctl restart postfix
```



```
root@server:/var/www/html# newaliases
root@server:/var/www/html# systemctl restart postfix
root@server:/var/www/html# systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
     Loaded: loaded (/lib/systemd/system/postfix.service; enabled; vendor pres>
     Active: active (exited) since Mon 2022-01-31 07:00:39 PST; 6s ago
    Process: 12625 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 12625 (code=exited, status=0/SUCCESS)

Jan 31 07:00:39 server systemd[1]: Starting Postfix Mail Transport Agent...
Jan 31 07:00:39 server systemd[1]: Finished Postfix Mail Transport Agent.

root@server:/var/www/html#
```

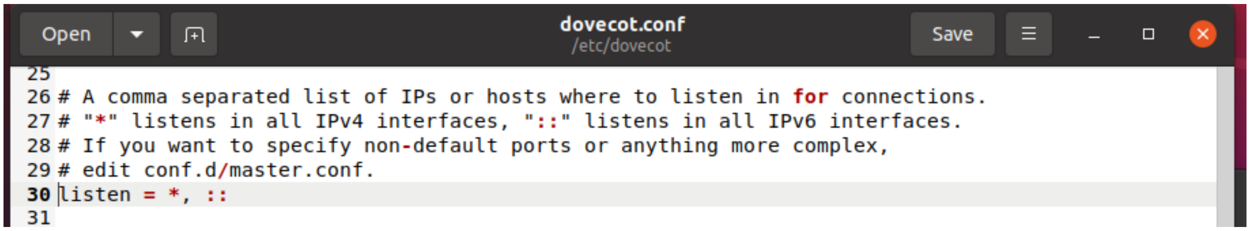
Next we will install and configure Dovecot.

```
#apt -y install dovecot-core dovecot-pop3d dovecot-imapd
```



```
Creating config file /etc/dovecot/conf.d/auth-static.conf.ext with new version

Creating config file /etc/dovecot/conf.d/auth-system.conf.ext with new version

Creating config file /etc/dovecot/conf.d/auth-vpopmail.conf.ext with new versio
n
Created symlink /etc/systemd/system/multi-user.target.wants/dovecot.service →/
lib/systemd/system/dovecot.service.
dovecot.socket is a disabled or a static unit, not starting it.
Setting up dovecot-imapd (1:2.3.7.2-1ubuntu3.5) ...

Creating config file /etc/dovecot/conf.d/20-imap.conf with new version
Setting up dovecot-pop3d (1:2.3.7.2-1ubuntu3.5) ...

Creating config file /etc/dovecot/conf.d/20-pop3.conf with new version
Processing triggers for ufw (0.36-6ubuntu1) ...
Processing triggers for systemd (245.4-4ubuntu3.14) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
Processing triggers for dovecot-core (1:2.3.7.2-1ubuntu3.5) ...
root@server:/var/www/html#
```

Edit /etc/dovecot/dovecot.conf and uncomment line 30



```
25
26 # A comma separated list of IPs or hosts where to listen in for connections.
27 # "*" listens in all IPv4 interfaces, "::" listens in all IPv6 interfaces.
28 # If you want to specify non-default ports or anything more complex,
29 # edit conf.d/master.conf.
30 listen = *, ::
31
```

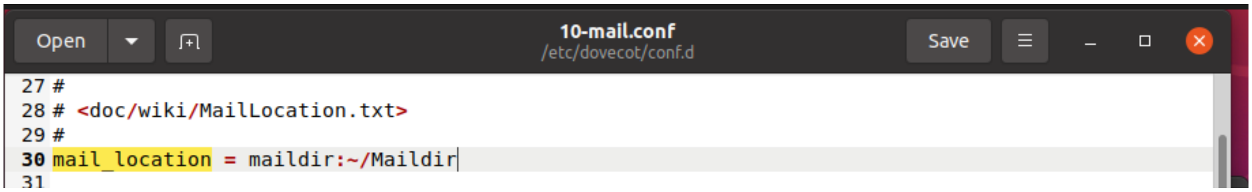
Edit /etc/dovecot/conf.d/10-auth.conf

```
disable_plaintext_auth = no
auth_mechanisms = plain login
```

Edit /etc/dovecot/conf.d/10-mail.conf

as

```
mail_location =maildir:~/Maildir
```

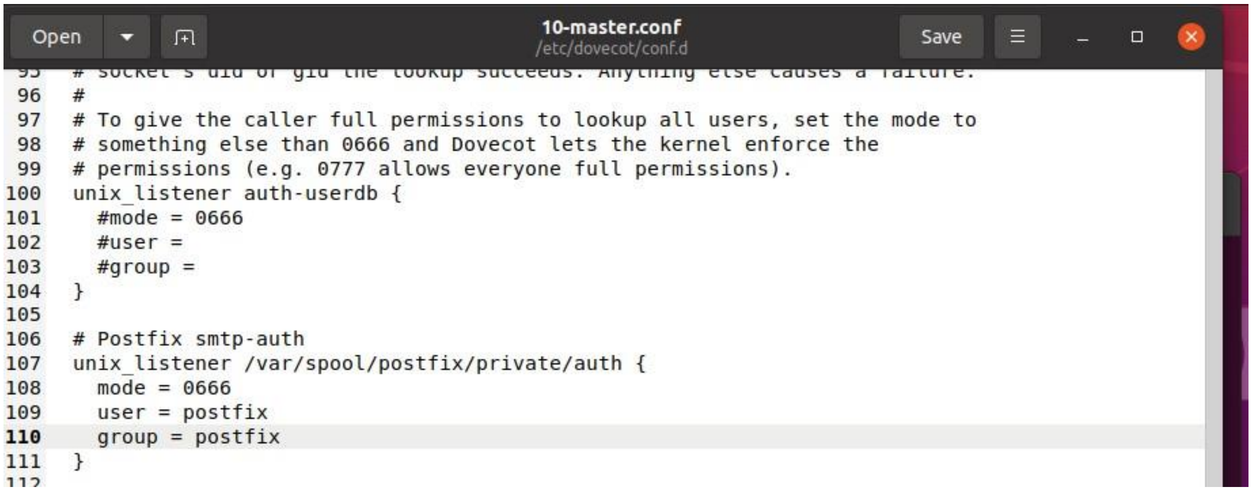


```
#
# <doc/wiki/MailLocation.txt>
#
mail_location = maildir:~/Maildir
```

Edit /etc/dovecot/conf.d/10-master.conf

As

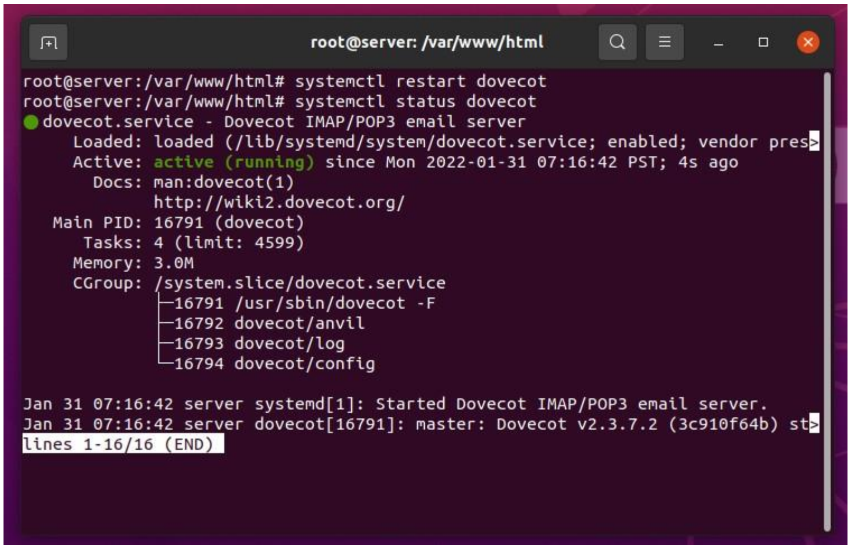
```
  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix
  }
```



```
  # socket's uid or gid the lookup succeeds. Anything else causes a failure.
  #
  # To give the caller full permissions to lookup all users, set the mode to
  # something else than 0666 and Dovecot lets the kernel enforce the
  # permissions (e.g. 0777 allows everyone full permissions).
  unix_listener auth-userdb {
    #mode = 0666
    #user =
    #group =
  }

  # Postfix smtp-auth
  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix
  }
```

Finally restart the Dovecot

```
#systemctl restart dovecot
```



```
root@server:/var/www/html# systemctl restart dovecot
root@server:/var/www/html# systemctl status dovecot
● dovecot.service - Dovecot IMAP/POP3 email server
     Loaded: loaded (/lib/systemd/system/dovecot.service; enabled; vendor pres>
     Active: active (running) since Mon 2022-01-31 07:16:42 PST; 4s ago
       Docs: man:dovecot(1)
             http://wiki2.dovecot.org/
   Main PID: 16791 (dovecot)
      Tasks: 4 (limit: 4599)
     Memory: 3.0M
     CGroup: /system.slice/dovecot.service
             ├─16791 /usr/sbin/dovecot -F
             ├─16792 dovecot/anvil
             ├─16793 dovecot/log
             └─16794 dovecot/config

Jan 31 07:16:42 server systemd[1]: Started Dovecot IMAP/POP3 email server.
Jan 31 07:16:42 server dovecot[16791]: master: Dovecot v2.3.7.2 (3c910f64b) st>
lines 1-16/16 (END)
```

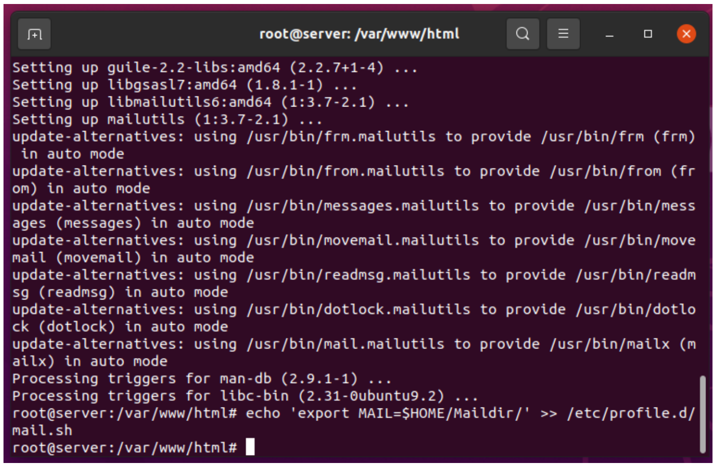
To test the Email server add Mail User Accounts to use Mail Service.

Install mail client

```
# apt -y install mailutils
```

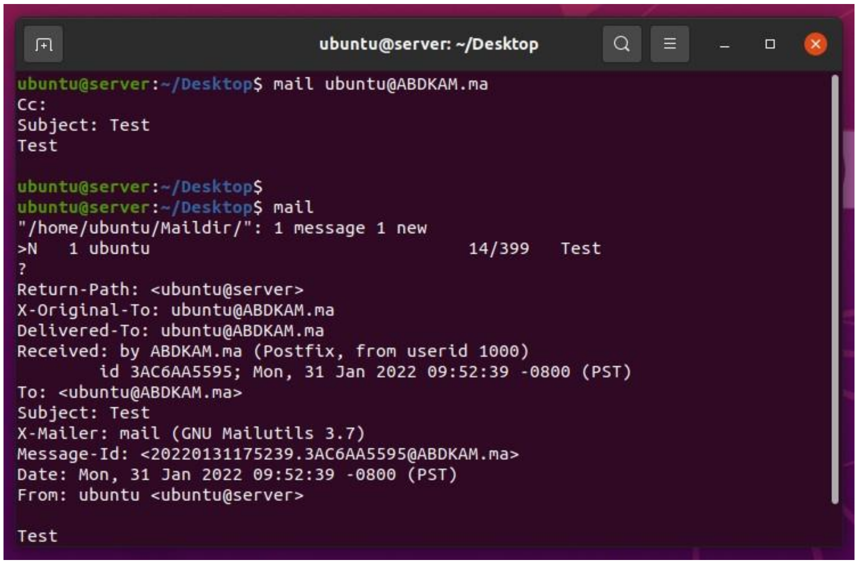
Set environment variables to use Maildir

```
# echo 'export MAIL=$HOME/Maildir/' >> /etc/profile.d/mail.sh
```



```
Setting up guile-2.2-libs:amd64 (2.2.7+1-4) ...
Setting up libgsasl7:amd64 (1.8.1-1) ...
Setting up libmailutils6:amd64 (1:3.7-2.1) ...
Setting up mailutils (1:3.7-2.1) ...
update-alternatives: using /usr/bin/frm.mailutils to provide /usr/bin/frm (frm)
 in auto mode
update-alternatives: using /usr/bin/from.mailutils to provide /usr/bin/from (fr
om) in auto mode
update-alternatives: using /usr/bin/messages.mailutils to provide /usr/bin/mess
ages (messages) in auto mode
update-alternatives: using /usr/bin/movemail.mailutils to provide /usr/bin/move
mail (movemail) in auto mode
update-alternatives: using /usr/bin/readmsg.mailutils to provide /usr/bin/readm
sg (readmsg) in auto mode
update-alternatives: using /usr/bin/dotlock.mailutils to provide /usr/bin/dotlo
ck (dotlock) in auto mode
update-alternatives: using /usr/bin/mail.mailutils to provide /usr/bin/mailx (m
ailx) in auto mode
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
root@server:/var/www/html# echo 'export MAIL=$HOME/Maildir/' >> /etc/profile.d/
mail.sh
root@server:/var/www/html# █
```

We will send a mail to Ubuntu user (itself) to test the configurations.



```
ubuntu@server:~/Desktop$ mail ubuntu@ABDKAM.ma
Cc:
Subject: Test
Test

ubuntu@server:~/Desktop$
ubuntu@server:~/Desktop$ mail
"/home/ubuntu/Maildir/": 1 message 1 new
>N   1 ubuntu                         14/399   Test
?
Return-Path: <ubuntu@server>
X-Original-To: ubuntu@ABDKAM.ma
Delivered-To: ubuntu@ABDKAM.ma
Received: by ABDKAM.ma (Postfix, from userid 1000)
        id 3AC6AA5595; Mon, 31 Jan 2022 09:52:39 -0800 (PST)
To: <ubuntu@ABDKAM.ma>
Subject: Test
X-Mailer: mail (GNU Mailutils 3.7)
Message-Id: <20220131175239.3AC6AA5595@ABDKAM.ma>
Date: Mon, 31 Jan 2022 09:52:39 -0800 (PST)
From: ubuntu <ubuntu@server>

Test
```

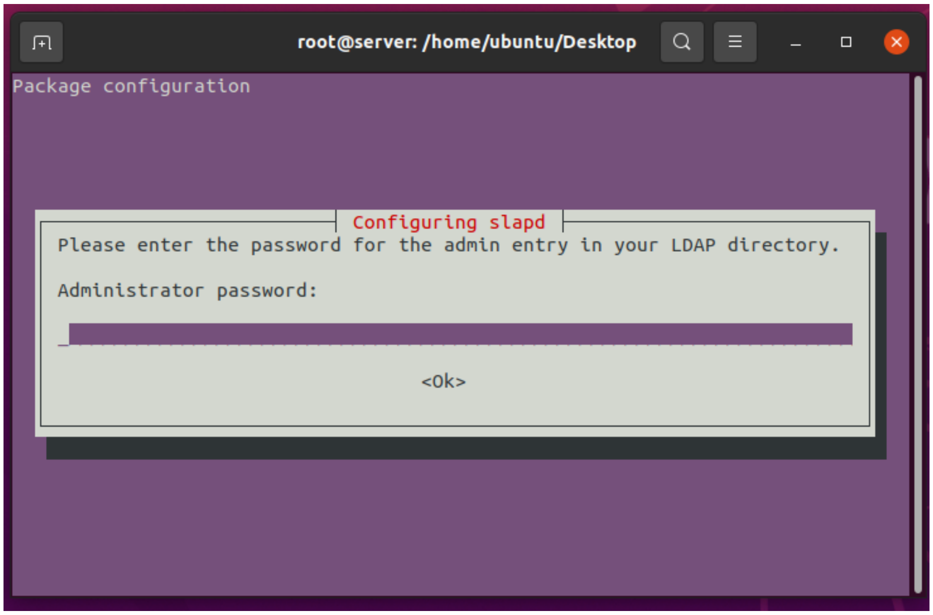
7. Configure LDAP for Centralized Authentication

We need to setup hostname of the server

```
#hostnamectl set-hostname ldap.abdkam.ma
```

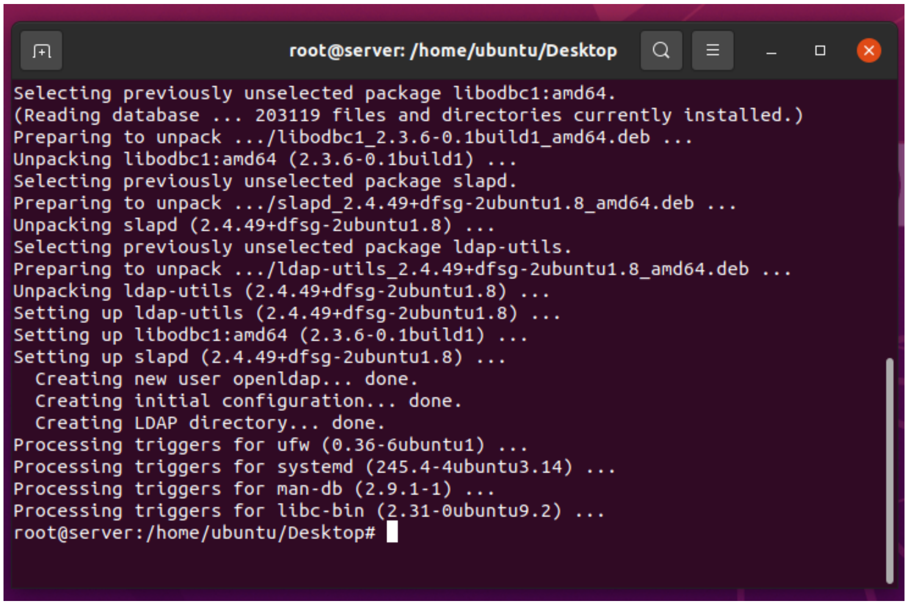
Install OpenLDAP

```
#apt -y install slapd ldap-utils
```



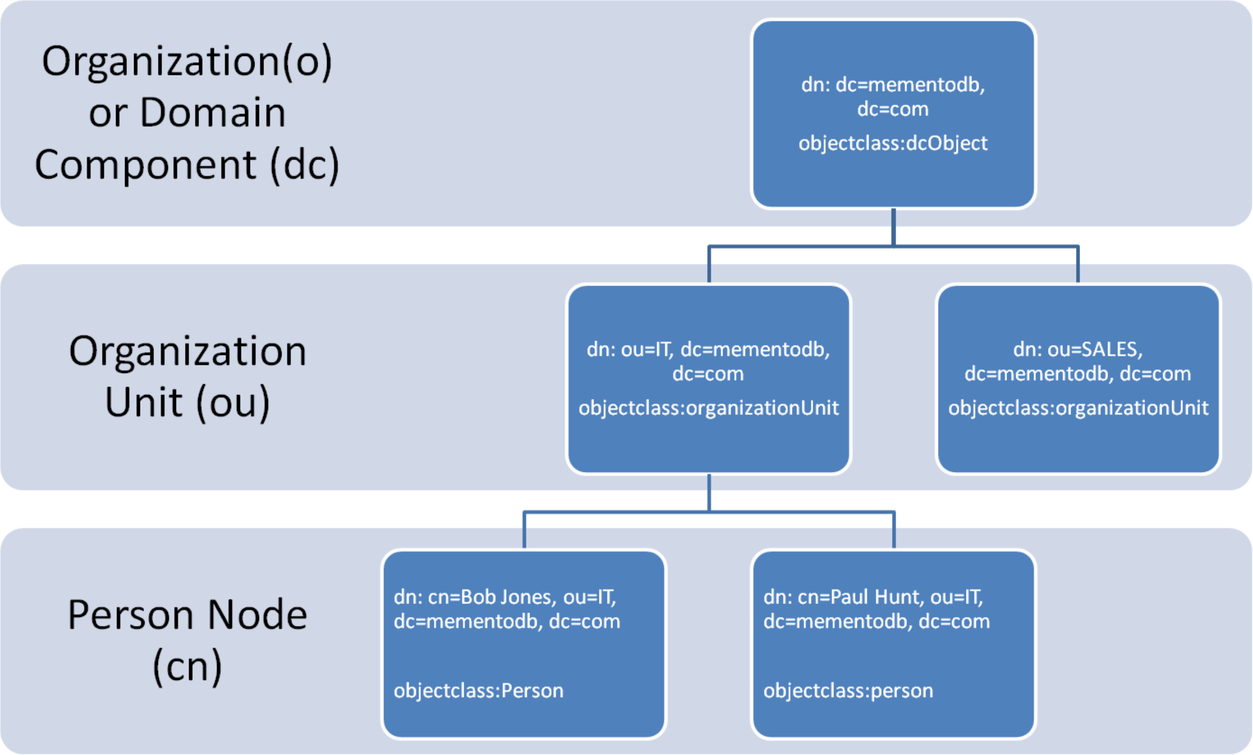
```
Package configuration

                    Configuring slapd
 Please enter the password for the admin entry in your LDAP directory.

 Administrator password:

 _
```

Needs to setup LDAP directory password (“ubuntu@123”).



```
Selecting previously unselected package libodbc1:amd64.
(Reading database ... 203119 files and directories currently installed.)
Preparing to unpack .../libodbc1_2.3.6-0.1build1_amd64.deb ...
Unpacking libodbc1:amd64 (2.3.6-0.1build1) ...
Selecting previously unselected package slapd.
Preparing to unpack .../slapd_2.4.49+dfsg-2ubuntu1.8_amd64.deb ...
Unpacking slapd (2.4.49+dfsg-2ubuntu1.8) ...
Selecting previously unselected package ldap-utils.
Preparing to unpack .../ldap-utils_2.4.49+dfsg-2ubuntu1.8_amd64.deb ...
Unpacking ldap-utils (2.4.49+dfsg-2ubuntu1.8) ...
Setting up ldap-utils (2.4.49+dfsg-2ubuntu1.8) ...
Setting up libodbc1:amd64 (2.3.6-0.1build1) ...
Setting up slapd (2.4.49+dfsg-2ubuntu1.8) ...
  Creating new user openldap... done.
  Creating initial configuration... done.
  Creating LDAP directory... done.
Processing triggers for ufw (0.36-6ubuntu1) ...
Processing triggers for systemd (245.4-4ubuntu3.14) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
root@server:/home/ubuntu/Desktop#
```

OpenLDAP is a directory server which handles an organizations resources in a hierarchal form. For example


Organization(o) or Domain Component (dc)
dn: dc=mementodb, dc=com
objectclass:dcObject
Organization Unit (ou)
dn: ou=IT, dc=mementodb, dc=com
objectclass:organizationUnit
dn: ou=SALES, dc=mementodb, dc=com
objectclass:organizationUnit
Person Node (cn)
dn: cn=Bob Jones, ou=IT, dc=mementodb, dc=com
objectclass:Person
dn: cn=Paul Hunt, ou=IT, dc=mementodb, dc=com
objectclass:person

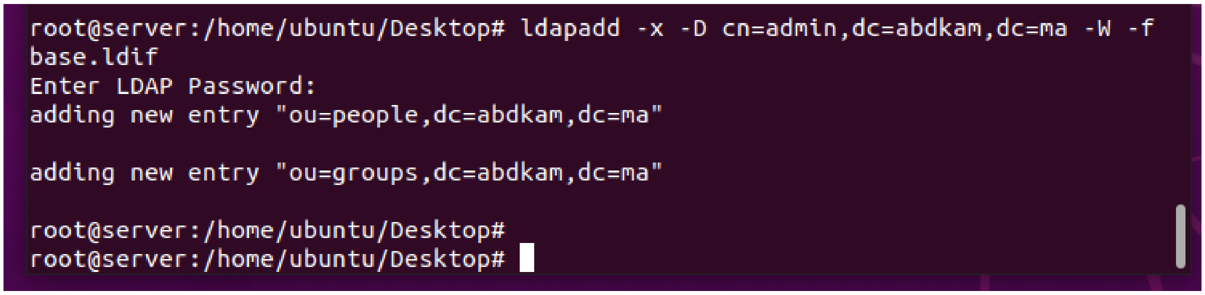
The DN is the name that uniquely identifies an entry in the directory. OU stands for Organization Unit and DC stands for Domain Controller.

We will create two dn by creating a file base.ldif

```
dn: ou=people,dc=abdkam,dc=ma
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=abdkam,dc=ma
objectClass: organizationalUnit
ou: groups
```

Next we need to add these dn's in LDAP Directory

```
# ldapadd -x -D cn=admin,dc=abdkam,dc=ma -W -f base.ldif
```

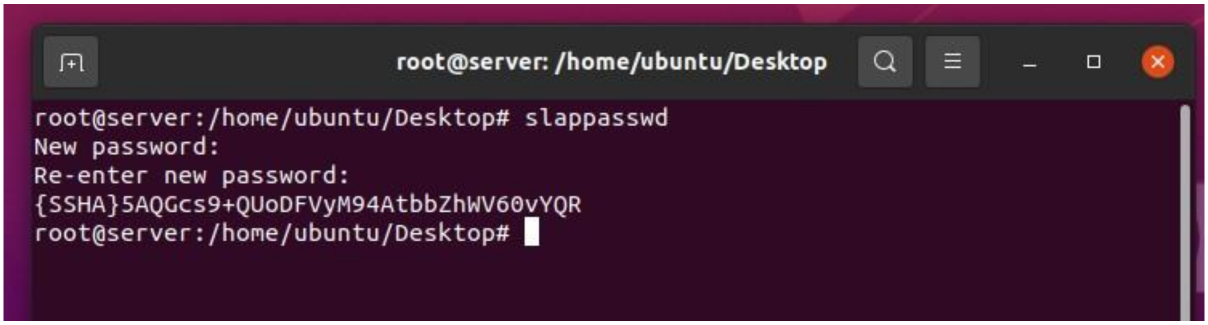


```
root@server:/home/ubuntu/Desktop# ldapadd -x -D cn=admin,dc=abdkam,dc=ma -W -f
base.ldif
Enter LDAP Password:
adding new entry "ou=people,dc=abdkam,dc=ma"

adding new entry "ou=groups,dc=abdkam,dc=ma"

root@server:/home/ubuntu/Desktop#
root@server:/home/ubuntu/Desktop# 
```

To add a new user in the directory we will first create a Hashed password

```
#slappasswd
```

For example for password "test" the Hash value is "{SSHA}5AQGcs9+QUoDFVyM94AtbbZhWV60vYQR"



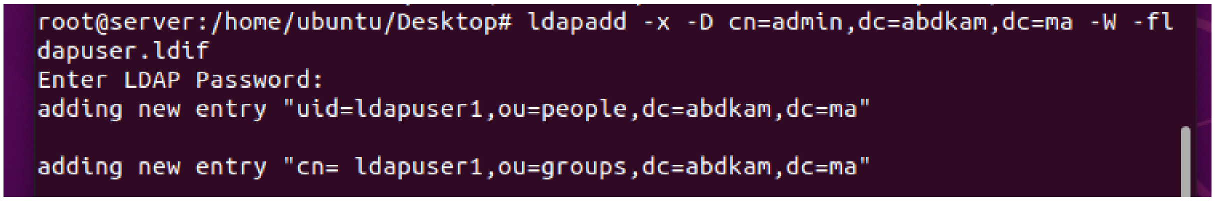
```
root@server:/home/ubuntu/Desktop# slappasswd
New password:
Re-enter new password:
{SSHA}5AQGcs9+QUoDFVyM94AtbbZhWV60vYQR
root@server:/home/ubuntu/Desktop# 
```

Next we need to create a text file ldapuser.ldif, replace password with the one created in previous step.

```
dn: uid=ldapuser1,ou=people,dc=abdkam,dc=ma
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: ldapuser1
sn: ubuntu
userPassword: {SSHA}5AQGcs9+QUoDFVyM94AtbbZhWV60vYQR
loginShell: /bin/bash
uidNumber: 2000
gidNumber: 2000
homeDirectory: /home/ ldapuser1

dn: cn= ldapuser1,ou=groups,dc=abdkam,dc=ma
objectClass: posixGroup
cn: ldapuser1
gidNumber: 2000
memberUid: ldapuser1
```

To add the user, command is

```
#ldapadd -x -D cn=admin, dc=abdkam,dc=ma -W -f ldapuser.ldif
```



```
root@server:/home/ubuntu/Desktop# ldapadd -x -D cn=admin,dc=abdkam,dc=ma -W -fl
dapuser.ldif
Enter LDAP Password:
adding new entry "uid=ldapuser1,ou=people,dc=abdkam,dc=ma"

adding new entry "cn= ldapuser1,ou=groups,dc=abdkam,dc=ma"
```

8- Enhancements (security):

As personal effort to make this project rendering more valuable, we gave an important portion of our time to the network security, for this purpose, we thought about securing one of the html pages with a password, as well as the “slappaswd” for LDAP administrator, you may have noticed that all the passwords used during the process are stored with their hashed values more precisely using the {SSHA} encryption.

Hashing is a one way encryption. Meaning, you cannot get the original text back from the hash. Now in information security, passwords are recommended to be stored in a hashed format so applications/systems can verify if the correct password is entered without them storing your password. This makes it harder to steal. Because what you don't have has less likelihood of being stolen. Let us try to explain with an example. You made an account on Facebook. Now Facebook doesn't need to ever tell your password back to you or anyone else. They just need to verify whether the password you entered is correct or not. How can they do it? Obviously, they can save your password and whenever you enter the password, they can match it with the one they have already. But, that password can be copied, stolen or a number of bad things can happen to it. So they use hash. Let us assume you set your password to "eidia". Hashing, or running it through a hashing algorithm, will give you a random seeming string (let us assume) "euromed". Facebook immediately forgets "eidia" and stores only "euromed". Now everytime you enter password "eidia", they hash it, Match if the result is "euromed", and grant or deny you access. As it is a one way encryption, "euromed" can not be decrypted to"eidia". So even if someone hacks facebook and get the password file dump they will be stuck with random looking hashes. And Facebook itself cannot use your password.

Bibliography :

MAIL Postfix : https://www.aktifperunding.com/news/detail?id=9;

http://www.postfix.org/postconf.5.html;

DNS server : https://doc.ubuntu-fr.org/bind9;

FTP : https://phoenixnap.com/kb/install-ftp-server-on-ubuntu-vsftpd;

HTTP : https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-20-04;

HTTP authentication directives :

https://docs.nginx.com/nginx/admin-guide/security-controls/configuring-http-basic-authentication/;