S&NA

System Administrator

a system admin is a person responsible for the configuration, management and reliable operations of computer system, especially multi users computers such as servers.

System administration refers to the management of one or more hardware and software systems.

Components of SA

=> Installing and config servers
=> Maintaing Servers and Servers based activities
=> Troubleshooting Servers related problems
=> Work as a support and
=> solves issues related to user, aplications
=> Project management
=> System Monitoring
=> Back up & recovery
=> Manage Access Control

Command Line

SHELL:

Shell is a UNIX Term. It is a program that allows user to interact and give commands to the OS.
SHELL is a command language interpreter that executes commands.

↳ BASH

stands for Bourne Again SHELL.

BASH is a Unix Shell that runs programs in a command line interpreter.
BASH has many built-in commands and consists of combinations of built-in commands

It has ability to launch programs and to control the programs that are launched by it.

JOB Control:

When a job is started, it has takes over the terminal.
It can issues control codes.
Once the program is done, it gives full control back to BASH.

Commands:

Consider a user yyang logged into the system

=> wants to launch Firefox command

[yyang@server-7 $ firefox &]

user id — ready to accept command — program to run — command to run program

=> To stop the running job and so control returned to the Bash simply press

=> Ctrl + Z

=> to identify no of jobs running

=> [user id-7$ jobs]

output [7]+ Running firefox &

The output shows
job name (Firefox)
job number ([7])
Job is in 2 states
either running or stopped

=> To bring job to foreground i.e give it back the control of terminal

=> [user id-7$ fg [number]]

To send job to background and give control back to the terminal

[userid -]$ bg [number]

Environment Variable:

is a variable that effect the way running process will behave on a computer.

Printing all variable

[userid -]$ printenv

Setting Environment Variable

[userid -]$ variable = value

e.g

[userid -]$ FOO = BAR

=> To export variable for other program

[userid -7$ export FOO

E.V

=> We can use combination is commands like

[userid -7$ export FOO="You are Welcome"]

=> To print value of E.V

[userid-7$ printenv FOO

=> To unset E.V

[userid -7$ unset (variable name)

eg unset FOO

Pipes

Pipes are mech through which output of one program can be sent as input of other program.

The vertical bar (|) reps pipes.

In Linux: command in Linux pipes executed concurrently

In windows: commands runs in order and intermediate result in stored files.

Redirection

Redirection is the mechanism of taking output of a program and have it automatically send to a file.

3 classes
- ↳ output to a file
- ↳ append to a file
- ↳ send to a file as I/P

(i) To collect output of a program to a file

we use (>) greater than symbol to send output to a file

```
[userid -]$ ls > /temp/director_listing
```

- ls → output of program
- > → command symbol
- /temp/director_listing → file in which o/p is to be sent

(ii) To append some output or text/code to the end of a directory

we use (>>) double greater than sign

[useeid -7$ echo "Direc list" >> /temp/directory_listing

(iii) To use output of a file as input to some program

we use (<) sign that followed by file path name

[userid -7$ grep("root") < /etc/passwd

This command will send output from password directory to grep program

ommand-Line Shortcuts

Enviromental Variable as a parameter

BASH allows to use E.V as parameter
We use $ befor E.V while passing it as a parmeter to a program

e.g
passing E.V FOO as a parameter
we write
$FOO
so the value of FOO will be passed

Multiple Commands

We can write multiple command on a same line by seperating them with a semicolon (;)

e.g

Tusenid -7$ Foo = "100" ; printev FOO

Backtick

Backticks are represented by (`)

Anything inside the backticks is treated as a command to be executed.

Backtick is not a quotation sign. It has a very special meaning. Everything you write in the backticks is executed first before the main command and the result of command inside back ticks is used as parameter of outer main command

eg

[user id -]$ kill `cat /var/run/named/named.pid`

this returns process #

[user id -]$ kill 2833

Outline #6

Managing Software

Every program owned by user
Every user has unique ID number (UID)
" " belong to a Group
Group: a collection of users established by SA.
A user may belongs to multiple groups.
Groups have also unique ID Number (GID)

Accessibility of programs based on UID & GID

User can be a normal user or root user

Normal user
↳ can access which they own
↳ or of files of which permission is given because the file's accessing permission given to user

Root user
↳ access to all files and program
↳ access whether the permissions is given or not
↳ also called super user

User info kept

↳ in Active Directory AD

↳ contains nitty gritty details of users and groups database.

↳ details includes SIDs for users, groups and other objs.

↳ Linux contains all info in /etc/passwd file.

↳ allows to change info without using any kind of special tool just by using text editor

The /etc/passwd File

Stores user's credentials like

↳ Username → Yang

↳ password → xx:

↳ User ID → 501:

↳ Group ID → 504:

↳ GECOS/Name → Yeang Yang

↳ Directory → /home/Yang

↳ Shell → /bin/bash

The /etc/shadow file

↳ Stores encrypted password info of user id.
↳ /etc/passwd file
contains password in encrypted form
↳ so /etc/shadow file
contains password which is only readable by the root user of system and some privildge program that has allowed access.
↳ introduce b/c password could be cracked easily by growing home PCs Technology.

like /etc/passwd file each line in /etc/shadow file reps some info

Login name
Encrypted Password
Day since Jan 1, 1970, password was last changed
Day before pass may change
Day after pw must
Day before pass expire & user is to warn
Day after " " & account is disabled
A reserved file

The /etc/group file

Following fields of each line in /etc/group

Group name
Group password
Group ID (GID)
Group Members

Understanding
Set UID Eq Set GID command

'chmod' command (r,w,x)

Permisson

chmod u+x file
u+w foo.sh

User ->
Group ->

read -> ls
write -> eg write on file
mk on dir
execute -> run exe file

to see file ls -l

Scanned with CamScanner

Installing GRUB Legacy from GRUB SHELL

1. Install Launch GRUB shell using grub command

[user@d ~]$ grub

2. Display GRUB's current root Device

[user@d ~]$
grub> root

3. Set GRUB's root device to the partition that contains the boot directory on local hard disk

grub> root (hd0,0)

Make sure that the stage1 image can be found on the root device

grub> find /grub/stage1

Finally, (re)install the GRUB boot loader directly on MBR of hard disk

grub> setup (hd0)

4. Quite Grub

grub> quite

Enabling & Disabling Services

Enabling a Service

The start up runlevel of services/programs can also be managed using chkconfig utility.

↳ To view all the runlevels in which the carpald.sh program is configured to start up, type

=> [userid -]# chkconfig --list carpald

output:

carpal 0:off 1:on 2:off ... 6:off

↳ To make carpald.sh program start up in runlevel 2, type

[userid -]# --level 2 carpald on

output:

carpald 0:off 1:on 2:on ... 6:off

↳ GUI tools can also be used to run programs in different levels. configured in carpad.sh.

Disabling a Service

↳ To disable a service, you must know the name of service you want to disable.

↳ use chkconfig utility to disable / off it permenantly

↳ To disable a service eg "Life Saving" carpaled.sh program, type

[root@ id -] # chkconfig carpaled off

↳ To check list of runlevel for program

[user id] # -list carpaled.

↳ To delete a service permanently

[user id -] # chkconfig -del carpaled

IP Tables & Filtering

IP Addressing

Internet protocol addressing is a process of assigning numeric label to each device connected in a compute network.

↳ made up of 32 bits

8 bits : 8 bits : 8 bits : 8 bits

$2^8 : 2^8 : 2^8 : 2^8$

0-255 : 0-255 : 0-255 : 0-255

↳ divided into 2 portions :

(i) host bits position

(ii) Network bit position

↳ Subnet

logical division of an network

↳ Subnetting

process of dividing a network logically

Firewall:

Software utility that acts as a filter for data entering or leaving a computer network.

↳ works by blocking ports accessing unauthorized or restricted data.

↳ controls network traffic and denies network connections that are not following security policies

IP Tables:

Before IP table Linux systems use IP-chains as firewall

Distdy:

ran as a seperate program not as a part of Kernel

NetFilter org create a new program IP Tables.

↳ now become default firewall of Fedor Linux and RedHat

IP-Tables

↳ basic firewall

↳ is a command line firewall utility that uses policy chains to allow or block traffic

↳ When connection tries to establish, iptables checks the list of rules in its list to match it.

↳ connection depends upon the matching of rule in tables

↳ IP tables is rule based firewall system.
↳ By default installed with OS.
↳ Continous monitor ingoing and outgoing data packets
↳ By default, running without any rules
↳ We can create, add, edit rules init.

Basic Str.

"Tables has chains & chains which has rules"

Tables ⇒ chains ⇒ Rules.

Rules control the packets for I/p & O/p

IP Table Filtering

↳ IP tables contains rules
↳ Kernel check each data packet according to the defined rule.

↳ IP Filtering
is simple mechanism that decides which type of IP datagram will be processed and which will be discarded
↳ Discarding means ignoring as it was never recieved.

Packet Forwarding:
routing datapacket and make decision acc to routing table

Packet Filtering:
uses set of rules of packet filtering.

↳ Linux Kernel
has built in packet filtering mechanism ip-filtering, IP tables

Rules

There are 5 rules

(i) Input:

The input chain is used for any packet coming into the system.
Ilp chain for managing packets input to the server & used by Filter Table.

(ii) Output:

The output chain is for any packet leaving out the system.
Used by Filter Table.

(iii) Forward:

The forward chain is for packets that are forwarded through the system

(iv) Pre Routing:

Prerouting allows altering of packets before they reach the input chain

v) Post Routing:

allows altering packets after they exist the output chain & used by mangle & NAT Table

Targets

Every iptables have some "targets" which are executed whenever a given criteria is matched

Accept: package is accepted & goes to app for processing

Drop: packet is dropped, no info regarding drop is sent to sender

Reject: packet is dropped & info is sent to sender

LOG: packet details are sent for logging.

DNAT: Rewrites the destination IP of the packet

SNAT: Rewrites the source of IP of packet

Type of IP Tables use in filtering

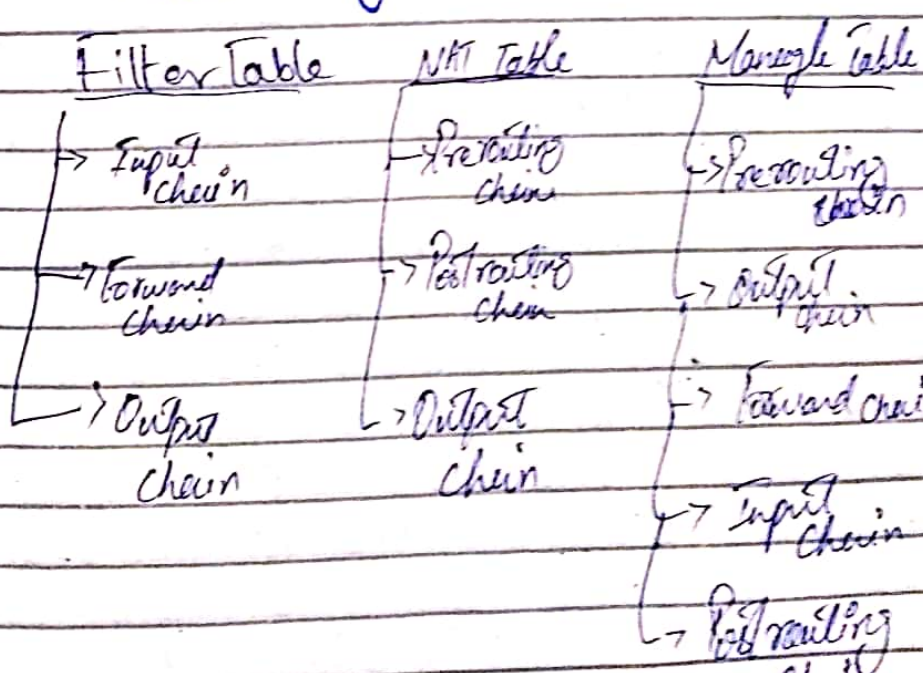
The three-build in Tables with chain rules

Filter: The default table for handling network packets

NAT: Used to alter packets that create a new connection

Mangle: Used for specific type of packet alteration

Graphically



Filter Table

↳ Filter is default for iptables
↳ always created by default
↳ mainly used for filtering packets.
↳ this is the place where we actually take action against packets.
↳ look, what they contain
&
↳ perform Drop or Accept

Built-in Chains

Input : Applied to a network packet that are target for server
↳ packets as input
↳ add rules to control conn b/w Server & Server
↳ e.g. request from http server goes through this chain

Output : Applied to locally generated packe
↳ response from server
↳ outgoing from firewall

Forward : Applied to packet routed through host.
↳ for packet routed through servers..

NAT Table

Network address translation table (NAT)

↳ is methodology of modifying network address info. in IP datagram packet headers.

↳ Technique to change the destination/target IP-address

↳ used to connect multiple computer in a private address range using public internet.

↳ It should only be used to translate packet's source field or des field.

Built-in Chains

Prerouting: Its translate packets before routing. Alters network packets when they arrive

Output: Alters packet before they send out

Post routing: Alters packet before they leave.

Mangle table

Mangling refers to modifying the ip-packet.

↳ any sort of modification in packet is called mangling

↳ used for specialized packet alterations.

Built-in Chains:

Input: Alter n/w packet target for host

Output: Alter locally generated data packet before they sent out

Forward: Alter network packets routed through host

Prerouting:
Alter incoming n/w packets before they are routed

Postrouting:
Alter n/w packets before they are sent out.

Outline # 4

Installing Linux

Fedora Installation

Methods of installation:

FTP (File Transfer protocol): performing n/w installation

HTTP : installation tree served from web server

NFS (Network File System): the distribution tree is shared on an NFS server

SMB (Server Message Block): installation tree can be shared on Samba Server

=> Installation

↳ Boot off DVD-ROM
press install or upgrade Fedora
↳ select language

=> Initialize Disk
↳ select type of storage devices involved
e.g. hard disk
↳ Data discarding option

=> Configure Network
↳ write host name
↳ can change after installation

=> Network Connection

↳ chose network connection type
i.e wired, wireless, broadband, PPPoE, DSL
↳ automatically configuration through (DHCP)

=> Time Zone Config

↳ configure UTC (coordinate universal time)
↳ select nearest valid location
time will set up automatically

=> Set root password

↳ root most privileged user
↳ equivalent to Admin Account in Windows
↳ Enter password
↳ Confirm "

=> Storage Config

↳ '/' identifies root partition
(= to C:)

↳ '/boot' identifies contains files for boot process
(= to windows)
contains files to be executed before kernel begin execut.

↳ '/usr' all programs resides

↳ '/home' contain's every user's home directory.

'tmp' : contains temporary files

Swap : where virtual memory is stored
not accessible by user.

=> Installation options
↳ select (create custom layout)
default
↳ select disk setup
=> create & select disk partition
=> complete dialog box with inform

↳ Repeate
Select
Select disk setup

=> Configure Boot loader
↳ handles procedure of actual startup
↳ GRUB boot loader in Linux
↳ install boot loader often
↳ specifying a storage device
↳ can also installed on (MBR master boot record)
MBR is first thing the system will read.

=> Initial System Configuration
↳ after boot process pass through one time config
↳ Read Liscence & understand thoroughly.

=> Create user
↳ allows to create a local user
non-privilidged user
↳ Select Add To Administrators Group
complete fields and Fwd
Full Name → 'master'
User Name → 'master'
Password → ~
Confirm " → ~.

=> Login
↳ system completion
login to system
↳ use credentials of user

Installing Ubntu Server

=> Installation
↳ insert installation media
↳ select boot option accordingly
↳ select language
↳ select install UBNTU.
↳ Select language of os
↳ Select Country / Region
↳ Select keyboard layout
=> Configure Network
↳ Select host name
name of server

=> Setup user & Password

↳ Select & confirm

Full Name → Master admin

Username → master

Password → x

Confirm " → x

=> Configure Time Zone

↳ sets time automatically acc to time zone

if not

↳ select manually

=> Other Tasks

↳ Select automatic update option

ON or OFF

↳ Select & install GRUB boot loader

↳ after installation reboot system

and login using credentials

Active Directory

Active directory is a directory service that runs on Microsoft Windows Server

Function

- enable administrator to manage permissions.
- manage control access to network resources

Data is stored in form of objects, which includes

- users, groups, application & devices.

Configuration of Samba Server

Samba Server

=> Feature

- powerfull server
- allows access to diff files & printers on window based & other OS.
- uses a protocal CIFS (common internet file system)

=> Protocol

- Samba is implementation of CIFS
- CIFS is new file system that allows access to files & printers on diff machines in n/w
- CIFS client can read, write & remove files on host serv

=> Mechanism

- uses SMB (Server message block) to access Shared Resource over n/w
- Client send SMB request to access a service
- Host/server responds with an SMB

=> Why Samba

- Linux doesn't support SMB so
- Compatible system SAMBA is installed
- It allows access to shared res using SMB btw Two systems
- Window user don't even knows they are accessing from which system.
- It is so versatile, It can installed on any Unix platform

Port

SMB uses either

139 port

445 port

eg

TCP protocol

=> Configuration Command

i) install samba server

yum install samba* -y

ii) enabling & starting

systemctl enable smb

systemctl start smb

iii) Allowing firewall in samba server sec policies

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

iv) Reloading firewall to add rule

firewall-cmd --reload

(vii) path for samba file for config.

cd /etc/samba

(viii) samba configuration file

=> to use vim editor for configuration

vim smb.conf ;

(ix) configuration in smb.conf file

insert following data for conf

[share]

Commuil = Sambaserver
path = /samba-share
browsable = yes
valid users = std1, std2 &BSIT
hosts allow = 10.53.14.0/24
writeable = yes
Write list = std1 &BSIT
guest = ok
readonly = no

(x) validate config file

testparm

(iv) create folder for configuration

makdir samba-share

(iv) Detect problems & troubleshoot on Network

Logs

/var/log/messages.

(x) Restart

#systemctl restart samba

Apache Server

↳ also called web servers
↳ they are configured in such away that they can access publically over the network/internet.
↳ so everyone can access them
Eg user services

(i) install

```
# yum install http*
```

(ii) Enable, start & check status

```
# systemctl enable httpd.service
#  "     start    "
#  "     status   "
```

(iii) Enable firewall & reload to configure

```
# firewall-cmd --permanent --add-service=http
# firewall-cmd --reload.
```

(iv) path of config file

```
cd /etc/httpd/conf
```

(v) configuration file

```
httpd.conf
```

(vii) open & configure using vim editor

vim httpd.conf

(viii) add configurations.

<virtualhost 10.53.4.14.807
ServerAdmin root@studdillab
ServerAdmin www.studdillab.com
DocumentRoot /var/www/html

</virtualhost>

(ix) First website page

index.html

can config using vim editor.

vim index.html.

(x) Restart

#Systemctl restart httpd.services.

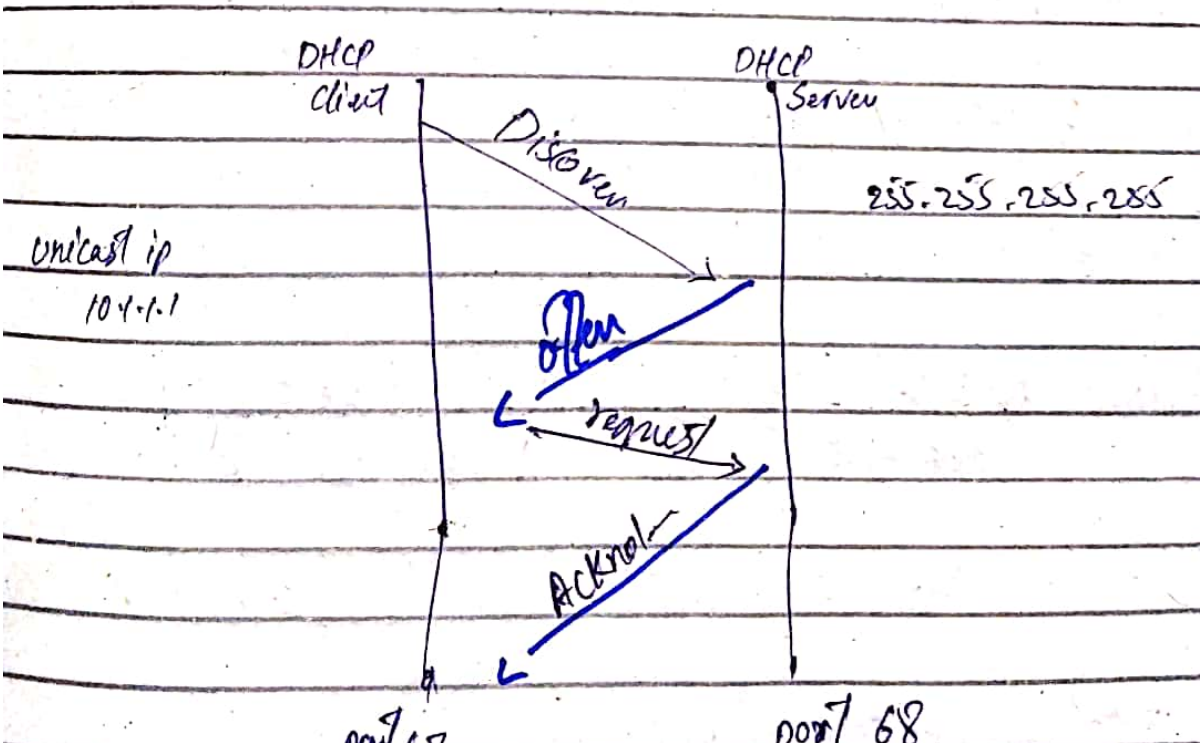
DHCP server

Dynamic host configuration protocol

↳ protocol use TCP/IP network
↳ automatically assigns IP, & other configuration like
subnet mask, gateway, DNS server

↳ configurations to connect devices so they can exchange info

↳ communication only possible if sender knows the destination & targeted machine.
↳ creates a pool of ip-address



Mechanism

↳ Client checks if DHCP available on network system.

↳ DHCP server offers ip to client automatically assigns it

↳ Client request a particular address

↳ DHCP server assign the particular requested IP to a client and send acknowledgment

(i) install

Yum install dhcp*

(ii) Services

#systemctl enable dhcp.services
" . start "
" status "

(iii) Adding firewall config & reloading to add this firewall in further traffic

firewall-cmd --permanent --add-services = dhcp.
firewall-cmd --reload.

(iv) configuration file path

cd /etc/dhcp

(v) configuration file name

dhcp.conf

(vi) use vim editor to add configuration

vim dhcp.conf

(vii) Configurations

example

subnet 192.168.100.0 subnet mask 255.255.255.0

Range 192.168.100.101 192.168.100.150

(ix) Restart

systemctl restart dhcp.services

to config & save all.

FTP Server

FTP
- File transfer protocol
- to transfer data files within or between machines

(i) installation
yum install vsftpd

(ii) directory created after installation
/var/ftp/pub

(iii) Services

# systemctl	enable	vsftp.services
# "	start	"
# "	status	"

(iv) Add firewall & reload so data can flow through it

firewall-cmd --permanent --add-services = vsftp
firewall-cmd --reload.

(v) Configuration file path

cd /etc/vsftpd/

(vi) config file name

vsftp.conf

(vii) Configs to add in file
example

(vii) add configs using vim editor

vim vsftp.conf

(viii) Restart
after all configuration

#Systemctl restart vsftp.services