(Server Configaration)

Proof of concept by Ramakrishna

##### TO CONFIGURE CLUSTERS ######

'Step 1:-To Configure Master Cluster'

(A)Configure 3 Web Servers in 3 PC's

Hostname: www.ramakrishna.com

IP's:-192.168.1.10 , 192.168.1.20 , 192.168.1.30

Gateway:- 192.168.1.150

(B)Required:2 LAN Card System

Assign the IP's As Given Below

ETH0: 200.200.200.100 (for WAN)

ETH1: 192.168.1.100 (for LAN)

# hostname master.ramakrishna.com (assign the hostname)

# vi /etc/sysconfig/network (to make host permanent)

(C)Enable Routing:-

# vi /etc/sysctl.conf (open this file)

Go to line no.7 & Change the Value '0' to '1'

:wq(save & quit the file)

# service network restart

'Step 2:-To Configure Slave Cluster'

(A)Required:2 LAN Card System

Assign the IP's As Given Below

ETH0: 200.200.200.200 (for WAN)

ETH1: 192.168.1.200 (for LAN)

# hostname slave.zoom.com (assign the hostname)

# vi /etc/sysconfig/network (to make host permanent)

(B)Enable Routing:-

# vi /etc/sysctl.conf (open this file)

Go to line no.7 & Change the Value '0' to '1'

:wq(save & quit the file)

# service network restart

'Step 3:-Do the Configuration in Master Cluster'

(A)Install the Packages:-

# yum install piranha\* sshd\* -y

(B)Generate Piranha User Password:-

# piranha-passwd

Password:-redhat

(C)Restart the Service:-

# service piranha-gui restart

# chkconfig piranha-gui on

(D)Run the Application & do configuration :-

# firefox http://127.0.0.1:3636

Username: piranha

Password: redhat

(E)Go to GLOBAL SETTINGS

Primary Server Public IP: 200.200.200.100

Primary Server Private IP: 192.168.1.100

NAT Router IP: 192.168.1.150

NAT Router Mask: 255.255.255.0

NAT Router Device: eth1:1

Click on ACCEPT

(F)Go to REDUNDANCY (for SLAVE)

Redundant Server Public IP: 200.200.200.200

Redundant Server Private IP: 192.168.1.200

HeartBeat Interval: 6

Assume Dead After : 18

HeartBeat Runs on Port: 539

Select the Option: Monitor NIC Links for Failure

Select the Option: Use Sync Dameon

Click on Accept

(G)Go to VIRTUAL SERVERS

Click on Add--->Activate--->Edit

Name: http

Port: 80

Virtual IP: 200.200.200.50

IP Netmask: 255.255.255.0

Device: eth0:1

Quiesce Server: YES

Click on Accept

(H)Go to REAL SERVER

Click on Add--->Actvate--->Edit

Name:- web1

Address: 192.168.1.10

Click on Accept

Click on Add--->Actvate--->Edit

Name:- web2

Address: 192.168.1.20

Click on Accept

Click on Add--->Actvate--->Edit

Name:- web3

Address: 192.168.1.30

Click on Accept

(I)Go to Control Monitoring

Select--->Auto Update

(J)Restart the Service:-

# service piranha-gui restart

# service pulse restart

(K)Go to Slave Server & Install the Packages:-

# yum install piranha\* sshd\* -y

(L)From Master Server Copy the Configuration file into Slave Server

# scp -rv /etc/sysconfig/ha/lvs.cf 200.200.200.200:/etc/susconfig/ha/lvs.cf

(M)Restart the Service in SLAVE SERVER:-

# service piranha-gui restart

# service pulse restart

**CRONJOB**

#crontab -e

#in that file

#54 21 19 08 1 tar -cvzf /opt/home.tar.gz /home

##########check it in #########3

# cd /opt

#ls

##54 =minute

##21 =hour

##19 =day

##08 = month

##01 =week

##############**Dump configuration**######################

###########Create a partition############

fdisk /dev/sda

:n

:enter

:+100MB

:w

#partprobe /dev/sda

#mkfs.ext4 /dev/sda8

#mkdir /part8

#mount /dev/sda8 /part8

#cd /part8

#touch a1 a2 a3 a4 a5

#cd

########Taking a full backup############

#dump -0uf /opt/full /part8

#restore -tf /opt/full

#cd /part8

#touch b1 b2 b3 b4 b5

#cd

########Taking a 1st Increamental backup#####

#dump -2uf /opt/1inc /part8

#restore -tf /opt/1inc

#cd /part8

#touch c1 c2 c3 c4 c5

#cd

#########Taking a 2nd Increamental backup######

#dump -3uf /opt/2inc /part8

#restore -tf /opt/2inc

##########Taking a differential backup#########

#dump -1uf /opt/diff /part8

#cd /part8

#ls

#####Remove all files#######################

#rm -rf \*

#restore -rf /opt/full

#ls

#restore -rf /opt/1inc

#restore -rf /opt/2inc

#ls

##############Dump configuration######################

###########Create a user#########

#useradd rose

#su - rose

$touch a1 a2 a3 a4

$exit

########Taking a full backup############

#dump -0uf /opt/full /home

#restore -tf /opt/full

#su - rose

$touch b1 b2 b3 b4 b5

$ls

$exit

########Taking a 1st Increamental backup#####

#dump -2uf /opt/1inc /home

#restore -tf /opt/1inc

#su - rose

$touch c1 c2 c3 c4 c5

$exit

#########Taking a 2nd Increamental backup######

#dump -3uf /opt/2inc /home

#restore -tf /opt/2inc

##########Taking a differential backup#########

#dump -1uf /opt/diff /home

# cd /home

#rm -rf \*

#restore -rf /opt/full

#ls

#restore -rf /opt/1inc

#restore -rf /opt/2inc

#ls

########## **TO CONFIGURE THE HTTPS** #########

first configure the http

#### Step 1 ### TO ASSIGN THE HOSTNAME #####

#hostname www.zoomgroup.com

# hostname ( to check )

#ifconfig ( to check the ip )

#vi /etc/hosts ( to provide the ip & hostname )

127.0.0.1 localhost.localdomain localhost

192.168.0.20 www.zoomgroup.com www

:wq ( save & quit )

#vi /etc/hostname ( to make permanent )

www.ramakrishnagroup.com

:wq ( save & quit )

#### Step 2 #### TO INSTALL THE PACKAGE ####

#yum install http\* mod\_ssl\* -y

#rpm -qa http\* mod\_ssl\* ( to query )

#### Step 3 ### TO CONFIGURE THE M.C.F OF HTTP #####

#vim /etc/httpd/conf/httpd.conf

come end of file

<VirtualHost \*:80>

ServerAdmin root@ramakrishnagroup.com

DocumentRoot /var/www/html

DirectoryIndex ramakrishnagroup.html

ServerName www.ramakrishnagroup.com

</VirtualHost>

:wq ( save & quit )

#cd /var/www/html ( To enter the dir )

#vi zoomgroup.html ( to create a home page )

#### Step 4 ### TO START THE SERVICE #####

#service httpd restart

#### Step 5 ### TO OPEN THE BROWSER ####

firefox http://www.zoomgroup.com

#### Step 6 ##### TO CREATE THE CERTIFICATES & KEY ######

#cd /etc/pki/tls/certs ( to enter the dir )

#make zoom.crt ( to create the certificates )

#ls ( to check )

#mv zoom.key /etc/pki/tls/private ( To move the key )

### Step 7 #### TO CONFIGURE THE M.C.F OF HTTPS ####

vim /etc/httpd/conf.d/ssl.conf

go to line 100 replace localhost.crt zoom.crt

go to line 107 replace localhost.key zoom.key

come end of file & add this parameter above the line last of file

above the line </VirtualHost> add this line

ServerAdmin root@ramakrishnagroup.com

DocumentRoot /var/www/html

DirectoryIndex ramakrishnagroup.html

ServerName www.ramakrishna.com

:wq ( save & quit )

#### Step 8 ### TO START THE SERVICE ####

service httpd restart

#### Step 9 ### TO OPEN THE BROWSER ####

firefox https://www.ramakrishna.com

### Step 10 ### TO REDIRECT HTTP TO HTTPS ####

vim /etc/httpd/conf/httpd.conf

come end of file

above the line </VirtualHost> add this line

Redirect / https://www.ramakrishna.com:443

:wq ( save & quit )

#service httpd restart ( to start the service )

#### Step 11 ### THEN OPEN THE BROWSER ###

firefox http://www.ramakrishna.com

#### Step 12 ## TO CHECK THE LOGFILES OF HTTP ###

tail /var/log/httpd/access\_log

### Step 13 ### TO CHECK THE LOGFILES OF HTTPS ###

tail /var/log/httpd/ssl\_access\_log

**IPv6**

#nmcli connection show

#nmcli connection modify eth0 ipv6.addresses 2001::9/64 ipv6.dns 2001::9 ipv6.method manual connection.autoconnect yes

#nmcli connection reload

#nmmcli connection up eth0

# ping6 2001::9

**FIREWALL**

########## **TO BLOCK ALL INCOMING TRAFFIC** #######

# vi firewall

iptables -F

iptables -A INPUT -j REJECT

:wq!

and check from client

########## TO ALLOW A IP ####

#vi firewall

iptables -F

iptables -A INPUT -s 192.168.1.20 -j ACCEPT

iptables -A INPUT -j REJECT

:wq!

and check from client

########## TO BLOCK A PORT #######

#vi firewall

iptables -F

iptables -A INPUT -p tcp --dport 22 -j REJECT

:wq!

and check from client

########## TO BLOCK A PORT #######

# vi firewall

iptables -F

iptables -A INPUT -s 192.168.1.10 -p tcp --dport 22 -j ACCEPT

iptables -A INPUT -p tcp --dport 22 -j REJECT

:wq!

and check from client

########## TO BLOCK THE MULTIPLE PORT #######

#vi firewall

iptables -F

iptables -A INPUT -m multiport -p tcp --dport 22,80 -j REJECT

:wq!

and check from client

########## TO BLOCK THE MULTIPLE PORT #######

#vi firewall

iptables -F

iptables -A INPUT -m multiport -s 192.168.1.20 -p tcp --dport 22,80 -j ACCEPT

iptables -A INPUT -m multiport -p tcp --dport 22,80 -j REJECT

:wq!

and check from client

To configure the ipv6 using ip tool

1. To assign the ipv6

ip -6 addr add dev eth0 2001::1/64

1. To check the ipv6

ip -6 addr show dev eth0

1. To assign the gateway

ip -6 route add dev eth0 2001::5

1. To check the gateway

ip -6 route show dev eth0

1. To remove the gateway

ip -6 route del dev eth0 2001::5

ip -6 route show dev eth0 ( to check )

1. To remove the ip

Ip -6 addr del dev eth0 2001::1/64

Ip -6 addr show deveth0 ( to check )

1. To assign the dns ipv6

vi /etc/resolv.conf

nameserver 2001::10

:wq ( save & quit )

1. To check the ping

ping6 2001::1

1. To browser the website

<http://[2001::8>]

To configure the ipv6 using ifconfig tool

1. To assign the ipv6

Ifconfig eth0 inet6 add 2001::1/64

1. To check the ipv6

Ifconfigeth0

1. To remove the ipv6

Ifconfig eth0 inet6 del 2001::1/64

Ifconfigeth0 ( to check the ip )

#######################**KERNEL UPGRADING**############################

# uname -a

#cd /opt

#scp -rv 192.168.50.250:/opt/kernel\*

#cd /opt

#rpm -ivh kernel\* --nodeps

#reboot

# select new kernel

# uname -a

####### **TO CONFIGURE THE SYSLOG SERVER** #####

#yum install rsyslog\*

#rpm -q rsyslog ( to query the pkg )

#vim /etc/rsyslog.conf ( to open the m.c.f )

go to line 15 16 19 & 20

then remove the #

:wq ( save & quit )

#service rsyslog restart ( to start the service )

##### TO CONFIGURE THE SYSLOG CLIENT ####

#vim /etc/rsyslog.conf ( to open the m.c.f )

go to line 90 & remove the #

then assign the syslog server ip

replace remote\_host to 192.168.50.48

:wq ( to save & quit )

#service rsyslog restart ( to start the service )

#useradd jack ( to create a user )

#su - jack

$exit

#### THEN CHECK FROM SYSLOG SERVER ####

#tail -f /var/log/secure

##### **TO CONFIGURE THE MYSQL DATABASE** ######

Step 1

##### TO INSTALL THE PACKAGE ######

yum groupinstall \*mariadb\* -y

rpm -qa maridb\* ( to query the pkgs )

#### Step2 ### TO START THE SERVICE #####

service mariadb restart

#### Step 3 #### TO ASSIGN THE PASSWORD FOR MYSQL DATABASE ####

mysqladmin -u root password redhat

#### Step 4 #### TO LOGIN INTO MYSQL DATABASE #####

mysql -u root -p

-------- OUTPUT --------

password: assign the password

##### Step 5 ##### TO SHOW THE MYSQL DATABASE #########

MariaDB(none)> show databases;

-------- OUTPUT --------

+--------------------+

| Database |

+--------------------+

| information\_schema |

| mysql |

| test |

+--------------------+

3 rows in set (0.00 sec)

###### Step 6 #### TO CREATE A DATABASE ######

<MariaDB(none)>creat database zoom;

-------- OUTPUT --------

Query OK, 1 row affected (0.00 sec)

##### Step 7 #### TO CHECK THE DATABASE ######

MariaDB(none)> show databases;

#### Step 8 #### TO ENTER THE DATABASE ######

MariaDB(none)> use zoom;

#### Step 9 ### TO DISPLAY THE DATABASE TABLE ####

MariaDB> show tables;

-------- OUTPUT --------

Empty set (0.00 sec)

##### Step 10 ##### TO CREATE A TABLE WITH FIELDS #######

MariaDB(none)> create table linux (Name varchar(20) not null, Phone varchar(10), Status varchar(10));

-------- OUTPUT --------

Query OK, 0 rows affected (0.07 sec)

###### Step 11 #### TO SHOW THE TABLE ######

MariaDB(none)> show tables;

-------- OUTPUT --------

+----------------+

| Tables\_in\_zoom |

+----------------+

| linux |

+----------------+

1 row in set (0.00 sec)

##### Step 13 ##### TO DISPLAY THE TABLE FIELDS #######

MariaDB(none)>describe linux;

-------- OUTPUT --------

+--------+-------------+------+-----+---------+-------+

| Field | Type | Null | Key | Default | Extra |

+--------+-------------+------+-----+---------+-------+

| Name | varchar(20) | NO | | NULL | |

| Phone | varchar(10) | YES | | NULL | |

| Status | varchar(10) | YES | | NULL | |

+--------+-------------+------+-----+---------+-------+

3 rows in set (0.00 sec)

##### Step 14 ###### TO ADD VALUES TO FIELDS IN TABLE ######

MariaDB(none)> insert into linux (Name,Phone,Status) values("jack",9944337755,"sales");

MariaDB(none)> insert into linux (Name,Phone,Status) values("rose",9849112244,"finance");

-------- OUTPUT --------

Query OK, 1 row affected, 1 warning (0.00 sec)

#### Step 15 #### TO DISPLAY THE VALUES FROM TABLE ######

MariaDB(none)> select \* from linux;

-------- OUTPUT --------

+-------+------------+--------+

| Name | Phone | Status |

+-------+------------+--------+

| jack | 9944337755 | sales |

| rose | 9849112244 |finance |

+-------+------------+--------+

1 row in set (0.00 sec)

##### Step 16 ###### TO CHECK THE PARTICULAR ROW #######

MariaDB>select \* from linux where Name="jack";

-------- OUTPUT --------

+-------+------------+--------+

| Name | Phone | Status |

+-------+------------+--------+

| jack | 9944337755 | sales |

+-------+------------+--------+

1 row in set (0.00 sec)

###### Step17 #### TO REMOVE THE PARTICULAR ROW FROM TABLE #####

MariaDB> delete from linux where Name="jack";

-------- OUTPUT --------

Query OK, 1 row affected (0.00 sec)

#### Step 18 #### TO DISPLAY THE TABLE ######

MariaDB> select \* from linux;

-------- OUTPUT --------

+-------+------------+--------+

| Name | Phone | Status |

+-------+------------+--------+

| rose | 9849112244 |finance |

+-------+------------+--------+

1 row in set (0.00 sec)

MariaDB>exit ( to come out from mysql database )

###### Step 19 ##### TO TAKE THE BACKUP FROM MYSQL DATABASE ######

#cd /var/lib/mysql ( to enter the dir )

#ls ( to check the contains )

#mysqldump -u root -p zoom > /mnt/zoomback.sql ( to take the backup )

-------- OUTPUT --------

Enter password: assign the password

#cd /mnt ( to enter the dir )

#ls ( to check the backup file )

###### Step 20 ##### TO REMOVE THE MYSQL DATABASE ########

#mysql -u root -p

-------- OUTPUT --------

password: assign the password

MariaDB>drop database zoom;

-------- OUTPUT --------

Query OK, 2 rows affected (0.00 sec)

MariaDB>exit ( to come out from mysql database )

##### Step 21 ###### TO ENTER THE DATABASE DIR LOCATION #####

#cd /var/lib/mysql ( to enter the dir )

#ls ( to check the db dir )

#### Step 22 ##### TO RESTORE THE BACKUP DATABASE ######

#mysql -u root -p

-------- OUTPUT --------

password: assign the password

##### Step 23 #### TO RESTORE CREATE A NEW DATABASE #####

MariaDB>create database new\_zoom; ( to create the database )

-------- OUTPUT --------

Query OK, 2 rows affected (0.00 sec)

MariaDB>exit ( to come out from mysql db )

###### TO Step 24 #### TO ENTER THE MYSQL DATABASE LOCATION #####

# cd /var/lib/mysql

#mysql -u root -p new\_zoom < /mnt/zoomback.sql

-------- OUTPUT --------

Enter password: assign the password

#ls ( to check the contains )

#cd new\_zoom ( To enter the db dir )

#ls ( to check the restore files )

##### TO Step 25 ##### TO CHECK THE RESTORE DB INTO MYSQL DB #####

#mysql -u root -p

-------- OUTPUT --------

password: assign the password

#### Step 26 ### TO DISPLAY THE DATABASE #####

MariaDB>use new\_zoom; ( to enter the db )

MariaDB>show tables; ( to check the table )

MariaDB>describe linux; ( to check the fields )

MariaDB>select \* from linux;

##### **TO CONFIGURE NAGIOS MONITORING TOOL** #####

'Step 1:-Check the Ip & Assign the Hostname'

# ifconfig (to check ip)

# hostname nagios.zoom.com

# vi /etc/hosts (provide the entry in host file)

192.168.0.1 nagios.zoom.com nagios

:wq!

# vi /etc/hostname (to make host permanent)

#nagios.zoom.com

'Step 2:-Install the Dependencies for Nagios'

# yum install http\* gcc\* php\* glib\* gd\* --skip-broken -y

'Step 3:-Create Nagios System User & Group'

# useradd nagios

# passwd nagios (assign the password:1)

# groupadd nagcmd

'Step 4:-Make nagcmd group as a Secondary for User:nagios,apache'

# usermod -G nagcmd nagios

# usermod -G nagcmd apache

'Step 5:-Install Nagios Application'

Download & Move the Application Directory or File in /opt location

# cd /opt

# ls (for to check)

# tar -xvzf nagios-4.0.7.tar.gz (to uncompress & extract)

# ls (to check)

# cd nagios-4.0.7 (access dir)

# ./configure --with-command-group=nagcmd

# make all

# make install

# make install-init

# make install-config

# make install-commandmode

# make install-webconf

'Step 5:-Provide the Email Address in the File'

# vim /usr/local/nagios/etc/objects/contacts.cfg

Go to line no.34 & Change the Email ID for Alerts

For example:- root@zoom.com (save & quit the file)

'Step 6:-Create Nagios Admin Account for Acessing Application'

# htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

Password: redhat (for example)

# service httpd restart

# systemctl enable httpd.service

'Step 7:-Install Nagios Plugins'

# cd .. (come one step back)

# ls (to check)

# tar -xvzf nagios-plugins-2.0.2.tar.gz

# cd nagios-plugins-2.0.2 (access dir)

# ./configure --with-nagios-user=nagios --with-nagios-group=nagios

# make

# make install

'Step 8:-Verify the Configuration & Start Nagios Service'

# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

# service nagios start

# chkconfig --add nagios

# chkconfig nagios on

'Step 9:-Access Nagios Application'

# firefox http://nagios.zoom.com/nagios

Username:nagiosadmin Password:redhat

'Step 10:-To Add Host & Services'

# vim /usr/local/nagios/etc/objects/localhost.cfg

Copy the lines from line no.24 to 31 (i.e, 8 lines) & Paste at the last of the file & do the changes as given below:-

( For Example we have a ftp server running on 192.168.0.25 ip)

define host{

use linux-server

host\_name ftp.zoom.com

alias ftp.zoom.com

address 192.168.50.250

}

:wq(save & quit the file)

# service nagios restart

To Check:-Go to Nagios Web Interface & Select the Option:Hosts from left side

'To Add the service (for ex:ftp) based on above Host'

# vim /usr/local/nagios/etc/objects/localhost.cfg

Copy the lines from line no.149 to 155 (i.e, 7 lines) & Paste at the last of the file & do the changes as given below:-

define service{

use local-service

host\_name ftp.zoom.com

service\_description FTP

check\_command check\_ftp

notifications\_enabled 0

}

:wq(save & quit the file)

# service nagios restart

To Check:-Go to Nagios Interface & Select the Option:services from left side

**Configuration of ipv6**

1. Check for ipv6 support in the current running kernel

#test -f /proc/net/if\_inet6 && echo "Running kernel is IPv6 ready”

1. To try to load ipv6 module

You can try to load the IPv6 module executing

# modprobe ipv6

If this is successful, this module should be listed, testable with following auto-magically line:

# lsmod |grep -w 'ipv6' && echo "IPv6 module successfully loaded"

And the check shown above should now run successfully.

Note: unloading the module is currently not supported and can result, under some circumstances, in a kernel

1. Ipv6 testing & debugging programms

To check the pinging

# ping6 2001::1

To check the traceroute

# traceroute6 [www.google.com](http://www.google.com)

To check the tracepath

# tracepath6 [www.google.com](http://www.google.com)

To check the tcpdump

#tcpdump -t -n -i eth0 -s 512 -vv ip6 or proto ipv6

To check the dns

# host -t AAAA [www.zoom.com](http://www.zoom.com)

To check the telnet

# telnet www.zoom.com 80

To check the ssh

# ssh -6 2001::1

To check the browser

#http://[2001::1]

1. To disable the nic card using the ip tool

# ip link set dev eth0 up

1. To enable the nic card using the ip tool

# ip link set dev eth0 down

6. To disable the nic card using the ifconfig tool

# ifdown eth0

7. To enable the nic card using the ifconfig tool

# ifup eth0

8. To access the /proc filesystem

#CONFIG\_PROC\_FS=y

# cat /proc /sys/net/ipv6/conf/all/forwarding

# echo “1” > /proc/sys/net/ipv6/conf/all/forwarding

To configure the webserver on ipv6

Vim /etc/httpd/conf/httpd.conf ( to open the m.c.f )

Come end of file

<VirtualHost [2001::1]:80>

ServerAdmin [root@zoom.com](mailto:root@zoom.com)

DocumentRoot /var/www/html

DirectoryIndex zoom.html

ServerName [www.zoom.com](http://www.zoom.com)

</VirtualHost>

:wq ( save & quit )

# service httpd restart ( to start the service )

# firefox <http://[2001::1>]

To configure the dns server on ipv6

/etc/named.conf

listen-on-v6 { any; };

:wq ( save & quit )

Cd /var/named ( to enter the dir )

Vi zoom.for ( to configure the f.l.z )

$TTL 1D

@ IN SOA dns.zoom.com. rname.invalid. (

1. ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

NS dns.zoom.com.

dns AAAA 2001::1

:wq ( save & quit )

service named restart ( to start the service )

#dig dns.zoom.com ( to check the f.l.z )

#host -t aaaa [dns.zoom.com](http://www.zoom.com) 2001::1

Then check from client side

vi /etc/resolv.conf ( to provide the dns ip )

nameserver 2001::1

:wq ( save & quit )

Ping6 dns.zoom.com

To configure the dhcp server

1. Vi /etc/dhcp

interface eth0 {

server-preference 255;

renew-time 60;

rebind-time 90;

prefer-life-time 130;

valid-life-time 200;

allow rapid-commit;

option dns\_servers 2001:db8:0:f101::1 sub.domain.example;

link AAA {

range 2001:db8:0:f101::1000 to 2001:db8:0:f101::ffff/64;

prefix 2001:db8:0:f101::/64;

};

};

##### **TO CONFIGURE THE NTP SERVER** ######

first check the date & time of pc

syste-config-date ( to check the date & time )

it should be correct according our time zone ist

#### Step 1 #### TO ASSIGN THE HOSTNAME #####

#hostname ntp.zoom.com

#hostname ( To check the hostname )

#ifconfig ( to check the ip )

#vi /etc/hosts ( to provide the ip & hostname )

192.168.0.1 ntp.zoom.com ntp

:wq ( save & quit )

vi /etc/hostname ( to make permanent )

ntp.zoom.com

:wq ( save & quit )

#### Step 2 ### TO INSTALL THE PACKAGE ####

yum install ntp\* -y

rpm -qa ntp\* ( To query the pkg )

### Step 3 ### TO CONFIGURE THE M.C.F #####

vi /etc/ntp.conf ( to open the m.c.f )

go to line 18

18 restrict 192.168.50.0 mask 255.255.255.0 nomodify notrap nopeer

server 127.127.1.0 iburst

:wq ( save & quit )

#### Step 4 ### TO START THE SERVICE ####

#service ntpd restart

######## THEN CHECK FROM CLIENT SIDE ####

#date

#ntpdate -u 192.168.0.1 ( To assign the ntp server ip)

##### **TO** **INSTALL THE ORACLE IN LINUX** #########

Step 1

Note---> /home partitions siz should be 10GB or MORE

##### TO CREATE A PARTITION ######

fdisk /dev/sda

press n ( to create a new partition )

press enter ( to take default cylinders

press +20G ( to create a partition )

press p ( to check the partition )

press w ( to save & quit )

partx -a /dev/sda ( to update the kernel )

#### Step 2 ### TO FORMAT THE PARTITION ####

mkfs.ext4 /dev/sda8

##### Step 3 ### TO ASSIGN THE MOUNT POINT ####

mkdir -p /0u1/app/orcale ( to create the parent dir )

mount /dev/sda8 /0u1/app/orcale ( to assign the m.p )

mount ( to check the m.p )

##### Step 4 #### TO PROVIDE THE PERMISSION ####

chmod 775 /0u1/app/orcale

ls -ld /0u1/app/orcale ( to check the permission )

#### Step 5 ### TO INSTALL THE PACKAGE #####

yum install gcc\* glib\* comp\* openmotif\*

#### Step 6 #### TO CREATE A USER #####

useradd oracle

tail /etc/passwd ( to check the user )

#### Step 7 ### TO ASSIGN THE PASSWORD #####

passwd oracle

tail /etc/shadow

#### Step 8 #### TO CREATE THE GROUPS ####

groupadd dba

groupadd oinstall

#### Step 9 #### TO MAKE A PRIMARY GROUP OF USER ####

usermod -g oinstall oracle

groups orcale ( to check the primary group )

#### Step 10 ### TO MAKE SECONDARY GROUP OF USER ####

usermod -G dba oracle

#### Step 11 #### TO UNCOMPRESS THE ORACLE APPLICATION

cd /opt ( to enter the dir )

ls ( to check the oracle app )

unzip linux\*

ls ( to check )

#### Step 12 ### TO PROVIDE THE PERMISSION FOR DATABASE DIR ###

chmod -R 777 database

ls -ld database ( to check the dir )

#### Step 13 #### TO CHECK THE LOGIN ORACLE USER IN GRAPHICAL INTERFACE ####

gdmflexviserver

then login oracle user

#### Step 14 #### TO INSTALL THE ORACLE APPLICATION ####

cd /opt/database

ls ( to check the files )

./runInstaller ( to install the oracle )

**PROXY SERVER**

##### STEP1 ASSIGN ISP DNS #####

#vi /etc/resolv.conf

nameserver 192.168.50.250

:wq!

#### STEP 2 CHECK AND INSTALL THE PACKAGES ##########

#rpm -qa squid\*

#yum install squid\* -y

#### step 3 EDIT THE CONFIGURATION FILE ##############

#vim /etc/squid/squid.conf

go to line no 13 add your rule

acl zoom\_network src 192.168.50.0/24

http\_access allow zoom\_network

:wq(save & quit )

#service squid restart

###################GO TO CLIENT SIDE#################################

OPEN WEB SERVER

firefox &

go to EDIT ---> PREFERENCES--->ADVANCE--->NETWORK--->SETTINGS

check manually proxy tab

assign proxy server ipaddress and port no 3128

#### STEP 4 TO BLOCK A PARTICULAR WEB SITE #####

again open configuaration file

"open again configuration file and add above of the previous rules"

acl zoom1 url\_regex www.yahoo.com

http\_access deny zoom1

:wq!

#service squid restart

##################GO TO CLIENT SIDE AND CHECK IT#############################

open browser

http://www.yahoo.com

#### STEP 5 TO BLOCK PARTICULAR IP ADDRESS ###########

"open again configuration file and add above of the previous rules"

acl zoom2 src 192.168.50.10

http\_access deny zoom2

:wq!

#service squid restart

##################GO TO CLIENT SIDE AND CHECK IT#############################

open browser

http://www.yahoo.com, gmail,bmw

############BLOCK THE MULTIPLE IPS######################

vi /ip

192.168.50.10

192.168.50.11

192.168.50.12

:wq!

"open again configuration file and add above of the previous rules"

#vi /etc/squid/squid.conf

acl zoom3 src "/ip"

http\_access deny zoom3

:wq!

#service squid resart

##################GO TO CLIENT SIDE AND CHECK IT#############################

open browser

http://www.yahoo.com, gmail,bmw

##############BLOCK THE MULTIPLE WEBSITE#############

#vi /web

www.yahoo.com

www.gmail.com

www.zooom.com

:wq!

"open again configuration file and add above of the previous rules"

#vi /etc/squid/squid.conf

acl zoom4 url\_regex "/web"

http\_access deny zoom4

:wq!

#service squid restart

##################GO TO CLIENT SIDE AND CHECK IT#############################

open browser

http://www.yahoo.com, gmail,bmw

###############TO BLOCK THE PORT #####################

acl rule5 port 80

http\_access deny rule5

:wq!

#service squid restart

##################GO TO CLIENT SIDE AND CHECK IT#############################

open browser

http://www.yahoo.com, gmail,bmw

ftp://192.168.50.250

### Step 4 CHECK THE OUTPUT AT CLIENT SIDE ######

#################TO ALLOW PARTICULAR TIME##########################3

#vi /etc/squid/squid.conf

acl zoom6 time S M T W H F A 9:30-17:30

http\_access allow zoom6

:wq!

#service squid restart

##################GO TO CLIENT SIDE AND CHECK IT#############################

open browser

http://www.yahoo.com, gmail,bmw

####################TO BLOCK THE PARTICULAR TIME########################

#vi /etc/squid/squid.conf

acl rule7 time S M T W H F A 13:00-14:30

http\_access deny rule7

:wq!

# service squid restart

##################GO TO CLIENT SIDE AND CHECK IT#############################

open browser

http://www.yahoo.com, gmail,bmw

###################TO BLOCK PARTICULAR MAC ADDRESS########################3

#vi /etc/squid/squid.conf

acl rule8 arp 00:DA:23:98:CA:11

http\_access deny rule8

:wq!

#service squid restart

######################GO TO CLIENT SIDE############################

open the browser

http://www.zoomgroup.com

####### **TO CONFIGURE THE PXE SERVER** ######

yum install dhcp tftp tftp-server syslinux \*tftpboot\* wget vsftpd

##### TO CONFIGURE THE DHCP SERVER ####

vim /etc/dhcp/dhcpd.conf

# DHCP Server Configuration file.

# see /usr/share/doc/dhcp\*/dhcpd.conf.example

# see dhcpd.conf(5) man page

#

# option definitions common to all supported networks...

ddns-update-style interim;

ignore client-updates;

authoritative;

allow booting;

allow bootp;

allow unknown-clients;

# A slightly different configuration for an internal subnet.

subnet 192.168.0.0 netmask 255.255.255.0 {

range 192.168.0.50 192.168.0.253;

option domain-name-servers 192.168.0.199;

option domain-name "server1.example.com";

option routers 192.168.0.199;

option broadcast-address 10.5.5.31; #not important

default-lease-time 600;

max-lease-time 7200;

# PXE SERVER IP

next-server 192.168.50.199; # DHCP server ip

filename "pxelinux.0";

}

:wq ( save & quit )

##### TO CONFIGURE THE TFTP SERVER #####

#vi /etc/xinetd.d/tftp

service tftp

{

socket\_type = dgram

protocol = udp

wait = yes

user = root

server = /usr/sbin/in.tftpd

server\_args = -s /tftpboot

disable = no

per\_source = 11

cps = 100 2

flags = IPv4

}

:wq ( save & quit )

##### TO CONFIGURE THE TFTP SERVICE FOR NETWORK BOOT FILES ###

#mkdir /tftpboot/pxelinux.cfg ( to create a dir )

#mkdir /tftpboot/netboot

#cd /tftpboot ( to enter the dir )

#ls ( to check the dirs )

then copy the os into /var/ftp/pub

##### COPY INTRD.IMG & VMLINUZ INTO /TFTPBOOT/NETBOOT ###

#cp /var/ftp/pub/centos7/images/pxeboot/vmlinuz /tftpboot/netboot

#cp /var/ftp/pub/centos7/images/pxeboot/initrd.img /tftpboot/netboot

#### CREATE A NEW KICKSTART FILE ####

#vi /var/ftp/pub/centos7/ks7auto.cfg

#platform=x86, AMD64, or Intel EM64T

#version=DEVEL

# Firewall configuration

firewall --disabled

# Install OS instead of upgrade

install

# Use network installation

url --url="ftp://192.168.50.250/pub/centos7"

# Root password

rootpw --iscrypted $1$.Wn.ZraS$NMLCQlEDlwXkkYEUaoT1P0

# System authorization information

auth --useshadow --passalgo=sha512

# Use graphical install

graphical

firstboot --disable

# System keyboard

keyboard us

# System language

lang en\_US

# SELinux configuration

selinux --disabled

firewall --disabled

# Installation logging level

logging --level=info

# Reboot after installation

reboot

# System timezone

timezone Asia/Kolkata

# Network information

network --bootproto=dhcp --onboot=on

# System bootloader configuration

bootloader --location=mbr

# Partition clearing information

clearpart --all

# Disk partitioning information

#part /boot --fstype="ext4" --size=200

#part / --fstype="ext4" --size=12000

#part /home --fstype="ext4" --size=2000

#part /var --fstype="ext4" --size=12000

#part /usr --fstype="ext4" --size=10000

#part swap --fstype="swap" --size=4000

%packages

@base

@core

@desktop-debugging

@dial-up

@directory-client

@fonts

@gnome-desktop

@guest-agents

@guest-desktop-agents

@input-methods

@internet-browser

@multimedia

@network-file-system-client

@x11

chrony

%end

%post

%end

:wq ( save & quit )

##### TO CREATE PXE MENU FILE #####

# cd /tftpboot/pxelinux.cfg

vi default

default menu.c32

prompt 0

timeout 30

MENU TITLE unixme.com PXE Menu

LABEL centos7\_x64

MENU LABEL CentOS 7 X64

KERNEL /netboot/vmlinuz

APPEND initrd=/netboot/initrd.img inst.repo=ftp://192.168.50.250/pub/centos7 ks=ftp://192.168.50.250/pub/centos7/ks7auto.cfg

###########Give full permission#############

#chmod 777 -R /tftpboot

##### TO START THE SERVICE ####

#service dhcpd restart

#service xinetd restart

#service vsftpd restart

#### THEN CHECK FROM CLIENT SIDE ###

boot the client pc from nic card

###### **TO CONFIGURE THE SAMBA SERVER** #####

#useradd tom ( to create a user )

#tail /etc/passwd ( to check the user )

#mkdir /zoom ( to create a dir )

#cd /zoom ( to enter the dir )

#touch linux unix ccna ccnp ( to create the files )

#ls ( to check )

#### Step 1 ##### TO ASSIGN THE HOSTNAME ####

#hostname samba.zoom.com

vi /etc/hostname ( to open the file )

samba.zoom.com

:wq ( save & quit )

vi /etc/hosts ( to provide the ip & hostname )

192.168.0.1 samba.zoom.com samba

:wq ( save & quit )

#### Step 2 #### TO INSTALL THE PACKAGE ####

yum install samba\*

rpm -qa samba\* ( to query the pkg )

#### Step 3 ### TO CONFIGURE THE M.C.F #####

vim /etc/samba/smb.conf ( to open the m.c.f )

come end of file & copy the last 7 lines & paste

then remove the ;

[linux]

comment = Public Stuff

path = /zoom

valid users = tom jerry

public = yes

writable = yes

printable = no

write list = +staff

:wq ( save & quit )

#### Step 4 #### TO START THE SERVICE #####

#service smb restart

##### Step 5 #### TO ASSIGN THE SAMBA PASSWORD ####

#smbpasswd -a tom

#### Step 6 #### TO CHECK THE TESTING TOOL ###

#testparm

##### Step 7 #### TO CHECK FROM WINDOWS CLIENT ##

click > start > run

\\192.168.50.1\linux ( to assign the samba server ip & sharname )

then provide the username & password of samba server

#### Step 8 ### TO SHARE BETWEEN WINDOWS TO LINUX #

create a folder & create the files inside

then provide the sharing permission

#### Step 9 ### TO CHECK FROM LINUX MACHINE ###

#mount //192.168.50.120/windows /mnt -o username=administrator ( to provide the windows ip & sharename & username with m.p )

#mount ( to check the m.p )

#cd /mnt ( to enter the m.p )

#ls ( to check the files )

#### Step 10 ### TO SHARE FILE LINUX TO LINUX ###

#mount //192.168.50.1/linux /mnt -o username=tom ( to provide the samba server ip & sharename & username with m.p )

#mount ( to check the m.p )

#cd /mnt ( to enter the m.p )

#ls ( to check the file )

###############**Configure of pdc**#################33

#hostname pdc.zoom.com

#vi /etc/hostname

pdc.zoom.com

:wq!

#vi /etc/hosts

192.168.0.1 pdc.zoom.com pdc

:wq!

#yum install samba\*

#rpm -qa samba\*

#useradd jack

#passwd jack

a

a

###############M.C.F###################

#vi /etc/samba/smb.conf

In line no89 enter ZOOM.COM

and in Domain controler option

remove semi-colons line no 175 to 198

:wq!

################Assign the samba password############

#smbpasswd -a root

123 enter

123 enter

#smbpasswd -a jack

123 enter

123 enter

#service smb restart

#service nmb restart

##################Go to windows computer ################################

#right click on mycomputer-->click on computername-->click on change-->assign

domain name zoom.com --->ok assign root and passwd 123 -->ok-->ok

restart the computer and assign name jack and assign password and click on options select domain name and login

##########################################

######### **TO CONFIGURE THE WINBIND** ######

first we need active directory server on windows 2012

Example = domain : zoomgroup.com

FQDN : ad.zoomgroup.com

dns : 192.168.50.120

ad ip : 192.168.50.120

second we need a linux pc to install winbind

#### Step 1 ### TO ASSIGN THE HOSTNAME #####

#hostname client.zoomgroup.com

#hostname ( to check the hostname )

#ifconfig ( to check the ip )

#vi /etc/hosts ( to provide the ip & hostname )

192.168.50.10 client.zoomgroup.com client

:wq ( save & quit )

#vi /etc/sysconfig/network ( to make permanent )

HOSTNAME=client.zoom.com

:wq ( save & quit )

#############DNS IP IN client###########

# vi /etc/resolv.conf

nameserver 192.168.50.120

:wq!

##### Step 2 #### TO INSTALL THE PACKAGE ####

#yum install samba\* oddjob\* -y

#rpm -qa samba\* oddjob\* ( to query the pkg )

#service smb restart ( to start the service )

##### Step 3 ### TO CONFIGURE THE M.C.F ####

#authconfig-tui

┌────────────────┤ Authentication Configuration ├─────────────────┐

│ │

│ User Information Authentication │

│ [ ] Cache Information [\*] Use MD5 Passwords │

│ [ ] Use LDAP [\*] Use Shadow Passwords │

│ [ ] Use NIS [ ] Use LDAP Authentication │

│ [ ] Use IPAv2 [ ] Use Kerberos │

│ [\*] Use Winbind [\*] Use Fingerprint reader │

│ [\*] Use Winbind Authentication │

│ [\*] Local authorization is sufficient │

│ │

│ ┌────────┐ ┌──────┐ │

│ │ Cancel │ │ Next │ │

│ └────────┘ └──────┘ │

│ │

│ │

└─────────────────────────────────────────────────────────────────┘

┌─────────────────────┤ Winbind Settings ├─────────────────────┐

│ │

│ Security Model: (\*) ads │

│ ( ) domain │

│ Domain: ZOOMGROUP\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ │

│ Domain Controllers: AD.ZOOMGROUP.COM\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ │

│ ADS Realm: ZOOMGROUP\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ │

│ Template Shell: ( ) /sbin/nologin │

│ ( ) /bin/sh │

│ (\*) /bin/bash │

│ ( ) /bin/tcsh │

│ │

│ ┌──────┐ ┌─────────────┐ ┌────┐ │

│ │ Back │ │ Join Domain │ │ Ok │ │

│ └──────┘ └─────────────┘ └────┘ │

│ │

│ │

└──────────────────────────────────────────────────────────────┘

┌─────────────────────┤ Winbind Settings ├─────────────────────┐

│ │

│ ┌─────────────────┤ Save Settings ├──────────────────┐ │

│ │ │ │

│ │ Some of the configuration changes you've made │ \_\_ │

│ Dom│ should be saved to disk before continuing. If you │ \_\_ │

│ │ do not save them, then your attempt to join the │ \_\_ │

│ │ domain may fail. Save changes? │ │

│ │ │ │

│ │ ┌────┐ ┌─────┐ │ │

│ │ │ No │ │ Yes │ │ │

│ │ └────┘ └─────┘ │ │

│ │ │ │

│ │ │ │

│ └────────────────────────────────────────────────────┘ │

│ │

│ │

└──────────────────────────────────────────────────────────────┘

┌─────────────────────┤ Winbind Settings ├─────────────────────┐

│ │

│ Security Model: (\*) ads │

┌───────────────────────┤ Join Settings ├────────────────────────┐

│ │

│ Domain Administrator: Administrator\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ │

│ Password: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ │

│ │

│ ┌────────┐ ┌────┐ │

│ │ Cancel │ │ Ok │ │

│ └────────┘ └────┘ │

│ │

│ │

└────────────────────────────────────────────────────────────────┘

│ │

│ │

└──────────────────────────────────────────────────────────────┘

┌─────────────────────┤ Winbind Settings ├─────────────────────┐

│ │

│ Security Model: (\*) ads │

│ ( ) domain │

│ Domain: ZOOMGROUP\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ │

│ Domain Controllers: AD.ZOOMGROUP.COM\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ │

│ ADS Realm: ZOOMGROUP\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ │

│ Template Shell: ( ) /sbin/nologin │

│ ( ) /bin/sh │

│ (\*) /bin/bash │

│ ( ) /bin/tcsh │

│ │

│ ┌──────┐ ┌─────────────┐ ┌────┐ │

│ │ Back │ │ Join Domain │ │ Ok │ │

│ └──────┘ └─────────────┘ └────┘ │

│ │

│ │

└──────────────────────────────────────────────────────────────┘

[/usr/bin/net join -w ZOOMGROUP -S AD.ZOOMGROUP.COM -U Administrator]

Enter Administrator's password:<...>

Joined domain ZOOMGROUP.

##### Step 4 #### TO CREATE A DIR WITH DOMAIN NAME IN /HOME #

#vi /etc/pam.d/system-auth-ac

session required pam\_mkhomedir.so skel=/etc/skel umask=0022

:wq!

#mkdir -p /home/ZOOMGROUP/user1 ( to create a dir )

#chmod 777 -R /home/ZOOMGROUP ( to provide the permission )

##### Step 5 ### TO START THE SERVICE ####

#service smb restart

#service winbind restart

#service oddjobd restart

##### Step 6 ### TO CHECK THE AD USERS ####

#wbinfo -u

#### Step 7 ### TO LOGIN WITH AD USER #####

#su - user1@zoomgroup.com

**SAN STORAGE**

##### TO INSTALL THE PACKAGE ####

yum install targetcli\* -y

##### TO CONFIGURE THE ISCSI TARGET ####

mkdir /iscsi\_disks ( to create a dir )

#### TO ENTER THE ADMIN CONSOLE #####

targetcli

#### TO CREATE A DISK IMAGE ####

cd backstores/fileio ( to enter the dir )

create disk01 /iscsi\_disks/disk01.img 20G

cd /iscsi ( to enter the dir )

##### TO CREATE A TARGET #####

create iqn.2015-08.zoom.com:target1

cd /iscsi/iqn.2015-08.zoom.com:target1/tpg1/portals

create 192.168.50.1 ( set the ip to target )

cd ../luns

##### TO CREATE A LUN ####

create /backstores/fileio/disk01

cd ../acls

#### TO CREATE A ACL #####

create iqn.2015-08.zoom.com:acl

cd iqn.2015-08.zoom.com:acl ( to enter the dir )

#### TO PROVIDE THE AUTHENTICATION ###

set auth userid=tom

set auth password=a

exit ( to come out )

#### TO CHECK THE SAN ####

netstat -lnp | grep 3260

###### TO CHECK FROM CLIENT SIDE #####

yum install \*scsi\* -y

##### TO PROVIDE THE ISCSI SERVICE #####

vi /etc/iscsi/initiatorname.iscsi

InitiatorName=iqn.2015-08.zoom.com:acl

:wq!

#### TO PROVIDE THE ISCSI AUTHENTICATION ####

vi /etc/iscsi/iscsid.conf

# line 54 : uncomment

uncomment line 58 59 & assign the username & password

node.session.auth.username = tom

node.session.auth.password = a

:wq ( save & quit )

#### TO START THE SERVICE ####

systemctl start iscsid

##### TO DISCOVERY THE ISCSI SERVER ####

iscsiadm -m discovery -t sendtargets -p 192.168.0.1

###### TO CONFIRM STATUS AFTER DISCOVERY ####

iscsiadm -m node -o show

##### TO LOGIN THE TARGET ####

iscsiadm -m node --login

##### TO CONFIRM THE ESTABLISHED SESSION ####

iscsiadm -m session -o show

#### TO CONFIRM THE SAN PARTITION ####

fdisk -l

then create the partition

then format the partition

then assign the mount point

#### **TO TAKE BACKUP WITH SCP PROGRAMM** ###

mkdir /zoom ( to create dir )

scp -r /zoom 192.168.0.1:/mnt

#### TO RESTORE THE BACKUP #####

cd / ( to enter the dir )

ls ( to check )

rm -rf zoom ( to remove the dir )

ls ( to check )

scp -r 192.168.0.1:/mnt/zoom / ( to restore)

ls ( to check the backup file )

###### **TO CHECK THE SELINUX STATUS** ####

#sestatus

###### TO ENABLE THE SELINUX SERVICE ####

#vi /etc/selinux/config

SELINUX=enforcing

:wq ( save & quit )

#init 6 ( to reboot the pc )

#sestatus ( to check the selinux status )

#### TO CHECK THE SELINUX PERMISSION ON FILES ##

#ll -Z

#### TO CHECK THE SELINUX MODE ON SERVICES ###

#cd /sys/fs/selinux ( to enter the dir )

#ls ( to check )

#cd booleans ( to enter the dir )

#ls ( to check )

#getenforce http\_use\_nfs

#### TO APPLY THE SELINUX PERMISSION ON SERVICES #

#setsebool httpd\_use\_nfs 1 ( to enable )

#getsebool httpd\_use\_nfs ( to check )

#setsebool httpd\_use\_nfs 0 ( to disable )

#getsebool httpd\_use\_nfs ( to check )

**TEAMING**

**Step 1:**  
**Check the available network device status**

**[root@HOST1 ~]# nmcli device status**DEVICE  TYPE      STATE         CONNECTION  
eth0    ethernet  connected     System eth0  
eno1    ethernet  disconnected  —  
eno2    ethernet  disconnected  —  
lo      loopback  unmanaged     —

**Check the network connection status**

**[root@HOST1 ~]# nmcli connection show**  
NAME         UUID                                  TYPE            DEVICE  
System eth0  5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  802-3-ethernet  eth0

**Step 2:**

**Creating a team interface named team0 in active-backup mode**

**[root@HOST1 ~]# nmcli connection add con-name team0 type team ifname team0 config ‘{“runner”:       {“name”: “activebackup”}}’**Connection ‘team0’ (c30dca42-cc35-4578-95c6-ae79f33b5db3) successfully added.

**Verify the new team connection is created**

**[root@HOST1 ~]# nmcli connection show**  
NAME         UUID                                  TYPE            DEVICE  
team0        c30dca42-cc35-4578-95c6-ae79f33b5db3  team            team0  
System eth0  5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  802-3-ethernet  eth0

**Step 3:**

**Add the slave interface (eno1 and en02) and point the master to the newly created team interface team0**

**[root@HOST1 ~]# nmcli connection add con-name team0-sl1 type team-slave ifname eno1 master team0**Connection ‘team0-sl1’ (8d5be820-2e88-46a2-8c08-b34ec0caf8a0) successfully added.

**[root@HOST1 ~]# nmcli connection add con-name team0-sl2 type team-slave ifname eno2 master team0**Connection ‘team0-sl2’ (3372f52c-0164-49d5-9783-938df99f18bc) successfully added.

**Verify the connection status now . we can see team masters and slaves here**

**[root@HOST1 ~]# nmcli connection show**  
NAME         UUID                                  TYPE            DEVICE  
team0        c30dca42-cc35-4578-95c6-ae79f33b5db3  team            team0  
System eth0  5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  802-3-ethernet  eth0  
team0-sl2    3372f52c-0164-49d5-9783-938df99f18bc  802-3-ethernet  eno2  
team0-sl1    8d5be820-2e88-46a2-8c08-b34ec0caf8a0  802-3-ethernet  eno1

**Step 4:**

**Now assign the IP address to the team0 interface**

**[root@HOST1 ~]# nmcli connection modify team0 ipv4.addresses 192.168.20.100/24 ipv4.method manual connection.autoconnect=yes**

**Check the teaming status. Here we can see team0 interface status and active slave**

**[root@HOST1 ~]# teamdctl team0 state**setup:  
runner: activebackup  
ports:  
eno1  
link watches:  
link summary: up  
instance[link\_watch\_0]:  
name: ethtool  
link: up  
eno2  
link watches:  
link summary: up  
instance[link\_watch\_0]:  
name: ethtool  
link: up  
runner:  
active port: eno1

Step 5:

**Checking the redundancy**

Now bring down the current active slave interface and check the other interface becomes active

**[root@HOST1 ~]# nmcli connection down team0-sl**team0-sl1  team0-sl2

[root@HOST1 ~]# nmcli connection down team0-sl1

[root@HOST1 ~]# teamdctl team0 state  
setup:  
runner: activebackup  
ports:  
eno2  
link watches:  
link summary: up  
instance[link\_watch\_0]:  
name: ethtool  
link: up  
runner:  
active port: eno2

Now we can see the active port is changed to eno2 automatically.

######### **TO CONFIGURE THE TOMCAT** #########

#yum install tomcat\* -y

#vi /etc/tomcat/tomcat-users.xml

<role rolename="manager-gui"/>

<user username="tomcat" password="123456" roles="manager-gui"/>

:wq ( save & quit )

#service tomcat restart

open the browser

http://localhost:8080

click on tomcat Manager

then provide the username & password ( what we assign in m.c.f )

username tomcat

password 123456

then go to war file to deploy option

then browser select war file

then deploy

open the browser

http://127.0.0.1:8080/calendar

**TROUBLE SHOOTING**

##############TO CHANGE THE ROOT PASSWORD#######################

#reboot the system

#press space bar

#select rescue and press e

#come last paragraph of linux16 and write rd.break console=tty1

#ctrl+x

#come in single user mode

#mount -o,remount,rw /sysroot

#chroot /sysroot

#passwd root

apply the password

redhat

redhat

#touch /.autorelabel

#exit

#exit

#################TO APPLY THE GRUB PASSWORD###################3

#grub2-mkpasswd-pbkdf2

Enter password:123

REEnter password:123

#copy password from grub word name onwards

#vi /boot/grub2/grub.cfg

:se nu

line no 71

set superusers="root"

export superusers

password\_pbkdf2 root and paste it

#again reboot the system

select and e

Enter username:root

password:123

#and we able change root password

##########IF YOU WANT THE CHANGE GRUB PASSWORD ############3

we insert the os dvd and change the grub password

##### **CONFIGURE THE VIRTUALIZATION** #####

Step 1

##### TO CREATE A PARTITION #####

#fdisk /dev/sda

press n ( to create new partitionm

press enter ( to take default cylinder value )

press +10G ( to assign the size )

press w ( to save & quit )

#partprobe /dev/sda ( to update the kernel )

#### TO FORMAT THE PARTITION ####

#mkfs.ext4 /dev/sda8

#blkid /dev/sda8 ( to check the f.s )

##### TO PROVIDE THE MOUNT POINT ####

#mkdir /vm ( to create a dir )

#mount /dev/sda8 /vm ( to assign the m.p )

#mount ( to check the m.p )

######### Step 2 ##### TO COPY THE OS IMAGE #####

copy the os image into /opt

###### Step 3 #### INSTALL THE PACKAGES ###########

#yum install qemu\* virt\* libvirt\* -y

#rpm -qa qemu\* virt\* libvirt\* ( To query the pkg )

##### Step 4 #### TO CREATE A NETWORKING FOR VIRTUALIZATION ####

#cd /etc/sysconfig/network-scripts ( to enter the dir )

#vi ifcfg-br0 ( To create a bridge file )

DEVICE="br0"

ONBOOT=yes

TYPE=Bridge

BOOTPROTO=static

IPADDR=192.168.50.24

NETMASK=255.255.255.0

wq!

#vi ifcfg-enp1s6 ( to modify the file )

DEVICE="enp1s6"

ONBOOT=yes

BOOTPROTO=static

BRIDGE="br0"

:wq!

#service network restart

#virt-manager

########## **TO CONFIGURE THE VPN SERVER** #############

# we need 5 pcs

#

# 1 pc for isp router

#

# 2 pc for vpn server

#

# 2 pc for vpn clients

# one pc for 1 isp router with 2 ips one ip : 10.10.10.1

# two ip : 20.20.20.1

# enable the routing in isp router

#

# two pcs for vpn server for example india vpn & usa vpn with 2 ip one public & one private

#

# india vpn server public ip : 10.10.10.2

# gw ip : 10.10.10.1

#

# private ip : 192.168.1.1

#

# enable the routing on vpn server

#

#

# india vpn client private ip : 192.168.1.2

# gateway ip : 192.168.1.1

#

# usa vpn server public ip : 20.20.20.2

# gateway ip : 20.20.20.1

#

# private ip : 192.168.2.1

#

# enable the routing on vpn server

#

#

# usa vpn client private ip : 192.168.2.2

# gateway ip : 192.168.2.1

#

#

#### Step 1 ### TO INSTALL THE PACKAGE ###########

yum install libreswan\* ( to install the pkg )

rpm -qa libreswan\* ( to query the pkg )

#### Step 2 #### TO CREATE THE KEY #########

ipsec newhostkey --configdir /etc/ipsec.d --output /etc/ipsec.d/ipsec.secrets --bits 4096 (IN BOTH SIDE)

#Generated RSA key pair using the NSS database

#### Step 3 ##### TO CHECK THE KEY #######

ipsec showhostkey --left

ipsec showhostkey --left > india.key

################IN USA#######################

ipsec showhostkey --left

ipsec showhostkey --left > usa.key

##########COPY THE INDIA KEY IN USA#################

scp -rv india.key 20.20.20.2:/opt

##########COPY THE USA KEY IN INDIA################

scp -rv usa.key 10.10.10.2:/opt

#### Step 4 #### TO CONFIGURE THE M.C.F ######

vi /etc/ipsec.conf

come end of file & uncomment the last line

include /etc/ipsec.d/\*.conf

:wq ( save & quit )

#### Step 5 #### TO CREATE A FILE FOR VPN TUNNEL ######

vi /etc/ipsec.d/india.conf

conn mysubnet

also=mytunnel

###### TO ADD THE INDIA PRIVATE N/W ######

leftsubnet=192.168.1.0/24

###### TO ADD THE USA PRIVATE N/W ######

rightsubnet=192.168.2.0/24

########### TO ADD THE INDIA PUBLIC IP & KEY ###########

conn mytunnel

leftid=@india.zoom.com

left=10.10.10.2 (

cat india.key >> /etc/ipsec.d/10.10.10.conf

leftrsasigkey=

###### TO ADD THE USA PUBLIC IP & KEY #########

rightid=@usa.zoom.com

right=20.20.20.2

cat usa.key >> /etc/ipsec.d/10.10.10.conf (and make left into right)

rightrsasigkey=

authby=rsasig

# load and initiate automatically

auto=start

:wq ( save & quit )

#### Step 6 ### TO START THE SERVICE #############

service ipsec restart

###########USA SIDE#####################

usa side same configuration#################

#### Step 7 #### TO ADD THE SUBNET #####

ipsec auto --add mysubnet

#### Step 8 ### TO ADD THE TUNNEL ####

ipsec auto --add mytunnel

#### Step 9 #### TO UP THE SUBNET #####

ipsec auto --up mysubnet

### Step 10 ## TO UP THE TUNNEL ####

ipsec auto --up mytunnel

### Step 11 ### TO CHECK THE STATUS ####

service ipsec status

NOTE : same configuration we have to do on usa vpn server

##### **TO CONFIGURE THE ZIMBRA MAIL SERVER** #####

'Step 1:-Check the Ip & Assign the Hostname'

# ifconfig (to check ip)

# hostname zimbra.zoom.com

# vi /etc/hosts

192.168.50.123 zimbra.zoom.com

:wq(save & quit the file)

# vi /etc/hostname (to make hostname permanent)

Remove localhost.localdomain & add the System Hostname

zimbra.zoom.com

'Step 2:-Stop the Postfix Service'

# vim /etc/resolv.conf (provide DNS Server ip with nameserver)

nameserver 192.168.50.250

# service postfix stop

# systemctl disable postfix.service

'Step 4:-Install the Dependency for Zimbra'

# yum install perl-core\* -y

'Step 5:-Install the Zimbra Application'

# cd /opt

# wget ftp://192.168.50.250/pub/adv\_linux/zcs\* (to get app from lab server pc)

# ls (to check)

# tar -xvzf zcs\* (to uncompress & extract)

# ls (to check)

# cd zcs\* (access into dir)

# ./install.sh (run this file to install application)

Accept the License -->Go With Default Options

AfterInstalling Default App's

Enter the Option 7--->Press '4' to set admin password

Provide Password:redhat --->Press 'r' to return--->Press 'a' to apply

Press Enter

'Step 5:-Restart the Service'

# mkdir /opt/zimbra/perl5 (create one dir for perl5 app)

# service zimbra start

# /sbin/chkconfig zimbra on (to enable permanent)

'Step 6:-Access the Zimbra Mail Server Application'

# firefox https://zimbra.zoom.com:7071 (to access admin console)

Username:admin Password:redhat

**LDAP**

**backend**

dn: cn=module,cn=config

objectClass: olcModuleList

cn: module

olcModulepath: /usr/lib64/openldap

olcModuleload: back\_hdb

dn: olcDatabase=hdb,cn=config

objectClass: olcDatabaseConfig

objectClass: olcHdbConfig

olcDatabase: {1}hdb

olcSuffix: dc=zoom,dc=com

olcDbDirectory: /var/lib/ldap

olcRootDN: cn=admin,dc=zoom,dc=com

olcRootPW: {SSHA}ibHaZ4Bw6faqYmovuhxuHk1kpzsdGvwo

olcDbConfig: set\_cachesize 0 2097152 0

olcDbConfig: set\_lk\_max\_objects 1500

olcDbConfig: set\_lk\_max\_locks 1500

olcDbConfig: set\_lk\_max\_lockers 1500

olcDbIndex: objectClass eq

olcLastMod: TRUE

olcMonitoring: TRUE

olcDbCheckpoint: 512 30

olcAccess: to attrs=userPassword by dn="cn=admin,dc=zoom,dc=com" write by anonymous auth by self write by \* none

olcAccess: to attrs=shadowLastChange by self write by \* read

olcAccess: to dn.base="" by \* read

olcAccess: to \* by dn="cn=admin,dc=zoom,dc=com" write by \* read

**frontend**

dn: dc=zoom,dc=com

objectClass: top

objectClass: dcObject

objectclass: organization

o: Zoom Com

dc: Zoom

dn: cn=admin,dc=zoom,dc=com

objectClass: simpleSecurityObject

objectClass: organizationalRole

cn: admin

userPassword: {SSHA}opvTrxWAMtmZ9lx54kwS7WSYsm5u4inJ

dn: ou=people,dc=zoom,dc=com

objectClass: organizationalUnit

ou: people

dn: ou=groups,dc=zoom,dc=com

objectClass: organizationalUnit

ou: groups

########### **TO CONFIGURE THE LDAP SERVER** ##########

####### Step 1 ###### TO ASSIGN THE HOSTNAME ######

#vi /etc/hostname

ldap.zoom.com

:wq ( save & quit )

#ifconfig ( To check the ip & hostname )

#vi /etc/hosts

192.168.50.1 ldap.zoom.com ldap

:wq ( save & quit )

##### Step 2 ##### TO INSTALL THE PACKAGE #####

#yum install openldap\* ldap\* migration\* nss\* -y

###### Step 3 ##### TO CREATE A FILE ######

# vi /etc/openldap/slapd.conf

pidfile /run/openldap/slapd.pid

argsfile /run/openldap/slapd.args

:wq ( save & quit )

##### Step 4 #### TO REMOVE & CREATE THE DATABSE DIR #

# rm -rf /etc/openldap/slapd.d/\* ( to remove )

#slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d

#### Step 5 #### TO MODIFY THE M.C.F ######

# vi /etc/openldap/slapd.d/cn=config/olcDatabase\={0}config.ldif

change the line 6

olcAccess:{0}to \* by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth manage by \* break

:wq ( save & quit )

##### Step 6 #### TO CHANGE THE OWNER OF DIR ######

#chown -R ldap.ldap /etc/openldap/slapd.d

##### Step 7 ##### TO CHANGE THE PERMISSION #####

#chmod -R 700 /etc/openldap/slapd.d

##### Step 8 #### TO START THE SERVICE ####

#systemctl start slapd

#systemctl enable slapd

#### Step 9 #### TO ADD THE SCHEMA FILE #####

#ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/core.ldif

#ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif

#ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif

#ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif

##### Step 8 #### TO ASSIGN THE PASSWORD TO LDAP ADMIN ####

#slappasswd

slappasswd # generate encrypted password

New password: # input any password

Re-enter new password

{SSHA}xxxxxxxxxxxxxxxxx # remember

##### Step 9 ##### TO CREATE A NEW FILE ####

#vi backend.ldif

dn: cn=module,cn=config

objectClass: olcModuleList

cn: module

olcModulepath: /usr/lib64/openldap

olcModuleload: back\_hdb

dn: olcDatabase=hdb,cn=config

objectClass: olcDatabaseConfig

objectClass: olcHdbConfig

GolcDatabase: {1}hdb

olcSuffix: dc=zoom,dc=com

olcDbDirectory: /var/lib/ldap

olcRootDN: cn=admin,dc=zoom,dc=com

olcRootPW: {SSHA}xxxxxxxxxxxxxxxxxxxxxxxx

olcDbConfig: set\_cachesize 0 2097152 0

olcDbConfig: set\_lk\_max\_objects 1500

olcDbConfig: set\_lk\_max\_locks 1500

olcDbConfig: set\_lk\_max\_lockers 1500

olcDbIndex: objectClass eq

olcLastMod: TRUE

olcMonitoring: TRUE

olcDbCheckpoint: 512 30

olcAccess: to attrs=userPassword by dn="cn=admin,dc=zoom,dc=com" write by anonymous auth by self write by \* none

olcAccess: to attrs=shadowLastChange by self write by \* read

olcAccess: to dn.base="" by \* read

olcAccess: to \* by dn="cn=admin,dc=zoom,dc=com" write by \* read

####### Step 10 ###### TO ADD THE DATABASE #####

#ldapadd -Y EXTERNAL -H ldapi:/// -f backend.ldif

## Step 11 ## TO CREATE THE FILE WITH DOMAIN OU USER & GROUP ###

#vi frontend.ldif

dn: dc=zoom,dc=com

objectClass: top

objectClass: dcObject

objectclass: organization

o: Zoom Com

dc: Zoom

dn: cn=admin,dc=zoom,dc=com

objectClass: simpleSecurityObject

objectClass: organizationalRole

cn: admin

userPassword: {SSHA}xxxxxxxxxxxxxxxxxxxxxxxx

dn: ou=people,dc=zoom,dc=com

objectClass: organizationalUnit

ou: people

dn: ou=groups,dc=zoom,dc=com

objectClass: organizationalUnit

ou: groups

:wq ( save & quit )

##### Step 11 #### TO ADD IN LDAP DB ######

#ldapadd -x -D "cn=admin,dc=zoom,dc=com" -W -f frontend.ldif

##### Step 12 #### TO CREATE A LDAP USER & GROUP #####

#useradd jack ( to create a user )

#passwd jack ( to assign the password )

#tail /etc/passwd ( to check the users )

#tail /etc/shadow ( to check the password )

#vi /usr/share/migrationtools/migrate\_common.ph ( to open the file )

replace padl to zoom

:wq ( save & quit )

#grep jack /etc/passwd > jack.passwd

#ls ( to check )

#/usr/share/migrationtools/migrate\_passwd.pl jack.passwd jack.ldif

#ls ( To check )

#cat jack.ldif ( to read the file )

#ldapadd -x -D "cn=admin,dc=zoom,dc=com" -W -f jack.ldif

##### TO CONFIGURE THE NFS SERVER #####

#vi /etc/exports ( to open the m.c.f )

/home \*(rw,sync)

:wq ( save & quit )

service nfs restart ( to start the service )

#showmount -e ( to check )

##### TO CHECK THE LDAP DATABASE ######

#ldapsearch -x -b "dc=zoom,dc=com" '(objectclass=\*)'

######## TO CHECK FROM CLIENT SIDE #####

#yum install openldap\* ldap\* nss\* -y

authconfig-tui ( to provide the ldap server ip & domainname )

( \* ) use ldap

assign the domainname & ip

ok

#mount 192.168.50.1:/home /home ( to assign the m.p )

#mount ( to check the m.p )

**LDAP USER**

dn: uid=cent,ou=people,dc=zoom,dc=com

objectClass: inetOrgPerson

objectClass: posixAccount

objectClass: shadowAccount

uid: cent

cn: cent

sn: cent

userPassword: {SSHA}xxxxxxxxxxxxxxxxx

loginShell: /bin/bash

uidNumber: 1000

gidNumber: 1000

homeDirectory: /home/cent

dn: cn=cent,ou=groups,dc=zoom,dc=com

objectClass: posixGroup

cn: cent

gidNumber: 1000

memberUid: cent

**new**

dn: cn=admin,dc=zoom,dc=com

objectClass: simpleSecurityObject

objectClass: organizationalRole

cn: admin

userPassword: {SSHA}63nWqD9StHSb7zbFONprvAQzd3w+1t3Z

dn: ou=people,dc=zoom,dc=com

objectClass: organizationalUnit

ou: people

dn: ou=groups,dc=zoom,dc=com

objectClass: organizationalUnit

ou: groups

**olcDatabase={0}config**

# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.

# CRC32 1fe055b9

dn: olcDatabase={0}config

objectClass: olcDatabaseConfig

olcDatabase: {0}config

#olcAccess: {0}to \* by \* none

olcAccess: {0}to \* by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth manage by \* break

olcAddContentAcl: TRUE

olcLastMod: TRUE

olcMaxDerefDepth: 15

olcReadOnly: FALSE

olcRootDN: cn=config

olcSyncUseSubentry: FALSE

olcMonitoring: FALSE

structuralObjectClass: olcDatabaseConfig

entryUUID: 30037896-296a-1034-9a35-e77d0f527729

creatorsName: cn=config

createTimestamp: 20150105210431Z

entryCSN: 20150105210431.274666Z#000000#000#000000

modifiersName: cn=config

modifyTimestamp: 20150105210431Z

**SLAPD.CONF**

pidfile /run/openldap/slapd.pid

argsfile /run/openldap/slapd.args

###### **TO CONFIGURE THE SLAVE LDAP SERVER** #######

First configure the master ldap server

#### Step 1 #### IN MASTER LDAP SERVER ########

#vi /etc/hosts ( To provide the slave ip & hostname )

192.168.0.2 slave.zoom.com slave

:wq ( save & quit )

##### Step 2 #### TO STOP THE SERVICE #####

#service slapd stop

#### Step 3 ### TO COPY THE DATABASE INTO FILE #####

#slapcat -b "dc=zoom,dc=com" -l /opt/frontend.ldif

ls ( to check the file )

#cat frontend.ldif ( to read the file )

#### Step 4 ### TO COPY DB FILE INTO SLAVE PC ####

#scp frontend.ldif 192.168.0.2:/opt

#### Step 5 ### TO ADD THE SLAVE INFORMATION IN M.C.F ####

#vi /etc/openldap/slapd.conf

replogfile /var/lib/ldap/slapd.replog

replica host=slave.zoom.com:389

bindmethod=simple

suffix="dc=zoom,dc=com"

binddn="cn=Manager,dc=zoom,dc=com"

credentials=a

tls=0

:wq ( save & quit )

######### TO CONFIGURE THE SLAVE LDAP SERVER #######

in slave ldap pc

configure the same pratical steps of master ldap server till backend file step 9

###### Step 1 #### TO ADD MASTER LDAP CONFIGURATION IN SLAVE M.C.F ###

#vi /etc/openldap/slapd.conf ( to open the m.c.f )

updatedn "cn=admin,dc=zoom,dc=com"

updateref ldap://ldap.zoom.com

:wq ( save & quit )

# GIVE FULL PERMISSOM#

chown -R ldap. /var/lib/ldap

#### Step 2 #### ADD THE MASTER DB FILE INTO SLAVE DB ####

#cd /opt ( to enter the dir )

#ls ( to check the files )

#slapadd -l frontend.ldif

#### Step 3 ### START THE SERVICE #####

start the slapd service in master ldap server

start the splad service in slave ldap server

#### Step 4 ### TO CHECK THE LDAP DATABASE SERVER ####

#ldapsearch -x -b "dc=zoom,dc=com" '(objectclass=\*)'

#### Step 5 ### THEN CHECK FROM CLIENT SIDE ###

#authconfig-tui

┌────────────────┤ Authentication Configuration ├─────────────────┐

│ │

│ User Information Authentication │

│ [ ] Cache Information [\*] Use MD5 Passwords │

│ [ ] Use Hesiod [\*] Use Shadow Passwords │

│ [\*] Use LDAP [ ] Use LDAP Authentication │

│ [ ] Use NIS [ ] Use Kerberos │

│ [\*] Use Winbind [ ] Use Fingerprint reader │

│ [\*] Use Winbind Authentication │

│ [\*] Local authorization is sufficient │

│ │

│ ┌────────┐ ┌──────┐ │

│ │ Cancel │ │ Next │ │

│ └────────┘ └──────┘ │

│ │

│ │

└─────────────────────────────────────────────────────────────────┘

┌─────────────────┤ LDAP Settings ├─────────────────┐

│ │

│ [ ] Use TLS │

│ Server: ldap://192.168.0.1/,ldap://192.168.0.2\_\_\_│

│ Base DN: dc=zoom,dc=com\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ │

│ │

│ ┌──────┐ ┌──────┐ │

│ │ Back │ │ Next │ │

│ └──────┘ └──────┘ │

│ │

│ │

└───────────────────────────────────────────────────┘

note: to find slave ldap , 1 stop master service & try to login client system with ldap user