As Per New Revised Syllabus of
University of Mumbai
(w.e.f. 2018-2019)

ISBN :

Lab Manual for Linux Server Administration (USCS502) T.Y.B.Sc. Computer Science, Semester V

Dr. Girish Tere
Asst. Professor,
Dept. of Computer Science,
Thakur College of Science and Commerce
(Affiliated to University of Mumbai)

Lab Manual for Linux Server Administration

T.Y.B.Sc. (Computer Science) Sem V, University of Mumbai

Author: **Dr. Girish Tere, Asst. Professor,**
Department of Computer Science,
Thakur College of Science and Commerce,

First Edition: 2018

Printed at: **Thakur College of Science and Commerce,**
Thakur Village, Kandivali East,
Mumbai

Published by: **Thakur College of Science and Commerce,**
Thakur Village, Kandivali East,
Mumbai 400101
Website: http://tcsc.org.in

Preface:

I am very happy to prepare this Lab manual on Linux Server Administration for new syllabus of T.Y.B.Sc. CS (Sem V) students (w.e.f. 2018-2019). There are many Linux distributions based on mainly Red Hat Distribution family and Debian family. Practicals can be performed on any Linux OS. It may be main machine or it may be VM in VirtualBox or VMware Player. This manual illustrates the experiments and students need to perform practical on their given environment.

I am very thankful to Trustee of our college, **Shri Jitendra Singhji**, **Shri Manoj Singh**, who gave us all resources and always motivated us to work for students. I feel very happy and proud to work with our beloved Principal Madam, **Dr. (Mrs.) C. T. Chakraborty**. She always encourage us and demonstrates us, how to be happy in Life. I would like to express my sincere gratitude to Principal Madam for allowing me to write such Lab Manual for our students.

I would also like to express my sincere gratitude and deep appreciation to Head of Department, Ashish Trivedi Sir and all my colleagues in College and University of Mumbai. I am very thankful to my friend Mandar Bhave, Head of CS and IT Dept, D. G. Ruparel College, who has helped me a lot in completing Linux experiments.

-Dr. Girish Tere

USCS502: Linux Server Administration (Practical List)

- Practical shall be performed using any Linux Server (with 8GB RAM).

- Internet connection will be required so that Linux server (command line mode) can be connected to Internet.

1. Install DHCP Server in Ubuntu 16.04
2. Initial settings: Add a User, Network Settings, Change to static IP address, Disable IPv6 if not needed, Configure Services, display the list of services which are running, Stop and turn OFF auto-start setting for a service if you don't need it, Sudo Settings
3. Configure NTP Server (NTPd), Install and Configure NTPd, Configure NTP Client (Ubuntu and Windows)
4. SSH Server : Password Authentication
   Configure SSH Server to manage a server from the remote computer, SSH Client : (Ubuntu and Windows)
5. *Install DNS Server BIND, Configure DNS server which resolves domain name or IP address, Install BIND 9, Configure BIND, Limit ranges you allow to access if needed.*
6. *Configure DHCP Server, Configure DHCP (Dynamic Host Configuration Protocol) Server, Configure NFS Server to share directories on your Network, Configure NFS Client. (Ubuntu and Windows Client OS)*
7. *Configure LDAP Server, Configure LDAP Server in order to share users' accounts in your local networks, Add LDAP User Accounts in the OpenLDAP Server, Configure LDAP Client in order to share users' accounts in your local networks. Install phpLDAPadmin to operate LDAP server via Web browser.*
8. *Configure NIS Server in order to share users' accounts in your local networks, Configure NIS Client to bind NIS Server.*
9. *Install MySQL to configure database server, Install phpMyAdmin to operate MySQL on web browser from Clients.*
10. *Install Samba to share folders or files between Windows and Linux.*

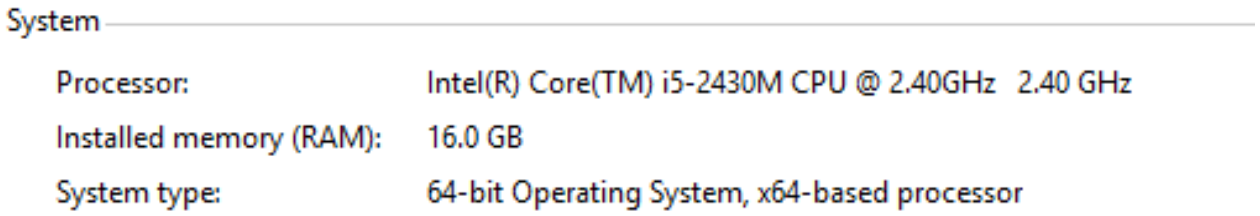
Using Ubuntu 16.04.4 LTS (Xenial Xerus)

Experiment 0: Ubuntu 16.04 LTS : Install

Aim: Install Ubuntu 16.04 LTS Desktop

Setup:

PC:

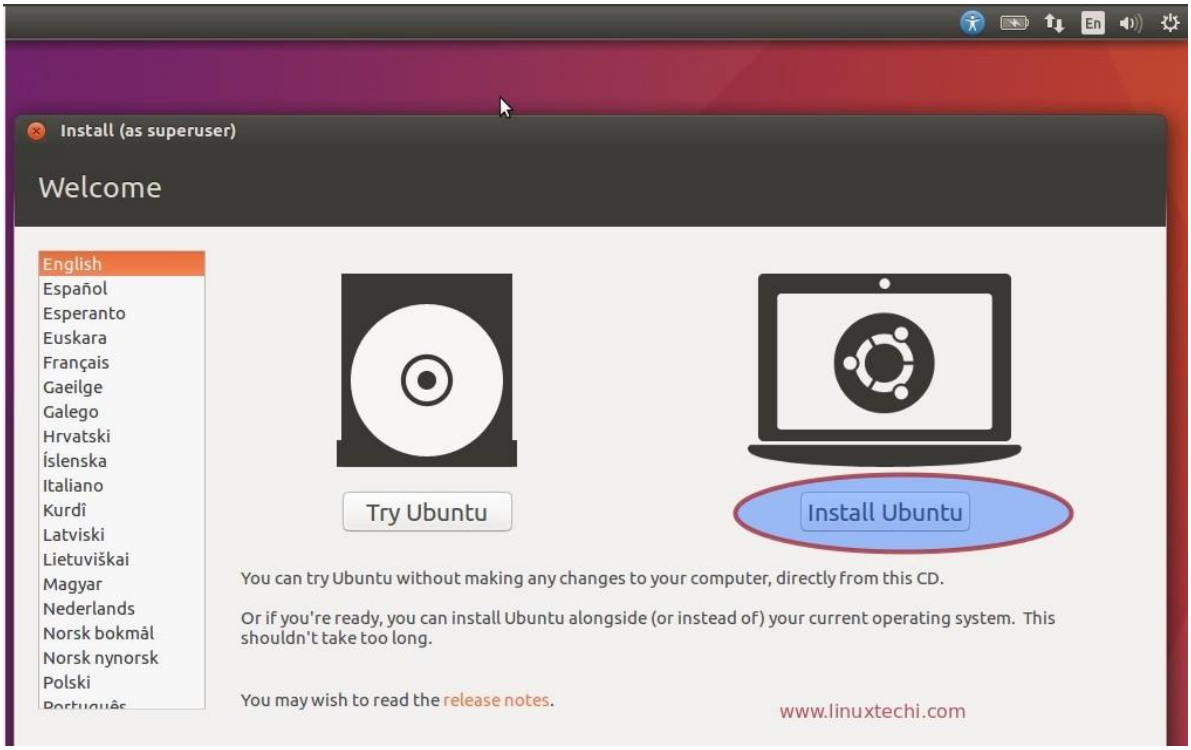


Ubuntu 16.04 LTS code name '**Xenial Xerus**' has been released recently on 21st April 2016. As this release is under LTS(Long Term Support) so its Desktop support will be for next 5 years and Server support will be for next 3 years. Some of new improved features of Ubuntu 16.04 LTS are listed below :

- New Linux Kernel 4.4
- Snap – New application Package format
- Introduction of LXD – new Container hypervisor on Linux, In Ubuntu 16.04 LTS docker containers can run inside LXD.
- Latest version of Openstack Mitaka included in this release.
- Ubuntu 16.04 will support IBM Z and LinuxONE Servers
- Python 3
- PHP 7
- Gnome Desktop 3.18
- Chromium 48
- LibreOffice 5.1

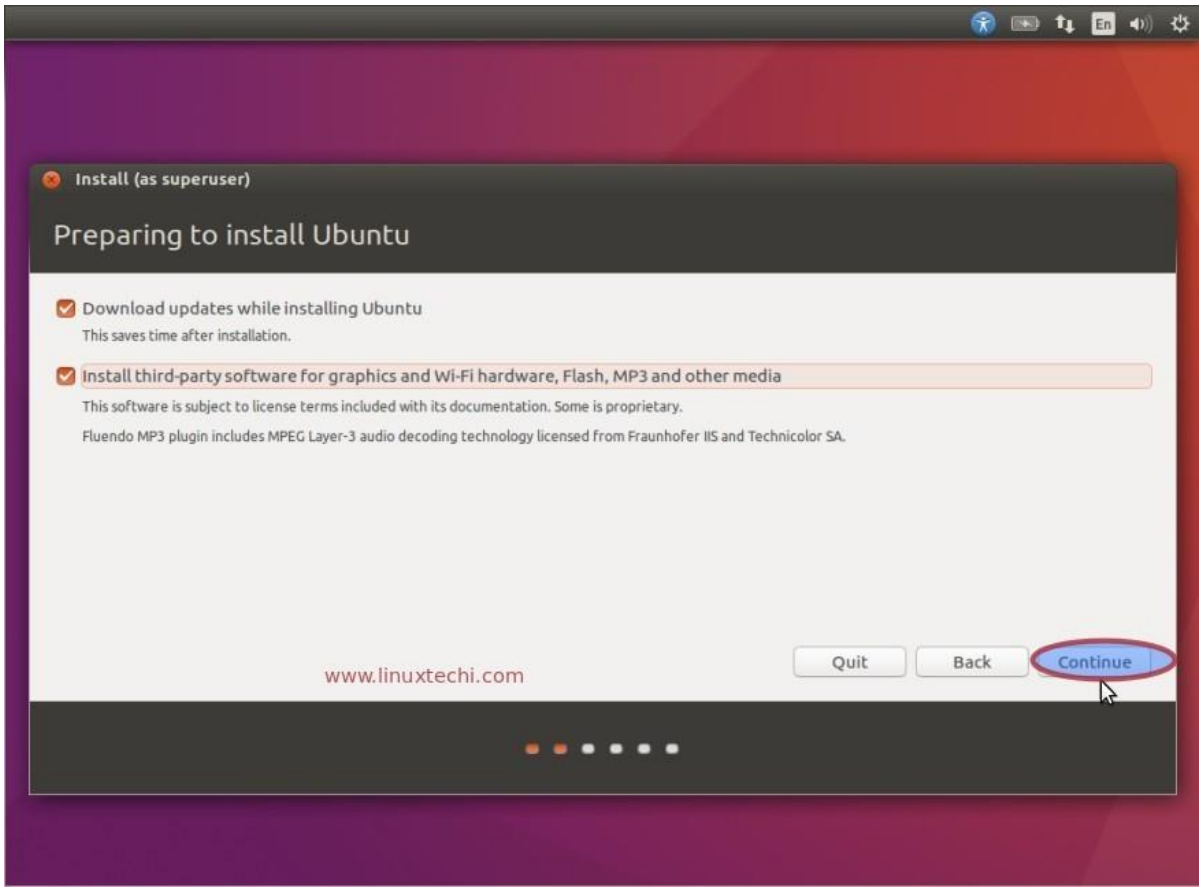
Step:1 Download Ubuntu 16.04 LTS ISO file.
Download ISO file of Ubuntu 16.04 LTS from their official Web site.
http://www.ubuntu.com/download/desktop
Once the ISO file is downloaded, burn it into a USB pendrive or DVD and Boot your system with bootable USB Pen drive or DVD, below screen will appear which is shown in step 2

Step:2 Select 'Install Ubuntu' to start installation.



Step:3 Preparing to Install Ubuntu 16.04 LTS

In case your system is connected to the Internet and wants to install third party tools during installation, you can select both the options as shown in below snap otherwise leave the options uncheck.

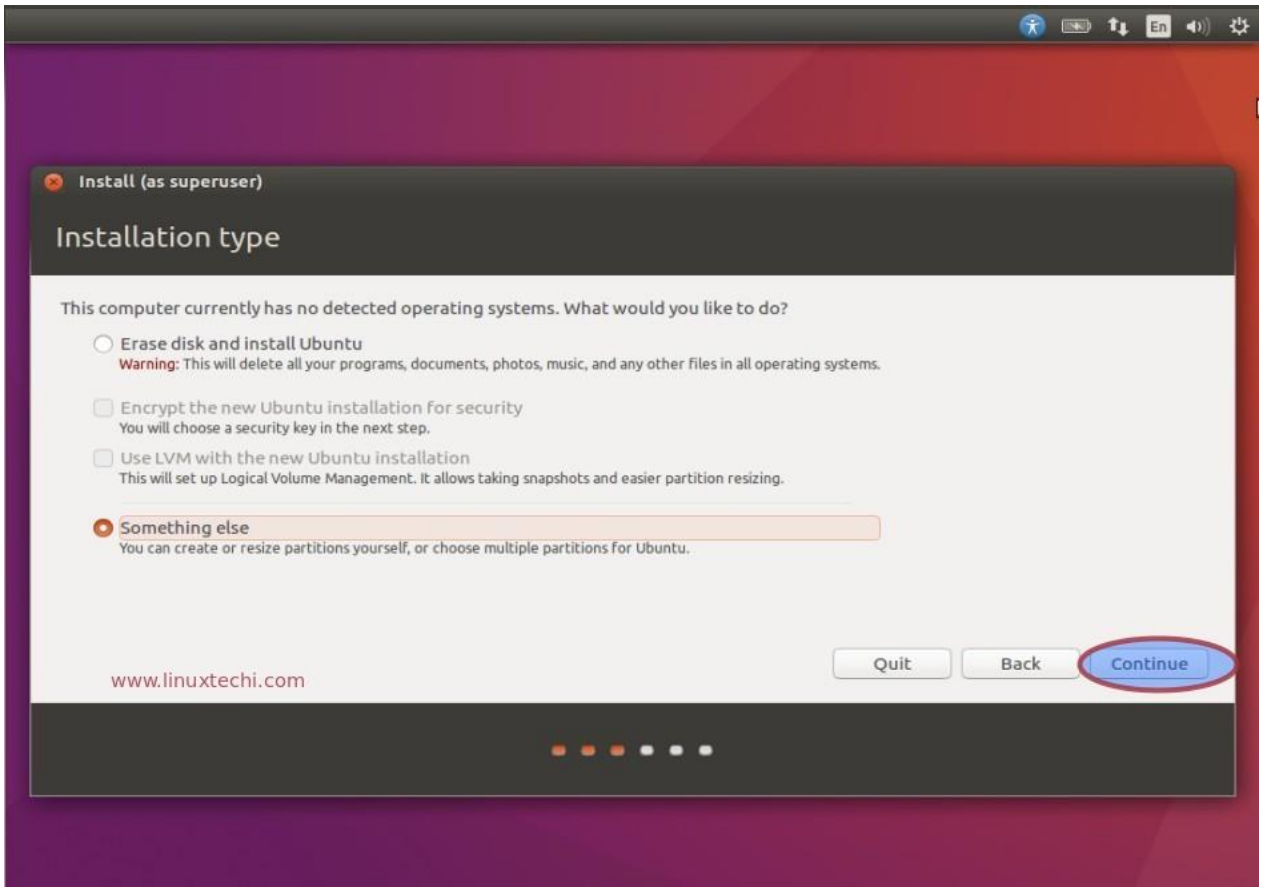


Click on **Continue** to proceed further.

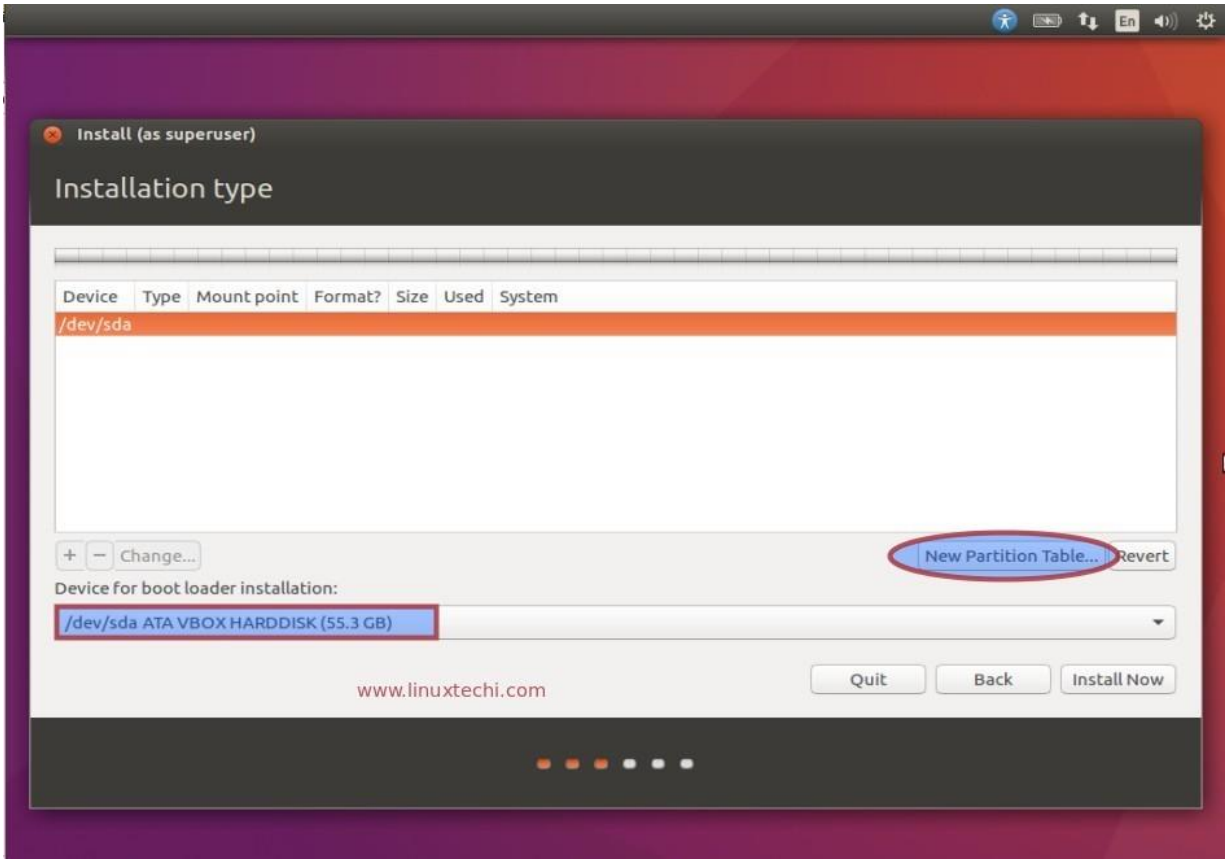
Step:4 Choose 'something else' option to create customize partition scheme.

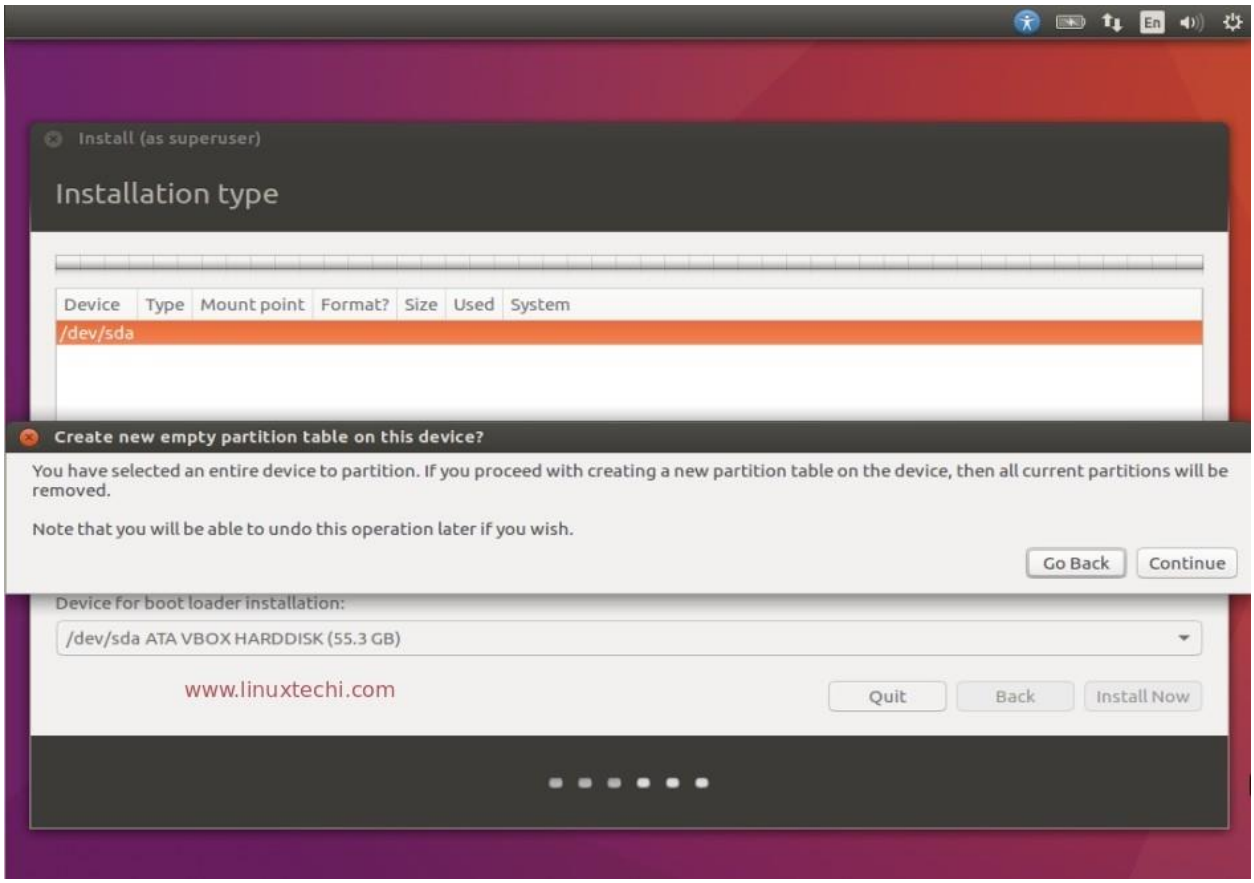
If you are planning to create your own customize partition table then select '**something else**' option in the below screen and Click on Continue.

In case you Select the first option '**erase disk and install ubuntu**', it will delete all data on disk and will install Ubuntu with the default partition scheme.



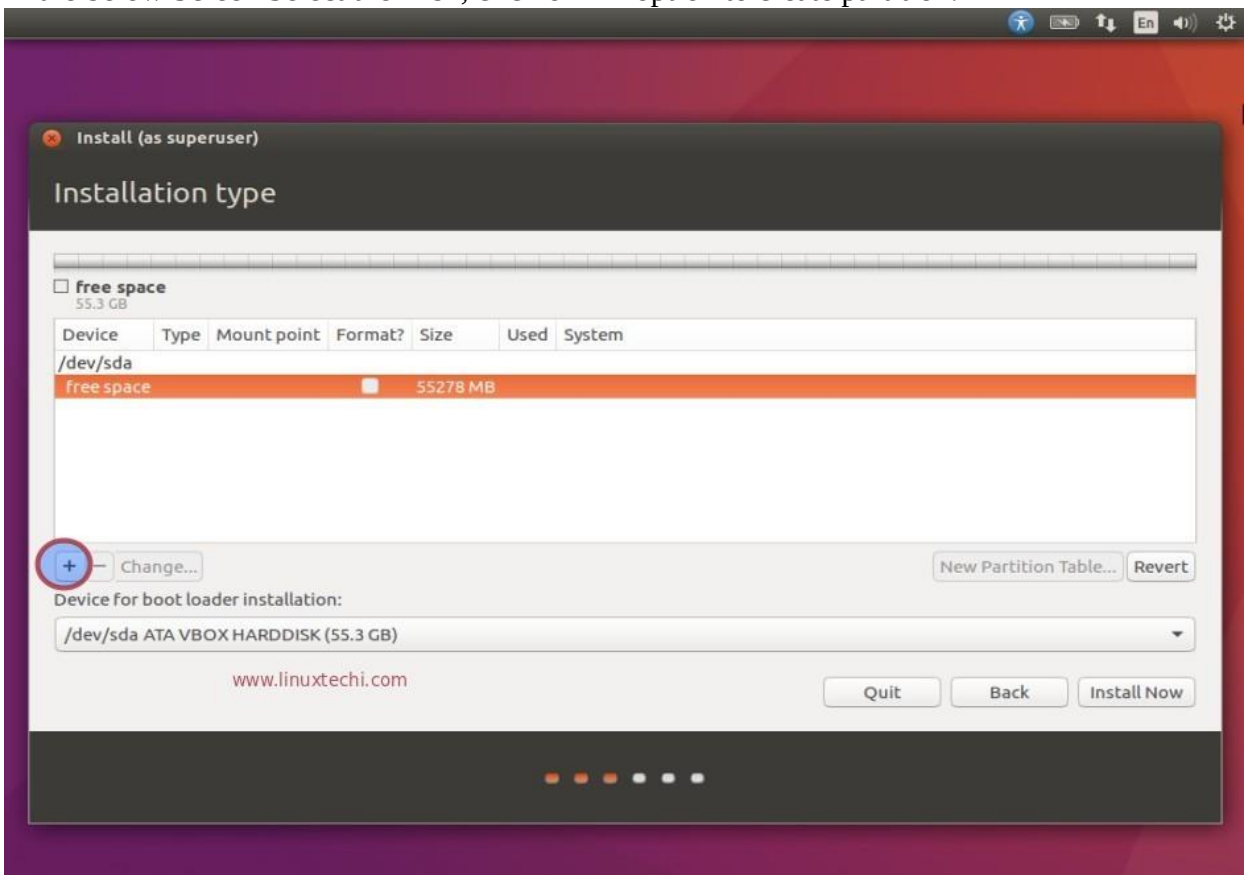
Click on New Partition Table.



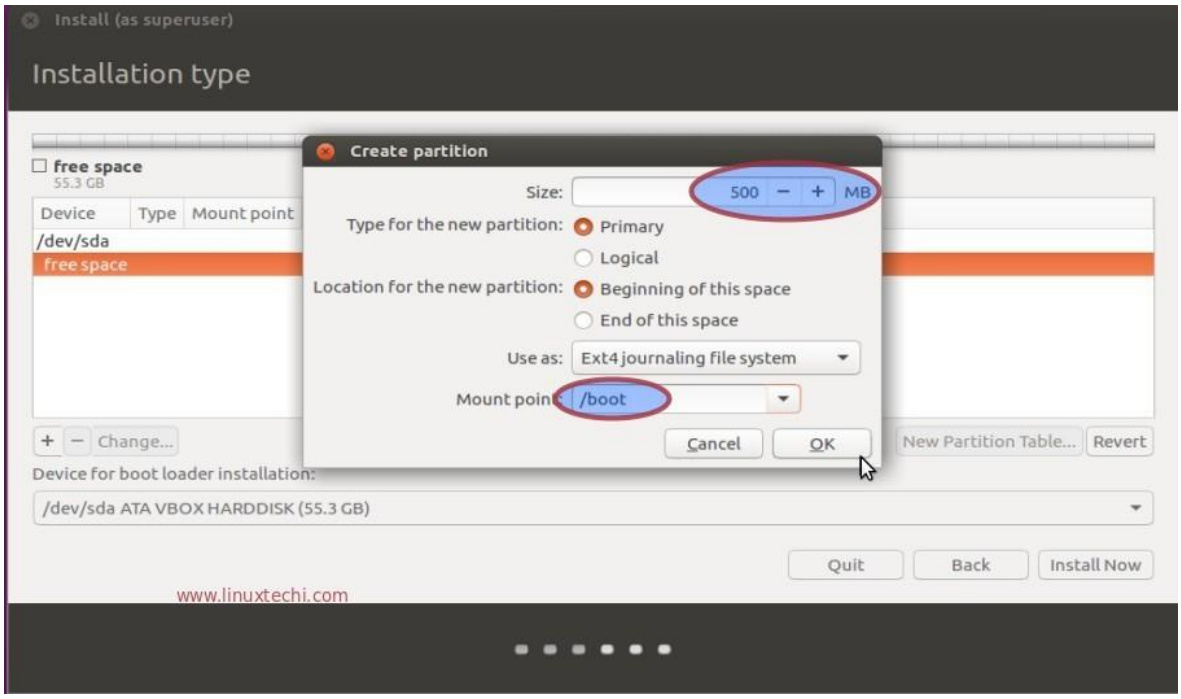


Click on Continue.

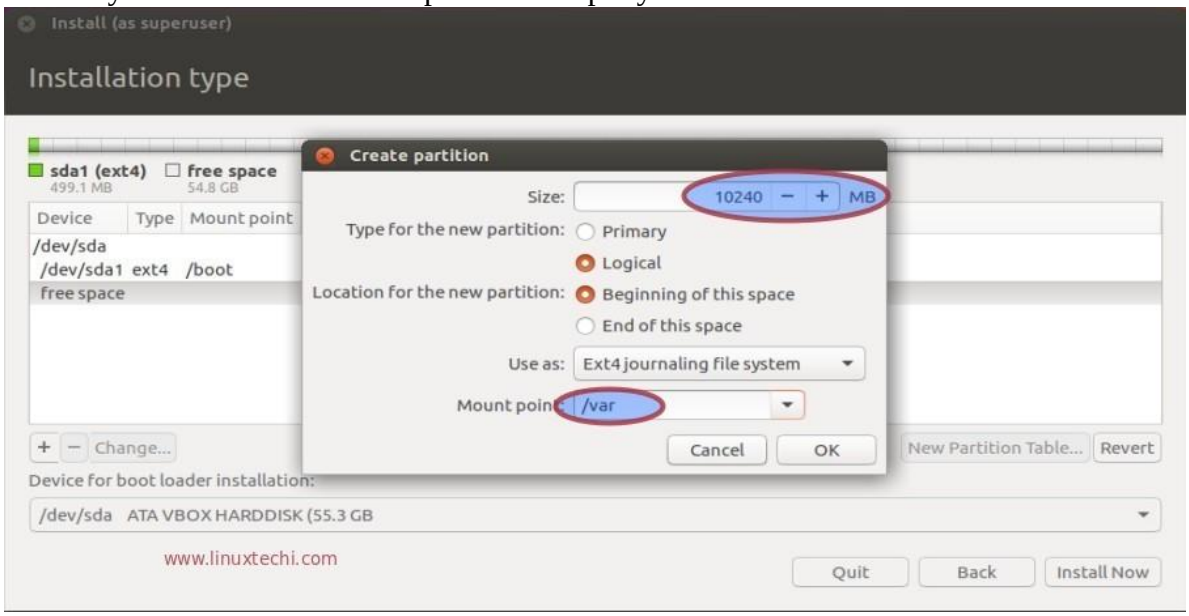
In the below Screen Select the Disk, click on '+' option to create partition.

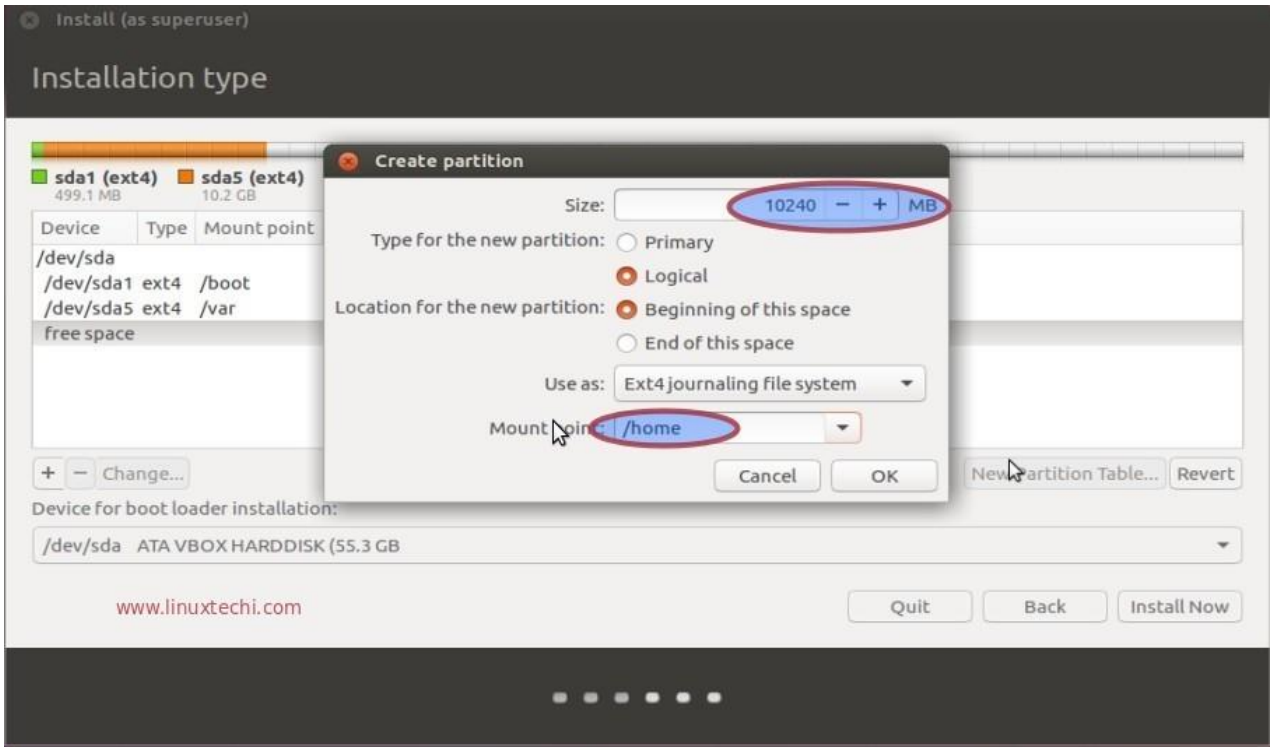


Specify the mount point as **/boot** and File system type as **ext4** and partition size as 500 MB.

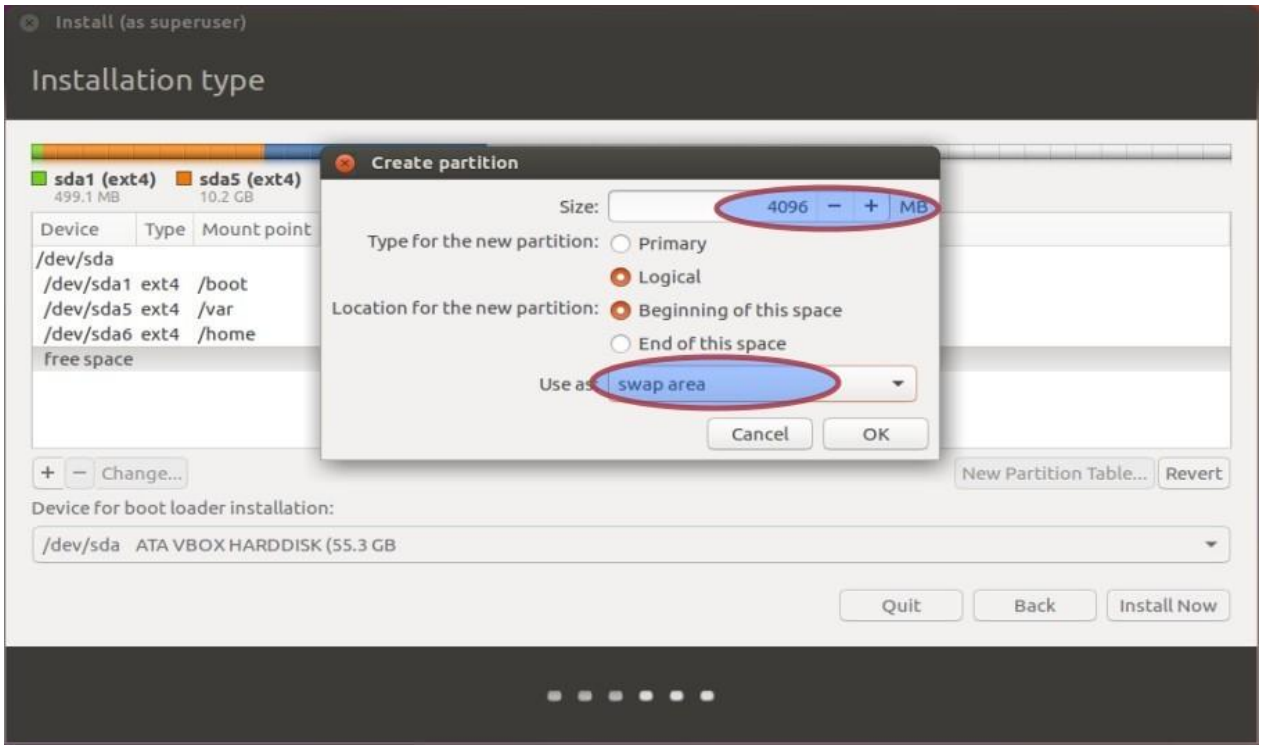


Similarly create **/var** and **/home** partitions as per your available disk.

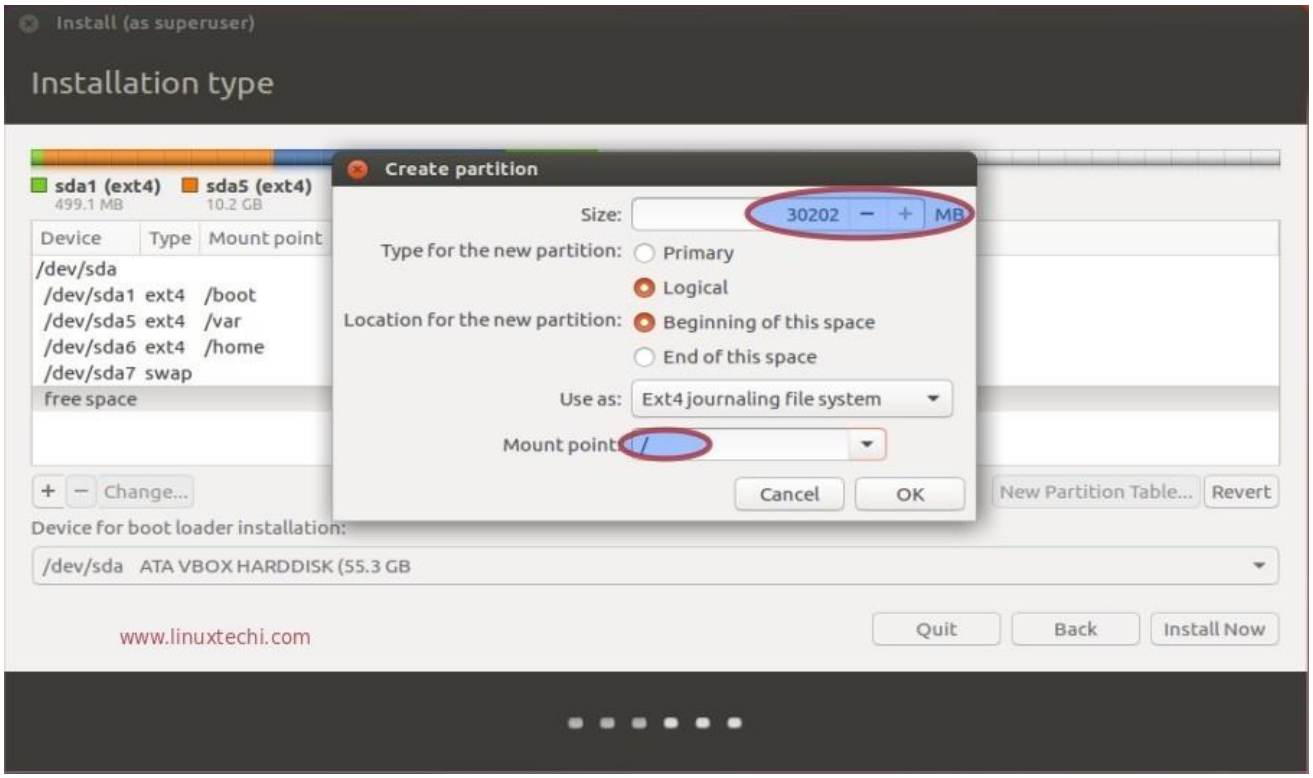




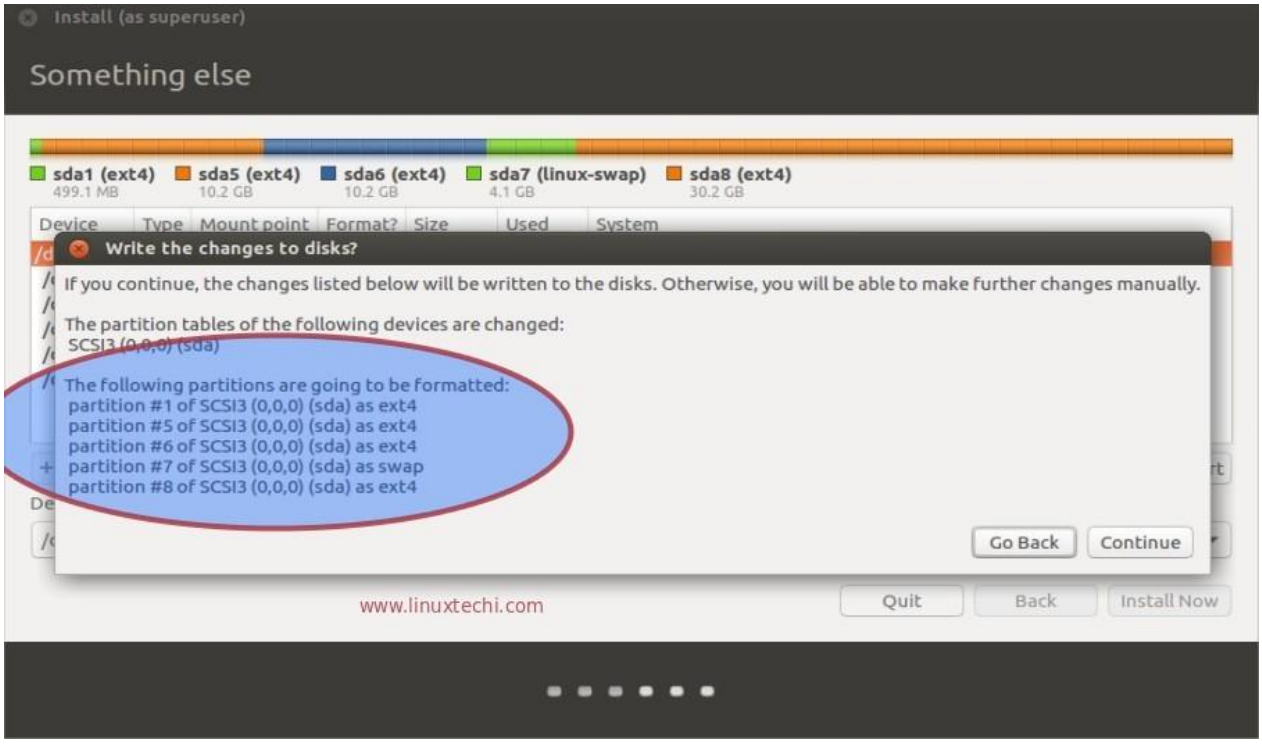
Create a Swap partition and size of swap should be double of your RAM, in my case RAM size is 2 GB so swap size should be 4 GB.



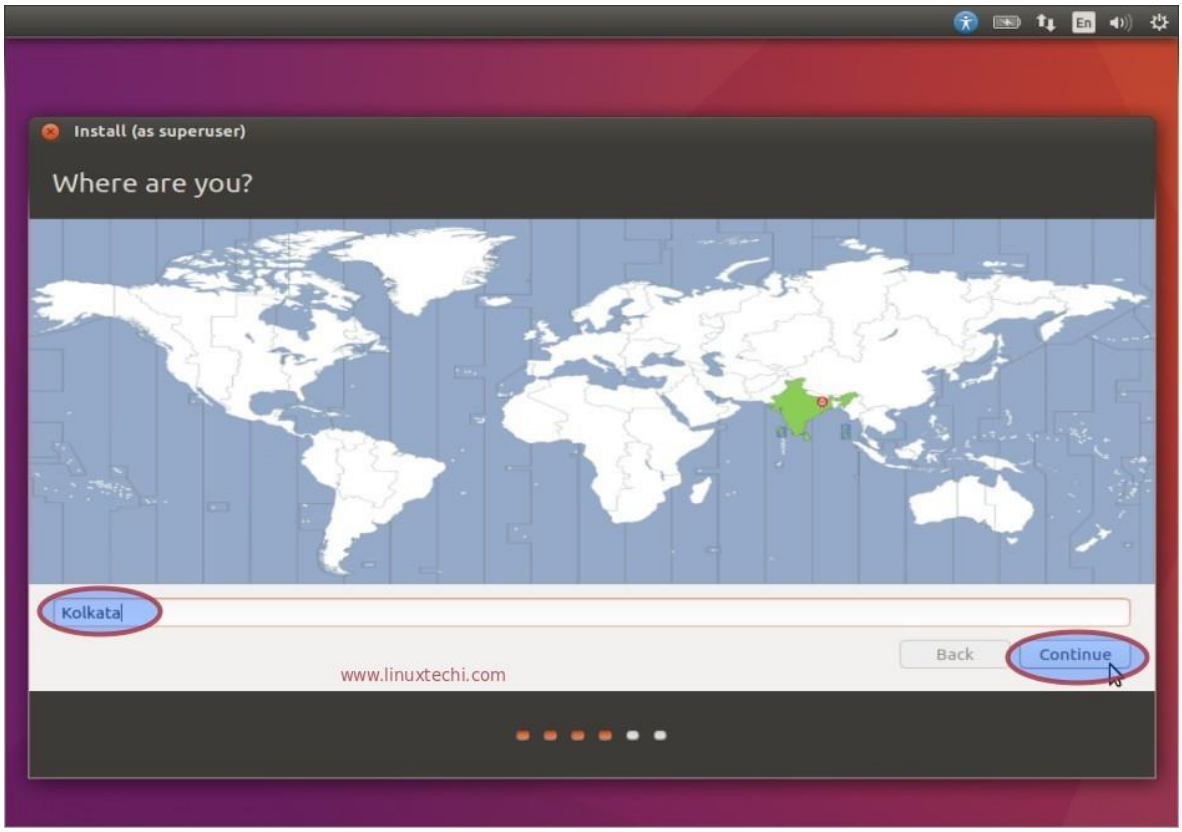
In the last create '/' partition on remaining size and file system type should be ext4.



Once you are done with partition table click on '**Install Now**'. It will show the below screen, click on Continue to Proceed.

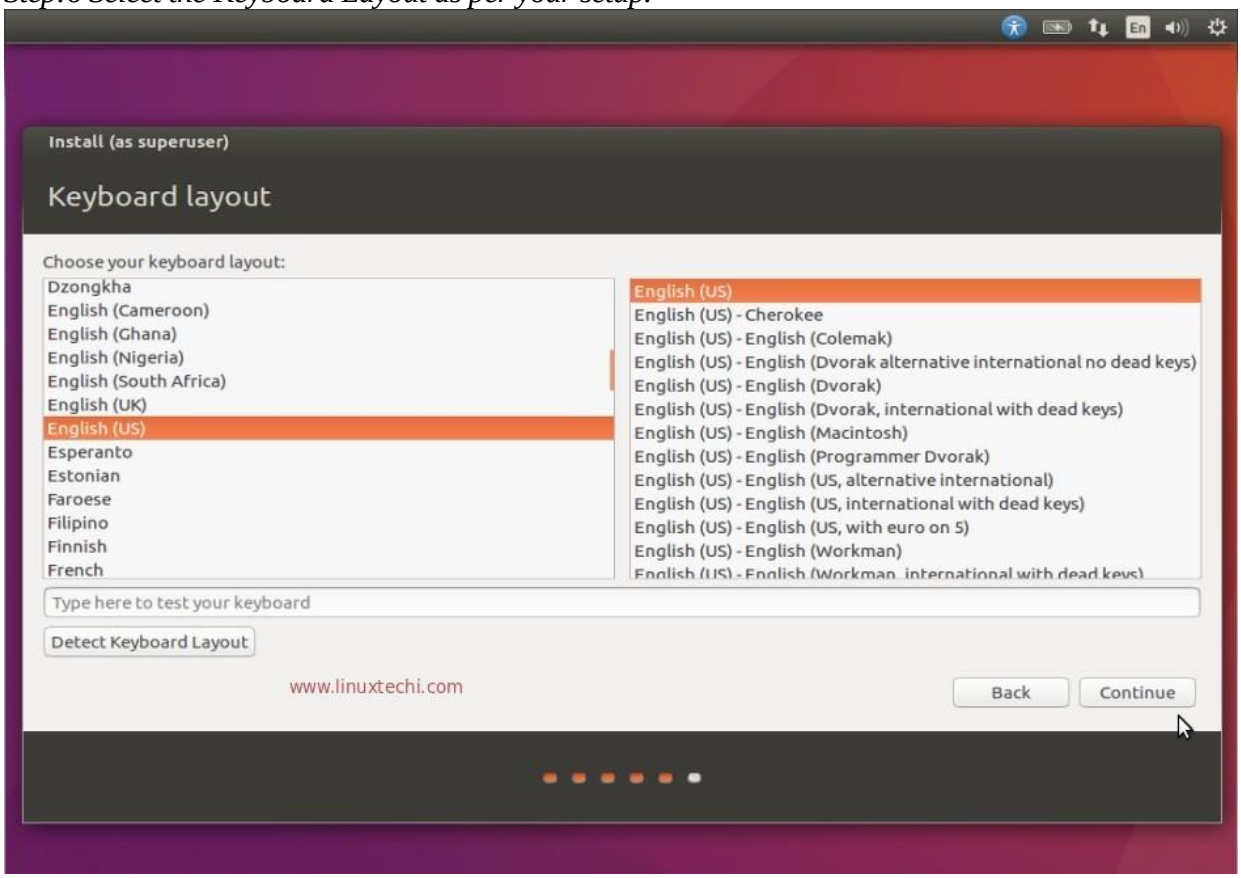


Step:5 Specify the Time Zone as per your location.



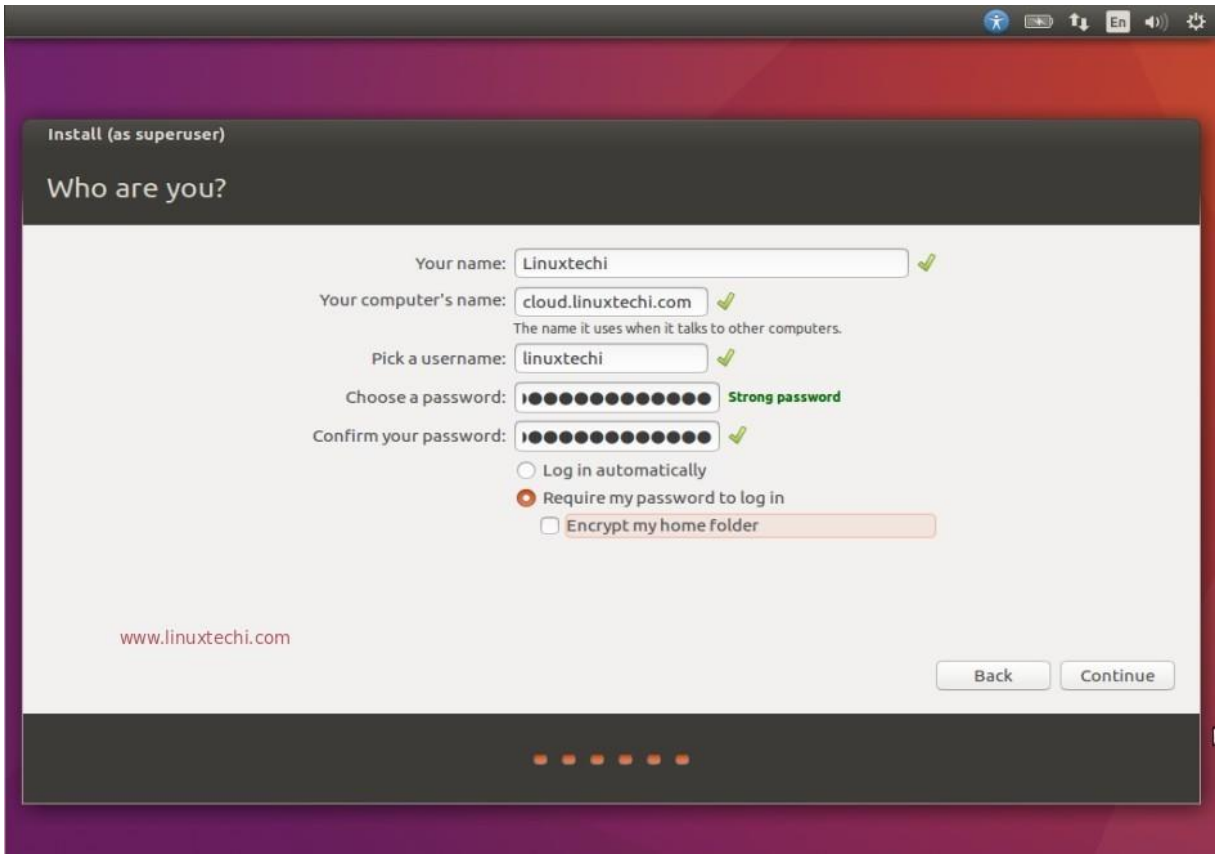
Click on Continue.

Step:6 Select the Keyboard Layout as per your setup.



Step:7 Specify the Hostname, User name and its password.

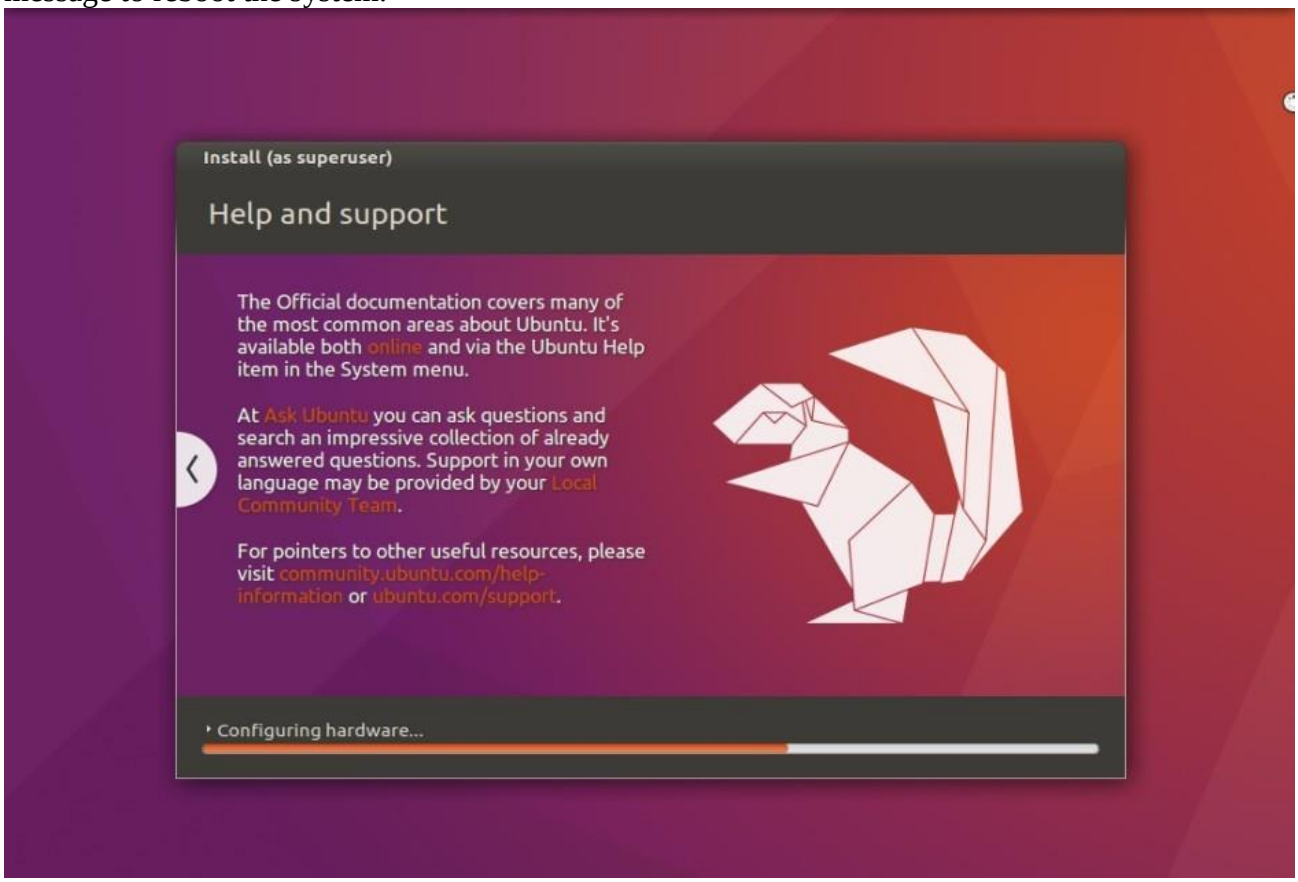
In this step specify the hostname for your system, user name and its password. We will using this user to login to the system after the installation.



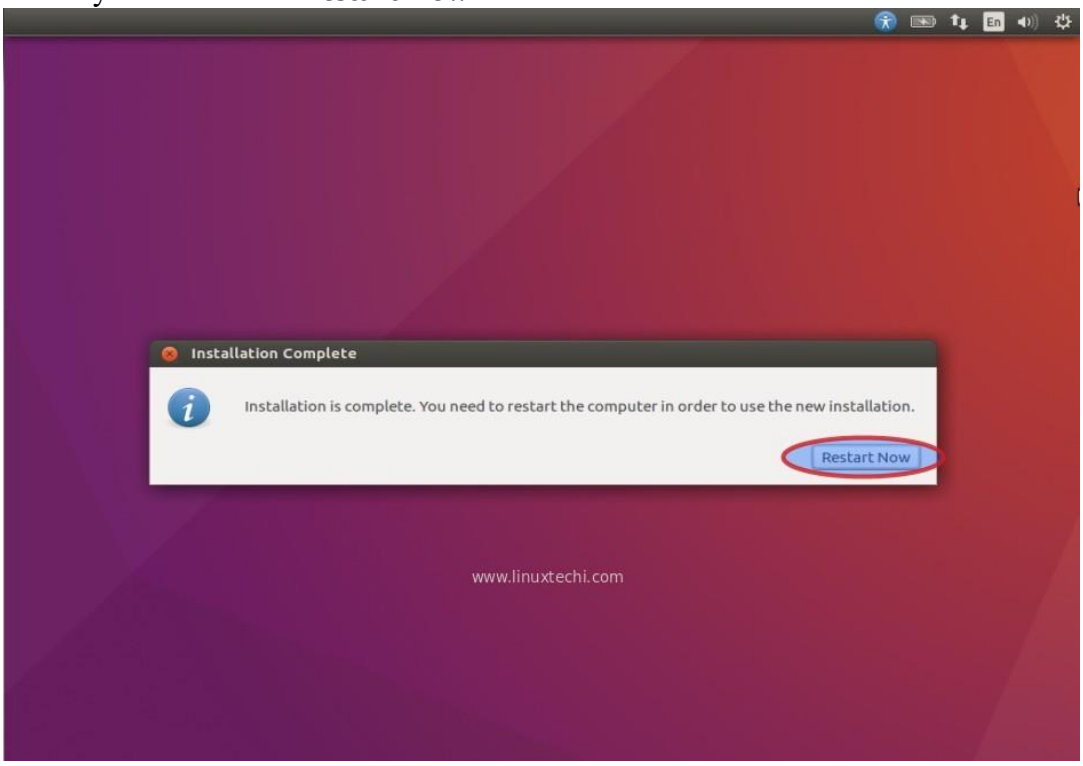
Click on Continue to start the installation

Step:8 Installation is in Progress.

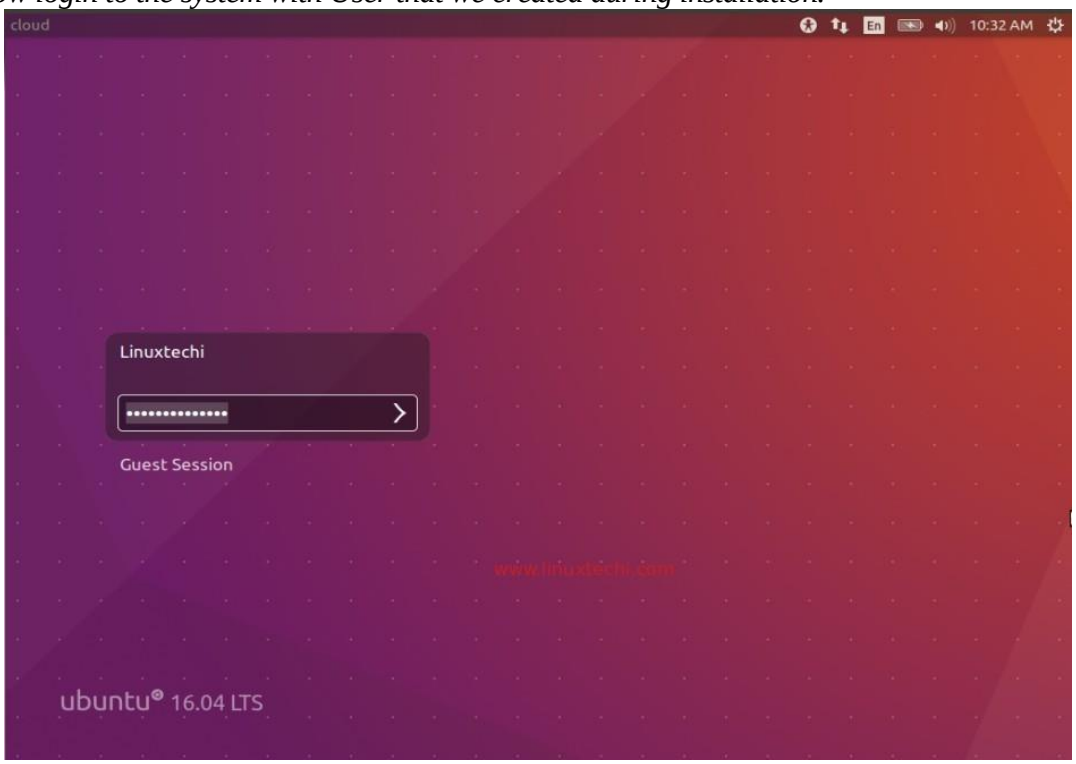
As we can see below that installation is progress, once the installation is completed we will get the message to reboot the system.

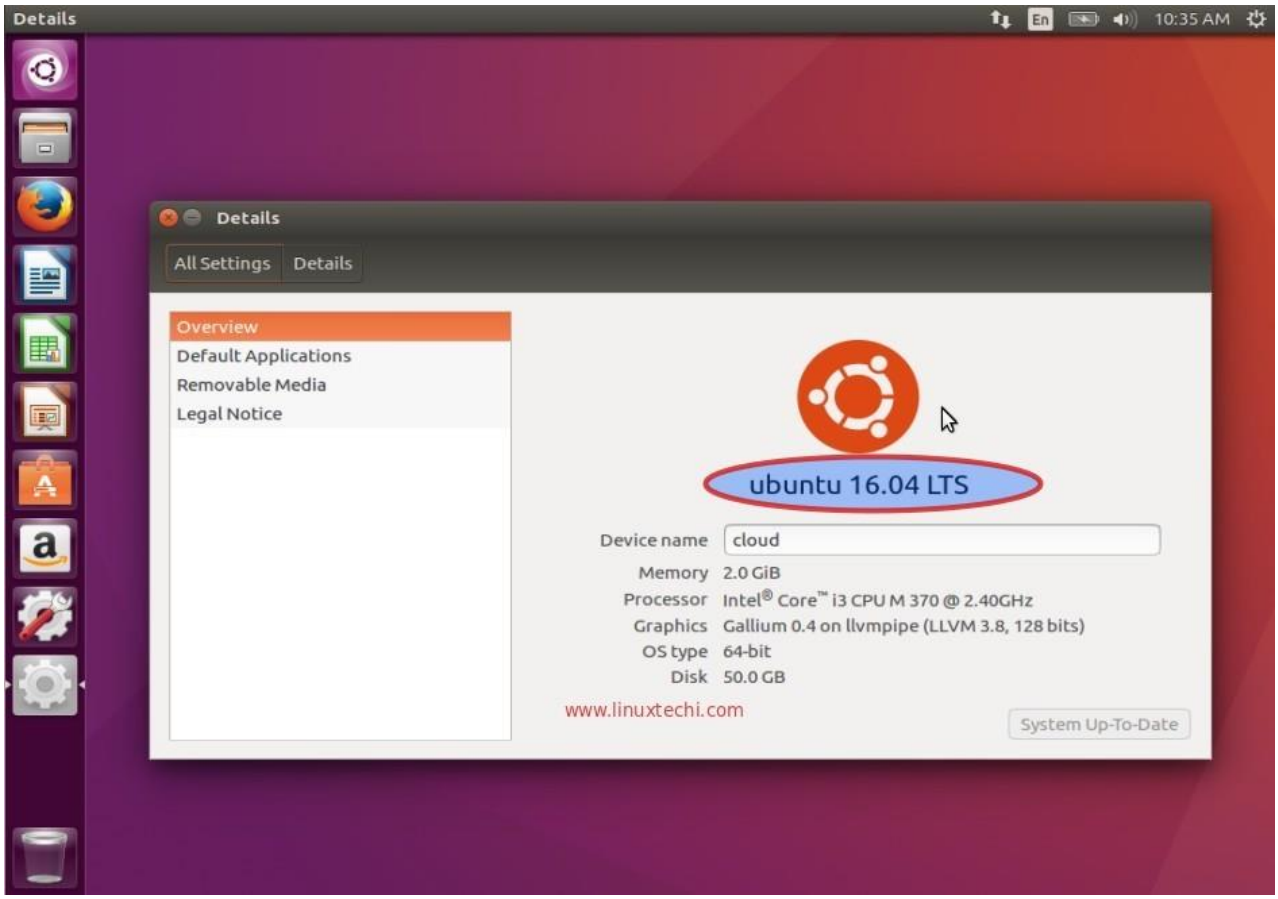


To Reboot the system click on '**Restart Now**'



Step:9 Now login to the system with User that we created during installation.





Installation of Ubuntu 16.04 LTS is completed.

Conclusions:

- Installed Ubuntu 16.04 LTS Desktop 64 bit OS
- Username:
- Password:
- IP address:
- HostName:

Courtesy: https://www.linuxtechi.com/install-ubuntu-16-04-with-screenshots/

Experiment 1:DHCP Server

The Dynamic Host Configuration Protocol (DHCP) is a network service that enables host computers to be automatically assigned settings from a server as opposed to manually configuring each network host. Computers configured to be DHCP clients have no control over the settings they receive from the DHCP server, and the configuration is transparent to the computer's user.

The most common settings provided by a DHCP server to DHCP clients include:
• IP address and netmask
• IP address of the default-gateway to use
• IP adresses of the DNS servers to use

The advantage of using DHCP is that changes to the network, for example a change in the address of the DNS server, need only be changed at the DHCP server, and all network hosts will be reconfigured the next time their DHCP clients poll the DHCP server. As an added advantage, it is also easier to integrate new computers into the network, as there is no need to check for the availability of an IP address. Conflicts in IP address allocation are also reduced.

Step 1. Install dhcpd:

```
$sudo apt-get install isc-dhcp-server
```

Step 2. Edit /etc/default/isc-dhcp-server to specify the interfaces dhcpd should listen to.

```
$sudo vi /etc/default/isc-dhcp-server
```

INTERFACES="ens33"

Step 3. Change the default configuration
Edit file /etc/dhcp/dhcpd.conf to enter particular configuration.

Enter the **domain name** and **domain-name-servers**:

```
option domain-name-servers ns1.example.org, ns2.example.org
option domain-name "example.org";
```

To make this server as official DHCP for your clients, find and uncomment the following line:

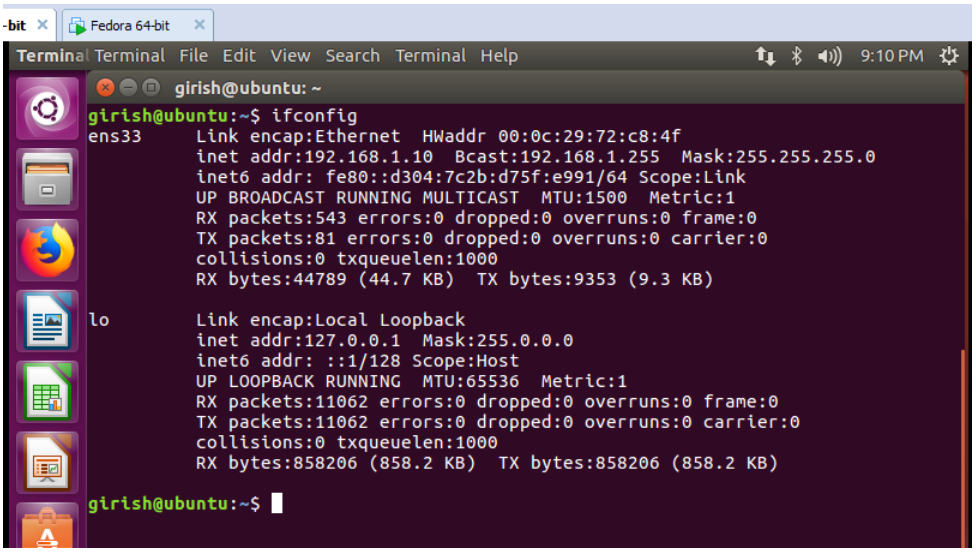
authorative;

```
$sudo vi /etc/dhcp/dhcpd.conf
```

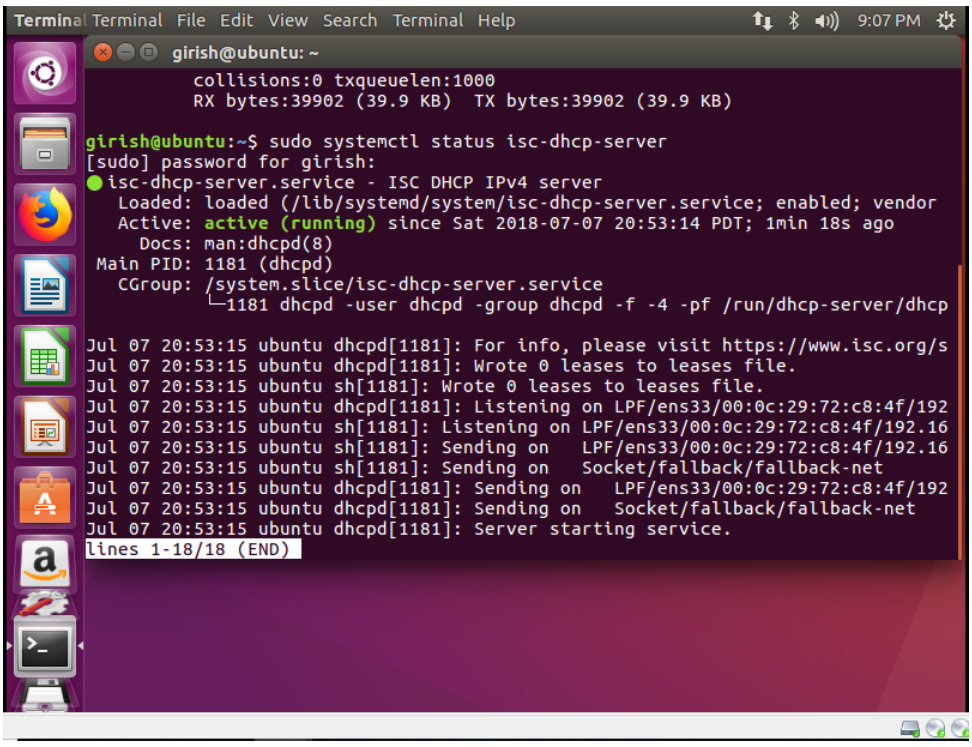
```
# A slightly different configuration for an internal subnet.
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.1.0 netmask 255.255.255.0 {
        range 192.168.1.20 192.168.1.30;
        option routers 192.168.1.1;
        option domain-name-servers ns1.example.org, ns2.example.org
```

```
        option domain-name "example.org";
}
```

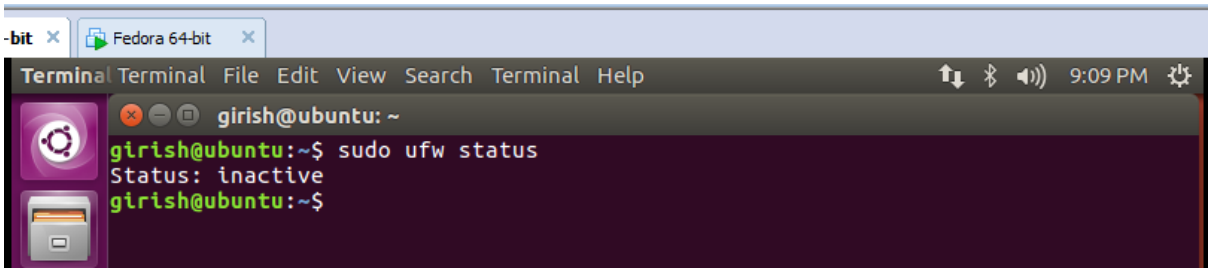
In this setup interface name is: ens33
IP address manually assigned to DHCP server: 192.168.1.10/24



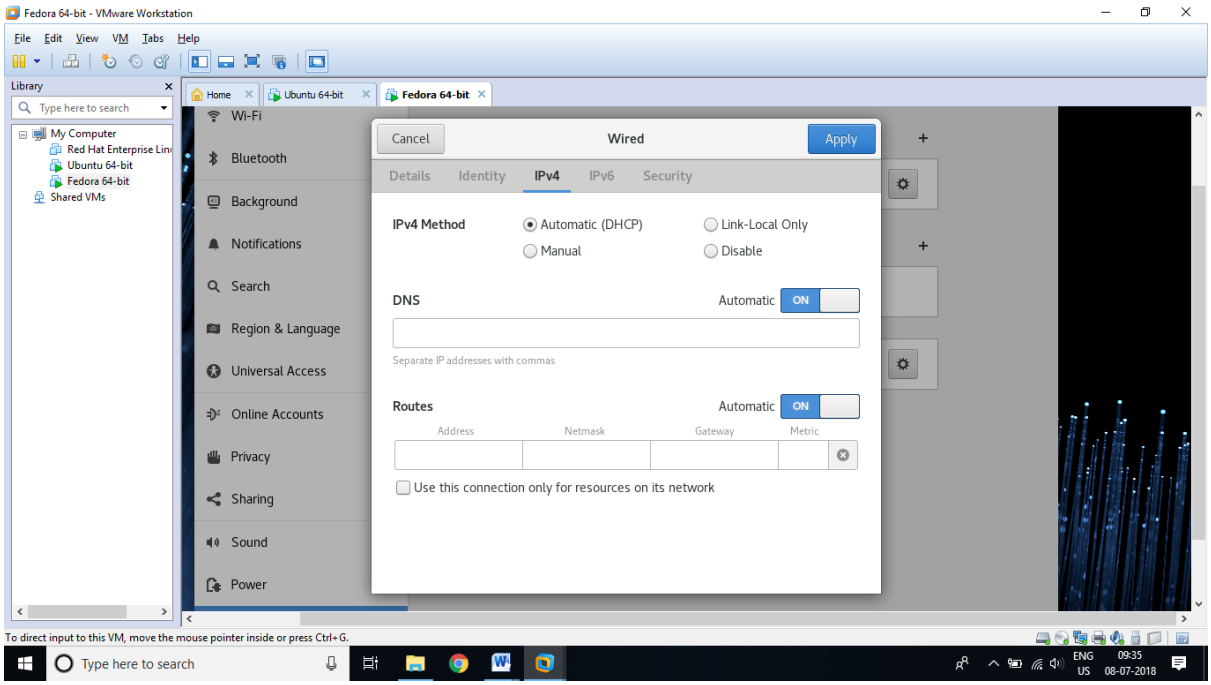
Step 4. Check status of DHCP server

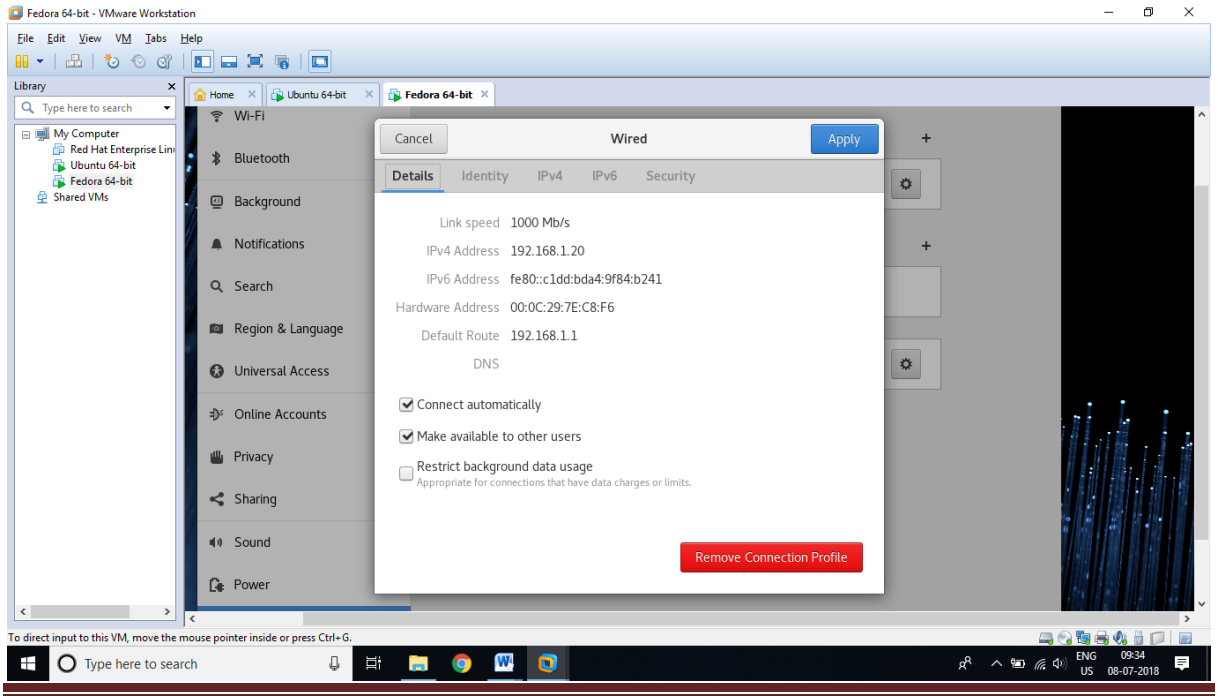


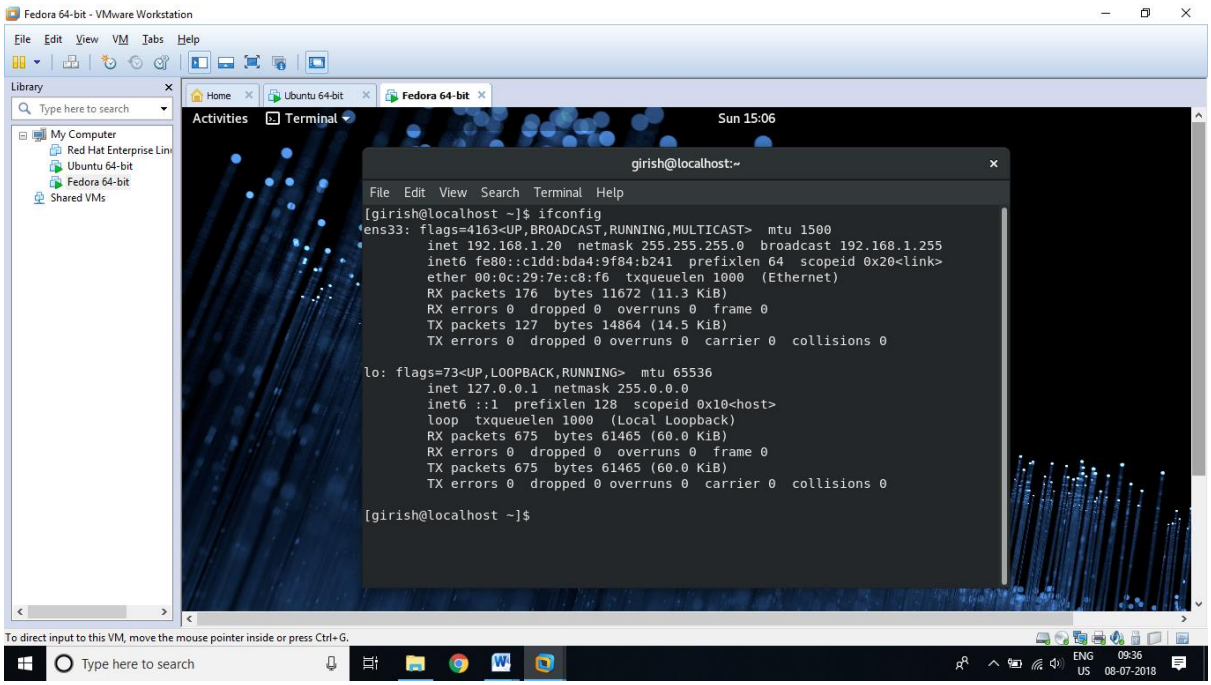
Step 4. Check status of Firewall (It must be inactive)



Step 5. Client Configuration (Client Machine is Fedora 28 Workstation)







Conclusion:
DHCP Server, Ubuntu 16.04, leased IP address 192.168.1.20 to Fedora 28 Workstation.

Imp. Note: While working on virtual machine, disable default DHCP Server in VMware or VirtualBox.

Challenge: Try to allot fix IP address to particular MAC.

```
host ubuntu-client {
    hardware ethernet 08:00:27:13:14:d5;    Use correct MAC address of client m/c
    fixed-address 192.168.1.30;
 }
```

Experiment 2: Initial Settings

Configure Networking on Ubuntu

During the installation of Ubuntu on your server an IP address was most likely obtained automatically. This dynamic IP address assignment will need to be changed to a static IP address. This section will cover the simple network configuration changes needed to set a static IP network address for your server. For this section, the directions assume the configuration is for a node with only one interface (eth0) after a default installation.

```
ifconfig -a
```

Basic network configuration and hostname on a Ubuntu system are stored in several files which must be edited to create a working configuration:

- /etc/network/interfaces describes the network interfaces
- /etc/hostname configures the nameserver credentials
- /etc/hosts resolves IP addresses to hostnames

Once the new configuration is saved the interface must be restarted.

Changing Network Configuration

Below is an example of a static IP configuration on a system with only one Ethernet interface (eth0) and 10.0.0.41/24 for the IP address. Opening the /etc/network/interfaces file will produce:

```
# This file describes the network interfaces available on your sys
# and how to activate them. For more information, see interfaces(5

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 10.0.0.41
    netmask 255.255.255.0
    network 10.0.0.0
    broadcast 10.0.0.255
    gateway 10.0.0.1
    dns-nameservers 10.0.0.1 8.8.8.8
    dns-domain tcsc.org
    dns-search tcsc.org
```

Open your /etc/network/interfaces file, locate the:

- "iface eth0..." line and change dynamic to static
- address line and change the address to the static IP address
- netmask line and change the address to the correct subnet mask
- gateway line and change the address to the correct gateway address
- dns-nameservers line and change (or add) the nameserver information

When you are happy with your configuration restart the interface with the command below. If you are connected using SSH you will lose your connection, re-connect using the new IP address:

```
ifdown eth0; ifup eth0
```

Changing the Hostname

To change the hostname to your preferred node name (example: prodnode01), you have to edit the /etc/hostname file:

```
prodnode01
```

Adding the FQDN (Hostname)

To ensure your server traffic will be routing correctly add the server's Fully Qualified Domain Name (FQDN) and IP address to the hosts file. Open the `/etc/hosts` file and add a line with the static IP address and the FQDN, similar to the example shown below:

```
192.168.0.0 prodnode01.tcsc.org
```

With all your files edited and saved, you should reboot so the new name and configuration will be used. Reboot the system and then use ifconfig or ipaddr to confirm that your new configuration is available.

[1] Add a user (try with useradd command also)

```
# add a new user "ubuntu"

xerus@dlp:~$
sudo adduser ubuntu

[sudo] password for xerus:
# own password

Adding user `ubuntu' ...
Adding new group `ubuntu' (1001) ...
Adding new user `ubuntu' (1001) with group `ubuntu' ...
Creating home directory `/home/ubuntu' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
# set password for new user

Retype new UNIX password:
# confirm

passwd: password updated successfully
Changing the user information for ubuntu
Enter the new value, or press ENTER for the default
Full Name []:
# if not need, Enter with empt

Room Number []:

Work Phone []:

Home Phone []:

Other []:

Is the information correct? [Y/n]
```

```
y

xerus@dlp:~$
```

[2] Giving privileges to a new user

```
xerus@dlp:~$
sudo usermod -G sudo ubuntu

xerus@dlp:~$
su - ubuntu

Password:
# try to execute a command which requires privilege

ubuntu@dlp:~$
sudo reboot

[sudo] password for ubuntu:
# password for 'ubuntu'

Broadcast message from xerus@dlp
        (/dev/pts/0) at 19:59 ...

The system is going down for reboot NOW!
```

Network Settings

[1] Change to static IP addres if you use Ubuntu as a server.
"ens3" is different on each environment, replace it to your own one.

```
root@dlp:~#
vi /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens3
# comment out

#
iface ens3 inet dhcp
# add these lines
```

```
iface ens3 inet static
address 10.0.0.30
# IP address

network 10.0.0.0
# network address

netmask 255.255.255.0
# subnet mask

broadcast 10.0.0.255
# broadcast address

gateway 10.0.0.1
# default gateway

dns-nameservers 10.0.0.10
# name server
# reboot once

root@dlp:~#
reboot
```

[2] Disable IPv6 if not needed.

```
root@dlp:~#
echo "net.ipv6.conf.all.disable_ipv6 = 1" >> /etc/sysctl.conf

root@dlp:~#
sysctl -p
root@dlp:~#
ip addr


1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
group default qlen 1
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
      valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP group default qlen 1000
   link/ether 52:54:00:ad:7d:9c brd ff:ff:ff:ff:ff:ff
   inet 10.0.0.30/24 brd 10.0.0.255 scope global ens3
      valid_lft forever preferred_lft forever
```

Configure Services

[1] It's possible to make sure services' status like follows.

```
# display the list of services which are running

root@dlp:~#
systemctl -t service


UNIT                    LOAD   ACTIVE SUB     DESCRIPTION
accounts-daemon.service      loaded active running Accounts Service
apparmor.service             loaded active exited  LSB: AppArmor initialization
console-setup.service        loaded active exited  Set console keymap
cron.service                 loaded active running Regular background program pr
dbus.service                 loaded active running D-Bus System Message Bus
...
...
...
ufw.service                  loaded active exited  Uncomplicated firewall
user@0.service               loaded active running User Manager for UID 0

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.

35 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.

# the list of all services

root@dlp:~#
systemctl list-unit-files -t service


UNIT FILE                    STATE
accounts-daemon.service           enabled
apt-daily.service            static
autovt@.service               enabled
bootlogd.service             masked
...
...
...
user@.service                static
uuidd.service                indirect
x11-common.service                masked

144 unit files listed.
```

[2] Stop and turn OFF auto-start setting for a service if you don'd need it. (it's Apparmor as an example below)

```
root@dlp:~#
systemctl stop apparmor
```

```
root@dlp:~#
systemctl disable apparmor
```

Sudo Settings

Configure Sudo to separate users' duty if some people share privileges.

[1] Install Sudo.

```
root@dlp:~#
apt-get -y install sudo
```

[2] Transfer root privilege to a user all.

```
root@dlp:~#
visudo
# add to the end: user 'xerus' can use all root privilege

xerus ALL=(ALL:ALL) ALL
# how to write ⇒ destination host=(owner) command

# push 'Ctrl + x' key to quit visudo
# verify with user 'xerus'

xerus@dlp:~$
/sbin/shutdown -r now

shutdown: Need to be root
# denied normally

xerus@dlp:~$
sudo /sbin/shutdown -r now

[sudo] password for xerus:
# xerus's password

Broadcast message from root@dlp
        (/dev/pts/0) at 17:33 ...

The system is going down for reboot NOW!
# executed
```

[3] In addition to the setting [1], set that some commands are not allowed.

```
root@dlp:~#
visudo
# add alias for the kind of shutdown commands

# Cmnd alias specification
Cmnd_Alias SHUTDOWN = /sbin/halt, /sbin/shutdown, \
```

```
/sbin/poweroff, /sbin/reboot, /sbin/init
# add ( commands in alias 'SHUTDOWN' are not allowed )

xerus    ALL=(ALL)    ALL,
!SHUTDOWN
# verify with user 'xerus'

xerus@dlp:~$
sudo /sbin/shutdown -r now

[sudo] password for xerus:
Sorry, user xerus is not allowed to execute '/sbin/shutdown -r now' as root on
dlp.server.world.
# denied normally
```

[4] Transfer some commands with root privilege to users in a group.

```
root@dlp:~#
visudo
# add aliase for the kind of user management comamnds

# Cmnd alias specification
Cmnd_Alias USERMGR = /usr/sbin/adduser, /usr/sbin/useradd, /usr/sbin/newusers, \
/usr/sbin/deluser, /usr/sbin/userdel, /usr/sbin/usermod, /usr/bin/passwd
# add to the end

%usermgr ALL=(ALL) USERMGR
root@dlp:~#
groupadd usermgr

root@dlp:~#
vi /etc/group
# add a user in this group

usermgr:x:1002:
xerus
# verify with user 'xerus'

xerus@dlp:~$
sudo /usr/sbin/useradd testuser

xerus@dlp:~$
# done normally

xerus@dlp:~$
sudo /usr/bin/passwd testuser

Enter new UNIX password:
# set testuser's password

Retype new UNIX password:
```

```
passwd: password updated successfully
```

[5] Transfer some commands with root privilege to a user.

```
root@dlp:~#
visudo
# add to the end

fedora     ALL=(ALL) /usr/sbin/visudo
cent     ALL=(ALL) /usr/sbin/adduser, /usr/sbin/useradd, /usr/sbin/newusers, \
   /usr/sbin/deluser, /usr/sbin/userdel, /usr/sbin/usermod, /usr/bin/passwd
suse     ALL=(ALL) /usr/bin/vim
# verify with user 'fedora'

fedora@dlp:~$
sudo /usr/sbin/visudo
# possible to open and edit

## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
##
# verify with user 'cent'

cent@dlp:~$
sudo /usr/sbin/userdel -r testuser

cent@dlp:~$
# done normally
# verify with user 'suse'

suse@dlp:~$
sudo /usr/bin/vim /root/.profile
# possible to edit or save

# ~/.profile: executed by Bourne-compatible login shells.
```

[6] The logs for sudo are kept in '/var/log/auth.log', but there are many kind of logs in it. So if you'd like to keep only sudo's log in a file, Set like follows.

```
root@dlp:~#
visudo
# add to the end

Defaults syslog=local1
root@dlp:~#
vi /etc/rsyslog.d/50-default.conf
# line 8: add

local1.*                        /var/log/sudo.log
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
```

```
root@dlp:~#
systemctl restart rsyslog
```

Update System

[1] Update System.

```
# Update List first

root@dlp:~#
apt-get update


Hit http://jp.archive.ubuntu.com/ubuntu xenial InRelease
Get: 1 http://jp.archive.ubuntu.com/ubuntu xenial-updates InRelease [92.2 kB]
Hit http://jp.archive.ubuntu.com/ubuntu xenial-backports InRelease
Get: 2 http://jp.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [3,312 B]
Get: 3 http://jp.archive.ubuntu.com/ubuntu xenial-updates/main i386 Packages [3,324 B]
Get: 4 http://jp.archive.ubuntu.com/ubuntu xenial-updates/main Translation-en [2,012 B]
Get: 5 http://jp.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 Packages [2,688 B]
Get: 6 http://jp.archive.ubuntu.com/ubuntu xenial-updates/universe i386 Packages [2,680 B]
Get: 7 http://jp.archive.ubuntu.com/ubuntu xenial-updates/universe Translation-en [2,000 B]
Get: 8 http://security.ubuntu.com/ubuntu xenial-security InRelease [92.2 kB]
Get: 9 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [632 B]
Get: 10 http://security.ubuntu.com/ubuntu xenial-security/main i386 Packages [632 B]
Get: 11 http://security.ubuntu.com/ubuntu xenial-security/main Translation-en [376 B]
Fetched 202 kB in 1s (112 kB/s)

Current status: 1 (+1) upgradable.

root@dlp:~#
apt-get -y upgrade
```

Important files in Ubuntu:

- /etc/network/interfaces describes the network interfaces
- /etc/hostname configures the nameserver credentials
- /etc/hosts resolves IP addresses to hostnames

Experiment 3: Configure NTP Server (NTPd)

(Ref. https://www.server-world.info/en/note?os=Ubuntu_16.04&p=ntp&f=1)

Time Synchronisation

NTP is a TCP/IP protocol for synchronising time over a network. Basically a client requests the current time from a server, and uses it to set its own clock.

Install NTPd and Configure NTP server for time adjustment. NTP uses 123/UDP.

[1] Install and Configure NTPd.

```
root@dlp:~#
apt-get -y install ntp
root@dlp:~#
vi /etc/ntp.conf
# line 18: omment out

#
 pool 0.ubuntu.pool.ntp.org iburst
#
 pool 1.ubuntu.pool.ntp.org iburst
#
 pool 2.ubuntu.pool.ntp.org iburst
#
 pool 3.ubuntu.pool.ntp.org iburst
#
 pool ntp.ubuntu.com
# add servers of your timezone for time synchronization

server ntp1.jst.mfeed.ad.jp iburst
server ntp2.jst.mfeed.ad.jp iburst
server ntp3.jst.mfeed.ad.jp iburst
# line 50: add the network range you allow to receive requests

restrict 10.0.0.0 mask 255.255.255.0 nomodify notrap
root@dlp:~#
systemctl restart ntp
# show status

root@dlp:~#
ntpq -p


     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*ntp1.jst.mfeed. 133.243.236.17   2 u    8   64    3   17.613    3.116   2.670
 ntp2.jst.mfeed. .INIT.          16 u    -   64    0    0.000    0.000   0.000
+ntp3.jst.mfeed. 133.243.236.17   2 u    3   64    3   18.134    2.303   3.591
```

Configure NTP Client : Ubuntu

Configure NTP Client.

[1] The settings of NTP Client on Ubuntu are mostly the same with Server's settings, so refer to NTPd Settings or Chrony Settings. For different settings from Server's one, Clients don't need to receive time synchronization requests from other computers, so it does not need to set access permission.

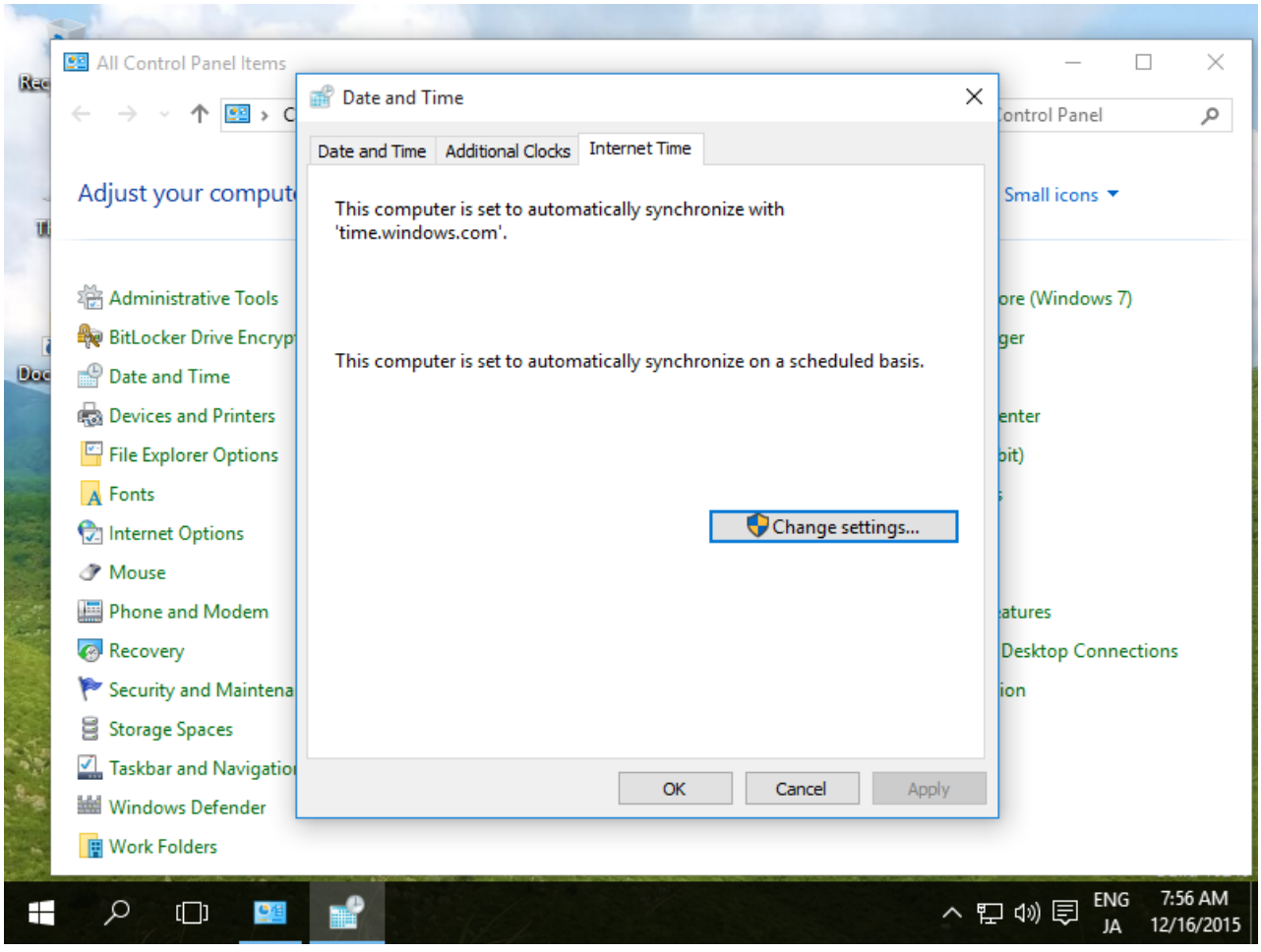
[2] If you don't use NTP service daemon but use a command to sync time at once, use ntpdate like follows.

```
root@client:~#
apt-get -y install ntpdate
root@client:~#
ntpdate ntp1.jst.mfeed.ad.jp

21 Apr 19:41:26 ntpdate[1458]: step time server 210.173.160.27 offset 0.667927 sec
```

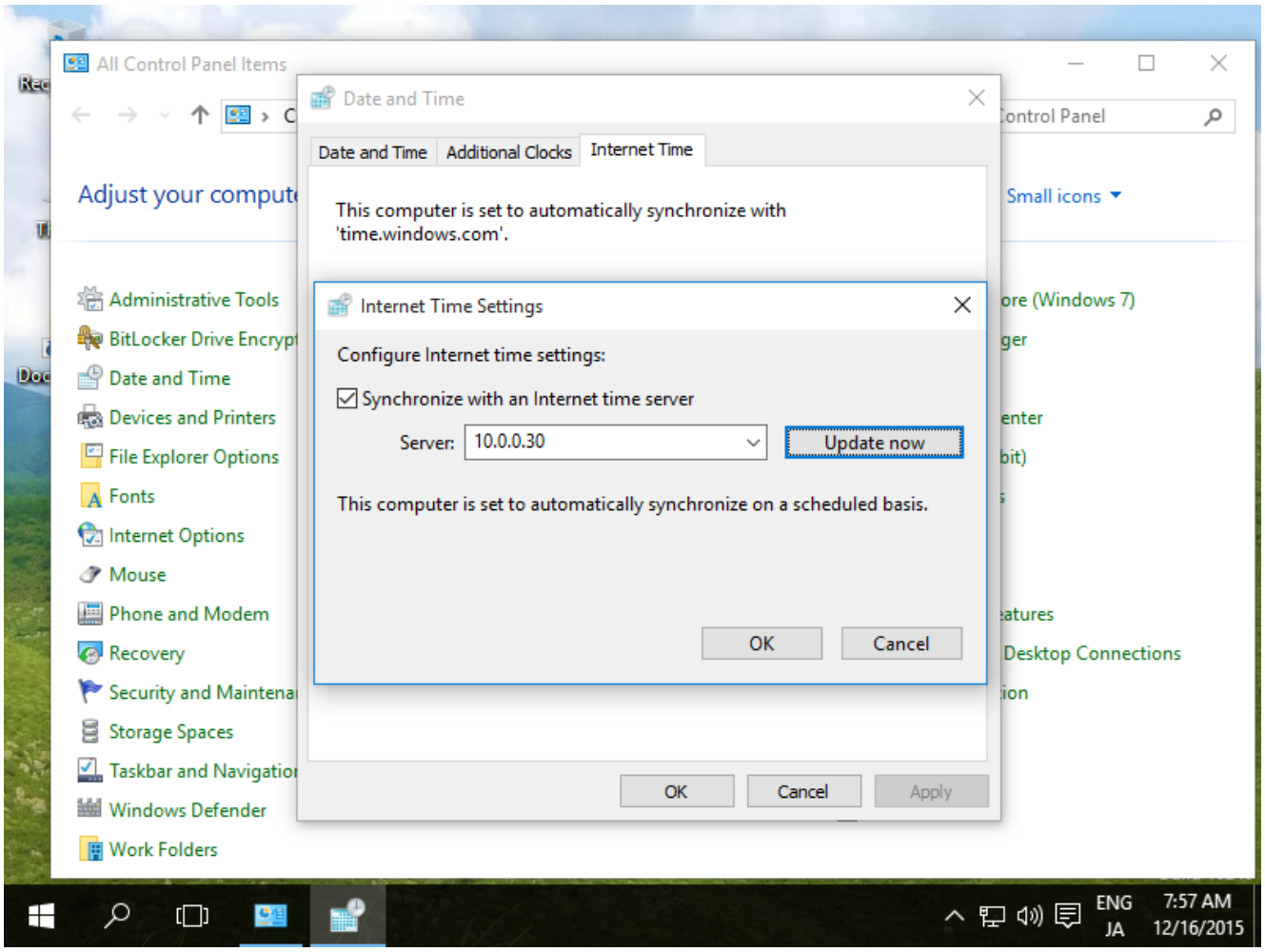
Configure NTP Client : Windows

Configure NTP Client on Windows. This example is based on Windows 10 Pro.

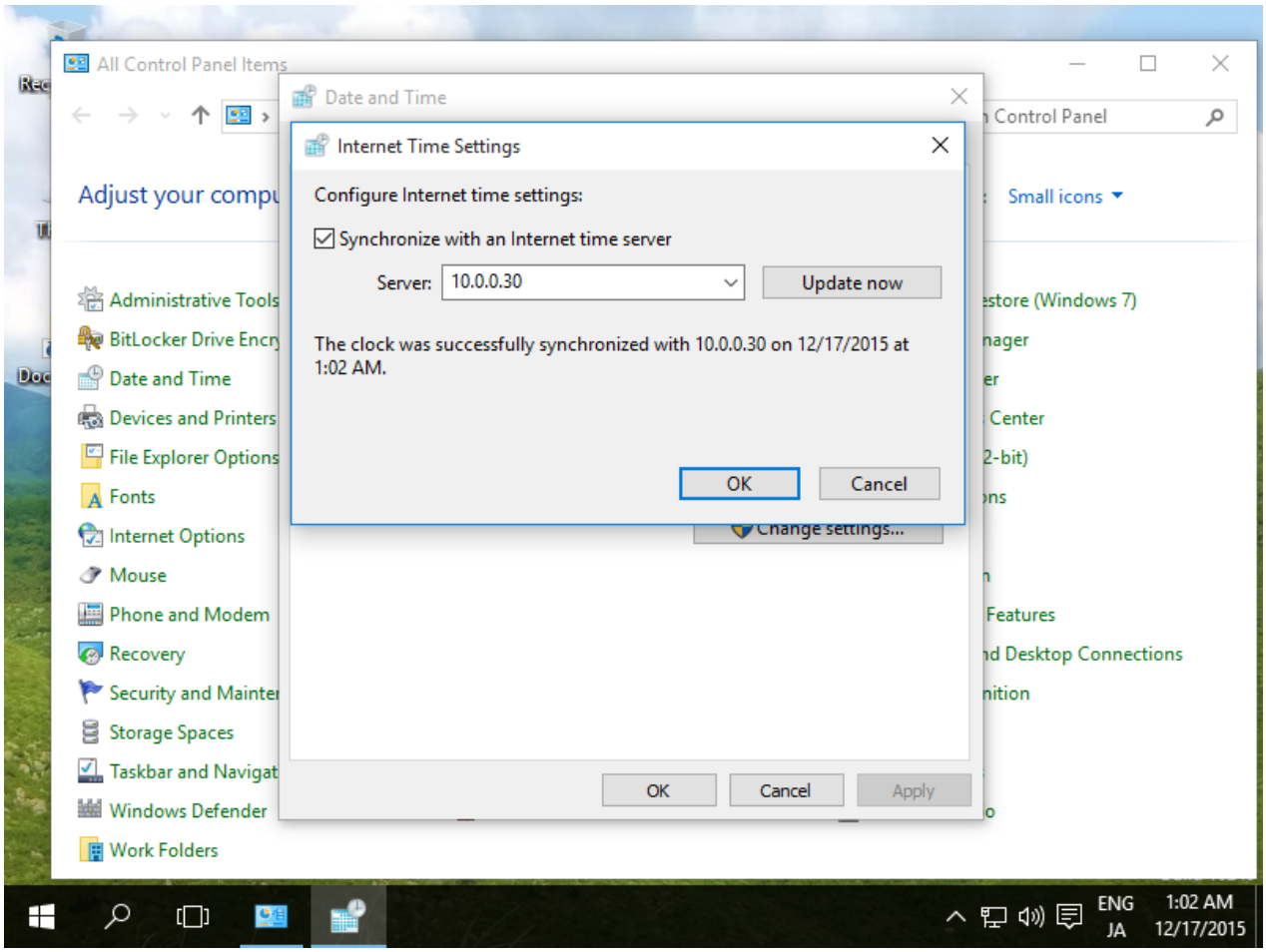
[3] Open [Control Panel] - [Date and Time] and move to [internet Time] tab, then [Change settings] button.



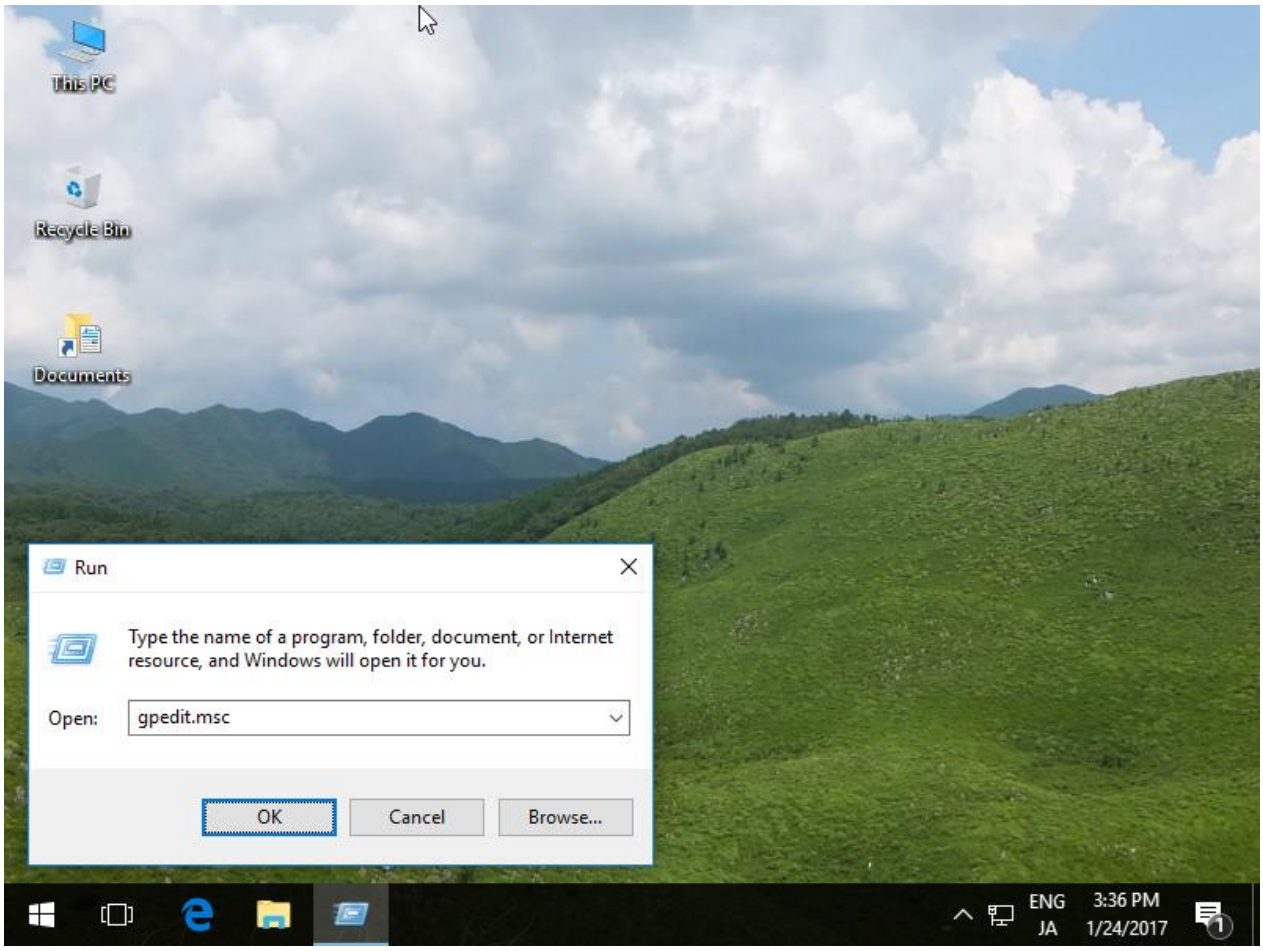
[4] Input NTP server you'd like to sync on [Server] section and [Update now] button.



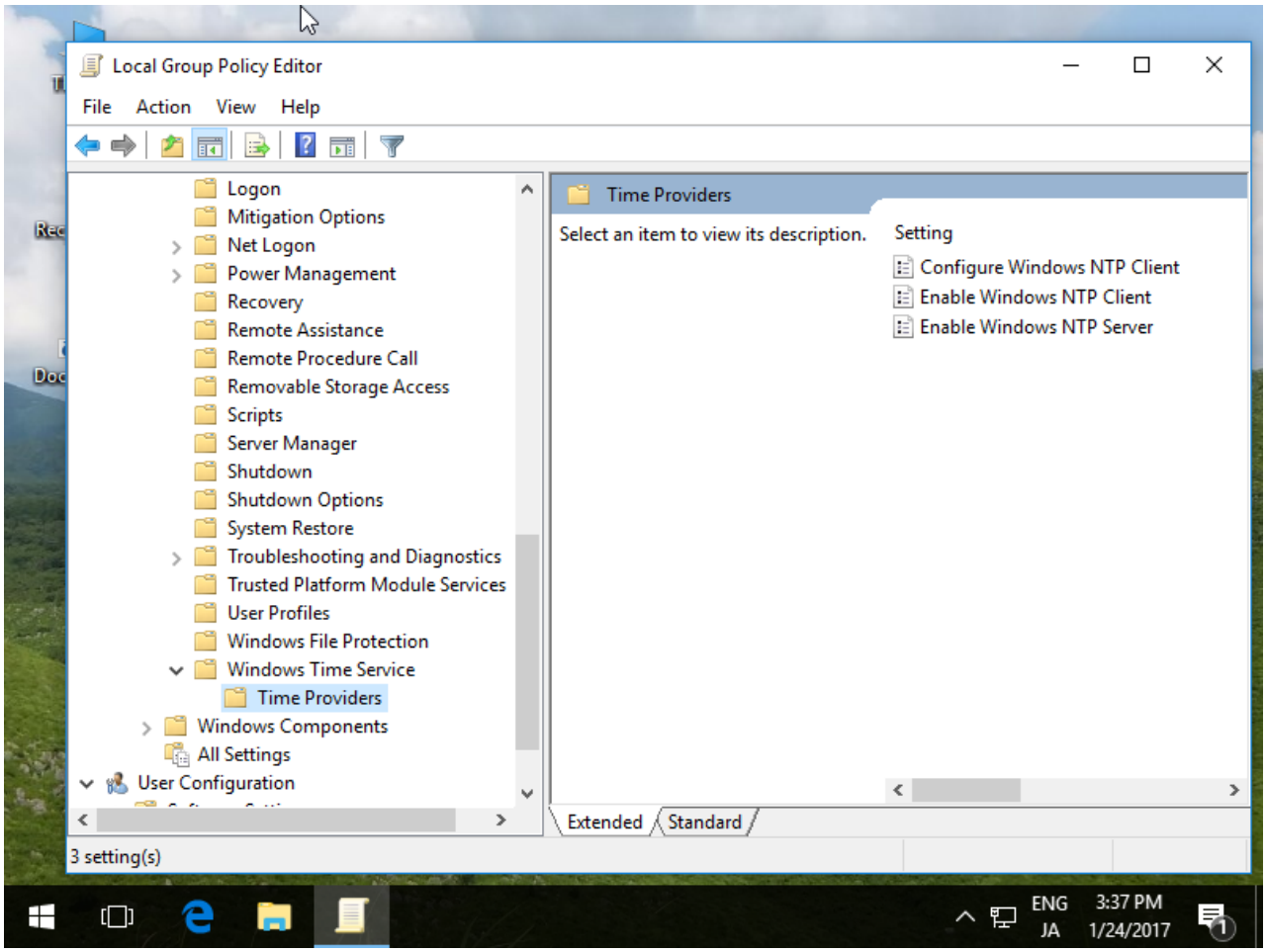
[5] It's OK to sync time if successful message is shown like follows.
The default setting of sync interval is 86400 sec (one day).
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient\SpecialPollInterval



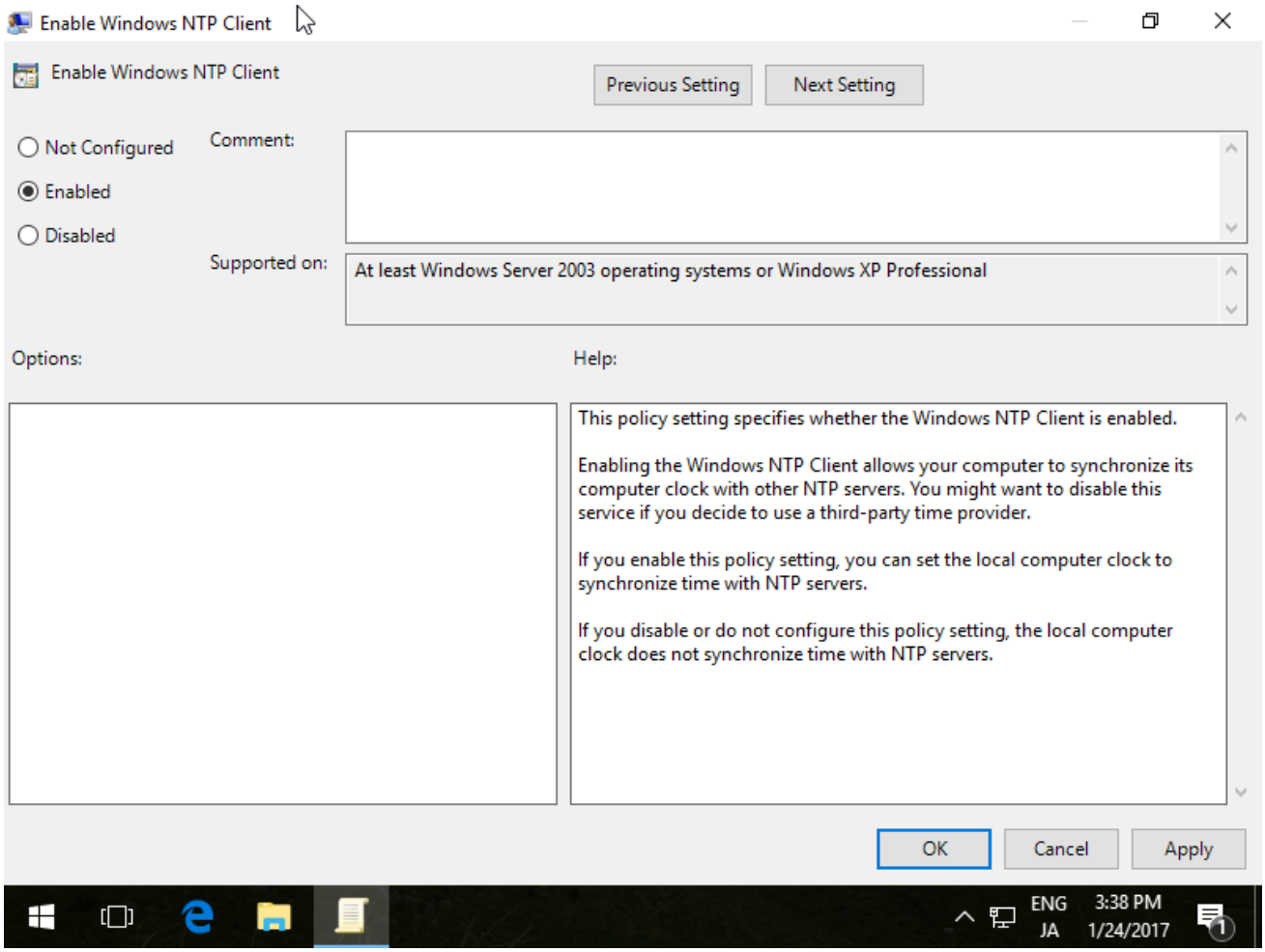
[6] If you'd like to configure NTP Client Service, Set like follows.
Right-click Windows icon and open [run] and input "gpedit.msc" like follows.



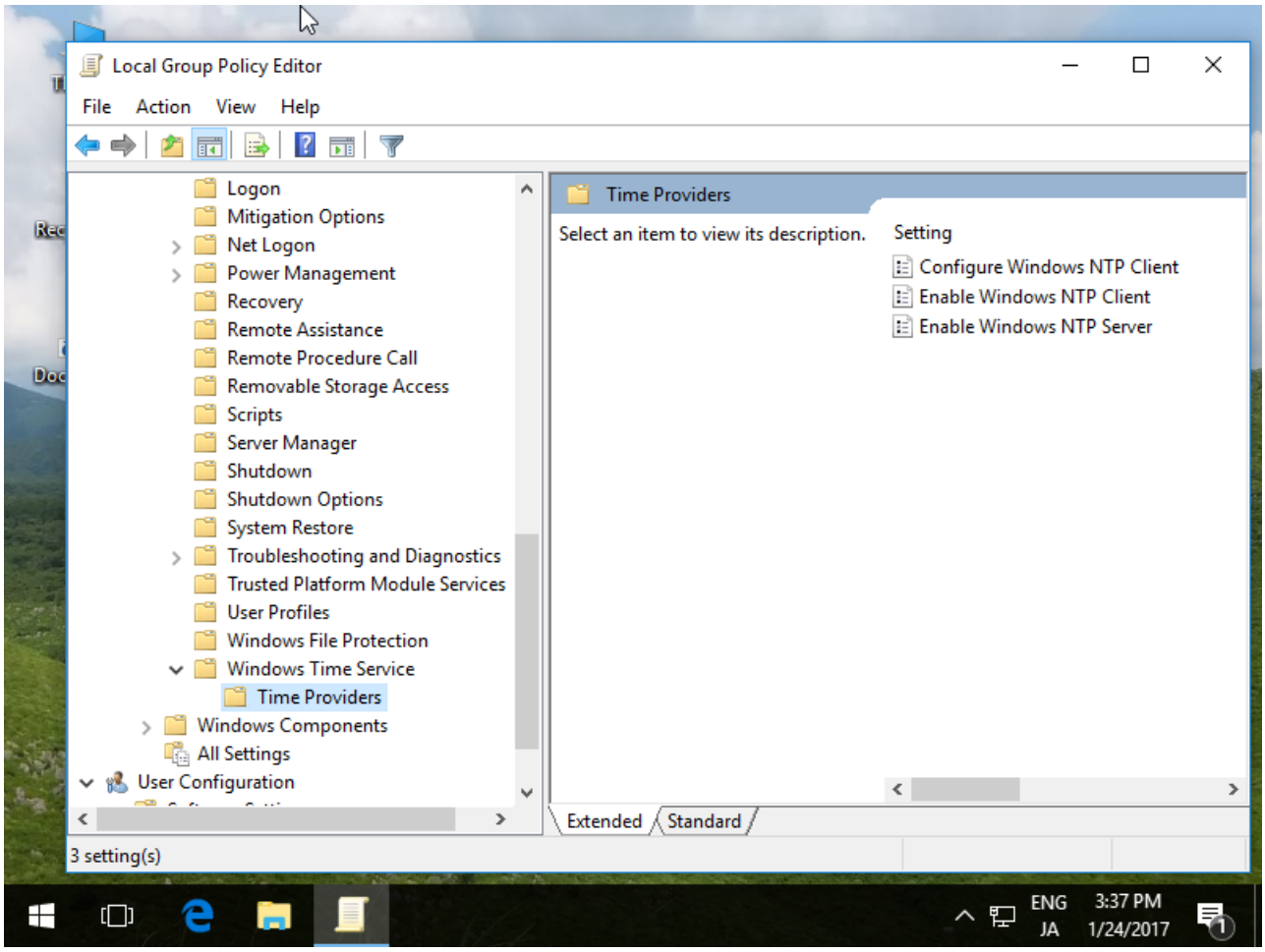
[7] Select [Administrative template] - [System] - [Windows Time Service] - [Time Providers] on the left Pane, and Open [Enable Windows NTP Client] on the right Pane.



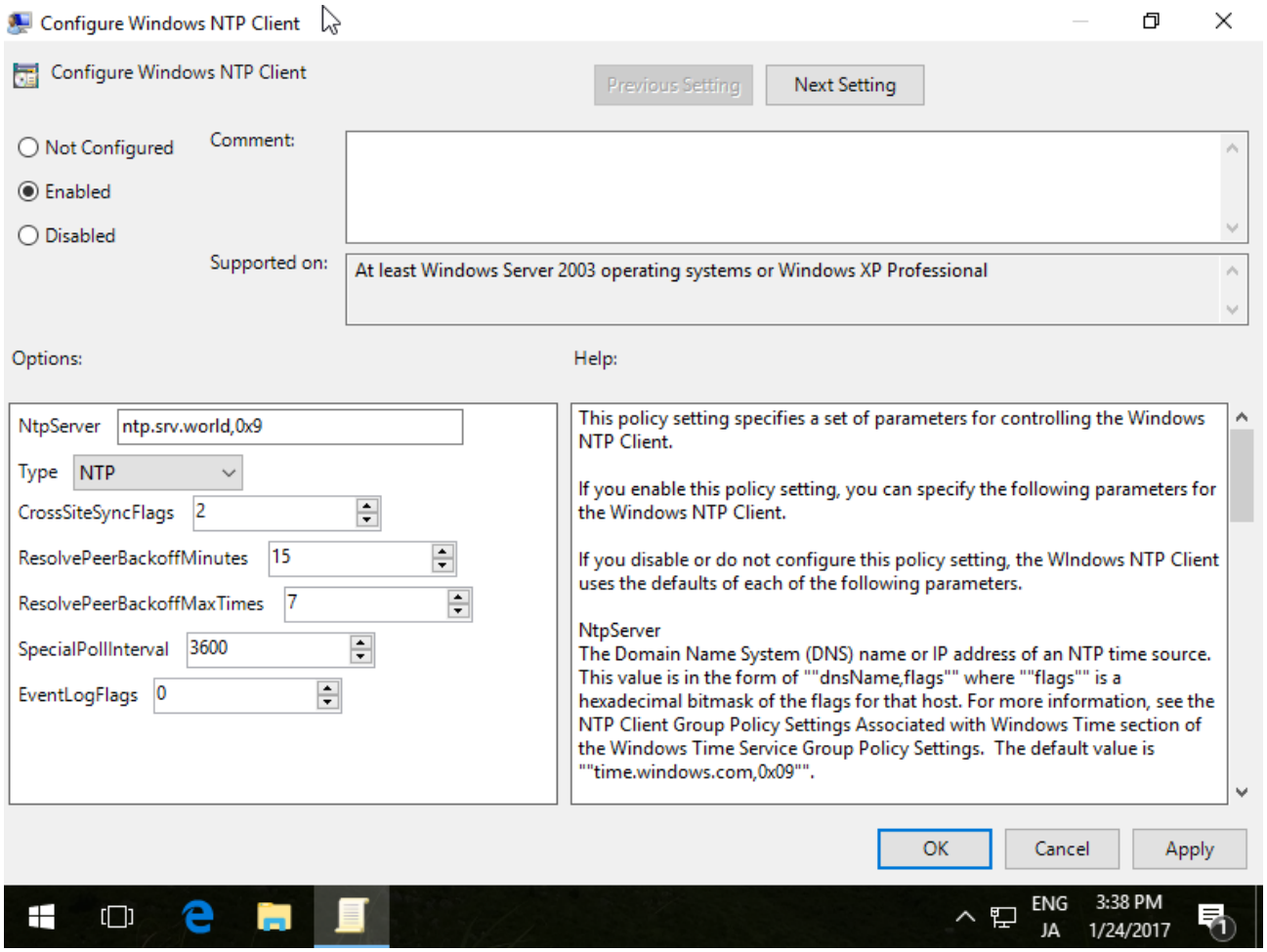
[8] Check a box [Enabled] which is upper-left like follows.



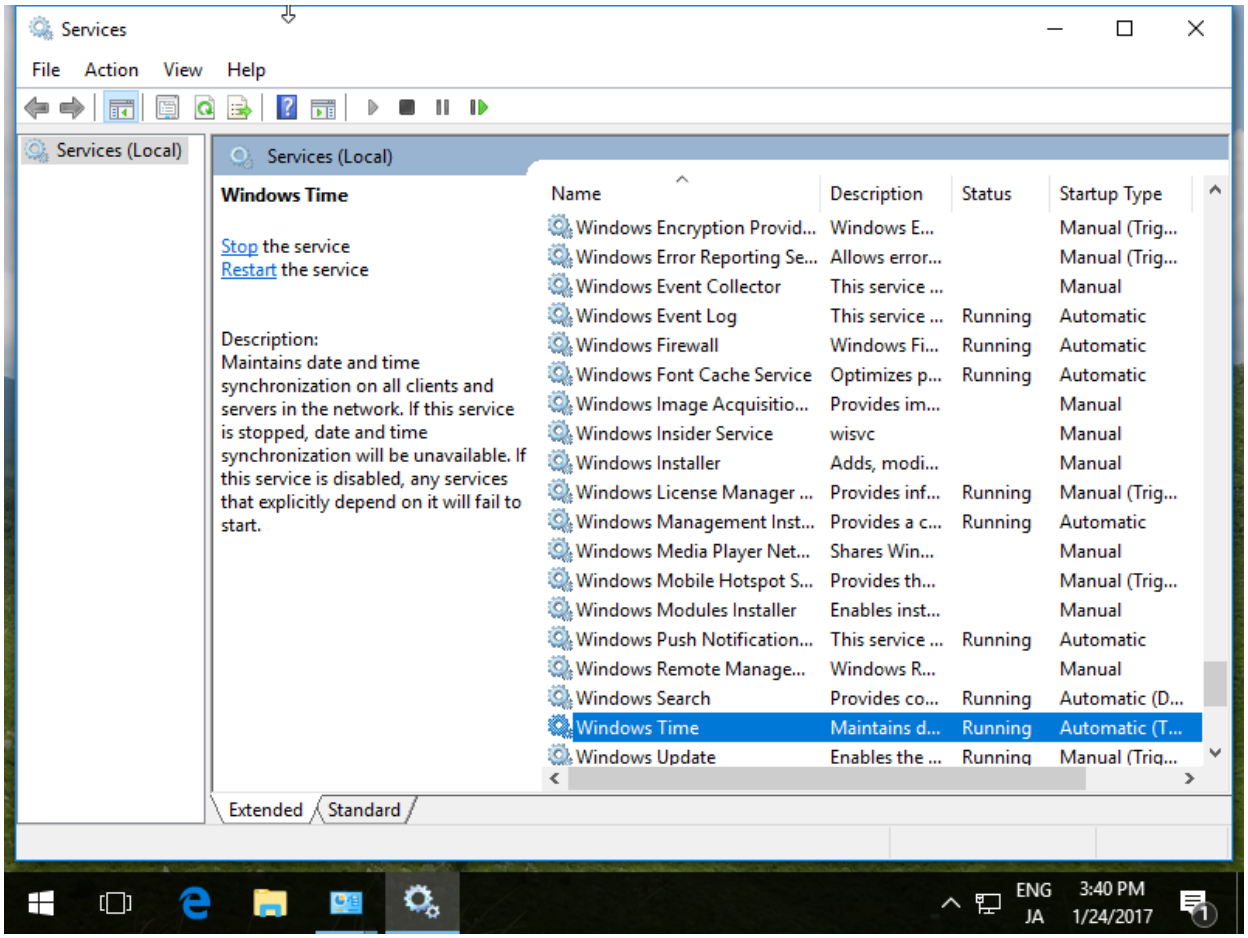
[9] Click to open [Configure Windows NTP Client] on the right Pane.



[10] Check a box [Enabled] which is upper-left and change values for your environment.
[NtpServer] ⇒ Hostname or IP address of your NTP Server.
The value [0x9] is generally OK to keep default. [0x9] means [0x01] + [0x08].
They mean like follows.
0x01 SpecialInterval
0x02 UseAsFallbackOnly
0x04 SymmetricActive
0x08 NTP request in Client mode
For [Type] section, It's OK to keep default [NT5DS] if your computer is in a Domain, but if not, change to [NTP].
For [SpecialPollInterval], set interval to sync time.



[11] Open [Control Panale] - [Administrative tools] - [Services], then Select [Windows Time] Service and click [Start the service] or [Restart the service]. Furthermore, Change [Startup type] to [Automatic] if it is not the value.


Services
File Action View Help
Services (Local)
Services (Local)
Windows Time
Stop the service
Restart the service
Description:
Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
Name
Description
Status
Startup Type
Windows Encryption Provid... Windows E... Manual (Trig...
Windows Error Reporting Se... Allows error... Manual (Trig...
Windows Event Collector This service ... Manual
Windows Event Log This service ... Running Automatic
Windows Firewall Windows Fi... Running Automatic
Windows Font Cache Service Optimizes p... Running Automatic
Windows Image Acquisitio... Provides im... Manual
Windows Insider Service wisvc Manual
Windows Installer Adds, modi... Manual
Windows License Manager ... Provides inf... Running Manual (Trig...
Windows Management Inst... Provides a c... Running Automatic
Windows Media Player Net... Shares Win... Manual
Windows Mobile Hotspot S... Provides th... Manual (Trig...
Windows Modules Installer Enables inst... Manual
Windows Push Notification... This service ... Running Automatic
Windows Remote Manage... Windows R... Manual
Windows Search Provides co... Running Automatic (D...
Windows Time Maintains d... Running Automatic (T...
Windows Update Enables the ... Running Manual (Trig...
Extended Standard
ENG
JA
3:40 PM
1/24/2017

Experiment 4: SSH Server : Password Authentication

(Ref: https://www.server-world.info/en/note?os=Ubuntu_16.04&p=ssh&f=1)

Introduction:

This section of the Ubuntu Server Guide introduces a powerful collection of tools for the remote control of, and transfer of data between, networked computers called *OpenSSH*. You will also learn about some of the configuration settings possible with the OpenSSH server application and how to change them on your Ubuntu system.

OpenSSH is a freely available version of the Secure Shell (SSH) protocol family of tools for remotely controlling, or transferring files between, computers. Traditional tools used to accomplish these functions, such as telnet or rcp, are insecure and transmit the user's password in cleartext when used. OpenSSH provides a server daemon and client tools to facilitate secure, encrypted remote control and file transfer operations, effectively replacing the legacy tools.

Configure SSH Server to manage a server from the remore computer. SSH uses 22/TCP.

[1] Password Authentication for Open SSH Server on Ubuntu is enabled by default, so it's possible to login without changing any settings. Furthermore, root account is prohibited Password Authentication by default with "PermitRootLogin prohibit-password", so default setting is good for use. But if you prohibit root login all, change like follows.

```
root@dlp:~#
apt-get -y install openssh-server
root@dlp:~#
vi /etc/ssh/sshd_config
# line 28: change to no

PermitRootLogin
no
root@dlp:~#
systemctl restart ssh
```

SSH Client : Ubuntu : Ubuntu

Configure SSH Client for Ubuntu.

[2] Install SSH Client.

```
root@client:~#
apt-get -y install openssh-client
```

[3] Connect to the SSH server with a common user.

```
# ssh [username@hostname or IP address]

root@client:~#
ssh ubuntu@dlp.srv.world
```

```
The authenticity of host 'dlp.srv.world (<no hostip for proxy command>)' can't be established.
ECDSA key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:60:90:d8.
Are you sure you want to continue connecting (yes/no)?
yes

Warning: Permanently added 'dlp.srv.world' (ECDSA) to the list of known hosts.
ubuntu@dlp.srv.world's password:
# password of the user

ubuntu@dlp:~$
# just logined
```

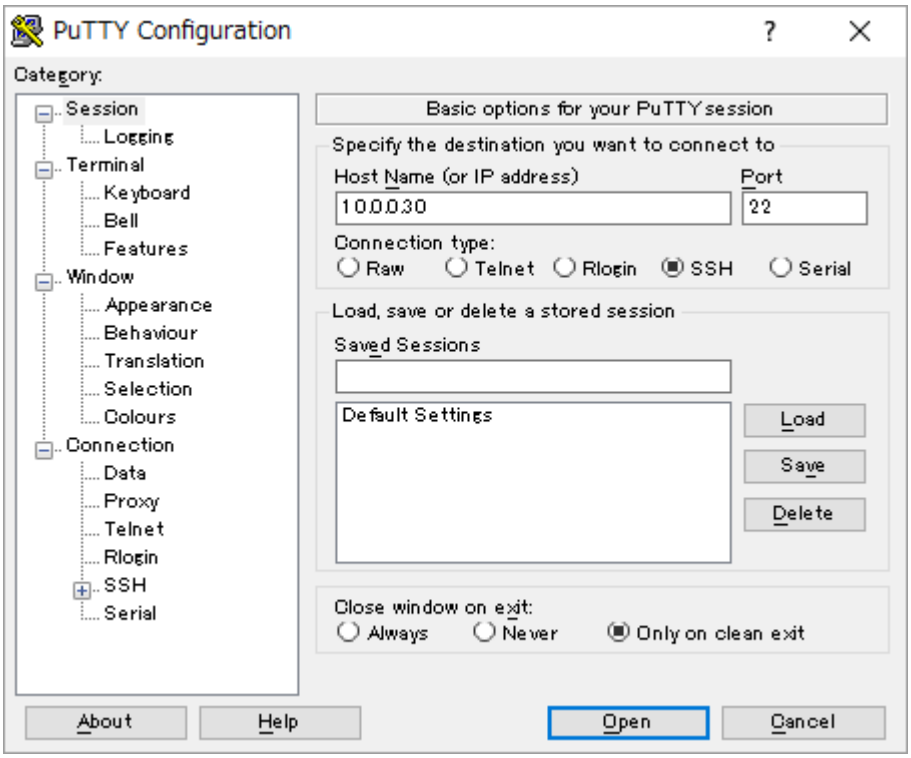
[4] It's possbile to execute commands on remote Host with adding commands to ssh command.

```
# for example, open /etc/passwd on remote host

ubuntu@client:~$
ssh ubuntu@dlp.srv.world "cat /etc/passwd"

ubuntu@dlp.srv.world's password:

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
...
...
ubuntu:x:1000:1000:ubuntu,,,:/home/ubuntu:/bin/bash
sshd:x:108:65534::/var/run/sshd:/usr/sbin/nologin
```

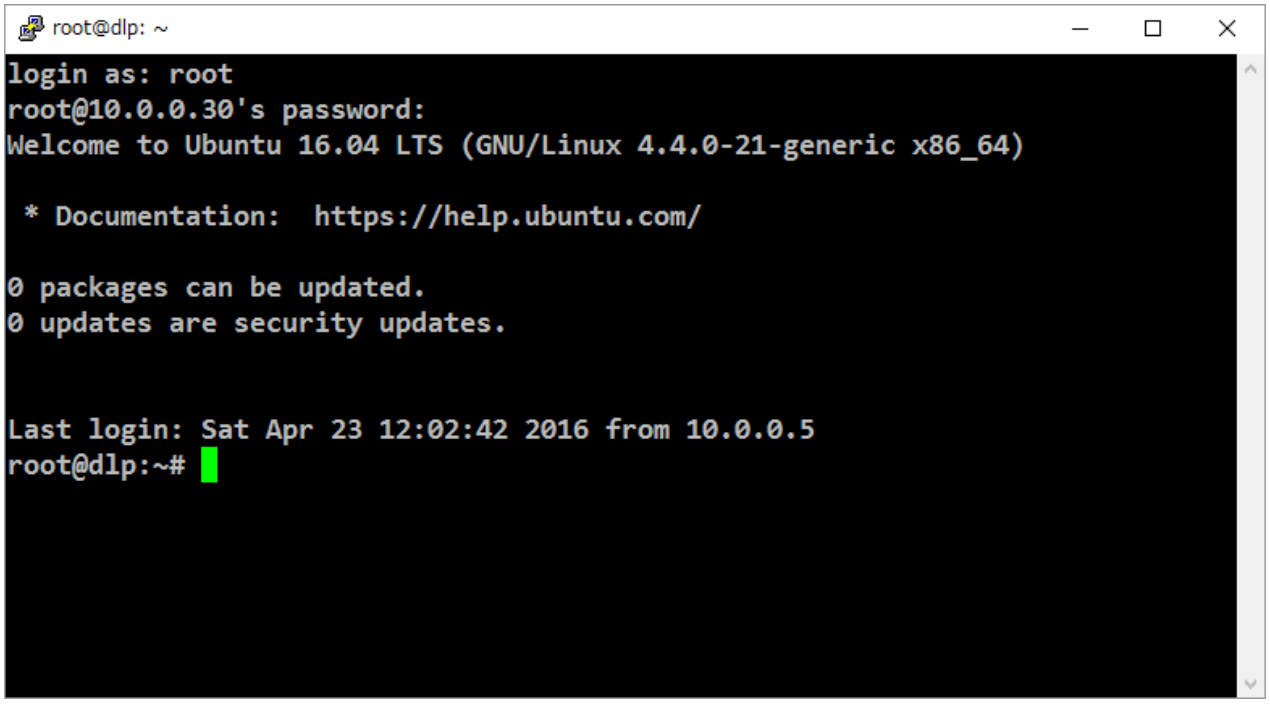
SSH Client : Windows

Configure SSH Client for Windows.

[5] Get a SSH Client for Windows. This example shows to use Putty like follows. Input your server's IP address and Click 'Open' button.



[6] After authentication on SSH server, it's possible to login remotely with SSH.



Experiment 5: Install BIND

(Ref https://www.server-world.info/en/note?os=Ubuntu_16.04&p=dns&f=1)

Domain Name Service (DNS) is an Internet service that maps IP addresses and fully qualified domain names (FQDN) to one another. In this way, DNS alleviates the need to remember IP addresses. Computers that run DNS are called name servers. Ubuntu ships with BIND (Berkley Internet Naming Daemon), the most common program used for maintaining a name server on Linux. A very useful package for testing and troubleshooting DNS issues is the dnsutils package.

Overview
The DNS configuration files are stored in the /etc/bind directory. The primary configuration file is /etc/bind/named.conf.
The *include* line specifies the filename which contains the DNS options. The *directory* line in the /etc/bind/named.conf.options file tells DNS where to look for files. All files BIND uses will be relative to this directory.
The file named /etc/bind/db.root describes the root nameservers in the world. The servers change over time, so the /etc/bind/db.root file must be maintained now and then. This is usually done as updates to the bind9 package. The *zone* section defines a master server, and it is stored in a file mentioned in the *file* option.
It is possible to configure the same server to be a caching name server, primary master, and secondary master. A server can be the Start of Authority (SOA) for one zone, while providing secondary service for another zone. All the while providing caching services for hosts on the local LAN.

Configure DNS server which resolves domain name or IP address.
BIND uses 53/TCP, UDP

[1] Install BIND 9

```
root@dlp:~#
apt-get -y install bind9 bind9utils
```

[2] Configure BIND.
This example is set with grobal IP address [172.16.0.80/29], Private IP address [10.0.0.0/24], Domain name [srv.world]. However, Please use your own IPs and domain name when you set config on your server. (Actually, [172.16.0.80/29] is for private IP address, though.)

```
root@dlp:~#
vi /etc/bind/named.conf
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
# comment out

#
 include "/etc/bind/named.conf.default-zones";
# add

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

```
include "/etc/bind/named.conf.external-zones";
root@dlp:~#
vi /etc/bind/named.conf.internal-zones
# create new

# define for internal section

view "internal" {

        match-clients {
                localhost;
                10.0.0.0/24;
        };
# set zone for internal


        zone "srv.world" {
                type master;
                file "/etc/bind/srv.world.lan";
                allow-update { none; };
        };
# set zone for internal *note


        zone "0.0.10.in-addr.arpa" {
                type master;
                file "/etc/bind/0.0.10.db";
                allow-update { none; };
        };
        include "/etc/bind/named.conf.default-zones";
};

root@dlp:~#
vi /etc/bind/named.conf.external-zones
# create new

# define for external section

view "external" {
# define for external section


        match-clients { any; };
# allow any query


        allow-query { any; };
# prohibit recursions
```

```
        recursion no;
# set zone for external


        zone "srv.world" {
                type master;
                file "/etc/bind/srv.world.wan";
                allow-update { none; };
        };
# set zone for external *note


        zone "80.0.16.172.in-addr.arpa" {
                type master;
                file "/etc/bind/80.0.16.172.db";
                allow-update { none; };
        };
};

# *note : For How to write for reverse resolving, Write network address reversely like
below
# 10.0.0.0/24
# network address       ⇒ 10.0.0.0
# range of network      ⇒ 10.0.0.0 - 10.0.0.255
# how to write          ⇒ 0.0.10.in-addr.arpa

# 172.16.0.80/29
# network address       ⇒ 172.16.0.80
# range of network      ⇒ 172.16.0.80 - 172.16.0.87
# how to write          ⇒ 80.0.16.172.in-addr.arpa
```

[3] Limit ranges you allow to access if needed.

```
root@dlp:~#
vi /etc/bind/named.conf.options
options {
directory "/var/cache/bind";
// If there is a firewall between you and nameservers you want

// to talk to, you may need to fix the firewall to allow multiple

// ports to talk. See http://www.kb.cert.org/vuls/id/800113
// If your ISP provided one or more IP addresses for stable

// nameservers, you probably want to use them as forwarders.

// Uncomment the following block, and insert the addresses replacing

// the all-0's placeholder.
// forwarders {
```

```
//      0.0.0.0;

// };
# query range you allow

allow-query { localhost; 10.0.0.0/24; };

# the range to transfer zone files

allow-transfer { localhost; 10.0.0.0/24; };

# recursion range you allow

allow-recursion { localhost; 10.0.0.0/24; };
dnssec-validation auto;

auth-nxdomain no; # conform to RFC1035

# change if not use IPV6

listen-on-v6
{ none; };

};
```

Name Resolution

Create zone files that servers resolve IP address from domain name.

[1] For internal zone,
This example uses internal address [10.0.0.0/24], domain name [srv.world], but please use your own one when you set config on your server.

```
root@dlp:~#
vi /etc/bind/srv.world.lan
$TTL 86400
@   IN  SOA     dlp.srv.world. root.srv.world. (
        2016042101  ;Serial
        3600        ;Refresh
        1800        ;Retry
        604800      ;Expire
        86400       ;Minimum TTL
)
# define name server


        IN  NS      dlp.srv.world.
# define name server's IP address
```

```
        IN  A       10.0.0.30
# define mail exchanger


        IN  MX 10   dlp.srv.world.

# define IP address of a hostname


dlp     IN  A       10.0.0.30
```

[2] For external zone,
This example uses external address [172.16.0.80/29], domain name [srv.world], but please use your own one when you set config on your server.

```
root@dlp:~#
vi /etc/bind/srv.world.wan
$TTL 86400
@   IN  SOA     dlp.srv.world. root.srv.world. (
        2016042101  ;Serial
        3600        ;Refresh
        1800        ;Retry
        604800      ;Expire
        86400       ;Minimum TTL
)
# define name server


        IN  NS      dlp.srv.world.
# define name server's IP address


        IN  A       172.16.0.82
# define mail exchanger


        IN  MX 10   dlp.srv.world.

# define IP address of a hostname


dlp     IN  A       172.16.0.82
```

Address Resolution

Create zone files that servers resolve domain names from IP address.

[3] For internal zone,
This example uses internal address [10.0.0.0/24], domain name [srv.world], but please use your own one when you set config on your server.

```
root@dlp:~#
vi /etc/bind/0.0.10.db
$TTL 86400
@   IN  SOA     dlp.srv.world. root.srv.world. (
        2016042101  ;Serial
        3600        ;Refresh
        1800        ;Retry
        604800      ;Expire
        86400       ;Minimum TTL
)
# define name server


        IN  NS      dlp.srv.world.

# define the range of this domain included


        IN  PTR     srv.world.
        IN  A       255.255.255.0

# define hostname of an IP address


30      IN  PTR     dlp.srv.world.
```

[4] For external zone,
This example uses external address [172.16.0.80/29], domain name [srv.world], but please use your own one when you set config on your server.

```
root@dlp:~#
vi /etc/bind/80.0.16.172.db
$TTL 86400
@   IN  SOA     dlp.srv.world. root.srv.world. (
        2016042101  ;Serial
        3600        ;Refresh
        1800        ;Retry
        604800      ;Expire
        86400       ;Minimum TTL
)
# define name server


        IN  NS      dlp.srv.world.

# define the range of this domain included


        IN  PTR     srv.world.
        IN  A       255.255.255.248
```

```
# define hostname of an IP address


82      IN  PTR     dlp.srv.world.
```

Start BIND

Restart BIND to take effect changes and make sure it's no ploblem.

[1] Change resolv.conf for name resolution to refer to own DNS.
("ens3" is different on each environment, Replace it to your own one)

```
root@dlp:~#
vi /etc/network/interfaces
# change to own one

dns-nameservers
10.0.0.30
root@dlp:~#
systemctl restart ifup@ens3 bind9
```

[2] Try to resolv normally.

```
root@dlp:~#
dig dlp.srv.world.



; <<>> DiG 9.10.3-P4-Ubuntu <<>> dlp.srv.world.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30428
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dlp.srv.world.             IN      A

;; ANSWER SECTION:
dlp.srv.world.      86400   IN      A       10.0.0.30

;; AUTHORITY SECTION:
srv.world.          86400   IN      NS      dlp.srv.world.

;; Query time: 0 msec
;; SERVER: 10.0.0.30#53(10.0.0.30)
;; WHEN: Fri Apr 22 17:08:09 JST 2016
;; MSG SIZE  rcvd: 75
```

```
root@dlp:~#
dig -x 10.0.0.30



; <<>> DiG 9.10.3-P4-Ubuntu <<>> -x 10.0.0.30
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41939
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;30.0.0.10.in-addr.arpa.            IN      PTR

;; ANSWER SECTION:
30.0.0.10.in-addr.arpa. 86400   IN      PTR     dlp.srv.world.

;; AUTHORITY SECTION:
0.0.10.in-addr.arpa.    86400   IN      NS      dlp.srv.world.

;; ADDITIONAL SECTION:
dlp.srv.world.      86400   IN      A       10.0.0.30

;; Query time: 0 msec
;; SERVER: 10.0.0.30#53(10.0.0.30)
;; WHEN: Fri Apr 22 17:10:15 JST 2016
;; MSG SIZE  rcvd: 111
```

Set CNAME

If you'd like to set another name to your Host, define CNAME record in zone file.

[1] Set CNAME record in zone file.

```
root@dlp:~#
vi /etc/bind/srv.world.lan
$TTL 86400
@   IN  SOA     dlp.srv.world. root.srv.world. (
# update serial


        2016042102  ;Serial
        3600        ;Refresh
        1800        ;Retry
        604800      ;Expire
        86400       ;Minimum TTL
)
        IN  NS      dlp.srv.world.
        IN  A       10.0.0.30
```

```
        IN  MX 10   dlp.srv.world.

dlp     IN  A       10.0.0.30
# aliase IN CNAME server's name

ftp     IN  CNAME   dlp.srv.world.

root@dlp:~#
rndc reload

server reload successful
root@dlp:~#
dig ftp.srv.world.



; <<>> DiG 9.10.3-P4-Ubuntu <<>> ftp.srv.world.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41265
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ftp.srv.world.             IN      A

;; ANSWER SECTION:
ftp.srv.world.      86400   IN      CNAME   dlp.srv.world.
dlp.srv.world.      86400   IN      A       10.0.0.30

;; AUTHORITY SECTION:
srv.world.          86400   IN      NS      dlp.srv.world.

;; Query time: 0 msec
;; SERVER: 10.0.0.30#53(10.0.0.30)
;; WHEN: Fri Apr 22 17:16:13 JST 2016
;; MSG SIZE  rcvd: 93
```

Slave DNS Server

Configure BIND as a Slave DNS Server.
The following example shows an environment that master DNS is "172.16.0.82", Slave DNS is "slave.example.host".

[1] Configure DNS master server.

```
root@dlp:~#
vi /etc/bind/named.conf.options
options {
directory "/etc/bind";
```

```
// If there is a firewall between you and nameservers you want

// to talk to, you may need to fix the firewall to allow multiple

// ports to talk. See http://www.kb.cert.org/vuls/id/800113
// If your ISP provided one or more IP addresses for stable

// nameservers, you probably want to use them as forwarders.

// Uncomment the following block, and insert the addresses replacing

// the all-0's placeholder.
// forwarders {

//      0.0.0.0;

// };
# add a range you allow to transfer zones

allow-transfer { localhost; 10.0.0.0/24;
172.16.0.80/29;
 };
auth-nxdomain no; # conform to RFC1035

listen-on-v6 { none; };

};
root@dlp:~#
rndc reload

server reload successful
```

[2] Configure DNS slave server.

```
root@slave:~#
vi /etc/bind/named.conf.external-zones
# add settings like follows

      zone "srv.world" {
            type slave;
            masters { 172.16.0.82; };
            file "/etc/bind/slaves/srv.world.wan";
      };

root@slave:~#
mkdir /etc/bind/slaves

root@slave:~#
chown bind. /etc/bind/slaves

root@slave:~#
```

```
rndc reload

server reload successful
root@slave:~#
ls /etc/bind/slaves

srv.world.wan
# zone file in master DNS has been just transfered
```

Experiment 6: Network File System (NFS)

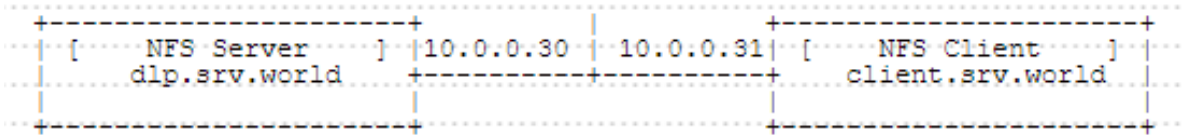
(Ref https://www.server-world.info/en/note?os=Ubuntu_16.04&p=nfs&f=1)

NFS allows a system to share directories and files with others over a network. By using NFS, users and programs can access files on remote systems almost as if they were local files.
Some of the most notable benefits that NFS can provide are:

- Local workstations use less disk space because commonly used data can be stored on a single machine and still remain accessible to others over the network.
- There is no need for users to have separate home directories on every network machine. Home directories could be set up on the NFS server and made available throughout the network.
- Storage devices such as floppy disks, CDROM drives, and USB Thumb drives can be used by other machines on the network. This may reduce the number of removable media drives throughout the network.

Configure NFS Server

Configure NFS Server to share directories on your Network.
This example is based on the environment below.



[1] Configure NFS Server.

```
root@dlp:~#
apt-get -y install nfs-kernel-server
root@dlp:~#
vi /etc/idmapd.conf
# line 6: uncomment and change to your domain name

Domain =
srv.world
root@dlp:~#
vi /etc/exports
# write settings for NFS exports

/home 10.0.0.0/24(rw,no_root_squash)
root@dlp:~#
systemctl restart nfs-server
```

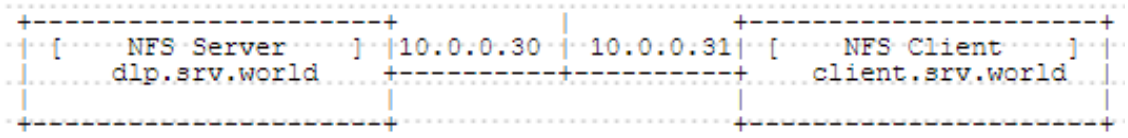
For basic options of exports

Option	Description
rw	Allow both read and write requests on a NFS volume.
ro	Allow only read requests on a NFS volume.

sync	Reply to requests only after the changes have been committed to stable storage. (Default)
async	This option allows the NFS server to violate the NFS protocol and reply to requests before any changes made by that request have been committed to stable storage.
secure	This option requires that requests originate on an Internet port less than IPPORT_RESERVED (1024). (Default)
insecure	This option accepts all ports.
wdelay	Delay committing a write request to disc slightly if it suspects that another related write request may be in progress or may arrive soon. (Default)
no_wdelay	This option has no effect if async is also set. The NFS server will normally delay committing a write request to disc slightly if it suspects that another related write request may be in progress or may arrive soon. This allows multiple write requests to be committed to disc with the one operation which can improve performance. If an NFS server received mainly small unrelated requests, this behaviour could actually reduce performance, so no_wdelay is available to turn it off.
subtree_check	This option enables subtree checking. (Default)
no_subtree_check	This option disables subtree checking, which has mild security implications, but can improve reliability in some circumstances.
root_squash	Map requests from uid/gid 0 to the anonymous uid/gid. Note that this does not apply to any other uids or gids that might be equally sensitive, such as user bin or group staff.
no_root_squash	Turn off root squashing. This option is mainly useful for disk-less clients.
all_squash	Map all uids and gids to the anonymous user. Useful for NFS exported public FTP directories, news spool directories, etc.
no_all_squash	Turn off all squashing. (Default)
anonuid=UID	These options explicitly set the uid and gid of the anonymous account. This option is primarily useful for PC/NFS clients, where you might want all requests appear to be from one user. As an example, consider the export entry for /home/joe in the example section below, which maps all requests to uid 150.
anongid=GID	Read above (anonuid=UID)

Configure NFS Client (Ubuntu)

Configure NFS Client. This example is based on the environment below.



[1] Configure NFS Client.

```
root@client:~#
apt-get -y install nfs-common
root@client:~#
vi /etc/idmapd.conf
# line 6: uncomment and change to your domain name

Domain =
srv.world
root@client:~#
mount -t nfs dlp.srv.world:/home /home

root@client:~#
df -hT


Filesystem              Type      Size  Used Avail Use% Mounted on
udev                    devtmpfs  2.0G     0  2.0G   0% /dev
tmpfs                   tmpfs     396M  5.6M  390M   2% /run
/dev/mapper/ubuntu--vg-root ext4       25G  1.4G   23G   6% /
tmpfs                   tmpfs     2.0G     0  2.0G   0% /dev/shm
tmpfs                   tmpfs     5.0M     0  5.0M   0% /run/lock
tmpfs                   tmpfs     2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/vda1               ext2      472M   55M  393M  13% /boot
tmpfs                   tmpfs     100K     0  100K   0% /run/lxcfs/controllers
tmpfs                   tmpfs     396M     0  396M   0% /run/user/0
dlp.srv.world:/home     nfs4       25G  1.4G   23G   6% /home
# /home from NFS server is mounted
```

[2] Configure NFS mounting on fstab to mount it when the system boot.

```
root@client:~#
vi /etc/fstab
# add like follows

dlp.srv.world:/home   /home  nfs     defaults        0       0
```

[3] Configure auto-mounting.
For example, set NFS directory on /mntdir.

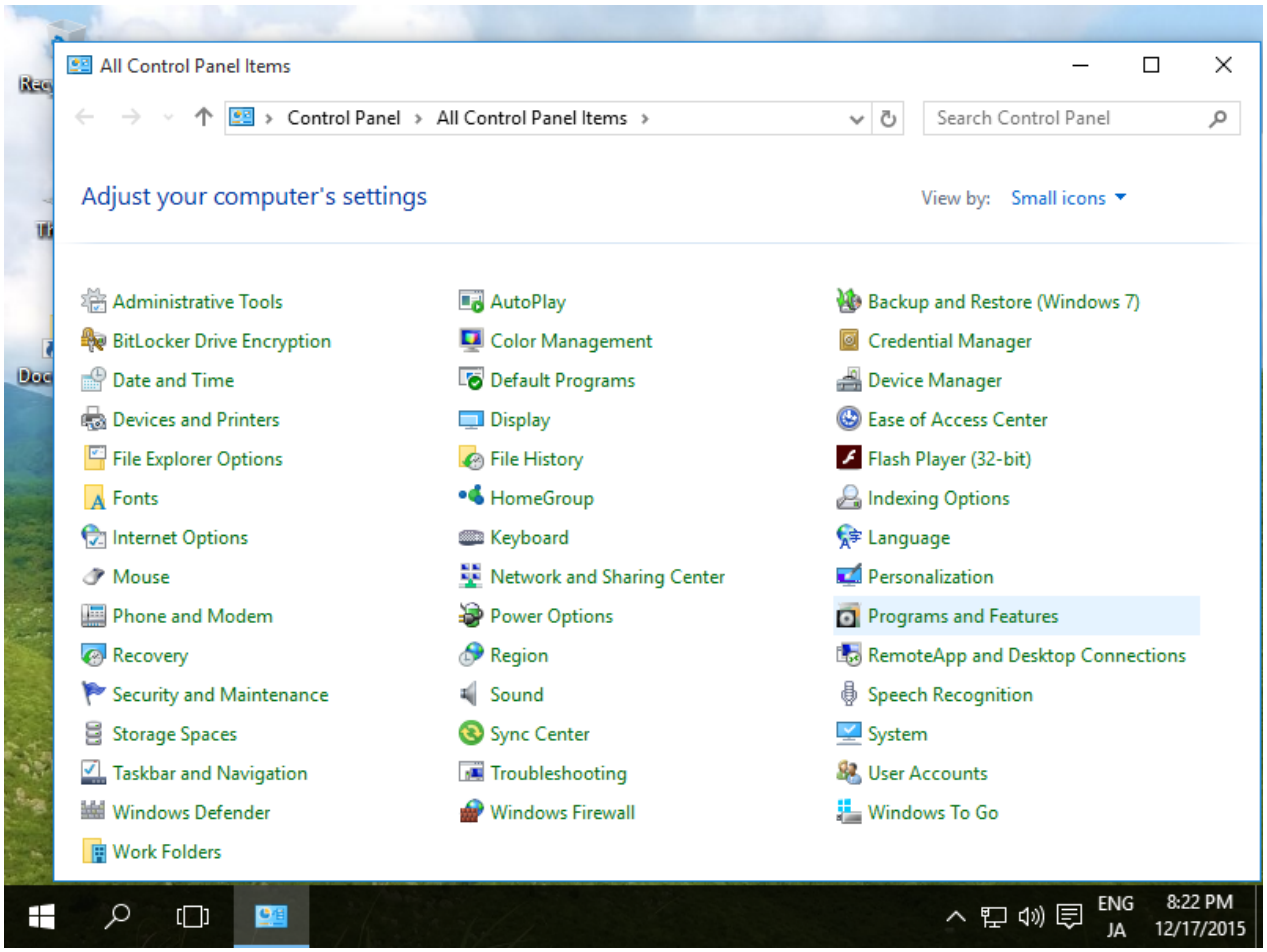
```
root@client:~#
```

```
apt-get -y install autofs
root@client:~#
vi /etc/auto.master
# add follows to the end

/-    /etc/auto.mount

root@client:~#
vi /etc/auto.mount
# create new : [mount point] [option] [location]

/mntdir -fstype=nfs,rw  dlp.srv.world:/home

root@client:~#
mkdir /mntdir

root@client:~#
systemctl restart autofs
# move to the mount point to verify it works normally

root@client:~#
cd /mntdir

root@client:/mntdir#
ll


total 12
drwxr-xr-x  3 root   root   4096 Apr 22 11:45 ./
drwxr-xr-x 24 root   root   4096 Apr 25 09:42 ../
drwxr-xr-x  4 ubuntu ubuntu 4096 Apr 22 15:46 ubuntu/

root@client:/mntdir#
cat /proc/mounts | grep mntdir


/etc/auto.mount /mntdir autofs
rw,relatime,fd=6,pgrp=4209,timeout=300,minproto=5,maxproto=5,direct 0 0
dlp.srv.world:/home /mntdir nfs4
rw,relatime,vers=4.0,rsize=524288,wsize=524288,namlen=255,hard,proto=tcp,
port=0,timeo=600,retrans=2,sec=sys,clientaddr=10.0.0.31,local_lock=none,addr=10.0.0
.30 0 0
```

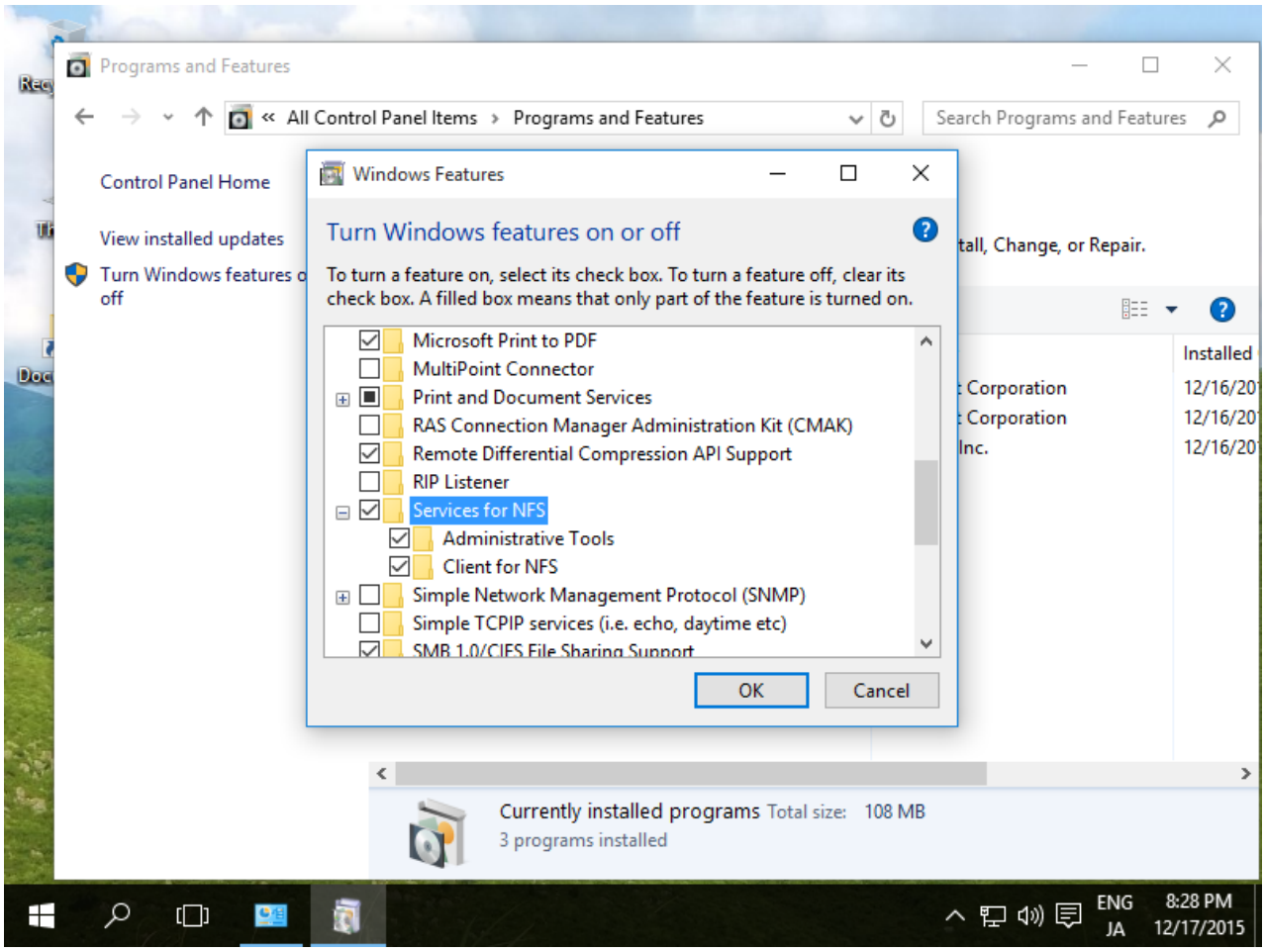
Configure NFS Client(Win Client)

Configure NFS Client on Windows Client OS.
This example is on Windows 10 Enterprise.

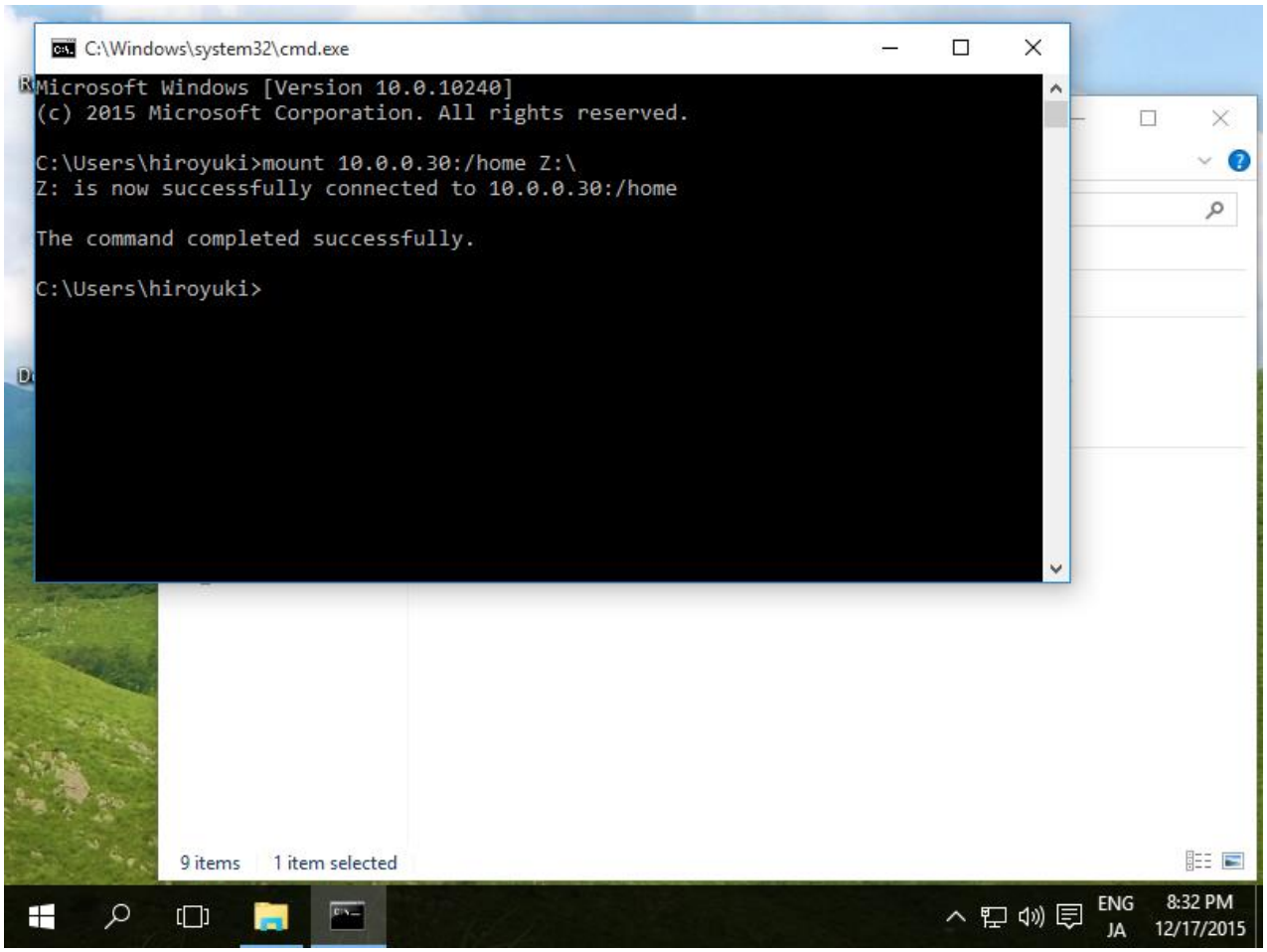
[1] Open [Control Panel] - [Programs and Fetures].



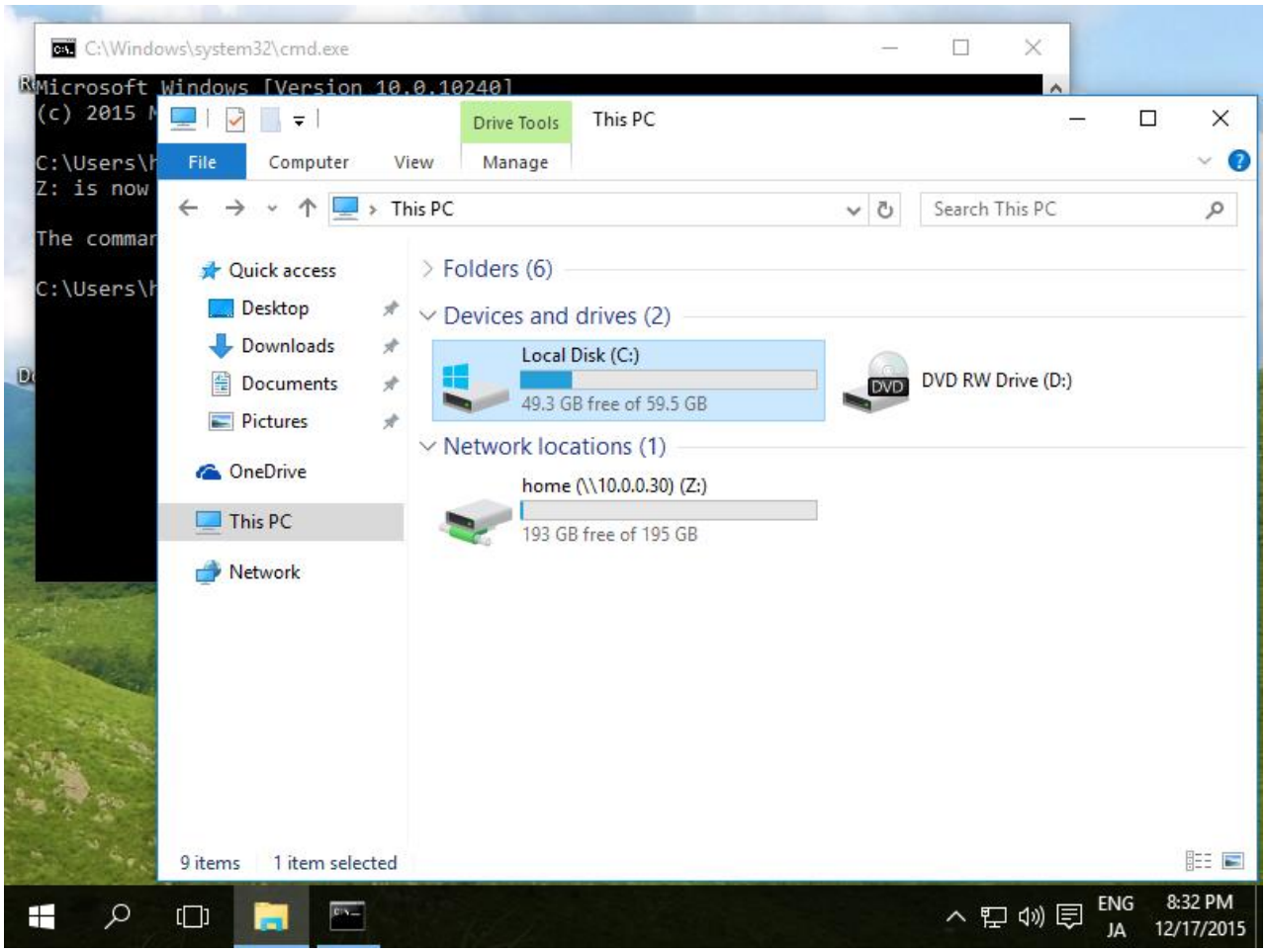
[2] Click [Turn Windows fetures on or off] on the left-side and check boxes on [Services for NFS] like follows and click [OK] button.



[3] It's ready to mount NFS shared. Run cmd.exe with administrator privilege and input commands like follows.
⇒ mount [NFS server's hostname or IP address]:/[shared name] [local drive]:\
If connected normally, successful message is shown like follows.



[4] Open explorer, then mounted NFS shared is displayed like follows.


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10240]
(c) 2015 M
C:\Users\h
Z: is now
The commar
C:\Users\h
Drive Tools
This PC
File
Computer
View
Manage
This PC
Search This PC
Quick access
Desktop
Downloads
Documents
Pictures
OneDrive
This PC
Network
Folders (6)
Devices and drives (2)
Local Disk (C:)
49.3 GB free of 59.5 GB
DVD
DVD RW Drive (D:)
Network locations (1)
home (\\10.0.0.30) (Z:)
193 GB free of 195 GB
9 items
1 item selected
ENG
JA
8:32 PM
12/17/2015

Experiment 7: Configure LDAP Server

(Ref https://www.server-world.info/en/note?os=Ubuntu_16.04&p=openldap&f=1)

The Lightweight Directory Access Protocol, or LDAP, is a protocol for querying and modifying a X.500-based directory service running over TCP/IP. The current LDAP version is LDAPv3, as defined in *RFC4510*, and the implementation in Ubuntu is OpenLDAP.
So the LDAP protocol accesses LDAP directories. Here are some key concepts and terms:

- A LDAP directory is a tree of data *entries* that is hierarchical in nature and is called the Directory Information Tree (DIT).
- An entry consists of a set of *attributes*.
- An attribute has a *type* (a name/description) and one or more *values*.
- Every attribute must be defined in at least one *objectClass*.
- Attributes and objectclasses are defined in *schemas* (an objectclass is actually considered as a special kind of attribute).
- Each entry has a unique identifier: its *Distinguished Name* (DN or dn). This, in turn, consists of a *Relative Distinguished Name* (RDN) followed by the parent entry's DN.
- The entry's DN is not an attribute. It is not considered part of the entry itself.

Configure LDAP Server in order to share users' accounts in your local networks.

[1] Install OpenLDAP.

```
root@dlp:~#
apt-get -y install slapd ldap-utils
# set LDAP admin password during installation like follows


 +-------------------------------------------------| Configuring slapd |--+
 | Please enter the password for the admin entry in your LDAP directory.  |
 |                                                                        |
 | Administrator password:                                                |
 |                                                                        |
 | ********_______________________________________________________________ |
 |                                                                        |
 |                        <Ok>                                            |
 |                                                                        |
 +------------------------------------------------------------------------+

# confirm settings

root@dlp:~#
slapcat


dn: dc=srv,dc=world
objectClass: top
objectClass: dcObject
objectClass: organization
o: srv.world
dc: srv
structuralObjectClass: organization
entryUUID: 10b94454-b747-1035-8c5c-7fa90ef080bf
```

```
creatorsName: cn=admin,dc=srv,dc=world
createTimestamp: 20160526043549Z
entryCSN: 20160526043549.180234Z#000000#000#000000
modifiersName: cn=admin,dc=srv,dc=world
modifyTimestamp: 20160526043549Z

dn: cn=admin,dc=srv,dc=world
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword::
e1NTSEF9Y2w1NklOTW9VaytSVnNUMUxlME9ZUlJDZHFaN1pVSEs=
structuralObjectClass: organizationalRole
entryUUID: 10bf9dea-b747-1035-8c5d-7fa90ef080bf
creatorsName: cn=admin,dc=srv,dc=world
createTimestamp: 20160526043549Z
entryCSN: 20160526043549.221895Z#000000#000#000000
modifiersName: cn=admin,dc=srv,dc=world
modifyTimestamp: 20160526043549Z
```

[2] Add base dn.

```
root@dlp:~#
vi base.ldif
# create new

# change to your own suffix for the field 'dc=srv,dc=world'

dn: ou=people,dc=srv,dc=world
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=srv,dc=world
objectClass: organizationalUnit
ou: groups

root@dlp:~#
ldapadd -x -D cn=admin,dc=srv,dc=world -W -f base.ldif

Enter LDAP Password:
# LDAP admin password (set in installation of openldap)


adding new entry "ou=people,dc=srv,dc=world"

adding new entry "ou=groups,dc=srv,dc=world"
```

Add User Accounts

Add LDAP User Accounts in the OpenLDAP Server.

[1] Add a user.

```
# generate encrypted password

root@dlp:~#
slappasswd

New password:
Re-enter new password:
{SSHA}xxxxxxxxxxxxxxxxx
root@dlp:~#
vi ldapuser.ldif
# create new
# replace to your own domain name for "dc=***,dc=***" section
dn: uid=xerus,ou=people,dc=srv,dc=world
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: xerus
sn: ubuntu
userPassword: {SSHA}xxxxxxxxxxxxxxxxx
loginShell: /bin/bash
uidNumber: 2000
gidNumber: 2000
homeDirectory: /home/xerus

dn: cn=xerus,ou=groups,dc=srv,dc=world
objectClass: posixGroup
cn: xerus
gidNumber: 2000
memberUid: xerus

root@dlp:~#
ldapadd -x -D cn=admin,dc=srv,dc=world -W -f ldapuser.ldif

Enter LDAP Password:

adding new entry "uid=xerus,ou=people,dc=srv,dc=world"

adding new entry "cn=xerus,ou=groups,dc=srv,dc=world"
```

[2] Add users and groups in local passwd/group to LDAP directory.

```
root@dlp:~#
vi ldapuser.sh
# extract local users and groups who have 1000-9999 digit UID
# replace "SUFFIX=***" to your own domain name
# this is an example
#!/bin/bash

SUFFIX='dc=srv,dc=world'
LDIF='ldapuser.ldif'
```

```
echo -n > $LDIF
GROUP_IDS=()
grep "x:[1-9][0-9][0-9][0-9]:" /etc/passwd | (while read TARGET_USER
do
   USER_ID="$(echo "$TARGET_USER" | cut -d':' -f1)"

   USER_NAME="$(echo "$TARGET_USER" | cut -d':' -f5 | cut -d',' -f1 )"
   [ ! "$USER_NAME" ] && USER_NAME="$USER_ID"

   LDAP_SN="$(echo "$USER_NAME" | awk '{print $2}')"
   [ ! "$LDAP_SN" ] && LDAP_SN="$USER_ID"

   LASTCHANGE_FLAG="$(grep "${USER_ID}:" /etc/shadow | cut -d':' -f3)"
   [ ! "$LASTCHANGE_FLAG" ] && LASTCHANGE_FLAG="0"

   SHADOW_FLAG="$(grep "${USER_ID}:" /etc/shadow | cut -d':' -f9)"
   [ ! "$SHADOW_FLAG" ] && SHADOW_FLAG="0"

   GROUP_ID="$(echo "$TARGET_USER" | cut -d':' -f4)"
   [ ! "$(echo "${GROUP_IDS[@]}" | grep "$GROUP_ID")" ] &&
GROUP_IDS=("${GROUP_IDS[@]}" "$GROUP_ID")

   echo "dn: uid=$USER_ID,ou=people,$SUFFIX" >> $LDIF
   echo "objectClass: inetOrgPerson" >> $LDIF
   echo "objectClass: posixAccount" >> $LDIF
   echo "objectClass: shadowAccount" >> $LDIF
   echo "sn: $LDAP_SN" >> $LDIF
   echo "givenName: $(echo "$USER_NAME" | awk '{print $1}')" >> $LDIF
   echo "cn: $(echo "$USER_NAME" | awk '{print $1}')" >> $LDIF
   echo "displayName: $USER_NAME" >> $LDIF
   echo "uidNumber: $(echo "$TARGET_USER" | cut -d':' -f3)" >> $LDIF
   echo "gidNumber: $(echo "$TARGET_USER" | cut -d':' -f4)" >> $LDIF
   echo "userPassword: {crypt}$(grep "${USER_ID}:" /etc/shadow | cut -d':' -f2)" >>
$LDIF
   echo "gecos: $USER_NAME" >> $LDIF
   echo "loginShell: $(echo "$TARGET_USER" | cut -d':' -f7)" >> $LDIF
   echo "homeDirectory: $(echo "$TARGET_USER" | cut -d':' -f6)" >> $LDIF
   echo "shadowExpire: $(passwd -S "$USER_ID" | awk '{print $7}')" >> $LDIF
   echo "shadowFlag: $SHADOW_FLAG" >> $LDIF
   echo "shadowWarning: $(passwd -S "$USER_ID" | awk '{print $6}')" >> $LDIF
   echo "shadowMin: $(passwd -S "$USER_ID" | awk '{print $4}')" >> $LDIF
   echo "shadowMax: $(passwd -S "$USER_ID" | awk '{print $5}')" >> $LDIF
   echo "shadowLastChange: $LASTCHANGE_FLAG" >> $LDIF
   echo >> $LDIF
done

for TARGET_GROUP_ID in "${GROUP_IDS[@]}"
do
   LDAP_CN="$(grep ":${TARGET_GROUP_ID}:" /etc/group | cut -d':' -f1)"
```

```
   echo "dn: cn=$LDAP_CN,ou=groups,$SUFFIX" >> $LDIF
   echo "objectClass: posixGroup" >> $LDIF
   echo "cn: $LDAP_CN" >> $LDIF
   echo "gidNumber: $TARGET_GROUP_ID" >> $LDIF

   for MEMBER_UID in $(grep ":${TARGET_GROUP_ID}:" /etc/passwd | cut -d':' -
f1,3)
   do
      UID_NUM=$(echo "$MEMBER_UID" | cut -d':' -f2)
      [ $UID_NUM -ge 1000 -a $UID_NUM -le 9999 ] && echo "memberUid: $(echo
"$MEMBER_UID" | cut -d':' -f1)" >> $LDIF
   done
   echo >> $LDIF
done
)

root@dlp:~#
bash ldapuser.sh

root@dlp:~#
ldapadd -x -D cn=admin,dc=srv,dc=world -W -f ldapuser.ldif

Enter LDAP Password:

adding new entry "uid=ubuntu,ou=people,dc=srv,dc=world"
adding new entry "uid=redhat,ou=people,dc=srv,dc=world"
adding new entry "uid=cent,ou=people,dc=srv,dc=world"
adding new entry "uid=debian,ou=people,dc=srv,dc=world"
adding new entry "cn=ubuntu,ou=groups,dc=srv,dc=world"
adding new entry "cn=redhat,ou=groups,dc=srv,dc=world"
adding new entry "cn=cent,ou=groups,dc=srv,dc=world"
adding new entry "cn=debian,ou=groups,dc=srv,dc=world"
```

[3] If you'd like to delete LDAP User or Group, Do as below.

```
root@dlp:~#
ldapdelete -x -W -D 'cn=admin,dc=srv,dc=world'
"uid=ubuntu,ou=people,dc=srv,dc=world"

Enter LDAP Password:
root@dlp:~#
ldapdelete -x -W -D 'cn=admin,dc=srv,dc=world'
"cn=ubuntu,ou=groups,dc=srv,dc=world"

Enter LDAP Password:
```

Configure LDAP Client

Configure LDAP Client in order to share users' accounts in your local networks.

[1] Configure LDAP Client.

root@www:~#
apt-get -y install libnss-ldap libpam-ldap ldap-utils
(1) specify LDAP server's URI

```
 +---------------------| Configuring ldap-auth-config |----------------------+
 | Please enter the URI of the LDAP server to use. This is a string in the   |
 | form of ldap://<hostname or IP>:<port>/. ldaps:// or ldapi:// can also    |
 | be used. The port number is optional.                                     |
 |                                                                           |
 | Note: It is usually a good idea to use an IP address because it reduces   |
 | risks of failure in the event name service problems.                      |
 |                                                                           |
 | LDAP server Uniform Resource Identifier:                                  |
 |                                                                           |
 | ldap://dlp.srv.world/_____________________________________________________    |
 |                                                                           |
 |                          <Ok>                                             |
 |                                                                           |
 +---------------------------------------------------------------------------+
```

(2) specify suffix

```
 +---------------------| Configuring ldap-auth-config |----------------------+
 | Please enter the distinguished name of the LDAP search base. Many sites   |
 | use the components of their domain names for this purpose. For example,   |
 | the domain "example.net" would use "dc=example,dc=net" as the             |
 | distinguished name of the search base.                                    |
 |                                                                           |
 | Distinguished name of the search base:                                    |
 |                                                                           |
 | dc=srv,dc=world____________________________________________________________    |
 |                                                                           |
 |                          <Ok>                                             |
 |                                                                           |
 +---------------------------------------------------------------------------+
```

(3) specify LDAP version

```
  +---------------------| Configuring ldap-auth-config |----------------------+
  | Please enter which version of the LDAP protocol should be used by         |
  | ldapns. It is usually a good idea to set this to the highest available    |
  | version.                                                                  |
  |                                                                           |
  | LDAP version to use:                                                      |
  |                                                                           |
  |                          3                                                |
  |                          2                                                |
```

```
|                                                                    |
|                                                                    |
|                        <Ok>                                        |
|                                                                    |
+--------------------------------------------------------------------+
```

(4) select the one you like. (this example selects 'Yes')

```
+--------------------| Configuring ldap-auth-config |----------------------+
|                                                                         |
| This option will allow you to make password utilities that use pam to   |
| behave like you would be changing local passwords.                      |
|                                                                         |
| The password will be stored in a separate file which will be made       |
| readable to root only.                                                  |
|                                                                         |
| If you are using NFS mounted /etc or any other custom setup, you should |
| disable this.                                                           |
|                                                                         |
| Make local root Database admin:                                         |
|                                                                         |
|               <Yes>                  <No>                               |
|                                                                         |
+-------------------------------------------------------------------------+
```

(5) select the one you like. (this example selects 'No')

```
  +-------------------| Configuring ldap-auth-config |-------------------+
  |                                                                      |
  | Choose this option if you are required to login to the database to   |
  | retrieve entries.                                                    |
  |                                                                      |
  | Note: Under a normal setup, this is not needed.                      |
  |                                                                      |
  | Does the LDAP database require login?                                |
  |                                                                      |
  |               <Yes>                  <No>                            |
  |                                                                      |
  +----------------------------------------------------------------------+
```

(6) specify LDAP admin account's suffix

```
      +-------------| Configuring ldap-auth-config |-------------+
      | This account will be used when root changes a password.  |
      |                                                          |
      | Note: This account has to be a privileged account.       |
      |                                                          |
```

```
        | LDAP account for root:                          |
        |                                                 |
        | cn=admin,dc=srv,dc=world_____________________   |
        |                                                 |
        |                    <Ok>                         |
        |                                                 |
        +-------------------------------------------------+
```

(7) specify password for LDAP admin account

```
 +---------------------| Configuring ldap-auth-config |----------------------+
 | Please enter the password to use when ldap-auth-config tries to login to  |
 | the LDAP directory using the LDAP account for root.                       |
 |                                                                           |
 | The password will be stored in a separate file /etc/ldap.secret which     |
 | will be made readable to root only.                                       |
 |                                                                           |
 | Entering an empty password will re-use the old password.                  |
 |                                                                           |
 | LDAP root account password:                                               |
 |                                                                           |
 |
_____________________________________________________________________________ |
 |                                                                           |
 |                          <Ok>                                             |
 |                                                                           |
 +---------------------------------------------------------------------------+
```

```
root@www:~#
vi /etc/nsswitch.conf
# line 7: add

passwd:     compat
ldap

group:     compat
ldap

shadow:     compat
ldap
root@www:~#
vi /etc/pam.d/common-password
# line 26: change ( remove 'use_authtok' )

password     [success=1 user_unknown=ignore default=die]     pam_ldap.so
try_first_pass
root@www:~#
vi /etc/pam.d/common-session
# add to the end if need ( create home directory automatically at initial login )
```

session optional pam_mkhomedir.so skel=/etc/skel umask=077
root@www:~#
exit
Ubuntu 16.04 LTS www.srv.world ttyS0
www login:
debian

 # LDAP user

Password:

Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-22-generic x86_64)

*** Documentation: https://help.ubuntu.com/**

8 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Creating directory '/home/debian'.
debian@www:~$
 # just logined

debian@www:~$
passwd
 # try to change LDAP password

Enter login(LDAP) password:
 # input current password

New password:
 # input new password

```
Re-enter new password:
# confirm

LDAP password information changed for debian
passwd: password updated successfully
# just changed
```

Install phpLDAPadmin

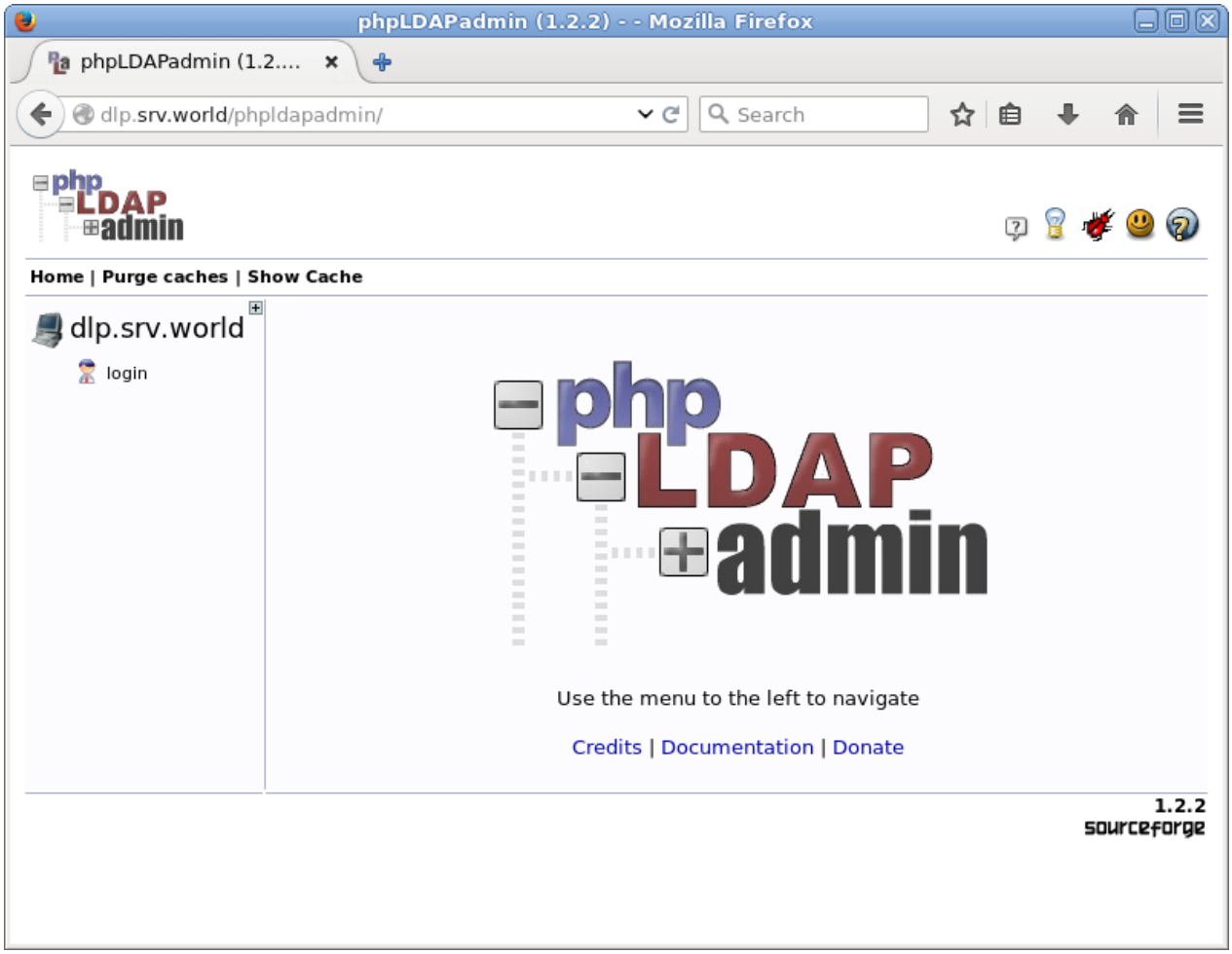
Install phpLDAPadmin to operate LDAP server via Web browser.

[1] Install and start Apache2, refer to here.
[2] Install PHP, refer to here.
[3] Install phpLDAPadmin.

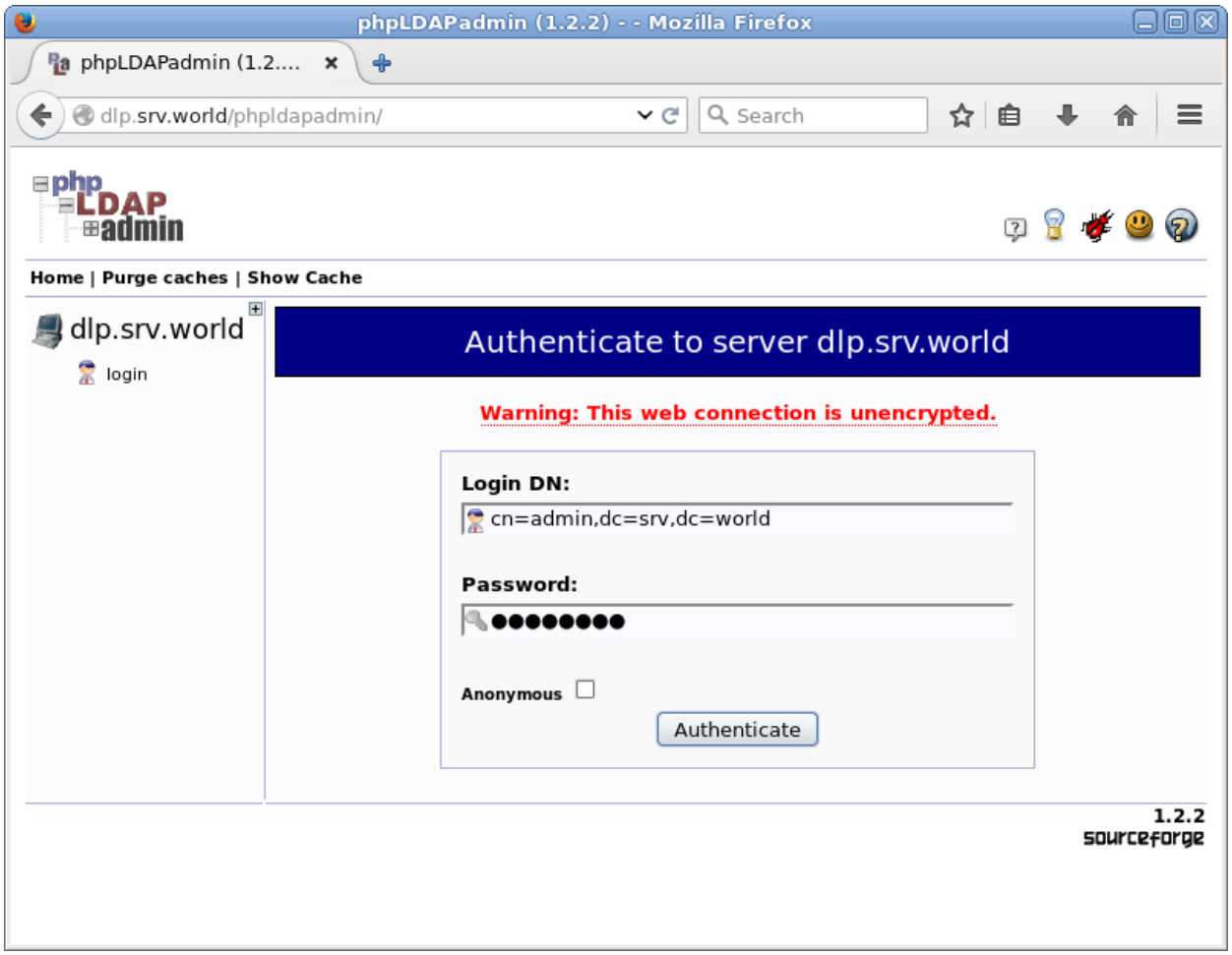
```
root@dlp:~#
apt-get -y install phpldapadmin
root@dlp:~#
vi /etc/phpldapadmin/config.php
# line 286: specify LDAP server's name

$servers->setValue('server','name','
dlp.srv.world
');
# line 293: specify LDAP server's IP

$servers->setValue('server','host','
127.0.0.1
');
# line 296: uncomment - LDAP server's port

$servers->setValue('server','port',389);
# line 300: change to your domain name

$servers->setValue('server','base',array('
dc=srv,dc=world
'));
# line 326: change to your domain name

$servers->setValue('login','bind_id','cn=admin,
dc=srv,dc=world
');
root@dlp:~#
vi /etc/apache2/conf-enabled/phpldapadmin.conf
# line 21: change access permission


#
Order allow,deny
```

```
#
Allow from all
   Order deny,allow
   Deny from all
   Allow from 127.0.0.1 10.0.0.0/24
root@dlp:~#
systemctl restart apache2
```

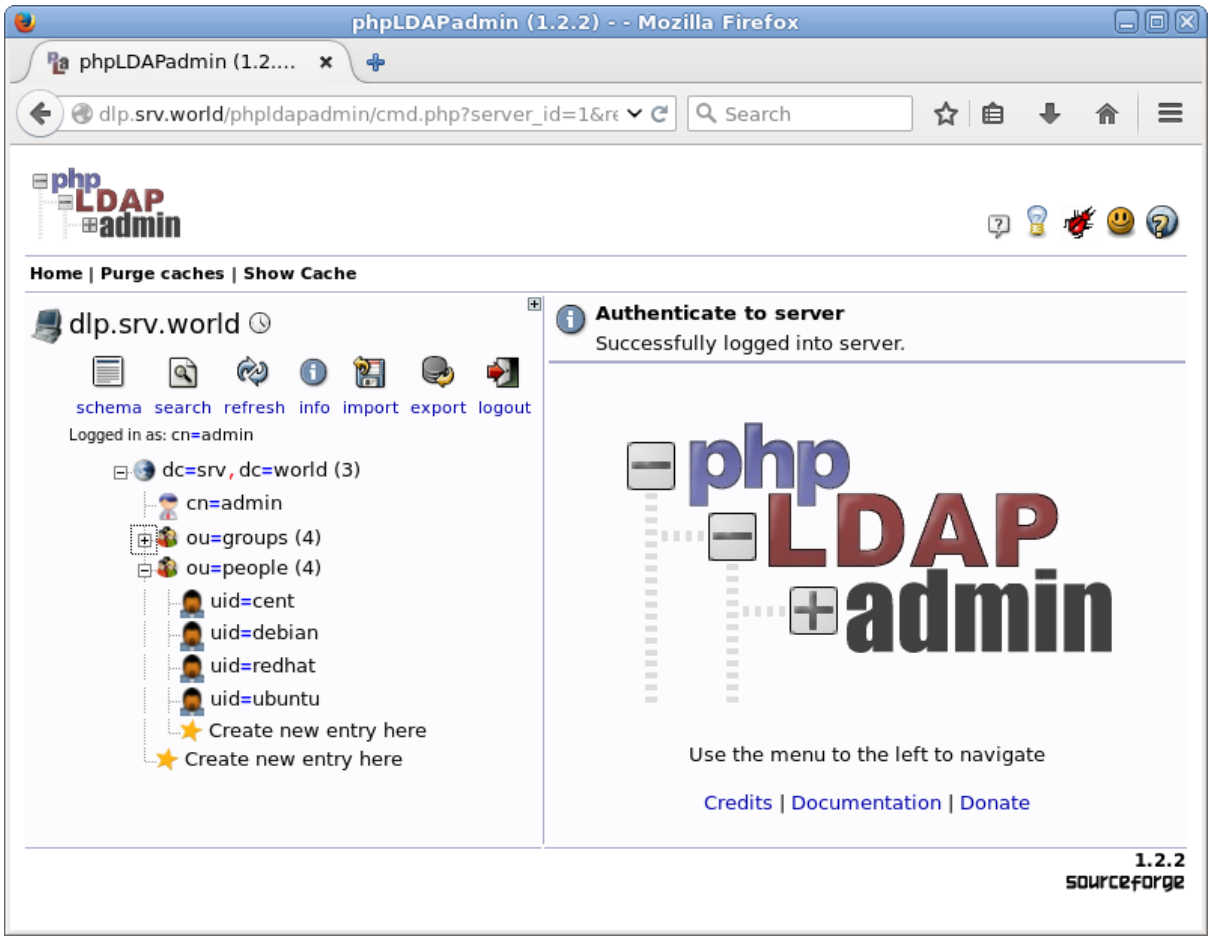
[4] Access to the "http://(server's hostname or IP address)/phpldapadmin/" from a client which is in the network allowed by http server and then Click "login".



[5] Authenticate with admin user.



[6] Just logined. It's possible to manage LDAP server on here.


phpLDAPadmin (1.2.2) - - Mozilla Firefox
phpLDAPadmin (1.2....
dlp.srv.world/phpldapadmin/cmd.php?server_id=1&re
Search
Home | Purge caches | Show Cache
dlp.srv.world
schema search refresh info import export logout
Logged in as: cn=admin
dc=srv, dc=world (3)
cn=admin
ou=groups (4)
ou=people (4)
uid=cent
uid=debian
uid=redhat
uid=ubuntu
Create new entry here
Create new entry here
Authenticate to server
Successfully logged into server.
Use the menu to the left to navigate
Credits | Documentation | Donate
1.2.2
sourceforge

Experiment 8: Configure NIS Server

(Ref https://www.server-world.info/en/note?os=Ubuntu_16.04&p=nis&f=1)

NIS, or **Network Information Systems,** is a network service that allows authentication and login information to be stored on a centrally located server. This includes the username and password database for login authentication, database of user groups, and the locations of home directories.

Configure NIS Server in order to share users' accounts in your local networks.

[1] Install NIS.

```
root@dlp:~#
apt-get -y install nis
Preconfiguring packages ...
# input domain name

# Autostart NIS during installation will be fail because configuration is none yet, so
wait for a moment to finish it.


 +---------------------------| Configuring nis |---------------------------+
 | Please choose the NIS "domainname" for this system. If you want this     |
 | machine to just be a client, you should enter the name of the NIS domain  |
 | you wish to join.                                                         |
 |                                                                           |
 | Alternatively, if this machine is to be a NIS server, you can either      |
 | enter a new NIS "domainname" or the name of an existing NIS domain.       |
 |                                                                           |
 | NIS domain:                                                               |
 |                                                                           |
 | srv.world_____________________________________________________________    |
 |                                                                           |
 |                      <Ok>                                                 |
 |                                                                           |
 +---------------------------------------------------------------------------+
```

[2] Configure as a NIS master Server.

```
root@dlp:~#
vi /etc/default/nis
# line 6: change (set NIS master server)

NISSERVER=
master
root@dlp:~#
vi /etc/ypserv.securenets
# This line gives access to everybody. PLEASE ADJUST!
# comment out

#
 0.0.0.0 0.0.0.0
```

```
# add to the end: IP range you allow to access

255.255.255.0   10.0.0.0

root@dlp:~#
vi /var/yp/Makefile
# line 52: change

MERGE_PASSWD=
true
# line 56: change

MERGE_GROUP=
true
root@dlp:~#
vi /etc/hosts
127.0.0.1       localhost
# add own IP address for NIS

10.0.0.30       dlp.srv.world       dlp

root@dlp:~#
systemctl restart nis
# update NIS database

root@dlp:~#
/usr/lib/yp/ypinit -m
At this point, we have to construct a list of the hosts which will run NIS
servers.  dlp 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:  dlp.srv.world
        next host to add:
# Ctrl+D key


The current list of NIS servers looks like this:

dlp

Is this correct? [y/n: y]
y


We need a few minutes to build the databases...
Building /var/yp/srv.world/ypservers...
Running /var/yp/Makefile...
make[1]: Entering directory '/var/yp/srv.world'
Updating passwd.byname...
Updating passwd.byuid...
```

```
Updating group.byname...
Updating group.bygid...
Updating hosts.byname...
Updating hosts.byaddr...
Updating rpc.byname...
Updating rpc.bynumber...
Updating services.byname...
Updating services.byservicename...
Updating netid.byname...
Updating protocols.bynumber...
Updating protocols.byname...
Updating netgroup...
Updating netgroup.byhost...
Updating netgroup.byuser...
Updating shadow.byname... Ignored -> merged with passwd
make[1]: Leaving directory '/var/yp/srv.world'

dlp.srv.world has been set up as a NIS master server.

Now you can run ypinit -s dlp.srv.world on all slave server.
```

[3] If you added users in local server, apply them to NIS database, too.

```
root@dlp:~#
cd /var/yp

root@dlp:/var/yp#
make
```

Configure NIS Client

Configure NIS Client to bind NIS Server.

[1] Install nis packages.

```
root@www:~#
apt-get -y install nis
Preconfiguring packages ...
# input domain name


 +---------------------------| Configuring nis |---------------------------+
 | Please choose the NIS "domainname" for this system. If you want this     |
 | machine to just be a client, you should enter the name of the NIS domain |
 | you wish to join.                                                        |
 |                                                                          |
 | Alternatively, if this machine is to be a NIS server, you can either     |
 | enter a new NIS "domainname" or the name of an existing NIS domain.      |
 |                                                                          |
 | NIS domain:                                                              |
```

```
|                                                                          |
| srv.world_____________________________________________________________   |
|                                                                          |
|                        <Ok>                                              |
|                                                                          |
+--------------------------------------------------------------------------+
```

[2] Configure as a NIS Client.

```
root@www:~#
vi /etc/yp.conf
#
# yp.conf      Configuration file for the ypbind process. You can define
#              NIS servers manually here if they can't be found by
#              broadcasting on the local net (which is the default).
#
#              See the manual page of ypbind for the syntax of this file.
#
# IMPORTANT:   For the "ypserver", use IP addresses, or make sure that
#              the host is in /etc/hosts. This file is only interpreted
#              once, and if DNS isn't reachable yet the ypserver cannot
#              be resolved and ypbind won't ever bind to the server.

# ypserver ypserver.network.com
# add to the end: [domain name] [server] [NIS server's hostname]

domain srv.world server dlp.srv.world
root@www:~#
vi /etc/nsswitch.conf
passwd:     compat
nis

# line 7; add

group:     compat
nis

# add

shadow:     compat
nis

# add
hosts:     files dns
nis

# add
# set follows if needed (create home directory automatically if none)

root@www:~#
vi /etc/pam.d/common-session
```

 # add to the end

session optional pam_mkhomedir.so skel=/etc/skel umask=077

root@www:~#
systemctl restart nis

root@www:~#
exit
Ubuntu 16.04 LTS www.srv.world ttyS0
www login:
ubuntu

 # NIS user

Password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-22-generic x86_64)

*** Documentation: https://help.ubuntu.com/**

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Creating directory '/home/ubuntu'.
ubuntu@www:~$
 # just logined
 # try to change NIS password

ubuntu@www:~$
yppasswd

Changing NIS account information for ubuntu on dlp.srv.world.
Please enter old password:
Changing NIS password for ubuntu on dlp.srv.world.

```
Please enter new password:
Please retype new password:

The NIS password has been changed on dlp.srv.world.
```

Experiment 9: Install MySQL

(Ref https://www.server-world.info/en/note?os=Ubuntu_16.04&p=mysql&f=1)

MySQL is a fast, multi-threaded, multi-user, and robust SQL database server. It is intended for mission critical, heavy-load production systems as well as for embedding into mass-deployed software.

Install MySQL to configure database server.

[1] Install MySQL.

```
root@www:~#
apt-get -y install mysql-server-5.7
# set MySQL's root password


 +--------------------+ Configuring mysql-server-5.7 +---------------------+
 | While not mandatory, it is highly recommended that you set a password   |
 | for the MySQL administrative "root" user.                               |
 |                                                                         |
 | If this field is left blank, the password will not be changed.          |
 |                                                                         |
 | New password for the MySQL "root" user:                                 |
 |                                                                         |
 | ********_____________________________________________________________ |
 |                                                                         |
 |                        <Ok>                                             |
 |                                                                         |
 +-------------------------------------------------------------------------+

# connect to MySQL

root@www:~#
mysql -u root -p

Enter password:
# MySQL root password you set above


Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.12-0ubuntu1 (Ubuntu)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

# try to display user info
```

```
mysql>
select user,host from mysql.user;


+------------------+-----------+
| user             | host      |
+------------------+-----------+
| debian-sys-maint | localhost |
| mysql.sys        | localhost |
| root             | localhost |
+------------------+-----------+
3 rows in set (0.00 sec)

mysql>
exit

Bye
```

Install phpMyAdmin

Install phpMyAdmin to operate MySQL on web browser from Clients.

[1] Install and start Apache httpd, refer to here.

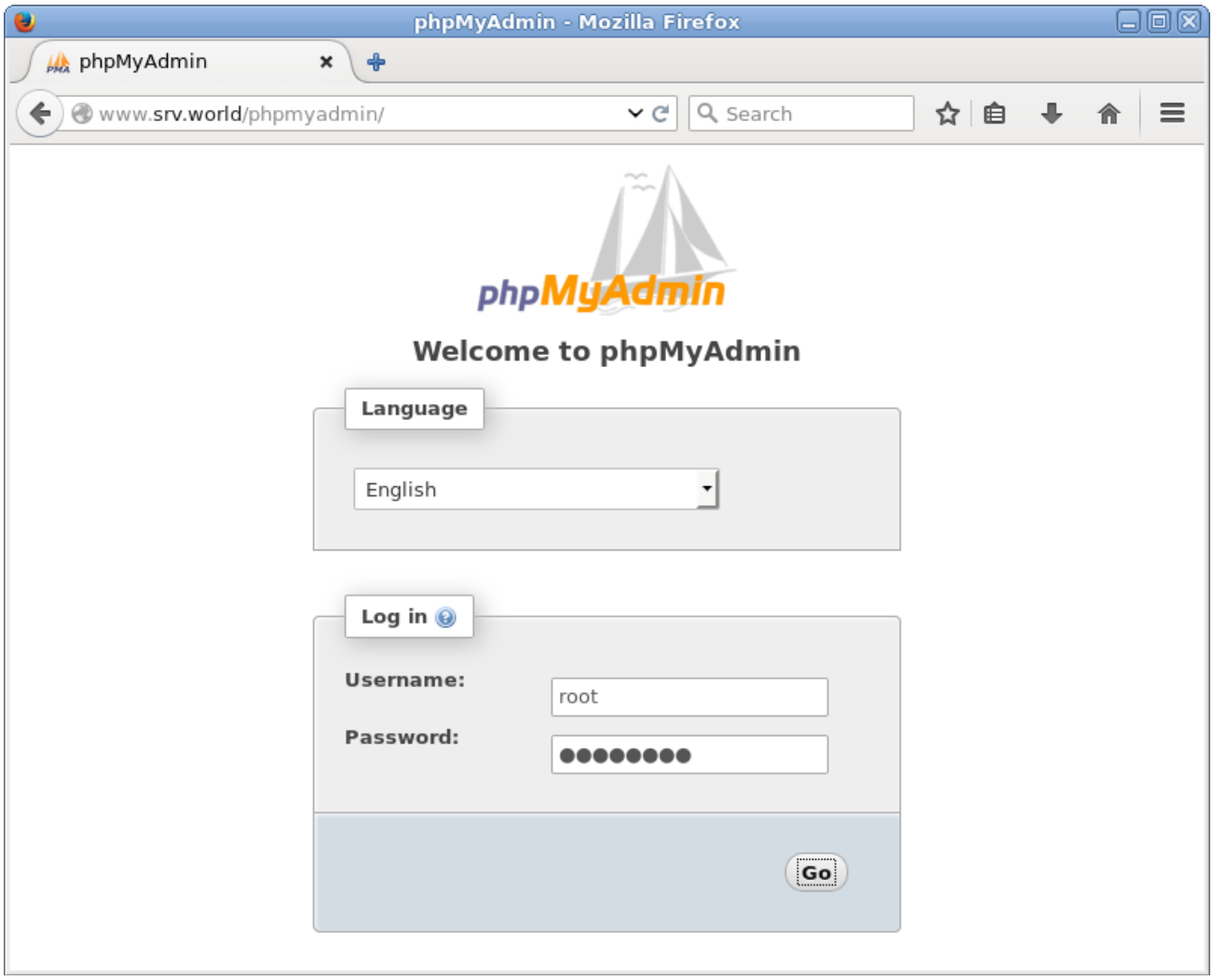
[2] Install PHP, refer to here.

[3] Install phpMyAdmin.

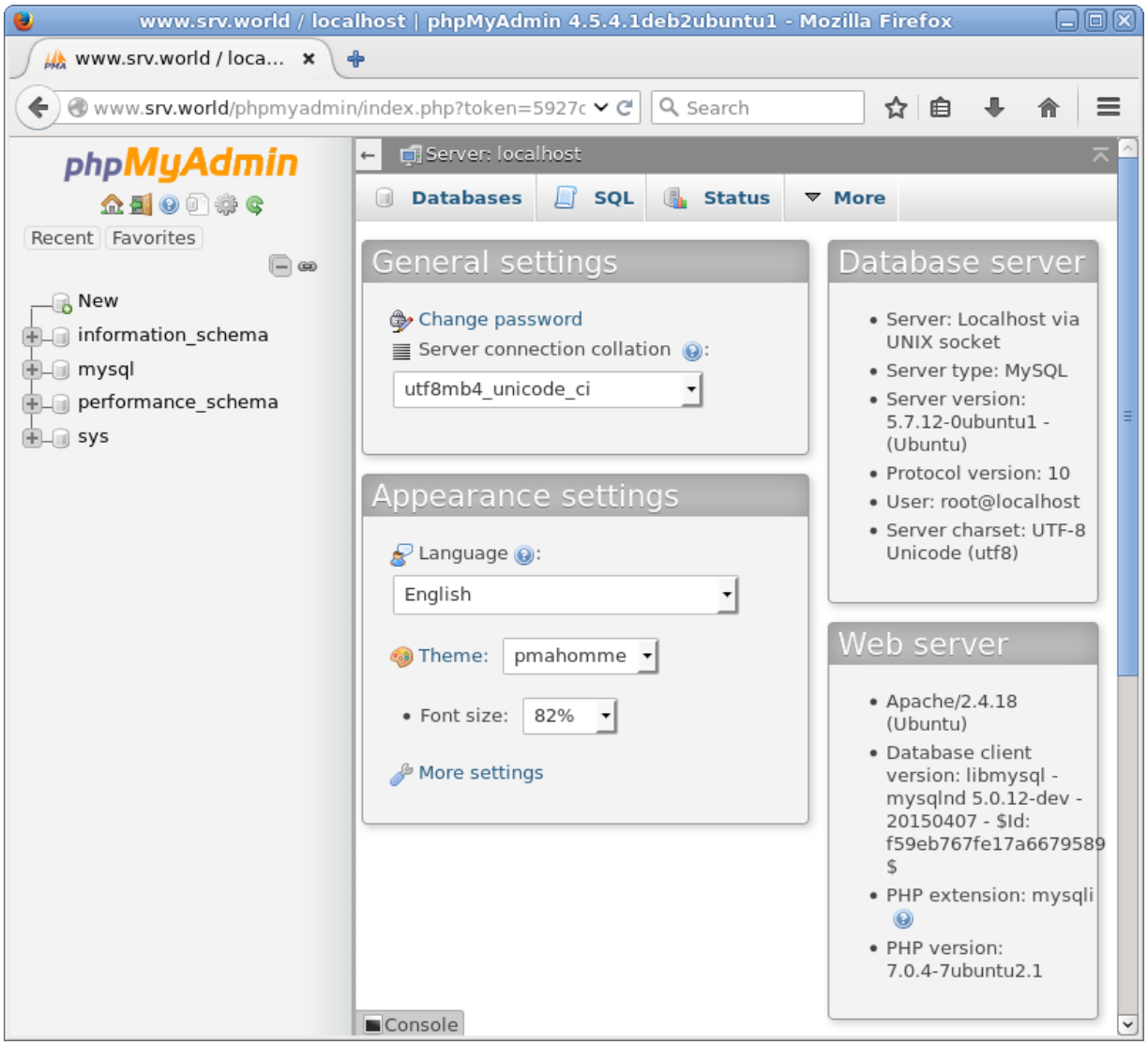
```
root@www:~#
apt-get -y install phpmyadmin php-mbstring php-gettext
# select which one you using (select apache2 on this example)


 +----------------------+ Configuring phpmyadmin +-------------------------+
 | Please choose the web server that should be automatically configured to  |
 | run phpMyAdmin.                                                          |
 |                                                                          |
 | Web server to reconfigure automatically:                                 |
 |                                                                          |
 |   [*] apache2                                                            |
 |   [ ] lighttpd                                                           |
 |                                                                          |
 |                                                                          |
 |                        <Ok>                                              |
 |                                                                          |
 +--------------------------------------------------------------------------+

# answer "No" to proceed on this example


 +----------------------+ Configuring phpmyadmin +-------------------------+
 |                                                                          |
```

```
| The phpmyadmin package must have a database installed and configured      |
| before it can be used.  This can be optionally handled with              |
| dbconfig-common.                                                         |
|                                                                          |
| If you are an advanced database administrator and know that you want to  |
| perform this configuration manually, or if your database has already     |
| been installed and configured, you should refuse this option.  Details   |
| on what needs to be done should most likely be provided in               |
| /usr/share/doc/phpmyadmin.                                               |
|                                                                          |
| Otherwise, you should probably choose this option.                       |
|                                                                          |
| Configure database for phpmyadmin with dbconfig-common?                  |
|                                                                          |
|              <Yes>                <No>                                   |
|                                                                          |
+--------------------------------------------------------------------------+

root@www:~#
vi /etc/phpmyadmin/apache.conf
# line 8: add access permission

Require ip 127.0.0.1 10.0.0.0/24
root@www:~#
systemctl restart apache2
```

[4] Access to "http://(your hostname or IP address)/phpmyadmin/" and login with a user in MySQL.



[5] Just logined. It's possible to operate MySQL on here.


www.srv.world / localhost | phpMyAdmin 4.5.4.1deb2ubuntu1 - Mozilla Firefox
www.srv.world / loca...
www.srv.world/phpmyadmin/index.php?token=5927c
Search
phpMyAdmin
Recent
Favorites
New
information_schema
mysql
performance_schema
sys
Server: localhost
Databases
SQL
Status
More
General settings
Change password
Server connection collation:
utf8mb4_unicode_ci
Appearance settings
Language:
English
Theme:
pmahomme
Font size:
82%
More settings
Database server
Server: Localhost via UNIX socket
Server type: MySQL
Server version: 5.7.12-0ubuntu1 - (Ubuntu)
Protocol version: 10
User: root@localhost
Server charset: UTF-8 Unicode (utf8)
Web server
Apache/2.4.18 (Ubuntu)
Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - $Id: f59eb767fe17a6679589$
PHP extension: mysqli
PHP version: 7.0.4-7ubuntu2.1
Console

Experiment 10: Fully accessed shared directory

(https://www.server-world.info/en/note?os=Ubuntu_16.04&p=samba&f=1)

Computer networks are often comprised of diverse systems, and while operating a network made up entirely of Ubuntu desktop and server computers would certainly be fun, some network environments must consist of both Ubuntu and Microsoft® Windows® systems working together in harmony.

Successfully networking your Ubuntu system with Windows clients involves providing and integrating with services common to Windows environments. Such services assist the sharing of data and information about the computers and users involved in the network, and may be classified under three major categories of functionality:

- File and Printer Sharing Services. Using the Server Message Block (SMB) protocol to facilitate the sharing of files, folders, volumes, and the sharing of printers throughout the network.
- Directory Services. Sharing vital information about the computers and users of the network with such technologies as the Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory®.
- Authentication and Access. Establishing the identity of a computer or user of the network and determining the information the computer or user is authorized to access using such principles and technologies as file permissions, group policies, and the Kerberos authentication service.

Install Samba to share folders or files between Windows and Linux.
For example, Create a fully accessed shared directory which anyone can access and write without authentication.

[1] Install Samba.

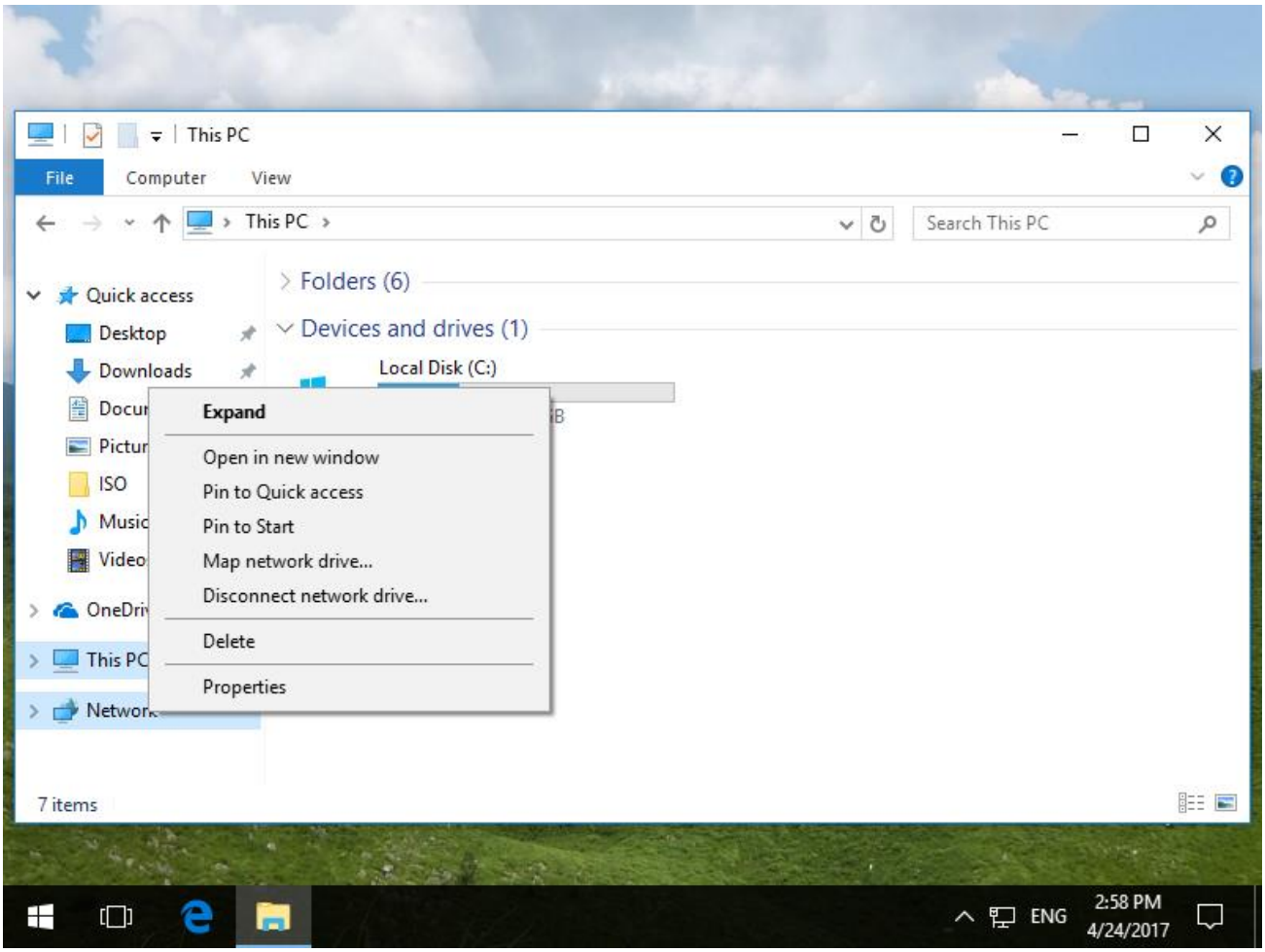
```
root@smb:~#
apt-get -y install samba
```

[2] Configure Samba.

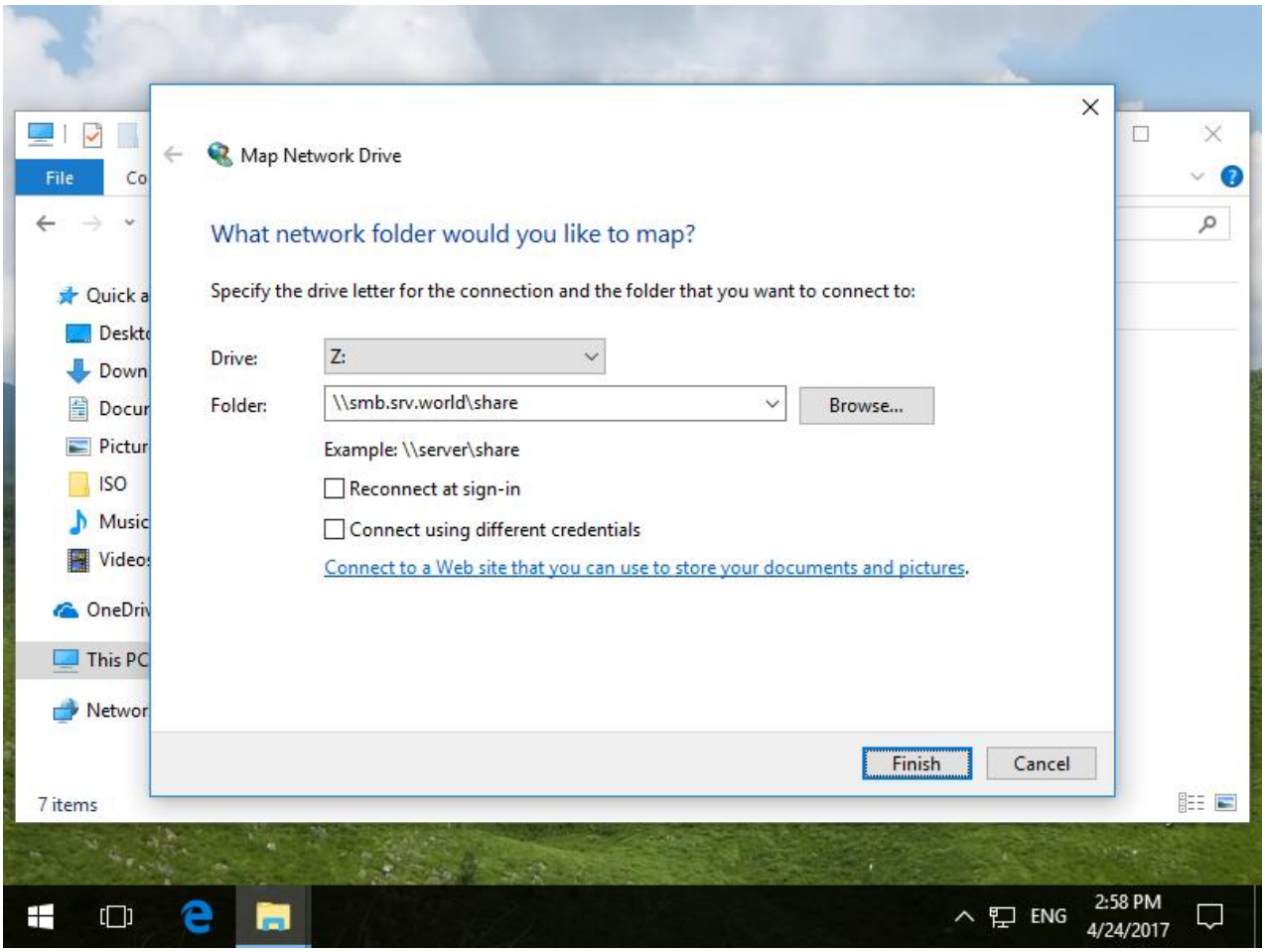
```
root@smb:~#
mkdir /home/share

root@smb:~#
chmod 777 /home/share

root@smb:~#
vi /etc/samba/smb.conf
# line 25: add

unix charset = UTF-8
# line 30: change (Windows' default)

workgroup =
WORKGROUP
# line 51: uncomment and change IP address you allow
```

```
interfaces = 127.0.0.0/8
10.0.0.0/24
# line 58: uncomment and add

bind interfaces only = yes
map to guest = Bad User
# add to the end

[Share]
# any name you like

   path = /home/share
# shared directory

   writable = yes
# writable

   guest ok = yes
# guest OK

   guest only = yes
# guest only

   create mode = 0777
# fully accessed

   directory mode = 0777
# fully accessed
root@smb:~#
systemctl restart smbd
```

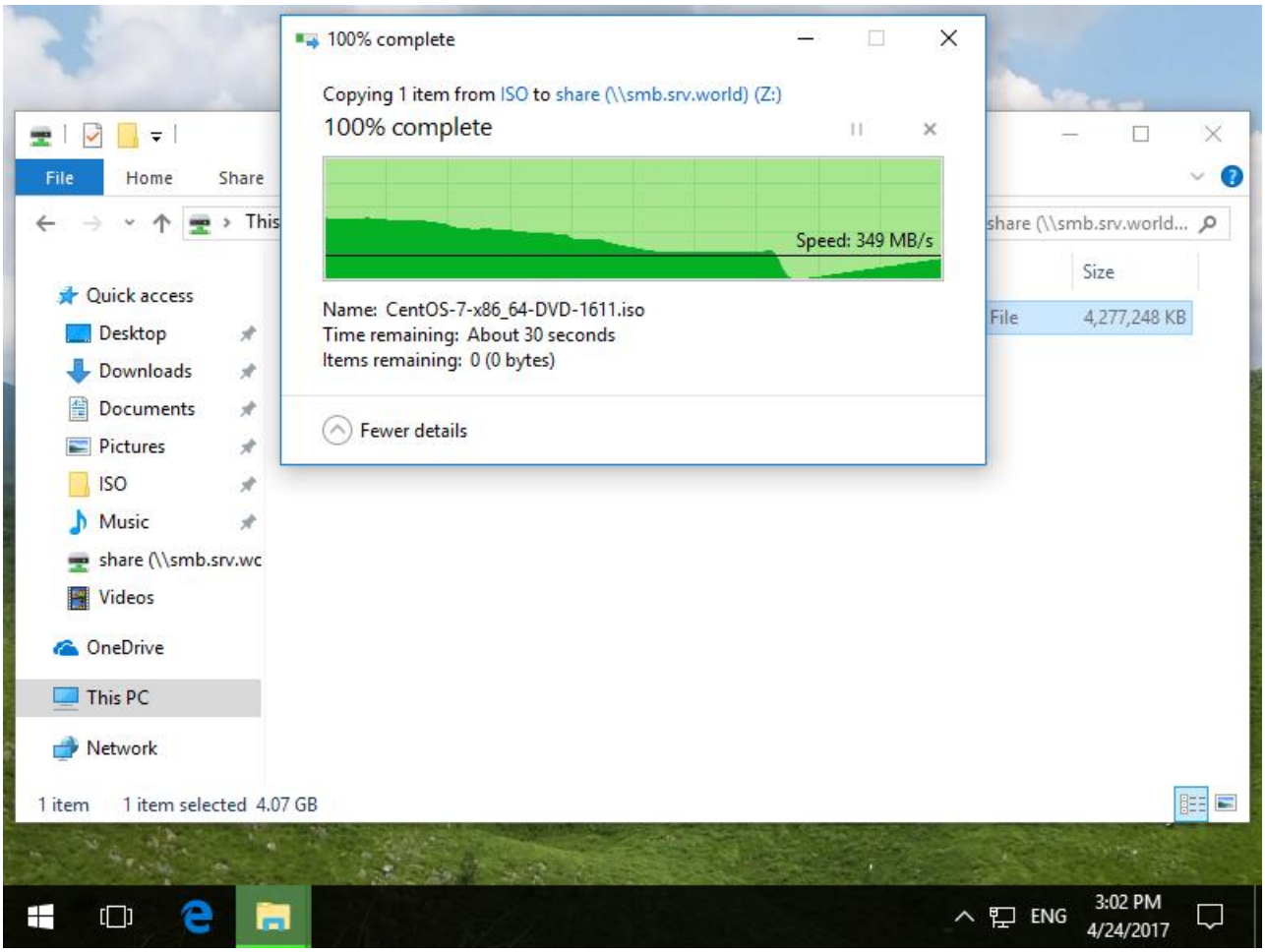
[3] Configure on Windows client. This example is on Windows 10.
Select [My Computer] - [Map Network Drive] like following example.



[5] Specify the shared folder's place in Folder section and Click the [Finish] button to enter.



[6] Just accessed to the shared Folder. smb.srv.world is hostname of Linux machine.



References:

1) Linux Administration: A Beginner's Guide, Wale Soyinka, Seventh Edition, McGraw-Hill Education, 2016
2) Ubuntu Server Guide, Ubuntu Documentation Team, 2016
3) https://www.server-world.info/en/note?os=Ubuntu_16.04&p=download