The Problem with Linux Servers

by Isa Raffee

Table of Contents

Configuring Network Services on Vector Linux 5.8 and Ubuntu Jaunty

Viewing the Network Interface

On the Ubuntu host, type:
root@ismail-laptop:~# ifconfig eth0

```
eth0      Link encap:Ethernet  HWaddr 00:16:d3:43:12:02

          inet6 addr: fe80::216:d3ff:fe43:1202/64 Scope:Link

          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

          RX packets:0 errors:0 dropped:0 overruns:0 frame:0

          TX packets:9 errors:0 dropped:0 overruns:0 carrier:0

          collisions:0 txqueuelen:1000

          RX bytes:0 (0.0 B)  TX bytes:1494 (1.4 KB)

          Interrupt:20 Base address:0xa000
```

Setting IP address on Ubuntu

To set a temporary IP address on Ubuntu type

ifconfig eth0 172.16.0.2 netmask 255.255.0.0 broadcast 172.16.255.255 up

Verify the network connections.

ifconfig eth0

eth0 Link encap:Ethernet HWaddr 00:16:d3:43:12:02

inet addr:172.16.0.2 Bcast:172.16.255.255 Mask:255.255.0.0

inet6 addr: fe80::216:d3ff:fe43:1202/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
<output truncated for brevity>

Test the configuration by pinging its IP address

root@ismail-laptop:~# ping 172.16.0.2

PING 172.16.0.2 (172.16.0.2) 56(84) bytes of data.

64 bytes from 172.16.0.2: icmp_seq=1 ttl=64 time=0.054 ms

64 bytes from 172.16.0.2: icmp_seq=2 ttl=64 time=0.039 ms

^C

--- 172.16.0.2 ping statistics ---

2 packets transmitted, 2 received, 0% packet loss, time 999ms

rtt min/avg/max/mdev = 0.039/0.046/0.054/0.010 ms

This IP address will be gone once you reboot the machine. To set IP address permanently follow these steps.

Setting IP address on Ubuntu via Configuration file

If the Ubuntu Server installer has set your server to use DHCP, you will want to change it to a static IP address so that people can actually use it.

Changing this setting without a GUI will require some text editing, but that's classic linux, right?

Let's open up the /etc/network/interfaces file. I'm going to use vi, but you can choose a different editor

sudo vi /etc/network/interfaces

For the primary interface, which is usually eth0, you will see these lines:

auto eth0
iface eth0 inet dhcp

As you can see, it's using DHCP right now. We are going to change dhcp to static, and then there are a number of options that should be added below it. Obviously you'd customize this to your network.

```
auto eth0
iface eth0 inet static
        address 192.168.1.100
        netmask 255.255.255.0
        network 192.168.1.0
        broadcast 192.168.1.255
        gateway 192.168.1.1
```

The auto directive identifies the network interface to be configured, in this case the loopback adapter as noted by the lo label.

`Auto lo`

Without the auto directive, the specifiied interface is not activated the next time you type the /etc/init.d/networking restart or the ifup -a commands.

`iface lo inet loopback`

The auto lo directive also need the directive shown above. The iface directuve applies Ipv4 networking as defined by the inet directive (Ipv6 would be configured with inet6), along with the loopback address, to the loopback adapter lo.

If you are using DNS to resolve IP addresses to machine names, you may want to add the DNS server (name servers) by editing the resolv.conf file:

sudo vi /etc/resolv.conf

On the line ‘nameserver xxx.xxx.xxx.xxx’ replace the x with the IP of your name server.

Now we’ll just need to restart the networking components:

sudo /etc/init.d/networking restart

Setting IP address on Vector Linux

On Vector Linux, you need to edit the network interface file for eth0

#vi /etc/rc.d/rc.inet1

```
## The settings
DEVICE='eth0'
DHCP='no'
IPADDR='172.16.0.1'
NETMASK='255.255.0.0'
GATEWAY='172.16.0.2'
PROBE='no'
```

Save and quit. Then you need to restart the network services.

```
root:# ./rc.inet1 stop
Stopping network eth0 ...

root:# ./rc.inet1 start
```

Ping the Vector Linux

root@ismail-laptop:~# ping 172.16.0.1

PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.

64 bytes from 172.16.0.1: icmp_seq=1 ttl=64 time=1.24 ms

64 bytes from 172.16.0.1: icmp_seq=2 ttl=64 time=0.185 ms

FTP from Vector Linux to Ubuntu Jaunty

On Ubuntu
root@ismail-laptop:~# ps -ef|grep ftp

proftpd 2930 1 0 21:05 ? 00:00:00 proftpd: (accepting connections)

root 7544 5961 0 21:48 pts/2 00:00:00 grep ftp

This shows that ftp server, proftpd is ready.

On Vector

root:# ftp 172.16.0.2
Connected to 172.16.0.2.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:172.16.0.2]
Name (172.16.0.2:root): root
331 Password required for root
Password:
230 User root logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful

Configuring Telnet Server in Ubuntu Jaunty

Telnet is run as a Super Server
root@ismail-laptop:/etc/init.d# cd /etc/xinetd.d
root@ismail-laptop:/etc/xinetd.d# ls -lrt

total 24

-rw-r--r-- 1 root root 727 2008-07-28 20:26 time

-rw-r--r-- 1 root root 580 2008-07-28 20:26 echo

-rw-r--r-- 1 root root 549 2008-07-28 20:26 discard

-rw-r--r-- 1 root root 660 2008-07-28 20:26 daytime

-rw-r--r-- 1 root root 798 2008-07-28 20:26 chargen

-rw-r--r-- 1 root root 392 2010-02-06 03:07 telnetd

If there is no telnetd file, create one like this
service telnetd

```
{

        disable         = no
        type            = INTERNAL
        socket_type     = stream
        protocol        = tcp
        user            = root
        wait            = no
}
```

After that restart the xinetd service

root@ismail-laptop:/etc# cd init.d/

root@ismail-laptop:/etc/init.d# ./xinetd

Usage: /etc/init.d/xinetd {start|stop|reload|force-reload|restart|status}

root@ismail-laptop:/etc/init.d# ./xinetd restart

Now from Vector, telnet to Ubuntu

root:# telnet 172.16.0.2
Trying 172.16.0.2...
Connected to 172.16.0.2.
Escape character is '^]'.
Ubuntu 9.04
ismail-laptop login: root

Password:
Last login: Sun Feb 14 16:23:21 SGT 2010 from 172.16.0.1 on pts/2
Linux ismail-laptop 2.6.28-13-generic #45-Ubuntu SMP Tue Jun 30 19:49:51 UTC 2009 i686
root@ismail-laptop:~#

Extra
You can check the status of the network interface by typing the following command:

NFS

Vector Linux is configured as the NFS server

Check that the NFS package is install

root:# slapt-get --installed | grep nfs
nfs-utils-1.0.10-i486-3 [inst=yes]: nfs-utils (Network File System daemons and utilities)

root:# slapt-get --installed | grep portmap
portmap-5.0-i486-3 [inst=yes]: portmap (a daemon to manage RPC connections)

Check where to start the NFS server daemon
root:# cd /etc/rc.d
vector://etc/rc.d
root:# ./rc.nfsd

Important Notes

If you are thinking of making Vector Linux as the ssh or NFS server, you must stop the firewall service by typing:
#cd /etc/rc.d
#./rc.firewall stop

Otherwise your ssh or NFS share will not be accessible from remote hosts. I wrote a rc script which will stop the firewall services, before the server starts the NFS and SSH. Follow the steps, and I remind you that this is for Vector linux.

root:# cd /etc/rc.d

vector://etc/rc.d

root:# cd rc4.d/

vector://etc/rc.d/rc4.d

root:# ls

K49ifplugd@ S50ifplugd@ S76tembokapi* S99cups*

K76firewall@ S70firewall@ S77nfsd* S99sshd*

vector://etc/rc.d/rc4.d

The rc script is called S76tembokapi. Make sure the script name begins with letter S (means start) and that the number is after the firewall script S70FIREWALL. That's why I chose number 76; after the firewall start and before the nfsd and sshd scripts started.

Create a directory to be shared

root:# cd /root/Desktop/
vector:/~/Desktop
root:# mkdir TopHits
vector:/~/Desktop
root:# vi somefile.txt

Write some things to the file and save.

Let's check if the nfsd service is running on the NFS server (the Vector Linux)

root:# ps -eflgrep nfs

root 3417 3372 0 08:00 pts/3 00:00:00 grep nfs

It shows that nfs server is not running

But before we start it let's edit the /etc/exports file

Edit the /etc/exports

Add a line that looks like this:
/root/Desktop/TopHits 172.16.0.2/255.255.0.0(rw,no_root_squash)

The IP address here is the NFS client, which is my case is the Ubuntu Jaunty.

After that run the following command to export the folders.

root:# exportfs -a -v

exportfs: /etc/exports [1]: Neither 'subtree_check' or 'no_subtree_check' specified for export "172.16.0.2/255.255.0.0:/root/Desktop/TopHits".

  Assuming default behaviour ('subtree_check').

  NOTE: this default will change with nfs-utils version 1.1.0

exporting 172.16.0.2/255.255.0.0:/root/Desktop/TopHits

Make sure you have the /root/Desktop/TopHIts created on your ssh server, otherwise you are not sharing anything.

Now let's restart the NFS server:

Before that we also note that for NFS to work, you need the rpc portmap and nfs service running. Now we already know how to check for nfs service. To check for the rpc portmap type:

vector://etc

root:# ps -ef|grep portmap

root 3423 3372 0 08:06 pts/3 00:00:00 grep portmap

vector://etc

root:# ps -ef|grep rpc

root 3425 3372 0 08:06 pts/3 00:00:00 grep rpc

Ok let's start the NFS server on the Vector Linux

root:# cd /etc/rc.d

vector://etc/rc.d

root:# ./rc.nfsd start

Starting RPC portmapper: /sbin/rpc.portmap

Starting RPC kernel lockd process: /sbin/rpc.lockd

Starting RPC NSM (Network Status Monitor): /sbin/rpc.statd

Starting NFS server daemons:

  /usr/sbin/exportfs -r

exportfs: /etc/exports [1]: Neither 'subtree_check' or 'no_subtree_check' specified for export "172.16.0.2/255.255.0.0:/root/Desktop/TopHits".

  Assuming default behaviour ('subtree_check').

  NOTE: this default will change with nfs-utils version 1.1.0

  /usr/sbin/rpc.rquotad

  /usr/sbin/rpc.nfsd 8

  /usr/sbin/rpc.mountd

Check for the necessary services:

```
root:# ps -ef|grep rpc

bin      3453     1  0 08:08 ?        00:00:00 /sbin/rpc.portmap

root     3462     1  0 08:08 ?        00:00:00 /sbin/rpc.statd

root     3465     1  0 08:08 ?        00:00:00 /usr/sbin/rpc.rquotad

root     3478     6  0 08:08 ?        00:00:00 [rpciod/0]

root     3479     1  0 08:08 ?        00:00:00 /usr/sbin/rpc.mountd

root     3496     1  0 08:10 ?        00:00:00 /usr/sbin/rpc.rquotad

root     3499     1  0 08:10 ?        00:00:00 /usr/sbin/rpc.mountd

root     3501  3372  0 08:10 pts/3    00:00:00 grep rpc
```

```
root:# ps -eflgrep nfs

root     3467     6  0 08:08 ?        00:00:00 [nfsd4]

root     3468     1  0 08:08 ?        00:00:00 [nfsd]

root     3469     1  0 08:08 ?        00:00:00 [nfsd]

root     3470     1  0 08:08 ?        00:00:00 [nfsd]
```

```
root     3471     1  0 08:08 ?        00:00:00 [nfsd]

root     3472     1  0 08:08 ?        00:00:00 [nfsd]

root     3473     1  0 08:08 ?        00:00:00 [nfsd]

root     3474     1  0 08:08 ?        00:00:00 [nfsd]

root     3475     1  0 08:08 ?        00:00:00 [nfsd]

root     3505  3372  0 08:11 pts/3    00:00:00 grep nfs
```

rpcinfo utility

The rpcinfo utility displays information about programs registered with portmap and makes RPC calls to programs to see if they are alive

Type the command:

```
# rpcinfo -p ubuntu.example.com
```

You can replace the hostname with IP address or localhost.

Use the -u option to display a list of versions of a daemon registered on a host

```
# rpcinfo -u ubuntu.example.com nfs

program 100003 version 2 ready and waiting

program 100003 version 3 ready and waiting

program 100003 version 4 ready and waiting
```

Now let's configure the NFS client on the Ubuntu Jaunty

Firstly, make a directory at the client

mkdir /mnt/share

Next mount the shareon the NFS client and in my case it's Ubuntu Jaunty:

mount -t nfs 172.16.0.1:/root/Desktop/TopHits /mnt/share

Check to see if it is mounted

root@ismail-laptop:~# mount

mount

/dev/sda1 on / type ext3 (rw,relatime,errors=remount-ro)

tmpfs on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)

proc on /proc type proc (rw,noexec,nosuid,nodev)

<*lines truncated for brevity*>
172.16.0.1:/root/Desktop/TopHits on /mnt/share type nfs (rw,addr=172.16.0.1)

Look at the last entry. It shows that the NFS share is mounted.

Let's edit the file from the NFS client

cd /mnt/share/

root@ismail-laptop:/mnt/share# ls

somefile.txt

root@ismail-laptop:/mnt/share# vi somefile.txt
hello world

hi earthlings! Greetings from mars.

You can also check that the file is updated on the NFS server

To unmount the share on the NFS client, type:

#umount /mnt/share

Note:
Based on several tests, NFS server service in Vector Linux will not start unless you have NFS share entries in your /etc/export file. If the file is blank, nfs services will not even work.

Issues on UIDs of NFS Server and Client

On the NFS client
root@ismail-laptop:~# grep ismail /etc/passwd

ismail:x:1000:1000:ismail,,,:/home/ismail:/bin/bash

On the NFS server

root:# grep ismail /etc/passwd

ismail:x:1001:100::/home/ismail:

The user has different UID on the server and at the client. Let's see if this affect the file sharing

On the nfs client
mount -t nfs 172.16.0.1:/home/ismail /home/ismail

#mount
172.16.0.1:/home/ismail on /home/ismail type nfs (rw,addr=172.16.0.1)

Access and try edit the files

On the client the user can view the file but unable to edit the file

SO now I will try to change the UIDs to 1001

On the client, I have to make some adjustment to the user who currently has UID 1001
usermod -u 1005 idris

Now I assigned the user ismail UID with 1001

root@ismail-laptop:/home/ismail# grep ismail /etc/passwd

ismail:x:1001:1000:ismail,,,:/home/ismail:/bin/bash

Now the UID is the same let's try to edit the shared file

ismail@ismail-laptop:~$ vi ismailfile
good job

yes I need to change the UID to edit the file

Yes the user can now edit the shared file.

Making NFS share called “portsmouth”

On the NFS server and in my case Vector Linux

root:# mkdir /portsmouth
root:# chmod 1777 /portsmouth/

root:# ls -ld /portsmouth/

drwxrwxrwt 2 root root 4096 2010-02-24 12:11 /portsmouth//

Now the portsmouth directory only allow users to edit their own file. Furthermore users cannot delete files that do not belong to them.

On the NFS server, again mine is Vecotr Linux, set up the directories to be shared.

root:# vi /etc/exports
/portsmouth 172.16.0.2/255.255.0.0(rw,root_squash)

Then type:

root:# exportfs -v -a

exporting 172.16.0.2/255.255.0.0:/root/Desktop/TopHits

exporting 172.16.0.2/255.255.0.0:/home/ismail

exporting 172.16.0.2/255.255.0.0:/portsmouth

Restart the NFS server

root:# ./rc.nfsd start

Starting RPC portmapper: /sbin/rpc.portmap

Starting RPC kernel lockd process: /sbin/rpc.lockd

Starting RPC NSM (Network Status Monitor): /sbin/rpc.statd

Starting NFS server daemons:

/usr/sbin/exportfs -r

/usr/sbin/rpc.rquotad

/usr/sbin/rpc.nfsd 8

/usr/sbin/rpc.mountd

Note that in my case I do not need to restart the portmap service

Now let's configure NFS on Ubuntu. I will make Ubuntu as the NFS server and the NFS client.
The portmap script is found at /etc/rc.d/init.d
/./portmap

On the NFS client, make directory so that users will access their files.
root@ismail-laptop:/mnt# mkdir portsmouth

root@ismail-laptop:/mnt# ll portsmouth/

total 0

root@ismail-laptop:/mnt# ll -d portsmouth/

drwxr-xr-x 2 root root 4096 2010-02-24 14:41 portsmouth/

Now mount the share
root@ismail-laptop:~# mount -t nfs 172.16.0.1:/portsmouth /mnt/portsmouth/

root@ismail-laptop:~# mount

/dev/sda1 on / type ext3 (rw,relatime,errors=remount-ro)

<information truncated for brevity>
172.16.0.1:/portsmouth on /mnt/portsmouth type nfs (rw,addr=172.16.0.1)

Now try to create files and try to delete other users' files
root@ismail-laptop:~# su - idris

idris@ismail-laptop:~$ pwd

/home/idris

idris@ismail-laptop:~$ cd /mnt/portsmouth/

idris@ismail-laptop:/mnt/portsmouth$ ls -l

total 8

-rw-r--r-- 1 ismail ismail 5 2010-02-24 15:13 ismail_recipes

-rw-r--r-- 1 ismail users 5 2010-02-24 15:11 ismail_secrets

idris@ismail-laptop:/mnt/portsmouth$ rm ismail_recipes

rm: remove write-protected regular file `ismail_recipes'? y

rm: cannot remove `ismail_recipes': Operation not permitted

User idris cannot remove ismail's files

Note
The sticky bit is set on the NFS server, not the client

This is what it looks like on the NFS server
root:# ls -ld portsmouth/

drwxrwxrwt 2 root root 4096 2010-02-24 15:13 portsmouth//

And after you mount on the client, it appears that the sticky bit is set automatically by NFS

idris@ismail-laptop:~$ ls -ld /mnt/portsmouth/

drwxrwxrwt 2 root root 4096 2010-02-24 15:13 /mnt/portsmouth/

Important Notes

When you mount an NFS share on the client, the client thought that he is creating files on the local machine, but the truth is that the files he created all reside in the NFS server. Once you unmount the NFS share, the client files are not on his or her home directory. They are found on the NFS server.

Configuring NFS on Ubuntu Jaunty

Check if the packages are install

root@ismail-laptop:/etc# dpkg --list | grep nfs

root@ismail-laptop:/etc# dpkg --list | grep portmap

If they are not install, then type:

apt-get install nfs-kernel-server nfs-common portmap

Creating config file /etc/default/nfs-kernel-server with new version

```
 * Starting NFS common utilities                    [ OK ]
 * Exporting directories for NFS kernel daemon...          [ OK ]
 * Starting NFS kernel daemon                       [ OK ]
```

Processing triggers for libc6 ...

ldconfig deferred processing now taking place

Check if nfs and portmap are running:

```
root@ismail-laptop:~# ps -ef|grep nfs
root     30523     2  0 19:01 ?        00:00:00 [nfsd4]
root     30524     2  0 19:01 ?        00:00:00 [nfsd]
root     30525     2  0 19:01 ?        00:00:00 [nfsd]
root     30526     2  0 19:01 ?        00:00:00 [nfsd]
root     30527     2  0 19:01 ?        00:00:00 [nfsd]
root     30528     2  0 19:01 ?        00:00:00 [nfsd]
root     30529     2  0 19:01 ?        00:00:00 [nfsd]
root     30530     2  0 19:01 ?        00:00:00 [nfsd]
root     30531     2  0 19:01 ?        00:00:00 [nfsd]

root     30552 23453  0 19:01 pts/2    00:00:00 grep nfs
root@ismail-laptop:~# ps -ef|grep portmap
daemon   30114     1  0 19:01 ?        00:00:00 /sbin/portmap
root     30581 23453  0 19:01 pts/2    00:00:00 grep portmap
```

Edit the /etc/exports file and add the following

/root/Desktop/nfsshare 172.16.0.1/255.255.0.0(rw)
The IP address is the NFS client or clients. But in this case, my nfs client is the nfs server itself.

This is because Vector was unable to participate as it is down for maintenance. Thus I have to make Ubuntu as the NFS client and server.

Restart the nfsd service

```
root@ismail-laptop:/etc/init.d# ./nfs-kernel-server restart

 * Stopping NFS kernel daemon                                    [ OK ]

 * Unexporting directories for NFS kernel daemon...                    [ OK ]

 * Exporting directories for NFS kernel daemon...                          exportfs: /etc/exports [1]:
Neither 'subtree_check' or 'no_subtree_check' specified for export
"172.16.0.0/255.255.0.0:/root/Desktop/nfsshare".

  Assuming default behaviour ('no_subtree_check').

  NOTE: this default has changed since nfs-utils version 1.0.x



                                                                [ OK ]

 * Starting NFS kernel daemon                                    [ OK ]

root@ismail-laptop:/etc/init.d#
```

Mounting the NFS Share on the NFS Client

To mount the NFS share on the client , type:

```
root@ismail-laptop:~# mount -t nfs 172.16.0.1:/root/Desktop/nfsshare/ /mnt/share
```

Type mount to check that it is mounted

```
# mount


/dev/sda1 on / type ext3 (rw,relatime,errors=remount-ro)


<output truncated for brevity>
172.16.0.1:/root/Desktop/nfsshare/ on /mnt/share type nfs (rw,addr=172.16.0.1)
```

It shows here that the NFS share is mounted on the client at the /mnt/share directory.

You can access the NFS share by typing:

root@ismail-laptop:~# cd /mnt/share/

root@ismail-laptop:/mnt/share# ls

freeRecipex.txt

Edit the file

vi freeRecipex.txt

hello world

we are from Mars, Grretings!

Check that the file contents are the same at /root/Desktop/nfsshare/ directory. This is at the NFS server.

root@ismail-laptop:~# cd /root/Desktop/nfsshare/

root@ismail-laptop:~/Desktop/nfsshare# less freeRecipex.txt

Yes, the contents are the same.

Auto Mount NFS Shares on Clients

To auto mount the NFS share when clients boot-up, you will need to edit the /etc/fstab file

root@ismail-laptop:~# cd /etc

root@ismail-laptop:/etc# cp fstab fstab.bak

root@ismail-laptop:/etc# vi fstab

In my case I have included the following lines:

172.16.0.1:/home/ismail /home/ismail nfs defaults 0 0

172.16.0.1:/portsmouth /mnt/portsmouth nfs defaults 0 0

Reboot the NFS client and check that the NFS shares are mounted

Note:
To mount the partitions that are in the /etc/fstab, you can also type:

#mount -a

All partitions will be mounted

Starting NFS Server Automatically in Vector Linux

In my case the NFS server upon booting did not start automatically. I have to start it manually each time I booted up my server. To automatically start up NFS server service, you will need to edit the /etc/rc.d scripts.

On Vector Linux

Go to /etc/rc.d/rc4.d

root:# cd /etc/rc.d/rc4.d/

Create a script called S77nfsd (You can give it any name, but make sure the script name starts with Capital S, to indicate start of script. Script names that start with letter K means stopping or killing of service.)

The contents of my S77nfsd script are as follow:

root:# more S77nfsd

#!/bin/bash

cd /etc/rc.d

./rc.nfsd start

Save and quit, and remember to chmod to ugo+x

#chmod ugo+x S77nfsd

What we actually do is to place the script at runlevel 4 and the script will in this case start the NFS server service when the system reaches runlevel 4. Try to see if this works by rebooting the system.

In my case after I rebooted the system, NFS server service was started automatically. Do a ps -ef| grep nfs to check this.

Note:

In Vector Linux the sshd service is also not started by default when you booted up the system. You can also include a script which started the sshd service in the /etc/rc.d/rc4.d directory. You can call this script S99sshd and the contents of the script may look like the following:

```
#!/bin/bash

cd /etc/rc.d

./rc.sshd start
```

Again chmod ugo+x S99sshd so that the system can execute the script. That's it. Try to reboot the system and when you have boot up, you can see that sshd service has started.

And please remember that in Vector Linux even though you started the SSH server service, you may at times unable to ssh to your Vector Linux SSH server. This is because of the firewall service. In my case I stop the firewall service to use ssh. Type:

```
#cd /etc/rc.d/
#./rc.firewall stop
```

Configuring DHCP server in Ubuntu Jaunty

DHCP server: Ubuntu
DHCP client: Vector linux

On DHCP server, install DHCP package

```
root@ismail-laptop:~# apt-get install dhcp3-server

<output truncated for brevity>
Setting up dhcp3-common (3.1.1-5ubuntu8.2) ...

Setting up dhcp3-client (3.1.1-5ubuntu8.2) ...

 * Reloading AppArmor profiles ...                                        [ OK ]
```

Setting up dhcp3-server (3.1.1-5ubuntu8.2) ...

Generating /etc/default/dhcp3-server...

 * Reloading AppArmor profiles ... [OK]

 * Starting DHCP server dhcpd3 * check syslog for diagnostics.

[fail]

invoke-rc.d: initscript dhcp3-server, action "start" failed.

To check if the dhcp packages are installed, type:

dpkg --list | grep dhcp

ii dhcp3-client 3.1.1-5ubuntu8.2 DHCP client

ii dhcp3-common 3.1.1-5ubuntu8.2 common files used by all the dhcp3* packages

ii dhcp3-server 3.1.1-5ubuntu8.2 DHCP server for automatic IP address assignm

Next on the DHCP server edit the configuration file. But before that I could never strees enough on making a backup copy of the original file.

root@ismail-laptop:~# cd /etc/dhcp3/

root@ismail-laptop:/etc/dhcp3# ls

dhclient.conf dhclient-enter-hooks.d dhclient-exit-hooks.d dhcpd.conf

root@ismail-laptop:/etc/dhcp3# cp -p dhcpd.conf dhcpd.conf.bak

Now edit the file and include the following lines:;

#i added the following

subnet 72.16.0.0 netmask 255.255.0.0 {

range 172.16.0.10 172.16.0.20;

}

The above entries said that to assign IP address in the range of 172.16.0.10 to 172.16.0.20 to a host (dhcp client).

Check that the DHCP server is running. And if changes were done on the configuration file, you have to restart the dhcpd service.

cd /etc/init.d/

./dhcp3-server status

Status of DHCP server: dhcpd3 is not running.

Start the dhcpd server,
./dhcp3-server start

- Starting DHCP server dhcpd3 [OK]

Configuring the dhcp client (Vector LInux)

Edit the network settings of the dhcp client. Change the DHCP value to "yes"

root:# cd /etc/rc.d
vector://etc/rc.d
root:# vi rc.inet1

The settings
DEVICE='eth0'
DHCP='yes'
IPADDR='172.16.0.1'
NETMASK='255.255.0.0'
GATEWAY='172.16.0.2'
PROBE='no'

Save and quit. Then you need to restart the network services.

root:# ./rc.inet1 stop
Stopping network eth0 ...

root:# ./rc.inet1 start

```
Starting network eth0 using a DHCP server...
dhcpcd: MAC address = 00:11:85:77:d0:a7
dhcpcd: your IP address = 172.16.0.10
eth0      Link encap:Ethernet  HWaddr 00:11:85:77:D0:A7
          inet addr:172.16.0.10  Bcast:172.16.255.255  Mask:255.255.0.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:671 (671.0 b)  TX bytes:594 (594.0 b)
          Interrupt:20
```

From the output, it shows that the dhcp client was assign the IP address of 172.16.0.10. Remember that we have assigned a range of IP addresses on the DHCP server i.e. IP addresses from 172.16.0.10 to 172.16.0.20.

Verify this IP address and check that you can now ping the DHCP server, and that the DHCP server can ping its clients.

```
root:# ping 172.16.0.2
PING 172.16.0.2 (172.16.0.2) 56(84) bytes of data.
64 bytes from 172.16.0.2: icmp_seq=1 ttl=64 time=0.213 ms
64 bytes from 172.16.0.2: icmp_seq=2 ttl=64 time=0.204 ms
```

Yes the dhcp client can ping the DHCP server

Try ping the dhcp client from the DHCP server

```
# ping 172.16.0.10

PING 172.16.0.10 (172.16.0.10) 56(84) bytes of data.

64 bytes from 172.16.0.10: icmp_seq=1 ttl=64 time=1.26 ms

64 bytes from 172.16.0.10: icmp_seq=2 ttl=64 time=0.202 ms
```

Yes this shows that the dhcp client can ping the DHCP server.

Next we are going to assign IP address based on a specificHardware MAC address.

Assgining IP address with a specific MAC address

Suppose our dhcp client has a MAC address of 00:11:85:77:d0:a7 and we want to fixed its IP address as 172.16.0.99. These are the steps:

Firstly on the DHCP server, edit the dhcpd.conf and add the following lines.

```
# cd /etc/dhcp3/

root@ismail-laptop:/etc/dhcp3# ls

dhclient.conf  dhclient-enter-hooks.d  dhclient-exit-hooks.d  dhcpd.conf  dhcpd.conf.bak


root@ismail-laptop:/etc/dhcp3# vi dhcpd.conf
#I add this

subnet 172.16.0.0 netmask 255.255.0.0 {

  range 172.16.0.07 172.16.0.99;}



host examplehost {

hardware ethernet 00:11:85:77:d0:a7;

fixed-address 172.16.0.99;

}
```

Save and quit. Then restart the dhcpd service.

You can also run the following command

```
# service dhcp3-server restart

 * Stopping DHCP server dhcpd3                                          [ OK ]

 * Starting DHCP server dhcpd3                                           [OK].
```

On the dhcp client, in my case the Vector Linux, type:

```
#/etc/rc.d/./rc.inet1 stop

#/etc/rc.d/./rc.inet1 start
```

if it fail to obtain IP address then type:

#dhcpcd

This is the DHCP client daemon. Then check the IP address. It should now assign the IP address based on the MAC address.

ifconfig eth0

eth0 Link encap:Ethernet HWaddr 00:11:85:77:D0:A7

inet addr:172.16.0.15 Bcast:172.16.255.255 Mask:255.255.0.0

UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1

Note

You can include the DNS server in the DHCP server

```
option domain-name-servers 172.16.0.2;
```

Exploring ssh between Vector Linux and Ubuntu

ssh server: Ubuntu

ssh client: Vector linux

Configure IP address on Ubuntu
ifconfig eth0 172.16.0.2 netmask 255.255.0.0 broadcast 172.16.255.255 up

Configure IP address on Vector
Go to /etc/rc.d
vi rc.inet1
Change the IP address as required
Quit and save
Restart the network interface
/etc/rc.d/./rc.inet1 restart

Verify it
ifconfig eth0

Check that both hosts can ping to each other

Check sshd running on Ubuntu

root@ismail-laptop:/etc# ps -ef|grep sshd

root 3457 1 0 14:22 ? 00:00:00 /usr/sbin/sshd

root 8430 7360 0 14:57 pts/1 00:00:00 grep sshd

Now ssh from Vector to Ubuntu

#ssh 172.16.0.2

After providing the password you should be able to ssh to Ubuntu SSH server.

Note:
In case you are unable to ssh into the Vector Linux ssh server, you can also try tostop the firewall service like this:

root:# cd /etc/rc.d

vector://etc/rc.d

root:# ./rc.firewall stop

Loading kernel modules ...

error: "net.ipv4.tcp_syncookies" is an unknown key

net.ipv4.conf.all.rp_filter = 1

net.ipv4.icmp_echo_ignore_broadcasts = 1

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.all.secure_redirects = 1

net.ipv4.conf.all.log_martians = 1

Flushing Tables ...

Firewall completely flushed! Now running with no firewall.

Then try to ssh again. You should be able to ssh to the remote host.

Using Secure Copy

To secure copy from Vector (the ssh client) to Ubuntu (the ssh server)

root:# scp forubuntu.doc ismail@172.16.0.2:/home/ismail

ismail@172.16.0.2's password:

forubuntu.doc 100% 5805 5.7KB/s 00:00

Note:Please refer to the documentation for Configuring or Exploring SSH to learn about how to configure ssh client and ssh server

Note:

Let's say you received the message below:

```
root:# scp tbr.txt 172.16.0.2:/root/Desktop/

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
26:3a:2e:97:51:e3:09:52:88:57:a6:bf:79:35:e3:87.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending key in /root/.ssh/known_hosts:2
RSA host key for 172.16.0.2 has changed and you have requested strict checking.H
ost key verification failed.
```

This happen when you reconfigure your SSH server. To solve this simply delete the 2nd line as suggested in your ssh client machine and not on the ssh server.

SSH Without Password

On the local host type:
#ssh-keygen -t dsa

In my case ssh without password only works with dsa and not rsa.

root:# ssh-keygen -t dsa

Generating public/private dsa key pair.

Enter file in which to save the key (/root/.ssh/id_dsa):

/root/.ssh/id_dsa already exists.

Overwrite (y/n)? y

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /root/.ssh/id_dsa.

Your public key has been saved in /root/.ssh/id_dsa.pub.

The key fingerprint is:

d7:57:23:0f:f2:23:77:4f:ca:49:d5:22:e0:ed:1d:8f root@vector.linux.net

It will produce two files in the ~/.ssh directory; the public key and the private key. You will need to copy the public key to the remote host that you wish to remotely logon without password.

-rw-r--r-- 1 root root 611 2010-03-21 22:46 id_dsa.pub

-rw------- 1 root root 668 2010-03-21 22:46 id_dsa

You can use scp to copy the public key to the remote host. You can copy it to the /tmp direcory or anywhere.

Copy the public key to the remote host
root:# scp id_dsa.pub 172.16.0.2:/tmp

root@172.16.0.2's password:

id_dsa.pub 100% 611 0.6KB/s 00:00

Next you will need to add the contents of the public key to the remote host's ~/.ssh/authorized_keys file.

You will need to ssh first into the remote host. And you will need to provide the password (later you will not have to provide)

root:# ssh 172.16.0.2 -l root

root@172.16.0.2's password:

Once on the remote host, type:

cd /tmp

cat id_dsa.pub >> /root/.ssh/authorized_keys

If the .ssh directory on the remote host does not exist. You will need to creat it and chmod it to 700.

And don't forget to remove the public key at the /tmp directory

cd /tmp

rm id_dsa.pub

Exit the ssh by typing

root@ubuntu:/tmp# exit

logout

Connection to 172.16.0.2 closed.

Now ssh into the remote host again and this time it won't prompt you for password

root:# ssh 172.16.0.2 -l root

Linux ubuntu.example.com 2.6.28-13-generic #45-Ubuntu SMP Tue Jun 30 19:49:51 UTC 2009 i686

Run X Applications remotely via SSH

Check that ssh server allow for X11 forwarding
root@ismail-laptop:~# cd /etc/ssh/
root@ismail-laptop:/etc/ssh# vi sshd_config

Make sure the line below reads
X11Forwarding yes

On ssh client (Vector)
ssh -X root@172.16.0.2

Successfully login

You are able to access ssh server (Ubuntu) from ssh client (Vector). You can then type nautilus to

access the directories and files of the remote host. An interesting exercise is to run X applications to the remote ssh server.

To run X appliactions remotely that is to lauch applications like xterm, mplayer,xeyes,etc
on the remote server.

Export DISPLAY
#export DISPLAY=:0.0
#xterm&

An xterm window will appear on the remote host (Ubuntu)
More interesting is to run mplayer on the remote ssh server

From ssh client, after you have ssh -X to the remote ssh server

type

#root@ssh-client:mplayer somemp3file

The song will be played remotely. You can also play video file as well.

Below is a video clip that is played remotely to the ssh server from the ssh client

Note to restart the sshd services
#cd /etc/rc.d
#./rc.sshd restart

Configuring DNS server in Ubuntu Jaunty

In this exercise, I will be using Ubuntu Jaunty and the DNS server and the DNS client will be Vector Linux.

Before we start, make sure that both server and client are able to ping to each other.

In my exercise, I will be using a class B private IP instead of the usual C class that you often see on other tutorials. I will be using the 172.16.0.0 network IP addresses.

My DNS server has the following settings:

```
root@ismail-laptop:~# more /etc/network/interfaces

auto eth0

iface eth0 inet static

address 172.16.0.2

netmask 255.255.0.0

gateway 172.16.0.1
```

My DNS client has the following settings;

```
root:# more /etc/rc.d/rc.inet1
DEVICE='eth0'

DHCP='no'

IPADDR='172.16.0.1'

NETMASK='255.255.0.0'

GATEWAY='172.16.0.2'

PROBE='no'
```

You can choose whatever private IP address range, e.g.the 10.x.x.x or the192.168.1.x etc.

Now let's configure the DNS client first. It's very easy. On the DNS client you only need to edit the /etc/resolv.conf file and enter the DNS server IP address as shown

root:# cd /etc/

vector://etc

root:# vi resolv.conf
nameserver 172.16.0.2

Save and exit. You need not have to restart any services on the client.

Install BIND DNS Server

Install the DNS server, type
apt-get install bind9 dnsutils

Configure BIND

To configure BIND DNS server, you will need to configure the following:

- **the named.conf.local file**
- **the forward zone file**
- **the reverse zone file**

Configure the named.conf.local for a Local Network

The file, /etc/bind/named.conf.local is used to create a regular DNS server. Anything that is configured here is added to the main /etc/bind/named.conf file. I added the statements or you can call it stanza which points to the forward zone file, and also the reverse zone file.

```
root@ismail-laptop:~# cd /etc/bind

root@ismail-laptop:/etc/bind# more named.conf.local

zone "example.com" {

type master;

file "/etc/bind/db.example.com";

};


zone "16.172.in-addr.arpa" {

type master;

file "/etc/bind/db.16.172";

};
```

The first stanza points to the forward zone file while the second stanza points to the reverse zone file.

You need to create a file /etc/bind/db.example.com for the forward zone file and for the reverse zone file, you need to create a file called /etc/bind/db.16.172. Take note that the reverse zone file name has the IP address network reverse. Since mine is 172.16.0.0 network, with subnet mask of

255.255.0.0, the network portion written revers is 16.172.

Edit the confgiuration file but make a copy first

root@ismail-laptop:/etc/bind# cp -p named.conf.local named.conf.local.bkp

The forward zone file

They provide a template.Thus you can use it and copy

root@ismail-laptop:/etc/bind# cp db.local /etc/bind/db.example.com

```
root@ismail-laptop:/etc/bind# more db.example.com
;
; BIND data file for local loopback interface
;
$TTL   604800
@      IN     SOA    ns1.example.com. root.localhost. (
                           2             ; Serial
                      604800             ; Refresh
                       86400             ; Retry
                     2419200             ; Expire
                      604800 )    ; Negative Cache TTL
;
       IN     NS     ns1.example.com.
ns1    IN     A      172.16.0.2
mars   IN     A      172.16.0.1


www    IN     CNAME  mars
```

Note

You need not type all thses but you can easily copy and rename as I did here

root@ismail-laptop:/etc/bind# cp db.local db.example.com

But you will need to make the necessary changes.

I also deleted the lines associated with the IPV4 and IPV6 localhost address

@ IN A 127.0.0.1

@ IN AAAA ::1

The @ sign is a shorthand that refers to the current origin zone in the /etc/named.conf file

The reverse zone file

This is the zone definition for reverse DNS. You will need to replace with your network address in reverse notation.

There is a template to produce the reverse zone file. Type the following command:

```
root@ubuntu:/etc/bind# cp -p db.local db.16.172

root@ismail-laptop:/etc/bind# more db.16.172

;

; BIND reverse data file for local loopback interface

;

$TTL   604800

@      IN     SOA    ns1.example.com. root.localhost. (

                            1             ; Serial

                       604800             ; Refresh

                        86400             ; Retry

                      2419200             ; Expire

                       604800 )    ; Negative Cache TTL

;

@      IN     NS     ns1.example.com.

2.0    IN     PTR    ns1.example.com.

1.0    IN     PTR    mars.example.com.


1.0    IN     PTR    www.example.com.
```

Look at the leftest most column, and you will see these numbers 2.0, 1.0. These numbers refers to the last octal segment of the IP address of my servers. Yes if you notice, it is reverse.

172.16.0.1 – my Web server (www.example.com), which double up as a file server (mars.example.com) ; so the last octal IP address reversed is written as 2.0

172.16.0.2 – my DNS server; so the last octal IP address reversed is written as 1.0

Another thing to take note is the difference between the forward zone and reverse zone is that the reverse zone only has PTR and NS records. Aslo the PTR records cannot have CNAME aliases.

A reverse zone is not required for a functional DNS server. But without a reverse zone, reverse searches **based on IP address** are not possible.

Restart the BIND DNS server

To restart BIND, type:
cd /etc/init.d

root@ismail-laptop:/etc/init.d# ./bind9 restart

Log files which are useful in troubleshooting mis-configured DNS server can be found in /var/log/daemon.log

BIND Command Utilities

You have an array of utilities to choose from to check if the DNS server configuration is working. You can type the following commands either on the DNS server itself or the DNS client.

- nslookup
- host
- dig

Using nslookup

On the DNS server

root@ismail-laptop:~# nslookup example.com

Server: 172.16.0.2

Address: 172.16.0.2#53

*** Can't find example.com: No answer

root@ismail-laptop:~# nslookup 172.16.0.2

Server: 172.16.0.2

Address: 172.16.0.2#53

2.0.16.172.in-addr.arpa name = ns1.example.com.

Using host

On the DNS server

root@ismail-laptop:~# host ns1.example.com

ns1.example.com has address 172.16.0.2

root@ismail-laptop:~# host mars.example.com

mars.example.com has address 172.16.0.1

root@ismail-laptop:~# host www.example.com

www.example.com is an alias for mars.example.com.

mars.example.com has address 172.16.0.1

You may want to use options -la with host command

root@ismail-laptop:~# host -la example.com

Trying "example.com"

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21533

;; flags: qr aa ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 0

```
;; QUESTION SECTION:
;example.com.                   IN      AXFR

;; ANSWER SECTION:
example.com.            604800  IN      SOA     ns1.example.com. root.localhost. 2 604800 86400 2419200 604800
example.com.            604800  IN      NS      ns1.example.com.
mars.example.com.       604800  IN      A       172.16.0.1
ns1.example.com.        604800  IN      A       172.16.0.2
www.example.com.        604800  IN      CNAME           mars.example.com.
example.com.            604800  IN      SOA     ns1.example.com. root.localhost. 2 604800 86400 2419200 604800

Received 188 bytes from 172.16.0.2#53 in 8 ms
```

Try using the IP address of the DNS server. This is where you can realize the use of the reverse zone file.

root@ismail-laptop:~# host -la 172.16.0.2

```
Trying "2.0.16.172.in-addr.arpa"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10323
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;2.0.16.172.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
2.0.16.172.in-addr.arpa. 604800     IN      PTR     ns1.example.com.

;; AUTHORITY SECTION:
16.172.in-addr.arpa.        604800  IN      NS      ns1.example.com.
```

```
;; ADDITIONAL SECTION:
ns1.example.com.        604800  IN      A       172.16.0.2

Received 100 bytes from 172.16.0.2#53 in 0 ms
```

Using dig

On the DNS server

```
root@ismail-laptop:~# dig example.com

; <<>> DiG 9.5.1-P2.1 <<>> example.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54108
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;example.com.                   IN      A

;; AUTHORITY SECTION:
example.com.            604800  IN      SOA     ns1.example.com. root.localhost. 2 604800 86400 2419200 604800

;; Query time: 0 msec
;; SERVER: 172.16.0.2#53(172.16.0.2)
;; WHEN: Mon Mar  1 11:22:16 2010
;; MSG SIZE  rcvd: 83
```

```
root@ismail-laptop:~# dig ns1.example.com

; <<>> DiG 9.5.1-P2.1 <<>> ns1.example.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30512
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;ns1.example.com.                IN      A

;; ANSWER SECTION:
ns1.example.com.        604800  IN      A       172.16.0.2

;; AUTHORITY SECTION:
example.com.            604800  IN      NS      ns1.example.com.

;; Query time: 0 msec
;; SERVER: 172.16.0.2#53(172.16.0.2)
;; WHEN: Mon Mar  1 11:23:38 2010
;; MSG SIZE  rcvd: 63
root@ismail-laptop:~# dig mars.example.com

; <<>> DiG 9.5.1-P2.1 <<>> mars.example.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16626
```

```
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;mars.example.com.              IN      A

;; ANSWER SECTION:
mars.example.com.       604800  IN      A       172.16.0.1

;; AUTHORITY SECTION:
example.com.            604800  IN      NS      ns1.example.com.

;; ADDITIONAL SECTION:
ns1.example.com.        604800  IN      A       172.16.0.2

;; Query time: 7 msec
;; SERVER: 172.16.0.2#53(172.16.0.2)
;; WHEN: Mon Mar  1 11:24:14 2010
;; MSG SIZE  rcvd: 84
```

root@ismail-laptop:~# dig www.example.com

```
; <<>> DiG 9.5.1-P2.1 <<>> www.example.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5950
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 1
```

;; QUESTION SECTION:

;www.example.com. IN A

;; ANSWER SECTION:

www.example.com. 604800 IN CNAME mars.example.com.

mars.example.com. 604800 IN A 172.16.0.1

;; AUTHORITY SECTION:

example.com. 604800 IN NS ns1.example.com.

;; ADDITIONAL SECTION:

ns1.example.com. 604800 IN A 172.16.0.2

;; Query time: 0 msec

;; SERVER: 172.16.0.2#53(172.16.0.2)

;; WHEN: Mon Mar 1 11:24:39 2010

;; MSG SIZE rcvd: 102

Using dig for Reverse Name Resolution

DNS implements reverse name resolution by means of a special doamin in-addr.arpa (IPV4) or (ip6.arpa (IPV6)

To determine the domain name that corresponds to an IP address 172.16.0.2 a resolver would query DNS named 2.0.16.172.in-addr.arpa PTR

Using the dig command you will append the words in-addr.arpa to display the PTR record. The IP address is also typed reverse.

```
# dig 2.0.16.172.in-addr.arpa PTR
; <<>> DiG 9.5.1-P2.1 <<>> 2.0.16.172.in-addr.arpa PTR

;; global options:  printcmd

;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14886

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 1, ADDITIONAL: 1


;; QUESTION SECTION:

;2.0.16.172.in-addr.arpa.  IN     PTR


;; ANSWER SECTION:

2.0.16.172.in-addr.arpa. 604800  IN     PTR    ns1.example.com.

2.0.16.172.in-addr.arpa. 604800  IN     PTR    mail.example.com.

2.0.16.172.in-addr.arpa. 604800  IN     PTR    ubuntu.example.com.


;; AUTHORITY SECTION:

16.172.in-addr.arpa.      604800 IN     NS     ns1.example.com.


;; ADDITIONAL SECTION:

ns1.example.com.    604800 IN     A      172.16.0.2


;; Query time: 0 msec

;; SERVER: 172.16.0.2#53(172.16.0.2)

;; WHEN: Tue Mar 23 00:43:46 2010

;; MSG SIZE  rcvd: 140
```

Instead of reformatting the IP address as in the preceeding example, you can use the -x option with dig to perform a reverse query.

```
# dig -x 172.16.0.2
```

Or you can use the host command

```
#host 172.16.0.2
2.0.16.172.in-addr.arpa domain name pointer mail.example.com.

2.0.16.172.in-addr.arpa domain name pointer ubuntu.example.com.

2.0.16.172.in-addr.arpa domain name pointer ns1.example.com.
```

Using ping

On DNS server or client

Now this is the reason we use DNS so that we don't need to configure each /etc/hosts file on each terminal. The DNS server maintains the IP address of the hosts in the network. Cool.

root@ismail-laptop:~# ping mars.example.com

PING mars.example.com (172.16.0.1) 56(84) bytes of data.

64 bytes from www.example.com (172.16.0.1): icmp_seq=1 ttl=64 time=0.459 ms

^C

--- mars.example.com ping statistics ---

1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 0.459/0.459/0.459/0.000 ms

root@ismail-laptop:~# ping www.example.com

PING mars.example.com (172.16.0.1) 56(84) bytes of data.

64 bytes from mars.example.com (172.16.0.1): icmp_seq=1 ttl=64 time=0.365 ms

64 bytes from www.example.com (172.16.0.1): icmp_seq=2 ttl=64 time=0.367 ms

Testing DNS Configuration Using BIND Utilities

The following are the excerpts from the output that are executed on the **DNS client, Vector Linux**

root:# host www.example.com

www.example.com CNAME mars.example.com

mars.example.com A 172.16.0.1

root:# host mars.example.com

mars.example.com A 172.16.0.1

root:# host ns1.example.com

```
ns1.example.com        A        172.16.0.2

root:# host 172.16.0.2
Name: ns1.example.com
Address: 172.16.0.2

vector://etc
root:# nslookup
> www.example.com
www.example.com                CNAME        mars.example.com
mars.example.com       A        172.16.0.1
> mars.example.com
mars.example.com       A        172.16.0.1
> ns1.example.com
ns1.example.com        A        172.16.0.2
> example.com
 *** example.com has no A record (Authoritative answer)
>
exit
root:# host -la example.com
 !!! example.com has only one nameserver ns1.example.com
example.com.                   IN       SOA      ns1.example.com. root.localhost. (
                               2        ;serial number (version)
                               604800   ;slave refresh period (1 week)
                               86400    ;slave retry interval (1 day)
```

```
                        2419200 ;slave expire time (4 weeks)
                        604800  ;negative response TTL (1 week)
                        )
example.com.            IN      NS      ns1.example.com.
mars.example.com.       IN      A       172.16.0.1
ns1.example.com.        IN      A       172.16.0.2
www.example.com.        IN      CNAME           mars.example.com.
example.com.            IN      SOA     ns1.example.com. root.localhost. (
                        2       ;serial number (version)
                        604800  ;slave refresh period (1 week)
                        86400   ;slave retry interval (1 day)
                        2419200 ;slave expire time (4 weeks)
                        604800  ;negative response TTL (1 week)
```

MX Configuration. Which Is It?

Should the mail server entry in the forward zone be this:

```
    IN    MX    10 mail
```

or this

```
    IN    MX    10 mail.example.com.    ?
```

I used both and I can send and received mails. The only issue is that for both settings, I still receive e-mail address as whoever@mail.example.com instead of whoever@example.com. And to send mails, you need to use toyou@mail.example.com as toyou@example.com will caused the mail to be rejected and undelivered.

Actually both syntax are correct. The former requires less typing.

Notes

If you don't put a period at the end of a host name in a SOA, NS, A, or CNAME record, BIND will automatically tack on the zone file's domain name to the name of the host. So, BIND assumes an A record with www refers to www.my-site.com. This may be acceptable in most cases, but if you forget to put the period after the domain in the MX record for my-site.com, BIND attaches the my-site.com at the end, and you will find your mail server accepting mail only for the domain my-site.com.mysite.com.

The following is valid

```
mail.gite.in           86400    IN cname mail.cyberciti.biz.
```

The period at the end of the hostname mail.gite.in is missing but acceptable. But you need to put the period after the domain biz.

More Examples

Mail Servers in Zone

```
; zone fragment example.com
; mail servers in the same zone
; will support email with addresses of the format
; user@example.com
$TTL 2d ; zone default = 2 days or 172800 seconds
$ORIGIN example.com.
example.com. IN       SOA   ns1.example.com. root.example.com. (
               2003080800 ; serial number
               3h         ; refresh =  3 hours
               15M        ; update retry = 15 minutes
               3W12h      ; expiry = 3 weeks + 12 hours
               2h20M      ; minimum = 2 hours + 20 minutes
               )
              IN      MX     10  mail  ; short form
; the line above is functionally the same as the line below
; example.com. IN     MX     10  mail.example.com.
; any number of mail servers may be defined
              IN      MX     20  mail2.example.com.
; use an external back-up
              IN      MX     30  mail.example.net.
; the local mail server(s) need an A record
mail          IN      A      192.168.0.3
mail2         IN      A      192.168.0.3
```

No Mail Servers in Zone

```
; zone fragment for example.com
; mail servers not in the zone
; will support email with addresses of the format
; user@example.com
$TTL 2d ; zone default = 2 days or 172800 seconds
$ORIGIN example.com.
example.com. IN       SOA   ns1.example.com. root.example.com. (
               2003080800 ; serial number
               3h         ; refresh =  3 hours
               15M        ; update retry = 15 minutes
               3W12h      ; expiry = 3 weeks + 12 hours
               2h20M      ; minimum = 2 hours + 20 minutes
               )
; mail servers not in zone - no A records required
               IN     MX     10  mail.foo.com.
               IN     MX     20  mail2.foo.com.
```

Note

MX don't need A record. Mails still can be send and receive.

You don't need to have A record for mail as shown below.

mail IN A 172.16.0.2

Without such entry, mails can still be send and receive.

```
Subject: Jam 12

To: <ismail@example.com>

Cc: <root@example.com>

Date: Wed,  3 Mar 2010 00:49:44 +0800 (SGT)

From: root@mail.example.com (root)



Special Encore
```

The logs to prove it

```
Mar  3 00:49:44 ismail-laptop postfix/pickup[16001]: 06BA728098: uid=0 from=<root>

Mar  3 00:49:44 ismail-laptop postfix/cleanup[16215]: 06BA728098: message-
id=<20100302164944.06BA728098@ubuntu.example.com>

Mar  3 00:49:44 ismail-laptop postfix/qmgr[16004]: 06BA728098: from=<root@mail.example.com>, size=375, nrcpt=2 (queue
active)

Mar  3 00:49:44 ismail-laptop postfix/local[16217]: 06BA728098: to=<ismail@example.com>, relay=local, delay=0.07,
delays=0.05/0.01/0/0.01, dsn=2.0.0, status=sent (delivered to mailbox)

Mar  3 00:49:44 ismail-laptop postfix/local[16218]: 06BA728098: to=<root@example.com>, relay=local, delay=0.07,
delays=0.05/0.02/0/0.01, dsn=2.0.0, status=sent (delivered to mailbox)

Mar  3 00:49:44 ismail-laptop postfix/qmgr[16004]: 06BA728098: removed
```

But I just include it because I would want to execute host command on the host ns1.example.com

The excerpts above show that root@mail.example.com send out mails to ismail@example.com and root@example.com . Also note how I am able to use example.com instead of mail.example.com. This is explained in the coming sections.

Anyway I tested using both and using the nslookup,host and dig utilities, I get the following output

Using IN MX 10 mail

nslookup mail.example.com

Server: 127.0.0.1

```
Address:        127.0.0.1#53


mail.example.com      canonical name = ubuntu.example.com.

Name: ubuntu.example.com

Address: 172.16.0.2

# host mail.example.com

mail.example.com is an alias for ubuntu.example.com.

ubuntu.example.com has address 172.16.0.2

# dig mail.example.com


; <<>> DiG 9.5.1-P2.1 <<>> mail.example.com

;; global options:  printcmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16611

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 1


;; QUESTION SECTION:

;mail.example.com.                  IN      A


;; ANSWER SECTION:

mail.example.com.       604800  IN      CNAME           ubuntu.example.com.

ubuntu.example.com.     604800  IN      A       172.16.0.2


;; AUTHORITY SECTION:

example.com.            604800  IN      NS      ns1.example.com.
```

;; ADDITIONAL SECTION:

ns1.example.com. 604800 IN A 172.16.0.2

;; Query time: 0 msec

;; SERVER: 127.0.0.1#53(127.0.0.1)

;; WHEN: Tue Mar 2 05:10:57 2010

;; MSG SIZE rcvd: 105

Try pinging

ping mail.example.com

PING ubuntu.example.com (172.16.0.2) 56(84) bytes of data.

64 bytes from ubuntu.example.com (172.16.0.2): icmp_seq=1 ttl=64 time=0.043 ms

64 bytes from mail.example.com (172.16.0.2): icmp_seq=2 ttl=64 time=0.046 ms

Using IN MX 10 mail.example.com.

root@ismail-laptop:/etc/postfix# nslookup mail.example.com

Server: 127.0.0.1

Address: 127.0.0.1#53

mail.example.com canonical name = ubuntu.example.com.

Name: ubuntu.example.com

Address: 172.16.0.2

root@ismail-laptop:/etc/postfix# host mail.example.com

mail.example.com is an alias for ubuntu.example.com.

ubuntu.example.com has address 172.16.0.2

root@ismail-laptop:/etc/postfix# dig mail.example.com

```
; <<>> DiG 9.5.1-P2.1 <<>> mail.example.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40719
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;mail.example.com.          IN      A

;; ANSWER SECTION:
mail.example.com. 604800    IN      CNAME   ubuntu.example.com.
ubuntu.example.com.         604800  IN      A       172.16.0.2

;; AUTHORITY SECTION:
example.com.                604800  IN      NS      ns1.example.com.

;; ADDITIONAL SECTION:
ns1.example.com.   604800   IN      A       172.16.0.2

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Mar  2 05:24:03 2010
;; MSG SIZE  rcvd: 105
```

Which Comes First, DNS or /etc/hosts?

If you want to know whether your computer looks for the DNS or /etc/hosts file when looking for the IP address, type the following command:

root@ubuntu:~# cat /etc/host.conf

order hosts,bind

multi on

The first line suggest that the local database /etc/hosts is searched before DNS server . There is another file which your computer will look up to i.e. The /etc/nsswitch.conf file. In fact the /etc/nsswitch.conf file supercedes the /etc/hosts file when your computer looks for an IP address. For example, if there's an active NIS server, a Samba database of database, an LDAP server, you may see the following entry

```
hosts: files dns nis ldap winbind
```

In my case it looks like this

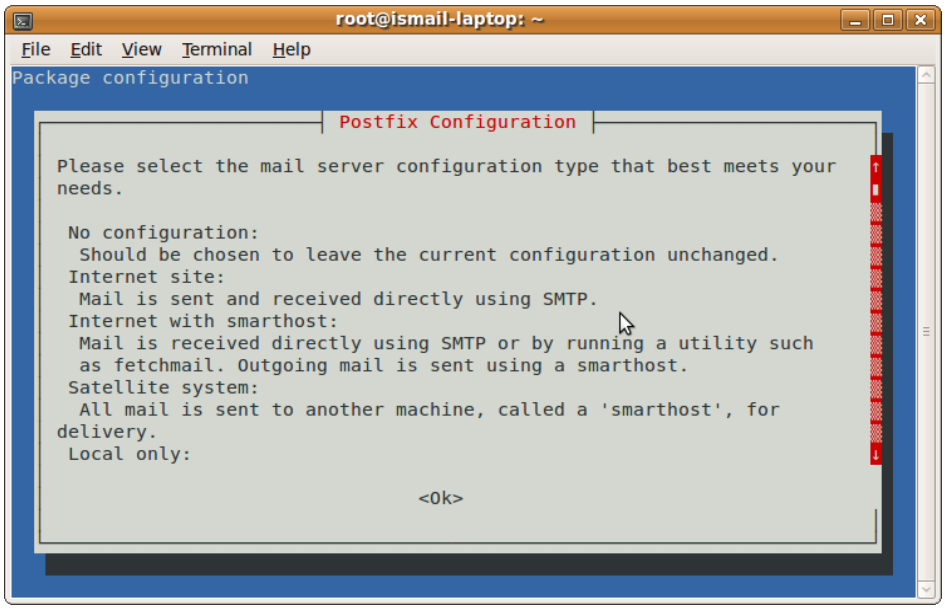
```
hosts:          files mdns4_minimal [NOTFOUND=return] dns mdns4
```

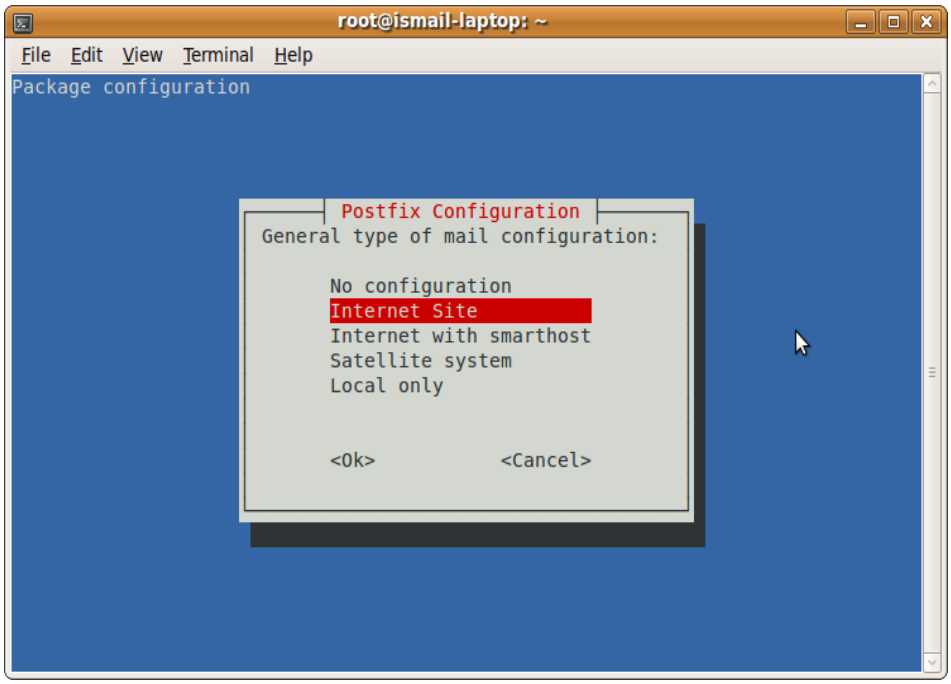
Configuring Mail Services Using Postfix in Ubuntu Jaunty

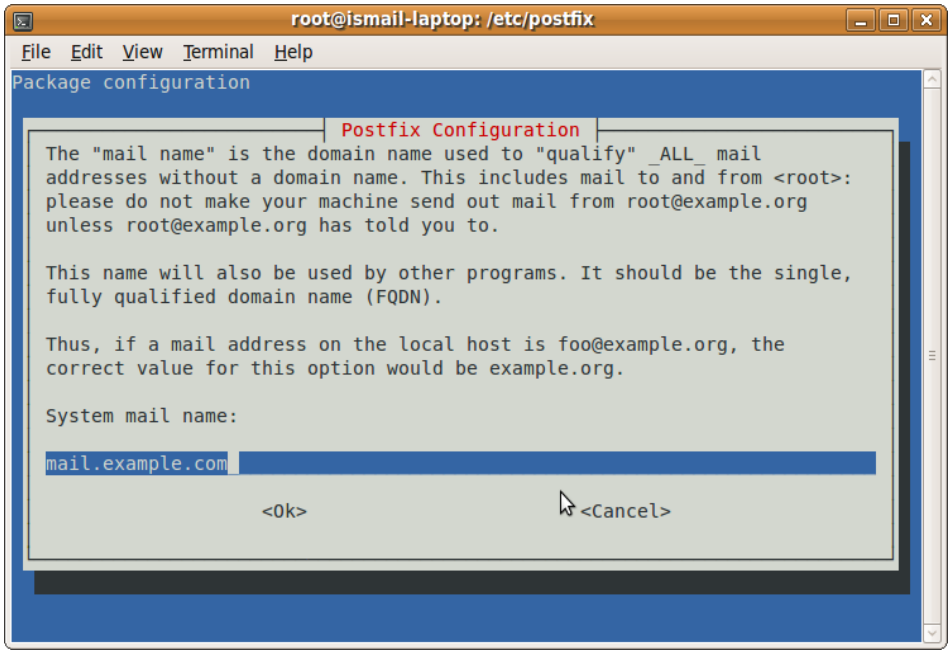
Install postfix as the mail server

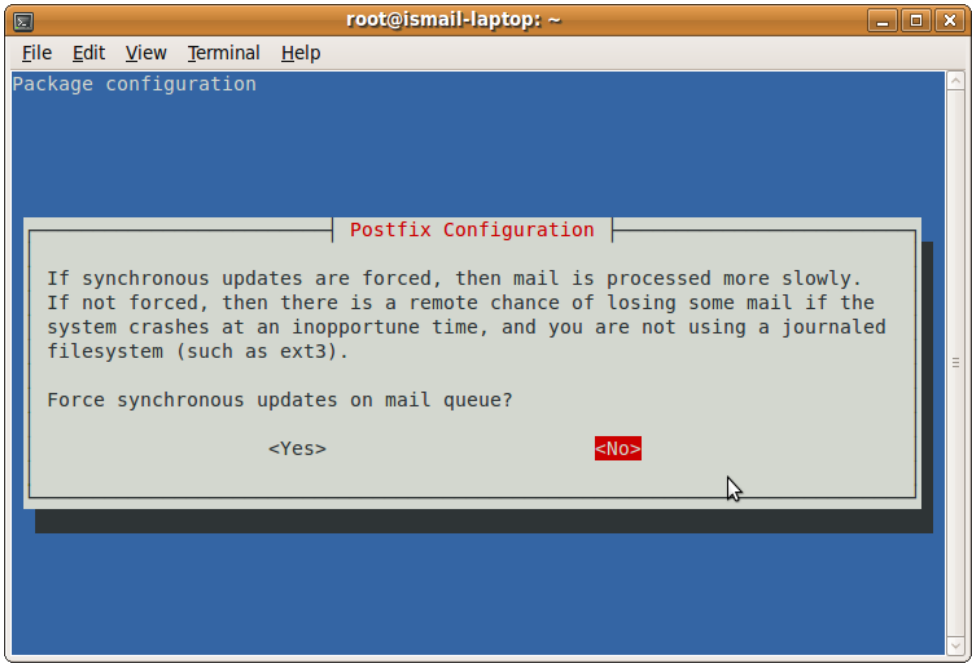
root@ismail-laptop:~# apt-get install postfix

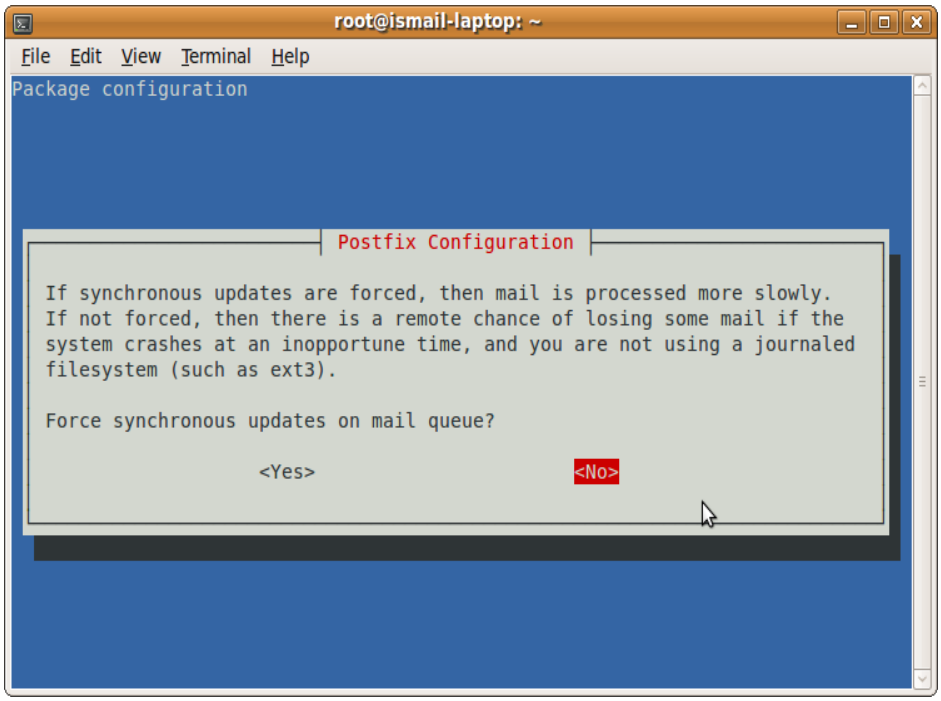
you will be prompted in a number of text-based screens to configure Postfix

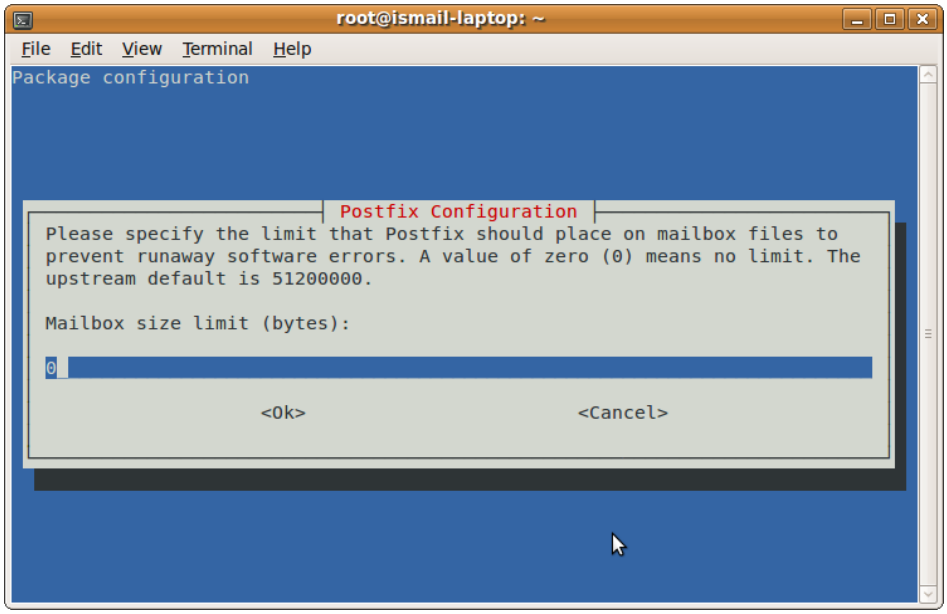

root@ismail-laptop: ~
File Edit View Terminal Help
Package configuration
Postfix Configuration
Please select the mail server configuration type that best meets your needs.
No configuration:
Should be chosen to leave the current configuration unchanged.
Internet site:
Mail is sent and received directly using SMTP.
Internet with smarthost:
Mail is received directly using SMTP or by running a utility such as fetchmail. Outgoing mail is sent using a smarthost.
Satellite system:
All mail is sent to another machine, called a 'smarthost', for delivery.
Local only:
<Ok>

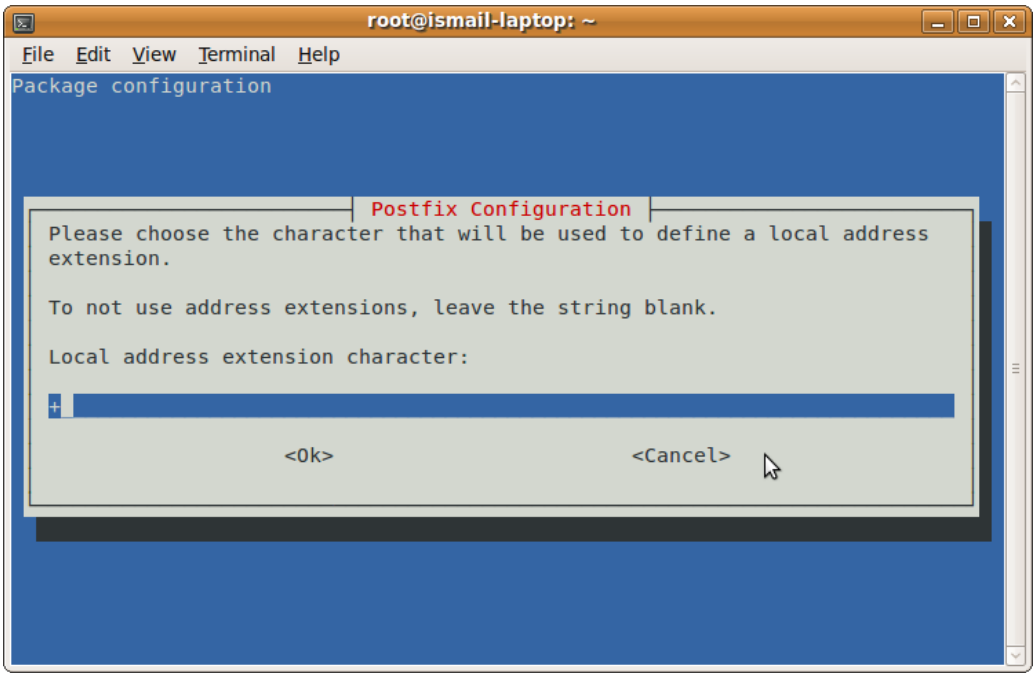

root@ismail-laptop: ~
File Edit View Terminal Help
Package configuration
Postfix Configuration
General type of mail configuration:
No configuration
Internet Site
Internet with smarthost
Satellite system
Local only
<Ok>
<Cancel>

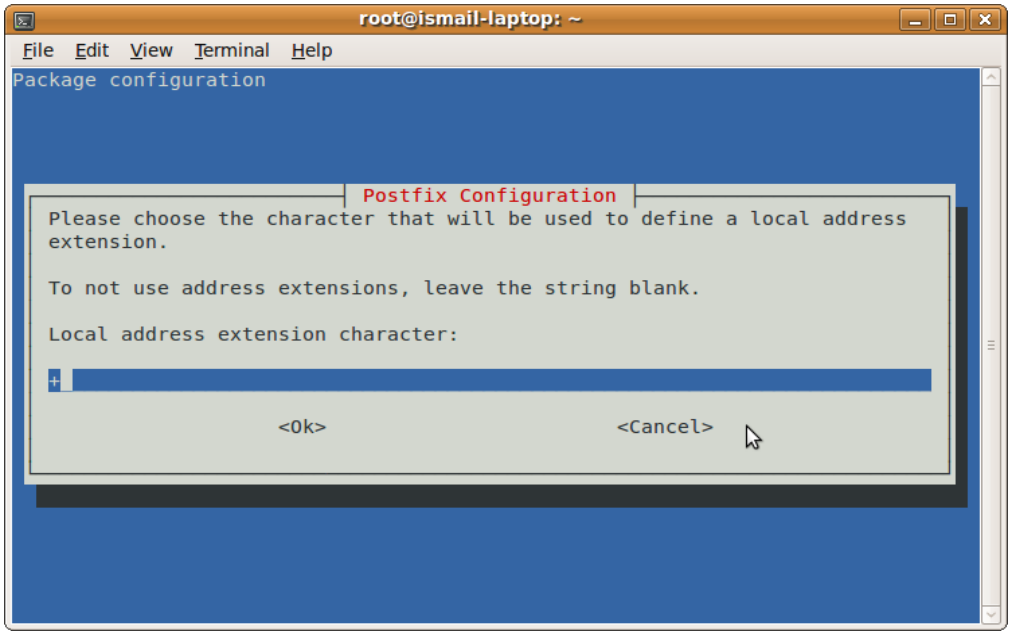

root@ismail-laptop: /etc/postfix
File Edit View Terminal Help
Package configuration
Postfix Configuration
The "mail name" is the domain name used to "qualify" _ALL_ mail
addresses without a domain name. This includes mail to and from <root>:
please do not make your machine send out mail from root@example.org
unless root@example.org has told you to.
This name will also be used by other programs. It should be the single,
fully qualified domain name (FQDN).
Thus, if a mail address on the local host is foo@example.org, the
correct value for this option would be example.org.
System mail name:
mail.example.com
<Ok>
<Cancel>

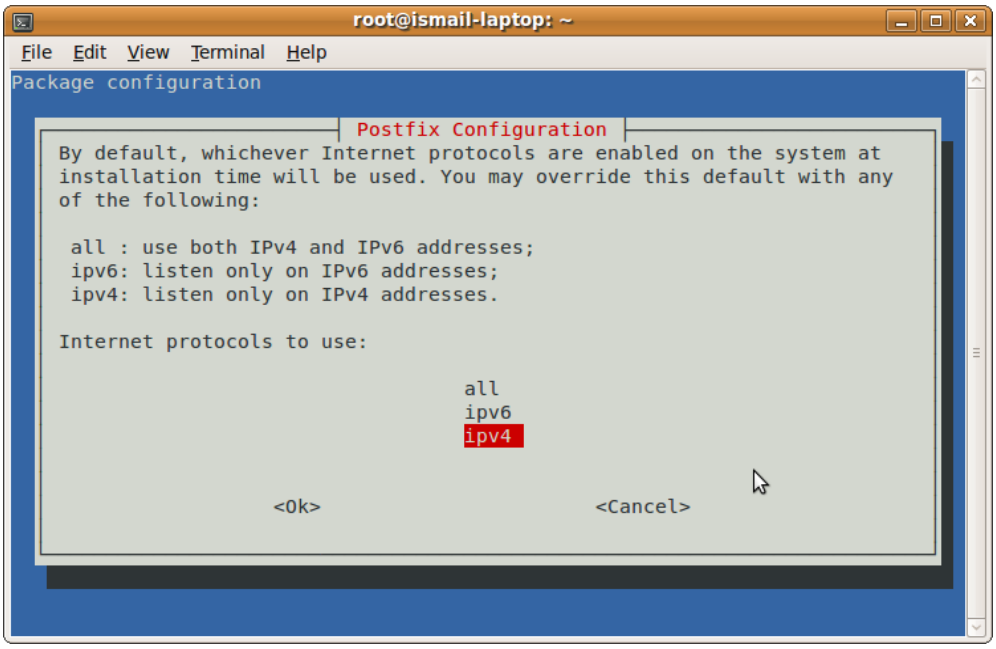

root@ismail-laptop: ~
File Edit View Terminal Help
Package configuration
Postfix Configuration
If synchronous updates are forced, then mail is processed more slowly.
If not forced, then there is a remote chance of losing some mail if the
system crashes at an inopportune time, and you are not using a journaled
filesystem (such as ext3).
Force synchronous updates on mail queue?
<Yes>
<No>

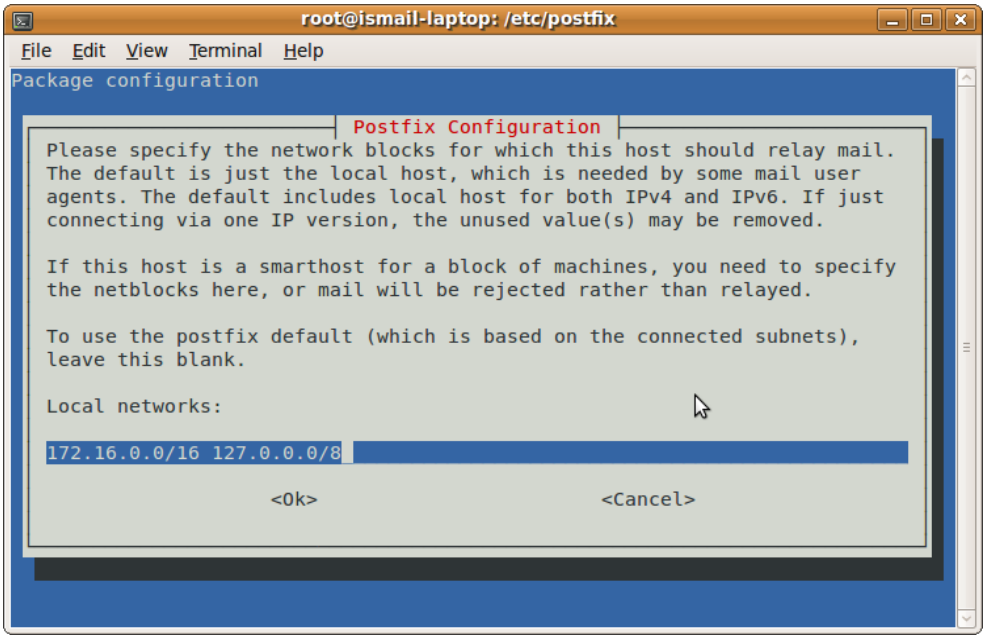

root@ismail-laptop: ~
File Edit View Terminal Help
Package configuration
Postfix Configuration
If synchronous updates are forced, then mail is processed more slowly.
If not forced, then there is a remote chance of losing some mail if the
system crashes at an inopportune time, and you are not using a journaled
filesystem (such as ext3).
Force synchronous updates on mail queue?
<Yes>
<No>


root@ismail-laptop: ~
File Edit View Terminal Help
Package configuration
Postfix Configuration
Please specify the limit that Postfix should place on mailbox files to
prevent runaway software errors. A value of zero (0) means no limit. The
upstream default is 51200000.
Mailbox size limit (bytes):
0
<Ok>
<Cancel>


root@ismail-laptop: ~
File Edit View Terminal Help
Package configuration
Postfix Configuration
Please choose the character that will be used to define a local address extension.
To not use address extensions, leave the string blank.
Local address extension character:
+
<Ok>
<Cancel>


root@ismail-laptop: ~
File Edit View Terminal Help
Package configuration
Postfix Configuration
Please choose the character that will be used to define a local address extension.
To not use address extensions, leave the string blank.
Local address extension character:
+
<Ok>
<Cancel>





To reconfigure the these features run

root@ismail-laptop:~# dpkg-reconfigure postfix

Note
After modifying main.cf, be sure to run '/etc/init.d/postfix reload'

You will need to further configure Postfix

Backup the main configuration file

root@ismail-laptop:~# cd /etc/postfix/

root@ismail-laptop:/etc/postfix# cp main.cf main.cf.bak

Try the telnet command to explore some of the settings. I tested using IP address, 172.16.0.2 which is the IP for my localmachine, localhost, etc

root@ismail-laptop:~# telnet 172.16.0.2 25

Trying 172.16.0.2...

Connected to 172.16.0.2.

Escape character is '^]'.

220 ismail-laptop ESMTP Postfix (Ubuntu)

root@ismail-laptop:~# telnet 127.0.0.1 25

Trying 127.0.0.1...

Connected to 127.0.0.1.

Escape character is '^]'.

220 ismail-laptop ESMTP Postfix (Ubuntu)

I changed the myhostname directive

myhostname = mars.example.com

You must restart postfix

/etc/init.d/./postfix reload

root@ismail-laptop:/etc/postfix# telnet localhost 25

Trying ::1...

Trying 127.0.0.1...

Connected to localhost.

Escape character is '^]'.

220 mars.example.com ESMTP Postfix (Ubuntu)

From the above excerpt output, the hostname is changed. I will change it back to ubuntu.example.com as it is a Ubuntu machine. This will also serve as my mail server in DNS settings.

Important
It's important that you changed your machine hostname so that it reflects the same hostname as in the configuration file. I changed my hostname to ubunt.example.com by typing

vi /etc/hostname
ubunt.example.com

You will then need to reboot the server or you can easily typed

/etc/init.d/./hostname.sh

I could also telnet from mail client, Vector Linux host which I have also configured as my DNS client

root:# telnet 172.16.0.2 25

Trying 172.16.0.2...

Connected to 172.16.0.2.

Escape character is '^]'.

220 mars.example.com ESMTP Postfix (Ubuntu)

I edited the forward and reverse zone files in DNS. I tested these settings

root@ismail-laptop:/etc/bind# host mail.example.com

mail.example.com is an alias for ubuntu.example.com.

ubuntu.example.com has address 172.16.0.2

root@ismail-laptop:/etc/bind# host ubuntu.example.com

ubuntu.example.com has address 172.16.0.2

root@ismail-laptop:/etc/bind# host 172.16.0.2

2.0.16.172.in-addr.arpa domain name pointer ubuntu.example.com.

2.0.16.172.in-addr.arpa domain name pointer ns1.example.com.

2.0.16.172.in-addr.arpa domain name pointer mail.example.com.

I can also ping from my DNS client, Vector Linux

root:# ping ubuntu.example.com

```
PING ubuntu.example.com (172.16.0.2) 56(84) bytes of data.

64 bytes from ubuntu.example.com (172.16.0.2): icmp_seq=1 ttl=64 time=0.376 ms

64 bytes from mail.example.com (172.16.0.2): icmp_seq=2 ttl=64 time=0.321 ms


--- ubuntu.example.com ping statistics ---

2 packets transmitted, 2 received, 0% packet loss, time 999ms

rtt min/avg/max/mdev = 0.321/0.348/0.376/0.033 ms
```

root:# ping mail.example.com

PING ubuntu.example.com (172.16.0.2) 56(84) bytes of data.

64 bytes from ns1.example.com (172.16.0.2): icmp_seq=1 ttl=64 time=0.324 ms

64 bytes from ubuntu.example.com (172.16.0.2): icmp_seq=2 ttl=64 time=0.336 ms

Sending Test Mail

root@ismail-laptop:~# mailx

No mail for root

root@ismail-laptop:~# mail -s "Test Mail"

To: root@example.com

Cc:

Hi this is a test mail

root@ismail-laptop:~# mail

"/var/mail/root": 1 message 1 new

>N 1 root Mon Mar 1 18:32 13/448 Test Mail

Press enter to read mail

Subject: Test Mail

To: <root@example.com>

Date: Mon, 1 Mar 2010 18:32:59 +0800 (SGT)

From: root@mail.example.com (root)

Hi this is a test mail

&

To quit press q and enter
& q

Held 1 message in /var/mail/root

Note that the mail is from root@mail.example.com

You can read old mails at /var/mail/root

Sending Mail from local user to local user on localhost

Now try to send mail from a user of the local host
root@ismail-laptop:~# su - ismail

To run a command as administrator (user "root"), use "sudo <command>".

See "man sudo_root" for details.

ismail@ismail-laptop:~$ mail -s "test mail from user ismail"

To: root@example.com

Cc:

Hi there!

ismail@ismail-laptop:~$

ismail@ismail-laptop:~$ mailx

No mail for ismail

ismail@ismail-laptop:~$ exit

logout

root@ismail-laptop:~# mailx

"/var/mail/root": 2 messages 1 new

R 1 root Mon Mar 1 18:32 16/493 Test Mail

>N 2 ismail Mon Mar 1 18:52 13/461 test mail from user ismai

&

Subject: test mail from user ismail

To: <root@example.com>

Date: Mon, 1 Mar 2010 18:52:32 +0800 (SGT)

From: ismail@mail.example.com (ismail)

Hi there!

&

Just Experimenting...

I tried to send mail to a remote host but failed. This is from the /var/log/mail.info

```
Mar  1 18:56:21 ismail-laptop postfix/qmgr[9125]: 0C11328080: from=<root@mail.example.com>, size=390, nrcpt=1 (queue active)

Mar  1 18:56:21 ismail-laptop postfix/smtp[11221]: connect to mars.example.com[172.16.0.1]:25: Connection refused

Mar  1 18:56:21 ismail-laptop postfix/smtp[11221]: 0C11328080: to=<root@mars.example.com>, relay=none, delay=0.04,
delays=0.03/0.01/0/0, dsn=4.4.1, status=deferred (connect to mars.example.com[172.16.0.1]:25: Connection refused)
```

Since I have include the mail server, this is the forward and reverse zone files in my DNS

My DNS Forward Zone File

2.0.16.172.in-addr.arpa domain name pointer mail.example.com.

root@ismail-laptop:/etc/bind# more db.example.com

```
;

; BIND data file for local loopback interface

;

$TTL    604800

@       IN      SOA     ns1.example.com. root.localhost. (

                              2             ; Serial

                         604800             ; Refresh

                          86400             ; Retry

                        2419200             ; Expire

                         604800 )           ; Negative Cache TTL

;
```

```
        IN      NS      ns1.example.com.
        IN      MX      10 mail.example.com.
ns1     IN      A       172.16.0.2
mars    IN      A       172.16.0.1
ubuntu  IN      A       172.16.0.2

www     IN      CNAME       mars
mail    IN      CNAME       ubuntu
```

My DNS Reverse Zone file

root@ismail-laptop:/etc/bind# more db.16.172

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns1.example.com. root.localhost. (
                              1           ; Serial
                         604800           ; Refresh
                          86400           ; Retry
                        2419200           ; Expire
                         604800 )         ; Negative Cache TTL
;
@       IN      NS      ns1.example.com.
2.0     IN      PTR     ns1.example.com.
1.0     IN      PTR     mars.example.com.

1.0     IN      PTR     www.example.com.
```

2.0 IN PTR mail.example.com.

2.0 IN PTR ubuntu.example.com.

This is what my /etc/postfix/main.cf configuration file looks like:

root@ismail-laptop:/etc/postfix# less main.cf | grep -v "^#" |more

smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)

biff = no

append_dot_mydomain = no

readme_directory = no

smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem

smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key

smtpd_use_tls=yes

smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache

smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

myhostname = ubuntu.example.com

alias_maps = hash:/etc/aliases

alias_database = hash:/etc/aliases

myorigin = /etc/mailname

mydestination = example.com, ismail-laptop, localhost.localdomain, localhost

relayhost =

mynetworks = 172.16.0.0/16 127.0.0.0/8

mailbox_size_limit = 0

recipient_delimiter = +

inet_interfaces = all

inet_protocols = ipv4

I changed the entries in bold because for the mydestination value it should read mail.example.com instead of just example.com

As for the mynetworks, it should have comma in between entries.

You can use the postconf utility to edit the main.cf file:

postconf -e "mydestination = mail.example.com, ismail-laptop, localhost.localdomain, localhost"

postconf -e "mynetworks = 127.0.0.0/8, 172.16.0.0/16"

Make Postfix to receive mail from the Internet

Instruct Postfix to receive on all interfaces:

```
sudo postconf -e "inet_interfaces = all"
```

(optional) Make Postfix accept IPv4, IPv6 protocols

If you're not using IPv6 yet, and you're paranoid, use "ipv4" instead of "all". Again, this is to suit your own network sensibilities.

```
sudo postconf -e "inet_protocols = all"
```

Restart Postfix

./postfix restart

* Stopping Postfix Mail Transport Agent postfix [OK]

- Starting Postfix Mail Transport Agent postfix [OK]
-

Send mail from root to user, ismail

mail -s "new server"

To: ismail@mail.example.com

Cc:

testing

Cttl+D will exit the mail

Check if user ismail receive the mail
su - ismail
ismail@ismail-laptop:~$ mailx

"/var/mail/ismail": 3 messages 1 new

R 1 root Mon Mar 1 23:12 16/481 Scarlet

R 2 root@localhost Mon Mar 1 23:33 17/479 My first mail

>N 3 root Tue Mar 2 00:22 13/457 new server

&

Subject: new server

To: <ismail@mail.example.com>

Date: Tue, 2 Mar 2010 00:22:14 +0800 (SGT)

From: root@mail.example.com (root)

testing

&

Yes the newly received mail has the address ismail@mail.example.com

From the /var/log/mail.log

Mar 2 00:39:45 ismail-laptop postfix/pickup[11736]: 7376B28083: uid=0 from=<root>

Mar 2 00:39:45 ismail-laptop postfix/cleanup[13412]: 7376B28083: message-id=<20100301163945.7376B28083@ubuntu.example.com>

Mar 2 00:39:45 ismail-laptop postfix/qmgr[11737]: 7376B28083: from=<root@mail.example.com>, size=359, nrcpt=1 (queue active)

Mar 2 00:39:45 ismail-laptop postfix/local[13414]: 7376B28083: to=<ismail@mail.example.com>, relay=local, delay=0.06, delays=0.03/0.01/0/0.02, dsn=2.0.0, status=sent (delivered to mailbox)

Mar 2 00:39:45 ismail-laptop postfix/qmgr[11737]: 7376B28083: removed

Mail Bounce

User ismail tried to send mail to root@example.com . It will failed as shown by the logs. The recipient should be root@mail.example.com

root@ismail-laptop:/etc/bind# su - ismail

ismail@ismail-laptop:~$

ismail@ismail-laptop:~$ mail -s "USA idol"

To: root@example.com

Cc:

Winner

From the /var/log/mail.log

Mar 2 00:34:29 ismail-laptop postfix/pickup[11736]: A144028083: uid=1001 from=<ismail>

Mar 2 00:34:29 ismail-laptop postfix/cleanup[13032]: A144028083: message-id=<20100301163429.A144028083@ubuntu.example.com>

Mar 2 00:34:29 ismail-laptop postfix/qmgr[11737]: A144028083: from=<ismail@mail.example.com>, size=350, nrcpt=1 (queue active)

Mar 2 00:34:29 ismail-laptop postfix/smtp[13034]: A144028083: to=<root@example.com>, relay=none, delay=0.06, delays=0.05/0.01/0/0, dsn=5.4.6, status=bounced (mail for example.com loops back to myself)

Mar 2 00:34:29 ismail-laptop postfix/cleanup[13032]: AFE5628089: message-id=<20100301163429.AFE5628089@ubuntu.example.com>

Mar 2 00:34:29 ismail-laptop postfix/qmgr[11737]: AFE5628089: from=<>, size=2096, nrcpt=1 (queue active)

Mar 2 00:34:29 ismail-laptop postfix/bounce[13035]: A144028083: sender non-delivery notification: AFE5628089

Mar 2 00:34:29 ismail-laptop postfix/qmgr[11737]: A144028083: removed

Mar 2 00:34:29 ismail-laptop postfix/local[13036]: AFE5628089: to=<ismail@mail.example.com>, relay=local, delay=0.05, delays=0.02/0.02/0/0.01, dsn=2.0.0, status=sent (delivered to mailbox)

Mar 2 00:34:29 ismail-laptop postfix/qmgr[11737]: AFE5628089: removed

The mail is returned to the sender as shown below

```
>N   4 Mail Delivery Syst Tue Mar  2 00:34  65/2127  Undelivered Mail Returned

 N   5 root             Tue Mar  2 00:39  13/463   Super Bargain

&

Date: Tue,  2 Mar 2010 00:34:29 +0800 (SGT)

From: MAILER-DAEMON@mail.example.com (Mail Delivery System)

Subject: Undelivered Mail Returned to Sender

To: ismail@mail.example.com



This is a MIME-encapsulated message.
```

```
--A144028083.1267461269/ubuntu.example.com

Content-Description: Notification

Content-Type: text/plain; charset=us-ascii


This is the mail system at host ubuntu.example.com.


I'm sorry to have to inform you that your message could not

be delivered to one or more recipients. It's attached below.


For further assistance, please send mail to postmaster.


If you do so, please include this problem report. You can

delete your own text from the attached returned message.


                  The mail system


<root@example.com>: mail for example.com loops back to myself


--A144028083.1267461269/ubuntu.example.com

Content-Description: Delivery report

Content-Type: message/delivery-status


Reporting-MTA: dns; ubuntu.example.com

X-Postfix-Queue-ID: A144028083

X-Postfix-Sender: rfc822; ismail@mail.example.com

Arrival-Date: Tue,  2 Mar 2010 00:34:29 +0800 (SGT)


Final-Recipient: rfc822; root@example.com

Action: failed
```

```
Status: 5.4.6

Diagnostic-Code: X-Postfix; mail for example.com loops back to myself


--A144028083.1267461269/ubuntu.example.com

Content-Description: Undelivered Message

Content-Type: message/rfc822


Received: by ubuntu.example.com (Postfix, from userid 1001)

            id A144028083; Tue,  2 Mar 2010 00:34:29 +0800 (SGT)

Subject: USA idol

To: <root@example.com>

X-Mailer: mail (GNU Mailutils 1.2)

Message-Id: <20100301163429.A144028083@ubuntu.example.com>

Date: Tue,  2 Mar 2010 00:34:29 +0800 (SGT)

From: ismail@mail.example.com (ismail)


Winner


--A144028083.1267461269/ubuntu.example.com--

&
```

SOLVED:How to Send Mails to username@example.com

To be able to send mails to username@example.com instead of username@mail.example.com you will need to check that the directive mydestination has the value example.com and not mail.example.com. It's simple as that. In my case the mydestination directive looks like this:

mydestination = example.com, ismail-laptop, localhost.localdomain, localhost

The Postfix main.cf configuration file has the following settings:

root@ismail-laptop:~# less /etc/postfix/main.cf |grep -v "^#" | more

```
smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
```

```
biff = no

append_dot_mydomain = no

readme_directory = no
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

myhostname = ubuntu.example.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = example.com, ismail-laptop, localhost.localdomain, localhost
relayhost =
mynetworks = 127.0.0.0/8, 172.16.0.0/16
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = ipv4
```

The BIND forward zone file looks like this:

```
;

; BIND data file for local loopback interface

;

$TTL    604800

@       IN      SOA     ns1.example.com. root.localhost. (

                        3         ; Serial
```

```
                604800         ; Refresh

                 86400         ; Retry

                2419200         ; Expire

                604800 )        ; Negative Cache TTL

;

        IN      NS      ns1.example.com.

        IN      MX      10 mail.example.com.

ns1     IN      A       172.16.0.2

mars    IN      A       172.16.0.1

ubuntu  IN      A       172.16.0.2

mail    IN      A       172.16.0.2



www     IN      CNAME   mars
```

In this example, user ismail will send mail to root@example.com and idris@example.com

```
# su - ismail

ismail@ismail-laptop:~$ mail -s "Stock Prices"

To: root@example.com

Cc: idris@example.com

Stocks Prices will be out
```

Press Ctrl+D to send the mail
Switch user to the respective users to see if the mails are received.

```
ismail@ismail-laptop:~$ su - idris
```

```
Password:

idris@ismail-laptop:~$ mailx

"/var/mail/idris": 3 messages 1 new

 R   1 root              Tue Mar  2 00:54  16/515   Breaking News

>N   3 ismail            Wed Mar  3 00:29  14/491   Stock Prices
```

```
Subject: Stock Prices

To: <root@example.com>

Cc: <idris@example.com>

Date: Wed,  3 Mar 2010 00:29:13 +0800 (SGT)

From: ismail@mail.example.com (ismail)



Stocks Prices will be out
```

```
# su – root
#mailx
Subject: Stock Prices

To: <root@example.com>

Cc: <idris@example.com>

Date: Wed,  3 Mar 2010 00:29:13 +0800 (SGT)

From: ismail@mail.example.com (ismail)



Stocks Prices will be out
```

From the excerpts shown above, mails can be received for both root and user idris. So in this case we have solve the issue of sending mail to username@example.com instead of typing username@mail.example.com.

SOLVED: @example.com instead of @mail.example.com

Now if you look carefully at the mail the origin of the mail reads

From: ismail@mail.example.com (ismail)

We do not want to see @mail.example.com. What we want is to see @example.com. To solve this you will need to edit the following file.

vi /etc/mailname
example.com

It should read example.com instead of mail.example.com

How I knew that you need to change this file, is that when I look at the postfix configuration file, it has the following parameter

myorigin = /etc/mailname

Just experimenting

I tried to send to root@ubuntu.example.com. because I thought ubuntu is a CNAME to mail as configure in the forward zone DNS. I failed to send.

nslookup mail.example.com

Server: 127.0.0.1

Address: 127.0.0.1#53

mail.example.com canonical name = ubuntu.example.com.

Name: ubuntu.example.com

Address: 172.16.0.2

Why it failed? Eventhough ubuntu is a CNAME to mail, but the ubuntu.example.com entries that I saw in the logs as shown here, actually refers to the hostname in the main.cf configuration file.

From the Logs

Mar 2 00:54:05 ismail-laptop postfix/cleanup[14694]: C950D28083: message-id=<20100301165405.C950D28083@**ubuntu.example.com**>

From the main.cf configuration file

myhostname = ubuntu.example.com

If you change the myhostname directive value to something else, let's say whatever.example.com,

you will see it in the logs as shown below:

Mar 2 04:24:58 ismail-laptop postfix/cleanup[5633]: 70D8528083: message-id=<20100301202458.70D8528083@**whatever.example.com**>

But later I remove the cname to the mail and I could send mail to username@ubuntu.example.com

Sending another mail from root to another user

From user root to user idris

mail -s "Breaking News"

To: idris@mail.example.com

Cc:

Man escaped from zoo

Checking mail from user idris

root@ismail-laptop:~# su - idris

idris@ismail-laptop:~$ mailx

"/var/mail/idris": 1 message 1 new

>N 1 root Tue Mar 2 00:54 13/470 Breaking News

&

Subject: Breaking News

To: <idris@mail.example.com>

Date: Tue, 2 Mar 2010 00:54:05 +0800 (SGT)

From: root@mail.example.com (root)

Man escaped from zoo

&

From the /var/log/mail.log

```
Mar  2 00:54:05 ismail-laptop postfix/pickup[11736]: C950D28083: uid=0 from=<root>

Mar  2 00:54:05 ismail-laptop postfix/cleanup[14694]: C950D28083: message-
id=<20100301165405.C950D28083@ubuntu.example.com>

Mar  2 00:54:05 ismail-laptop postfix/qmgr[11737]: C950D28083: from=<root@mail.example.com>, size=368, nrcpt=1 (queue
active)

Mar  2 00:54:05 ismail-laptop postfix/local[14696]: C950D28083: to=<idris@mail.example.com>, relay=local, delay=0.06,
delays=0.03/0.01/0/0.02, dsn=2.0.0, status=sent (delivered to mailbox)

Mar  2 00:54:05 ismail-laptop postfix/qmgr[11737]: C950D28083: removed
```

Postfix Virtual Domain Hosting

Local files versus network databases

The examples in this text use table lookups from local files such as DBM or Berkeley DB. These are easy to debug with the **postmap** command:

> Example: `postmap -q info@example.com hash:/etc/postfix/virtual`

See the documentation in LDAP_README, MYSQL_README and PGSQL_README for how to replace local files by databases. The reader is strongly advised to make the system work with local files before migrating to network databases, and to use the **postmap** command to verify that network database lookups produce the exact same results as local file lookup.

> Example: `postmap -q info@example.com ldap:/etc/postfix/virtual.cf`

Virtual Alias Domains

The following segments include examples and how-to from the Postfix website

As simple as can be: shared domains, UNIX system accounts

The simplest method to host an additional domain is to add the domain name to the domains listed in the Postfix mydestination configuration parameter, and to add the user names to the UNIX password file.

This approach makes no distinction between canonical and hosted domains. Each username can receive mail in every domain.

In the examples we will use "example.com" as the domain that is being hosted on the local Postfix machine.

```
/etc/postfix/main.cf:
    mydestination = $myhostname localhost.$mydomain ... example.com
```

The limitations of this approach are:

- A total lack of separation: mail for info@my.host.name is delivered to the same UNIX system account as mail for info@example.com.
- With users in the UNIX password file, administration of large numbers of users becomes inconvenient.

Postfix virtual ALIAS example: separate domains, UNIX system accounts

With the approach described in this section, every hosted domain can have its own info etc. email address. However, it still uses UNIX system accounts for local mailbox deliveries.

With virtual alias domains, each hosted address is aliased to a local UNIX system account or to a remote address. The example below shows how to use this mechanism for the example.com domain.

In /etc/postfix/main.cf include the following:

```
#Pair No.1:This one works with using the 2 lines for virtual alias domains and m

aps

mydestination = $myhostname, localhost.localdomain, localhost, example.com



#Pair No.1:these 2 lines needed for virtual domain but still using local UNIX ac

cts

virtual_alias_domains = example.net, isa.net

virtual_alias_maps = hash:/etc/postfix/virtual
```

In /etc/postfix/virtual, type

```
# more /etc/postfix/virtual

info@example.net ismail@example.com

sales@example.net idris@example.com

@example.net tbr@example.com



info@isa.net ismail@example.com

custcare@isa.net idris@example.com
```

```
@isa.net tbr@example.com
```

what the configuration allows you to do

- you can send mail to virtual domains of example.net and isa.net

for the virtual domain example.net:

- mail sent to info@example.net will go to local user ismail@example.com
- mail sent to sales@example.net will go to local user idris@example.com
- mail sent to anything_else@example.net will go to local user tbr@example.com

similarly for the virtual domain isa.net:

- mail sent to info@isa.net will go to local user ismail@example.com
- mail sent to sales@isa.net will go to local user idris@example.com
- mail sent to anything_else@isae.net will go to local user tbr@example.com

Execute the command "**postmap /etc/postfix/virtual**" after changing the virtual file, and execute the command "**postfix reload**" after changing the main.cf file.

Note: virtual aliases can resolve to a local address or to a remote address, or both. They don't have to resolve to UNIX system accounts on your machine.

More details about the virtual alias file are given in the virtual(5) manual page, including multiple addresses on the right-hand side.

Virtual aliasing solves one problem: it allows each domain to have its own info mail address. But there still is one drawback: each virtual address is aliased to a UNIX system account. As you add more virtual addresses you also add more UNIX system accounts. The next section eliminates this problem.

The next section is similar to the one that is just discussed. **The only difference is that we use a separate files for domain and addresses**

In /etc/postfix/main.cf include the following:

```
#Pair No.2:this one is to work with the birdtual directory for virtual alias dom

ains

mydestination = $myhostname, localhost.localdomain, localhost, example.com, /e
```

```
tc/postfix/birdtual/domains



#Pair No.2:alternative to virtual alias maps and domains is to create birdtual d

irectory

virtual_maps = hash:/etc/postfix/birdtual/addresses
```

In /etc/postfix/birdtual/addresses, type

```
# more /etc/postfix/birdtual/addresses

cheeyong.net DOMAIN

@cheeyong.net idris@example.com



cheeyong.com DOMAIN

@cheeyong.com ismail@example.com
```

In /etc/postfix/birdtual/domains, type

```
# more /etc/postfix/birdtual/domains

cheeyong.com

cheeyong.net
```

what the configuration allows you to do

- you can send mail to virtual domains of cheeyong.net and cheeyong.com
- mail sent to anything@cheeyong.net will go to local user idris@example.com
- mail sent to anything@cheeyong.com will go to local user ismail@example.com

Execute the command "**postmap /etc/postfix/virtual**" after changing the virtual file, and execute the command "**postfix reload**" after changing the main.cf file.

Note: virtual aliases can resolve to a local address or to a remote address, or both. They don't have to resolve to UNIX system accounts on your machine.

More details about the virtual alias file are given in the virtual(5) manual page, including multiple

addresses on the right-hand side.

Virtual aliasing solves one problem: it allows each domain to have its own info mail address. But there still is one drawback: each virtual address is aliased to a UNIX system account. As you add more virtual addresses you also add more UNIX system accounts. The next section eliminates this problem.

Postfix virtual MAILBOX example: separate domains, non-UNIX accounts

As a system hosts more and more domains and users, it becomes less desirable to give every user their own UNIX system account.

With the Postfix virtual(8) mailbox delivery agent, every recipient address can have its own virtual mailbox. Unlike virtual alias domains, virtual mailbox domains do not need the clumsy translation from each recipient addresses into a different address, and owners of a virtual mailbox address do not need to have a UNIX system account.

The Postfix virtual(8) mailbox delivery agent looks up the user mailbox pathname, uid and gid via separate tables that are searched with the recipient's mail address. Maildir style delivery is turned on by terminating the mailbox pathname with "/".

If you find the idea of multiple tables bothersome, remember that you can migrate the information (once it works), to an SQL database. If you take that route, be sure to review the "local files versus databases" section at the top of this document.

In /etc/postfix/main.cf include the following:

```
#Pair No.3 for virtual mailbox

mydestination = $myhostname, localhost.localdomain, localhost, example.com



#Pair No.3 this is for non-UNIX accounts

virtual_mailbox_domains = example.net

virtual_mailbox_base = /var/mail/vhosts

virtual_mailbox_maps = hash:/etc/postfix/vmailbox
```

```
virtual_minimum_uid = 100

virtual_uid_maps = static:5000

virtual_gid_maps = static:5000

virtual_alias_maps = hash:/etc/postfix/virtual
```

You have to create the /var/mail/vhosts directory

```
root@ubuntu:mkdir /var/mail/vhosts
```

Then you have to create the example.net directory.

```
root@ubuntu:/var/mail/vhosts# mkdir example.net
```

Under the example.net directory make the users files. In my case I have the info, sales and catchall users.

```
root@ubuntu:/var/mail/vhosts/example.net/# touch info sales catchall
```

If you run the tree command under vhosts directory, you will have:

```
# tree vhosts/

vhosts/

`-- example.net

   |-- catchall

   |-- info

   `-- sales



1 directory, 3 files
```

After this you have to create a user with a UID of 5000 and GID 5000. This is because in the main.cf file we have already declared the following:

```
virtual_uid_maps = static:5000

virtual_gid_maps = static:5000
```

In my case I created a user called myexample with a UID of 5000 as shown below:

#useradd -u 5000 -m myexample

Check the newly created user in the /etc/passwd file

grep myexample /etc/passwd

myexample:x:5000:5000::/home/myexample:/bin/bash

Then you need to change the ownerships of the directories and files of the /var/mail/vhosts so that they belong to user myexample and group myexample.

chown -R myexample.myexample vhosts/

Check that the vhosts directory is owned by user and group myexample

ll /var/mail/vhosts/

total 4

drwxr-sr-x 2 myexample myexample 4096 2010-03-11 16:48 example.net

Also check the files info, sales and catchall also belong to user myexample.

ll /var/mail/vhosts/example.net/*

-rw-r--r-- 1 myexample myexample 498 2010-03-11 17:04 /var/mail/vhosts/example.net/catchall

-rw-r--r-- 1 myexample myexample 4939 2010-03-11 17:04 /var/mail/vhosts/example.net/info

-rw-r--r-- 1 myexample myexample 512 2010-03-11 17:04 /var/mail/vhosts/example.net/sales

Execute the command "**postmap /etc/postfix/virtual**" after changing the virtual file, execute "**postmap /etc/postfix/vmailbox**" after changing the vmailbox file, and execute the command "**postfix reload**" after changing the main.cf file.

Note: mail delivery happens with the recipient's UID/GID privileges specified with

virtual_uid_maps and virtual_gid_maps. Postfix 2.0 and earlier will not create mailDIRs in world-writable parent directories; you must create them in advance before you can use them. Postfix may be able to create mailBOX files by itself, depending on parent directory write permissions, but it is safer to create mailBOX files ahead of time.

What this configuration allows you to do:

- creation of a virtual alias doamin called example.net.
- Mails sent to info@example.net will be sent to the info file i.e /var/mail/vhosts/example.net/info
- Mails sent to sales@example.net will be sent to the sales file i.e /var/mail/vhosts/example.net/sales
- Mails sent to anything@example.net will be sent to the catchall file i.e /var/mail/vhosts/example.net/catchall

Installing Dovecot

We will be using Dovecot as the IMAP server. Postfix and Dovecot works nicely.

apt-get install dovecot-imapd dovecot-pop3d

Let's configure the dovecot configuration file. But make sure you make a backup copy of the file first.

root@ubuntu:~# cd /etc/dovecot/

root@ubuntu:/etc/dovecot# vi dovecot.conf

In my case I have configured the following lines but in actual fact you don't need to configure much. Just take note the lines in bold.

```
protocols = imap imaps pop3 pop3s

disable_plaintext_auth = no

log_timestamp = "%Y-%m-%d %H:%M:%S "

mail_location = maildir:~/Maildir

mail_privileged_group = mail

protocol imap {

}

protocol pop3 {

  pop3_uidl_format = %08Xu%08Xv

}

protocol managesieve {

  sieve=~/.dovecot.sieve

  sieve_storage=~/sieve

}

auth default {

  mechanisms = plain

  passdb pam {

  }

  userdb passwd {

  }
```

```
  user = root
}

dict {
}
plugin {
}
```

Let me explain what the following lines mean

disable_plaintext_auth = no

The line above mean that plaintext authentication is allow. This is use when mail client access mails and need to provide password. I will discuss further on this at the next secion.

The following line is also important.

mail_location = maildir:~/Maildir
This line means that mails will be stored in the **/home/user/Maildir** directory. The directory is created once mail is sent to the user. I will discuss this further at the next section.

After you have edit the configuration file, you will need to restart the dovecot process by typing:

root@ubuntu:~# /etc/init.d/./dovecot restart

Real Life Situations

One day I could not use mail. I tested using the mail client and it gave me error message. I then telnet to the imap server using telnet ubuntu.example.com 110 and it failed. I also tried to restart the postfix and dovecot processes but that too did not resolve the issue. In the end I had to reboot the mail server and after which I chcked the dovecot process and they are running as shown below.

```
# ps -ef|grep dovecot
root      4822     1  0 20:29 ?        00:00:00 /usr/sbin/dovecot
root      4841  4822  0 20:29 ?        00:00:00 dovecot-auth
root      4845  4822  0 20:29 ?        00:00:00 dovecot-auth -w
dovecot   5025  4822  0 20:29 ?        00:00:00 pop3-login
```

```
dovecot   5027  4822  0 20:29 ?        00:00:00 imap-login

dovecot   5028  4822  0 20:29 ?        00:00:00 imap-login

dovecot   5029  4822  0 20:29 ?        00:00:00 imap-login

dovecot   6121  4822  0 20:30 ?        00:00:00 pop3-login

dovecot   6223  4822  0 20:31 ?        00:00:00 pop3-login
```

I am also able to telnet to the imap server. With that I am able to use mail again. It's funny how I am unable to restart the dovecot process and had to reboot the server.

You will also need to add in the following line in the postfix configurationo file.

root@ubuntu:~# vi /etc/postfix/main.cf

home_mailbox = Maildir/

That's it. Restart postfix process.

Note
You can test if your IMAP server is working by typing:

```
# telnet ubuntu.example.com 110

Trying 127.0.0.1...

Connected to ubuntu.example.com.

Escape character is '^]'.

+OK Dovecot ready.
```

Replace the mail server with your own mail server name. You can also use IP address.
Type quit to exit the telnet session.

Now let's configure the mail client.

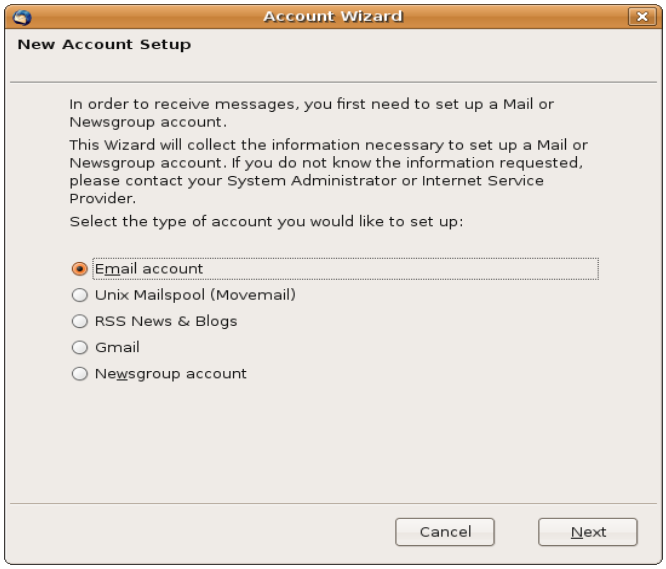
Configuration of Mail Client Using Evolution Mail

There are many mail clients availablebut in this section, users will read mails using Evolution Mail. There are some configuration before a user can read his mail. Below are the steps

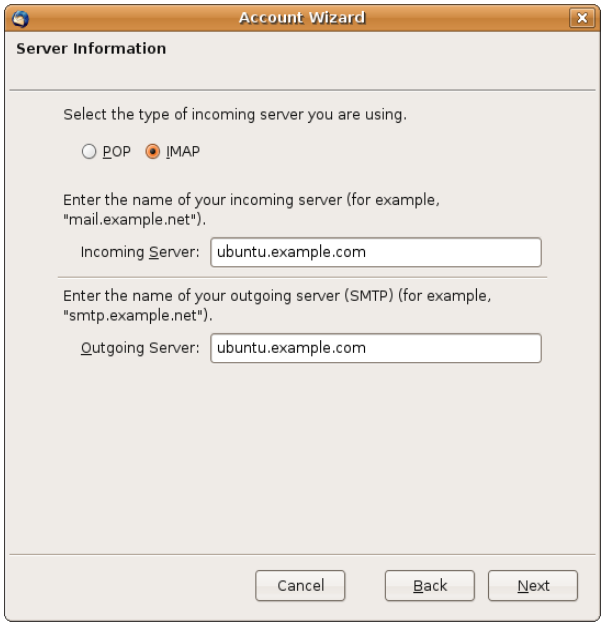
1. Launch Evolution Mail
2. Create a user account

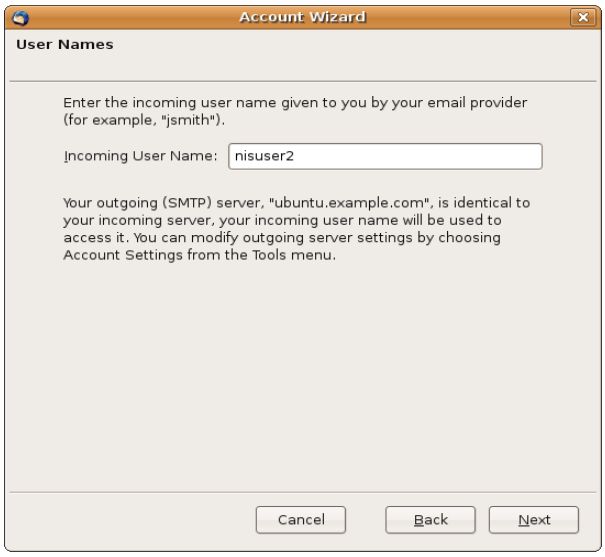
3. You can use the wizard to do this In the Identity section, provide the user's mail address e.g. ismail@example.com
4. In the Receiving Section, select IMAP as the server type. Type in the mail server in the server field. In my case, it's ubuntu.example.com
5. In the receiving Options section accept the default values.
6. In the Sending Email section the server type is SMTP and key in your mail server. In my case it's ubuntu.example.com
7. In the Account Mangement section, accept the default values.
8. Lastly click Done button and this complete the creation of a mail account. To start using the mail client, you will need to log in to the IMAP logon window using the user account login password.

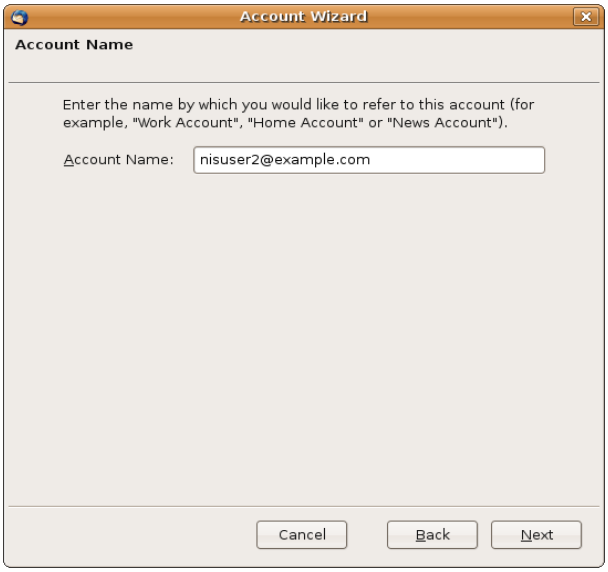
Below are the screenshots on how to configure the e-mail client using Mozilla Thunderbird.

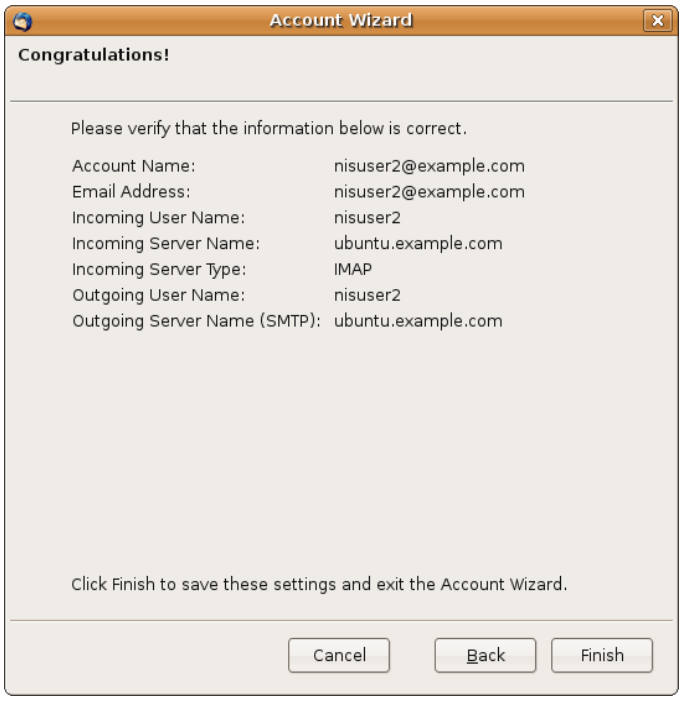


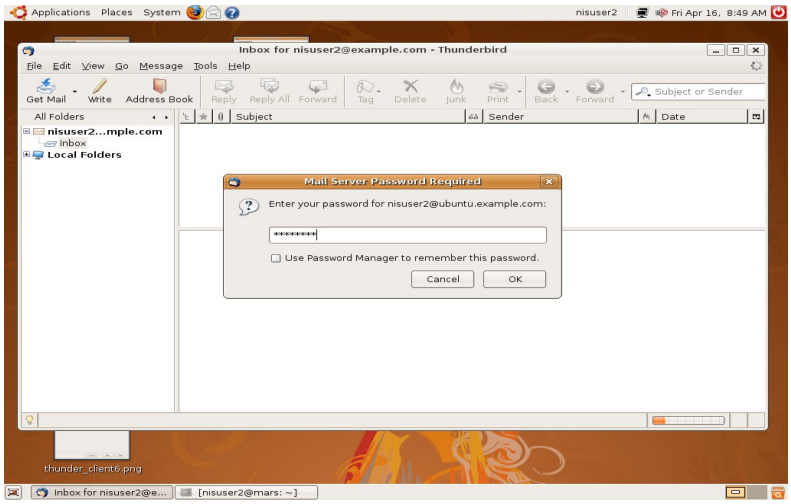

Account Wizard
Identity
Each account has an identity, which is the information that identifies you to others when they receive your messages.
Enter the name you would like to appear in the "From" field of your outgoing messages (for example, "John Smith").
Your Name:
nisuser2
Enter your email address. This is the address others will use to send email to you (for example, "user@example.net").
Email Address:
nisuser2@example.com
Cancel
Back
Next

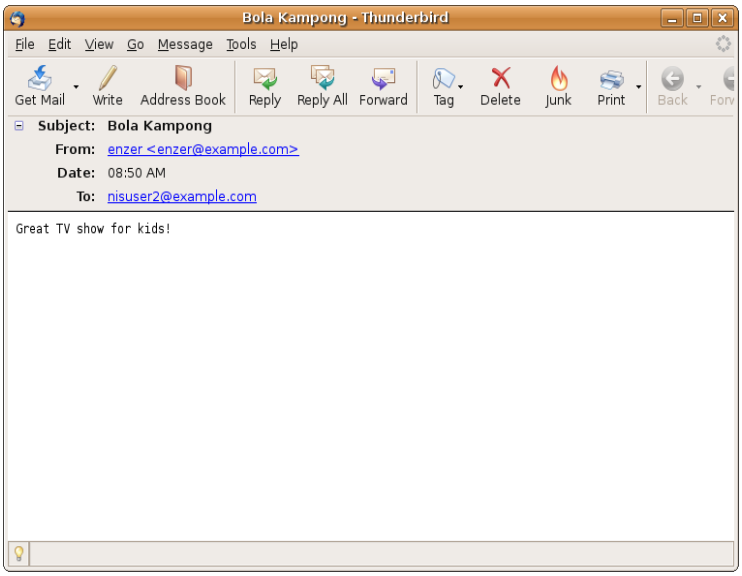

Account Wizard
Server Information
Select the type of incoming server you are using.
POP
IMAP
Enter the name of your incoming server (for example, "mail.example.net").
Incoming Server:
ubuntu.example.com
Enter the name of your outgoing server (SMTP) (for example, "smtp.example.net").
Outgoing Server:
ubuntu.example.com
Cancel
Back
Next


Account Wizard
User Names
Enter the incoming user name given to you by your email provider (for example, "jsmith").
Incoming User Name:
nisuser2
Your outgoing (SMTP) server, "ubuntu.example.com", is identical to your incoming server, your incoming user name will be used to access it. You can modify outgoing server settings by choosing Account Settings from the Tools menu.
Cancel
Back
Next

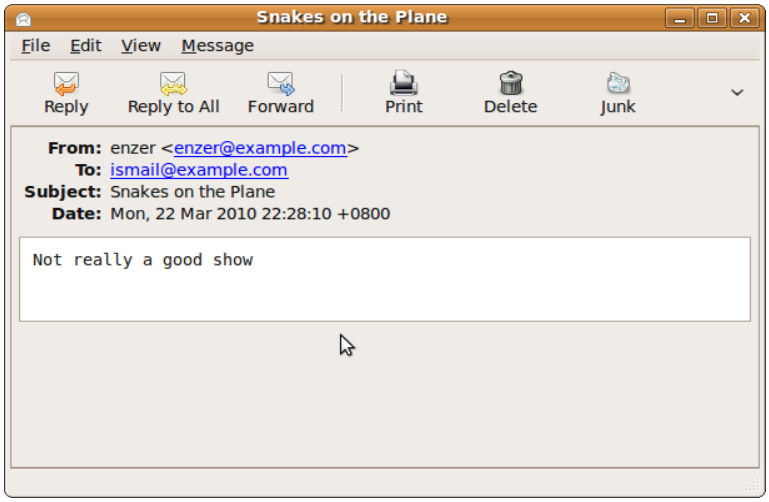

Account Wizard
Account Name
Enter the name by which you would like to refer to this account (for example, "Work Account", "Home Account" or "News Account").
Account Name:
nisuser2@example.com
Cancel
Back
Next


Account Wizard
Congratulations!
Please verify that the information below is correct.
Account Name: nisuser2@example.com
Email Address: nisuser2@example.com
Incoming User Name: nisuser2
Incoming Server Name: ubuntu.example.com
Incoming Server Type: IMAP
Outgoing User Name: nisuser2
Outgoing Server Name (SMTP): ubuntu.example.com
Click Finish to save these settings and exit the Account Wizard.
Cancel
Back
Finish


Applications Places System
nisuser2
Fri Apr 16, 8:49 AM
Inbox for nisuser2@example.com - Thunderbird
File Edit View Go Message Tools Help
Get Mail Write Address Book Reply Reply All Forward Tag Delete Junk Print Back Forward
Subject or Sender
All Folders
nisuser2...mple.com
Inbox
Local Folders
Subject Sender Date
Mail Server Password Required
Enter your password for nisuser2@ubuntu.example.com:
Use Password Manager to remember this password.
Cancel
OK
thunder_client6.png
Inbox for nisuser2@e...
[nisuser2@mars: ~]



A screenshot of a mail from user enzer@example.com to the newly created user ismail@example.com. Also included are the logs from the mail server.



The mail server logs:

1. Mar 22 22:27:24 ubuntu dovecot: imap-login: Login: user=<enzer>, method=PLAIN, rip=127.0.0.1, lip=127.0.0.1, secured

2. Mar 22 22:27:27 ubuntu dovecot: imap-login: Login: user=<ubuntuuser>, method=PLAIN, rip=127.0.0.1,

```
lip=127.0.0.1, secured

3. Mar 22 22:27:31 ubuntu dovecot: imap-login: Login: user=<ismail>, method=PLAIN, rip=127.0.0.1,
   lip=127.0.0.1, secured

4. Mar 22 22:28:11 ubuntu postfix/smtpd[8480]: connect from ubuntu.example.com[127.0.0.1]

5. Mar 22 22:28:11 ubuntu postfix/smtpd[8480]: D16D728135: client=ubuntu.example.com[127.0.0.1]

6. Mar 22 22:28:11 ubuntu postfix/cleanup[8484]: D16D728135: message-
   id=<1269268090.8402.0.camel@ubuntu.example.com>

7. Mar 22 22:28:11 ubuntu postfix/qmgr[4414]: D16D728135: from=<enzer@example.com>, size=505, nrcpt=1
   (queue active)

8. Mar 22 22:28:11 ubuntu postfix/local[8485]: D16D728135: to=<ismail@example.com>, relay=local,
   delay=0.13, delays=0.06/0.02/0/0.05, dsn=2.0.0, status=sent (delivered to maildir)

9. Mar 22 22:28:11 ubuntu postfix/qmgr[4414]: D16D728135: removed
```

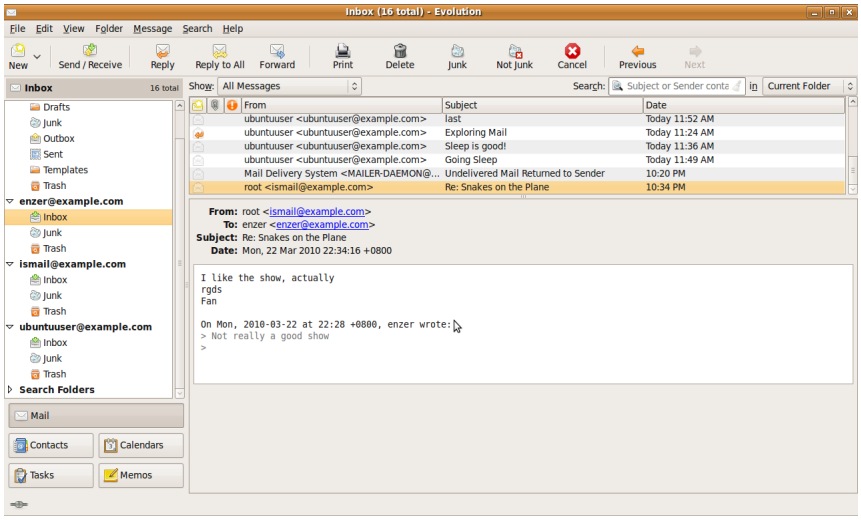
Lines 1 to 3, shows that the users, enzer, ubuntuuser and ismail are logging into the IMAP server using their UNIX account passwords. This example shows that you will require UNIX user accounts on the mail server. All mails are stored in the mail server under the /home/user/Maildir directory. But these accounts can also be transparent to the users meaning that the Administrator simply create these accounts on the mail server but they will not be able to login locally or remotely by ssh, telnet,etc. The administrator create such user accounts by specifying the -s /bin/false to the useradd command as shown below

#useradd -m -s /bin/false username

You can also connect another machine or laptop to the mail server in a LAN and acces your mail from remote hosts. Simply configure the mail client as discussed earlier on the remote machine and you can access your mails.

Lines 4 to 9 shows the sending and receiving of mails. It includes the hosts IP addresses and the usernames.

Below is a screenshot of the mail client Evolution Mail on the mail server. I configured several users mail accounts



Get Notification via E-mail

You can use the MAILTO variable to notify you via e-mail when a cron job is run. Simply add

MAILTO="enzer@example.com" to route messages associated with that script to that e-mail address. In my case my cron entries look like this:

47 16 * * * df -h | mail -s "Disk Free" ismail@example.com

Configuring Virtual Web Hosting Using Apache

Firstly you need to install Apache 2

Installing Apache 2

#apt-get install apache2

Once these are setup you should be able to connect to localhost in your browser and see a test page.

NameVirtualHost

Name-based virtual hosting means that a single server can host multiple sites

My preferred method of using name based virtual hosting is creating a seperate file for each domain. These can all be done within one file, but I'll be creating a new file for each site.

First we need to define to Apache that we're using name based virtual hosting instead of IP based. You can append the following line to your */etc/apache2/apache2.conf* to define this:

```
NameVirtualHost ip.address:port
```

In my case it looks like this:

#I added this for Name Virtual Host

NameVirtualHost 172.16.0.2:80

Debian and Ubuntu use */etc/apache2/sites-available/* and */etc/apache2/sites-enabled/* directories for defining virtual hosting.

One nice thing about this is that you can have more sites “available” than you have “enabled”, meaning not everything configured is actually live and listening. This is nice to quickly disable a site for whatever reason.

I like to create unique files for each of my domains within the */etc/apache2/sites-available/* folder.

```
root@ubuntu:~# cd /etc/apache2/sites-available/

root@ubuntu:/etc/apache2/sites-available# ll

total 16

-rw-r--r-- 1 root root  167 2010-03-14 17:34 cheeyong.com

-rw-r--r-- 1 root root  948 2009-08-18 22:24 default

-rw-r--r-- 1 root root 7364 2009-08-18 22:24 default-ssl
```

For example I have a file called “cheeyong.com” in that directory, with the following contents:

```
root@ubuntu:/etc/apache2/sites-available# more cheeyong.com

<VirtualHost 172.16.0.2:80>

ServerName cheeyong.com

ServerAlias www.cheeyong.com

ServerAdmin ismail@example.com

DocumentRoot /var/www/cheeyong.com/html

</VirtualHost>
```

What these settings do is as follows:

- ServerName listens for requests asking for a certain domain
- ServerAlias defines any additional domains that should match
- ServerAdmin is the contact for the site
- DocumentRoot is the path to the content for that site

Now that this file is created in the */etc/apache2/sites-available/* folder we're just about ready to start, but we need to enable it. We can do that by creating a symbolic link from one folder to the next.

```
#cd /etc/apache2/sites-enabled/
#ln -s ../sites-available/cheeyong.com
```

This site is now available (as in configured) and enabled (as in listening) once we restart the apache service:

```
sudo /etc/init.d/apache2 restart
```

DNS Configuration

I also include a DNS domain entry for each virtual web site. In my case I have two virtua web sites; example.com and cheeyong.com.

The main named DNS zone file

```
# more /etc/bind/named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "example.com" {
type master;
file "/etc/bind/db.example.com";
};

zone "cheeyong.com" {
type master;
file "/etc/bind/db.cheeyong.com";
};
```

```
# This is the zone definition for reverse DNS. replace 0.168.192 with your netwo
rk address in reverse notation - e.g my network address is 172.16
zone "16.172.in-addr.arpa" {
type master;
file "/etc/bind/db.16.172";
};
```

The forward zone file for the cheeyong.com domain

more /etc/bind/db.cheeyong.com

```
;
; BIND data file for local loopback interface
;
$TTL  604800
@     IN    SOA   ns1.cheeyong.com. root.localhost. (
                        3           ; Serial
                   604800           ; Refresh
                    86400           ; Retry
                  2419200           ; Expire
                   604800 )   ; Negative Cache TTL
;
      IN    NS    ns1.cheeyong.com.
      IN    MX    10 mail.example.com.
ns1   IN    A     172.16.0.2
mars  IN    A     172.16.0.2
ubuntu      IN    A     172.16.0.2
mail  IN    A     172.16.0.2
www   IN    CNAME mars
```

I did not include a reverse zone file for this domain. But here I included a sample of the reverse zone file of the example.com doman.

```
# more /etc/bind/db.16.172
;
; BIND reverse data file for local loopback interface
;
```

```
$TTL  604800
@     IN    SOA   ns1.example.com. root.localhost. (
                        1           ; Serial
                   604800           ; Refresh
                    86400           ; Retry
                  2419200           ; Expire
                   604800 )   ; Negative Cache TTL
;
@     IN    NS    ns1.example.com.
2.0   IN    PTR   ns1.example.com.
1.0   IN    PTR   mars.example.com.
1.0   IN    PTR   www.example.com.
2.0   IN    PTR   mail.example.com.
2.0   IN    PTR   ubuntu.example.com.
```

A tree command run on the directory /etc/bind

```
# tree /etc/bind
/etc/bind
|-- db.0
|-- db.127
|-- db.16.172
|-- db.255
|-- db.cheeyong.com
|-- db.empty
|-- db.example.com
|-- db.local
|-- db.root
|-- named.conf
|-- named.conf.bkp
|-- named.conf.local
|-- named.conf.local.bkp
|-- named.conf.options
|-- rndc.key
`-- zones.rfc1918
```

Testing

To test your configuration you can, temporarily, configure your */etc/hosts* file to point the domain to your IP address and see if your server loads up the correct site. This is only needed if the hostname or domain name does not already resolve to your IP address. Editing the */etc/hosts* by adding the following line:

```
ip.address domain.tld
```

Open your browser, try to access domain.tld and see if it loads the contents from your local DocumentRoot (from the configuration above). You might want to drop a file in the DocumentRoot to verify its pulling your local content.

```
#cd /var/www/ubuntu-tutorials.com/html
#echo "Hello World" > index.html
```

In my case I did not include the ip.address domain.tld in my /etc/hosts because I have already got DNS to work.

To create the test web page, you can use OpenOffice Word and save the file as index.html

This is a sample of the webpage www.cheeyong.com

Configuring Virtual Web Site for example.com

Copy the 000-default file to the new virtual web site.

root@ubuntu:/etc/apache2/sites-enabled# cp 000-default example.com

Create web page and logging directories:

root@ubuntu:~# mkdir /var/www/example.com

root@ubuntu:~# mkdir /var/log/apache2/example.com

Open example.com file and enter the following directive

root@ubuntu:~# cd /etc/apache2/sites-enabled/

```
root@ubuntu:/etc/apache2/sites-enabled# cat example.com
<VirtualHost *:80>
	ServerName example.com
	ServerAlias www.example.com
	ServerAdmin ismail@example.com

	DocumentRoot /var/www/example.com
	<Directory />
		Options FollowSymLinks
		AllowOverride None
	</Directory>
	<Directory /var/www/example.com>
		Options Indexes FollowSymLinks MultiViews
		AllowOverride None
		Order allow,deny
		allow from all
	</Directory>

	ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
	<Directory "/usr/lib/cgi-bin">
		AllowOverride None
		Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
		Order allow,deny
		Allow from all
```

```
        </Directory>


        ErrorLog /var/log/apache2/example.com


        # Possible values include: debug, info, notice, warn, error, crit,
        # alert, emerg.
        LogLevel warn


        CustomLog /var/log/apache2/example.log combined


    Alias /doc/ "/usr/share/doc/"
    <Directory "/usr/share/doc/">
        Options Indexes MultiViews FollowSymLinks
        AllowOverride None
        Order deny,allow
        Deny from all
        Allow from 127.0.0.0/255.0.0.0 ::1/128
    </Directory>


</VirtualHost>
```

Add a simple web page like:

root@ubuntu:/var/www/example.com# cat index.html

Welcome to example.com Website!

Next you will need to configure the DNS to resolve the website name

The example.com zone file contains the following:

```
root@ubuntu:/etc/bind# cat db.example.com
;
; BIND data file for local loopback interface
```

```
;
$TTL  604800
@     IN    SOA   ns1.example.com. root.localhost. (
                        3          ; Serial
                   604800          ; Refresh
                    86400          ; Retry
                  2419200          ; Expire
                   604800 )  ; Negative Cache TTL
;
      IN    NS    ns1.example.com.
      IN    MX    10 mail.example.com.
ns1   IN    A     172.16.0.2
mars  IN    A     172.16.0.1
ubuntu      IN    A     172.16.0.2
mail  IN    A     172.16.0.2
www   IN    A     172.16.0.2
```

The local zone file have the following entries:

```
root@ubuntu:/etc/bind# cat named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

```
zone "example.com" {

type master;

file "/etc/bind/db.example.com";

};


zone "cheeyong.com" {

type master;

file "/etc/bind/db.cheeyong.com";

};


zone "ismail.com" {

type master;

file "/etc/bind/db.cheeyong.com";

};


# This is the zone definition for reverse DNS. replace 0.168.192 with your
network address in reverse notation - e.g my network address is 172.16


zone "16.172.in-addr.arpa" {

type master;

file "/etc/bind/db.16.172";

};
```

From the ouput above, pay attention to the lines that are in bold. The domain example.com has its own DNS entry but if you look at the domain, ismail.com, it is included in the cheeyong.com domain. For the virtual site www.ismail.com, the name server is ns1.cheeyong.com as shown below.

```
root@ubuntu:/etc/bind# cat db.cheeyong.com

;

; BIND data file for local loopback interface

;
```

```
$TTL  604800

@     IN    SOA   ns1.cheeyong.com. root.localhost. (

                        3           ; Serial

                   604800           ; Refresh

                    86400           ; Retry

                  2419200           ; Expire

                   604800 )   ; Negative Cache TTL

;

      IN    NS    ns1.cheeyong.com.

      IN    MX    10 mail.example.com.

ns1   IN    A     172.16.0.2

www   IN    A     172.16.0.2

ubuntu      IN    A     172.16.0.2

mail  IN    A     172.16.0.2


www.ismail.com    IN    A     172.16.0.2
```

This means that you can have many virtual web sites in one name server.

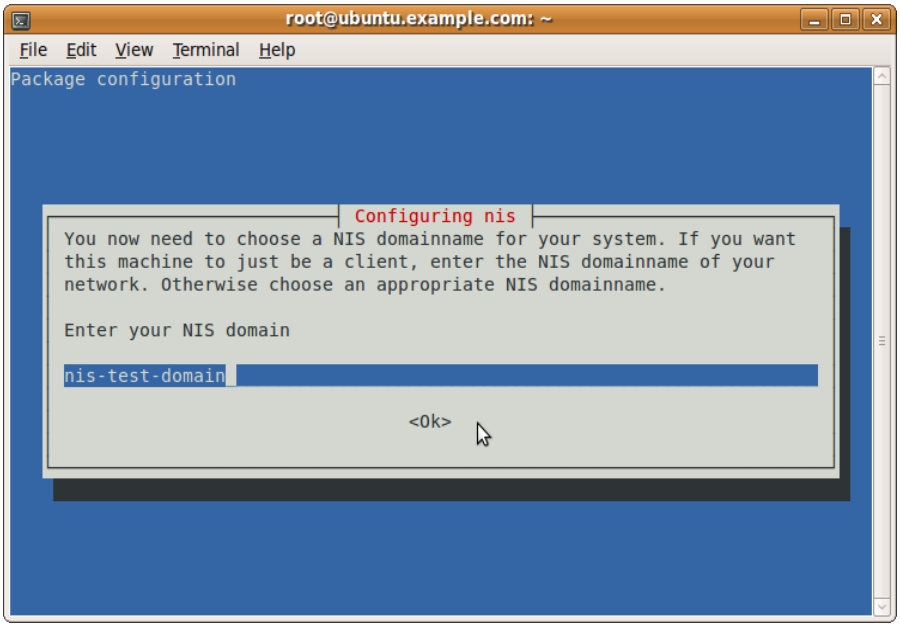
Exploring NIS in Ubuntu

NIS is use to maintain the same usernames and passwords on every client. NIS is a very useful tool for centralized login management but the password information passes over the network unencrypted. NIS is independent of NFS (file sharing) although the two are often hosted on a single server.

Installation of NIS Server

NIS client and server are included into a single package. To install NIS on the Ubuntu server type:

apt-get install nis



* Setting NIS domainname to: nis-test-domain

- Starting NIS services
- * binding to YP server... * .... * .... * ....

There are several configuration files needed to be configured in Ubuntu. They are:

- /etc/defaultdomain
- /etc/default/nis
- /etc/ypserv.conf
- /etc/ypserv.securenets

Other than tweaking the configuration files above, you will need to explore the contents of the following file:

- /var/yp/Makefile

Editing the /etc/defaultdomain file

Firstly edit the /etc/defaultdomain. You can manually edit this file and it is very simple. It basically contains one line i.e. In this file you will type the domain name of the NIS system on the local network. Alternatively, to edit the file, you can also type **dpkg-reconfigure nis** command. If you chose to edit the file manually, you will need to restart nis by executing /etc/init.d/./nis restart. In my example, the /etc/defaultdomain file looks like this:

```
root@ubuntu:~# cat /etc/defaultdomain

nis-test-domain
```

*In **Fedora and Red Hat** you will need to specify the NIS domain name in the /etc/sysconfig/network configuration file:*

NISDOMAIN=nisdomainname

Next edit the /etc/default/nis file.

Editing the /etc/default/nis file

In Ubuntu, you can specify if this machine will be a NIS server or client by simply editing some of the directives in this configuration file.

But first make a backup copy of the /etc/default/nis file.

cp -p nis nis.bak

Now edit the following directives. Change the NISSERVER value to master.

NISSERVER=master

The NISCLIENT parameter should be set to true for NIS clients and also NIS server. An NIS server can also be a NIS client. Thus set the following directive is set to true even for a NIS server.

NISCLIENT=true

Optional:

Some administrators allow clients to change personal information associated with their account like their comment field and the type of shell (e.g. Bash, Bourne shell, etc). The directive YPCHANGEOK allows such changes. The default value in my case is shown below:

YPCHANGEOK=chsh

Such value to the directive allows user to change their shell. You can also add chfn to allow clients to change their comments field.

YPCHANGEOK=chsh,chfn

Editing the /etc/ypserv.conf file

I did not edit anything here. This file requires no editing, but some directives here are meant to promote security. But a better approach is to to edit the /etc/ypserv.securenets configuration file. The directives here are formatted in four columns, separated by four colons:

- Host – Corresponds to the allowed IP addresses such as 192.168.0.1,10.0.0.0/255.0.0.0 and 172.16.0.0/16
- Domain – Specifies the NIS domain name
- Map – Corresponds to the database in the /var/yp configuration file
- Security – Corresponds to access limits. If set to none always allows access. If port allows access on ports below 1024 and deny; which always denies access.

The defaults settings is shown below.

```
# This is the default - restrict access to the shadow password file,

# allow access to all others.

*                           : *       : shadow.byname    : port

*                           : *       : passwd.adjunct.byname : port

*                           : *       : *                : none
```

*In **Fedora and Red Hat***
The following grants access to anyone logging in from IP address in the range of 192.168.0.1 to 192.168.0.255

192.168.0.1/24 : * : * :none

Editing the /etc/ypserv.securenets

I did not edit anything in this file.

You must include the local server as shown below:

```
255.0.0.0       127.0.0.0
```

You should delete the following line that is by default configured. But in my case, I just leave it.

```
# This line gives access to everybody. PLEASE ADJUST!
0.0.0.0        0.0.0.0
```

As the comments points out that the line gives access to anyone. This means that unauthorized systems can send RPC requests to the NIS server and retrieve the NIS maps.

But if you delete the line, don'f forget to include the IP address of the NIS server! To accept NIS requests from certain hosts, you can type the following formats:

host 192.168.0.152

In Fedora and Red Hat
The formats are written as:

#accept requests from 192.168.0.1 to 192.168.0.62
255.255.255.192 192.168.0.0
#accept requests starting with 192.168.14
255.255.255.0 192.168.14.0

Building the Database Maps

The ypinit needs only to run on the NIS server and not on the NIS clients. The -m option with the ypinit will create the **domain** subdirectory under **/var/yp** directory. So in my case if I run the tree command under /var/yp, I will see the domain directory.

```
root@ubuntu:/var/yp# tree
.
|-- Makefile
|-- binding
|   |-- nis-test-domain.1
|   `-- nis-test-domain.2
|-- nicknames
```

```
|-- nis-test-domain
|   |-- group.bygid
|   |-- group.byname
|   |-- hosts.byaddr
|   |-- hosts.byname
|   |-- netgroup
|   |-- netgroup.byhost
|   |-- netgroup.byuser
|   |-- netid.byname
|   |-- passwd.byname
|   |-- passwd.byuid
|   |-- protocols.byname
|   |-- protocols.bynumber
|   |-- rpc.byname
|   |-- rpc.bynumber
|   |-- services.byname
|   |-- services.byservicename
|   |-- shadow.byname
|   `-- ypservers
`-- ypservers


2 directories, 23 files
```

Now the econfigured Makefile (var/yp/Makefile) can be used to process the files you want to share into a database map. You need to type the following:

```
# /usr/lib/yp/ypinit -m
At this point, we have to construct a list of the hosts which will run NIS
servers.  ubuntu.example.com is in the list of NIS server hosts.  Please continue to add
the names for the other hosts, one per line.  When you are done with the
list, type a <control D>.
       next host to add:  ubuntu.example.com
       next host to add:
```

```
I typed control-D

The current list of NIS servers looks like this:

ubuntu.example.com

Is this correct?  [y/n: y]  y

We need a few minutes to build the databases...

Building /var/yp/nis-test-domain/ypservers...

Running /var/yp/Makefile...
```

```
ubuntu.example.com has been set up as a NIS master server.

The command ypinit -m processes files cited in /var/yp/Makefile into the
/var/yp/nis-test-domain directory.


Now you can run ypinit -s ubuntu.example.com on all slave server.
```

Future changes to any files of the shadow password suite can be added to the NIS database with the following command:

```
make -C /var/yp
```

```
If you encountered errors, you can check if the /etc/resolv.conf is set correctly.
Just make sure your /etc/resolv.conf is set to the correct DNS server

# vi /etc/resolv.conf
nameserver 172.16.0.2


Also check that your eth0 is set to the correct IP address. If not here is how you
configure eth0 interface

# vi /etc/network/interfaces
auto eth0

iface eth0 inet static

address 172.16.0.2

netmask 255.255.0.0

gateway 172.16.0.1

If you need to restart the networking process, type:
# /etc/init.d/./networking restart
```

You may want to restart portmap and nis.

```
root@ubuntu:~# /etc/init.d/./portmap restart

 * Stopping portmap daemon...                                  [ OK ]

 * Starting portmap daemon...                                 [ OK ]


root@ubuntu:/etc/init.d# /etc/init.d/./nis restart

    • Starting NIS services                                    [ OK ]
```

Testing the NIS setup

Execute the ypwhich command which will return the name of the NIS server that supplies the NIS services to a NIS clients.

```
# ypwhich

ubuntu.example.com
```

From the NIS server,check that ypserv and ypbind is connected to portmap.

```
root@ubuntu:/etc/init.d# rpcinfo -u ubuntu.example.com ypserv

program 100004 version 1 ready and waiting

program 100004 version 2 ready and waiting


root@ubuntu:/etc/init.d# rpcinfo -u ubuntu.example.com ypbind

program 100007 version 1 ready and waiting

program 100007 version 2 ready and waiting
```

The ypbind existed as this NIS server is also a NIS client
The following command will yield the same output as the localhost is used for the server name.

```
root@ubuntu:/etc/init.d# rpcinfo -u localhost ypbind

program 100007 version 1 ready and waiting

program 100007 version 2 ready and waiting
```

Check that the ypserv is connected to portmap
rpcinfo -p | grep ypserv

```
    100004    2   udp    746  ypserv

    100004    1   udp    746  ypserv

    100004    2   tcp    747  ypserv

    100004    1   tcp    747  ypserv
```

On the NIS server, you may want to run the following command. It prints a list of all registered RPC programs on the localhost.

```
root@ubuntu:~# rpcinfo -p localhost

   program vers proto   port

    100000    2   tcp    111  portmapper

    100000    2   udp    111  portmapper

    100024    1   udp  44434  status

    100024    1   tcp  55464  status

    100004    2   udp    607  ypserv

    100004    1   udp    607  ypserv

    100004    2   tcp    608  ypserv

    100004    1   tcp    608  ypserv

    100009    1   udp    610  yppasswdd

 600100069    1   udp    613  fypxfrd

 600100069    1   tcp    614  fypxfrd

    100007    2   udp    620  ypbind

    100007    1   udp    620  ypbind

    100007    2   tcp    621  ypbind

    100007    1   tcp    621  ypbind

    100003    2   udp   2049  nfs

    100003    3   udp   2049  nfs

    100003    4   udp   2049  nfs

    100021    1   udp  49482  nlockmgr

    100021    3   udp  49482  nlockmgr
```

```
    100021    4   udp  49482  nlockmgr
    100021    1   tcp  46772  nlockmgr
    100021    3   tcp  46772  nlockmgr
    100021    4   tcp  46772  nlockmgr
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100005    1   udp  48006  mountd
    100005    1   tcp  46911  mountd
    100005    2   udp  48006  mountd
    100005    2   tcp  46911  mountd
    100005    3   udp  48006  mountd
    100005    3   tcp  46911  mountd
```

Troubleshooting Tip . . .

If the server is not working properly, stop the ypserv process and start it again with debugging on as shown below:

```
root@ubuntu:~# /usr/sbin/ypserv –debug
```

The –debug option keeps ypserv in the foreground and causes it to send error messages and debugging output to standard error.

Configuring the NIS client

You need to install the NIS package on the NIS client,

#apt-get install portmap nis

Set the following directives in the /etc/default/nis configuration file

```
NISSERVER=false
NISCLIENT=true
```

Edit the `/etc/yp.conf` to Specify an NIS Server (only for NIS client)

On the NIS client, edit the /etc/yp.conf file

root@ubuntu:/etc# vi yp.conf

You can type using the following formats:
ypserver server_name
ypserver *IP_Address_Of_NIS_Server*

Problems may occur when an NIS client searches for an NIS server, especially when there are problems with name resolutions (DNS). Thus it is better to have a fixed IP address for the NIS server. You can try using either one of the following formats:

```
root@ubuntu:/etc# vi yp.conf

domain nis-test-domain server ubuntu.example.com
```

or

```
domain nis-test-domain server 172.16.0.2
```

or

ypserver 172.16.0.2

In my case I tested all formats and both work. The first format requires that your DNS is able to resolve the hostname. In case your DNS is not working you should include the host IP mappings in the /etc/hosts file in the NIS clients. Edit the /etc/hosts and include your server IP address. In my case I have already have DNS working. So this addition is just in case the DNS fail to resolve the NIS server.

```
172.16.0.2      ubuntu.example.com
```

The nsswitch.conf File

The Network Services switch file /etc/nsswitch.conf determines the order of lookups performed when a certain piece of information is requested, just like the /etc/host.conf file which determines the way host lookups are performed. For example, the line

```
hosts: files nis dns
```

Specifies that host lookup functions should first look in the local /etc/hosts file, followed by a NIS lookup and finally through the domain name service (/etc/resolv.conf and named), at which point if no match is found an error is returned. This file must be readable for every user.

passwd_compat, group_compat and shadow_compat are only supported by glibc 2.x.

On an NIS client system, check the /etc/nsswitch.conf configuration file. By default, the following directives read the local password database first.

```
passwd:         compat

group:          compat

shadow:         compat
```

Options:

- compat: Use compatibility setup
- nisplus: Use NIS+ (NIS version 3)
- nis: Use NIS (NIS version 2), also called YP
- dns: Use DNS (Domain Name Service)
- files: Use the local files `/etc/passwd, /etc/group, ...`

In my case the /etc/nsswitch.conf configration file on the NIS client looks like this:

```
passwd: nis files
group: nis files
shadow: nis files
```

If you reverse the files and nis, locally available users can log in more quickly.

Testing NIS Client

You can use the nisdomainname to set or view the NIS domain name, but setting it in this way does not maintain the name when the system reboots.

```
# nisdomainname

nis-test-domain
```

Check that the NIS client connects to the correct NIS server by typing:

root@mars:~# ypwhich

ubuntu.example.com

Real life experience

In my case, after the NIS client boots up ypwhich shows error message. I checked that ypbind service is running. But it may not started up properly. So I started it again by typing;

/etc/init.d/./nis restart

After that when I execute ypwhich, it gave me the correct NIS domain.

I then decided to include a rc startup script at runlevel 2. But first I checked that a startup script to start NIS is already included.

```
# cd /etc/rc2.d/

# ll *nis*

lrwxrwxrwx 1 root root 13 2010-03-25 12:19 S18nis -> ../init.d/nis
```

I then wrote a startup script called S99mynis with the contents as follow:

```
#cat /etc/rc2.d/S99mynis
#!/bin/bash
/etc/init.d/./nis restart
```

What the script does is simply to restart the NIS service again.

Make sure the NIS server is up and running

```
# rpcinfo -u ubuntu.example.com ypserv

program 100004 version 1 ready and waiting

program 100004 version 2 ready and waiting
```

After starting ypbind, check that it has registered with portmap.

```
# rpcinfo -u localhost ypbind

program 100007 version 1 ready and waiting

program 100007 version 2 ready and waiting
```

If the NIS client connects to the NIS server, you should be able to log in to the client with an account that exists only on the NIS server (login by tlnet, ssh or X login). You can set up a user on the NIS server and try logging on in the NIS client, using the account. If successful that user should be logged into the appropriate home directory assuming it exists. If that doesn't exists, NIS assumes that such user home directories are top-level root directory(/) which is insecure.

Creating NIS User

On the NIS Server, create a NIS user. **You only need to create this account on the NIS server and not on the client.**

root@ubuntu:~# useradd -m nisuser

root@ubuntu:~# passwd nisuser

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

Whenever you add new users or modify the user information, you need to build or import the maps. This is done so that the NIS master server maps are synchronized with the passwd map.

ypinit: Build or Import Maps

To build the Maps, type

```
# /usr/lib/yp/ypinit -m
```

or you can also type:

```
root@ubuntu:~# cd /var/yp

root@ubuntu:/var/yp# make

This is equivalent to the command "make -C /var/yp"
```

```
make[1]: Entering directory `/var/yp/nis-test-domain'

Updating passwd.byname...
```

```
Updating passwd.byuid...

Updating netid.byname...

Updating shadow.byname...

make[1]: Leaving directory `/var/yp/nis-test-domain'
```

You can check to see if the user's authentication information has been updated by using the ypmatch command, which should return the user's encrypted password string.

```
root@ubuntu:/var/yp# ypmatch nisuser passwd

nisuser:x:5002:100::/home/nisuser:/bin/sh

root@ubuntu:/var/yp# getent passwd nisuser

nisuser:x:5002:100::/home/nisuser:/bin/sh
```

You can also use the getent command, which has similar syntax. Unlike ypmatch, getent doesn't provide an encrypted password when run on an NIS server, it just provides the user's entry in the /etc/passwd file. On a NIS client, the results are identical with both showing the encrypted password.

Log in to NIS server from NIS client with Account on the NIS server

After creating the NIS user account on the NIS server, try log in to NIS server from the NIS client using telnet or ssh.

On the NIS client

```
root@mars:~# telnet ubuntu.example.com

Trying 172.16.0.2...

Connected to ubuntu.example.com.

Escape character is '^]'.

Ubuntu 9.04

ubuntu.example.com login: nisuser

Password:

Last login: Thu Mar 25 14:39:45 SGT 2010 from www.example.com on pts/2

Linux ubuntu.example.com 2.6.28-13-generic #45-Ubuntu SMP Tue Jun 30 19:49:51 UTC 2009
i686
```

Now try to ssh from the NIS client to the NIS server.

```
root@mars:~# ssh ubuntu.example.com -l nisuser

The authenticity of host 'ubuntu.example.com (127.0.0.1)' can't be established.

RSA key fingerprint is 26:3a:2e:97:51:e3:09:52:88:57:a6:bf:79:35:e3:87.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added 'ubuntu.example.com' (RSA) to the list of known
hosts.

nisuser@ubuntu.example.com's password
Last login: Tue Mar 30 23:47:11 2010 from ubuntu.example.com

nisuser@ubuntu:~$
```

You should be able to login to the NIS server from the NIS client using X login.

NIS and NFS

NIS works well with NFS and thus you should use NFS so that the users home direcories can be mounted from the NIS server and user then can access their files from any NIS clients.

On the NIS/NFS server, the /etc/exports configuration file contains the following:

```
/home     172.16.0.1/255.255.0.0(rw,no_root_squash)
```

You will need to run the `/etc/exportfs -v -a` command. Ofcourse you will need to check that the NFS service are running on the NIS/NFS server.

On the NIS/NFS client, you will need to mount the NFS share. You may want to include the NFS share in the /etc/fstab so that when the NIS client boots up, the NFS share is mounted. I included the following line:

```
172.16.0.2:/home    /home/    nfs  defaults  0    0
```

If you do not want to include it in the /etc/fstab file, you can manually mount it with the following command:

```
#mount -t nfs 172.16.0.2:/home /home
```

Yppasswd:Changes NIS Passwords

The yppasswd replaces the fucntionality of passwd on clients when you are usingf NIS for

passwords. The passwd changes the information in the /etc/shadow file on the local system while the yppasswd changes password information in the /etc/shadow file on the NIS master server.

The yppasswd cannot change root and system passwords as by default NIS does not store passwords of users with UIDs less than 500. You have to use passwd to change these users' passwords locally.

To use yppasswd, the yppasswdd daemon must be running on the NIS master server.

Changing password on NIS client

In this exercise I as a NIS client on a NIS client machine will change the NIS client password. Then I will access the NIS client's email and check if the e-mail password is updated.

On a NIS client, after login, in my case the username its nisuser2, change the password by typing:

```
nisuser2@mars:~$ yppasswd

Changing NIS account information for nisuser2 on
ubuntu.example.com.

Please enter old password:

Changing NIS password for nisuser2 on ubuntu.example.com.

Please enter new password:

Please retype new password:
```

The NIS password has been changed on ubuntu.example.com.

root@ubuntu:/home/nisuser2#

Now let's access nisuser2 e-mails and see if the password is updated. Lauch Thunderbird and it will prompt you for the user's password. I keyed in the old password and the alert message that read “Login to server ubuntu.exampe.com failed”. This shows that the NIS client password has been updated. To confirm this, I log in using the newpassword.

Yes I can access my e-mail using the new password.

passwd Versus yppasswd

When a user who is authenticated using NIS passwords runs passwd to change her password, all

appears to work properly, yet the user's password is not changed . The user needs to use yppasswd. The root and system accounts in contrast must use passwd to change their passwords. A common solution to this problem is first to rename passwd, for example, to rootpasswd, and then to change its permissionsnto only root can execute it. Second, create a link to yppasswd named passwd.

```
root@ubuntu:~# ls -l /usr/bin/passwd

-rwsr-xr-x 1 root root 37084 2009-04-04 13:49 /usr/bin/passwd

#mv /usr/bin/passwd /usr/bin/rootpasswd
#chmod 700 /usr/bin/rootpasswd
#ln -s /usr/bin/yppasswd /usr/bin/passwd
#ls -l /usr/bin/{yppasswd,passwd,rootpasswd}
lrwxrwx /usr/bin/passwd --> /usr/bin/yppasswd
-rwx------- /usr/bin/rootpasswd
-r-xr-xr-x /usr/bin/yppasswd
```

With this setuo, a nonroot user changing his password using passwd will run yppasswd, which is appropriate. If root runs passwd (really yppasswd),yppasswd displays an error that will remind the administrator to run rootpasswd.

Yppasswdd: The NIS Password Update Daemon

The NIS password update daemon, yppasswdd runs only on the masterserver, and not necessary to run it on the slave servers. When a user runs yppasswd on a client, yppasswd changes information with the yppasswdd daemon to update the user's password on other information.

Allow GECOS and Login Shell Modification

By default yppasswdd does not allow users to change GECOS information or the login shell when they run yppasswd. You can allow users to change this information with options on the command line when you start yppasswdd or by modifying the yppasswdd configuraton file. The section below will show you how to use the -e chfn -e chsh options to change the GECOS and login shell information.

On the NIS server

root@ubuntu:/usr/sbin# ps -ef|grep yppasswdd

root 10218 1 0 13:26 ? 00:00:00 /usr/sbin/rpc.yppasswdd -D /etc -e chsh

root 15137 4187 0 14:48 pts/0 00:00:00 grep yppasswdd

root@ubuntu:/usr/sbin# kill -9 10218

Enable chfn and chsh

root@ubuntu:/usr/sbin# /usr/sbin/rpc.yppasswdd -D /etc -e chsh -e chfn

root@ubuntu:/usr/sbin# ps -ef|grep yppasswdd

root 15424 6930 0 14:50 pts/1 00:00:00 man yppasswdd

root 15445 1 0 14:52 ? 00:00:00 /usr/sbin/rpc.yppasswdd -D /etc -e chsh -e chfn

On NIS client

```
root@mars:~# telnet ubuntu.example.com

Trying 172.16.0.2...

Connected to ubuntu.example.com.

Escape character is '^]'.

Ubuntu 9.04

ubuntu.example.com login: nisuser

Password:

Last login: Thu Mar 25 14:39:45 SGT 2010 from www.example.com on pts/2

Linux ubuntu.example.com 2.6.28-13-generic #45-Ubuntu SMP Tue Jun 30 19:49:51
UTC 2009 i686

nisuser@ubuntu:~$ yppasswd -f

Changing NIS account information for nisuser on ubuntu.example.com.

Please enter password:

Changing full name for nisuser on ubuntu.example.com.

To accept the default, simply press return. To enter an empty

field, type the word "none".

Name []: MR NISUSER

Location []: SG

Office Phone []:

Home Phone []:
```

```
The GECOS information has been changed on ubuntu.example.com.
```

On the NIS server or client check that the information have been changed.

```
# ypmatch nisuser passwd

nisuser:x:5002:5002:MR NISUSER,SG:/home/nisuser:/bin/bash
```

User "Root" Changing Passwords

The root user can change other users' passwords issuing the yppasswd command with the -p switch that specifies the username that needs the change.

```
#yppasswd -p nisuser
```

Successful X Log in from NIS Client to NIS server

Now remember that the user account is only created on the server and not on the client. After log in to the client and if you try to use passwd command hoping to change passwords, you will receive the following error message.

Disabling NIS on the NIS server Upon Booting

Sometimes you may want to disable NIS services on the NIS server. This is when you don't need the NIS service or you just want to stop the NIS service upon booting. If let's say you did not stop the NIS service and your NIS server is not available, your NIS clients will take a long time to boot up. Those NIS clients will see messages like the one below

```
*Starting NIS Services
*Binding to YP Server
*....
*....
*....
*....
*....
*....
*....
*....
*....
*.... [fail]
```

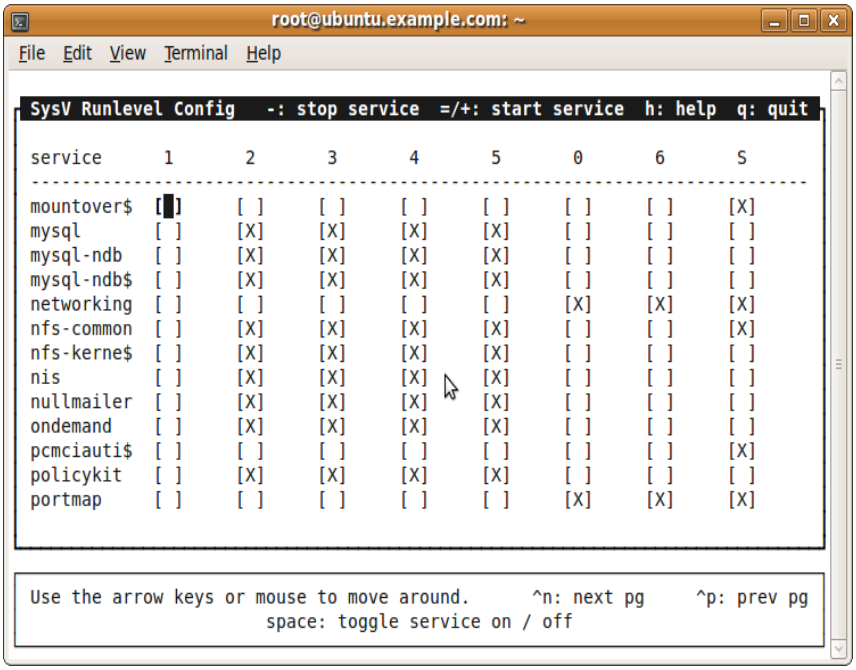
In my case the NIS server is also the NIS client, and when I changed the IP address of the NIS server, my NIS server could not see itself and thus will take a long time to boot. It is therefore good to disable NIS if you are not using it. To control the services that are automatically started during boot-up, you can install sysv-rc-conf script as shown below:

apt-get install sysv-rc-conf

After installing, you can lauch the script by typing:

sysv-rc-conf

It will launch the program as shown below:



Disable or enable the service by pressing the sapcebar and to quit press q. In my case I stop the NIS service in the 2,3,4 and 5 runlevels upong booting

Reboot the machine and see if the NIS messages appear on booting.

If you did not install the sysv-rc-conf program , you can also press the Ctrl+Alt+F1 to go to a console and type

```
/etc/init.d/portmap stop
/etc/init.d/nis stop
```

To check if NIS is configured to run at which runlevels, execute the following command:

root@ubuntu:~# sysv-rc-conf --list nis

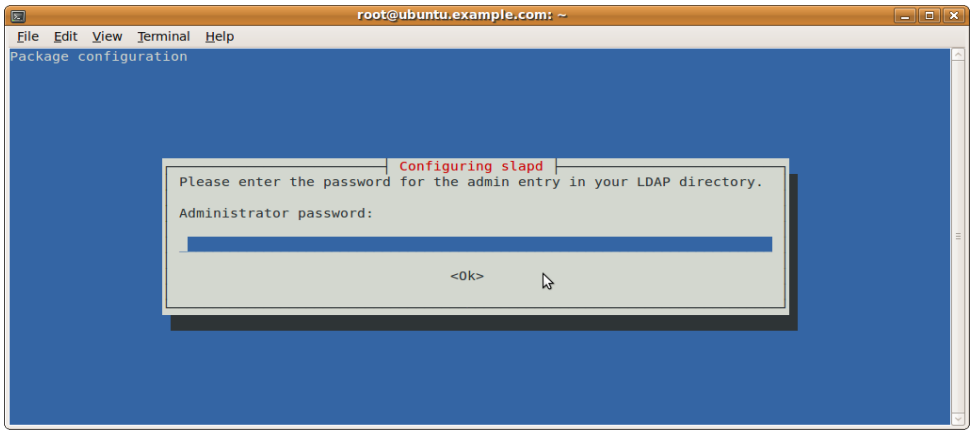
nis 1:off 2:on 3:on 4:on 5:on

Exploring LDAP in Ubuntu Jaunty

In this section we will explore OpenLDAP and create a LDAP Address Book from Thunderbird

Install OpenLDAP

apt-get install slapd ldap-utils




```
Setting up slapd (2.4.15-1ubuntu3) ...

make: Entering directory `/var/yp'

make[1]: Entering directory `/var/yp/nis-test-domain'

Updating netid.byname...

make[1]: Leaving directory `/var/yp/nis-test-domain'

make: Leaving directory `/var/yp'

make: Entering directory `/var/yp'

make[1]: Entering directory `/var/yp/nis-test-domain'

Updating group.byname...

Updating group.bygid...

Updating netid.byname...

make[1]: Leaving directory `/var/yp/nis-test-domain'

make: Leaving directory `/var/yp'

  Creating new user openldap... make: Entering directory `/var/yp'

make[1]: Entering directory `/var/yp/nis-test-domain'

Updating netid.byname...
```

```
make[1]: Leaving directory `/var/yp/nis-test-domain'

make: Leaving directory `/var/yp'

make: Entering directory `/var/yp'

make[1]: Entering directory `/var/yp/nis-test-domain'

Updating passwd.byname...

Updating passwd.byuid...

Updating netid.byname...

Updating shadow.byname...

make[1]: Leaving directory `/var/yp/nis-test-domain'

make: Leaving directory `/var/yp'

done.

  Creating initial slapd configuration... done.

  Creating initial LDAP directory... done.

 * Reloading AppArmor profiles ...
[ OK ]

Starting OpenLDAP: slapd.
```

Use **ldapsearch** to view the tree

ldapsearch -xLLL -b cn=config -D cn=admin,cn=config -W olcDatabase={1}hdb

Enter LDAP Password:

```
dn: olcDatabase={1}hdb,cn=config

objectClass: olcDatabaseConfig

objectClass: olcHdbConfig

olcDatabase: {1}hdb

olcDbDirectory: /var/lib/ldap

olcSuffix: dc=example,dc=com

olcAccess: {0}to attrs=userPassword,shadowLastChange by dn="cn=admin,dc=exampl

 e,dc=com" write by anonymous auth by self write by * none

olcAccess: {1}to dn.base="" by * read

olcAccess: {2}to * by dn="cn=admin,dc=example,dc=com" write by * read

olcLastMod: TRUE
```

```
olcDbCheckpoint: 512 30

olcDbConfig: {0}set_cachesize 0 2097152 0

olcDbConfig: {1}set_lk_max_objects 1500

olcDbConfig: {2}set_lk_max_locks 1500

olcDbConfig: {3}set_lk_max_lockers 1500

olcDbIndex: objectClass eq
```

The output above is the current configuration options for the *hdb* backend database. Which in this case containes the *dc=example,dc=com* suffix.

Test the LDAP server with the following query.

```
# ldapsearch -x -s base namingContexts

# extended LDIF

#

# LDAPv3

# base <> (default) with scope baseObject

# filter: (objectclass=*)

# requesting: namingContexts

#

#

dn:

namingContexts: dc=example,dc=com

# search result

search: 2

result: 0 Success

# numResponses: 2

# numEntries: 1
```

Create a Database Directory

```
root@ubuntu:~# cd /var/lib

root@ubuntu:/var/lib# tree ldap

ldap

|-- DB_CONFIG

|-- __db.001

|-- __db.002

|-- __db.003

|-- __db.004

|-- __db.005

|-- __db.006

|-- alock

|-- dn2id.bdb

|-- id2entry.bdb

|-- log.0000000001

`-- objectClass.bdb

0 directories, 12 files
```

Testing using ldapsearch
ldapsearch -x -b 'dc=example,dc=com' '(objectclass=*)'

```
# extended LDIF

#

# LDAPv3

# base <dc=example,dc=com> with scope subtree

# filter: (objectclass=*)

# requesting: ALL

#



# example.com
```

```
dn: dc=example,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: example.com
dc: example

# admin, example.com
dn: cn=admin,dc=example,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

The ldap.conf configuration file

```
root@ubuntu:~# more /etc/ldap/ldap.conf
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE  dc=example,dc=com
```

```
#URI   ldap://ldap.example.com ldap://ldap-master.example.com:666


#SIZELIMIT   12

#TIMELIMIT   15

#DEREF       never
```

slapcat

```
dn: dc=example,dc=com

objectClass: top

objectClass: dcObject

objectClass: organization

o: example.com

dc: example

structuralObjectClass: organization

entryUUID: 84ca1e18-cc6b-102e-8997-07ec49a1f86f

creatorsName:

createTimestamp: 20100325150456Z

entryCSN: 20100325150456.509391Z#000000#000#000000

modifiersName:

modifyTimestamp: 20100325150456Z


dn: cn=admin,dc=example,dc=com

objectClass: simpleSecurityObject

objectClass: organizationalRole

cn: admin

description: LDAP administrator

userPassword:: e2NyeXB0fVpzYzhRUkJzYWVjaWc=

structuralObjectClass: organizationalRole

entryUUID: 84cb43b0-cc6b-102e-8998-07ec49a1f86f

creatorsName:

createTimestamp: 20100325150456Z

entryCSN: 20100325150456.517057Z#000000#000#000000
```

```
modifiersName:
modifyTimestamp: 20100325150456Z
```

Add Entries to the Directory

root@ubuntu:/etc/ldap# more sa1.ldif

```
dn: dc=example,dc=com
changetype: add
dc: example
objectClass: dcObject
objectClass: organization
organizationName: Example Associates Inc.
```

The following command modifies the LDAP directory based on the sa1.ldif file.

root@ubuntu:/etc/ldap# ldapmodify -xD "cn=admin,dc=example,dc=com" -W -f sa1.ldif

Enter LDAP Password:

adding new entry "dc=example,dc=com"

ldap_add: Already exists (68)

The slapcat displays all entries in the LDAP directory
root@ubuntu:/etc/ldap# slapcat

```
dn: dc=example,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: example.com
dc: example
structuralObjectClass: organization
entryUUID: 84ca1e18-cc6b-102e-8997-07ec49a1f86f
creatorsName:
```

```
createTimestamp: 20100325150456Z

entryCSN: 20100325150456.509391Z#000000#000#000000

modifiersName:

modifyTimestamp: 20100325150456Z


dn: cn=admin,dc=example,dc=com

objectClass: simpleSecurityObject

objectClass: organizationalRole

cn: admin

description: LDAP administrator

userPassword:: e2NyeXB0fVpzYzhRUkJzYWVjaWc=

structuralObjectClass: organizationalRole

entryUUID: 84cb43b0-cc6b-102e-8998-07ec49a1f86f

creatorsName:

createTimestamp: 20100325150456Z

entryCSN: 20100325150456.517057Z#000000#000#000000

modifiersName:

modifyTimestamp: 20100325150456Z
```

The next file adds to the LDAP directory the object class organizationalUnit named employees (ou=employees). The DN is ou=employees followed by the DSE:

```
root@ubuntu:/etc/ldap# more sa2.ldif

dn: ou=employees,dc=example,dc=com

changetype: add

objectClass: organizationalUnit

ou: employees


root@ubuntu:/etc/ldap# ldapmodify -xD "cn=admin,dc=example,dc=com" -W -f
sa2.ldif

Enter LDAP Password:

adding new entry "ou=employees,dc=example,dc=com"
```

```
Note: If you repeat the command again, i.e. To add again you will receive the
message
adding new entry "dc=example,dc=com"

ldap_add: Already exists (68)
```

With this object class in place, you can add employees to the LDAP directory. You can use the following file to add an employee.

root@ubuntu:/etc/ldap# more sa3a.ldif

```
dn: cn=Isa Raffee,ou=employees,dc=example,dc=com

changetype: add

cn: Isa Raffee

cn: Raffee

objectClass: inetOrgPerson

mail:ismail@example.com

givenName: Isa

surname: Raffee

displayName: Isa Bin Raffee

telephoneNumber:999 999 9999

homePhone: 000 000 0000

initials: IR
```

root@ubuntu:/etc/ldap# ldapmodify -xD "cn=admin,dc=example,dc=com" -W -f sa3a.ldif

Enter LDAP Password:

adding new entry "cn=Isa Raffee,ou=employees,dc=example,dc=com"

Now slapcat shows the employee you just added:

root@ubuntu:/etc/ldap# slapcat

```
dn: dc=example,dc=com

objectClass: top

objectClass: dcObject
```

```
objectClass: organization
o: example.com
dc: example
structuralObjectClass: organization
entryUUID: 84ca1e18-cc6b-102e-8997-07ec49a1f86f
creatorsName:
createTimestamp: 20100325150456Z
entryCSN: 20100325150456.509391Z#000000#000#000000
modifiersName:
modifyTimestamp: 20100325150456Z

dn: cn=admin,dc=example,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e2NyeXB0fVpzYzhRUkJzYWVjaWc=
structuralObjectClass: organizationalRole
entryUUID: 84cb43b0-cc6b-102e-8998-07ec49a1f86f
creatorsName:
createTimestamp: 20100325150456Z
entryCSN: 20100325150456.517057Z#000000#000#000000
modifiersName:
modifyTimestamp: 20100325150456Z

dn: ou=employees,dc=example,dc=com
objectClass: organizationalUnit
ou: employees
structuralObjectClass: organizationalUnit
entryUUID: 9938a77e-ccad-102e-8617-51c7ac9f71f4
creatorsName: cn=admin,dc=example,dc=com
createTimestamp: 20100325225757Z
```

```
entryCSN: 20100325225757.572547Z#000000#000#000000
modifiersName: cn=admin,dc=example,dc=com
modifyTimestamp: 20100325225757Z

dn: cn=Isa Raffee,ou=employees,dc=example,dc=com
cn: Isa Raffee
cn: Raffee
objectClass: inetOrgPerson
mail: ismail@example.com
givenName: Isa
sn: Raffee
displayName: Isa Bin Raffee
telephoneNumber: 999 999 9999
homePhone: 000 000 0000
initials: IR
structuralObjectClass: inetOrgPerson
entryUUID: 4fcab73c-ccb0-102e-861c-51c7ac9f71f4
creatorsName: cn=admin,dc=example,dc=com
createTimestamp: 20100325231722Z
entryCSN: 20100325231722.868567Z#000000#000#000000
modifiersName: cn=admin,dc=example,dc=com
modifyTimestamp: 20100325231722Z
```

The following adds another employee at the third level

root@ubuntu:~# cd /etc/ldap

root@ubuntu:/etc/ldap# more sa3b.ldif

```
dn: cn=Marsita Tahir,ou=employees,dc=example,dc=com
changetype: add
cn: Marsita Tahir
cn: tahir
```

```
objectClass: inetOrgPerson

mail:ubuntuuser@example.com

givenName: Marsita

surname: Tahir

displayName: Marsita Bte Tahir

telephoneNumber:111 111 1111

homePhone: 2222 222 2222

initials: MT
```

root@ubuntu:/etc/ldap# ldapmodify -xD "cn=admin,dc=example,dc=com" -W -f sa3b.ldif

Enter LDAP Password:

adding new entry "cn=Marsita Tahir,ou=employees,dc=example,dc=com"

You can use slapcat to verify the entry

```
dn: cn=Marsita Tahir,ou=employees,dc=example,dc=com

cn: Marsita Tahir

cn: tahir

objectClass: inetOrgPerson

mail: ubuntuuser@example.com

givenName: Marsita

sn: Tahir

displayName: Marsita Bte Tahir

telephoneNumber: 111 111 1111

homePhone: 2222 222 2222

initials: MT

structuralObjectClass: inetOrgPerson

entryUUID: 3742308e-ccef-102e-9d1e-816c4806e891

creatorsName: cn=admin,dc=example,dc=com

createTimestamp: 20100326064740Z

entryCSN: 20100326064740.002420Z#000000#000#000000

modifiersName: cn=admin,dc=example,dc=com
```

```
modifyTimestamp: 20100326064740Z
```

Note
It's important to get the value of cn correct when executing the ldapmodify command because in my case the value of cn is admin and if I typed ldapadmin for cn, I will receive this error message.

ldap_bind: Invalid credentials (49)

The next example uses the ldapmodify modify instruction to replace the cn attribute,mail attribute and add a title attrribute for the employee Isa Raffee. Because the file specifies Isa's DN, the server knows which entry to modify.

```
root@ubuntu:/etc/ldap# cat sa3bm.ldif

dn: cn=Isa Raffee,ou=employees,dc=example,dc=com

changetype:modify

replace: mail
mail: enzer@example.com

-

add: title

title: CTO
```

root@ubuntu:/etc/ldap# ldapmodify -xD "cn=admin,dc=example,dc=com" -W -f sa3bm.ldif

Enter LDAP Password:

modifying entry "cn=Isa Raffee,ou=employees,dc=example,dc=com"

Verify using slapcat

```
dn: cn=Isa Raffee,ou=employees,dc=example,dc=com

cn: Isa Raffee

cn: Raffee

objectClass: inetOrgPerson

givenName: Isa

sn: Raffee

displayName: Isa Bin Raffee

telephoneNumber: 999 999 9999
```

```
homePhone: 000 000 0000

initials: IR

structuralObjectClass: inetOrgPerson

entryUUID: 947e2b6e-ccf3-102e-9d21-816c4806e891

creatorsName: cn=admin,dc=example,dc=com

createTimestamp: 20100326071854Z

mail: enzer@example.com

title: CTO

entryCSN: 20100326072345.802737Z#000000#000#000000

modifiersName: cn=admin,dc=example,dc=com

modifyTimestamp: 20100326072345Z
```

The final example deletes Isa from the LDAP directory

```
# cat sa3ad.ldif

dn: cn=Isa Raffee,ou=employees,dc=example,dc=com

changetype: delete
```

root@ubuntu:/etc/ldap# ldapmodify -xD "cn=admin,dc=example,dc=com" -W -f sa3ad.ldif

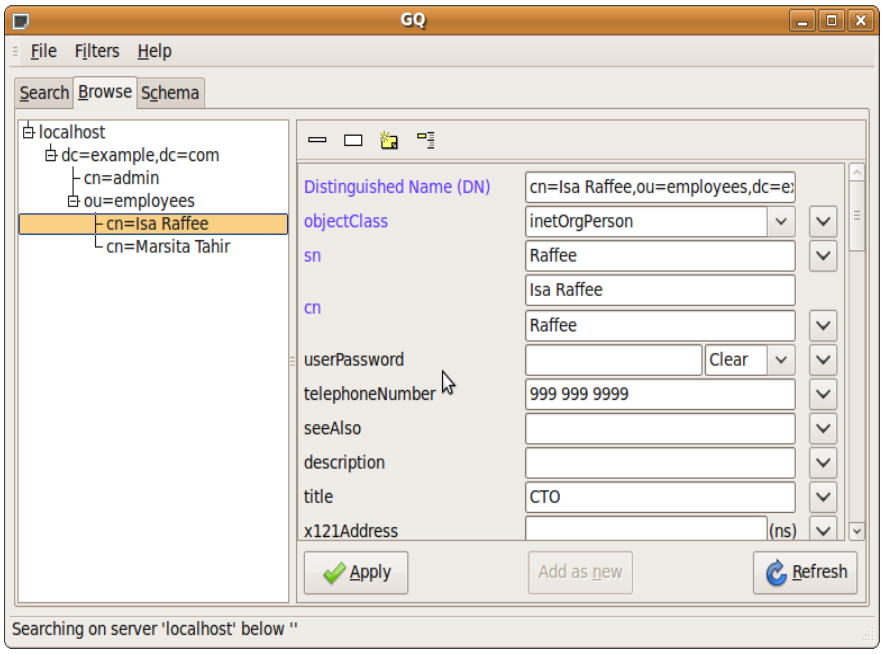
Enter LDAP Password:

deleting entry "cn=Isa Raffee,ou=employees,dc=example,dc=com"

I verified using slapcat and the record was deleted from the LDAP directory.

Tools for working with LDAP

Gq:An LDAP Client
The gq utility is a graphical LDAP client you can use to display, edit and delete entries. Below is a snaphot of browsing the LDAP directory.

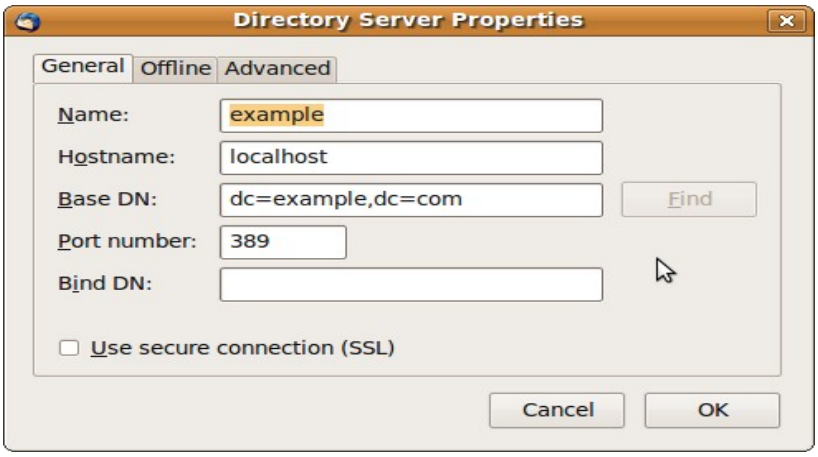


Accessing an LDAP Address Book from Thunderbird

Now that with have configured the LDAP address book, we will use Thunderbird to search for mail addresses. The following are the steps to set up an LDAP Address book uing Mozilla Thunderbird.

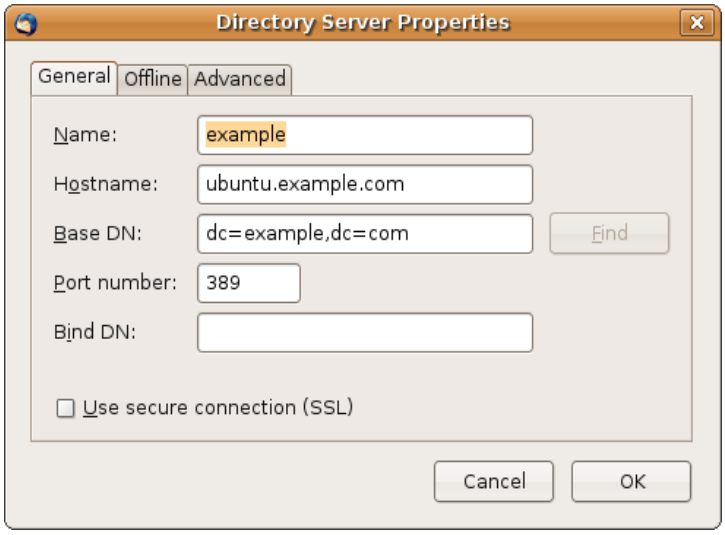
Launch Thunderbird, click the Address Book button.

From the Address Book window, Select File--> New --> LDAP Directory. Fill up the fields as shown below.



Name – The name that identifies the server on your LDAP servers list

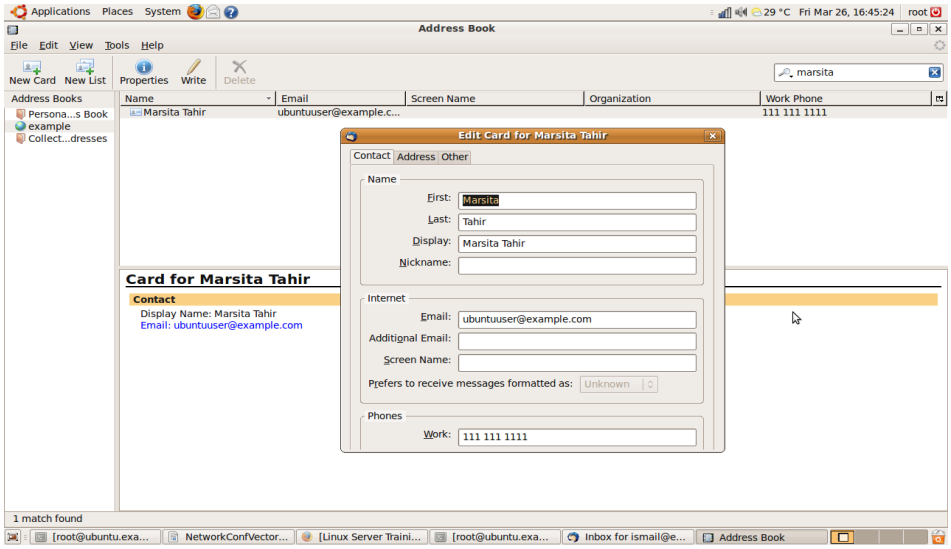
Hostname – The name or IP address of the host that host the LDAP content. In the LDAP clients you should type the hostname of the LDAP server, in my case it's ubuntu.example.com as shown below:



Base DN – Indicates the point in the LDAP directory to begin searching. In my example, dc=example,dc=com is the search base.

Port – Enter IP address of the LDAP server. The port number is 389 by default.

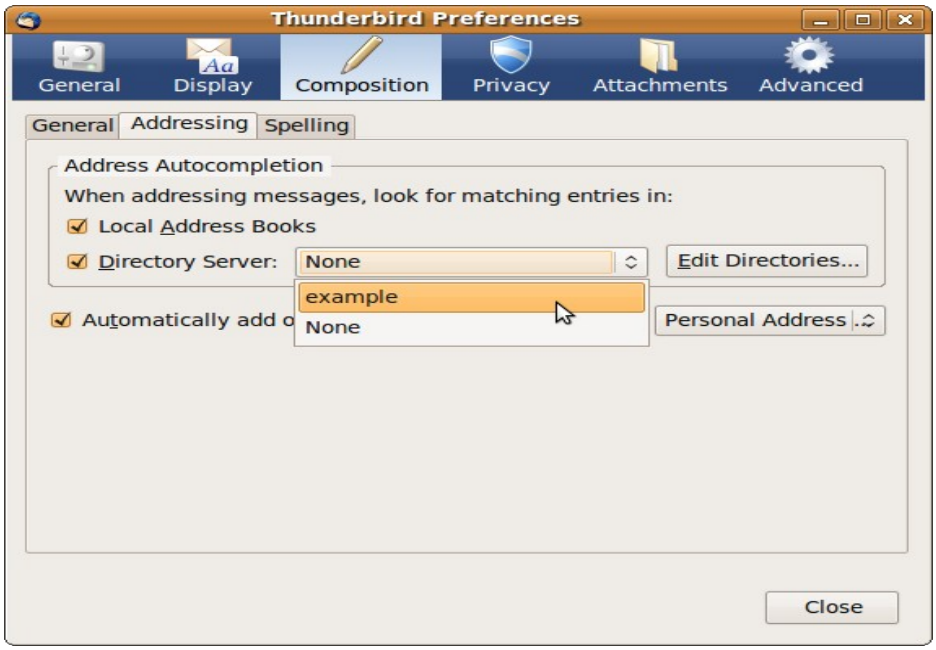
If you ant to search the directory for an e-mail address, with the name of the LDAP address book selected in the left column, type a search term into the search box on the Thunderbird Address Book window and press ENTER.



After an entry is found, you can double click the entry to see more information on the person.

To write an e-mail to the selected person, click select to open a compose window and ready to send an e-mail

You can also add the LDAP server to compose e-mail – Select Edit --> Preferences, choose the composition button, then the address tab. Check the Directory Server. From the dropdown box you can choose the LDAP server you just added to Thunderbird.



The next time you compose a message, typing an e-mail address will auto-complete with address from your LDAP directory.

With this I conclude in the section of searching an LDAP address book directory by name, e-mail address or other information.

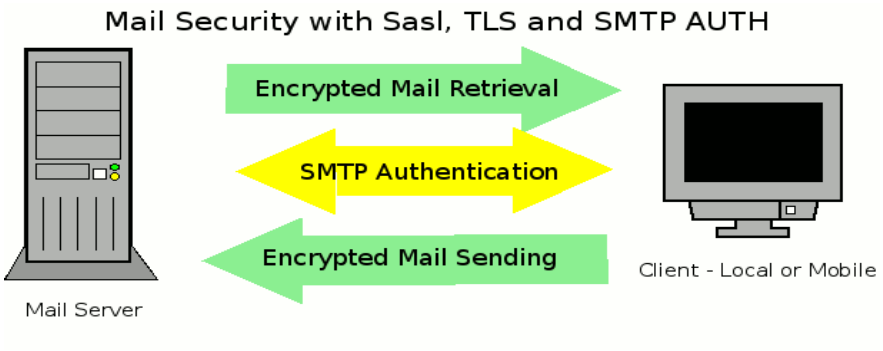
Appendix A

The goal of this configuration is to create a secure mail server using encrypted communication to retrieve mail and to send mail through your mail server.

1. Encrypted Connection to Retrieve Mail
Retrieve mail by connecting to server using port 993 (IMAPS). The importance here is that user names, passwords and data are encrypted when your mail is retrieved.

2. Encrypt the Connection to Send Mail
Encrypting the connection to retrieve your mail is only half the battle, you also need to encrypt it to send mail on port 25 (SMTP with TLS).

3. **Provide Access for Mobile Users**
   The mynetworks setting in Postfix will determine who can send mail through your mail server. The problem when users are traveling is that you will not be able to determine the IP Address or subnet to enter it into the mynetworks setting. Therefore, it is important to be able to use SMTP AUTH which will provide connections for mobile users who are authenticated through the server so they can send mail.



Now there is one problem you need to recognize. The mail that you send and retrieve from your mail server is plain text but is protected because of the security you have set up. However, when you send mail, once it leaves your mail server it is not protected and travels to the next mail server in plain text in which it could be captured and read. If you want to protect the contents of your mail you must use encryption to protect your mail from source to destination. Meaning, you encrypt it and someone on the other end must unencrypt with keys that you need to provide them. The real advantage of protecting your connections when you are sending and retrieving is that your passwords are protected to and from your mail server.

Appendix B

Unable to Access Internet

In my case I use my laptop as a server serving requests from my LAN clients and also to access the Internet. Many times I have to edit the nameserver, that is the /etc/resolv.conf configuration file to either to serve the Internet or to accept requests from my LAN clients. In this section, I will show you how to make the necessary network configuration changes.

To access the Internet make sure the /etc/resolve is empty and not pointing to any LAN IP address.

If you previously configured the machine to point to a DNS server, your /etc/resolv.conf should contain an entry like:

```
root@ubuntu:~# cat /etc/resolv.conf

nameserver someIPaddress
```

So make sure the file is empty as the program wvdial will assign a DNS IP address provided by the ISP.

Check your /etc/network/interfaces file. Mine looks like this:

```
root@ubuntu:~# cat /etc/network/interfaces

auto lo

iface lo inet loopback



#auto eth0

#iface eth0 inet dhcp



auto eth0

iface eth0 inet static

address 172.16.0.2

netmask 255.255.0.0

gateway 172.16.0.1
```

Type wvdial to start connecting to the Intenet via modem

```
#wvdial
```

View the IP route

```
root@ubuntu:~# ip route show

10.64.64.64 dev ppp0  proto kernel  scope link  src 180.129.46.134

169.254.0.0/16 dev eth0  scope link  metric 1000

172.16.0.0/16 dev eth0  proto kernel  scope link  src 172.16.0.2
```

You will still not able to access the Internet because of the third line.

Stop interface eth0

```
root@ubuntu:~# ifdown eth0
```

View the IP route again

```
root@ubuntu:~# ip route show

10.64.64.64 dev ppp0  proto kernel  scope link  src 180.129.46.134
```

The eth0 route was removed.

Now restart wvdial

```
#wvdial
```

View the IP route again

```
root@ubuntu:~# ip route show

10.64.64.64 dev ppp0  proto kernel  scope link  src 124.197.75.123

default dev ppp0  scope link
```

You should be able to access the Internet

route -n

The flag means Only a single host can be reached via this route.

Appendix C

Exploring grub in Ubuntu

Let's view the grub configuration file. Type the following commands.

```
root@ubuntu:~# set -o vi

root@ubuntu:~# cd /boot/grub/

root@ubuntu:/boot/grub# cat menu.lst
```

It will display a long list. In my case I just wanted to view the lines that are not commented. Type:

root@ubuntu:/boot/grub# grep -v "^#" menu.lst

```
default            0



timeout            5


title        Ubuntu 9.04, kernel 2.6.28-13-generic

uuid         bf44916d-b656-46ff-9fa0-970a1f6248af

kernel       /boot/vmlinuz-2.6.28-13-generic root=UUID=bf44916d-b656-46ff-9fa0-
970a1f6248af ro quiet splash

initrd       /boot/initrd.img-2.6.28-13-generic

quiet



title        Ubuntu 9.04, kernel 2.6.28-13-generic (recovery mode)

uuid         bf44916d-b656-46ff-9fa0-970a1f6248af

kernel       /boot/vmlinuz-2.6.28-13-generic root=UUID=bf44916d-b656-46ff-9fa0-
970a1f6248af ro  single

initrd       /boot/initrd.img-2.6.28-13-generic



title        Ubuntu 9.04, kernel 2.6.28-11-generic

uuid         bf44916d-b656-46ff-9fa0-970a1f6248af

kernel       /boot/vmlinuz-2.6.28-11-generic root=UUID=bf44916d-b656-46ff-9fa0-
970a1f6248af ro quiet splash

initrd       /boot/initrd.img-2.6.28-11-generic
```

```
quiet



title        Ubuntu 9.04, kernel 2.6.28-11-generic (recovery mode)

uuid         bf44916d-b656-46ff-9fa0-970a1f6248af

kernel       /boot/vmlinuz-2.6.28-11-generic root=UUID=bf44916d-b656-46ff-9fa0-
970a1f6248af ro  single

initrd       /boot/initrd.img-2.6.28-11-generic



title        Ubuntu 9.04, memtest86+

uuid         bf44916d-b656-46ff-9fa0-970a1f6248af

kernel       /boot/memtest86+.bin

quiet



title        Windows XP

root         (hd0,1)

makeactive
```

Default 0 means it will load the 1st stanza and default 1 means that it will set to the second stanza. Tmeout value refers to the time in seconds before it loads the OS.

If you want to hide the menu, include the following directive.

hiddenmenu

If you want the menu to appear on booting, comment out the hiddenmenu directive like this:

#hiddenmenu

You could add a passord to protect grub by inserting the following directive.

password *somepassword*

for example

password topsecret

It is highly recommend that you include password to protect grub because a cracker can who have

access to the grub menu can set the system to boot at any runlevel, including one that could provide administrative access without any other password. You should also set password for the recovery-mode stanza.

You can use MD5 algorithm to encrypt the password by running the following command:

#grub-md5-crypt

Then you will need to copy the encrypted password to the directive.
password --md5 1gLhU0/$aW78kHK1QfV3P2b2znUoe/

The title directive specifies what is display on the main GRUB menu.

title Ubuntu 9.04, kernel 2.6.28-13-generic

root (hd0,1) directive specifies the partition with /boot directory files.

In this case, it is the second partition of the first hard drive.

The kernel directive points to the filename of the Linux kernel

kernel /boot/vmlinuz-2.6.28-13-generic root=UUID=bf44916d-b656-46ff-9fa0-970a1f6248af ro quiet splash

The quiret and splash options hide associated messages, using the default Ubuntu splash screen. Let's say you want to watch messages as the system boots, delete these two options.

The initrd, which refers to the initial RAM disk loads the associated image file.

initrd /boot/initrd.img-2.6.28-13-generic

Appendix D

Anything Under the Sun

Control Attributes with chattr

To study the usefulness of the command chattr, create a file let's sat abc.txt

touch abc.txt

Now change its attributes, giving immunity to the file.
chattr +i abc.txt

Now try to delete the file.

rm abc.txt

rm: cannot remove `abc.txt': Operation not permitted

Even the roo user is not able to remove the file. If you want to remove the file, as root user run the following command:

chattr -i abc.txt

Then you should be able to delete the file:

rm abc.txt

So with immunity, it will help to minimize careless mistakes.

Special File Permissions

The following are the special file perminssions available in Linux

- Set user ID - SUID
- Set group ID – SGID
- Sticky bit

SUID Bit

An example of set user ID command is the passwd command. To see its permissions, type:

root@ubuntu:~# ls -l /usr/bin/passwd

-rwsr-xr-x 1 root root 37084 2009-04-04 13:49 /usr/bin/passwd

Take note of the owner of the command. It belongs to root. The SUID bit allows normal users to run a program or script as the owner of the script or program. For the command passwd, the letter s appears at the user execute permissions. Without this regular users would not be able to change their passwords.

To set the SUID bit on a file, run the following command

#chmod u+s *filename*

Alternatively yo can type:

#chmod 4544 filename

The first 4 in 4544 refers to the SUID bit.The 544 refers to read and execute permissions for the user and read-only permissions for everyone else. You can practice this by running the following commands:

```
root@ubuntu:~# ls -l abc.txt

-rw-r--r-- 1 root root 0 2010-04-14 13:04 abc.txt

root@ubuntu:~# chmod 4544 abc.txt

root@ubuntu:~# ls -l abc.txt

-r-sr--r-- 1 root root 0 2010-04-14 13:04 abc.txt
```

The SGID Bit

The SGID bit is commonly used for directories shared by a specific group of owners. For example, the SGID bit set on a /home/linuxgurus directory , with a group owner of linuxgurus, allows each member of the linuxgurus group to add files to and read files from that directory. To set the SGID bit on the directory, run the following command

#chmod g+s directory

Alternatively, you can type:

#chmod 2474 directory

The first digit 2 refers to the SGID. The 474 allows read and write permissions for the group owner and read permissions for everyone else.

The Sticky Bit

The sticky bit is usually applied to a directory. To set the sticky bit type:

#chmod o+t directory

If you want to set read, write and execute permissions for all users on the directory, you can type:

#chmod 1777 directory

The digit 1 represents the sticky bit.

Configuring X

To configure X, type:

#dpkg-reconfigure xserver-xorg

Note:
the command dpkg-reconfigure zserver-xorg with the option -phigh configure the X server in less detail

The configuration wil be be written to a file with a date time stamp format. If it makes sense you can copy it to the /etx/X11/xorg.conf file.

#init 1

#Xorg -configure

#exit

Useful Commands for dpkg

To verfiy that a a package is install type:

dpkg -l vino

Desired=Unknown/Install/Remove/Purge/Hold

| Status=Not/Inst/Cfg-files/Unpacked/Failed-cfg/Half-inst/trig-aWait/Trig-pend

|/ Err?=(none)/Hold/Reinst-required/X=both-problems (Status,Err: uppercase=bad)

||/ Name Version Description

+++-==========-==========-
==========

ii vino 2.26.1-0ubuntu VNC server for GNOME

To view the full list of files for a particular package type
dpkg -L vino

To find the source of a particular file type:
dpkg -S /usr/bin/vino-passwd

vino: /usr/bin/vino-passwd

Take note that the command does not work on every file as some files are composite configuration files created from two or more packages.

Wireless Network

To view available wireless network access points, type:;

```
root@ubuntu:~# iwlist ath0 scanning

ath0      Scan completed :

          Cell 01 - Address: 00:1B:11:3C:3E:2D

                    ESSID:"Tun Lin Soe"

                    Mode:Master

                    Frequency:2.437 GHz (Channel 6)
```

```
                    Quality=2/70  Signal level=-93 dBm  Noise level=-95 dBm
                    Encryption key:on
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s
                              9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s; 36 Mb/s
                              48 Mb/s; 54 Mb/s
                    Extra:bcn_int=100
                    IE: WPA Version 1
                        Group Cipher : TKIP
                        Pairwise Ciphers (1) : TKIP
                        Authentication Suites (1) : PSK
                    Extra:ath_ie=dd0900037f01010020ff7f
          Cell 02 - Address: 00:24:56:D4:52:81
                    ESSID:"2WIRE683"
                    Mode:Master
                    Frequency:2.437 GHz (Channel 6)
                    Quality=20/70  Signal level=-75 dBm  Noise level=-95 dBm
                    Encryption key:on
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 6 Mb/s; 9 Mb/s
                              11 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s; 36 Mb/s
                              48 Mb/s; 54 Mb/s
                    Extra:bcn_int=100
```

To connect to a network ESSID of some_wireless_access_point, type:

iwconfig eth1 essid some_wireless_access_point

To connect to the network named Crystal with the noted encryption key , type:

#iwconfig eth1 essid Crystal enc 2C0BB80617

the word enc and key options are synonymous

To identify the current ESSID access point, type

iwgetid -a

To identify the current channel
iwgetid -c

Detected Connection

Zero Configuration Networking implemented by Apple as Bonjour, by Microsoft as Automatic Private IP Addressing (APIPA) and by Linux as Avahi.

Remote GUI Access Using Remote Desktop

There are three ways to configure remote access to a GUI system namely:

- Using ssh-X
- Remote Access via XDMCP
- Remote Access via VNC

Remote Access via SSH

To remote access via ssh, type:

#ssh -X ipaddress_of_remote_host

Once you provide the password and login, you can run X applications, like xeyes, nautilus, xterm and mplayer. The applications will be launched at the remote host. I don't see this as useful because I could not control the remote host applications.

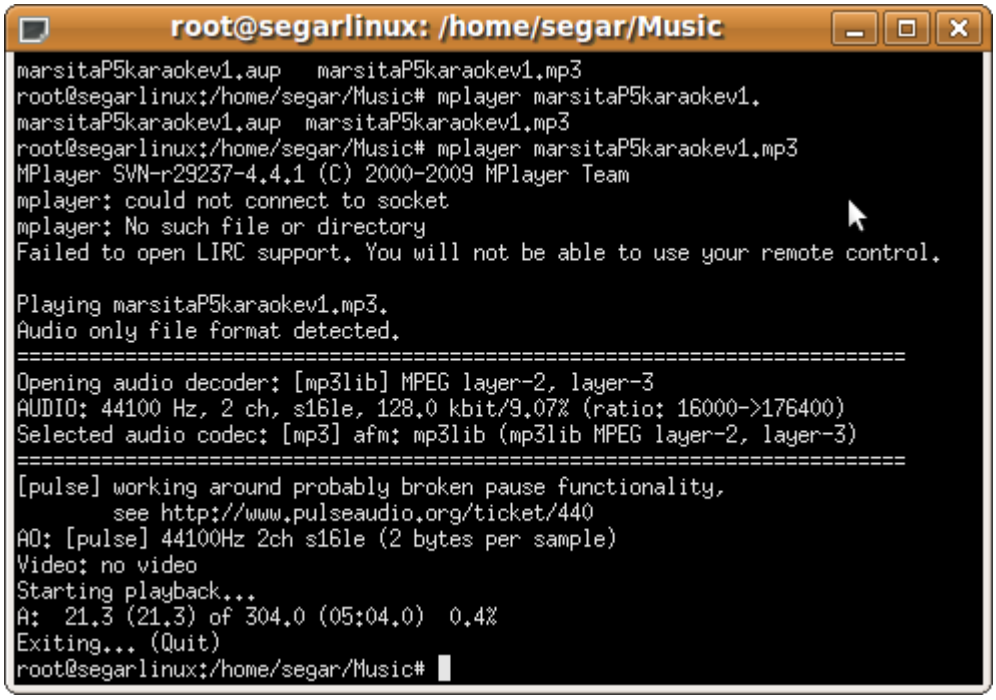
But I came across where the remote applications were launched on the local host. This is useful as you can control the remote host and use the remote applications.

In case you are unable to launch the remote applications on your local host, type the following

Important Tip

xterm -display :0.0 -e ssh -X root@192.168.1.100 &

This will launch an xterm window of the remote host on your local host. Thus you can control and open remote applications. Try to eject, run xeyes, play mp3 files, shutdown etc, But this will only allow you to have a remote xterm on your local host. All other GUI applications will still appear on the remote host and not on your local host.



Remote Access via Remote Desktop

In this section I will discuss about Remote Desktop
Firstly you will need to install the xvnc server, vino. Then you will need to install VNC client vinagre

Installing the xvnc Server, Vino

Install vino

#apt-get install vino

Installing the VNC Client, xvncviewer

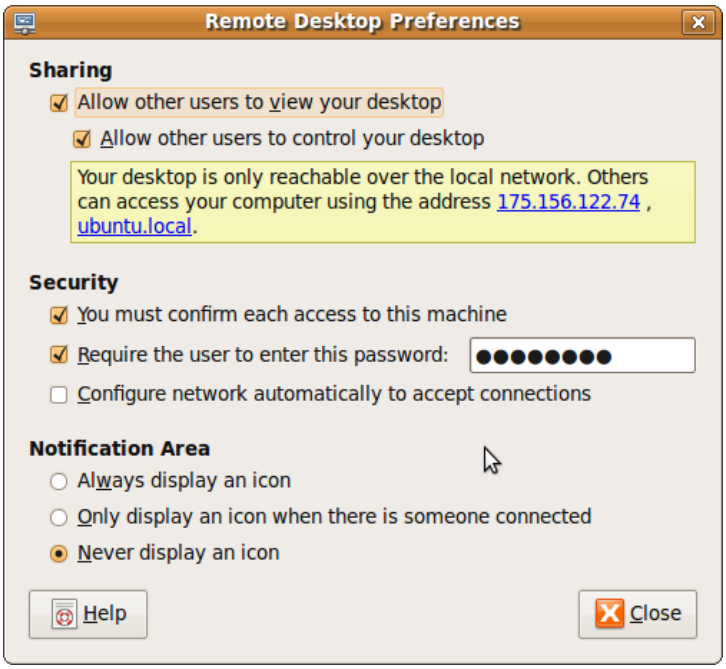
Install VNC client package by typing:

#apt-get install xvnc4viewer

Configure Remote Desktop Preferences

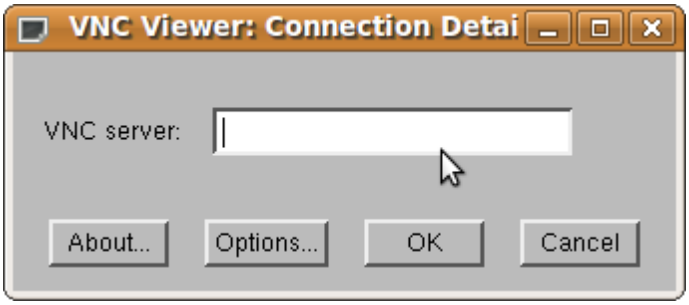
Configure Remote Desktop Preferences. You have to configure this on the remote desktop.

Click System-->Preference-->Remote Desktop

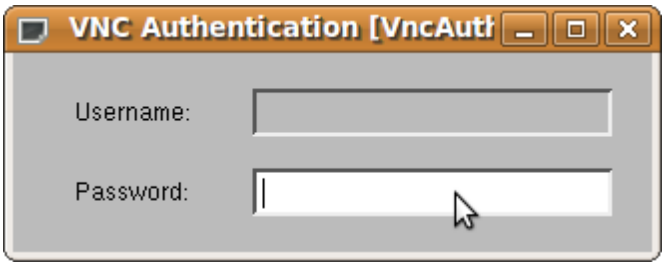


Lauch the xvncviewer, type:

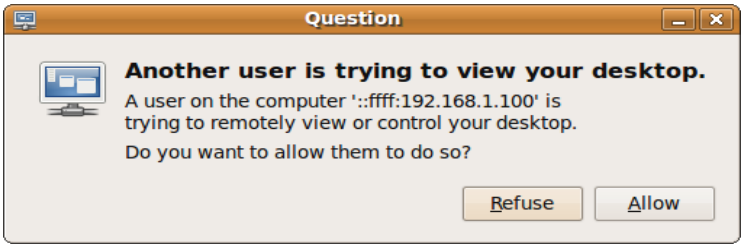
xvnc4viewer



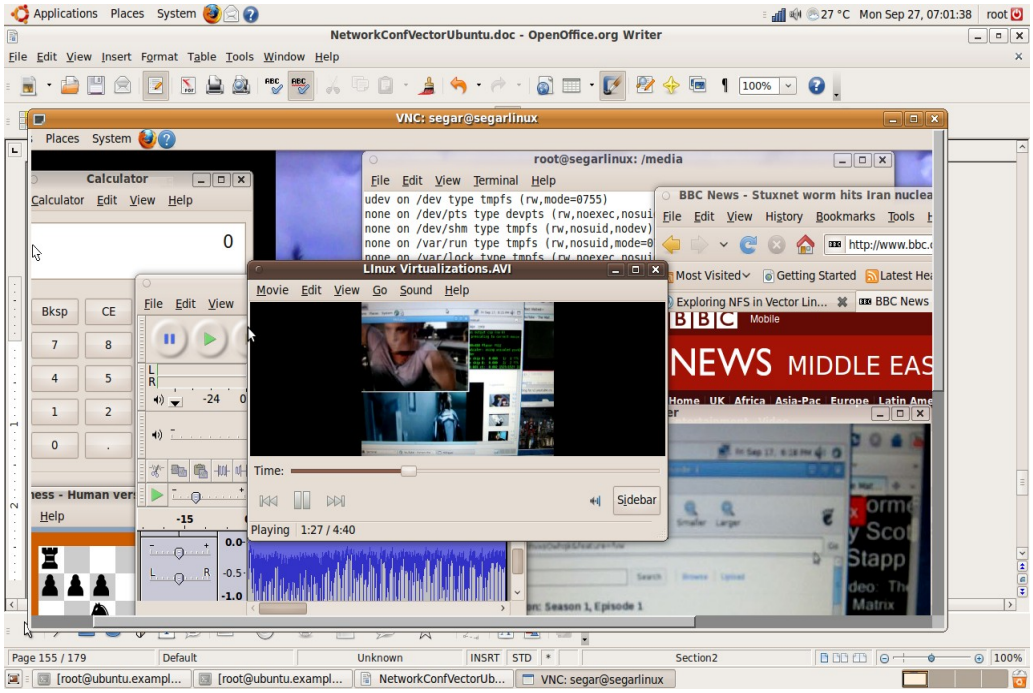
Type the IP address or the name of the xvnc server that was given.



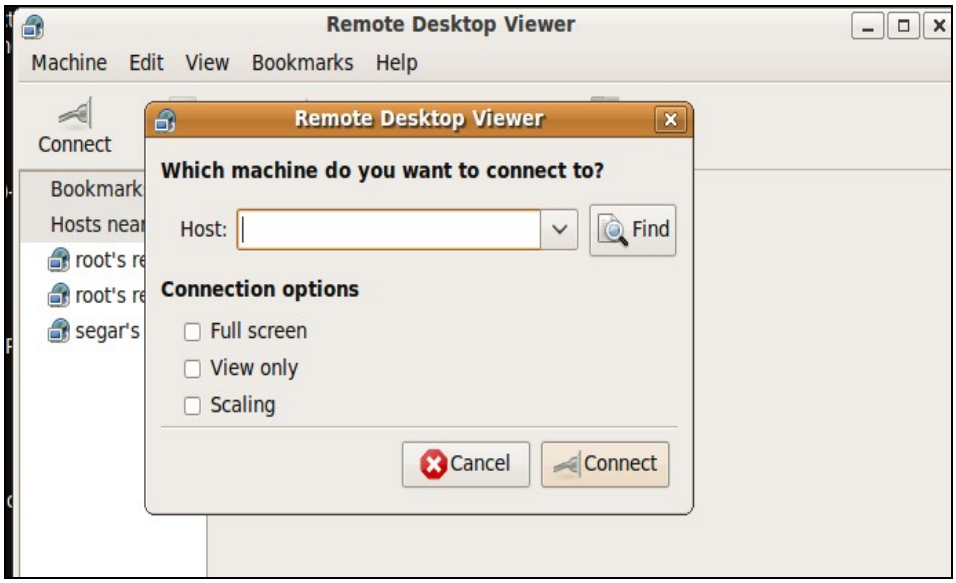
Type the password that you have set in the Remote Desktop configuration. The window on the remote desktop will pop up prompting for permission to allow a user who is trying to vire your desktop. Click the Allow button.



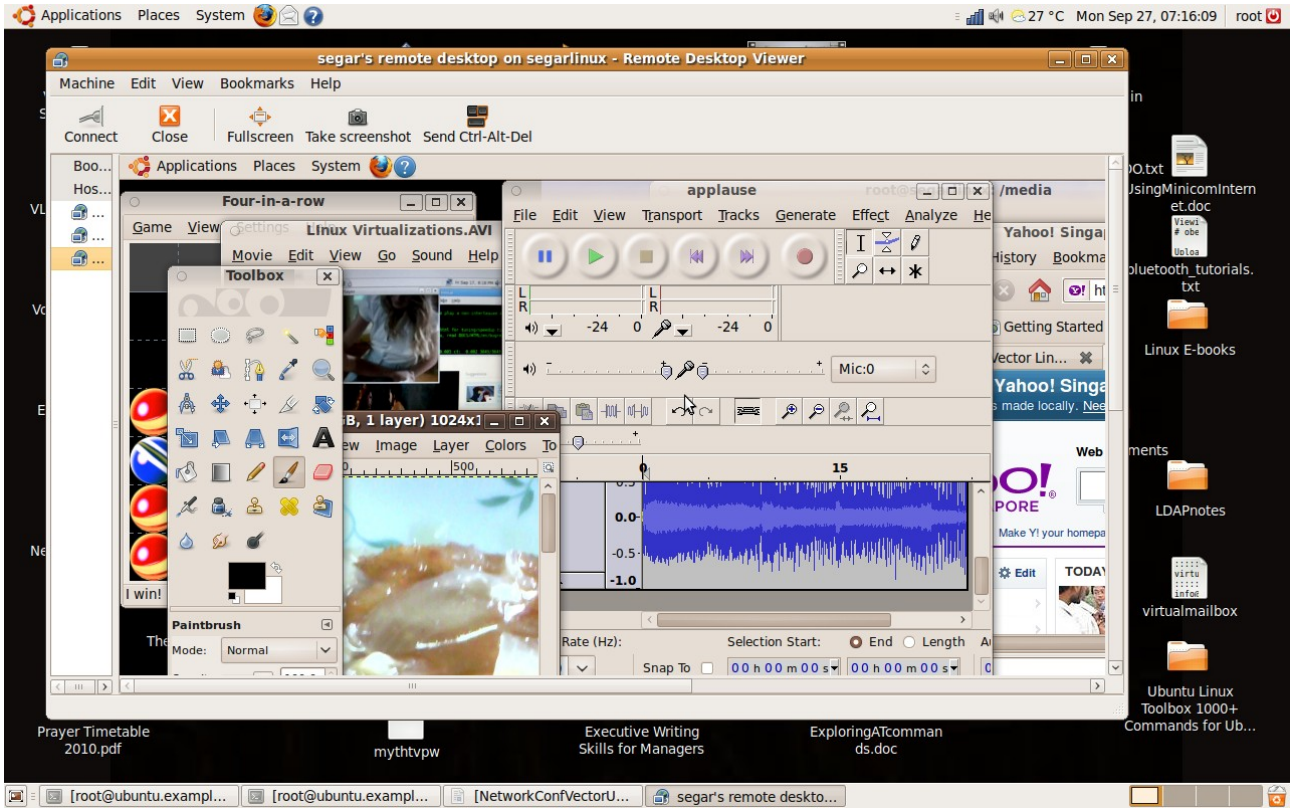
The snapshot below shows the remote desktop that is located in my study room. I am connected via wireless from a laptop in my living room. The remote desktop is running 2 video movies, website, a chess game, calculator,a terminal console, OpenOffice Word and Audacity, a music editor software. The whole experience of remote desktop in Linux is vey impressive. There is no lagging in the applications, whether it's web browsing playing games, music editing, running shell scripts, playing movies, etc. And all these are possible even when the remote desktop is connected via wireless.



Another method to remote desktop is by using Ubuntu Remote Desktop Viewer. This package should by available in many linux distros. You need not install it as it comes with the OS installation. To launch the application, Click Applications-->Internet-->Remote Desktop Viewer.



Below is a screenshot of Linux Remote Desktop Viewer in action. As you can see the remote desktop is running a movie, web browsing, music editing, playing game, photo editing using Gimp, running a terminal and etc. Again the connection is wireless.


Applications Places System
27 °C Mon Sep 27, 07:16:09 root
segar's remote desktop on segarlinux - Remote Desktop Viewer
Machine Edit View Bookmarks Help
Connect Close Fullscreen Take screenshot Send Ctrl-Alt-Del
Applications Places System
Four-in-a-row
Linux Virtualizations.AVI
Movie Edit View Go Sound Help
Toolbox
Paintbrush
Mode: Normal
applause
File Edit View Transport Tracks Generate Effect Analyze
Mic:0
Rate (Hz):
Selection Start:
End
Length
Snap To
Image Layer Colors
Yahoo! Singa
Getting Started
Linux E-books
LDAPnotes
virtualmailbox
Ubuntu Linux Toolbox 1000+ Commands for Ub...
Prayer Timetable 2010.pdf
mythtvpw
Executive Writing Skills for Managers
ExploringATcommands.doc
[root@ubuntu.exampl...
[root@ubuntu.exampl...
[NetworkConfVectorU...
segar's remote deskto...

Appendix E

A Tale of a Vector Linux NFS Client and a Ubuntu NFS Server

In this section, I will show you how I managed to configure a Vector Linux client which is a and NFS client, that could log in to a Ubuntu file server. The Ubuntu file server is a NFS server.

Configuration of Ubuntu as a NFS server.

To configure Ubuntu as a NFS server, please refer to the documentation which I have explained earlier.

The /etc/exports file on the Ubuntu server contains the following:

```
/home     172.16.0.1/255.255.0.0(rw,no_root_squash)
```

The IP address on the Ubuntu server are configured as shown below:

root@ubuntu:~# cat /etc/network/interfaces

```
auto lo
iface lo inet loopback
#auto eth0
#iface eth0 inet dhcp
auto eth0
iface eth0 inet static
address 172.16.0.2
netmask 255.255.0.0
gateway 172.16.0.2
```

The nameserver in the /etc/resolv.conf points to the Ubuntu server itself as it serves as the DNS server

```
root@ubuntu:~# cat /etc/resolv.conf


# Generated by NetworkManager
```

```
nameserver 172.16.0.2
```

For NFS to work make sure that the portmapper and nfs services are running. As for NIS the ypserv, ypbind, yppasswdd are necessary. Run the following command to check for all these services.

```
root@ubuntu:~# rpcinfo -p localhost

   program vers proto   port

    100000    2   tcp    111  portmapper

    100000    2   udp    111  portmapper

    100024    1   udp  38860  status

    100024    1   tcp  51383  status

    100004    2   udp   1020  ypserv

    100004    1   udp   1020  ypserv

    100004    2   tcp   1021  ypserv

    100004    1   tcp   1021  ypserv

    100009    1   udp   1023  yppasswdd

 600100069    1   udp    602  fypxfrd

 600100069    1   tcp    603  fypxfrd

    100007    2   udp    609  ypbind

    100007    1   udp    609  ypbind

    100007    2   tcp    610  ypbind

    100007    1   tcp    610  ypbind
```

```
100003    2   udp   2049  nfs

100003    3   udp   2049  nfs

100003    4   udp   2049  nfs

100021    1   udp  38082  nlockmgr

100021    3   udp  38082  nlockmgr

100021    4   udp  38082  nlockmgr

100021    1   tcp  50577  nlockmgr

100021    3   tcp  50577  nlockmgr

100021    4   tcp  50577  nlockmgr

100003    2   tcp   2049  nfs

100003    3   tcp   2049  nfs

100003    4   tcp   2049  nfs

100005    1   udp  37644  mountd

100005    1   tcp  44896  mountd

100005    2   udp  37644  mountd

100005    2   tcp  44896  mountd

100005    3   udp  37644  mountd

100005    3   tcp  44896  mountd
```

Creation of Client User Account

On the Ubuntu NIS/NFS server, create a client user account with the command as shown below.

useradd -m vectornfs3

The -m option will create a home directory /home/vectornfs3 for the user vectornfs3. Provide a password for the user by typing:

passwd vectornfs3

Check that the newly created user existed in the /etc/passwd file

root@ubuntu:~# grep vectornfs3 /etc/passwd

vectornfs3:x:5006:5006::/home/vectornfs3:/bin/bash

Take note of the user ID and group ID of the user. This is important as these ID numbers must be the same as NFS client. Otherwise there will be permission issues when creating files and directories.

Removal of hidden configuration files

On the newly crerated user account, you must remove the hidden configuration files of the user at the /home/username folder. This is because the server is Ubuntu wheareas the client is Vector Linux and these two Linux distributions have different login configuration files. Basicaaly you want to have the NFS client configuration files on the user's home directory of the NFS server.

On the Ubuntu NFS server, the following files were found on the newly created user account.

```
root@ubuntu:~# cd /home/vectornfs2

root@ubuntu:/home/vectornfs2# ls -la

total 24

drwxr-xr-x  2 vectornfs2 vectornfs2 4096 2010-04-18 12:05 .
```

```
drwxr-xr-x 17 root       root       4096 2010-04-18 12:05 ..

-rw-r--r--  1 vectornfs2 vectornfs2  220 2009-03-02 22:22 .bash_logout

-rw-r--r--  1 vectornfs2 vectornfs2 3115 2009-03-02 22:22 .bashrc

-rw-r--r--  1 vectornfs2 vectornfs2  357 2009-03-27 15:22 examples.desktop

-rw-r--r--  1 vectornfs2 vectornfs2  675 2009-03-02 22:22 .profile
```

In my case, I remove all these files including the hidden ones.

After we remove these files, we need to place the configuration files of the user in this case from a Vector Linux client. So what files must we create? To get the files I first create a user account on the Vector Linux. That way I would know the configuration files being created. Then I would copy these files to the user' s home directory on the NFS server. Then I would make sure the ownership are correct. So with a clear game plan, let's begin.

Creation of User Acoount on the NFS Client

Before you continue, make sure your NFS client is not mounted onto the NFS share. If you are then you need to unmount the /home directory.

On the Vector Linux NFS client, login as root user. You cannot log in as the new user eventhough you have created a new user account on the Ubuntu NFS server. This is because you still need to create the user account on the Vector Linux NFS client. That said login to the NFS client as root user and create a user account as shownbelow:

root:# useradd -m vectornfs2

Provide password to the new user:

root:# passwd vectornfs2

Check that the user account existed on the /etc/passwd file

root:# grep vector /etc/passwd

vectornfs2:x:5007:100::/home/vectornfs2:

It seems that the shell has not been defined. Define bash shell for the user by typing:

#usermod -s /bin/bash vectornfs2

Check again the /etc/passwd file

root:# grep vector /etc/passwd

vectornfs2:x:5007:100::/home/vectornfs2:/bin/bash

After that make sure the UID and if possible the GID of the user are the same on the NFS server and client. In my case, the UID of the user vectornfs2 at both NFS server and client are the same i.e. 5007.

#usermod -u 5007 vectornfs2

Testing the NFS Client

To test the NFS client, mount the NFS share at the NFS client by typing:

#mount -t nfs 172.16.0.2:/home /home

Check that the /home directory of the NFS server is now mounted as /home directory on the NFS client.

On the NFS client

#cd /home/vectornfs2

#touch abc.txt

On the NFS server, you should be able to see the newly created file, abc.txt in the /home/vectornfs2 directory. Now before you proceed unmount the NFS share as we will copy the user's configuration login files from the NFS client. Unmount the share by typing:

#cd /

#umount /home

To mount the NFS share at boot time, you will need to edit the /etc/fstab configuration file. Make sure you make a backup of the file before you edit it. A misconfigured configuration file may cause

the host not to boot up.

#cp -p /etc/fstab /etc/fstab.bak

Edit the /etc/fstab file and include a line like the one below:

172.16.0.2:/home home nfs defaults 0 0

After that you can again test the NFS share by typing

#mount -a

#mount

You will see the at the last line of the output something like the one below:

```
172.16.0.2:/home on /home type nfs (rw,addr=172.16.0.2)
```

Copy User's Configuration Files from NFS Client to NFS Server

Now if the NFS is working the next thing is to ensure the user's login configuration file like the .bashrc file and etc are at the user's home directory in the NFS server. To do that we need to copy the user's login configuration files from the NFS client to the NFS server. In my case, I use secure copy or scp command. You can run the scp command from the NFS server or client.

If you are at the NFS client, type:

#scp /home/vectornfs2/.bashrc 172.16.0.2:/home/vectornfs2

Continue to copy all the files, hidden files and directories from the user home directory in the NFS client to the NFS server. To copy the hidden files you can use the following wildcards.

#cp -p .[a-zA-Z0-9]* /destination_folder

To copy hidden directories, type:

#cp -rp .[a-zA-Z0-9]* /destination_folder

Once all the files are copied, logout and reboot the NFS client.

Login to the NFS Client

As the NFS client is booting up look out for the messages which corresponds to the NFS service. If you have NFS error messages, it is likely that your NFS configuration on the NFS client has failed. This may be due to portmap not running or fail to mount the NFS share. If you encountered those error messages, then you will need to tweak the start up scripts. I will discuss this shortly. But if everything started properly and you can use X login to the NFS client using the newly created user, then everything is successful.

Tweaking the Startup Scripts Due to NFS Failure

In my case my NFS client had NFS related error messages upon booting up. I cannot use X login using the new user account. I suspected that the NFS client had failed to mount the NFS share. So I created a script called S78nfsmount in the /etc/rc.d/rc4.d directory in the NFS client. The contents of the script looks like this:

#cat S78nfsmount

#!/bin/bash

/bin/mount -a

That's it. And make sure you give the execute rights to the script.

#chmod u+x S78nfsmount

Now reboot the NFS client. This time I am able to login using X login. After login in you can check that the NFS share is correctly mounted. Refer to the section “Testing NFS Client'.

Configuring E-mail Client on Vector Linux

E-mail Server: Ubuntu Jaunty using Postfix and Dovecot as IMAP server.

I configured a e-mail client using Seamonkey mail on the NFS client to read and write mails to other users. It's easy. In my case I am using an IMAP server so I need to specify the IMAP server name or IP address. The following figures are snapshots of setting up an e-mail account on the client.

Configuring LDAP Client on Vector Linux

LDAP server: Ubuntu Jaunty

The LDAP client application that I use is the Address book. You can add and use an LDAP

directory your address book. This will allow you to search the directory for email addresses and other information. You can also use the directory for address autocompletion when you addressing mail messages.

Steps to add LDAP directory to Address Book in SeaMonkey

1. Lauch SeaMonkey Email
2. Click Window --> Address Book
3. In Address Book, click File-->New--> LDAP directory
4. Key in the following:

    Name: example

    Hostname: ubuntu.example.com

    Base DN: dc=example,dc=com

To seach for entry in Address Book

In Seamonkey, click Window-->Address Book.

In Address Book, select the name of the address book that you just configured, in my case its called example.

Click example and search for the email address as show below:

Real Life Experience

Ubuntu Jaunty Server & Vector Linux 5.9 Client
The following are the services that are explored between Ubuntu Jaunty Server and Vector Linux 5.9 Client:

ssh – Vector client can easily ssh into Ubuntu but the other way can be mentally challenging.

DNS - ok
Mail – ok
NFS – ok
NIS – NIS client not configured yet in Vector

logging via xlogin using NIS/NFS – have not tried due to NIS client configuration in Vector

logging via xlogin using NFS - ok

LDAP: Address book – ok

Appendix F

Configure Secure Virtual Hosts

To configure a secure virtual host you need to take four basic steps:

- Enable the SSL module (alreaddy available from the default Apache packages)
- Create the SSL certificate
- Change the configuration files associated with a regular virtual host to limit its purview to the standard port 80 for regular websites.
- Create a a secure virtual host, based on the virtual host template just used for regular websites.

Enable the SSL Module

To include the SSL module in the Apache configuration, type:

```
root@ubuntu:~# a2enmod ssl

Enabling module ssl.

See /usr/share/doc/apache2.2-common/README.Debian.gz on how to configure SSL and
create self-signed certificates.

Run '/etc/init.d/apache2 restart' to activate new configuration!
```

The next time Apache is restarted, the ssl.conf and ssl.load files are included in the list of enabled modules in the /etc/apache2/mods-enabled directory. If you want to reverse the process, the a2dismod command will do just that.

```
root@ubuntu:~# /etc/init.d/./apache2 restart

   • Restarting web server apache2
     ... waiting [ OK ]
```

Create the SSL Certificate

Without a private-public SSL key, connections to secure websites using the https:// in a web browser won't be secure. Properly secured websites on the Internet use an official key pair generated by a CA. Official key pairs are expensive and are not required to learn how to configure a secure virtual websites. Encryption is based on a public private key infrasture. The filenames with encryption keys

listed in this section (server.key, server.csr, and server.crt) are arbitrary.

To create a self-signed certificate, you will use the openssl command.

Create the server.key. The following command generates RSA (genrsa) parameters for an encrytion key using the triple DES (-des3) encrytion standard, in the server.key file of 1024 bytes.

```
root@ubuntu:~# openssl genrsa -des3 -out server.key 1024

Generating RSA private key, 1024 bit long modulus

.....................................................................++++++

.++++++

e is 65537 (0x10001)

Enter pass phrase for server.key:

Verifying - Enter pass phrase for server.key:
```

The passphrase requires at least four characters.

After the server.key is available, create a Certificate Signing Request (CSR). The CSR can be sent to a CA for processing for a digital identity certificate. The openssl req command uses the X.509 standard to create a new key (-new-key) which sends output (-out) to the server.csr file.If you are setting up a server.csr to send to a CA, the entries should reflect your true identity.

```
root@ubuntu:~# openssl req -new -key server.key -out server.csr

Enter pass phrase for server.key:

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:SG

State or Province Name (full name) [Some-State]:OpenSource

Locality Name (eg, city) []:MyCity

Organization Name (eg, company) [Internet Widgits Pty Ltd]:GroupofTwo
```

```
Organizational Unit Name (eg, section) []:One Section

Common Name (eg, YOUR name) []:Ghazalisco

Email Address []:ismail@example.com



Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:1234

An optional company name []:company ghazalisco
```

```
Now you can submit the server.csr to a CA for processing.
```

For the purpose of this tutorial I will create a self-signed certificate

```
root@ubuntu:~# openssl x509 -req -days 30 -in server.csr -signkey server.key
-out server.crt

Signature ok

subject=/C=SG/ST=OpenSource/L=MyCity/O=GroupofTwo/OU=One
Section/CN=Ghazalisco/emailAddress=ismail@example.com

Getting Private key

Enter pass phrase for server.key:
```

Now that a server certificate (server.crt) and server key (server.key) are available in the local directory, the following command moves them to the appropriate directories, which will be used when configuring a secure virtual host.

root@ubuntu:~# cp server.crt /etc/ssl/certs/

root@ubuntu:~# cp server.key /etc/ssl/private/

Now your're about ready to create a secure virtual host. But first you need to prepare any existing regular hosts.

Prepare Existing Hosts

Create a Secure Virtual Host

To set up a secure virtual host, start with the 000-default file in the /etc/apasche2/sites-enabled directory as a template. Use it as a template. Copy the file as follows:

#cd /etc/apache2/sites-enabled
#cp 000-default secure1

In my case I just use an existing virtual site www.example.com. The configuration file is shown below:

```
root@ubuntu:/etc/apache2/sites-available# cat cheeyong.com

<VirtualHost 172.16.0.2:443>

ServerName cheeyong.com

ServerAlias www.cheeyong.com

ServerAdmin ismail@example.com

DocumentRoot /var/www/cheeyong.com/html

SSLEngine on

SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire

SSLCertificateFile /etc/ssl/certs/server.crt

SSLCertificateKeyFile /etc/ssl/private/server.key

ErrorLog /var/log/apache2/error.log



LogLevel warn



CustomLog /var/log/apache2/access.log combined

</VirtualHost>
```

The first secure virtual host requires a NameVIrtualHost directive that points to the TCP/IP port assosciated with secure web services:

NameVIrtualHost *:443

While this particular NameVirtualHost *.443 directive is requires only once, every secure virtual host requires a pointer to the same TCP/IP port, with the following virtual host container header:

<VirtualHost *:443>

Four directives are needed. They are:

SSLEngine on

SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire

SSLCertificateFile /etc/ssl/certs/server.crt

SSLCertificateKeyFile /etc/ssl/private/server.key

The first directive activates the SSL Engine
The second directive sets the SSL Options. The options here supports websites without a password (+FakeBasicAuth), use the SSL keys created (+ExportCertData) and deny access to inappropriate systems (+StrictRequire
)

The third and fourth directives access the certificae and key files just created.

You will then need to restart Apache. You should then be able to access the secure website in the same way you access any other secure website.

Just checking
You should check the /etc/apache2/ports.conf file that it contains the following line

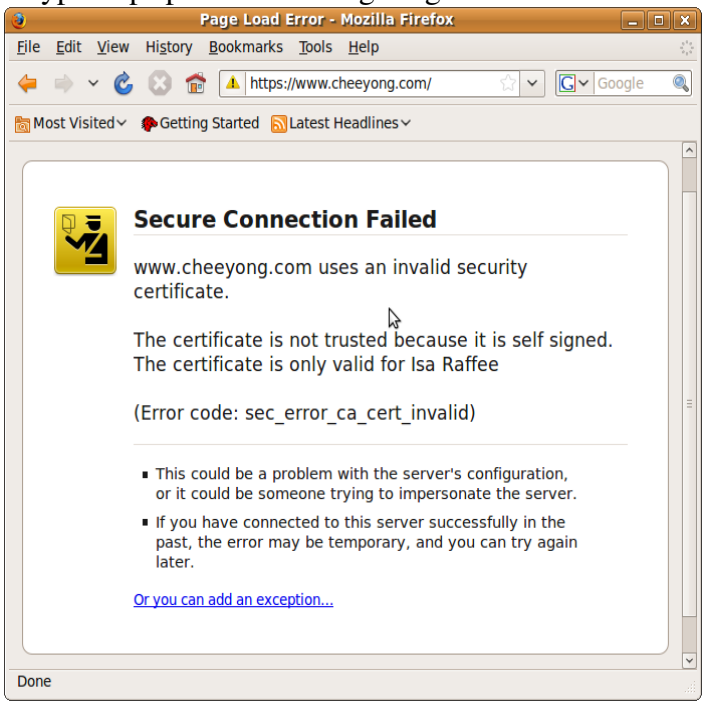
Listen 443

Restart Apache

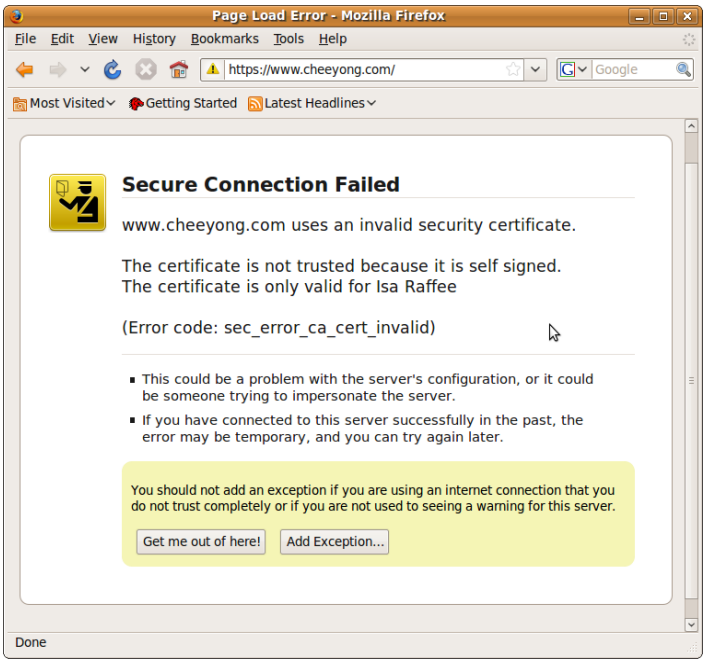
```
root@ubuntu:/etc/apache2/sites-enabled# /etc/init.d/./apache2 restart

 * Restarting web server apache2
Apache/2.2.11 mod_ssl/2.2.11 (Pass Phrase Dialog)

Some of your private key files are encrypted for security reasons.

In order to read them you have to provide the pass phrases.

Server ubuntu.example.com:443 (RSA)

Enter pass phrase:

OK: Pass Phrase Dialog successful.
                                                                        [ OK ]
```

Launch the Secure Website

In my case I have configured the virtual website www.cheeyong.com as a secure virtual host. To access the site, you must type https prefix at the begining of the URL.



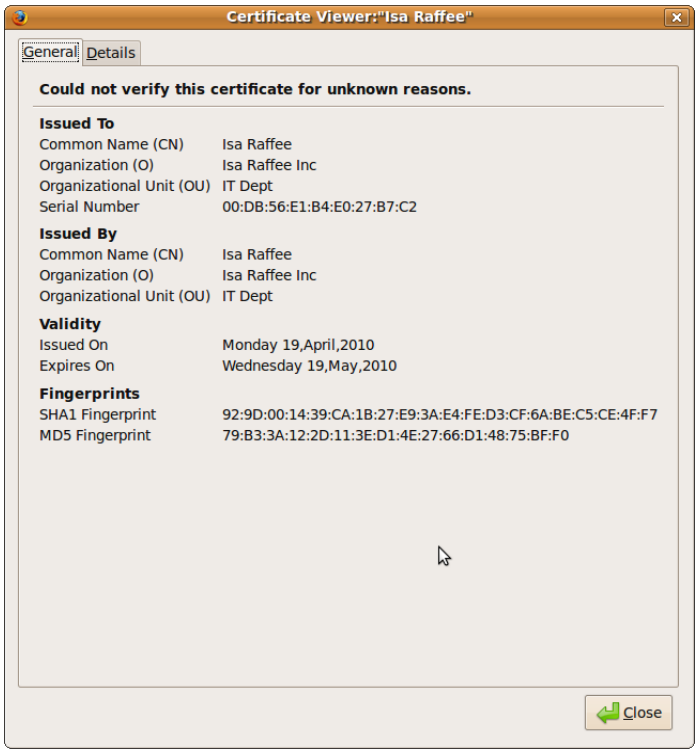
Click the hyperlink “Or you can add an exception...”



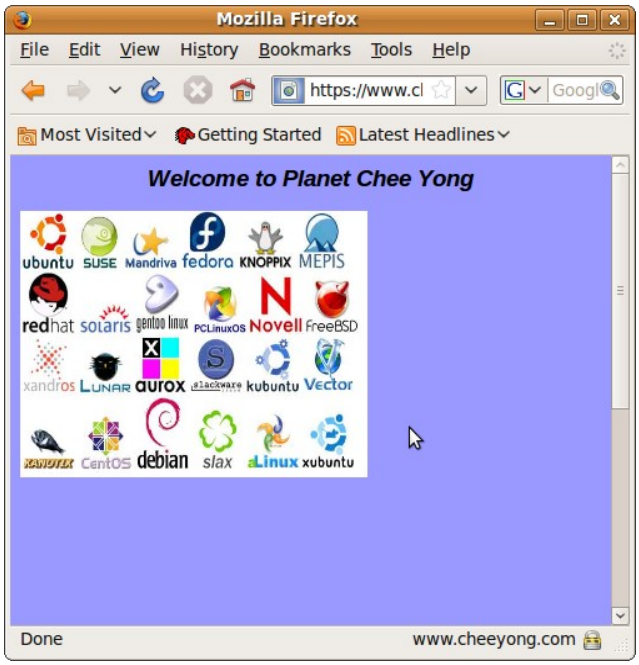
Click the “Add exception” button

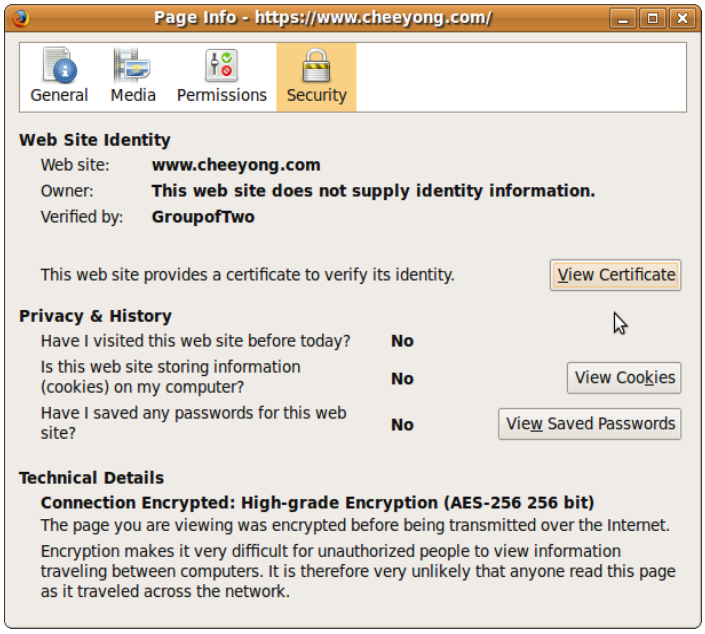
Click the “Get Certificate” button.

After you click the “Get Certificate” button the View button is enabled and click it to view the certificate details. If you look carefully, there is a check box which says “Permanently store this exception”. If you tick this the next time you visit the secure site, you will not be prompted to add the security exception. In my case I leave it uncheck.

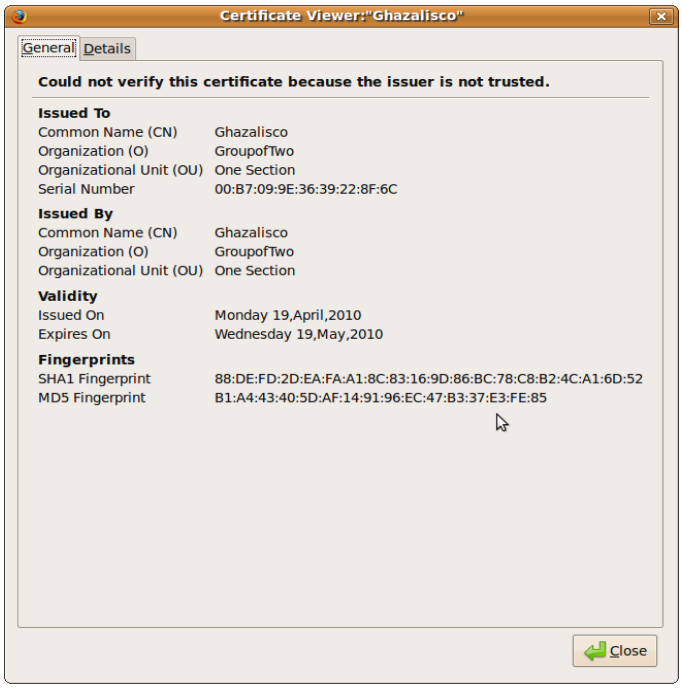


Finally the secure site is displayed. Notice the padlock icon at the bottom right corner of the website. You can click this icon to view the certificate information.





Click the View Certificate button.



The Apache Control Command

The apache2ctl is a front end to the Apache daemon:

root@ubuntu:~# apache2ctl

Usage: /usr/sbin/apache2ctl start|stop|restart|graceful|graceful-stop|configtest|status|fullstatus

/usr/sbin/apache2ctl <apache2 args>

To restart and stop without interrupting any currently active connections, type:

root@ubuntu:~# apache2ctl graceful

or

root@ubuntu:~# apache2ctl graceful-stop

Real life situations

```
In my case, after I had configured secure virtual sites, Apache could not start
properly. The processes that were running were as shown below

root@ubuntu:~# ps -ef|grep apache

root      3886  2292  0 07:09 tty8     00:00:00 /bin/sh -e /etc/rc2.d/S91apache2 start

root      3897  3886  0 07:09 tty8     00:00:00 /bin/sh /usr/sbin/apache2ctl start

root      3902  3897  0 07:09 tty8     00:00:00 /usr/sbin/apache2 -k start

root      5315  4662  0 07:24 pts/0    00:00:00 grep apache

I could not load any websites and thus I had to restart the Apache daemons. The
apace2ctl command s and the init scripts command could not stop or restart the Apache
daemons as shown below:

root@ubuntu:~# apache2ctl restart

httpd not running, trying to start

(98)Address already in use: make_sock: could not bind to address 0.0.0.0:80

no listening sockets available, shutting down

Unable to open logs

So I have to use the kill command as shown below.

root@ubuntu:~# ps -ef|grep apache

root      3886  2292  0 07:09 tty8     00:00:00 /bin/sh -e /etc/rc2.d/S91apache2 start

root      3897  3886  0 07:09 tty8     00:00:00 /bin/sh /usr/sbin/apache2ctl start

root      3902  3897  0 07:09 tty8     00:00:00 /usr/sbin/apache2 -k start

root      5315  4662  0 07:24 pts/0    00:00:00 grep apache

root@ubuntu:~# kill -9 3897

root@ubuntu:~# ps -ef|grep apache

root      5432  4662  0 07:24 pts/0    00:00:00 grep apache

root@ubuntu:~#

root@ubuntu:~# apache2ctl start

Apache/2.2.11 mod_ssl/2.2.11 (Pass Phrase Dialog)

Some of your private key files are encrypted for security reasons.

In order to read them you have to provide the pass phrases.



Server cheeyong.com:443 (RSA)
```

```
Enter pass phrase:


OK: Pass Phrase Dialog successful.

root@ubuntu:~# ps -ef|grep apache

root      5562     1  1 07:25 ?        00:00:00 /usr/sbin/apache2 -k start

www-data  5564  5562  0 07:25 ?        00:00:00 /usr/sbin/apache2 -k start

www-data  5565  5562  0 07:25 ?        00:00:00 /usr/sbin/apache2 -k start

www-data  5566  5562  0 07:25 ?        00:00:00 /usr/sbin/apache2 -k start

www-data  5567  5562  0 07:25 ?        00:00:00 /usr/sbin/apache2 -k start

www-data  5568  5562  0 07:25 ?        00:00:00 /usr/sbin/apache2 -k start

root      5570  4662  0 07:25 pts/0    00:00:00 grep apache
```

Let's now explore the other options when used with the apache2ctl command.

Using the status option

```
root@ubuntu:~# apache2ctl status

Forbidden


You don't have permission to access /server-status on this server.


-------------------------------------------------------------------------


Apache/2.2.11 (Ubuntu) PHP/5.2.6-3ubuntu4.5 with Suhosin-Patch mod_ssl/2.2.11

OpenSSL/0.9.8g Server at localhost Port 80
```

Using the fullstatus option

```
root@ubuntu:~# apache2ctl fullstatus

Forbidden


You don't have permission to access /server-status on this server.


-------------------------------------------------------------------------
```

```
Apache/2.2.11 (Ubuntu) PHP/5.2.6-3ubuntu4.5 with Suhosin-Patch mod_ssl/2.2.11

OpenSSL/0.9.8g Server at localhost Port 80
```

Not much different with the status option

Using the configtest option

```
root@ubuntu:~# apache2ctl configtest

Syntax OK
```

This option is useful in checking the syntax for the /etc/apache2 apache2.conf files.

Using the -S

```
root@ubuntu:~# apache2ctl -S

VirtualHost configuration:

172.16.0.2:80          is a NameVirtualHost

         default server example.com (/etc/apache2/sites-enabled/example.com:1)

         port 80 namevhost example.com (/etc/apache2/sites-enabled/example.com:1)

         port 80 namevhost ismail.com (/etc/apache2/sites-enabled/ismail.com:1)

172.16.0.2:443         cheeyong.com (/etc/apache2/sites-enabled/cheeyong.com:1)

wildcard NameVirtualHosts and _default_ servers:

*:80                   is a NameVirtualHost

         default server ubuntu.example.com (/etc/apache2/sites-enabled/000-default:1)

         port 80 namevhost ubuntu.example.com (/etc/apache2/sites-enabled/000-default:1)

         port 80 namevhost ubuntu.example.com (/etc/apache2/sites-enabled/000-
default.bkp:1)

Syntax OK
```

This option displays the TCP/IP port numbers, configuration files for each regular and secure virtual host.