**Find Commands**

**Type in the name of config file or query to search entire root partition**

find / -type f -name "$\_QUERY"

**Searching etc directory type in the name of config file OR Query to search /etc**

find /etc |grep "$\_QUERY2"

**Find a string or query inside a specified directory or file .This will search for a STRING, not file.**

grep -Ri "$\_QUERY3" \* "$\_DIR"

# grep -Ri 4/ \* /

# find 4 followed by / \* everything in root /

**Find files related to user**

find / -user "$\_USERQ"

**Find GROUP related files**

Find / -group "$\_GROUPQ"

**Find config files**

find / . -type f -name "\*.conf"

**Find files by by extention**

find / -type f -name "\*$\_EXTENSION"

**Find logs**

find / . -type f -name "\*.log"

**Find files CHANGED in last hour**

find / -cmin -60

**Find files MODIFIED in last hour**

find / -mmin -60

**Find files ACCESSED in last Hour**

find / -amin -60

**Service audit Commands**

**Displaying All services**

$service --status-all

$chconfig --list

$which

$who

$w

**Finding running Processes:**

**Top:** shows all top processes running

**ps aux , ps x :** shows all processes running in the back ground. On the TTYcolunm if there is a question mark then that means there is no terminal involved with that process running

STAT: the status of the procecess, this can have multiple meanings.

R running

S for sleeping

T Stopped

n Low priority

l multiy threaded

Sl : sleeping and multithreaded

VSZ: virutal memory size

RSS: resident set size, the phycial memory being used.

**Finding open Ports and their processes**

**How To Find which process**es are listening on ports, will display everything that is a current process and is listening to an open port. This will not display an open port but will display the PID. Later use the PID (NOTE) lsof might not be installed by default and may need to be installed. Lsof should be ran by super user.

sudo lsof -i

Lets assume the command above gave us mysqld service but not the port number that it is using. NOTE THE PID NUMBER IS INDICATED IN BLUE. Notice that his command did not specify the port number. INDICATED IN RED. NOTE only the process that have a (LISTEN) are applications that have a port open.

EX:

[lu@lu ~]$ sudo lsof -i

mysqld **20737** mysql 21u IPv6 392419 0t0 TCP \*:mysql (LISTEN)

To find out which port mysqld is using, use the following **lsof** command to see which port it is using. Insert the PID inbetween -p and -i. This will display the port that was not available before.

EX:

[lu@lu ~]$ sudo lsof -Pan -p 20737 -i

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

mysqld 20737 mysql 21u IPv6 392419 0t0 TCP \*:3306 (LISTEN)

**To see which process is bound** by a **specific port,** for example if you do not know the service associated with the port thats open. in this case lets assume we do not know why port 3306 is open, this command will list the information needed to determine with what the port is associated with. For some magical reason we find out that a port is open owe can use the following command to see the command its used.

[lu@lu ~]$ sudo lsof -i :3306

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

mysqld 20737 mysql 21u IPv6 392419 0t0 TCP \*:mysql (LISTEN)

**Finding out** a service is running and its PID, location and working directory. In this case its mysqld

**EX: this will list everthing associated with mysqld, the number in bold after mysql is the pid of the process.** Indicated In blue

[lu@lu ~]$ **ps aux |grep mysqld**

mysql **20737** 0.1 2.4 596048 95072 ? Ssl 20:26 0:00 /usr/bin/mysqld --pid-file=/run/mysqld/mysqld.pid

lu 20948 0.0 0.0 10700 2280 pts/0 S+ 20:35 0:00 grep mysqld

**Ex: insert the PID inbetween “ /proc/ /exe” to see its permissions, date it started and where its being executed.** In this example my PID for my mysqld service is 20737.

[lu@lu ~]$ sudo ls -l /proc/20737/exe

lrwxrwxrwx 1 mysql mysql 0 Mar 24 20:26 /proc/20737/exe -> /usr/bin/mysqld

**Using** pwdx to find out working directory of a process. Insert PID after pdwx command, in this example its my mysqld process 20737.

[lu@lu ~]$ sudo pwdx 20737

20737: /var/lib/mysql

**netstat -tulpn: USE THIS** INSTEAD SO MUCH EASIER

**To summarize:**

To list everything that’s listening on ports, Note only processes with (LISTEN) have open ports. This will display the PID, service, the user it’s running under, the ipv6 or ipv4 protocol, and name of process.

sudo lsof -i

grab the PID to find out which port it’s listening to, will display the port that its listening to.

sudo lsof -Pan -p 21226 -i

**Other Useful commands**

**whatis:** this command will tell you what the service is, it can be useful to find out if a service is running or not, for example: is apache is not running, whatis will return that apache is nothing important, if it is, it will give you a brief description of what it is.

EX: [lu@lu ~]$ whatis mysqld

mysqld (8) - the MySQL server

**Who:** who commands works with almost all Linux and UNIX like oses. It show who is logged on to your system. It displays information about currently logged in users. By default, this includes the login name, tty name, date and time of login and remote hostname if not local.

**Grep , Egrep, fgrep:**

**Egrep:** search for one or more files for lines that match a regular expression, this does not include regular expressions themselves. Find strings inside files that match the search query.

Ex:

$ egrep '(Luis|luis)' Filename.txt

**Fgrep:** search for one or more files for lines that match a liteal, text-string patter. Because fgrep does not support regular expressions, it is faster than grep. FASTgrep.

EX: print lines in a file that dont contain any spaces, -v print all lines that dont match pattern.

$ fgrep -v ' ' file

EX: print lines in file that contain the words in spell\_list

$ fgrep -f spell\_list file

**grep:** search one or more files for lines that match a regular expression.

EX: Show were the variable ServerToken is available, -i ignore uppercase and lowercase letters.

grep -ri 'ServerTokens' \*

**Programs to be aware of, apart of the unix standard**

**Communication:**

**login:** sign on to unix

**rlogin**: sign onto remote unix

**mailx**: read or send email

**talk:** write to other terminals. EX: talk pts/1

**telnet**: connect to another system

**write:** talk to other terminals

Comparing files:

cmp: compare two files

comm: compare items in files

diff: compare two files

diff3: compare three files

sdiff: compare two files side by side

File Managment:

cat: join fils are display them

file: determine a files type

ln: create files aliases

rcp: copy files to remote systems

rmdir: remove directories

tail: show the last few lines of a file

wc: count lines, words and characters

System status

df: show free disk space

du : show disk usage

env: show enviroment variables

gawk:

**Quick Commands**

Check who is running a service

**$ ps -ef |grep apache**

rmp -qa |grep httpd

**dpkg -l |grep apache**

find if apache was installed through apt manager

ls -la /usr/local/src

where locally compiled sources would be in

**Find out information about the operating system**

cat /etc/issue

cat /etc/\*-release

**Find out where the root is of the server along where the configuration**

**file is located.**

apachectl -v

**Manual way of finding configuration file on the server**

RHEL

find / |grep "httpd\.conf"

DEB

find / grep "apache2\.conf"

**Search for exact keywords in files for the files in current directory**

grep -Ri DocumentRoot .

**Check for syntax error in apache configuration**

apachectl -t

gives all virtual host IP, name, configuration location

apachectl -t -D DUMP\_VHOSTS

check to see which modules are enabled.

apachectl -t D DUMP\_MODULES

Find which apache modules are enabled in debian

apache2/mods-available

apache2/mods-enablaed

Enable or disable apaceh modudels

enable a module a2enmod

disable a module

a2dismod

Finding Error Logs. if " ${APACHE\_LOG\_DIR} " is returned, it means that it is an enviromental variable and "export APACHE\_LOG\_DIR" should be searched instead

grep -Ri ErrorLog /etc/apache2

grep -R "export APACHE\_LOG\_DIR" /etc/apache2

to see log files in real time

tail -f logfile