Labs Manual

LPIC-1: System Administrator

Verion: 5.0



*Author: Trung Nguyên Kbuôr*

**CONTENT**

|  |  |
| --- | --- |
| Lab 1: Installation Linux | 3 |
| Lab 2: System Architecture | 4 |
| Lab 3: Working on Command Line | 7 |
| Lab 4: Manage Share Libraries, Streaming edit and redirect | 12 |
| Lab 5: Working with file in linux | 14 |
| Lab 6: Package management | 16 |
| Lab 7: Process management | 18 |
| Lab 8: Disk management | 20 |
| Lab 9: Maintain the integrity of filesystems | 21 |
| Lab 10: User and Group | 22 |
| Lab 11: File Permission | 24 |
| Lab 12: Shell Scripts | 27 |
| Lab 13: Scheduling jobs | 29 |
| Lab 14: Networking Fundamentals | 30 |
| Lab 15: SSH | 34 |
| Lab 16: User Interfaces and Desktops | 38 |
| Lab 17: Essential System Services | 43 |
| Lab 18: Security | 47 |
| Lab 19: Configure IPv6 | 48 |

**Lab 1**

## Installation Linux

Objectives

* Installation Linux from local device
* Installation Linux from internet

### Task 1: Introduction this labs

* Introduction Lab topology
* Login this lab

### Task 2: Installation Linux Distro centOS 7.x

* Login this labs by remote desktop.
* Open VMware wordstation.
* Power ON the virtual machine Server-02.
* The VM auto boot CD-ROM include centOS 7 Operation System.
* Encrypt your data store in the server
* Layout disk such as below:
  + /swap: 1GB
  + /boot: 1GB
  + /home: 5 GB
  + /: all space capacity
* Set root password such as ‘student’.
* Now, wait the Linux installation and click **“Reboot”** after finish.

### Task 3: Installation Debian from internet

* Power ON the virtual machine Server-03 and process such as lecture module 1.

**Lab 2**

## System Architecture

### Task 1: Shutdown Linux

Perform this task on Server-01

* Shutdown the system after 1 minutes

# shutdown +1 “Test shutdown”

* Try command lines:

# init 0

# telinit 0

# shutdown now

### Task 2: Restart Linux

* Shutdown the system after 1 minutes

# shutdown –r +1 “Test shutdown”

* Try command lines:

# init 6

# telinit 6 # reboot

### Task 3: Check hardware on Linux

* List all hardware on CentOS:

# lshw

* List all pci on CentOS:

# lspci

* List all usb on CentOS:

# lsusb

* Check CPU info on linux:

# cat /proc/cpuinfo

* Check Memory info on linux:

# cat /proc/meminfo

### Task 4: Working with systemd init

Perform this task on Server-01

* Check the current runlevel:

# runlevel

* Check the default target:

# systemctl get-default

* To list all currently loaded target units, type the following command at a shell prompt:

# systemctl list-units --type target

What is current target? ………………………………………………………..

* Change default target to poweroff.target

# systemctl …………………………………………………………………………………………

* Reboot this server, waiting the server booting. What’s happened?
* Interrupt the boot loader when the menu appears by pressing any key.
* Move the selection to the default entry (the first one) using the cursor keys.
* Press **e** to edit the current entry.
* Move the cursor to the line that starts with **linux16**.
* Move the cursor to the end of the line (using the **End** key), and append the following text:

systemd.unit=rescue.target

* Press **Ctrl+x** to boot using the modified configuration.
* When prompted for the root password, enter “**student**”.
* Set the default systemd target back to the multi user target.
* Press **Ctrl+d** to continue booting into the (new) default target.
* Login and reboot for verify.

**Lab 3**

## Working on Command Line

### Task 1: Basic command line

Perform this task on Server-01

* What is current linux kernel in your system?
* Show content in file below, what is CentOS version?

# /etc/centos-release

* Check current time, date, timezone in your server.
* Set correct time, date, timezone.
* Set static hostname on server such as “server-01.robusta.local”
* Show first 20 line on /var/log/dmerg
* Show command history on this server
* Clear command history on this server
* Change current working directory to /tmp
* Run command:

# which mv

* Run command:

# ls

* Run command:

# alias ‘ls=ls -l’

* Run again command:

# ls

* What’s happened?

### Task 2: Working with directory and files

Perform this task on Server-01

* Create new directory **/LPI1**
* In the /LPI1 directory, create 03 sub-directory **lecture**, **lab**, **exam** by

### single mkdir command

* With single command, create the empty files with the file name **system\_changes-machineY-month\_Z.txt** in the **/LPI1** directory. Replace Y with the machine number (form 1 to 10) and replace Z with the months **jan, feb, and mar**. (Total create 30 empty file).
* With single command, Create the **/LPI1/syschanges** directory with the subdirectories **jan, feb,**and **mar.**
* Sort all newly created files by month into the corresponding subdirectory
* Compress /LPI1 to /tmp/lpi1.tar.gz
* Remove all newly created files related to machine 9 and 10
* Rename subdirectory **jan** to **Thang\_1**
* Rename all file in **Thang\_1** directory correct month is **Thang\_1**
* Remove directory **/LPI1/syschanges**
* With single command, create the directory tree below:

mywebsite

|

+ + +

| | | branches tags trunk

|

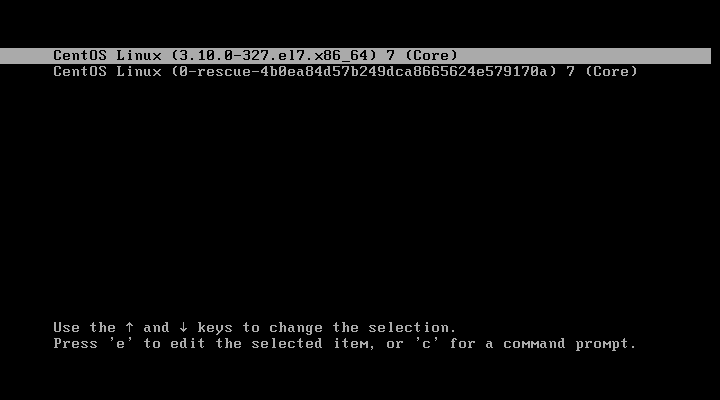
+ + +

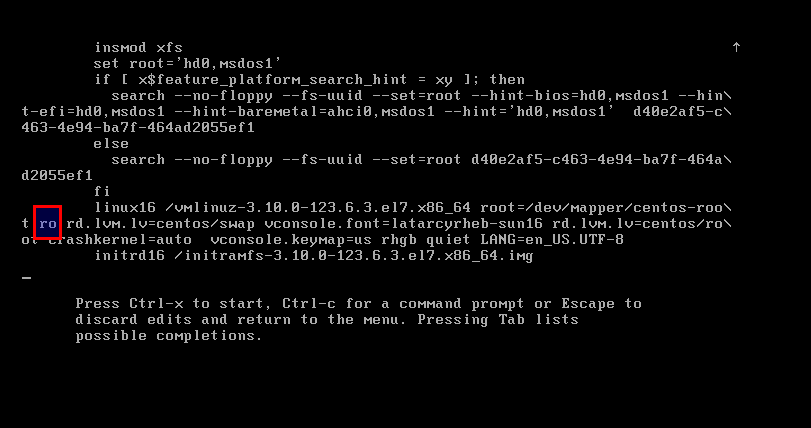
| | | cgi-bin htdocs scripts

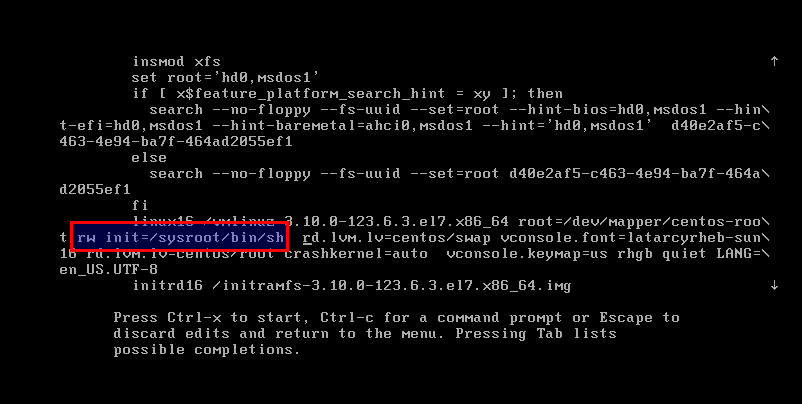
### Task 3: Forgot root password CentOS 7.x

Perform this task on Server-02

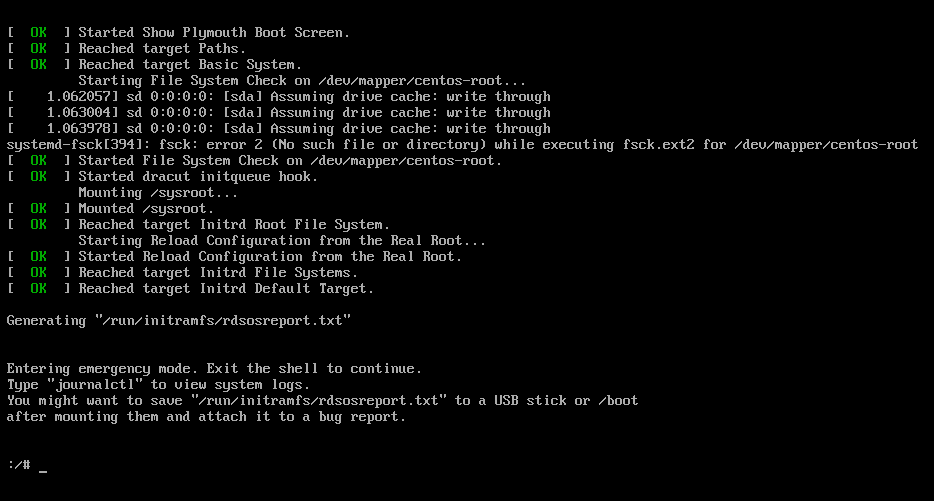
* Booting Server-02, press any key to access boot menu.
* In the boot menu, choose first row and press ‘e’



* The default such as:
* Change **ro** to **rw init=/sysroot/bin/sh** such as:



* Now press **Control+x** to start on single user mode



* Type command such as below:

# chroot /sysroot # passwd root

# touch /.autorelabel

* Reboot VM and verify with new password

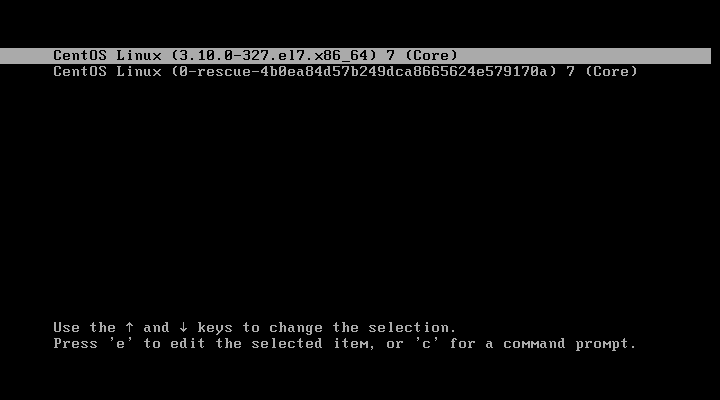
### Task 4: Set password for Grub Boot Loader 2 on CentOS 7.x

Perform this task on Server-02

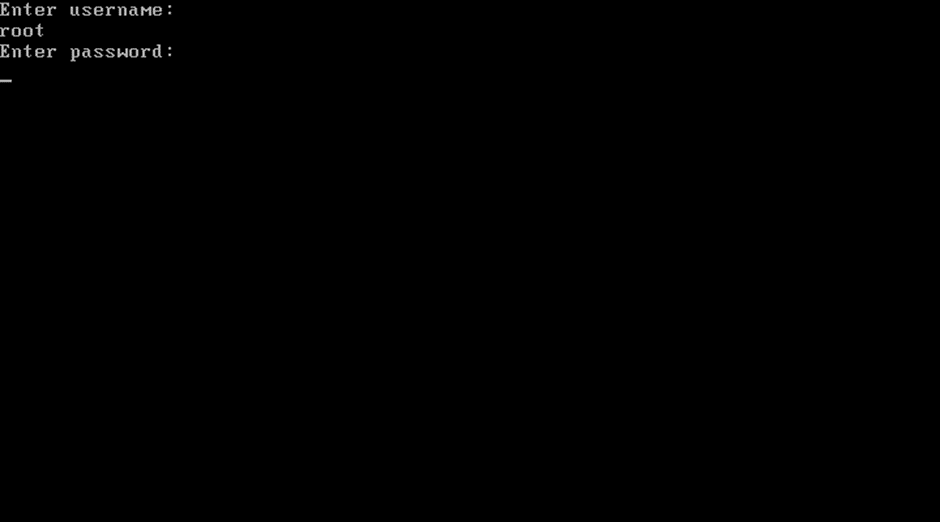
* Set password for user root of Grub Boot Loader 2

# grub2-setpassword

* Reboot OS
* Booting VM02-CentOS-7.x, press any key to access boot menu.
* In the boot menu, choose first row and press ‘e’



* The console require enter username and password:



**Lab 4**

## Manage Share Libraries, Streaming edit and redirect

### Task 1: Manage shared libraries

Perform this task on Server-01

* Display current locations for modules for a particular user and program:

# ldconfig -p

* To find the shared libraries that a calendar program (/usr/bin/cal):

# /usr/bin/cal

* To set the environment variable for developers, first make a directory in your home directory

# mkdir $HOME/libs

* Set the variable

# LD\_LIBRARY\_PATH=$HOME/libs

* Export the variable

# export LD\_LIBRARY\_PATH

* Check that it is exported

# env

* To set this permanently edit /etc/profile or ~/.bash\_profile. Now unset the variable

# unset LD\_LIBRARY\_PATH

### Task 2: Streaming edit and redirect

Perform this task on Server-01

* Run this command:

# echo redhat | passwd --stdin root

* Logout and login again verify
* Change password to ‘student’
* Copy first 10 lines in **/etc/passwd** to **/tmp/task2\_lab4.txt**
* Export column 1 of file **/tmp/task2\_lab4.txt** to **/tmp/1.txt**
* Export column 2 of file **/tmp/task2\_lab4.txt** to /**tmp/2.txt**
* Export column 6 of file **/tmp/task2\_lab4.txt to /tmp/6.txt**
* Print to console and store in to **/tmp/cut.txt** with column 1,2,6 of file

**/tmp/task2\_lab4.txt**, column separate by ‘:’

* Using paste command, merge 3 file /**tmp/1.txt, /tmp/2.txt** and

### /tmp/6.txt to /tmp/paste.txt

* Compare 02 file with command:

# diff -q /tmp/paste.txt /tmp/cut.txt # diff -s /tmp/paste.txt /tmp/cut.txt

* Using paste comand, create new file paste2.txt with paste2.txt and cut.txt are identical
* Create new empty file **~/demo.txt.**
* Add context such as below to **~/demo.txt** file:

Linux is Unix Unix not linux liNux like uNix

* Add 3 black line after every line and save overwrite name **~/demo.txt**
* With sed command, replace all like to “**linux**” – not match case in

**~/demo.txt** to LINUX (ex: LiNUx, linuX -> LINUX)

* With sed command, replace all like to “**unix**” – not match case in

### ~/demo.txt to [UNI]x

* Delete all black line.
* Convert all character on file ~/demo.txt to UPPER CASE.
* Process all example command in Module 3 - Lesson 3

**Lab 5**

## Working with file in linux

### Task 1: Edit file with vi command

Perform this task on Server-01

* Edit file **~/.vimrc** and adding:

set number

* Use **vi** command, create new file **/tmp/truyenkieu.txt** with contents below:

Dau long hai a to nga

Thuy Kieu la chi em la Thuy Van Mai cot cach, tuyet tinh than

Moi nguoi mot ve muoi phan ven muoi

* Use vi command, delete line 3.
* Use vi command, replace all **Thuy** to **Thu'y**

### Task 2: grep and egrep

Perform this task on Server-01

* Copy file **/etc/ssh/sshd\_config** to **/tmp/**
* Add to end of line **/tmp/sshd\_config**:

Dong nao bat dau bang dau # co nghia la ghi chu

* Show all lines on **/tmp/sshd\_config** without notes line.
* Use **egrep** command, print to console total CPU support virtualization on linux. If you see **vmx** or **svm** in the core information on **/proc/cpuinfo**, then your hardware (CPU) supports the virtualization.

### Task 3: Managing links between files/directory

Perform this task on Server-01

* With single command, create new file **~/newfile.txt** has content:
* Create soft link **~/newfile.txt** to **/tmp/softlinknewfile**.**abc**
* Using **ls** command verify softlink.
* Create new hardlink **~/newfile.txt** to /**hardlink.doc**
* Using **vi** command, add everything to **~/newfile.txt**
* Using **cat** and **diff** command verify/compare contents on softlink and hardlink.
* Using **vi** command, add everything to **/tmp/softlinknewfile.abc**
* Using **cat** and **diff** command verify/compare contents on orginal file and hardlink.
* Using **vi** command, add everything to /hardlink.doc
* Using **cat** and **diff** command verify/compare contents on orginal file and softlink.
* Remove **/tmp/softlinknewfile**.**abc**, verify **~/newfile.txt and**

### /hardlink.doc

* Create again softlink
* **Delete file ~/newfile.txt,** verify softlink and hardlink file, content on file.
* Create /**tmp/test** directory and 10 file {**1..10}.txt** into this.
* Create **/source** directory and copy random 5 files .**tx**t form /**tmp**/**test**/ with command below:

# cd /tmp/test

# shuf -zn5 -e \*.txt | xargs -0 cp -vt /source/

* Create symbolic link of /**source**.
* Create hard link of /source -> result?

**Lab 6**

## Package management

### Task 1: Mount CD-ROM ISO CentOS

*Perform this task on Server-02*

* Insert CentOS CD to Server from VMware Workstation.
* Create folder **/mnt/cdrom**
* Mount CD-ROM to mount point:

# mount …………<path/to/cdrom> /mnt/cdrom

* Change directory to Package folder:

# cd /mnt/cdrom/Packages/

### Task 2: Using RPM command

* List all rpm package install on system:

# rpm –qa

* Install package tcpdump on system:

# rpm –ivh tcpdump-………rpm

* If have requirement package, install the requirement package before install tcpdump package.

-

### Task 3: Install Repository Local

*Perform this task on Server-02*

### Step 1: Install package create Repository

* Package called **“createrepo”** to create our local repository.

Using rpm command line install package createrepo-xxx.rpm (need install another package requirement)

### Step 2: Create source repository

* Create folder for repository:

[root@localhost ~]# mkdir /localrepo

* Copy all packages of CentOS to **/localrepo** directory:

### Step 3: Create file config repo

Create and edit file localrepo.repo:

vi /etc/yum.repos.d/localrepo.repo

Add contents:

[localrepo] name=……………………………………………………………………

baseurl=……………………………………………………………

gpgcheck=0 enabled=1

### Step 4: Active repository

# createrepo -v /localrepo/

**Task 4: Using yum command On Server-02:**

* Clean all cache:

# yum clean all

* Install service:

# yum –disablerepo=“\*” –enablerepo=“localrepo” install httpd\*

### On Server-01:

* Type command:

# tree

* Install epel repository:

# wget <http://dl.fedoraproject.org/pub/epel/epel-release-latest-> 7.noarch.rpm

# rpm -ivh epel-release-latest-7.noarch.rpm

* Use yum command verify epel repo id.
* Install package tree:

# yum install -y tree

**Lab 7**

# Process management

### Task 1: Manage processes

*Perform this task on Server-02*

* Check the system uptime with uptime command.
* Check the usage memory and swap on your system
* Run command below:

# find / -ctime -1 > /tmp/changed-file-list.txt

* Press Ctrl-Z to suppend forceground command

# [CTRL-Z]

[2]+ Stopped

find / -ctime -1 > /tmp/changed-file-list.txt

* Run all command such as below:

# NCORES=4

* Create more background processes:

# for I in $( seq $((NCORES\*2)) )

* do
* sha1sum /dev/zero &
* done
* Inspect the CPU usage (as a percentage) of all your sha1sum processes, using the **ps** and **pgrep** commands. What do you notice?

# ps -o pid,pcpu,nice,comm $(pgrep sha1sum)

* Use the killall command to terminate all your sha1sum processes.

### Task 2: Use the screen tool

*Perform this task on Server-02*

* Install screen package.
* Create new screen with session name LPI1
* After connect to screen session, using command:

# vi /tmp/testscreen.txt

* Type any contents.
* Dettach this screen (not terminate)
* Create second screen
* Connect to second screen, and show all contents into file /etc/hosts
* Dettach second screen
* List al screen on your system.
* Re-attach first screen and save this open file.
* Terninate all screen.
* Set password for screen with password like ‘123456’

### Task 3: Manage priority of the processes

* Run all command such as below:

# NCORES=2

* Create more background processes:

# for I in $( seq $((NCORES\*2-1)) )

* do
* sha1sum /dev/zero &
* done
* Start new **sha1sum /dev/zero** with nice level 10.
* Using the ps command, inspect the CPU usage of your sha1sum commands.
* Use the renice command to set the nice level of the sha1sum with a nice level of 10 down to -10.
* Identify the sha1sum process using the most CPU. It will be near the top.
* In top command, press **‘r’,** then enter the PID of sha1sum command with nice level of -10 and enter 0, then press Enter.

**Lab 8**

# Disk management

### Task 1: Working with fdisk command

*Perform this task on Server-01*

* On first SCSI hard disk, create 03 new partitions with capacity 2GB (new partition 1st), 2GB (new partition 2nd) with fdisk command and 2GB (new partition 3rd).
* Format new partition 2nd to ext2 file system and mount to **/ext2**
* Format new partition 3rd to ext4 file system and mount to **/ext4**
* Edit /etc/fstab and configure auto mount new partition 2 to /ext2 and new partition 3 to /ext4 when system startup. After that, reboot system for verify.

### Task 2: Swap

*Perform this task on Server-01*

* Create swap form new partition 1 (created task above).
* Turn on new swap and verify.
* Set auto mount swap partition when system startup and verify.
* Create new directory /swap
* Change directory to /swap
* Create a file /swap/swapfile has file size=1GB (using dd command)
* Type command:

# chmod 600 /swap/swapfile

* Create swap from /swap/swapfile.
* Turn on new swap and verify.
* Set auto mount swap partition when system startup and verify.

### Task 3: Working with parted command

*Perform this task on Server-02*

* Add new disk form VMware Workstation with 10GB capacity to Server-02.
* Use **partprobe** command re-load new hard disk.
* Set partition table for new hard disk such as GPT.
* Create new partition with 5GB.
* Format new partition such as xfs and mount to **/xfs**

**Lab 9**

# Maintain the integrity of filesystems

* On Server-01, convert partition /dev/sda6 with ext4 file systems.
* On Server-01, Copy 3 files (random) on /var/log to /ext4
* On Server-01, Extend /dev/sda7 to 8GB and verify current data.
* On Server-01, reduce /dev/sda7 to 6GB and verify current data.
* On Server-01, Delete 3 partition /dev/sda5, /dev/sda6
* On Server-02, Copy 3 files (random) on /var/log to /xfs
* On Server-02, Extend /dev/sdb1 to 10GB and verify current data.
* On Server-02, how to reduce /dev/sdb1 to 6GB???

**Lab 10**

# User and Group

### Task 1: Manage Local User and Group

*Perform this task on Server-01*

* Adding 2 directories backup and document into /etc/skel. After that, directory Adding file welcome.txt in /etc/skel/document such as below:

# cat welcome.txt

Chao mung ban den voi LPI

Moi chi tiet lien he voi administrator

* Create new 3 user: **tom, jessica, steven** have default group is **quota**.
* Verify file/directory in home directory of **tom, jessica, steven** user’s.
* Set password ‘redhat’ for 3 users: **tom, jessica, steven**
* Create user **putin** without logon to your system and verify.
* Change home directory of **steven** to **/ftp/data/steven**
* Edit file /etc/motd such as:

# cat /etc/motd

Chao mung ban den voi may chu cua toi

* Using **vi**, change uid in **/etc/passwd** file of **tom** user to 0. Reboot server and login with **tom** user and password is **redhat**.
* Configure **jessica** user require change password next logon.
* Modify user putin can logon to your system.
* General password hv03 such as:

# matkhau=$(openssl rand -base64 12) # echo $matkhau

# usermod –p $matkhau putin

* What is password of user **putin**?
* Logout current user and login with **putin** user.
* Check current time on your system.
* Change **mindays** of tom user is 3 days.
* Try change password of **tom** user? What happened?
* Set current date such as 4 days after and try change password **tom** user again. What happened?

### Task 2: Configure sudoers

*Perform this task on Server-01*

* Configure user **tom** has full privileges such as **root**, without password when use sudo command.
* Configure user **putin** can shutdown your system.

### Task 3: Configure quota

*Perform this task on Server-01*

* Check /dev/sda7 mounted to /ext4 directory.
* Check package create quota (quota-xxx.rpm). If it didn’t install, you can install such as (mount cdrom and install):

# rpm –ivh tcp\_warppers-7.xxx.rpm # rpm –ivh quota-xxx.rpm

* Configure quotas: user tom: 10MB, putin: 100MB on /dev/sda7
* Verify with dd command

**Lab 11**

# File Permission

### Task 1: Basic permision on Linux

*Perform this task on Server-01*

* Create user **hv01**, **hv02** member of **hocvien** group.
* Create user **hv03** member of **lpi** group
* Change password **hv01, hv02, hv03**
* Switch to user **hv01** and create file **/home/hv01/test.txt** with whatever contents.
* Switch to user **hv02**, and check such as:

$ cat /home/hv01/test.txt

$ cd /home/hv01

$ ls –l /home/hv01

$ mkdir /home/hv01/hv02

$ mkdir /home/hv02/lpi

* Switch to user **root**
* Create folder **/public**, sub-folder **/public/limit**
* Create 3 files **read.txt, write.txt, nonpermission.txt** in **/public**

folder with whatever contents.

* Create 2 files **hv01**.**txt** and **hv02**.**txt** in /**pub/limit.**
* What is permission, owner of new file/**folder**?
* Switch user to hv01 and check with command:

$ ls –l /public

$ ls –l /public/limit

$ cat /public/read.txt

$ vi /public/write.txt

Add another line and save

$ vi /public/limit/hv02.txt Add another line and save

$ cat /public/limit/hv01.txt

* Exit and back to root user
* Set permission of folder **/public/limit** is **740** and check with ls command
* Set owner of folder **/public/limit** is root and group is **hocvien**.
* Set permission of file **/public/read.txt** is 764
* Set permission of file **/public/write.txt** is 762
* Set permission of file **/public/nonpermision.txt** is 700
* Switch user to **hv01** and check:
  + List all file/directory in **/public**
  + List all file/directory in **/public/limit**
  + View contents of file **/public/limit/hv02.txt**
  + Add new line in **/public/limit/hv01.txt**
  + View contents of file **/public/read.txt**, **/public/write.txt**,

### /public/nonpermission.txt

* + Add new line in **/public/read.txt, /public/write.txt,**

### /public/nonpermission.txt

* + Exit and back to root and check command:
    - cat /**public/write.txt**
* Switch user to **hv03** and check:
  + List all file/directory in **/public**
  + List all file/directory in **/public/limit**
  + View contents of file **/public/limit/hv02.txt**
  + View contents of file **/public/read.txt**, **/public/write.txt**,

### /public/nonpermission.txt

* + Add new line in **/public/read.txt, /public/write.txt,**

### /public/nonpermission.txt

* + Exit and back to root and check command:
* cat /**public/write.txt**
* Set all folder and files in directory /public with permission of owner is read and write, group is read-only and others is non-permission.

-

* Change owner and group of **/public** directory is **hv01:hocvien**
* Set sticky bit for **/public** directory.
* Switch user to **hv03**
* Create file **test.txt** with whatever contents.
* Create folder **test.d**
* Delete file **test.txt** and **read.txt**

### Task 2: Special permision on Linux

*Perform this task on Server-01*

* Create and adding user **tom, jessica, steven** to group **accountant**
* In the **/test\_permission,** create new directory **Finances**
* Configure all new file, directory create into

**/test\_permission/Finances** all users is member of accountant group have read and write, other user cannot access into this. Only owner create this file should be delete this.

* Login tom, jessica, steven and putin user for verify.

### Task 3: Umask

*Perform this task on Server-01*

* By **root** user, set umask for user **putin** and **jessica** such as 0007
* Login to **putin** user and **jessica** verify by umask command and create and check permission to new file and new directory.
* Login to user tom and check umask, create new fil/directory and check this permission.

**Lab 12**

# Shell Scripts

* Create file **/bin/sysadmin** such as bash script, when run, main console show such as below:

[root@lpi1 ~]# **sysadmin**

1. Tao tai khoan
2. Health check
3. Shutdown
4. Reboot

5) Quit

Vui long chon chuc nang - Nhan Enter de xem lai bang chuc nang:

* When press 1:

Nhap username=

* If not type username or type incorrect username, require retype user.
* If type correct username, check the existed ussername. If not existed, create new username.
* Change password username such as:

Nhap username= abc123

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Tao tai khoan abc123 thanh cong!!!

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Ban muon dat mat khau cho user abc123? y Dat mat khau manual hay random?

1. manual
2. random

Vui long chon chuc nang - Nhan Enter de xem lai bang chuc nang:

Vui long chon chuc nang - Nhan Enter de xem lai bang chuc nang: 2 Mat khau ngau nhien la: w0kKuXp0gsM=

Changing password for user abc123.

passwd: all authentication tokens updated successfully. Dat mat khau thanh cong

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Set tai khoan abc123 muon quyen root: y

Set tai khoan abc123 co quyen root thanh cong. Su dung sudo truoc command de muon quyen

Press any key to continue

* When press 2:

\*\*\*\*\*\*\*\*\*\*\*\*\*\* HEATH CHECK SYSTEM \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

May chu: lpi1.trungnguyenkbuor.com

He dieu hanh: CentOS Linux release 7.2.1511 (Core) Thong tin kernel: 3.10.0-327.el7.x86\_64

Thong tin uptime: 21:48:09 up 2:08, 2 users, load average: 0.00, 0.01, 0.05 CPU: Intel(R) Core(TM) i5-4300U CPU @ 1.90GHz

So Core CPU: 2

Press any key to continue

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Thong | tin | Memory:  total | used | free | shared | buff/cache | available |
| Mem: |  | 1824 | 141 | 1376 | 8 | 306 | 1513 |
| Swap: |  | 2047 | 0 | 2047 |  |  |  |

* When press 3:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Ban muon shutdown he thong? Go 'Yes' de shutdown:

* When press 4:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Ban muon khoi dong lai he thong? Go 'Yes' de khoi dong lai:

* When press 5:

Vui long chon chuc nang - Nhan Enter de xem lai bang chuc nang: 5 Ban co muon thoat chuong trinh? y

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

HAVE A NICE DAY

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* [root@lpi1 ~]#

* For Press any key to continue, use such as below:

read -n 1 -s -r -p "Press any key to continue"

**Lab 13**

# Scheduling jobs

### Task 1: Working with crontab

* Create crontab every 2 minutes write current time to file

### /etc/timestamp.log

* Using **tail -f** for verity.
* Check current time on system.
* Create crontab reboot your system at 01:15am every Saturday.
* Set time to **20/4/2019 01:14** and verify.

### Task 2: Working with nohup

* Create 02 directories /**tmp/source** and **/tmp/backup**
* Create script auto cp all data into /**tmp/source** to **/tmp/backup** every 30 seconds.
* Touch 3 files (random) in /**tmp/source** and verify.

**Lab 14**

# Networking Fundamentals

### Task 1: Configure IP on server-01

* On Server-01, configure IP by edit file in /etc/sysconfigs/network-scripts with IP address is 172.20.10.11/24 and gateway is 172.20.10.2
* Configure Server can access internet with DNS is 8.8.8.8.

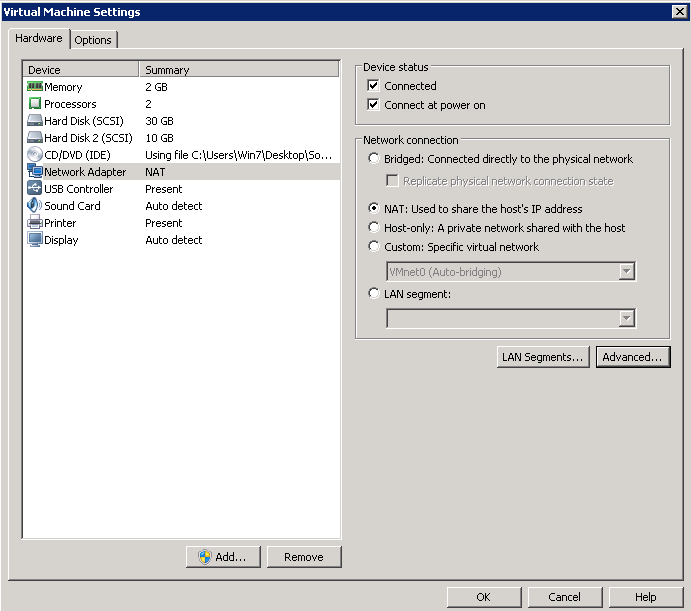
### Task 2: Configure IP on server-02

* On Server-02, configure IP by edit file in /etc/sysconfigs/network-scripts with IP address is 172.20.10.12/24 and gateway is 172.16.0.2
* Configure Server can access internet with DNS is 8.8.8.8

### Task 3: Basic troubleshooting

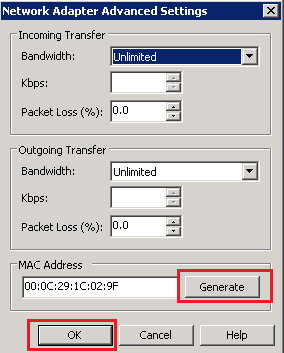
**Change MAC address of network on Server-02**

* Right click in the Virtual Machine and select “Settings…”
* Choose Network Adapter and select “Advande…”



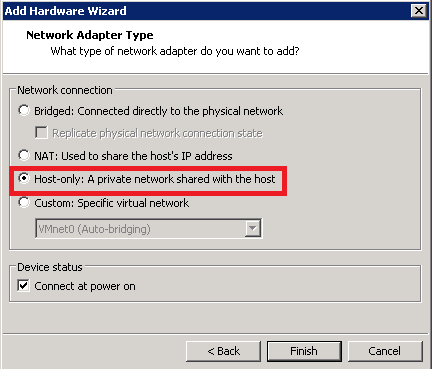
-

* Click Genaral:

-

* Final, Click OK.

Return cosole of VM and check network.

* On Server-01, add new network interface such as:

Config IP of new interface: IP: 192.168.100.10

NETMASK: 255.255.255.0

GATEWAY: 192.168.100.2

Restart network service. Check network:

# ip a

# ping robusta.vn

Check route:

# ip route

### Task 4: Configure NFS Client

Connect to //192.168.1.51 and copy file storage.rar to you PC. Extract this file.

Add Virtual machine to vmware workstation, power on (I moved it).

***Mount NFS***

Install package nfs client (On both server-01 and Server-02):

# yum install nfs-utils **-y**

Set domain of server, edit file /etc/idmapd.conf:

Domain = robusta.local

Start service and add service startup when boot:

# systemctl start rpcbind

# systemctl enable rpcbind

Mount NFS:

Create new folder: On server-01:

# mkdir /nfs

# mount -t nfs 172.20.10.100:/mnt/lpi/share/server-01/ /nfs

On server-02:

# mkdir /nfs

# mount -t nfs 172.20.10.100:/mnt/lpi/share/server-02/ /nfs

***Config fstab, open and edit file /etc/fstab:***

# add like follows 172.20.10.100:/mnt/lpi/share/server-01/ nfs defaults 0 0

***Reset and virify***

# reboot # df –HT

### Task 5: Configure iSCSI Client

Install package:

# yum -y install iscsi-initiator-utils

Discovery target and LUN mapping:

# iscsiadm --mode discovery -t sendtargets --portal 172.20.10.100

Retart service and login to target:

# systemctl restart iscsid.service # systemctl enable iscsid.service # iscsiadm -m node --login

Check new disk:

# fdisk –l

**Lab 15**

# SSH

### Task 1: Configure SSH Server

* *On Server-01,* disable user root login from ssh:

# vi /etc/ssh/sshd\_config PermitRootLogin no PermitEmptyPasswords no PasswordAuthentication yes

Restart ssh service and verify.

After that, change **PermitRootLogin yes** and process all tasks below.

### Task 2: SSH Client on Linux

* Install package ssh client on 02 server:

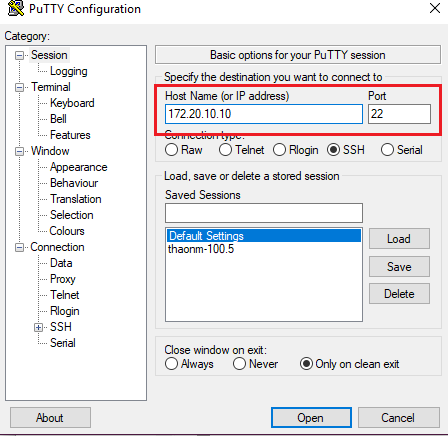
# yum -y install openssh-clients

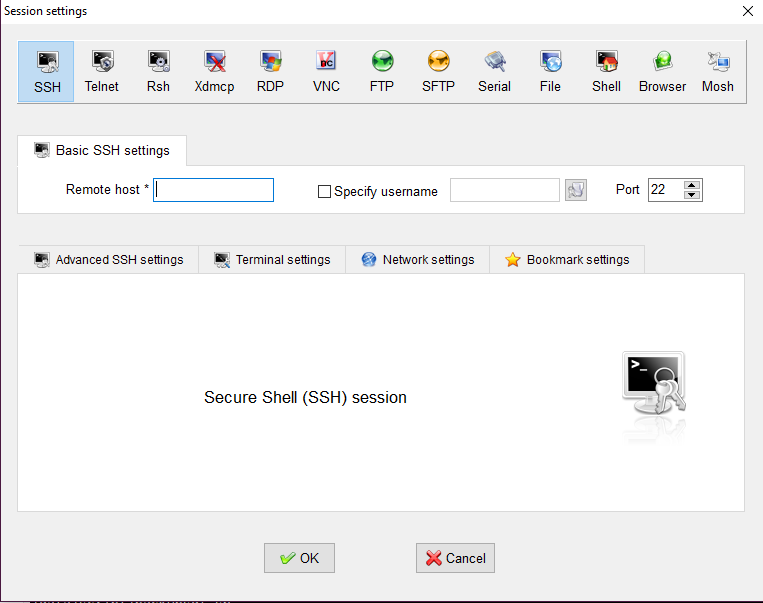
*On Server-02:*

# ssh [root@172.20.10.10](mailto:root@172.20.10.10)

### Task 3: SSH Client on Windows

Using putty:



Using MobaXterm Personal:

### Task 5: Copy using SSH

* On Server-01, create file test.txt:

# vi /root/test.txt Day la file test

* On Server-01, transfer file test.txt to Server-02 using scp command:

# scp ………………………………………………………………………………………………………………

### Task 7: SFTP

* On Server-02:

Create folder /demo and file demoupload.txt:

# mkdir /demo

# vi /demo/demoupload.txt

Day la file demo upload sftp

Using SFTP client on Linux:

# sftp [root@172.20.10.10](mailto:root@172.20.10.10)

**# show current**

sftp> pwd Remote working

**directory on remote server**

directory: <path>

**# show current directory on local server**

sftp> !pwd

**# show files in current directory on FTP server**

sftp> ls –l

**# show files in current directory on local server**

sftp> !ls -l

**# upload a file to remote server**

sftp> put /demo/demoupload.txt uploadfile.txt

**download some files from remote server**

sftp> get uploadfile.txt

**#exit sftp**

sftp> exit

### Task 6: SSH Keys Authentication

* Working this task with Server-01 such as SSH Server and Server-02 such as SSH Client.
* Create SSH key on SSH Client:

# **ssh-keygen –t rsa**

Generatingpublic/private rsa key pair.

Enter file in which to save the key (/root/.ssh/id\_rsa): # Enter Created directory '/root/.ssh'.

Enter passphrase (empty for no passphrase): # set passphrase (set no passphrase to Enter with empty)

Enter same passphrase again:

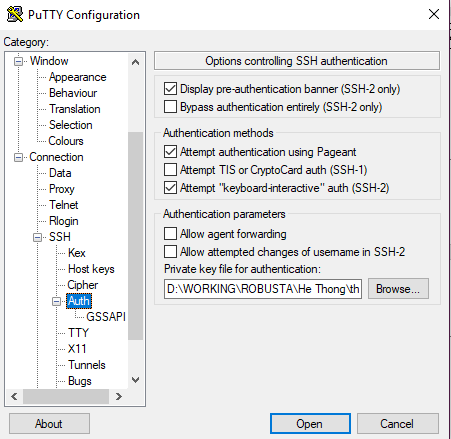
Your identification has been saved in /root/.ssh/id\_rsa. Your public key has been saved in /root/.ssh/id\_rsa.pub. The key fingerprint is: 38:f1:b4:6d:d3:0e:59:c8:fa:1d:1d:48:86:f0:fe:74

[root@trungnguyenkbuor.local](mailto:root@thaonm.local)

The key's randomart image is:

* Move private key correct file into home directory of user root and set permission for security.
* Transfer public key to SSH Server.
* Configure SSH using key authentication
* Reset SSH service and verify.

Using RSA key on Windows with putty:



**Lab 16**

# User Interfaces and Desktops

### Task 1: Use X11 on Linux

* Perform this task on Server-01
* Install X11 such as below:

# yum install xorg-x11-server-Xorg xorg-x11-xauth xorg- x11-apps xterm -y

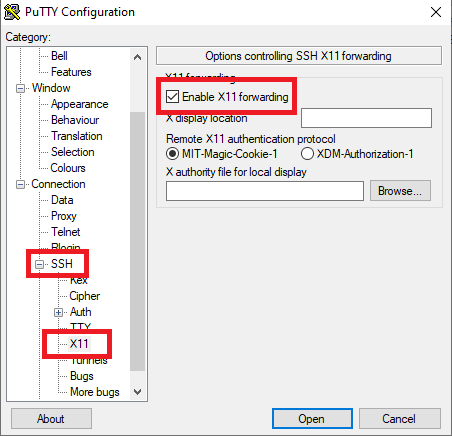
* Using putty, connect to Server-01 by SSH.
* Use command:

# xclock & # xeyes &

# xterm &

* Enable SSH allow X11 (restart ssh service after edited):

X11Forwarding yes X11DisplayOffset 10 X11UseLocalhost no

* On windows 7, download and install Xming: <https://sourceforge.net/projects/xming/>
* Using putty, connect to Server-01 by SSH with X11 enable:
* Use command:

# xclock & # xeyes &

# xterm &

### Task 2: GNOME desktop

* Install GNOME with yum, you can login with console:

# yum -y groups install "GNOME Desktop"

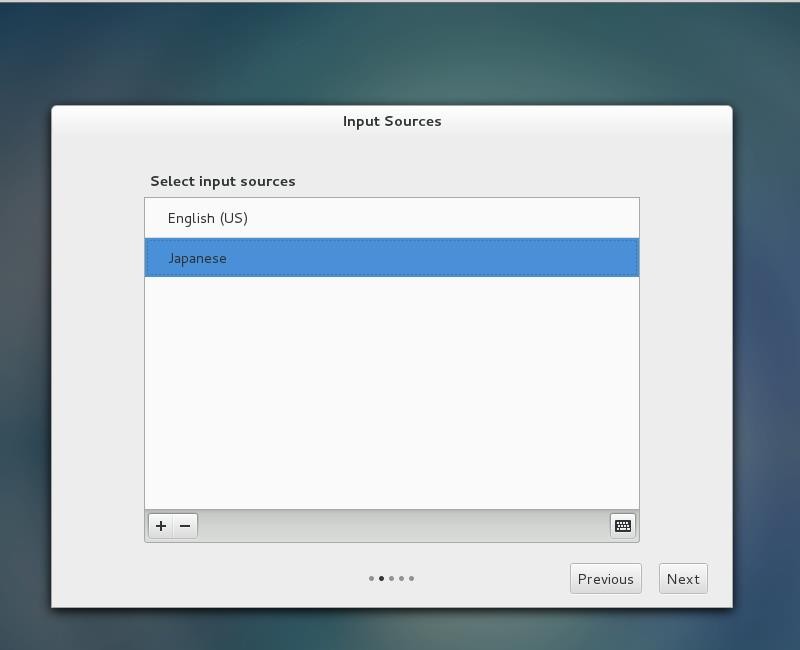
* Start GNOME Desktop:

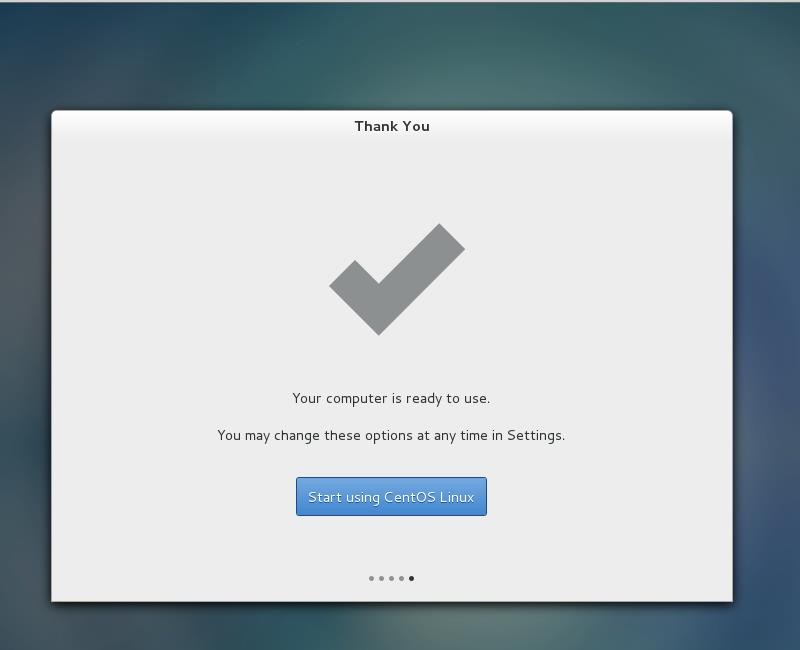
# startx

* GNOME Desktop Environment starts. For first booting, initial setup runs like follows. Select System language first.



* Select your keyboard type.



* Add online accounts if you'd like to. You can skip this step.
* Configuration finished and click "Start using CentOS Linux".
* Reboot system. What the target using after boot?
* Set default target is GUI. Reboot server and verify.

### Task 3: KDE desktop

* Perform this task on Server-02
* Installation of KDE desktop environment:

# yum groupinstall "KDE Plasma Workspaces" "X Window System"

* Update default target

# systemctl set-default graphical.target

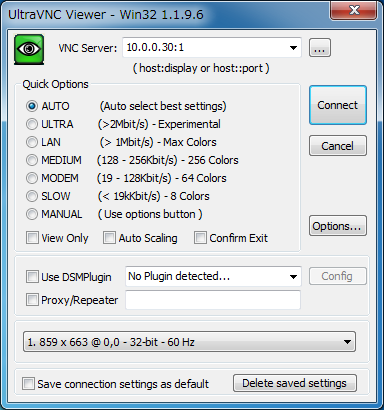
* All done. Reboot your system, accept license, verify and compare with GNOME

### Task 4: Remote desktop with VNC

* Perform this task on Server-01
* Install VNC server with tigervnc.
* Create new user remote01 grant all root privileges.
* Create VNC remote for root and remote01 user.
* Disable firewall such as below:

# systemctl stop firewalld

# systemctl disable firewalld

* Install VNC viewer on Windows 7 Remote desktop to Lab. Download from the site below to install UltraVNC. <http://www.uvnc.com/downloads/ultravnc.html>

### Task 5: Remote desktop with xrdp

* Perform this task on Server-01, require tigervnc install on server.
* Install epel repository:

# rpm -Uvh [https://dl.fedoraproject.org/pub/epel/epel-](https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm) [release-latest-7.noarch.rpm](https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm)

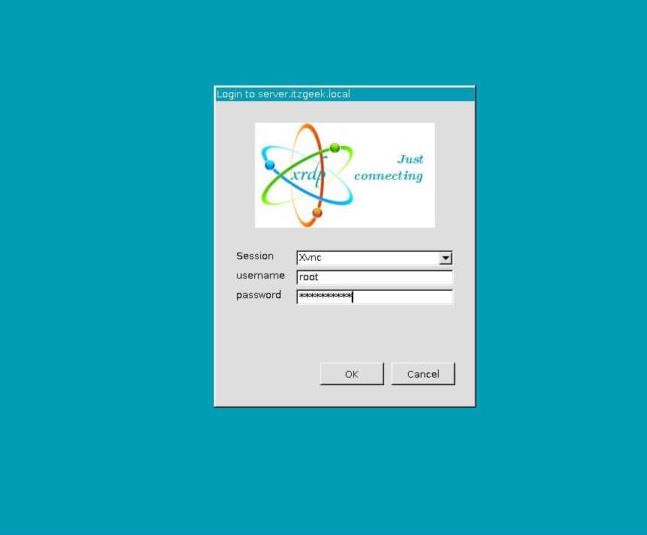
* Install xrdp with yum:

# yum -y install xrdp

* Start xrdp service:

# systemctl start xrdp.service # systemctl enable xrdp.service

* From Windows 7 of Remote desktop, using remote desktop client (mstsc) connect to CentOS Server.



**Lab 17**

# Essential System Services

### Task 1: Maintenance system time

* Check current hardware clock and content on /etc/adjtime.
* Change harware clock:

# hwclock set date="10/14/2010 16:55:05" # hwclock show

* Check agent current hardware clock and content on /etc/adjtime.
* Install chrony package on both 02 server.
* Configure Server-01 such as Network Time Server.
* Configure Server-02 such as NTP client.
* Change time/date on both 02 server and verify NTP working.

### Task 2: System logging

* Overview:

|  |  |  |
| --- | --- | --- |
| SERVER-02 |  | SERVER-01 |
|  |

Log client

* Install rsyslog:

Log Server

# yum -y install rsyslog

* Configure Log Managed Server to receive logs from client servers. On Server-01, edit file **/etc/rsyslog.conf**:

# uncomment such as below:

# Provides UDP syslog reception

$ModLoad imudp

$UDPServerRun 514

# Provides TCP syslog reception

$ModLoad imtcp

$InputTCPServerRun 514

* Start rsyslog service:

# systemctl start rsyslog.service

* Verify the syslog server listening.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # netstat | -antup | grep | 514 |  | |
| tcp 0 | 0 0.0.0.0:514 | 0.0.0.0:\* | LISTEN | 759/rsyslogd |
| tcp6 0  udp 0  udp6 0 | 0 :::514  0 0.0.0.0:514  0 :::514 | :::\*  0.0.0.0:\*  :::\* | LISTEN | 759/rsyslogd  759/rsyslogd 759/rsyslogd |

* Install rsyslog on Server-01:

# yum -y install rsyslog

* At the end of file place the following line to point the client message log to the server, on Server-02, edit file **/etc/rsyslog.conf**:

# uncomment such as below:

$ActionQueueFileName fwdRule1 # unique name prefix for spool files

$ActionQueueMaxDiskSpace 1g # 1gb space limit (use as much as possible)

$ActionQueueSaveOnShutdown on # save messages to disk on shutdown

$ActionQueueType LinkedList # run asynchronously

$ActionResumeRetryCount -1 # infinite retries if host is down

#add to end of file

\*.info;mail.none;authpriv.\*;cron.\* @172.20.10.12:514

* Start rsyslog service:

# systemctl start rsyslog.service

* On Log Server (Server-01):

# tail -10 /var/log/secure

* If you'd like to separate logs for each Host, for each date, Configure like follows on Log Server:

# vi /etc/rsyslog.conf # add: define logfiles

$template Secure\_log,"/var/log/secure.d/%fromhost%\_%$year%%$month%%$day%.secure"

# add: specify logfiles defined above

**authpriv.\* -?Secure\_log**

* On Log Server (Server-01):

# systemctl restart rsyslog # ll /var/log/secure.d

### Task 3: Mail Transfer Agent (MTA) basics Configure alias

* Edit file /etc/aliases, At the end of the list is a commented out line, uncomment it and change the name such as yourname:

root: trungnguyenkbuor

* Re read the aliases file:

# sendmail –bi Or

# newaliases

### Installation mail command on CentOS

* Installation mail command with mailx package:

# yum install –y mailx

* Create user with username such as your-name:

# useradd trungnguyenkbuor

# passwd trungnguyenkbuor

* Switch to user hv01:

# su hv01

* Create new email send to root and auto forward to your-name user (ex: trungnguyenkbuor):

**$ mail root**

Subject: Testing Email

day la mail gui cho root nhung forward cho tui

* Press CTRL+D to submit message
* Exit user hv01 and switch to your-name user (ie: trungnguyenkbuor) with run script logon:

**$ exit**

# su - trungnguyenkbuor

* Log on to your username:
* Check mail with mail command:

$ mail

Heirloom Mail version 12.5 7/5/10. Type ? for help. "/var/spool/mail/trungnguyenkbuor": 1 message 1 new

>N 1 [hv01@localhost.local](mailto:hv01@localhost.local) Fri Dec 8 17:44 22/862 "Testing Email"

&

* Type 1 after “&” sign for see new email 1:

& **1**

* If you want exit, press q and enter.

### Task 4: Printer

* Perform this task on Server-01
* Install cups and cups-pdf package
* Edit file /etc/cupsd.conf such as:

Listen \*:631

<Location />

……

Allow All

</Location>

<Location /admin>

……

Allow All

</Location>

<Location /admin/conf>

……

Allow All

</Location>

* Start service cups.
* Using Web browser on Windows 7, connect to http://ip:631 and verify.

**Lab 18**

# Security

Perform this lab on Server-01

### Task 1: Working with Selinux

* Check current Selinux on system with getenforce and sestatus command.
* Disbaled Selinux
* Reboot your system and verify.

### Task 2: Working with TCPwappers

* Edit file /etc/hosts, configure nodename such as:
  + mail.classroom.com 172.20.10.1
  + server-02.classroom.com 172.20.10.12
* Configure deny all ssh client from domain classroom.com but allow only mail.classroom.com should be connection.

### Task 3: Working with Firewalld

* Start firewalld services.
* Open port for printer server, webmin on server-01.
* Enabled SElinux
* Change Listen port 22 of SSH to 2222.
* Allow port 2222 from firewalld.
* Using SSH client, connect to Server-01 with port 2222.
* Using command:

# **semanage port -a -t ssh\_port\_t -p tcp 2222**

* Re-connect ssh and verify.

**Lab 19**

# Configure IPv6

Configure ensxx with a static ipv6 addresses as follows (keep current IPv4):

* Configure a Static IPv6 address in Server-01 as fddb:fe2a:ab1e::c0a8:64/64.
* Configure a Static IPv6 address in Server-02 as fddb:fe2a:ab1e::c0a8:02/64.
* The changes should be permanent even after the reboot.