Assignment 1

Requirement

- 2 Linux : Server and Client

1. Manual Mount

- Both Server and Client

```
yum install nfs-utils libnfsidmap
```

Server

- Enable and Start Service

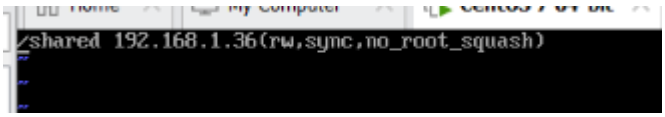
```
systemctl enable rpcbind
systemctl enable nfs-server
systemctl start rpcbind
systemctl start rpc-statd
systemctl start nfs-server
```

- Add Services and Ports For the firewall

```
firewall-cmd --permanent --add-service=rpc-bind
firewall-cmd --permanent --add-service=mountd
firewall-cmd --permanent --add-port=2049/tcp
firewall-cmd --permanent --add-port=2049/udp
firewall-cmd –reload
```

- สร้าง shared directoryและเปลี่ยน chmod ให้เป็น 777

```
mkdir /shared
chmod 777 /shared
vi /etc/exports
```



```
exportfs -r
showmount -e localhost
```

Client

- Enable and Start Service

```
systemctl enable rpcbind
systemctl start rpcbind
```

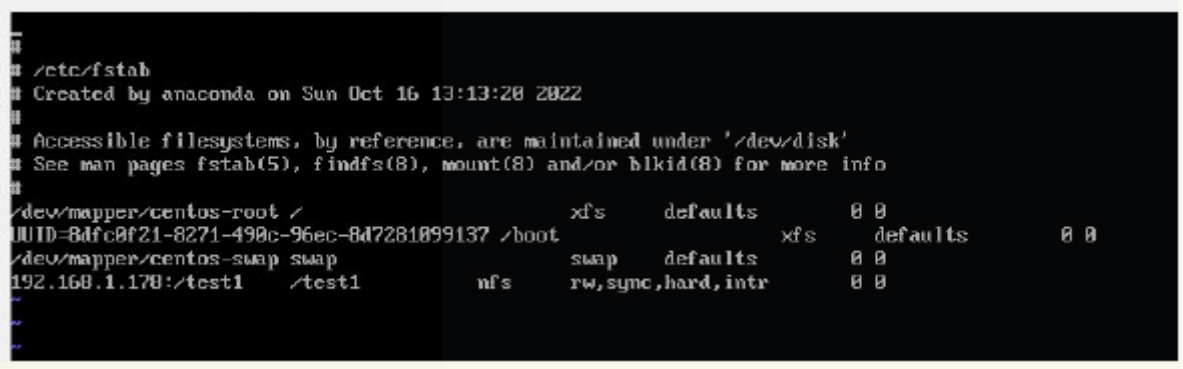
- เช็คว่าทำการ mount แล้วหรือยังและทำการ mount folder /shared

```
  showmount -e 192.168.1.35
  mount -t nfs 192.168.1.35:/shared /shared
  df -kh (เช็คว่าทำการ mount แล้วหรือยัง)
```

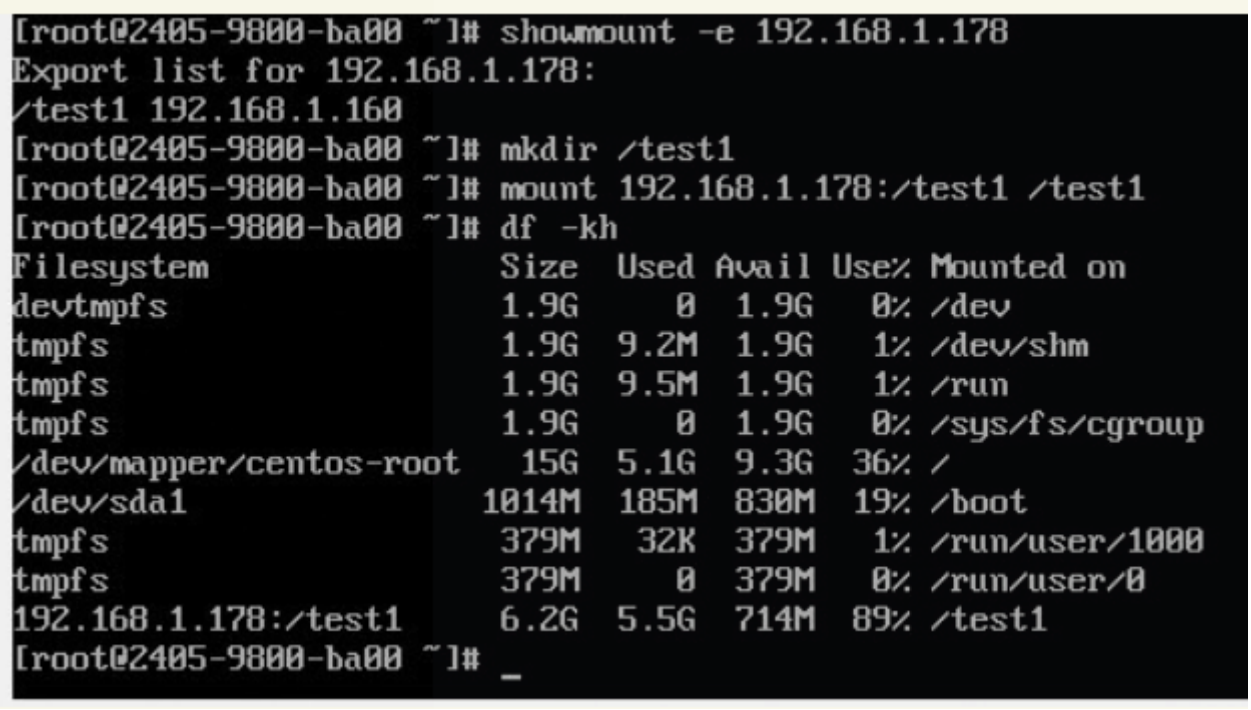
2. Auto Mount when reboot

Client

```
vi /etc/fstab
```



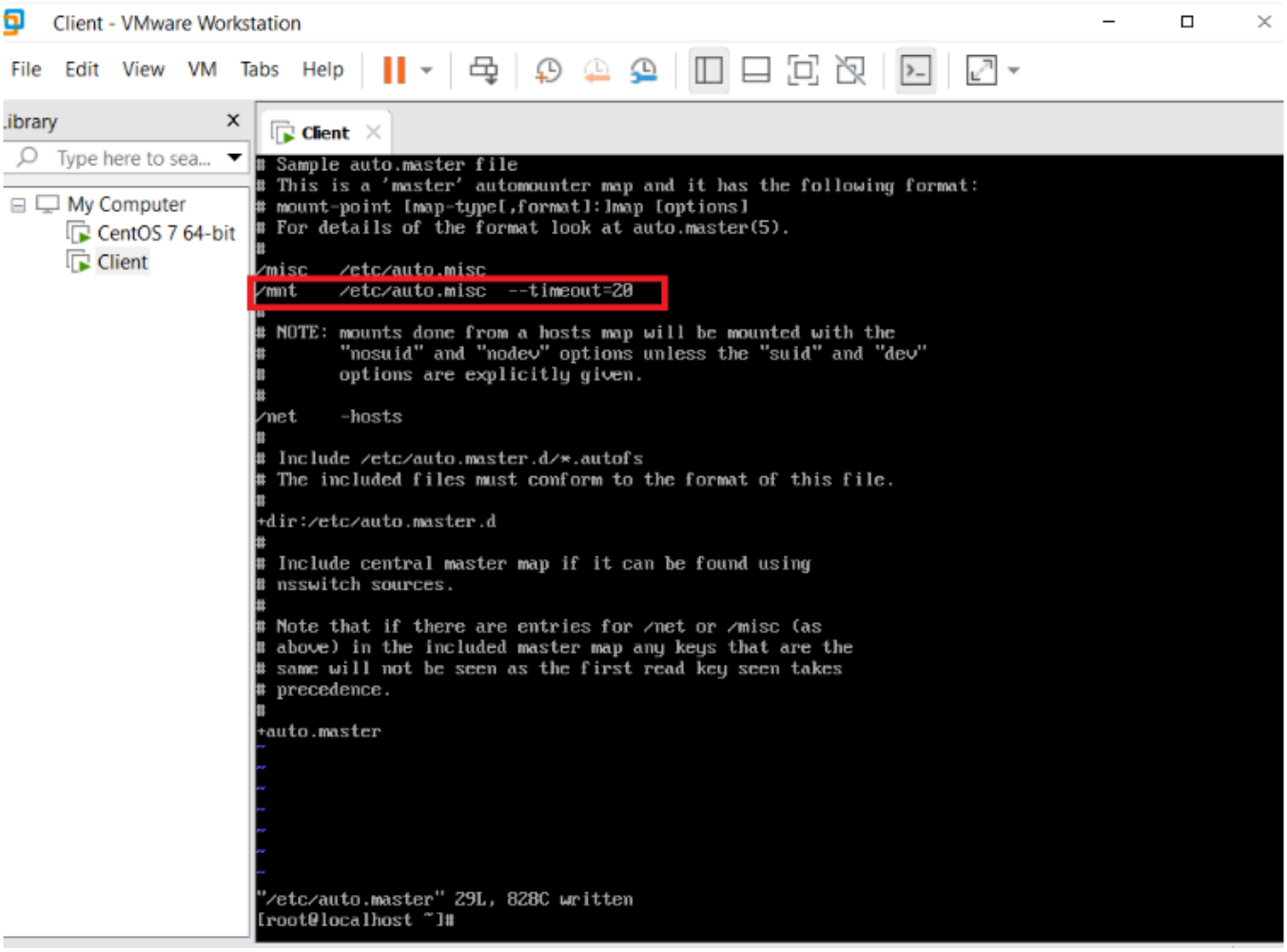

```
umount /test1/
mount -av
```



3. Autofs

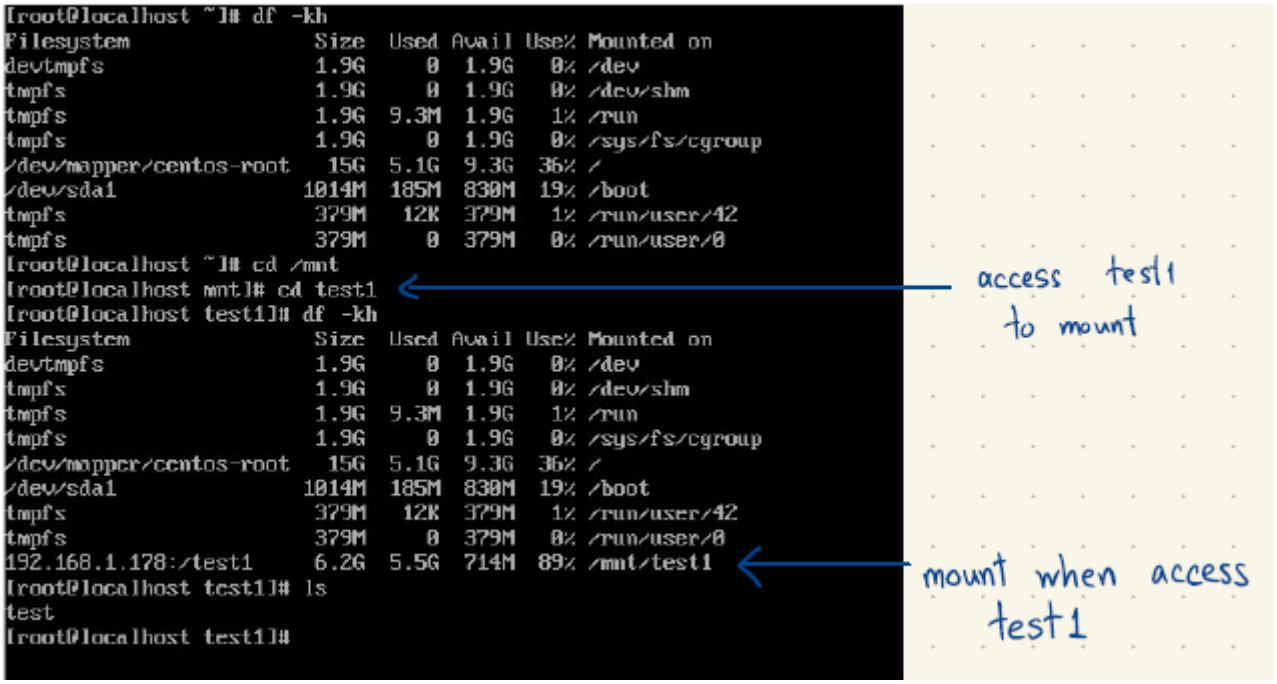
Client

```
yum install -y autofs
vi /etc/auto.master
```




```
vi /etc/auto.misc
```


```
systemctl enable autofs
systemctl start autofs
```



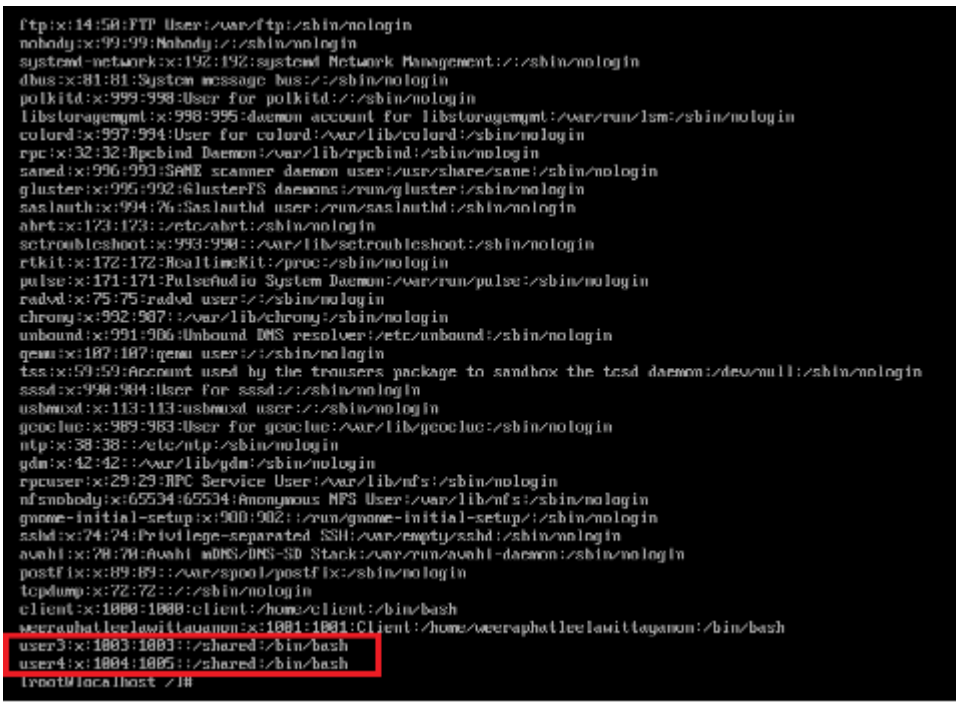
Assignment 2

Requirement

- 2 Linux [Server and Client] and 1 Window Client

Mount Directory In /etc/fstab

- Then Change home directory to directory where is mounted



Window Client

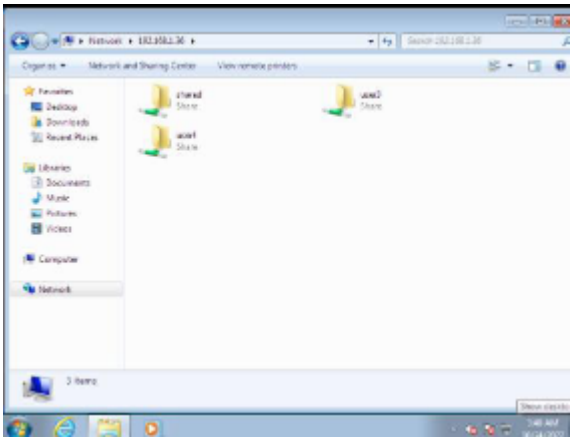
```
yum install samba
vi /etc/samba/smb.conf
```

- Parameter :

    1. path -> path of directory
    2. valid users = user2,user3 -> allowed user to this directory
    3. public ->make the directory visible
    4. writable -> make user write or create file

- Add Samba User

```
smbpasswd -a user2
smbpassed -a user3
```

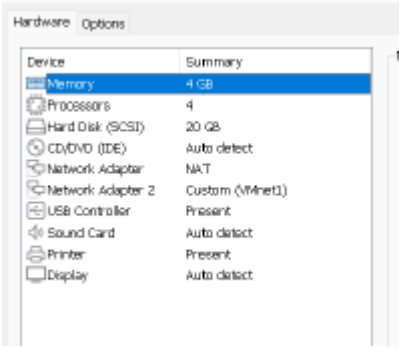


```
firewall-cmd --permanent --add-port=139/tcp
firewall-cmd --permanent --add-port=445/tcp
firewall-cmd --permanent --add-port=137/udp
firewall-cmd --permanent --add-port=138/udp
firewall-cmd --permanent --add-port=139/udp
firewall-cmd --reload
systemctl restart smb
```

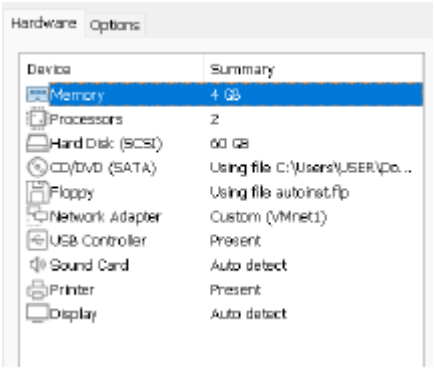
Assignment 3

Requirement

- 1 linux server and 1 Window Client
- SetUp Linux interface

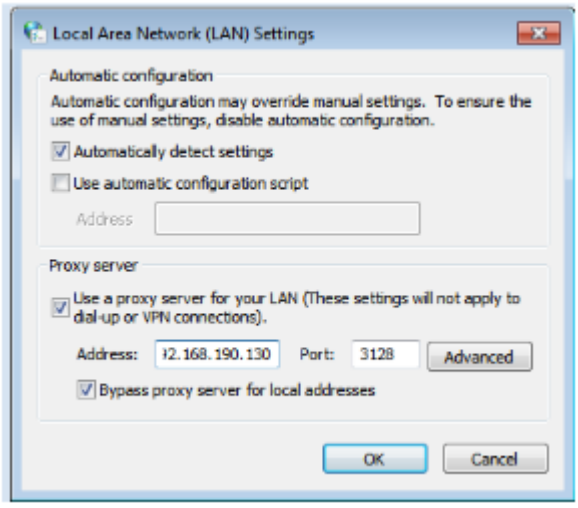


- SetUp Window interface




```
Yum install squid
Systemctl start squid
Systemctl enable squid
Systemctl status squid
```

- Config the squid.conf and setup the proxy in client



Config squid.conf and set the ACL for allow private ip class

```
acl localnet src 192.168.0.0/24 #
acl localnet src fc00::/7       #
acl localnet src fe80::/10      #
```

config proxy port

```
# Squid normally listens to port 3128
http_port 3128
```

verify that can use internet

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::9d35:220f:65df:773a%11
   IPv4 Address. . . . . . . . . . . : 192.168.205.128
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.205.2
```

Set proxy password

```
yum install -y httpd-tools
```

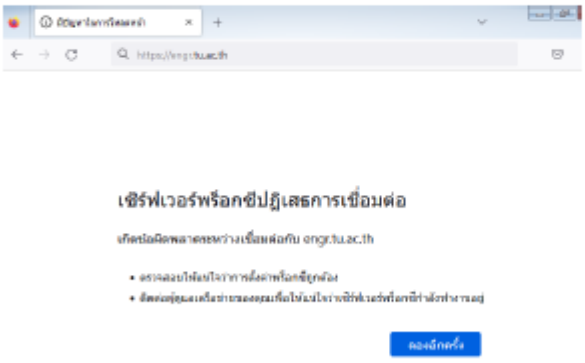
```
auth_param basic program /usr/lib64/squid/basic_ncsa_auth /etc/squid/passwd
auth_param basic children 5
auth_param basic realm Squid Basic Authentication
auth_param basic credentialsttl 2 hours
acl auth_users proxy_auth REQUIRE
http_access allow auth_users
```

```
[root@localhost ~]# htpasswd /etc/squid/passwd ninja
New password:
Re-type new password:
Adding password for user ninja
[root@localhost ~]# systemctl restart squid
```

Block Sites

```
[root@localhost squid]# cat /etc/squid/blocksites
.faccbook.com
.engr.tu.ac.th
```

```
acl blocked_urls dstdomain "/etc/squid/blocksites"
http_access deny blocked_urls
```



Assignment 4

Requirement

- 3 linux
    1. DNS Server
    2. Apache Server
    3. Syslog Server

DNS Server

```
yum install -y httpd
vi /etc/named.conf
```

```
zone "ece.local" IN {
        type master;
        file "ece.forward.zone";
        allow-update { none; };
};

zone "111.168.192.in-addr.arpa" IN {
        type master;
        file "ece.reverse.zone";
        allow-update { none; };
};
```

```
acl internals { 192.168.111.0/24; };

options {
        listen-on port 53 { 127.0.0.1; 192.168.111.1; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { localhost;any; };
```

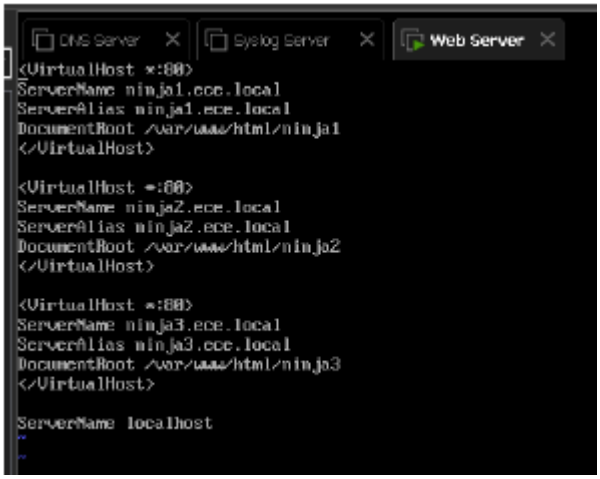
- Edit these files

```
vi /var/named/ece.forward.zone
vi /var/named/ece.reverse.zone
```

```
[root@localhost ~]# cat /var/named/ece.forward.zone
$TTL 3H
$ORIGIN ece.local.

@       IN SOA ns1.ece.local. root.ece.local. (
                                0       ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum

                IN NS ns1.ece.local.

ns1             IN A 192.168.111.1
ninja1          IN A 192.168.111.2
ninja2          IN A 192.168.111.2
ninja3          IN A 192.168.111.2
[root@localhost ~]# cat /var/named/ece.reverse.zone
$TTL 3H
$ORIGIN 111.168.192.in-addr.arpa.

@       IN SOA ns1.ece.local. root.ece.local. (
                                0       ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum

        IN NS ns1.ece.local.

1       IN PTR ns1.ece.local.
2       IN PTR ninja1.ece.local.
2       IN PTR ninja2.ece.local.
2       IN PTR ninja3.ece.local.
[root@localhost ~]#
```

Apache Server

- Make vhost.conf file



Syslog Server

```
yum install -y rsyslog
firewall-cmd --permanent --zone=public --add-port=514/tcp
firewall-cmd --permanent --zone=public --add-port=514/udp
firewall-cmd –reload
vi /etc/rsyslog.conf
```

```
# Provides UDP syslog reception
$ModLoad imudp$UDPServerRun 514
# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
```

```
systemctl start rsyslog
cat/var/log/messages
```

On DNS and Apache Server

```
vi /etc/rsyslog.conf
```

Assignment 5

Requiremnt

- 2 Linux servers : Bacula Server and Client

On Bacula Server

```
sudo yum install -y bacula-director bacula-storage bacula-console bacula-client
mariadb-server
sudo systemctl start mariadb
```

- Set the mariaDB to supported Bacula backup scheme.

- Edit the bacula-dir.conf for configuration Director, FileSet, Client, Storage, Catalog and Pool.

```
sudo mkdir -p /bacula/backup /bacula/restore
sudo chown -R bacula:bacula /bacula
sudo chmod -R 700 /bacula
sudo mkdir /etc/bacula/conf.d
vi /etc/bacula/bacula-dir.conf
```

```
Director {                            # define myself
  Name = BackupServer-dir
  DIRport = 9101                # where we listen for UA connections
  QueryFile = "/etc/bacula/query.sql"
  WorkingDirectory = "/var/spool/bacula"
  PidDirectory = "/var/run"
  Maximum Concurrent Jobs = 1
  Password = "MDg1YmMwNTkxZWE0ZWEzMmYwMzY1OWJlM"         # Console pas
  Messages = Daemon
  DirAddress = 127.0.0.1
}
```

```
# List of files to be backed up
FileSet {
  Name = "Full Set"
  Include {
    Options {
      signature = MD5
      compression = GZIP
    }
#
#  Put your list of files here, preceded by 'File
#    or include an external list with:
#
#    File = <file-name
#
#  Note: / backs up everything on the root partiti
#    if you have other partitions such as /usr or
#    you will probably want to add them too.
#
#  By default this is defined to point to the Bacu
#    directory to give a reasonable FileSet to bac
#    disk storage during initial testing.
#
    File = /
  }
```

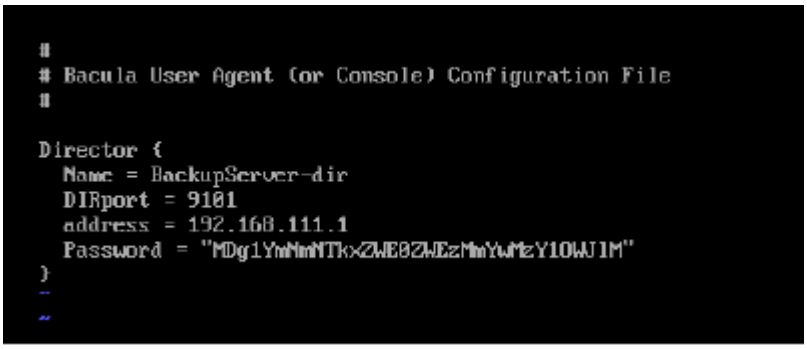
```
#
  Exclude {
    File = /var/spool/bacula
    File = /tmp
    File = /proc
    File = /tmp
    File = /.journal
    File = /.fsck
    File = /bacula
  }
}
```

```
# Definition of file storage device
Storage {
  Name = File
# Do not use "localhost" here
  Address = 192.168.111.3                # N.B. Use a fully qualified name here
  SDPort = 9103
  Password = "MDBiOGEyZWFmZTZmNTg1MmU3NzExODg5Y"
  Device = FileStorage
  Media Type = File
}
```

```
# File Pool definition
Pool {
  Name = File
  Pool Type = Backup
  Label Format = Local-
  Recycle = yes                       # Bacula can automatically recycle Volumes
  AutoPrune = yes                     # Prune expired volumes
  Volume Retention = 365 days         # one year
  Maximum Volume Bytes = 50G          # Limit Volume size to something reasonable
  Maximum Volumes = 100               # Limit number of Volumes in Pool
}
```

```
bacula-dir -tc /etc/bacula/bacula-dir.conf
```

- Edit bconsole.conf




```
bacula-sd -tc /etc/bacula/bacula-sd.conf
```

```
DIR_PASSWORD=`date +%s | sha256sum | base64 | head -c 33`
sudo sed -i "s/@@DIR_PASSWORD@@/${DIR_PASSWORD}/" /etc/bacula/bacula-dir.conf
sudo sed -i "s/@@DIR_PASSWORD@@/${DIR_PASSWORD}/" /etc/bacula/bconsole.conf
SD_PASSWORD=`date +%s | sha256sum | base64 | head -c 33`
sudo sed -i "s/@@SD_PASSWORD@@/${SD_PASSWORD}/" /etc/bacula/bacula-sd.conf
sudo sed -i "s/@@SD_PASSWORD@@/${SD_PASSWORD}/" /etc/bacula/bacula-dir.conf
FD_PASSWORD=`date +%s | sha256sum | base64 | head -c 33`
sudo sed -i "s/@@FD_PASSWORD@@/${FD_PASSWORD}/" /etc/bacula/bacula-dir.conf
sudo sed -i "s/@@FD_PASSWORD@@/${FD_PASSWORD}/" /etc/bacula/bacula-fd.conf
```

- Start and Enable bacula-dir service.

```
sudo systemctl start bacula-dir
sudo systemctl start bacula-sd
sudo systemctl start bacula-fd
sudo systemctl enable bacula-dir
sudo systemctl enable bacula-sd
sudo systemctl enable bacula-fd
```

```
sudo mkdir /etc/bacula/conf.d
sudo vi /etc/bacula/bacula-dir.conf
```

- At the end of the file add

```
@|"find /etc/bacula/conf.d -name '*.conf' -type f -exec echo @{} \;"
```

```
sudo vi /etc/bacula/conf.d/pools.conf
```

```
Pool {
  Name = RemoteFile
  Pool Type = Backup
  Label Format = Remote-
  Recycle = yes                       # Bacula can automatically recycle Volumes
  AutoPrune = yes                     # Prune expired volumes
  Volume Retention = 365 days         # one year
    Maximum Volume Bytes = 50G          # Limit Volume size to something
reasonable
  Maximum Volumes = 100               # Limit number of Volumes in Pool
}
```

```
sudo vi /etc/bacula/conf.d/filesets.conf
```

```
FileSet {
  Name = "Home and Etc"
  Include {
    Options {
      signature = MD5
      compression = GZIP
    }
    File = /home
    File = /etc
  }
  Exclude {
    File = /home/bacula/not_important
  }
}
```

```
sudo vi /etc/bacula/conf.d/clients.conf
```

```
Client {
  Name = ClientHost-fd
  Address = client_private_FQDN
  FDPort = 9102
  Catalog = MyCatalog
  Password = "Y2Q5ODUyMWM0YTFhYjA3NTcwYmU5OTA4Y"          # password for Remote
FileDaemon
  File Retention = 30 days            # 30 days
  Job Retention = 6 months            # six months
  AutoPrune = yes                     # Prune expired Jobs/Files
}
Job {
  Name = "BackupClientHost"
```

```
  JobDefs = "DefaultJob"
  Client = ClientHost-fd
  Pool = RemoteFile
  FileSet="Home and Etc"
}
```

```
sudo bacula-dir /etc/bacula/bacula-dir.conf
```

```
sudo systemctl restart bacula-dir
```

On Bacula Client

```
sudo yum install -y bacula-client bacula-console
```

```
sudo vi /etc/bacula/bacula-fd.conf
```

```
Director {
  Name = BackupServer-dir
  Password = "123456"
}

FileDaemon {                          # this is me
  Name = ClientHost-fd
  FDAddress = client_private_ip
  FDport = 9102                  # where we listen for the director
  WorkingDirectory = /var/spool/bacula
  Pid Directory = /var/run
  Maximum Concurrent Jobs = 20
}

Messages {
  Name = Standard
  director =  BackupServer-dir = all, !skipped, !restored
}
```

```
sudo bacula-fd -tc /etc/bacula/bacula-fd.conf
```

```
sudo systemctl restart bacula-fd
```

```
sudo systemctl enable bacula-fd
```

```
sudo mkdir -p /bacula/restore
sudo chown -R bacula:bacula /bacula
sudo chmod -R 700 /bacula
```

```
sudo vi /etc/bacula/bconsole.conf
```

```
#

Director {
  Name = bacula-dir
  DIRport = 9101
  address = 192.168.111.2
  Password = "123456"
}
~
~
```

```
bconsole
```

```
Select Client (File daemon) resource (1-2): 2
Connecting to Client ClientHost-fd at 192.168.111.2:9102

ClientHost-fd Version: 5.2.13 (19 February 2013)  x86_64-redhat-linux-gnu redhat (Core)
Daemon started 22-Nov-22 00:29. Jobs: run=0 running=0.
 Heap: heap=135,168 smbytes=21,682 max_bytes=21,829 bufs=52 max_bufs=53
 Sizeof: boffset_t=8 size_t=8 debug=0 trace=0
Running Jobs:
Director connected at: 22-Nov-22 00:29
No Jobs running.
====

Terminated Jobs:
====
*run
Automatically selected Catalog: MyCatalog
Using Catalog "MyCatalog"
A job name must be specified.
The defined Job resources are:
     1: BackupClient1
     2: BackupCatalog
     3: RestoreFiles
     4: BackupClientHost
Select Job resource (1-4): 4
Run Backup job
JobName:  BackupClientHost
Level:    Incremental
Client:   ClientHost-fd
FileSet:  Home and Etc
Pool:     RemoteFile (From Job resource)
Storage:  File (From Job resource)
When:     2022-11-22 00:29:17
Priority: 10
OK to run? (yes/mod/no): yes
Job queued. JobId=6
You have messages.
*_
```