**(1)HTTP – Port 80**

Step1 – yum install -y httpd

Step2 – systemctl restart httpd

Step3 - systemctl enable httpd

step 4 – systemctl status httpd

step 5 – firewall-cmd --add-service =httpd

step 6 – firewall-cmd --add-service =httpds

step 7 – firewall-cmd --relaod

step8 - firewall-cmd --add-service =httpd

step 9 – firewall-cmd --relaod

step 10 – firewall-cmd --add-service =httpds

step 11 – firewall-cmd --relaod

step 12- systemctl status httpd

step 13 - cd /var/www/html

step 14 – ls ( it will give output blank)

stpe15 – create a file :- (index .html ) opened this via vim

step 16 – vim index.html , press i and write some text ( Hi there how are you or any web page template like that )

step 17 – search in firefox : <http://localhost> ( it will show text which is we have put earlier on that file as it will work similar like website )

step 18 – yum install eliniks -y

(it would like to see this via terminal for that , I would need to install package of “eliniks”)

Step19 – eliniks <http://localhost>

Step 20 : go out click q and s and then we can modified this file as well with the help of that application

Video Link - <https://www.youtube.com/watch?v=KrJf7EmH2Gs>

# (2)How to Install and Configure MariaDB

Definition – for managing the data base of any organization such as like employee related data or inventory for that organization

(Google DEF - MariaDB is an **open source relational database management system** (RDBMS) that is a compatible drop-in replacement for the widely used MySQL database technology.

Mandb – manual page update

Updatedb – update database

Mysql – old version of rhel 6

Mariadb - upgraded version of mysql in rhel 7

Configuration file location – etc/my.cnf

Mariadb port – 3306 by default port number

Step 1 – install mariab db server with all dependency

Command – Yum install mariadb\* - y or Yum install mariadb-server -y

Step 2 – now we will start doemon

Command - systemctl start mariadb

Command - systemctl enable mariadb

Step 3- we will have to configure service in firewall – (Note – here service would - mysql service and doemon name would -mariadb)

Command - firewall-cmd --permanent --add-service=mysql (note – service not changed according to package name )

Command -firewall-cmd --reload

Step4 – create a password for login to root for handling and managing database –

Command - mysql\_secure\_installation

- hit enter

– set root password {y/n} y

New password : root

Confirm password : root

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

Installation done !

Step5 – for login mariadb we will use root user and password which is already we set on it .

Command – mysql -u root -p

Enter password : root

MariaDB [(none0] > ( Note -Successfully entered dialoged box will occurred )

Step6 – after entering maria db we can check database how may present theire

Command - MariaDB [(none0] > show databases;

Step6 – for creating a database

Command - MariaDB [(none0] > create database guru; (here guru the name of new database )

For checking that database is created or not hit the command

Command - MariaDB [(none0] > show databases;

Now exit form the MariaDB

Step 7 – if wanted to no body can access form the remote location , so that I would have to change in the MariaDB configuration file

Go to – vim /etc/my.cnf

Put the line – below pid line

Skip-networking =1

Step 8 – for updlating database form the machine , that can be possible ,

Command – mysql -u root -p </ database path (note - /mariadb.dump – database path )

Step 9– check this uploaded or note via again login into mariadb database

Command – mysql -u root -p

Enter password : root

It will prompt there,

Step 10 – for using the database in maria db for that , we will hit the below command

Command - MariaDB [(none0] > use <database name >

For cheking the table which is used in database ,

Command – MariaDB [(database name] > shows table

For any table information if you would like to search

Command - MariaDB [(database name] > describe <table name>

Video Link - <https://www.youtube.com/watch?v=wy9J0SJwAaY>

**(3) Samba**

**Port no – 137-139 : conf file – etc/samba/smb.conf**

(1)

#ping 176.108.0.10

#yum install samba -y

#vim /etc/samba/smb.conf

\*in configuration file -:

[samba\_1]

Comment = welcome to cloudblitz

Path = /shared

Browseable = yes

Writeable = yes

Public = yes

Write list = yes

Read list = Komal (note -its user name )

Read list = komal

Valid users = Komal

#cd /

#mkdir /shared

#useradd Komal

#passwd Komal

#smpasswd -a Komal

(2)

#setfacl -m u:Komal:rwx /shared

#setenforce 0

#getenforce

#systemctl start smb nmb

#systemctl enable smb nmb

#systemctl status smb nmb

\*In server side it self , if we want do with client that we can do however , while practical if we do not have the client machine we can test this itself on server)

#yum install samba-client -y

#smbclient -U Komal //192.168.0.1 /samba\_1

(Note -Ip Adderess of server)

\*in samba terminal

-Password

-ls

-p

-exit

For server side itself for client

#firewall-cmd - - add-service =samba - -permanent

#firwall-cmd --reload

For client side steps

#ping with client IP and server

#smbclient -U Komal //192.168.0.1 /samba\_1

#ls

(3) steps for samba with windows \*\*\*\*\*

First we would need to be add adapter and later that we will select **in Host only adapter in Adapter 3**

\*\* Add adapter -host only- adaptor No3

-->Now go to (1)This PC type (2)command prompt for windows in that (3)ping your IP that is 192.168.0.0 after that (4)go to again this pc and click on computer after that click **map network drive** will be open then type

[\\192.168.0.0\samba\_1](file:///\\192.168.0.0\samba_1) click ok. (5) after that samba\_1 directory will be open if you want to add you can check or you can add data from windows to Linux or Linux to windows machines .

**(4)NFS [Network file system ]**

**Port No – 2049**

NFS – is stand for network file system, helps you to share files and folders between Linux and Unix system (server and client) NFS enables you to mount a remote share locally . it’s developed by sun microsystem in 1990 and its can be acted as centralized storage system.

(1) \*\*\*Important Services \*\*\*\*

Rpcbind – The rpcbind server converts RPC program numbers into universal address

Nfs-lock/rpc-stad – NFS file locking implement file lock recovery when an NFS server crashes and reboots

NFS-server – It enables client to access NFS shares

Nfs -idmap – It translates user of group ids into names and translates user and group names into ids

(2)\*\*\*Important configuration files\*\*\*\*\*\*

#/etc/exports

#/etc/fstab

#/etc/sysconfig/nfs

#/etc/hosts.allow

#/etc/host.deny

\*\*\*\*steps to configure NFS Server \*\*\*\*\*\*\*\*\*\*\*\*\*\*

#yum install -y nfs-utils

#systemctl start nfs-server rpcbind

#systemctl restartnfs -server rpcbind

#systemctl enable nfs-server rpcbind

After that we would need to create one directory for Mount tha data on root

#mkdir /arjun

Allows NFS client to read of write to the created directory with the help of chmod command

#chmod 777 /arjun/

\*\*we would need to modify /etc/exports file to make an entry of directory /arjun that you want to share

(P3)

#vi /etc/exports

Create a nfs share something like below

/arjun 176.168.0.15(rw,sync,no\_root\_squash)

Point notes below---

>/arjun : shared directory

>176.168.0.15 : IP adderess of the client machine we can also add use the hostname , instaid of an IP address . it is also possible to define the range of client with subnet like 176.168.0.0/16

>rw : writeable permtion to shared folder

>sync : all changes to the according file system are immediately flushed to disk and the respective write operation are being waited for .

>no\_root\_squash: by default any file request made by user root on the client machine is trated as by the user nobody on the server

(p4)

\*\*\*exports the shared directory using the following commands

#exportfs -r

Point notes –

Exportfs -v : display the list and shares files and export option on server

Exportsfs -a : exports all directories listed in /etc/exports exportsfs -u : unexports one or more directories .

Exportfs -r : reexport all directories after modifying /etc/exports

\*\*after configuring nfs server , we need to mount that shared directory in the NFS client

(P5)\*\*configuring firewall\*\*\*\*

We need to configure the firewall on the NFS server to allow NFS client to access the NFS share to do that , run the following commands on NFS Server .

#firewall-cmd --permanent - -add-service mountd

#firewall-cmd --permanent - - add-service rpc-bind

#firewall-cmd - -permanent - -add – service

#firewall -cmd –reload

Client side steps

\*\*\*\*Configure NFS Client \*\*\*\*\*

We need to install NFS package on NFS client to mount a remote NFS share Install NFS package , using below command

#yum install -y nfs-utils

\*\*\*check the NFS share \*\*\*

Before mounting the nfs share we need to required to check the nfs shares available on the NFS server by running the following command on NFS clients

(P6)

#showmount -e 176.168.0.10

Point noted-

1>showmount -e it will shows the available shares on your local machine (NFS Server)

2>showmount -e (server-ip or hostname ): list the available shares on the remote server .

\*\*\*mount NFS Server \*\*\*\*\*\*

Now create a directory on NFS client to mount the nfs share /Arjun which we have created in the NFS server .

#mkdir /mnt /Krishna

\*\* use below command to mount a nfs share /arjun form nfs server 176.168.0.10 in /mnt /Krishna on nfs client .

#mount 176.168.0.10:/arjun /mnt/Krishna

\*\*for the verifying the mounted share on nfs client using the mount command

#mount | grep nfs

\*\*Also we can use df -hT command for cheking the mounted nfs server

# df -hT

\*\* create the file on the mounted directory to verify the read and write access on the nfs share

# touch /mnt /Krishna/test

(P7)

\*\*\*\*\*Automount NFS Server \*\*\*

To mount the share automatically on query reboot you would need to modify /etc/fstab of your nfs client .

# vim /etc/fstab

\*\*add on something entry like below ,

198.0.0.10 :/arjun / mnt/Krishna nfs nosuid ,rw,sync,hard,intr 0 0

Now save and close .

Reboot the client machine and check weather the share is automatically mounted or not .

**(5) SSH \_ Port No 22 (**/etc/ssh/sshd\_config)

* **Password authentication (first way)**
  + Access from client server having same network
    - ssh <username >@<ip of remote server>
* **Key based authentication (2nd ways**
  + Access from host server, to push private key
    - Generate public and private keys (having 600 permission) by ‘ssh-keygen’
    - scp id\_rsa <client username>@<ip of client>:<path to place rsa\_root>
  + Access from client server, to get access of host through private key
    - ssh –i id\_rsa <host user name>@<ip of host user>

Note: - public key must be in ‘authorized\_keys’

- passwordAuthentication should be off

* **Applying port forwording**
  + Change port in configuration file and password Authentication should off
  + Add port and give forward porting access in firewall
    - Firewall-cmd - -add-forword-ports:port=22:proto=tcp:toport=<new port>
  + Apply client server command using ‘-p <port no.>’
  + SCManage should be get updated

For practical 2nd –

Go to - vim /etc/ssh/sshd\_config - escape: set nu ( for line number )

Go to line

18 – change port number according to requirement -

19 – only I want to give the access (range of network through – we can define -192.168.0.0

20- here we can only device that can access the only via remotely - ( 192.168.0.2) we could set as well this –

Go down – check whether – #LoginGraceTime 2M - uncomment this - LoginGraceTime 2M

#permitRootLogin Yes uncomment this – permitRootLogin Yes ( we can disable this so that root can not abel to access via ssh to server )

#sticktmodes yes uncomment sticktmodes no

#maxauthtries 6 uncoment maxautheries 3 ( we can set password verified interval )

#maxsessions 10 uncomment maxsessions 10 ( with the help of this we can increase and decrese machine session)

#passwordAuthenctication yes (if I don’t want ask for password while accessing device we can set here no) like this - #passwordAuthenctication no

Save it -----

Restart

Enable

Status

**(6)#Telnet**

To access Remote Device in Plain Text (unsecure form data travel)

**Port No . 23**

Go to server machine –

#ifconfig

#yum repolist

#yum install telnet \* -y (telnet client and telnet server will installed)

#yum install xinetd -y

#systemctl start telnet.socket

#systemctl enable telnet.socket

#telent 192.168.1.100

Connect to 192.168.1.100 (root by default disable hence we can not access via root user so that user normal user for connecting inside)

Localhost : preet

Password : 1234

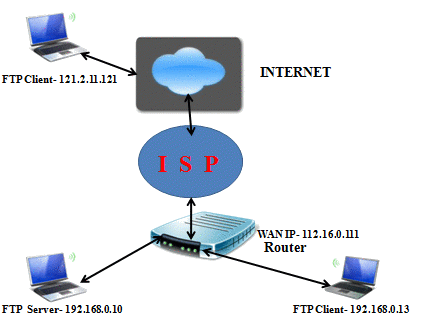
Access granted ..

**(7)FTP ( File transfer protocol ): -**

21- it is used for connection build

22 – it is used for the data transfer

FTP – used for the transfer of computer files from server to client on computer network



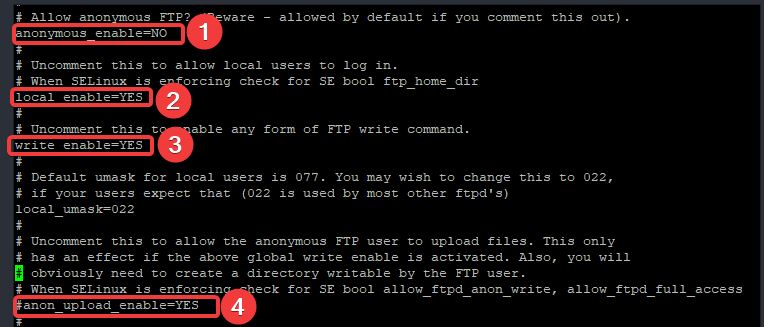
Note : first we have to test and ping both machine system (client and server ) .After that we would need to install vsftpd package on machine , with the help of yum install command .

(P1)#ping 8.8.8.8

#ping 192.168.0.13

#yum install vsftpd ftp -y

#vim /etc/vsftpd/vsftpd.conf



\*\*\*\*in configuration file we will need to be a make a changes to the configuration file in line 12,16,19,29 after that we will give into the kernel update with the help of systemctl-restart vsfdpd enable start command

(P2)

#systemctl restart vsftpd

#systemctl restart vsftpd

#systemctl enable vsftpd

\*\*\*after that we will move on ftp localhost as like database -center :-

#cd /Komal

#ftp localhost

\*\*\*in that Name ftp

Password – Nothing

Exit

\*\*\*\*On root we would need to create a one directory

#mkdir Komal /ram ( or ram)

#vim ram

#vim kom

#ftp local host

-exit

#cd /var/ftp

#mkdir /shyam

#ftp localhost

#cd Komal

#ftp local host

(P3)

\*\*\*\*\*\*\*\*\*after that we would need to be use setenforce and getenforce command for enhance security permition

#setenforce 0

#getenforce

\*getenforce is command for checking the permition is allocated or not

#cd /var/ftp

\*\*after that we would need to be give the full permition to the directory like as shyam

#ls

#chmod 777 shyam

#ls – ll

#cd

#cd Komal /ram (or ram )

#ftp local host

#cd shyam

#pwd

#ls

#put kom

\*\*\*\*put command is use for transferring the server data to data center

#ls

#exit

(P4)

If we want to transfer the data from database to server then we have need to process like this ,

#cd /var/ftp/shyam

#ls

#vim computer

#cd

#cd /ram

#cd shyam

#ls

#get computer

\*\*\*\*\*\* this command is use for the take a data from the dataset to server .

**(8)Port Forwarding**

Protocol port No 22 <ssh>-🡪 protocol Port No . 2222—its called port forwarding .(oprating same service in different port)

Go the machine ,

#firewall-cmd –list-all | grep forward --(it will give you sort way)

#firewall-cmd --help ( I will get more info about fort forwarding )

#firewall-cmd --help

#firewall-cmd –add-forward-port=port=22:proto=tcp:toport=2222 (hit enter) (this will only work for temp )

#firewall-cmd –add-forward-port=port=22:proto=tcp:toport=2222 --permanent ( this will work for permanent)

#sytemctl restart firewalld.service

#firwall–cmd --list-all ( check whether service is working or not )

**\*\*\*\*\*DHCP Configuration\*\*\*\*\***

https://www.youtube.com/watch?v=u\_QA0jakw\_U

**\*\*\*\*\*\*\*Configure Email Server using PostFix, Dovecot and Squirrel Mail in RHEL 7 (CentOS 7)\*\*\*\*\*\*\*\*\***

https://www.youtube.com/watch?v=RDaDqLlnev4

**\*\*\*\*\*DNS\*\*\*\*\***

https://www.youtube.com/watch?v=v-nrd2KuK4E&list=PLPTwEjck6TZ1wL0h-jOPLamWA-VTtdXHj&index=121

https://www.youtube.com/watch?v=VoEBl9eWfaU&list=PLPTwEjck6TZ1wL0h-jOPLamWA-VTtdXHj&index=122

**\*\*\*\*\*NIS\*\*\*\*\***

https://www.youtube.com/watch?v=g1SGfjcLu6A&list=PLPTwEjck6TZ1wL0h-jOPLamWA-VTtdXHj&index=94

https://www.youtube.com/watch?v=ePY8kckRU24&list=PLPTwEjck6TZ1wL0h-jOPLamWA-VTtdXHj&index=95

**\*\*\*\*\*\*IPV6\*\*\*\*\*\*\***

https://www.youtube.com/watch?v=tkVWrZdxNNY&list=PLPTwEjck6TZ1wL0h-jOPLamWA-VTtdXHj&index=88

**\*\*\* What does it mean by LDAP\*\*\*\*\*\*\***

https://www.youtube.com/watch?v=Xp9kLn9vRmw

**PART1\*\*\*\*\* ISCSI**

https://www.youtube.com/watch?v=QMfUpPDGhOg&list=PLPTwEjck6TZ1wL0h-jOPLamWA-VTtdXHj&index=75

**PART2 \*\*\*\*\*\*ISCSI**

https://www.youtube.com/watch?v=HiPzM07a3TM&list=PLPTwEjck6TZ1wL0h-jOPLamWA-VTtdXHj&index=76