-------------------------------------------------------------------------------------------------------------------

1: Set the selinux policy in Enfrocing mode

Ans:

```
[root@server0 ~]# vim /etc/selinux/config
SELINUX=enforcing
```

Exp: Selinux will be in active mode by seting mode to enforcing. idealy a system restart is needed after changing this.

---

2: run custom command

Configure a custom command with the name "custom" every one can excute /bin/ps -aux command

Ans:

```
[root@server6 ~]# vim /etc/bashrc
at last add a line
alias custom='/usr/bin/ps -aux'
[root@server6 ~]# source /etc/bashrc
[root@server6 ~]# custom
```

---

3: Configure ssh:

Configure SSH service on server1.example.com and domain my113t.org should not have ssh access

Ans:

```
[root@server0 ~]# yum install openssh-server*
[root@server0 ~]# systemctl enable sshd
[root@server0 ~]# systemctl start sshd
[root@server0 ~]# vim /etc/hosts.deny
sshd: .my113t.org
```

Exp: Above commands will install SSH service in server1.example.com and would reject my113.org  domains to use ssh service.

---

4:  Configure ipv6

Configure IPV6 on both system1(server1.example.com) and system2(server2.example.com) on eth0 device, this should not effect IPV4 network. In system1 IPV6 should be FDDB:FE2A:AB1E::C0A8:1.In system2  IPV6 should be FFUY:KK1V:RRGW:7YGS and after reboot both IPV4 and IPV6 should be able to communicate.

Ans:

```
[root@server0 ~]#nmcli conn add con-name
[root@server0 ~]# nmcli connection add con-name static type ethernet ifname eth0
Connection 'static' (277e191e-ea3c-43a3-909a-28a0d1451568) successfully added.
[root@server0 ~]# nmcli connection modify static ipv6.addresses 'fddb:fe2a:ab1e::c0a8:1/64
fddb:fe2a:ab1e::c0a8:fe' ipv4.addresses '172.25.0.11/24 172.25.0.254'
[root@server0 ~]# nmcli connection modify static ipv4.method manual
[root@server0 ~]# nmcli connection modify static ipv6.method manual
[root@server0 ~]# nmcli connection modify static
[root@server0 ~]# nmcli connection modify static connection.autoconnect yes
[root@localhost Desktop]# nmcli connection modify "System eth0" connection.autoconnect  no
[root@localhost Desktop]# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 172.25.254.254
[root@server0 ~]# nmcli connection modify static ipv4.dns '172.25.254.254'
ot@localhost Desktop]# nmcli connection show
NAME         UUID                                  TYPE             DEVICE
static       277e191e-ea3c-43a3-909a-28a0d1451568  802-3-ethernet   --
System eth0  5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  802-3-ethernet   eth0
[root@localhost Desktop]#

[root@server0 ~]# systemctl reboot
[root@localhost Desktop]# nmcli connection show
NAME         UUID                                  TYPE             DEVICE
static       277e191e-ea3c-43a3-909a-28a0d1451568  802-3-ethernet   eth0
```

```
System eth0  5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  802-3-ethernet  --
[root@localhost Desktop]#
```

---

5: Configure Network Teaming

Ans:

```
[root@server6 ~]# lab teambridge setup [to add eno1 & eno2 (dont do in exam)]
[root@server6 ~]# ifconfig  [to see the eno1 an eno2 is there ot not]
[root@server6 ~]# nmcli connection add type team con-name team0 ifname team0 config '{"runner": {"name": 
"activebackup"}}'
[root@server6 ~]# nmcli connection modify team0 ipv4.addresses '192.168.0.100/24'
[root@server6 ~]# nmcli connection modify team0 ipv4.method manual
[root@server6 ~]# nmcli connection add type team-slave con-name team0-port1 ifname eno1 master team0
[root@server6 ~]# nmcli connection add type team-slave con-name team0-port2 ifname eno2 master team0
[root@server6 ~]# nmcli connection up team0
[root@server6 ~]# ifconfig [You will find extra device team0]
[root@server6 ~]# teamdctl team0 state   [Shows runner as active backup]
[root@server6 ~]# ping 192.168.0.10
```

---

6: port forwarding:

Configure PORT FORWARDING incomming connection on port 513/tcp on the firewall to port 132/tcp on machine system2.group11.example.com (desktop2.example.com)

Ans:

```
[root@server0 ~]# systemctl disable iptables
[root@server0 ~]# systemctl disable ip6tables
[root@server0 ~]# systemctl stop iptables
[root@server0 ~]# systemctl stop ip6tables
[root@server0 ~]# systemctl mask iptables
[root@server0 ~]# systemctl mask ip6tables
[root@server0 ~]# systemctl start firewalld
[root@server0 ~]# systemctl enable firewalld

[root@server0 ~]# firewall-cmd --permanent --add-rich-rule 'rule family=ipv4 source 
address=172.25.0.10/32 forward-port port=513 protocol=tcp to-port=132'
[root@server0 ~]# firewall-cmd --reload
```

Exp: Iptables are perminantly stoped first and then All the connections made to port 513 will be redirected to port 132.

---

7: COnfigure Mail server

        Configure a null client on server1 which relay mail through ap1.group11.example.com using desktop1. group11.example.com organization name domain name on all outgoing mails.

Ans:

```
[root@server6 ~]# vim /etc/postfix/main.cf
myorigin = desktop6.example.com
inet_interfaces = loopback-only
relayhost = [smtp6.example.com]          [Search for /relayhost Copy line below and write]
local_transport = error: local delivary disabled  [Search for /local_transpot  and write new antry 
somewhare]
mynetworks = 127.0.0.0/8, [::1]/128
mydestination =
[root@server6 ~]# systemctl restart postfix
```

---

8:  NFS Server:

Export your "/public" directory via NFS to the group11.example.com domain. Make sure that client in group11.example.com domain should able to read only permission in /public.

Ans:

```
[root@server6 ~]# yum install nfs*
[root@server6 ~]# systemctl enable  nfs-server.service
[root@server6 ~]# systemctl start nfs.service
[root@server6 ~]# firewall-cmd --permanent --add-service=nfs
[root@server6 ~]# firewall-cmd --permanent --add-service=rpc-bind
[root@server6 ~]# firewall-cmd --permanent --add-service=mountd
[root@server6 ~]# firewall-cmd --reload
[root@server6 ~]# vim /etc/exports
/public *.example.com(ro)

[root@server6 ~]# mkdir /public
exporting *.example.com:/public

[root@server6 ~]# exportfs -rv
go to desktop system and run below command to verify

[root@server6 ~]# showmount -e 172.25.6.11
Export list for 172.25.6.11:
/public *.example.com
[root@server6 ~]#
```

---

9: Configure Secure nfs server :

Export your "/publicsecure" directory with use kerbores via NFS to the group11.example.com domain. Make sure that client in group11.example.com domain should able to read and write permission in /publicsecre. And create a subdirectory called "publicshare" and publicshare directory owner permission should be nahur. and nahur user should able to read and write. Use keytab for the system1 http://server1.grou11.example.com/pub/materials/system1.keytab.

Ans:

```
[root@server6 ~]# lab nfskrb5 setup [Do institute not in exam]
[root@server6 ~]# wget -O /etc/krb5.keytab http://classroom.example.com/pub/keytabs/server7.keytab
[root@server6 ~]# vim /etc/sysconfig/nfs
RPCNFSDARGS="-V 4.2"     ------------------->line number 13
[root@server6 ~]# systemctl enable nfs-secure-server.service
[root@server6 ~]# systemctl start nfs-secure-server.service
[root@server6 ~]# mkdir /publicsecure
[root@server6 ~]# vim /etc/exports
/publicsecure  desktopX.example.com(rw,sec=krb5p)   [If in exam asks for desktop only if not *.example.com (rw,sec=krb5p)

[root@server6 ~]# exportfs -rv

Go to deskto system and run below command to verfy

[root@server6 ~]# showmount -e 172.25.6.11
Export list for 172.25.6.11:
/publicsecure *.example.com
/public       *.example.com
[root@server6 ~]#
```

---

10: mount the nfs Mounts:

1. mount the /public permanently on the /mnt/secure on the system2 sysetm.
2. mount the secure nfs share /publicsecure permanently on the /mnt/securepath on system2 system. verify that user nahur user has read and write access on the /mnt/securepath on system2.

Ans:

```
[root@desktop6 ~]# lab nfskrb5 setup   [Dont do in exam]
[root@desktop6 ~]# yum insatall nfs-utils
[root@desktop6 ~]# wget -O /etc/krb5.keytab http://classroom.example.com/pub/keytabs/desktop6.keytab
[root@desktop6 ~]# systemctl enable nfs-secure  [Only nfs-secure]
```

```
[root@desktop6 ~]# systemctl start nfs-secure
[root@desktop6 ~]# vim /etc/fstab
server6.example.com:/pumblicsecure      /mnt/securepath        nfs     defaults,sec=krb5p,v4.2 0 0
server6.example.com:/public             /mnt/secure            nfs      defaults        0 0
[root@desktop6 ~]# mkdir /mnt/secureshare
[root@desktop6 ~]# mount -a
[root@desktop6 ~]# df -h

----> Go To Server system
[root@server6 ~]# chown ldapuser6:ldapuser6 /securenfs/
[root@server6 ~]# chcon -t public_content_t /securenfs/

----> Then Go TO client System
[root@desktop6 ~]# mount -a
[root@desktop6 ~]# su - ldapuser6
[ldapuser6@desktop6 ~]$ cd /mnt/securepath
[ldapuser6@desktop6 ~]$ touch file1
```

---

11: Configure SAMBA SHARE:

Share the directory "/common" via samba. Your Samba server must be a member of "STAFF" workgroup. The share name must be "common".Make sure that browseable must be enabled. The shared must be available to group11.example.com clients only. The user "frank" should have read access to the share with samba password "animous". webserver1

Ans:

```
[root@server6 ~]# yum install samba*
[root@server6 ~]# systemctl start smb
[root@server6 ~]# systemctl start nmb
[root@server6 ~]# systemctl enable smb.service
[root@server6 ~]# systemctl enable nmb.service
[root@server6 ~]# firewall-cmd --permanent --add-service=samba
[root@server6 ~]# firewall-cmd --reload
[root@server6 ~]# mkdir /common
[root@server6 ~]# semanage fcontext -a -t samba_share_t "/common(/.*)?"
[root@server6 ~]# restorecon -vvFR /common/
[root@server6 ~]# useradd -s /usr/sbin/nologin frank
[root@server6 ~]# smbpasswd -a frank
New SMB password:
Retype new SMB password:
Added user frank.
[root@server6 ~]# vim /etc/samba/smb.conf
        workgroup = STAFF     [Line number 88]

[common]                                        [End of the config file]
        comment = Public Stuff
        path = /common
        valid users = frank
        browseable = yes
        hosts allow = 172.25.
[root@server6 ~]# systemctl restart smb
[root@server6 ~]# systemctl restart nmb

------>   IF you want to test go to client system
[root@desktop6 ~]# yum install cifs-utils
[root@desktop6 ~]# mount //172.25.6.11/common /coss -o username=frank
[root@desktop6 ~]# mkdir /coss
[root@desktop6 ~]# mount //172.25.6.11/common /coss -o username=frank
[root@desktop6 ~]# df -Th
```

---

12: Configure SAMBA SHARE:

Share the directory "/secure" via samba. The share name must be "secure". Make sure that browseable must be enabled. The shared must be available to group11.example.com clients only. The user "rob" should have read access to the share with samba password "animous" and user "robby" should have read and write access to the share with samba password "animous".

Ans:

---

13: multiuser samba mount:
Mount the samba share permantly on the /mnt/secure mount point on system2 as a multiuser mount. mount samba share wirh the credentials of user robby user and passrod animous.

---

14: Configure "web server":

Configure your system as "web server" for the site http://sysetm1.group11.example.com. Download the web page station.html from http://classroom.example.com/pub/updates/station.html Rename the the downloaded page as "index.html" Copy the "index.html" page to the "document root" Do not make any modifications to the content of index.html.

Ans:

```
[root@server6 Desktop]# yum install httpd*
[root@server6 Desktop]# systemctl restart httpd
[root@server6 Desktop]# systemctl enable httpd
[root@server6 Desktop]# firewall-cmd --permanent --add-service=http
[root@server6 Desktop]# firewall-cmd --reload
[root@server6 Desktop]# cd /var/www/html/
[root@server6 Desktop]# wget http://classroom.example.com/pub/updates/station.html
[root@server6 Desktop]# ls
[root@server6 Desktop]# mv station.html index.html
[root@server6 Desktop]# vim /etc/httpd/conf.d/main.conf
<VirtualHost *:80>
  ServerAdmin root@server6.example.com
  DocumentRoot /var/www/html
  ServerName server6.example.com
</VirtualHost>
<Directory "/var/www/html">
  AllowOverride none
  Require all granted
</Directory>

----> Goto Client
[root@desktop6 ~]# curl -k http://server6.example.com  [Out put should gom in single line]
```

---

15: Configure "web server":

Create the directory "private" for the DocumentRoot of your webserver. Download the page "host.html" from http://server.group11.example.com/pub/matarials/host.html And move as index.html.It should be accessable to group11.example.com and not to any other host.

Ans:

```
[root@server6 private]# mkdir /var/www/html/private
[root@server6 private]# cd /var/www/html/private
[root@server6 private]# wget http://classroom.example.com/pub/updates/host.html
[root@server6 private]# mv host.html index.html
[root@server6 html]# vim /etc/httpd/conf.d/main.conf
<VirtualHost *:80>
   ServerAdmin root@server6.example.com
   Documentroot /var/www/html
   ServerName server6.example.com
</VirtualHost>
###########################################################
<Directory "/var/www/html/private">
  Order allow,deny
  Allow from .example.com
</Directory>                        ------> Modify only lines which are there in ####
<Directory "/var/www/html">
   AllowOverride none
   Require all granted
</Directory>
##############################################################
[root@server6 ~]# systemctl restart httpd
```

------> Go to client

```
[root@desktop6 ~]# yum install elinks*
[root@desktop6 ~]# elinks server6.example.com/private
```

------> Go to foundation system

open firefox
and search for   >  server6.example.com/private

It Should show Forbidden

16: Configure name virtual hosting server:

Configure the name virtual hosting server for the site http://www1.group11.example.com. Download the page "www.html" from http://server.group11.example.com/pub/materials and copy as index.html under documenRoot "/var/www/virtual". User called rock should able to add some content into /var/www/virtual directory and system1.group11.example.com should abel to access the virtual hosting.

Ans:

```
[root@server6 virtual]# mkdir /var/www/virtual
[root@server6 virtual]# cd /var/www/virtual
[root@server6 virtual]# wget http://classroom.example.com/pub/updates/www.html
[root@server6 virtual]# mv www.html index.html
[root@server6 virtual]# vim /etc/httpd/conf.d/virtual.conf
<VirtualHost *:80>
  ServerAdmin root@www1.example.com
  Documentroot /var/www/virtual
  ServerName www6.example.com
</VirtualHost>
<Directory "/var/www/virtual">
  Require all granted
  AllowOverride none
</Directory>
[root@server6 virtual]# systemctl restart httpd
```

---> Go to client  open terminal

```
[root@desktop6 ~]# curl -k http://www6.example.com            [one line output will com]
```

17: confiure ssl web server

Configure secure web server site name http://system1.group11.example.com ant the web site will nedd to protect with tls. and the certificate can be download from http://serevr.group11.example.com/pub/tls/private/system1.crt
http://serevr.group11.example.com/pub/tls/private/system1.key http://serevr.group11.example.com/pub/tls/private/system1.crt

Ans:

```
[root@server6 Desktop]# yum install mod_ssl
[root@server6 Desktop]# firewall-cmd --permanent --add-service=https
[root@server6 Desktop]# firewall-cmd --reload
[root@server6 Desktop]# cd /etc/pki/tls/certs
[root@server6 Desktop]# wget http://classroom.example.com/pub/tls/certs/server6.crt
[root@server6 Desktop]# wget http://classroom.example.com/pub/example-ca.crt
[root@server6 Desktop]# cd /etc/pki/tls/private/
[root@server6 Desktop]# wget http://classroom.example.com/pub/tls/private/server6.key
[root@server6 Desktop]# vim /etc/httpd/conf.d/main.conf
<VirtualHost *:80>
   ServerAdmin root@server6.example.com
   Documentroot /var/www/html
   ServerName server6.example.com
</VirtualHost>
<Directory "/var/www/html/private">
```

```
  Order allow,deny
  Allow from .example.com
</Directory>
<Directory "/var/www/html">
   AllowOverride none
   Require all granted
</Directory>
##############  Add Only lines Which are in side this Hashes To end of this file #####
<VirtualHost *:443>
ServerName server6.example.com
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5
SSLHonorCipherOrder on
SSLCertificateFile /etc/pki/tls/certs/server6.crt
SSLCertificateKeyFile /etc/pki/tls/private/server6.key
SSLCertificateChainFile /etc/pki/tls/certs/example-ca.crt
DocumentRoot /var/www/html
</VirtualHost>
########################################################################################
[root@server6 Desktop]# systemctl restart httpd
```

```
---> Go to the client system
---> Open browser and search for below sites
--->  https://server6.example.com    [This Is original to search and then search also]
--->  server6.example.com
--->  server6.example.com/private
--->  www6.example.com
```

Note: All should give proper output

---

18: Configure wsgi web server:

Configure "wsgi" web server site name "webappX.example.com" and download dynamic WSGI conent from http://classroom.example.com/pub/update/weapp.wsgi and stored inside  virtual web server DocumentRoot of your webserver. and donot effect virtual web serevr.

Ans:

```
[root@server6 Desktop]# yum install mod_wsgi
[root@server6 Desktop]# cd /var/www/virtual/
[root@server6 virtual]# wget http://classroom.example.com/pub/updates/webapp.wsgi
[root@server6 virtual]# vim /etc/httpd/conf.d/webapp.conf
<VirtualHost *:80>
ServerName webapp6.example.com
WSGIScriptAlias / /var/www/virtual/webapp.wsgi
</VirtualHost>
[root@server6 virtual]# systemctl restart httpd
```

```
----> Goto  Client System
----> Open Web browser and search the site
----> webapp6.example.com
```

---

19: CONFIGURE "target server":

configure target server use the this iqn iqn.2014-09.com.example.group11:system1 and 3G backing store device volume group name iscsi_storage. iscsi storage should availabe to sysetm2.group11.example.com sysetm only.

Asn:

```
[root@server6 virtual]# yum install targetcli
[root@server6 virtual]# fdisk /dev/vdb      [Create one partion more than 3GB i have created 3G]
[root@server6 virtual]# partprobe
[root@server6 virtual]# pvcreate /dev/vdb1
[root@server6 virtual]# vgcreate iscsi_storage /dev/vdb1
[root@server6 virtual]# lvcreate -L 3G -n iscsi_lv iscsi_storage
```

```
[root@server6 virtual]# systemctl enable target.service
[root@server6 virtual]# systemctl start target.service
[root@server6 virtual]# firewall-cmd --permanent --add-port=3260/tcp
[root@server6 virtual]# firewall-cmd --reload

[root@server6 virtual]# targetcli
Warning: Could not load preferences file /root/.targetcli/prefs.bin.
targetcli shell version 2.1.fb34
Copyright 2011-2013 by Datera, Inc and others.
For help on commands, type 'help'.
/> ls
o- / .....................................................................................................
[...]
  o-
backstores ..........................................................................................
[...]
  | o- block .............................................................................. [Storage
Objects: 0]
  | o- fileio ............................................................................. [Storage
Objects: 0]
  | o- pscsi .............................................................................. [Storage
Objects: 0]
  | o- ramdisk ............................................................................ [Storage
Objects: 0]
  o- iscsi ........................................................................................
[Targets: 0]
  o- loopback .....................................................................................
[Targets: 0]/> backstores/block create block1 /dev/iscsi_storage/iscsi_lv
Created block storage object block1 using /dev/iscsi_storage/iscsi_lv.
/> iscsi/ create iqn.2014-09.com.example:server6
Created target iqn.2014-09.com.example:server6.
Created TPG 1.
/> iscsi/iqn.2014-09.com.example:server6/tpg1/acls create iqn.2014-09.com.example:desktop6
Created Node ACL for iqn.2014-09.com.example:desktop6
/> iscsi/iqn.2014-09.com.example:server6/tpg1/luns create /backstores/block/block1
Created LUN 0.
Created LUN 0->0 mapping in node ACL iqn.2014-09.com.example:desktop6
/> iscsi/iqn.2014-09.com.example:server6/tpg1/portals create 172.25.6.11
Using default IP port 3260
Created network portal 172.25.6.11:3260.
/> ls
o- / .....................................................................................................
[...]
  o-
backstores ..........................................................................................
[...]
  | o- block .............................................................................. [Storage
Objects: 1]
  | | o- block1 .................................... [/dev/iscsi_storage/iscsi_lv (3.0GiB) write-thru
activated]
  | o- fileio ............................................................................. [Storage
Objects: 0]
  | o- pscsi .............................................................................. [Storage
Objects: 0]
  | o- ramdisk ............................................................................ [Storage
Objects: 0]
  o- iscsi ........................................................................................
[Targets: 1]
  | o- iqn.2014-09.com.example:server6 ...............................................................
[TPGs: 1]
  |   o- tpg1 ........................................................................... [no-gen-acls,
no-auth]
  |     o- acls ......................................................................................
[ACLs: 1]
  |     | o- iqn.2014-09.com.example:desktop6 ................................................. [Mapped
LUNs: 1]
  |     |   o- mapped_lun0 ............................................................ [lun0 block/
block1 (rw)]
  |     o- luns .....................................................................................
[LUNs: 1]
  |     | o- lun0 ................................................. [block/block1 (/dev/iscsi_storage/
iscsi_lv)]
  |     o- portals ..................................................................................
[Portals: 1]
  |       o-
172.25.6.11:3260 ........................................................................... [OK]
  o- loopback ...............................................................................
[Targets: 0]
/> exit
Global pref auto_save_on_exit=true
Last 10 configs saved in /etc/target/backup.
Configuration saved to /etc/target/saveconfig.json
[root@server6 virtual]#
```

---

20: Configure iscsi client.

        create a new 2024Mb iscsi target on your system1.group11.example.com machine. this target should be called iqn.2014-09.com.example.group11:system1 and assign file system ext4 and mount under /mnt/iscsi directory.

Ans:

```
[root@desktop6 ~]# yum install iscsi*
Loaded plugins: langpacks
rhel_dvd                                                                                 | 4.1 kB
00:00:00
Package iscsi-initiator-utils-6.2.0.873-21.el7.x86_64 already installed and latest version
Package iscsi-initiator-utils-iscsiuio-6.2.0.873-21.el7.x86_64 already installed and latest version
Nothing to do
[root@desktop6 ~]# systemctl start iscsi
[root@desktop6 ~]# systemctl enable iscsi
[root@desktop6 ~]# vim /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.2014-09.com.example:desktop6
[root@desktop6 ~]# iscsiadm -m discovery -t st -p server6.example.com
172.25.6.11:3260,1 iqn.2014-09.com.example:server6
[root@desktop6 ~]# iscsiadm -m node -T iqn.2014-09.com.example:server6 -p server6.example.com -l
Logging in to [iface: default, target: iqn.2014-09.com.example:server6, portal: 172.25.6.11,3260]
(multiple)
Login to [iface: default, target: iqn.2014-09.com.example:server6, portal: 172.25.6.11,3260] successful.
[root@desktop6 ~]# fdisk -l     [Check for /dev/sda]
[root@desktop6 ~]# fdisk /dev/sda
[Create 2024 mb patition (+2024M)]
[root@desktop6 ~]# partprobe
[root@desktop6 ~]# mkfs.ext4 /dev/sda1
[root@desktop6 ~]# mkdir /mnt/iscsi
[root@desktop6 ~]# blkid /dev/sda1
[Copy UUID and write enty in fstab with UUID as below]
[root@desktop6 ~]# vim /etc/fstab
UUID=2e8da35d-d037-4768-bc92-bdbc4b37bb5a /mnt/iscsi              ext4    _netdev         0 0
[root@desktop6 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda1        10G  3.1G  7.0G  31% /
Out put omited.........

[root@desktop6 ~]# mount -a
[root@desktop6 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda1        10G  3.1G  7.0G  31% /
Output omited........
/dev/sda1       2.0G  6.0M  1.8G   1% /mnt/iscsi
[root@desktop6 ~]# iscsiadm -m node -T iqn.2014-09.com.example:server6 -p server6.example.com -l
[root@desktop6 ~]# init 6
```

---

21: Configure mariadb.

install mariadb database and user root password is animous database sholud access only localhost. create a "Conatins" datebase and restore a data base backup http://server1.group11.example.com/pub/matarials/mariadb.dump. rob user can access "contains" database should be use password is "animous".

Ans:

```
[root@server6 ~]# yum groupinstall mariadb mariadb-client
[root@server6 ~]# systemctl start mariadb
[root@server6 ~]# systemctl enable  mariadb
[root@server6 ~]# ss -tulnp| grep mysql
tcp    LISTEN     0      50                    *:3306                  *:*      users:
(("mysqld",8370,13))
[root@server6 ~]# vim /etc/my.cnf
[mysqld]      ----> [Under This line]
skip-networking=1
[root@server6 ~]# systemctl restart mariadb
[root@server6 ~]# ss -tulnp| grep mysql
[Now This command should show nothing]
[root@server6 ~]# mysql_secure_installation
Enter current password for root (enter for none):   [Dont Give anything press enter]
Set root password? [Y/n] y
New password: animous [Give password]
Re-enter new password:  animous   [Retry same passwd]
Password updated successfully!
Reloading privilege tables..
 ... Success!
Remove anonymous users? [Y/n] y
Disallow root login remotely? [Y/n] y
Remove test database and access to it? [Y/n] y
Reload privilege tables now? [Y/n] y
[root@server6 ~]# mysql -u root -p
Enter password:
MariaDB [(none)]> create database conatins;
MariaDB [(none)]> exit
[root@server6 ~]# mysql -u root -p conatins < /root/mariadb.dump
Enter password:
[root@server6 ~]# mysql -u root -p
MariaDB [conatins]> CREATE USER rob@'%' IDENTIFIED BY 'animous';
MariaDB [conatins]> GRANT SELECT,INSERT,UPDATE,DELETE ON conatins.* TO rob@'%';
```

22: Script:

Write the script called /root/script. If you pass an argument as "redhat" it should print "fedora" . If you pass an argument as "fedora" it should print "redhat". If won't pass any argument (or) if you pass another argument other than "redhat" and "fedora"it will print standard error "/root/script redhat|fedora".

```
[root@server6 ~]# vim /root/script
#!/bin/bash
if [ "$1" = redhat ]; then
echo fedora
elif [ "$1" = fedora ]; then
echo redhat
else echo "/root/script redhat|fedora"
fi
[root@server6 ~]# chmod 744 /root/script
cript redhat|fedora
[root@server6 ~]# /root/script asa
/root/script redhat|fedora
[root@server6 ~]# /root/script redhat
fedora
[root@server6 ~]# /root/script fedora
redhat
[root@server6 ~]#
```

```
23: write a script to create a user:

        write a bash script /root/script to add a users from the list given in a file if the file is
given as a coomand line argument. if the file doesn't exit, then a message should be printed as "INPUT"
file not found and exit with an appropriate value. if the commandline argument is left blank, then a
message shuold be printed as useage: /root/script" and exit with an appropriate value. if the path of the
filename is wroung then it should print a message as "stdeer" and exit with an appropriate value.

Ans:

12  13   23
```