Devops Foundation - Linux Systems and Network Administration

School of Devops

Published
with GitBook

Table of Contents

Ops Essentials - Systems and Network Administration

This book is aimed to serve as a crash course for anyone with the Operations Engineer/ Systems Administrator / Systems Operations Background, to serve as a essential reference before taking up courses specific to Devops Engineers.

A Devops Engineer is typically someone with systems operations background with specific skills with new tools. He/She is responsible for enabling organizations with Devops Tools and Practices and help other team members such as Developers/QA Professionals to setup automated workflows. They are also responsible for building, deploying, automating and maintaining the infrastructure which not only runs the applications that the dev team is building, but also for setting up and maintaining the internal tools for CI/CD, Monitoring, Performance Measurement, Automated Provisioning and Configuration Management etc. He/She is also responsible optimizing applications and systems infrastructure. And when there are issues, he/she typically is the one who does initial troubleshooting, triaging and escalations.

To be a well rounded Devops Engineer, one has to have a knowledge on wide breadth of tools. Devops Engineers are typically Jack of All Trades, Master of a few. And most essentially, they should have a good understanding of underlying operating system. Even though role of Devops Engineer is not limitd to one OS, in most likeliness, its some flavor GNU/Linux. More over, today's systems are interconnected with complex networking systems. Hence, understanding of Linux as well as Computer Networks, servers as two essential skills when it comes to Devops Engineers. This book is been written to keeping this in mind and should serve as a essential reference for practical skills on systems and network administrators.

LICENSE

AUTHORS

- Gourav Shah
- Deepak Jain

- Ashwini Chaudhari
- Druva Ram

Linux Systems Administration

User and Group Managment

User and Group Managemnt

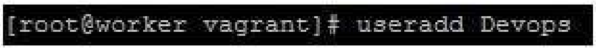
User Commands

The following commands are used to create, modify, delete, manipulate the properties of a user.

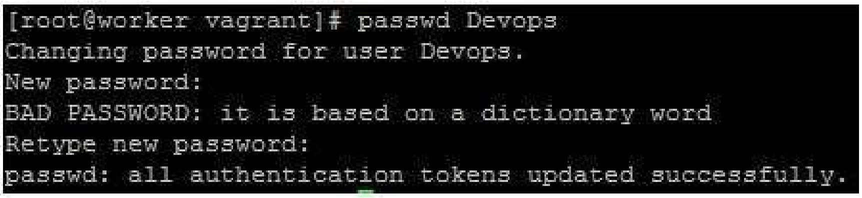
USERADD

This command Add/Creates user accounts in Linux. This command can be combined with various options

- useradd Devops - Adds a user named Devops. To unlock this account you need to set a password for this user
- passwd Devops - To set the password for the newly created user



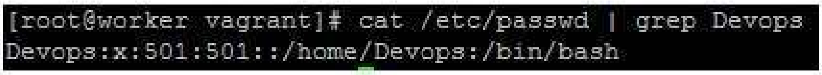
```
[root@worker vagrant]# useradd Devops
```



```
[root@worker vagrant]# passwd Devops
Changing password for user Devops.
New password:
BAD PASSWORD: it is based on a dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.
```

Once a new user is created, /etc/passwd file gets a new entry regarding the user created.

- cat /etc/passwd | grep Devops - Shows the entry created for user "Devops" in the passwd file



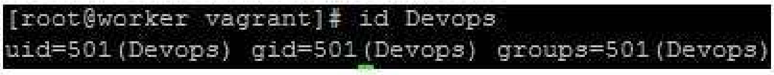
```
[root@worker vagrant]# cat /etc/passwd | grep Devops
Devops:x:501:501::/home/Devops:/bin/bash
```

Each line in the /etc/paaswd contains 7 columns which provides us the information about the user. It can be interpreted in the following way -

1. **Username** - Login name used to access the system - Devops
2. **Password** - The letter x signals that shadow passwords are used and that the hashed password is stored in /etc/shadow file
3. **UserID** - Devops has been assigned a UID of 501, which reflects the rule that the default UID values from 0 to 499 are typically reserved for system accounts
4. **GroupID** - The primary Group ID (GID) Group Identification Number stored in /etc/group file
5. **UserInfo** - Optional field to fill in extra information about the user like Role or Full Name of the user
6. **Home Directory** - Location of user's home directory
7. **Shell** - Location of user's shell

USERADD command can be combined with other options to customize user creation as per the requirement. Some of the options are -

- useradd -c "Devops User" Devops - Creates a user with "Devops user" as a comment in UserInfo field as stated above
- useradd -d /project/Devops Devops - Creates a user "Devops". Home directory for the user "Devops" is set as /project/Devops
- useradd -u 619 Devops - Creates a user "Devops". UserID for the user "Devops" is set as 619
- useradd -g 719 Devops - Creates a user "Devops". GroupID for the user "Devops" is set as 719
- useradd -g g0 -G g1,g2 Devops - Adds the user "Devops" to primary group g0 and to multiple groups(g1 and g2). You can check about the user is a part of which groups by using the command "id Devops"



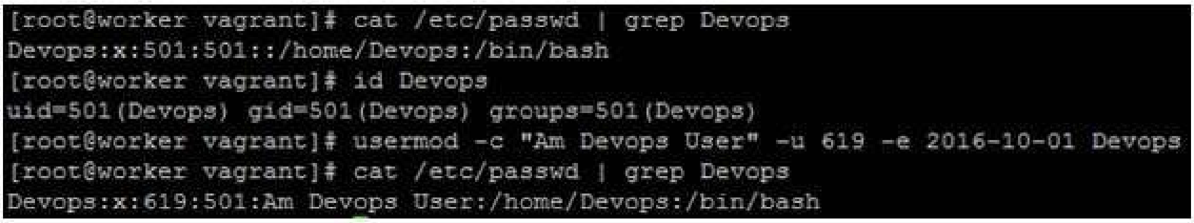
```
[root@worker vagrant]# id Devops
uid=501(Devops) gid=501(Devops) groups=501(Devops)
```

- useradd -e 2016-10-01 Devops - Creates a user "Devops" with account expiry date of October 1st,2016. Date should be mentioned in YYYY-MM-DD format. By default it is 0, never expires
- useradd -s /sbin/nologin Devops - Will add a user ‘tecmint‘ without login shell i.e. ‘/sbin/nologin‘ shell
- useradd -M Devops - Creates a user "Devops" with no home directory. When you combine useradd -m it will make sure that "Devops" user is created with Home directory if it does not exist

USERMOD

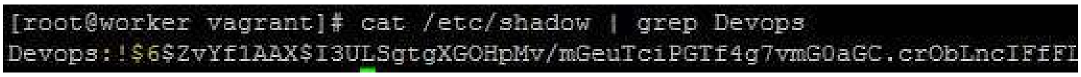
This command is similar to useradd except it takes actions on already existing users. It modifies the properties of already existing users . You can use this command with almost same options as you use with command useradd.

- usermod -c "Am Devops User" -u 619 -e 2016-10-01 Devops - Modifies the user "Devops" UserInfo property as stated in the above examples



```
[root@worker vagrant]# cat /etc/passwd | grep Devops
Devops:x:501:501::/home/Devops:/bin/bash
[root@worker vagrant]# id Devops
uid=501(Devops) gid=501(Devops) groups=501(Devops)
[root@worker vagrant]# usermod -c "Am Devops User" -u 619 -e 2016-10-01 Devops
[root@worker vagrant]# cat /etc/passwd | grep Devops
Devops:x:619:501:Am Devops User:/home/Devops:/bin/bash
```

- usermod -l Devops_ad Devops - Modifies the user login name from Devops to Devops_ad
- usermod -L Devops - Locks the user "Devops" account. After the account lock, Login is disabled and you will see a ! added before the encrypted password in /etc/shadow file means password is disabled an user account is locked



```
[root@worker vagrant]# cat /etc/shadow | grep Devops
Devops:!$6$ZvYf1AAX$I3ULSgtgXGOHpMv/mGeuTciPGTf4g7vmG0aGC.crObLncIFfFL
```

USERDEL

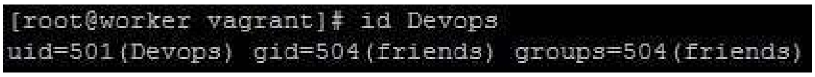
This command removes the user accounts and files associated to the user from Server/Workstation

- userdel -r Devops - Combining userdel with the -r option removes files in the user's home directory along with the home directory itself and the user's mail spool
- userdel -f Devops - This option forces the removal of the user account, even if the user is still logged in. This option is dangerous and may leave your system in an inconsistent state

ID

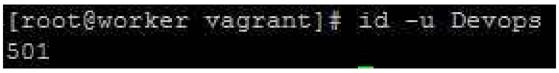
This command is used to get the system identifications of a specific user like UID, Groups a user belong to.

- id Devops - Displays the System identifications for the user "Devops"



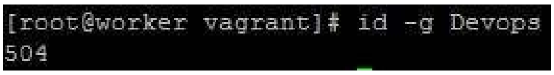
```
[root@worker vagrant]# id Devops
uid=501(Devops) gid=504(friends) groups=504(friends)
```

- id -u Devops - Displays UserID for the user "Devops"



```
[root@worker vagrant]# id -u Devops
501
```

- id -g Devops - Displays GroupId for the user "Devops"



```
[root@worker vagrant]# id -g Devops
504
```

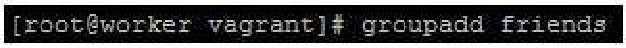
Group Commands

The following commands are used to create, modify, delete, manipulate the properties of a group.

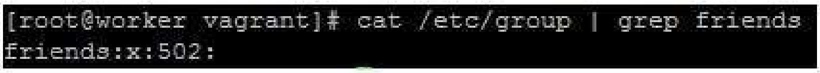
GROUPADD

Groups are a useful tool for permitting co-operation between different users. This command is used to add a new group to the system.

- groupadd friends - Adds a group named "friends" with default settings. You can gather more information about the group from the file /etc/group



```
[root@worker vagrant]# groupadd friends
```

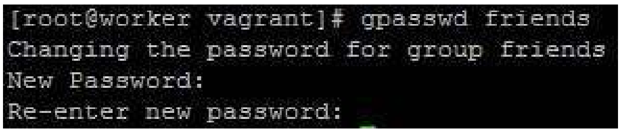


```
[root@worker vagrant]# cat /etc/group | grep friends
friends:x:502:
```

- groupadd -g 719 friends - Creates a group named "friends" set its GroupID as 719. When used with -g and GID already exists, groupadd refuses to create another group with existing GID
- groupadd -r friends - Creates a system group which are used for system purposes which practically means that GID is allocated from 1 to 499 if not specified

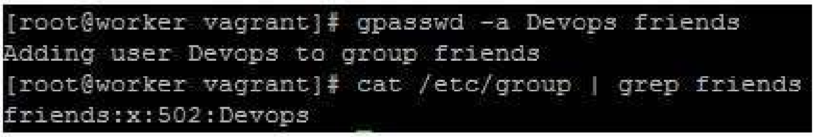
NOTE :- If you want to add an existing user to the named group, you can make use of the **gpasswd** command too instead of usermod and useradd. **gpasswd** is used to unlock the group and set password on the group

- gpasswd friends - Unlocks the group "friends" and sets the required password.



```
[root@worker vagrant]# gpasswd friends
Changing the password for group friends
New Password:
Re-enter new password:
```

- gpasswd -a Devops friends - Add the user "Devops" to group "friends". Replacing "-a" with "-r" command removes the user "Devops" from group "friends"



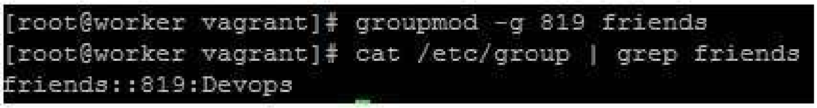
```
[root@worker vagrant]# gpasswd -a Devops friends
Adding user Devops to group friends
[root@worker vagrant]# cat /etc/group | grep friends
friends:x:502:Devops
```

- gpasswd --members Devops,Devops_ad friends - Adds a list of members(Devops,Devops_ad) to the group "friends". This command can be used to add multiple users to a group at a time.
- gpasswd -A Devops,Devops_ad friends - Makes Devops,Devops_ad group administrators. A group administrator can add and delete users as well as set, change, or remove the group password. A group can have more than one group administrator.
- gpasswd -r friends - Removes password authentication on the group "friends"

GROUPMOD

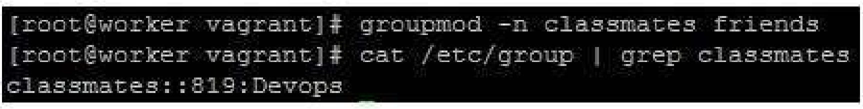
When a group already exists and you need to specify any of the options now, use the groupmod command. The logic of using groupmod is identical to groupadd as well as its syntax.

- groupmod -g 819 friends - Modifies the GroupID for the group "friends" to 819



```
[root@worker vagrant]# groupmod -g 819 friends
[root@worker vagrant]# cat /etc/group | grep friends
friends::819:Devops
```

- groupmod -n classmates friends - Replaces the name of group with "classmates"

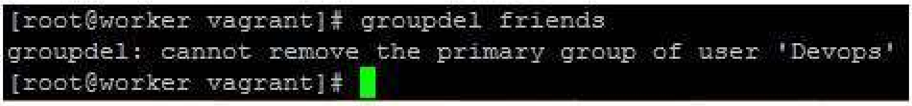


```
[root@worker vagrant]# groupmod -n classmates friends
[root@worker vagrant]# cat /etc/group | grep classmates
classmates::819:Devops
```

GROUPDEL

This command is used to delete the group. There are some conditions you should take care of before deleting a group. You may not remove the primary group of any existing user; you must remove the user before you remove that user's primary group.

- groupdel friends - Deletes the group named "friends". Below is the error if friends is the primary group of any user



```
[root@worker vagrant]# groupdel friends
groupdel: cannot remove the primary group of user 'Devops'
[root@worker vagrant]#
```

Lab 101 : Managing Users and Groups

Learn About User Commands

`$ man useradd`

`$ useradd --help`

`$ man id`

`$ id --help`

`$ man passwd`

`$ man usermod`

`$ man userdel`

Create a System User

Create the following users,

- dipti
- pooja
- ramesh
- suresh

Check the Default User Configurations

`$ useradd -D`

While creating users, mention the option to create home directories.

`$useradd -m dipti`

`$useradd -m ramesh`

`$useradd -m suresh`

`$useradd -m dipti`

Validate whether the users have been created

** Option 1 : Observe /etc/passwd

`$ tail /etc/passwd`

Expected Output:

dipti:x:501:501::/home/dipti:/bin/bash ramesh:x:502:502::/home/ramesh:/bin/bash suresh:x:503:503::/home/suresh:/bin/bash pooja:x:504:504::/home/pooja:/bin/bash

** Option 2 : using id command

`$ id dipti` `$ id ramesh` `$ id suresh` `$ id pooja`

Set Password

Check whether password exists, `$ cat /etc/passwd`

dipti:!!:16847:0:99999:7:::

Create password for each users, and validate,

```
$ passwd -m dipti
```

[Type and retype passwords]

New password: *

Retype new password: *

passwd: all authentication tokens updated successfully.

Validate

Logout as root user, and try logging in as the user you created password for.

`$ su - dipti` [verify you are able to login]

Also verify the contents of /etc/shadow which should have a encrypted string instead of !!

dipti:$6$t99EyAX/$3VCh3O9qjBEA7aevcRtV57B0HVNSM3WkhIXK9fe2JQMUQrsj8pxz5pDbmrnJIoDlJimes3kd.yXNUNqKpoGpa0:16847:0:99999:7:::

Commands to Managing Process

1)PS

2)TOP

3)PSTREE

4)FREE

5)UPTIME

6)KILL

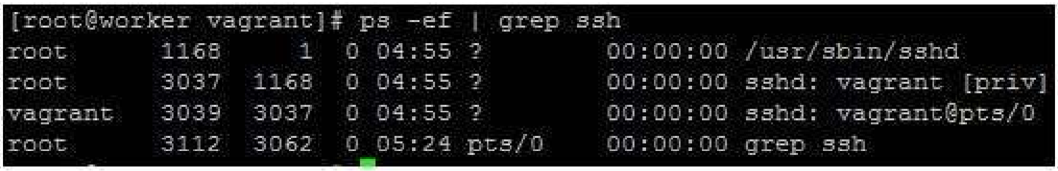
Managing Processes

PS

PS - This command is used list/see the processes that are running on the Linux system/server. Process is a running instance of a program. There are many commands which are used to monitor and control these processes in Linux and ps is one such command which is used to monitor them. Below are some of the examples which show their practical applications.

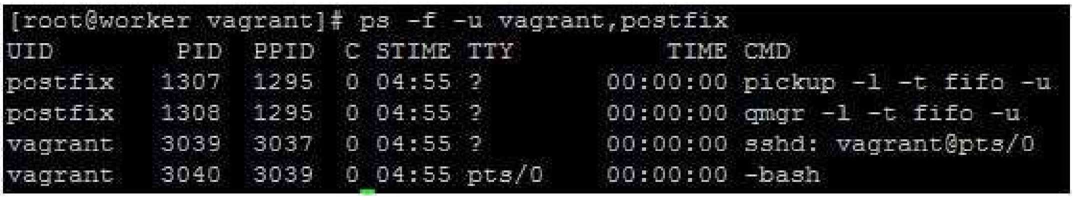
- ps -ef - List all the processes that are currently running, where -e is used to display all the process, -f is used to display full format listing

- ps -ef | grep ssh - List all the process which are related to ssh

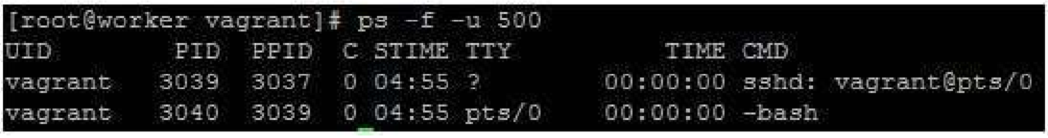


```
[root@worker vagrant]# ps -ef | grep ssh
root       1168     1  0 04:55 ?        00:00:00 /usr/sbin/sshd
root       3037  1168  0 04:55 ?        00:00:00 sshd: vagrant [priv]
vagrant    3039  3037  0 04:55 ?        00:00:00 sshd: vagrant@pts/0
root       3112  3062  0 05:24 pts/0    00:00:00 grep ssh
```

- ps -f -u vagrant,postfix - List the process related users vagrant and postfix. You can use UID too to find the process related to that particular user like (#ps -f -u 500)



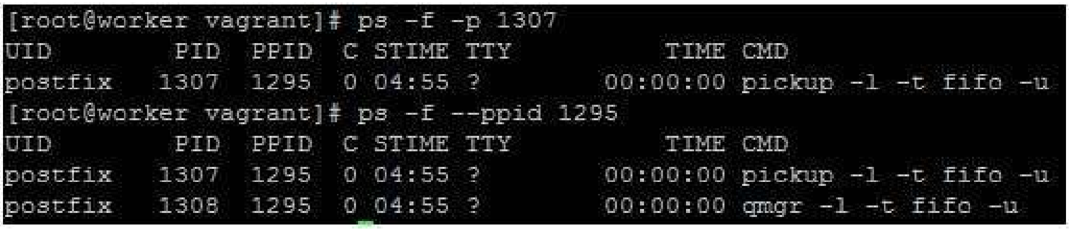
```
[root@worker vagrant]# ps -f -u vagrant,postfix
UID        PID  PPID  C STIME TTY          TIME CMD
postfix   1307  1295  0 04:55 ?        00:00:00 pickup -l -t fifo -u
postfix   1308  1295  0 04:55 ?        00:00:00 qmgr -l -t fifo -u
vagrant   3039  3037  0 04:55 ?        00:00:00 sshd: vagrant@pts/0
vagrant   3040  3039  0 04:55 pts/0    00:00:00 -bash
```



```
[root@worker vagrant]# ps -f -u 500
UID        PID  PPID  C STIME TTY          TIME CMD
vagrant   3039  3037  0 04:55 ?        00:00:00 sshd: vagrant@pts/0
vagrant   3040  3039  0 04:55 pts/0    00:00:00 -bash
```

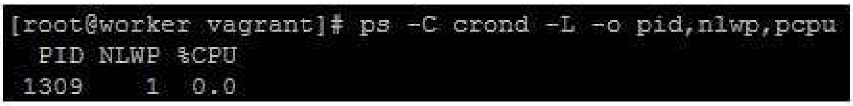
- ps -f -p 1307 - List the process which has PID of 1307. You can list multiple process by listing multiple PIDs separated by commas in a single command

- ps -f -ppid 1295 - List the process which has PPID of 1295



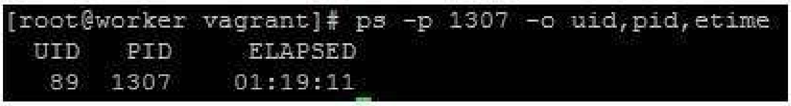
```
[root@worker vagrant]# ps -f -p 1307
UID        PID  PPID  C STIME TTY          TIME CMD
postfix   1307  1295  0 04:55 ?        00:00:00 pickup -l -t fifo -u
[root@worker vagrant]# ps -f --ppid 1295
UID        PID  PPID  C STIME TTY          TIME CMD
postfix   1307  1295  0 04:55 ?        00:00:00 pickup -l -t fifo -u
postfix   1308  1295  0 04:55 ?        00:00:00 qmgr -l -t fifo -u
```

- ps -C crond -L -o pid,pcpu,nlwp - List all threads for a particular process(crond). This is sometimes useful when a process gets hung and determine the threads running(NLWP)



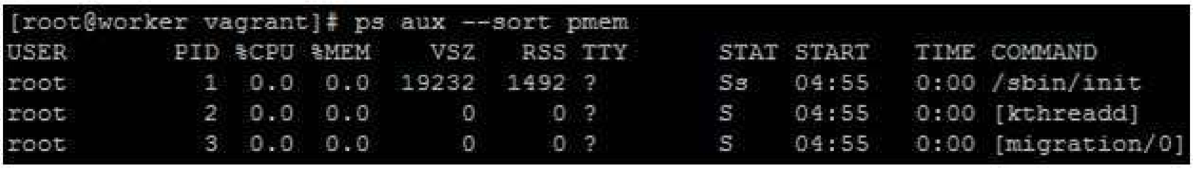
```
[root@worker vagrant]# ps -C crond -L -o pid,nlwp,pcpu
  PID NLWP %CPU
 1309    1  0.0
```

- ps -p 1307 -o uid,pid,etime - List the elapsed time for particular PID

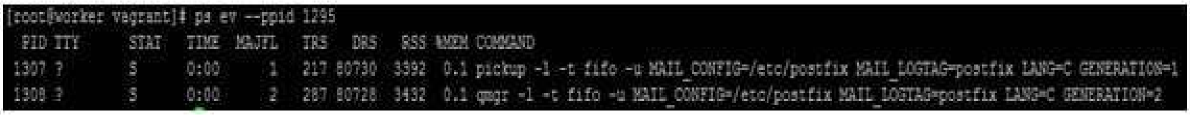


```
[root@worker vagrant]# ps -p 1307 -o uid,pid,etime
  UID   PID     ELAPSED
   89  1307    01:19:11
```

- ps aux --sort pmem - Sorts the highest memory consuming process at the bottom. You can further dig into that highest memory consuming PID/PPID and get the Memory percentage. You may use this data to find a memory leak. Where -v gives the components of virtual memroy



```
[root@worker vagrant]# ps aux --sort pmem
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0  19232  1492 ?        Ss   04:55   0:00 /sbin/init
root         2  0.0  0.0      0     0 ?        S    04:55   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    04:55   0:00 [migration/0]
```

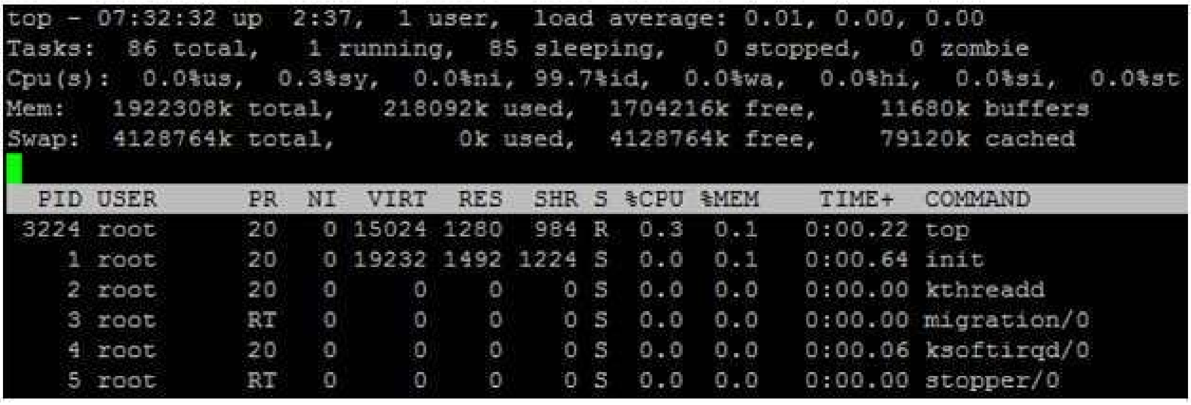


```
[root@worker vagrant]# ps ev --ppid 1295
  PID TTY      STAT   TIME  MAJFL   TRS   DRS   RSS %MEM COMMAND
 1307 ?        S      0:00      1   217 80730  3392  0.1 pickup -l -t fifo -u MAIL_CONFIG=/etc/postfix MAIL_LOGTAG=postfix LANG=C GENERATION=1
 1308 ?        S      0:00      2   287 80728  3432  0.1 qmgr -l -t fifo -u MAIL_CONFIG=/etc/postfix MAIL_LOGTAG=postfix LANG=C GENERATION=2
```

TOP

This command is much more interactive and real-time than the ps command. This also provides the percentage of resources actually consumed by the system.

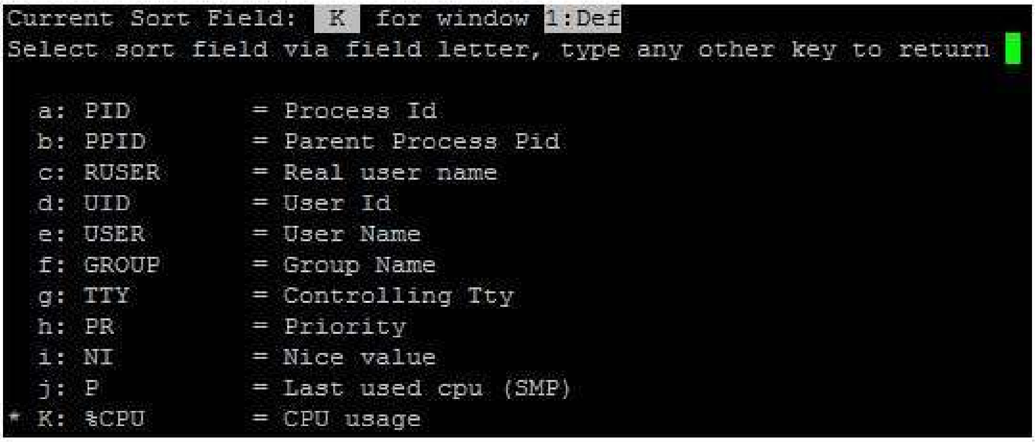
- top - Opens up an interactive session which gives information about the resource usage



```
top - 07:32:32 up  2:37,  1 user,  load average: 0.01, 0.00, 0.00
Tasks:  86 total,   1 running,  85 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.3%sy,  0.0%ni, 99.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   1922308k total,   218092k used,  1704216k free,    11680k buffers
Swap:  4128764k total,        0k used,  4128764k free,    79120k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 3224 root      20   0 15024 1280  984 R  0.3  0.1   0:00.22 top
    1 root      20   0 19232 1492 1224 S  0.0  0.1   0:00.64 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 migration/0
    4 root      20   0     0    0    0 S  0.0  0.0   0:00.06 ksoftirqd/0
    5 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 stopper/0
```

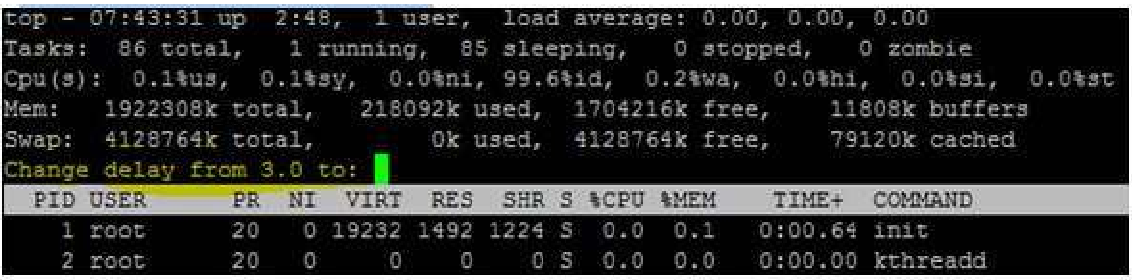
After the top command displays output screen, it is like an interactive session which require you to feed the commands to get the desired output as below

1. O - Gives you a range of options to sort according to the resources



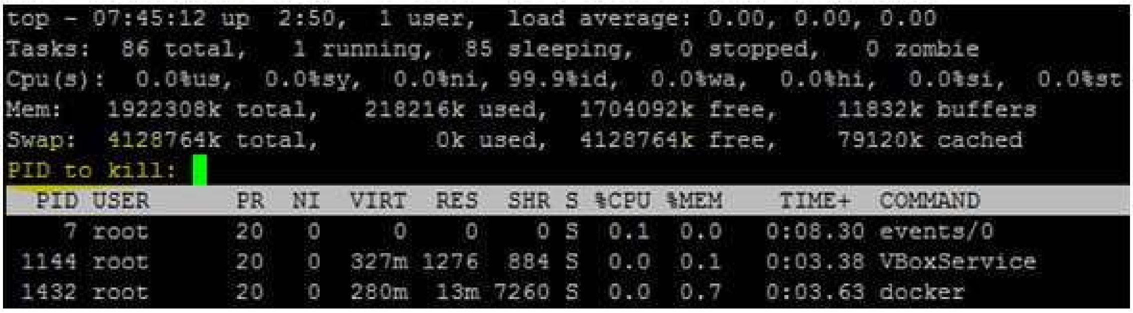
```
Current Sort Field:  K  for window 1:Def
Select sort field via field letter, type any other key to return

  a: PID        = Process Id
  b: PPID       = Parent Process Pid
  c: RUSER      = Real user name
  d: UID        = User Id
  e: USER       = User Name
  f: GROUP      = Group Name
  g: TTY        = Controlling Tty
  h: PR         = Priority
  i: NI         = Nice value
  j: P          = Last used cpu (SMP)
* K: %CPU       = CPU usage
```

2. d - Changes the auto refresh interval



```
top - 07:43:31 up  2:48,  1 user,  load average: 0.00, 0.00, 0.00
Tasks:  86 total,   1 running,  85 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.1%us,  0.1%sy,  0.0%ni, 99.6%id,  0.2%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   1922308k total,   218092k used,  1704216k free,    11808k buffers
Swap:  4128764k total,        0k used,  4128764k free,    79120k cached
Change delay from 3.0 to:
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    1 root      20   0 19232 1492 1224 S  0.0  0.1   0:00.64 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
```

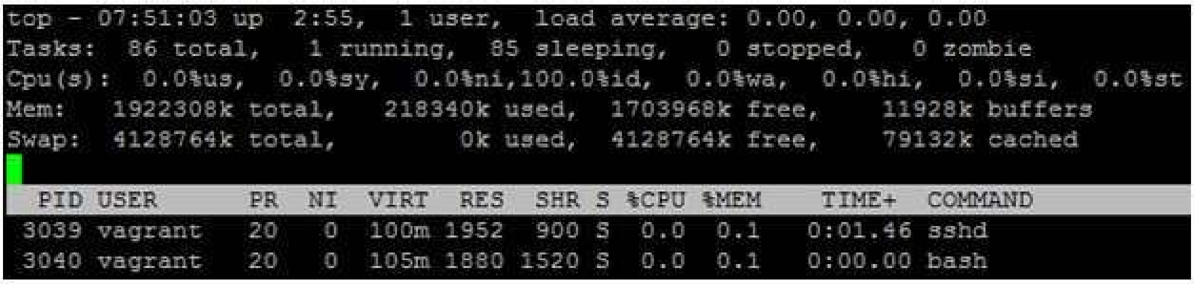
3. k - kill a process by desired PID



```
top - 07:45:12 up  2:50,  1 user,  load average: 0.00, 0.00, 0.00
Tasks:  86 total,   1 running,  85 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.0%sy,  0.0%ni, 99.9%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   1922308k total,   218216k used,  1704092k free,    11832k buffers
Swap:  4128764k total,        0k used,  4128764k free,    79120k cached
PID to kill:
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    7 root      20   0     0    0    0 S  0.1  0.0   0:08.30 events/0
 1144 root      20   0  327m 1276  884 S  0.0  0.1   0:03.38 VBoxService
 1432 root      20   0  280m  13m 7260 S  0.0  0.7   0:03.63 docker
```

4. SpaceTabKey - For instant refresh

5. top -u vagrant - List the process details for a specific user. In this case it is "vagrant"

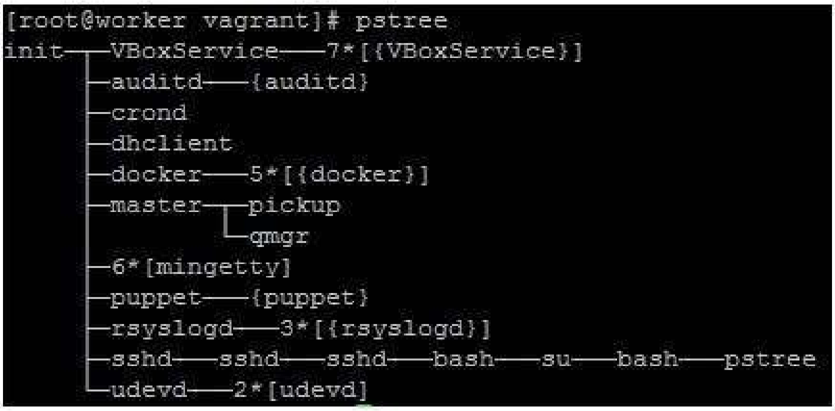


```
top - 07:51:03 up  2:55,  1 user,  load average: 0.00, 0.00, 0.00
Tasks:  86 total,   1 running,  85 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.0%sy,  0.0%ni,100.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   1922308k total,   218340k used,  1703968k free,    11928k buffers
Swap:  4128764k total,        0k used,  4128764k free,    79132k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 3039 vagrant   20   0  100m 1952  900 S  0.0  0.1   0:01.46 sshd
 3040 vagrant   20   0  105m 1880 1520 S  0.0  0.1   0:00.00 bash
```

PSTREE

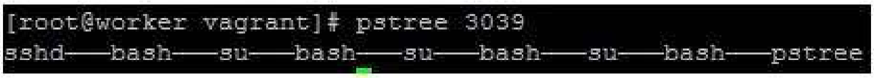
This command shows the processes that are running on the system too. But it is better in a visual way than ps command. This command shows the running processes in the form of a tree. It requires no root privileges to run this command.

- pstree - Gives you the process tree



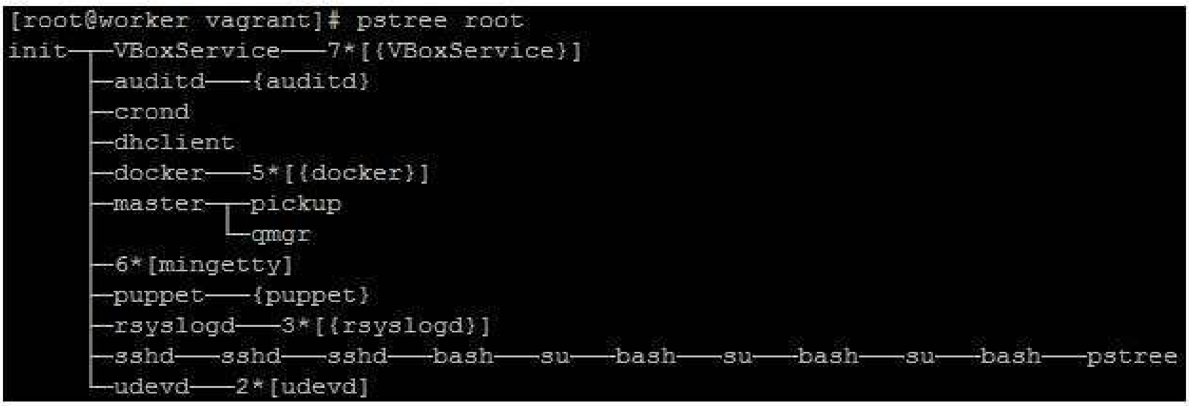
```
[root@worker vagrant]# pstree
init─┬─VBoxService───7*[{VBoxService}]
     ├─auditd───{auditd}
     ├─crond
     ├─dhclient
     ├─docker───5*[{docker}]
     ├─master─┬─pickup
     │        └─qmgr
     ├─6*[mingetty]
     ├─puppet───{puppet}
     ├─rsyslogd───3*[{rsyslogd}]
     ├─sshd───sshd───sshd───bash───su───bash───pstree
     └─udevd───2*[udevd]
```

- pstree 3039 - List a process based on the PID



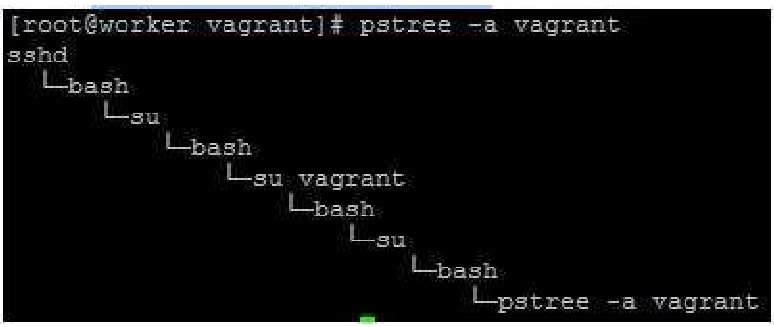
```
[root@worker vagrant]# pstree 3039
sshd───bash───su───bash───su───bash───su───bash───pstree
```

- pstree root - Displays process tree for the user "root"



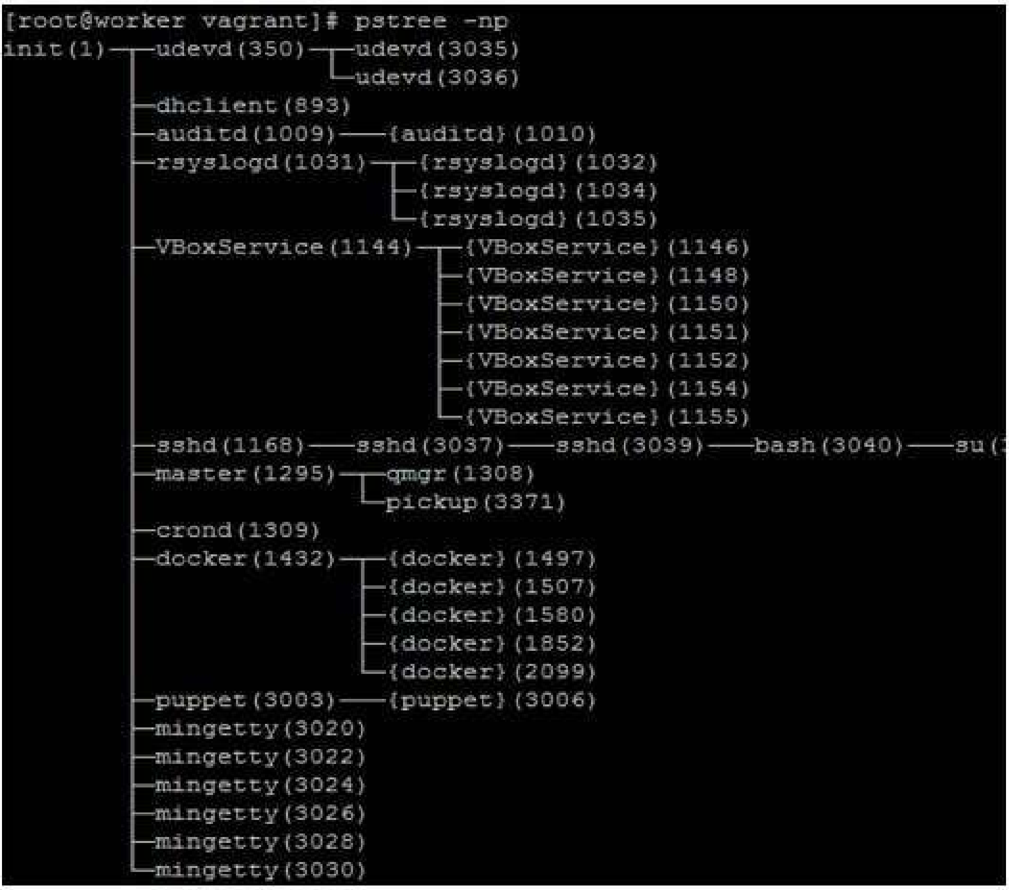
```
[root@worker vagrant]# pstree root
init─┬─VBoxService───7*[{VBoxService}]
     ├─auditd───{auditd}
     ├─crond
     ├─dhclient
     ├─docker───5*[{docker}]
     ├─master─┬─pickup
     │        └─qmgr
     ├─6*[mingetty]
     ├─puppet───{puppet}
     ├─rsyslogd───3*[{rsyslogd}]
     ├─sshd───sshd───sshd───bash───su───bash───su───bash───su───bash───pstree
     └─udevd───2*[udevd]
```

- pstree -a vagrant - Display the command line arguments associated with a particular process for particular user



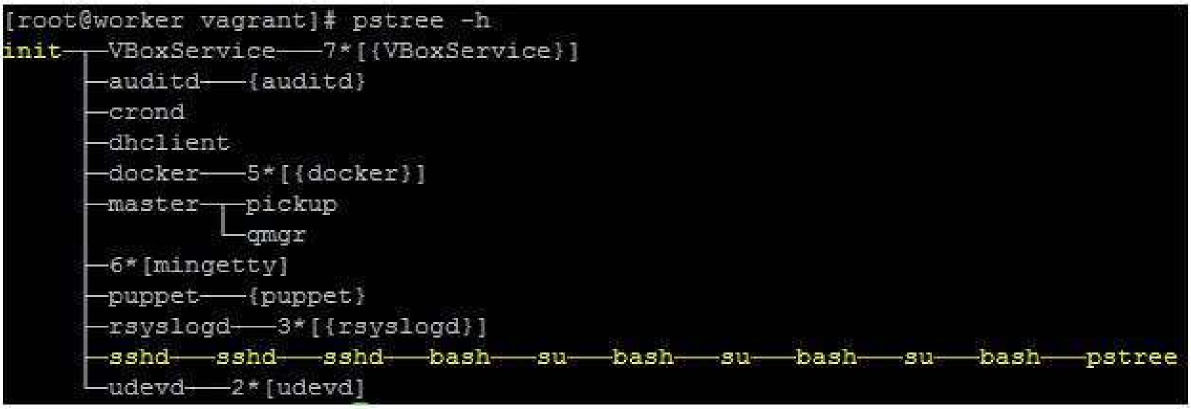
```
[root@worker vagrant]# pstree -a vagrant
sshd
  └─bash
      └─su
          └─bash
              └─su vagrant
                  └─bash
                      └─su
                          └─bash
                              └─pstree -a vagrant
```

- pstree -np - Displays the process in sorted way according to PID



```
[root@worker vagrant]# pstree -np
init(1)─┬─udevd(350)─┬─udevd(3035)
        │            └─udevd(3036)
        ├─dhclient(893)
        ├─auditd(1009)───{auditd}(1010)
        ├─rsyslogd(1031)─┬─{rsyslogd}(1032)
        │                ├─{rsyslogd}(1034)
        │                └─{rsyslogd}(1035)
        ├─VBoxService(1144)─┬─{VBoxService}(1146)
        │                   ├─{VBoxService}(1148)
        │                   ├─{VBoxService}(1150)
        │                   ├─{VBoxService}(1151)
        │                   ├─{VBoxService}(1152)
        │                   ├─{VBoxService}(1154)
        │                   └─{VBoxService}(1155)
        ├─sshd(1168)───sshd(3037)───sshd(3039)───bash(3040)───su(
        ├─master(1295)─┬─qmgr(1308)
        │              └─pickup(3371)
        ├─crond(1309)
        ├─docker(1432)─┬─{docker}(1497)
        │              ├─{docker}(1507)
        │              ├─{docker}(1580)
        │              ├─{docker}(1852)
        │              └─{docker}(2099)
        ├─puppet(3003)───{puppet}(3006)
        ├─mingetty(3020)
        ├─mingetty(3022)
        ├─mingetty(3024)
        ├─mingetty(3026)
        ├─mingetty(3028)
        └─mingetty(3030)
```

- pstree -h - Highlights the current process and its ancestors



```
[root@worker vagrant]# pstree -h
init─┬─VBoxService───7*[{VBoxService}]
     ├─auditd───{auditd}
     ├─crond
     ├─dhclient
     ├─docker───5*[{docker}]
     ├─master─┬─pickup
     │        └─qmgr
     ├─6*[mingetty]
     ├─puppet───{puppet}
     ├─rsyslogd───3*[{rsyslogd}]
     ├─sshd───sshd───sshd───bash───su───bash───su───bash───su───bash───pstree
     └─udevd───2*[udevd]
```

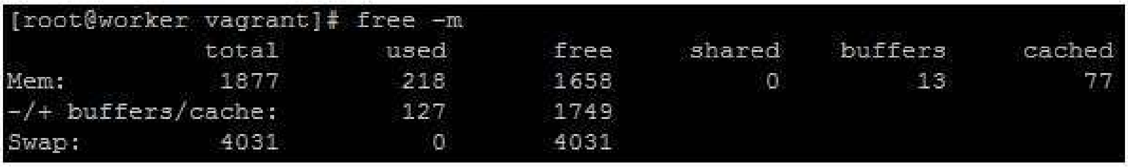
FREE

This command gives us the total amount of Free, Used Physical memory and Swap memory of the system. It also gives us the information about the Buffers used by the Kernel.

- free -m - Displays the amount of memory in MegaBytes. Amount of memory can also be seen in different units of Data. Following are the options

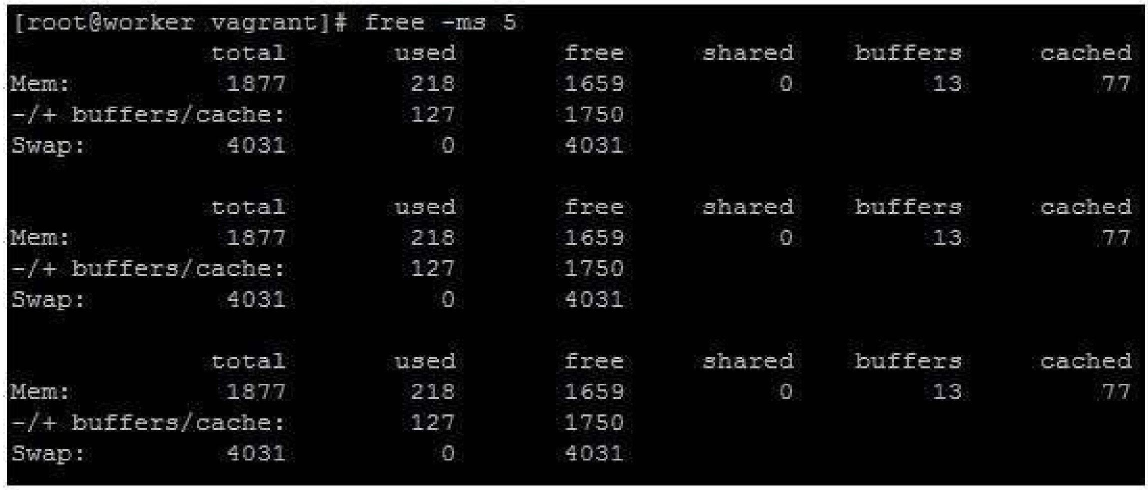
  1. -b for bytes
  2. -k for kilobytes

3. -m for megabytes
4. -g for gigabytes
5. --tera for terrabytes



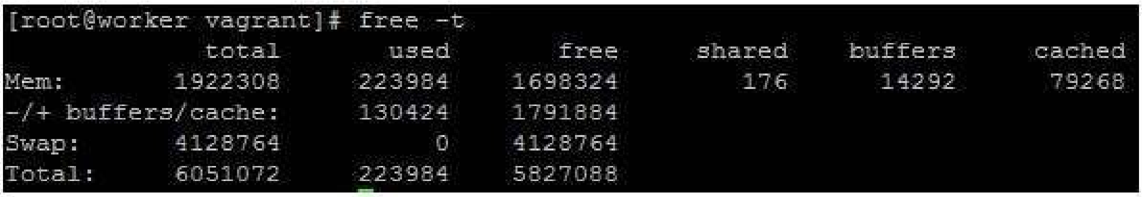
```
[root@worker vagrant]# free -m
             total       used       free     shared    buffers     cached
Mem:          1877        218       1658          0         13         77
-/+ buffers/cache:        127       1749
Swap:         4031          0       4031
```

- free -ms 5 - Displays the amount of memory in MegaBytes continuously every 5 seconds. "-s" is used in the command to achieve this cycle



```
[root@worker vagrant]# free -ms 5
             total       used       free     shared    buffers     cached
Mem:          1877        218       1659          0         13         77
-/+ buffers/cache:        127       1750
Swap:         4031          0       4031

             total       used       free     shared    buffers     cached
Mem:          1877        218       1659          0         13         77
-/+ buffers/cache:        127       1750
Swap:         4031          0       4031

             total       used       free     shared    buffers     cached
Mem:          1877        218       1659          0         13         77
-/+ buffers/cache:        127       1750
Swap:         4031          0       4031
```

- free -t - It will display an extra line showing the column totals

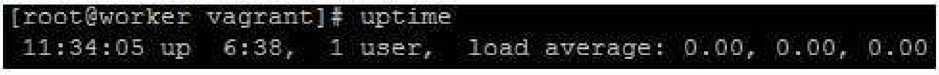


```
[root@worker vagrant]# free -t
             total       used       free     shared    buffers     cached
Mem:       1922308     223984    1698324        176      14292      79268
-/+ buffers/cache:     130424    1791884
Swap:      4128764          0    4128764
Total:     6051072     223984    5827088
```

UPTIME

This command gives you a one line display of current time, for how long the system is up, how users are logged on, system load averages

- uptime - Displays the uptime and average load

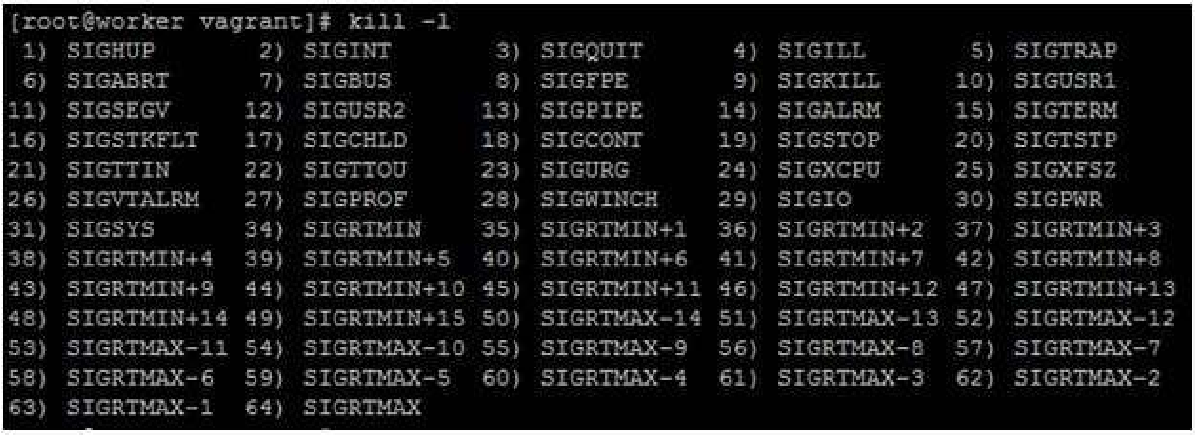


```
[root@worker vagrant]# uptime
 11:34:05 up  6:38,  1 user,  load average: 0.00, 0.00, 0.00
```

KILL

This command is used to send Terminate, Stop, Trap, Interrupt etc., signals to the process.

- kill -l - Displays the list of signal numbers that you can choose from



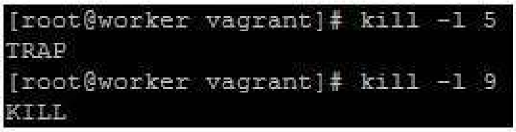
```
[root@worker vagrant]# kill -l
 1) SIGHUP       2) SIGINT       3) SIGQUIT      4) SIGILL       5) SIGTRAP
 6) SIGABRT      7) SIGBUS       8) SIGFPE       9) SIGKILL     10) SIGUSR1
11) SIGSEGV     12) SIGUSR2     13) SIGPIPE     14) SIGALRM     15) SIGTERM
16) SIGSTKFLT   17) SIGCHLD     18) SIGCONT     19) SIGSTOP     20) SIGTSTP
21) SIGTTIN     22) SIGTTOU     23) SIGURG      24) SIGXCPU     25) SIGXFSZ
26) SIGVTALRM   27) SIGPROF     28) SIGWINCH    29) SIGIO       30) SIGPWR
31) SIGSYS      34) SIGRTMIN    35) SIGRTMIN+1  36) SIGRTMIN+2  37) SIGRTMIN+3
38) SIGRTMIN+4  39) SIGRTMIN+5  40) SIGRTMIN+6  41) SIGRTMIN+7  42) SIGRTMIN+8
43) SIGRTMIN+9  44) SIGRTMIN+10 45) SIGRTMIN+11 46) SIGRTMIN+12 47) SIGRTMIN+13
48) SIGRTMIN+14 49) SIGRTMIN+15 50) SIGRTMAX-14 51) SIGRTMAX-13 52) SIGRTMAX-12
53) SIGRTMAX-11 54) SIGRTMAX-10 55) SIGRTMAX-9  56) SIGRTMAX-8  57) SIGRTMAX-7
58) SIGRTMAX-6  59) SIGRTMAX-5  60) SIGRTMAX-4  61) SIGRTMAX-3  62) SIGRTMAX-2
63) SIGRTMAX-1  64) SIGRTMAX
```

- kill - Generates SIGTERM signal requesting process to terminate
- kill -9 - Generates SIGKILL signal for process to terminate immediately or forcefully.You can kill multiple PIDs in the following way (kill -9 1234 4356 234) where 1234, 4356, 234 are distinct processes
- Kill -9 can be fed to the system in multiple ways like below

```
1. kill -s SIGKILL <PID> where SIGKILL is the signal name
2. kill -s SIGKILL <PID> where SIGKILL is the signal name
3. kill -s  9 <PID> where 9 is the signal number
```

NOTE :- Signal number can be determined by using the above mentioned command kill -l. Signal name can be found out by the same command too. The shorthand notation of the signal name can be found by the command kill -l signalnumber. Below is the example :-

- 9 is the signal number for SIGKILL. Getting the shorthand notation -



```
[root@worker vagrant]# kill -l 5
TRAP
[root@worker vagrant]# kill -l 9
KILL
```

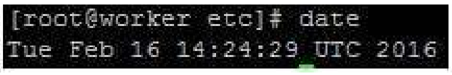
Scheduing Jobs

L 103 - Scheduling Jobs with Crontab and At

DATE & TIME ZONE

DATE - This command is used to get the information about Day, Current Date,Time,Timezone,Year

- #date



```
[root@worker etc]# date
Tue Feb 16 14:24:29 UTC 2016
```

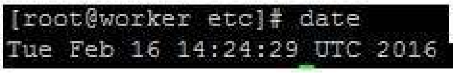
- #date +%D -s YYYY-MM-DD - Changes the date of the system/server (#date +%D -s 2016-04-01)

- #date +%T -s HH:MM:SS - Changes the time on the system/server(#date +%T -s 23:26:00 -u) where "-u" is used if your system clock is set to use UTC

Changing Time Zones

Time zones are used to set time on the servers according to your requirement. There are many methods in practice to change the time zones. One of the easiest way of changing the time zone is as follows -

.#date - Displays the date and current time and time zone and it is UTC currently

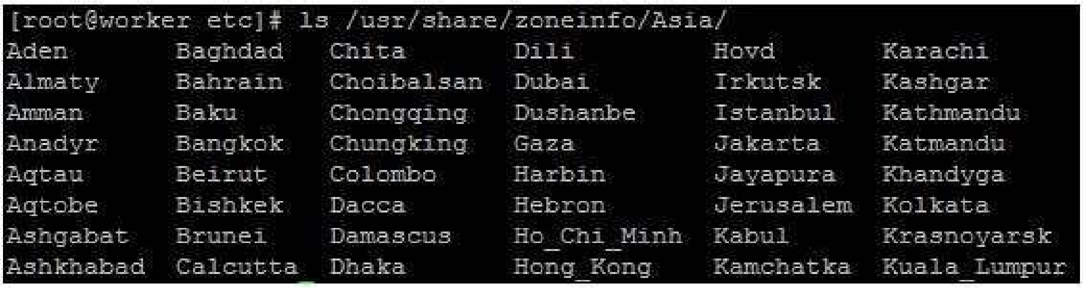


```
[root@worker etc]# date
Tue Feb 16 14:24:29 UTC 2016
```

.#cd /etc/ - Navigate to the directory /etc

.#rm localtime - Remove the file named "localtime"

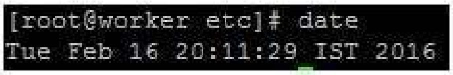
.#ls /usr/share/zoneinfo/Asia - Lists all the timezones available in Asia. If you list the folder /usr/share/zoneinfo/, you can see all the Zones available. You can choose the timezone accordingly



```
[root@worker etc]# ls /usr/share/zoneinfo/Asia/
Aden       Baghdad   Chita       Dili         Hovd       Karachi
Almaty     Bahrain   Choibalsan  Dubai        Irkutsk    Kashgar
Amman      Baku      Chongqing   Dushanbe     Istanbul   Kathmandu
Anadyr     Bangkok   Chungking   Gaza         Jakarta    Katmandu
Aqtau      Beirut    Colombo     Harbin       Jayapura   Khandyga
Aqtobe     Bishkek   Dacca       Hebron       Jerusalem  Kolkata
Ashgabat   Brunei    Damascus    Ho_Chi_Minh  Kabul      Krasnoyarsk
Ashkhabad  Calcutta  Dhaka       Hong_Kong    Kamchatka  Kuala_Lumpur
```

.#ln -s /usr/share/zoneinfo/Asia/Calcutta localtime - Link the Calcutta file from Asia directory to file "localtime"

.#date - Displays time from IST timezone and your timezone is changed



```
[root@worker etc]# date
Tue Feb 16 20:11:29 IST 2016
```

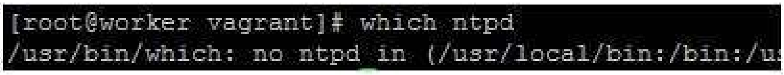
Network Time Protocol(NTP)

The Network Time Protocol (NTP) enables the accurate settings of time and date information in order to keep the time clocks on networked computer systems synchronized to a common reference over the network or the Internet. It is protocol which is run over the port "123" and uses UDP.

Below are the steps to configure NTP server on your local machine -

NTP Server actions

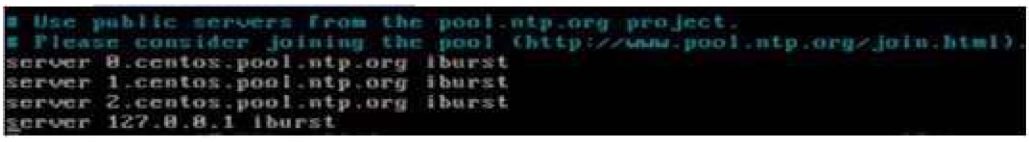
- #which ntpd - We will get know whether NTP package is installed on the machine and if installed it will show the executable file path



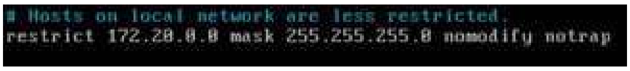
```
[root@worker vagrant]# which ntpd
/usr/bin/which: no ntpd in (/usr/local/bin:/bin:/u
```

- #yum install ntp - Installs the NTP package on your local machine

- #vi /etc/ntp.conf - Edit the configuration as per the requirement. I have removed server 3.centos.pool.ntp.org and added the loopback address,so that even if my Internet network goes down, I can fetch the time my local network or the hardware clock from my machine. Further, you need to allow clients from your networks to synchronize time with this server. To accomplish this, add the following line to NTP configuration file, where restrict statement controls, what network is allowed to query and sync time. REPLACE NETWORK IPs ACCORDINGLY



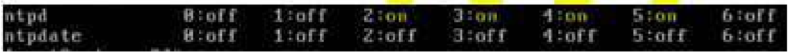
```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.centos.pool.ntp.org iburst
server 1.centos.pool.ntp.org iburst
server 2.centos.pool.ntp.org iburst
server 127.0.0.1 iburst
```



```
# Hosts on local network are less restricted.
restrict 172.28.0.0 mask 255.255.255.0 nomodify notrap
```

- chkconfig ntpd on - To make NTP daemon persistent even if the machine reboots, use chkconfig

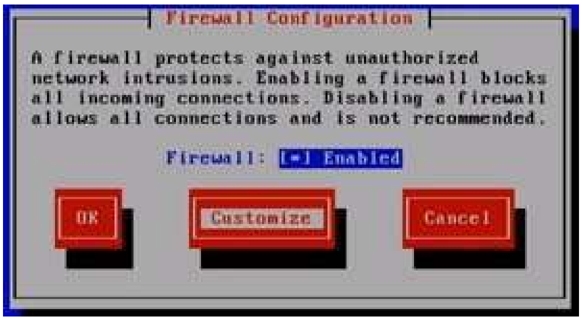
- chkconfig --list | grep ntpd - Just to br sure that chkconfig is configured



```
ntpd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
ntpdate         0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

- service ntpd start - Start the ntpd service

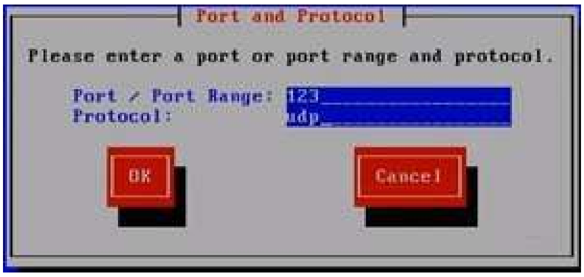
- system-config-firewall - Configure the firewall for port 123 which is used by ntp on the NTP server/current server



Firewall Configuration

A firewall protects against unauthorized network intrusions. Enabling a firewall blocks all incoming connections. Disabling a firewall allows all connections and is not recommended.

Firewall: [*] Enabled

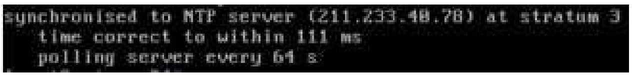


Port and Protocol

Please enter a port or port range and protocol.

Port / Port Range: 123
Protocol: udp

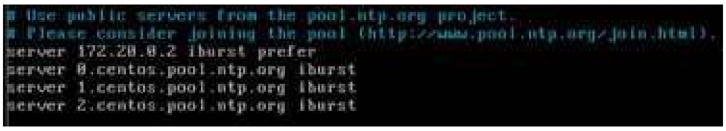
- ntpstat - To check if the ntp service is up and running. From the image you can see there is difference of 111ms which will reduce gradually to lower values. Another way to cross check the service is by the command #ntpq -p which shows the pool of ntp servers your server is connected to.



```
synchronised to NTP server (211.233.40.78) at stratum 3
   time correct to within 111 ms
   polling server every 64 s
```

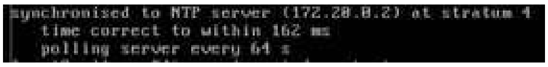
Client Server actions

- Follow the steps 1 and 2 as mentioned above in the NTP server actions
- vi /etc/ntp.conf - Enter the IP address of NTP server we have configured above, in the ntp.conf file of Client server. Add "prefer" in the entry you make in the ntp.conf file to use configured NTP server. Rest of the servers are used just as backup if your NTP server goes down.



```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 172.20.0.2 iburst prefer
server 0.centos.pool.ntp.org iburst
server 1.centos.pool.ntp.org iburst
server 2.centos.pool.ntp.org iburst
```

- chkconfig ntpd on - To make NTP daemon persistent even if the machine reboots
- ntpstat - With this you can see that your Client server is synchronised with your own NTP server



```
synchronised to NTP server (172.20.0.2) at stratum 4
   time correct to within 162 ms
   polling server every 64 s
```

MySQL

1. Install MySQL Server
2. Examine the MySQL Configurations
3. Generate MySQL Server Configurations using Percona’s Tool.
4. Install and Configure MySQL Admin
5. Connect to MySQL Database
6. Create a database and Tables
7. Query Data - SELECT
8. Modify Data - UPDATE/ALTER
9. Backup MySQL Database

Apache

10. Install Apache Web Server with Default Virtual host
11. Examine Apache Configurations
12. Create Virtual Hosts
13. Add Redirect and Rewrite Rules with Apache
14. Configure SSL with Apache

PHP Application

15. Install PHP
16. Configure PHP with Apache
17. Install and setup Wordpress with Apache with MySQL Backend

Nginx

18. Install Nginx
19. Examine Nginx Configurations
20. Configure Nginx as Load Balancer/ Reverse Proxy
21. Configure SSL Certificate with Nginx

Tomcat

22. Install Java and prerequisites
23. Install Tomcat
24. Tomcat Configurations
25. Deploy a Sample Application with Tomcat

Install MySQL Server

Install mysql-server

```
sudo yum install mysql-server
```

Start mysqld service

```
sudo service mysqld start
```

Validate

```
sudo service mysqld status
```

[Expected Output: "Should be Running"]

install MYSQL Client

```
sudo yum install mysql
```

To set/reset set a root MySQL password

Guide to reset root password

Reset MySQL Root Password (On MySQL Version 5.7.6 and later)

Stop MySQL Service and Start it again with --skip-grant-tables options

```
sudo service mysqld stop sudo mysqld_safe --skip-grant-tables &
```

Login to mysql server

```
mysql
```

From MySQL Prompt reset the password

```
FLUSH PRIVILEGES;
```

For MySQL 5.7.6 and later

```
ALTER USER 'root'@'localhost' IDENTIFIED BY 'password';
```

For MySQL 5.7.5 and earlier

```
SET PASSWORD FOR 'root'@'localhost' = PASSWORD('[password]');
```

d to logout

Restart MySQL Service

```
service mysqld stop service mysqld start
```

Validate

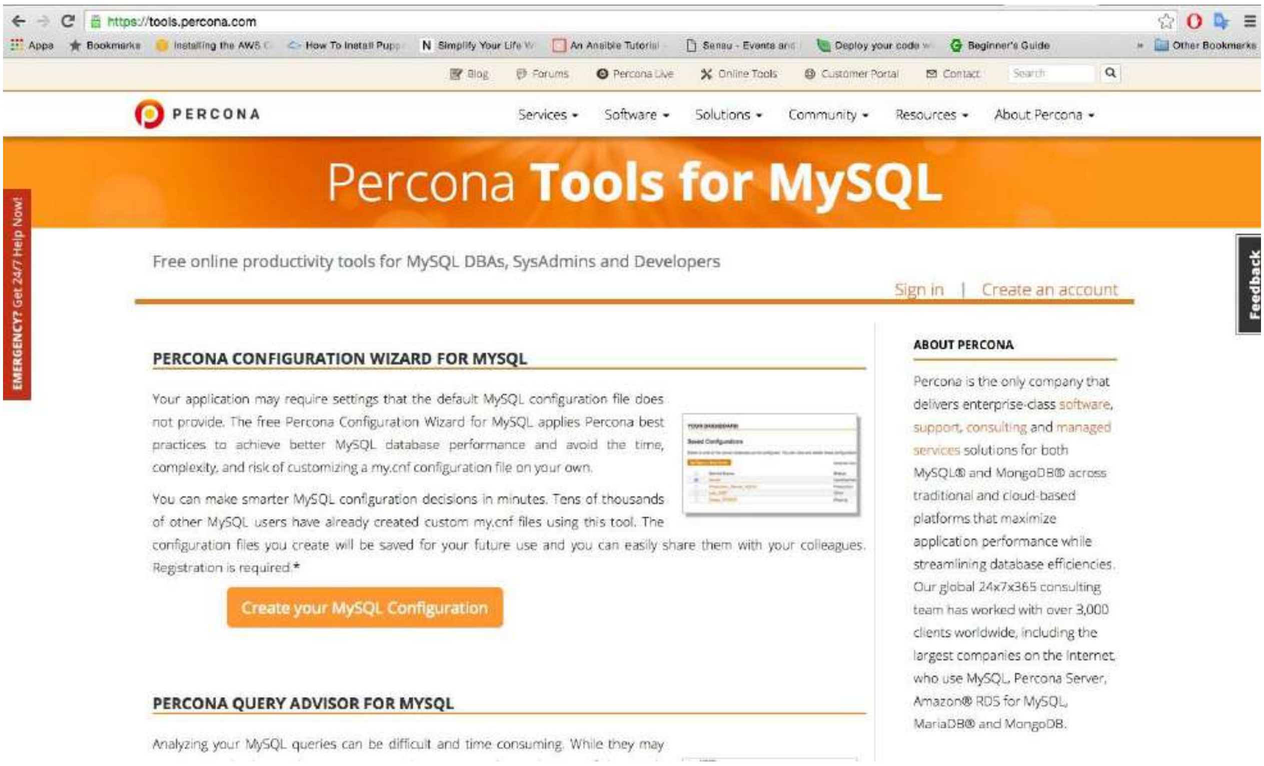
mysql -u root -p [Enter Password and login]

Generate MySQL Configs using Percona Wizard

- **Visit to Percona site(https://tools.percona.com)**

  Percona Tools

- **Click on Create Your mysql Configuration**



Percona **Tools for MySQL**

Free online productivity tools for MySQL DBAs, SysAdmins and Developers

PERCONA CONFIGURATION WIZARD FOR MYSQL

Your application may require settings that the default MySQL configuration file does not provide. The free Percona Configuration Wizard for MySQL applies Percona best practices to achieve better MySQL database performance and avoid the time, complexity, and risk of customizing a my.cnf configuration file on your own.

You can make smarter MySQL configuration decisions in minutes. Tens of thousands of other MySQL users have already created custom my.cnf files using this tool. The configuration files you create will be saved for your future use and you can easily share them with your colleagues. Registration is required.*

PERCONA QUERY ADVISOR FOR MYSQL

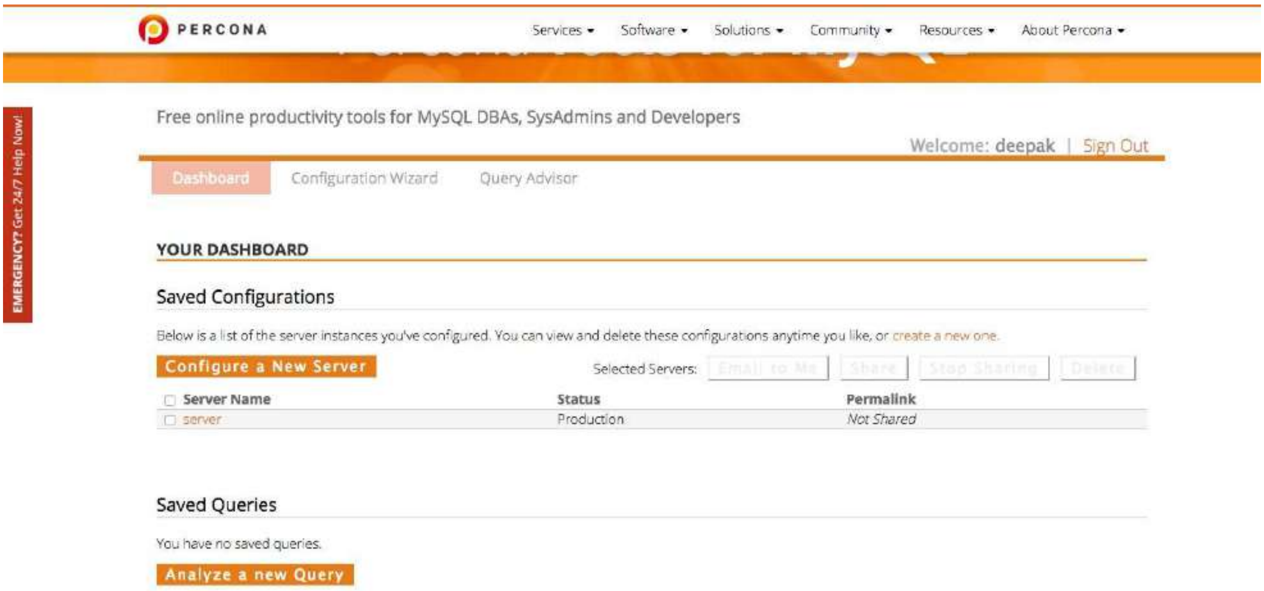
Analyzing your MySQL queries can be difficult and time consuming. While they may

ABOUT PERCONA

Percona is the only company that delivers enterprise-class software, support, consulting and managed services solutions for both MySQL® and MongoDB® across traditional and cloud-based platforms that maximize application performance while streamlining database efficiencies. Our global 24x7x365 consulting team has worked with over 3,000 clients worldwide, including the largest companies on the Internet, who use MySQL, Percona Server, Amazon® RDS for MySQL, MariaDB® and MongoDB.

- **Create An account or sign in (if you already have an account)**

- **goto Dashboard and Click on configure a new server**



PERCONA
Services ▾ Software ▾ Solutions ▾ Community ▾ Resources ▾ About Percona ▾
EMERGENCY? Get 24/7 Help Now!

Free online productivity tools for MySQL DBAs, SysAdmins and Developers

Welcome: deepak | Sign Out

Dashboard
Configuration Wizard
Query Advisor

YOUR DASHBOARD

Saved Configurations

Below is a list of the server instances you've configured. You can view and delete these configurations anytime you like, or create a new one.

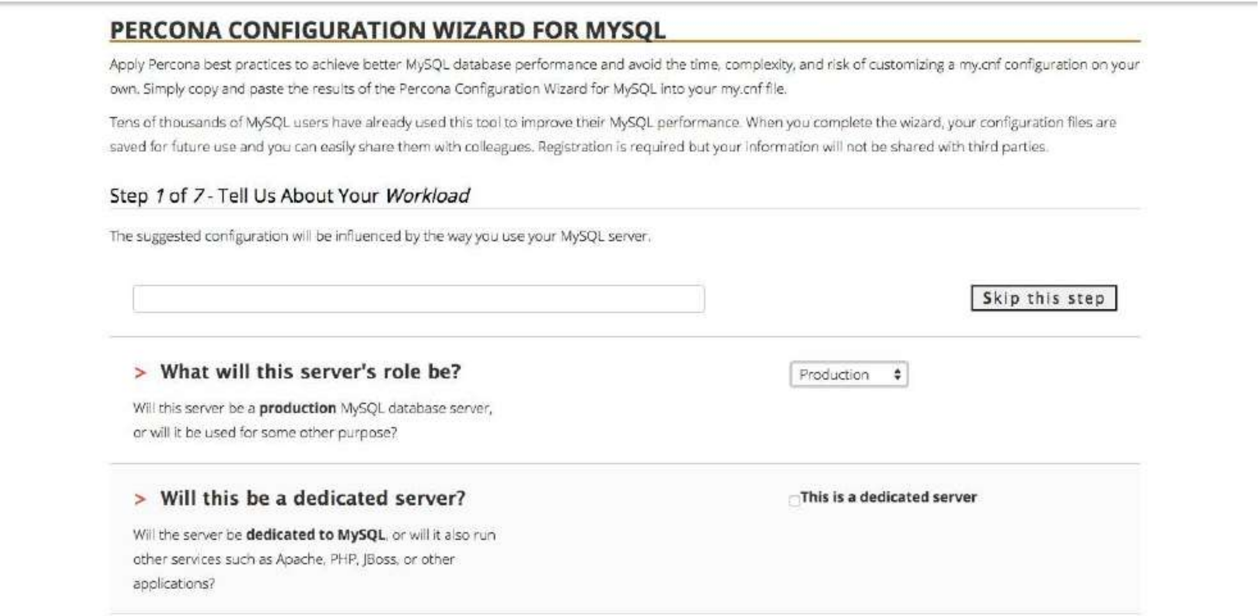
Configure a New Server
Selected Servers: Email to Me Share Stop Sharing Delete

□ Server Name	Status	Permalink
□ server	Production	*Not Shared*

Saved Queries

You have no saved queries.

- **answer the question on configuration wizard and click on next (you can leave some field blank which are not mandatory)**



PERCONA CONFIGURATION WIZARD FOR MYSQL

Apply Percona best practices to achieve better MySQL database performance and avoid the time, complexity, and risk of customizing a my.cnf configuration on your own. Simply copy and paste the results of the Percona Configuration Wizard for MySQL into your my.cnf file.

Tens of thousands of MySQL users have already used this tool to improve their MySQL performance. When you complete the wizard, your configuration files are saved for future use and you can easily share them with colleagues. Registration is required but your information will not be shared with third parties.

Step *1* of *7* - Tell Us About Your *Workload*

The suggested configuration will be influenced by the way you use your MySQL server.

> **What will this server's role be?**

Will this server be a **production** MySQL database server, or will it be used for some other purpose?

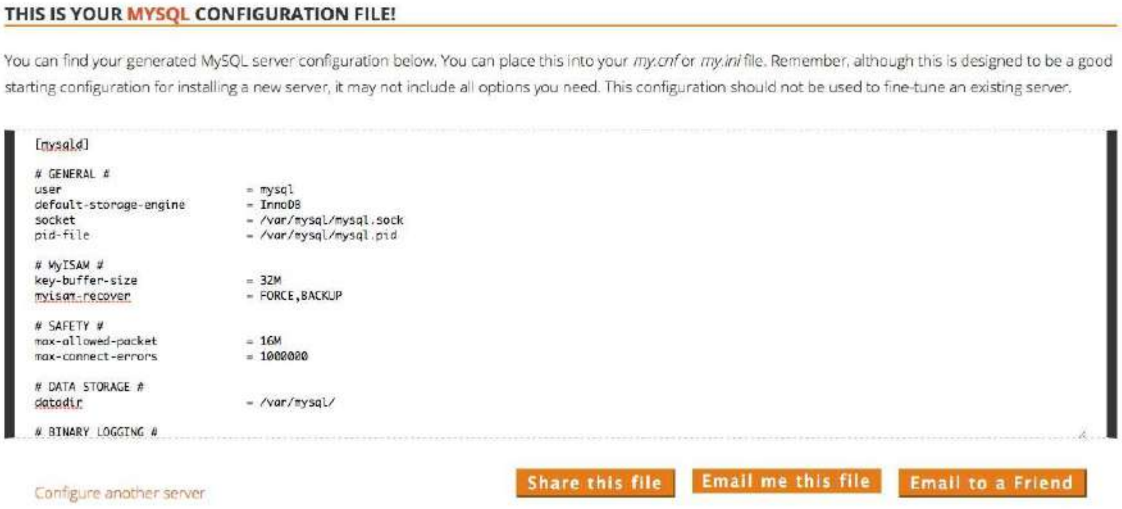
Production

> **Will this be a dedicated server?**

Will the server be **dedicated to MySQL**, or will it also run other services such as Apache, PHP, JBoss, or other applications?

□ **This is a dedicated server**

- **after click on DONE you will get your mysql configuration file**



THIS IS YOUR MYSQL CONFIGURATION FILE!

You can find your generated MySQL server configuration below. You can place this into your *my.cnf* or *my.ini* file. Remember, although this is designed to be a good starting configuration for installing a new server, it may not include all options you need. This configuration should not be used to fine-tune an existing server.

```
[mysqld]

# GENERAL #
user                           = mysql
default-storage-engine         = InnoDB
socket                         = /var/mysql/mysql.sock
pid-file                       = /var/mysql/mysql.pid

# MyISAM #
key-buffer-size                = 32M
myisam-recover                 = FORCE,BACKUP

# SAFETY #
max-allowed-packet             = 16M
max-connect-errors             = 1000000

# DATA STORAGE #
datadir                        = /var/mysql/

# BINARY LOGGING #
```

Install And Configure Apache

• Install apache

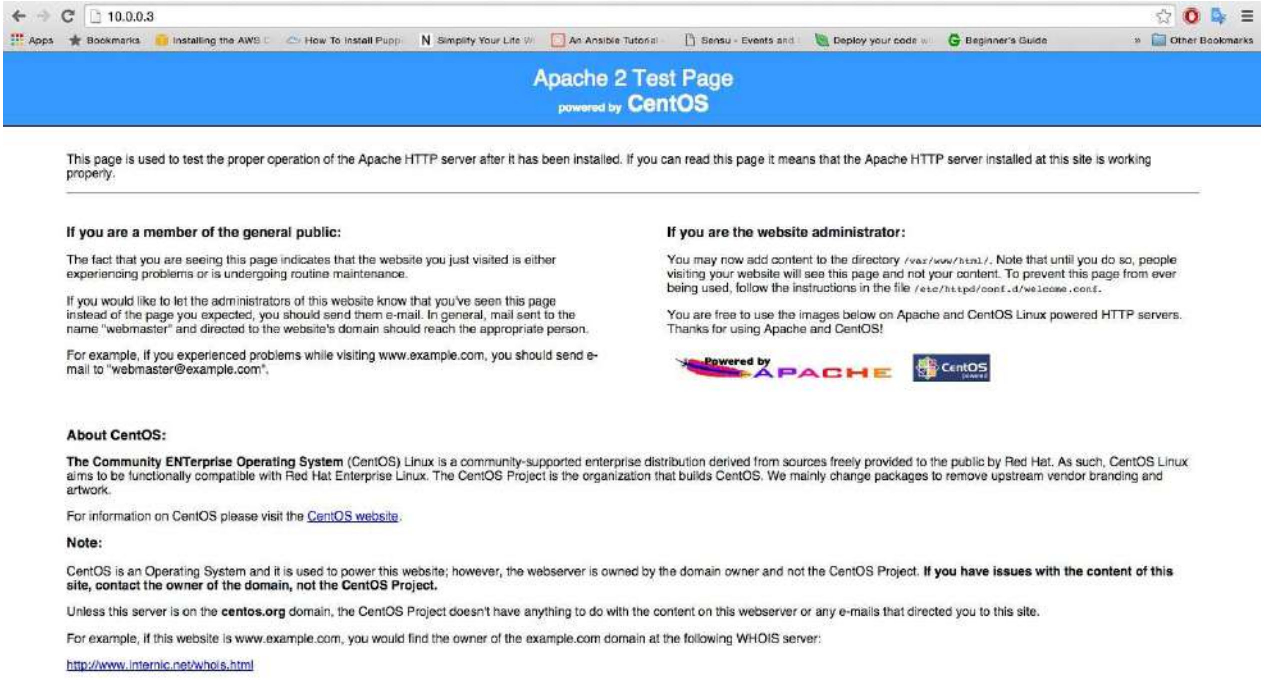
```
sudo yum install httpd
```

• Start httpd service

```
sudo service httpd start
```

direct your browser to your server’s IP address

Note :- if you are not able to access check firewall(iptables). Sudo service iptables stop .



Apache 2 Test Page
powered by CentOS

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the images below on Apache and CentOS Linux powered HTTP servers. Thanks for using Apache and CentOS!

About CentOS:

The Community ENTerprise Operating System (CentOS) Linux is a community-supported enterprise distribution derived from sources freely provided to the public by Red Hat. As such, CentOS Linux aims to be functionally compatible with Red Hat Enterprise Linux. The CentOS Project is the organization that builds CentOS. We mainly change packages to remove upstream vendor branding and artwork.

For information on CentOS please visit the CentOS website.

Note:

CentOS is an Operating System and it is used to power this website; however, the webserver is owned by the domain owner and not the CentOS Project. **If you have issues with the content of this site, contact the owner of the domain, not the CentOS Project.**

Unless this server is on the **centos.org** domain, the CentOS Project doesn't have anything to do with the content on this webserver or any e-mails that directed you to this site.

For example, if this website is www.example.com, you would find the owner of the example.com domain at the following WHOIS server:

http://www.internic.net/whois.html

• Create Virtual Hosts

1. create below directory

```
sudo mkdir -p /var/www/schoolofdevops
 cd /var/www/schoolofdevops
```

2. create index.html file and put below content

```
<h1> Welcome to School of Devops</h1>
```

3. create new virtual host file

```
sudo touch /etc/httpd/conf.d/schoolofdevops.conf
```

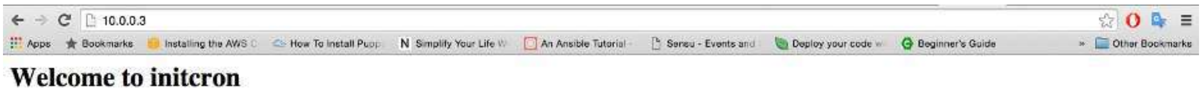
4. put below contenet in new virtual host file i.e. schoolofdevops.conf

```
<VirtualHost *:80>
     ServerAdmin root
     ServerName schoolofdevops.org
     ServerAlias www.schoolofdevops.org
     DocumentRoot /var/www/schoolofdevops/
</VirtualHost>
```

5. restart httpd service

```
sudo service httpd restart
```

6. visit our new page (http://serverip)



Welcome to initcron

- ## attach ssl certificate to schoolofdevops site

1. create ssl certificate and store them in /etc/httpd/ssl directory

follow this lab to create ssl certificate

2. install mod_ssl module

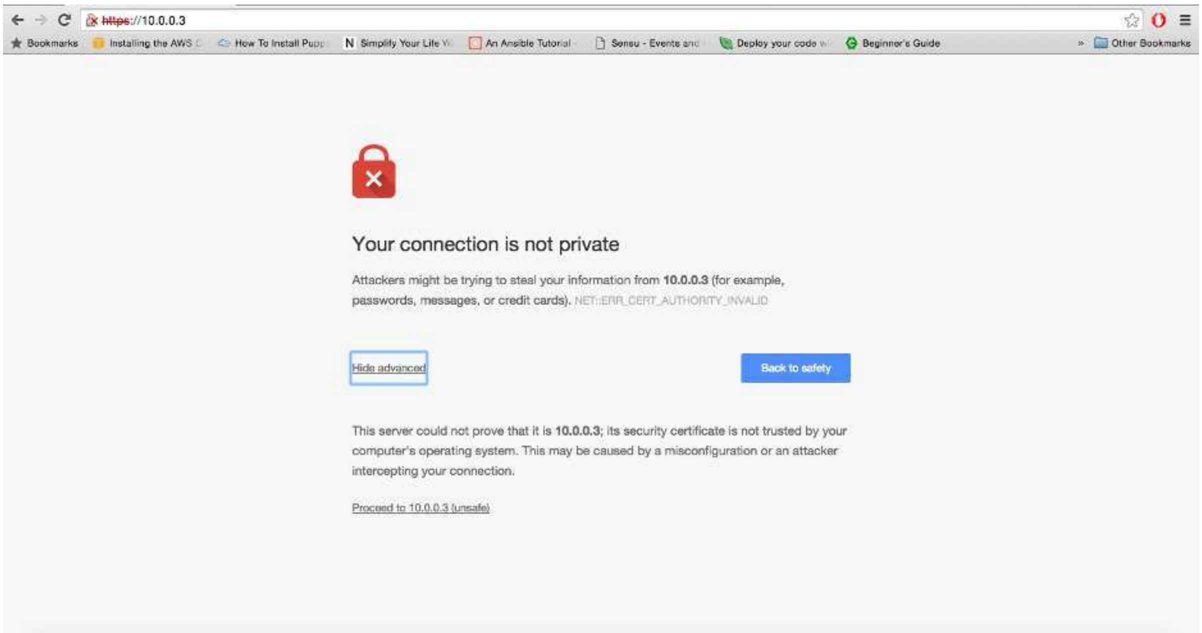
```
sudo yum install mod_ssl
```

3. add below contenet in /etc/httpd/conf.d/schoolofdevops.conf file

```
<VirtualHost *:443>
  ServerAdmin root
  ServerName schoolofdevops.org
  ServerAlias www.schoolofdevops.org
  DocumentRoot /var/www/schoolofdevops/
  SSLEngine on
  SSLCertificateFile /etc/httpd/ssl/server.crt
  SSLCertificateKeyFile /etc/httpd/ssl/server.key
</VirtualHost>
```

4. visit our https page (https://serverip)

Click on Proceed to IP button to check your page



Your connection is not private

Attackers might be trying to steal your information from **10.0.0.3** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **10.0.0.3**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 10.0.0.3 (unsafe)

Create and attach ssl certificate

- ## Make directory for the certificate

```
sudo mkdir /etc/httpd/ssl
cd /etc/httpd/ssl
```

- ## Create a server key and Certificate Signing Request

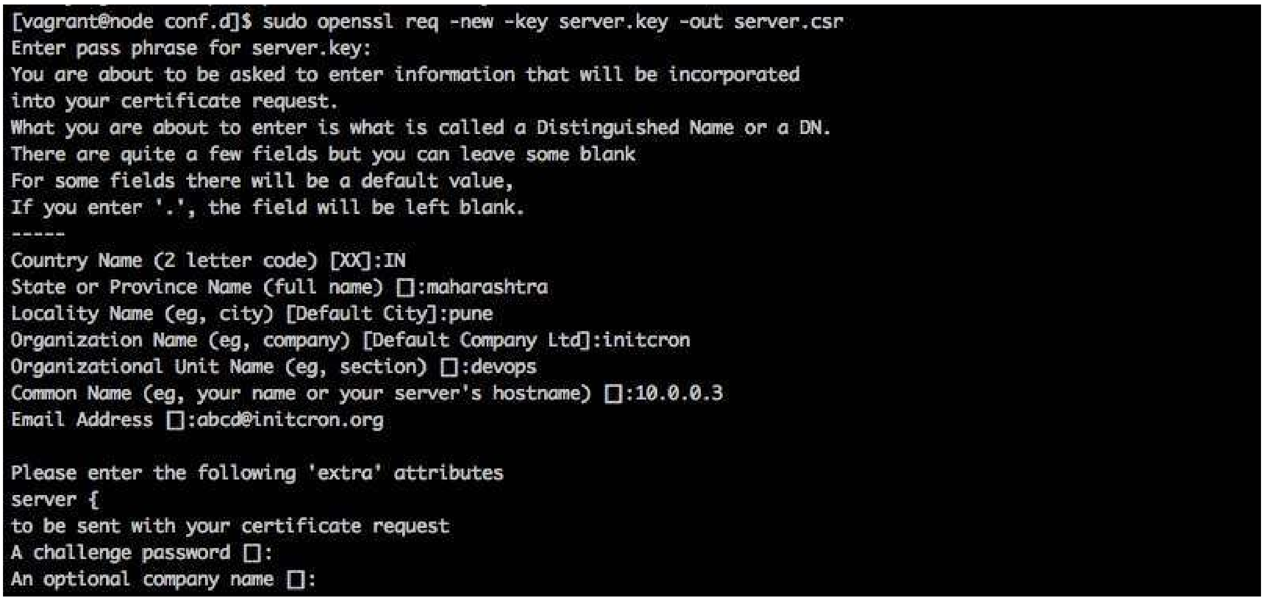
  - ### Creating the private server key

`sudo openssl genrsa -des3 -out server.key 1024`

Note:- you will be asked to enter a specific passphrase. Be sure to note this phrase carefully

  - ### creating a certificate signing request:

`sudo openssl req -new -key server.key -out server.csr`



```
[vagrant@node conf.d]$ sudo openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:IN
State or Province Name (full name) []:maharashtra
Locality Name (eg, city) [Default City]:pune
Organization Name (eg, company) [Default Company Ltd]:initcron
Organizational Unit Name (eg, section) []:devops
Common Name (eg, your name or your server's hostname) []:10.0.0.3
Email Address []:abcd@initcron.org

Please enter the following 'extra' attributes
server {
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

"Common Name" :- Enter your official domain name here or, if you don't have one yet, your site's IP address.

- ## Remove the passphrase

  ```
  sudo cp server.key server.tmp
  sudo openssl rsa -in server.tmp -out server.key
  ```

  Note:- In the event that nginx crashes or needs to reboot, you will always have to re-enter your passphrase to get your entire web server back online. So to avoid it remove the passphrase

- ## Sign you ssl certificate

  ```
  sudo openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
  ```

Install php

- **install php5 with mysql bindings**

  `sudo yum install php php-mysql` `sudo service httpd restart`

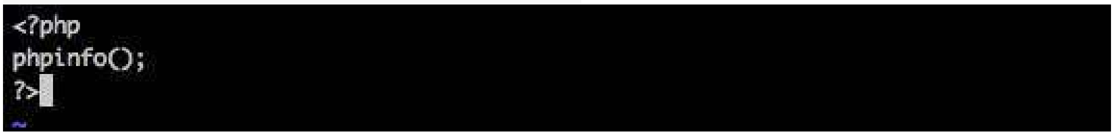
- **create info.php file and display it on browser**

  - **follow this lab to install apache if it is not installed**

    Install and configure apache

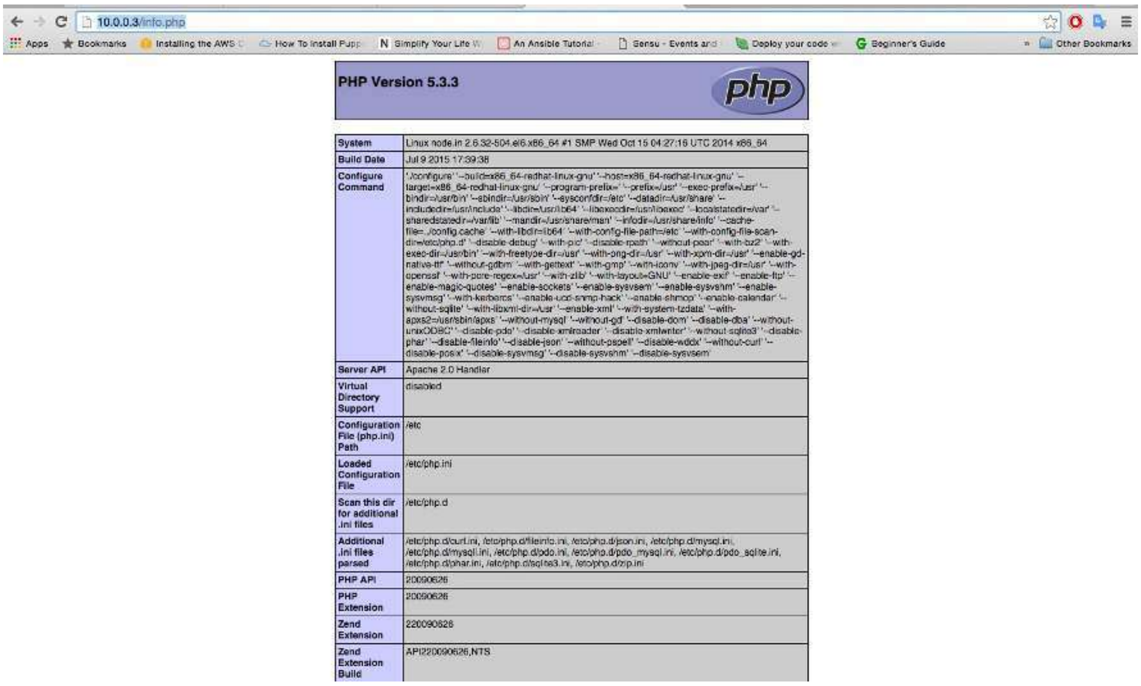
  - **Create the info.php file and add below content.**

    `sudo vi /var/www/schoolofdevops/info.php`



```
<?php
phpinfo();
?>
```

  - **check your info.php page by http://youripaddress/info.php**



PHP Version 5.3.3

System	Linux node.in 2.6.32-504.el6.x86_64 #1 SMP Wed Oct 15 04:27:16 UTC 2014 x86_64
Build Date	Jul 9 2015 17:39:38
Configure Command	'./configure' '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=../config.cache' '--with-libdir=lib64' '--with-config-file-path=/etc' '--with-config-file-scan-dir=/etc/php.d' '--disable-debug' '--with-pic' '--disable-rpath' '--without-pear' '--with-bz2' '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--enable-gd-native-ttf' '--without-gdbm' '--with-gettext' '--with-gmp' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl' '--with-pcre-regex=/usr' '--with-zlib' '--with-layout=GNU' '--enable-exif' '--enable-ftp' '--enable-magic-quotes' '--enable-sockets' '--enable-sysvsem' '--enable-sysvshm' '--enable-sysvmsg' '--with-kerberos' '--enable-ucd-snmp-hack' '--enable-shmop' '--enable-calendar' '--without-sqlite' '--with-libxml-dir=/usr' '--enable-xml' '--with-system-tzdata' '--with-apxs2=/usr/sbin/apxs' '--without-mysql' '--without-gd' '--disable-dom' '--disable-dba' '--without-unixODBC' '--disable-pdo' '--disable-xmlreader' '--disable-xmlwriter' '--without-sqlite3' '--disable-phar' '--disable-fileinfo' '--disable-json' '--without-pspell' '--disable-wddx' '--without-curl' '--disable-posix' '--disable-sysvmsg' '--disable-sysvshm' '--disable-sysvsem'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/curl.ini, /etc/php.d/fileinfo.ini, /etc/php.d/json.ini, /etc/php.d/mysql.ini, /etc/php.d/mysqli.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysql.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/sqlite3.ini, /etc/php.d/zip.ini
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension Build	API220090626,NTS

Install and setup Wordpress with Apache with MySQL Backend

1. Install and configure apache (skip this step if alreday installed)

follow this lab to install and configure apache

2. installed mysql-server

follow this lab to install and configure mysql

3. install php5

follow this link to install php5

4. Install and configure wordpress application

- ### Download wordpress application

  ```
  cd /var/www/html
  wget http://wordpress.org/latest.tar.gz
  tar -xzvf latest.tar.gz
  chown -r apache:apache wordpress
  rm -rf latest.tar.gz
  ```

  - ### Create database wordpress with full access to user wordpress

    goto Mysq Shell
    `mysql -u root -p`

    create database for wordpress
    `CREATE DATABASE wordpress;`

    create user for wordpress
    `CREATE USER wordpress@localhost;`

set password for wordpress user

`SET PASSWORD FOR wordpress@localhost= PASSWORD("password");`

Grant PRIVILEGES to wordpress user for wordpress database.

`GRANT ALL PRIVILEGES ON wordpress.* TO wordpress@localhost IDENTIFIED BY 'password';`

`FLUSH PRIVILEGES;`

`exit`

- ## Configure wordpress application

  Note:- Overwrite the index.php file or reomve any old index.php file which we have create before copying

  `sudo cp -r ./wordpress/* /var/www/schoolofdevops`

  Wordpress application require one php-module which is not present in your server

  php-gd

  `sudo yum install php-gd`

  `yum info php-gd`

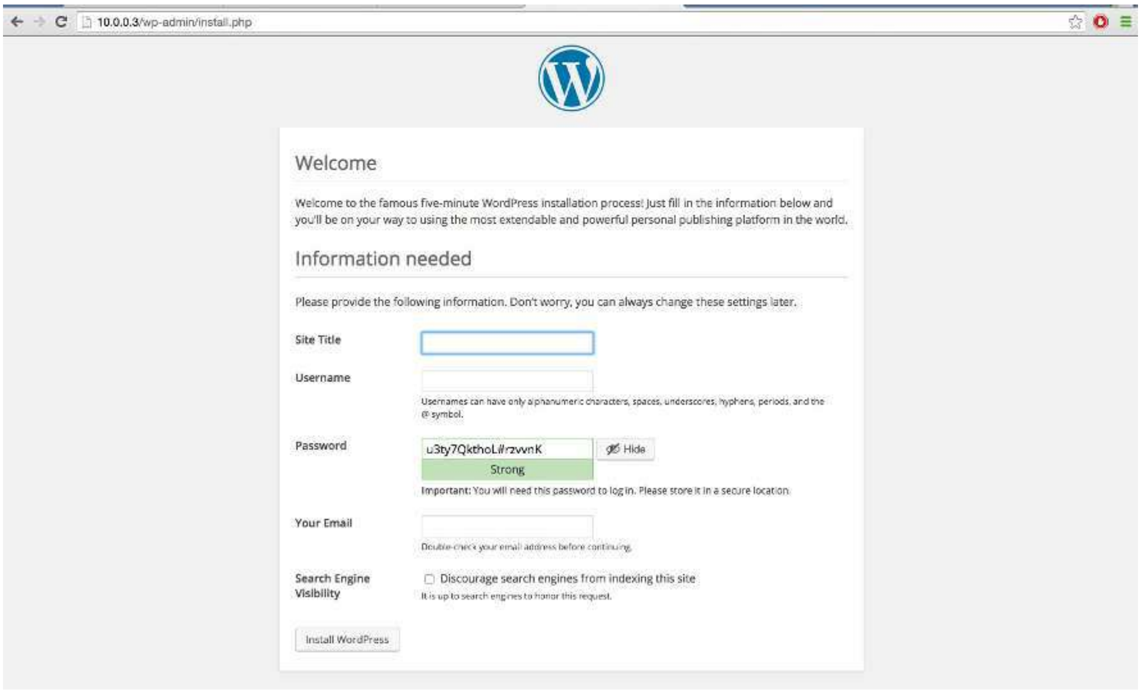
  Edit the wp-config.php file and put appropriate values of variable

  `vi /var/www/schoolofdevops/wp-config.php`

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'database_name_here');

/** MySQL database username */
define('DB_USER', 'username_here');

/** MySQL database password */
define('DB_PASSWORD', 'password_here');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

`sudo service httpd restart`

- ## check your wordpress application by visiting (http://youripaddress)



10.0.0.3/wp-admin/install.php

Welcome

Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.

Information needed

Please provide the following information. Don't worry, you can always change these settings later.

Site Title

Username

Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.

Password: u3ty7QkthoL#rzvvnK

Strong

Important: You will need this password to log in. Please store it in a secure location.

Your Email

Double-check your email address before continuing.

Search Engine Visibility: □ Discourage search engines from indexing this site

It is up to search engines to honor this request.

CDatabase Backups and Restore

Backing up Wordpress using mysqldump

```
cd /opt
mysqldump -u [username] –p[password] [database_name] > [wordpress_backup.sql]
```

Test the Backup

On the DB Server

Login to MySQL and verify existing data

`mysql -u root -p` USE wordpress; SHOW TABLES; ```

From MySQL Prompt, Delete Wordpress Database

```
USE mysql
DROP DATABASE WORDPRESS;
```

[Output: Query OK, 12 rows affected (0.28 sec)]

Validate the wordpress database is deleted

mysql> SHOW DATABASES; +--------------------+ | Database | +--------------------+ | information_schema | | mysql | | performance_schema | | sys | +--------------------+ 4 rows in set (0.00 sec)

Restore

`mysql -u root -p < /opt/wordpress_backup.sql`

Validate Data Restore

`mysql -u root -p` USE wordpress; SHOW TABLES; ```

Scheduling Daily/Nightly Backups

- ### Create a file wordpress_backup.sh and edit it

  `vi /root/wordpress_backup.sh`

- ### Write backup script for wordpress dump

  ```
  #!/bin/bash
  current_date=`date +%Y-%m-%d`
  sudo mkdir -p ~/wordpress_backup
  cd ~/wordpress_backup
  sudo mysqldump -u root -ppassword wordpress > wrodpress_backup_${current_date}.sql
  ```

- ### Schedule above script at 12:00 am daily

  `crontab -e`

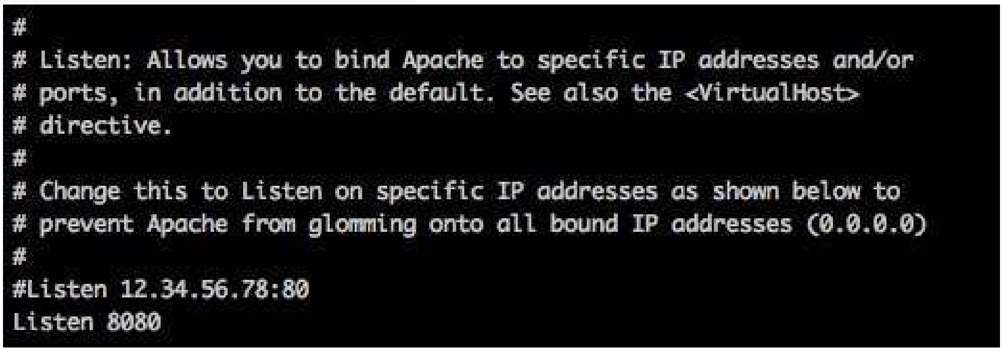
  add below entry in crontab as follow

  `0 0 * * * /bin/bash /root/wordpress_backup.sh`

Install and configure nginx as a reverse proxy

1. we have to run apache in the backend and nginx in the frontend so to run both in the one server we need to change the port of apache.

- Edit the httpd.conf file and find the below line and change the port number to 8080 `sudo vi /etc/httpd/conf/httpd.conf`



```
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, in addition to the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses (0.0.0.0)
#
#Listen 12.34.56.78:80
Listen 8080
```

- Restart Apache and validate `service httpd restart` `netstat -pan | grep 8080` [Output: tcp 0 0 :::8080 :::* LISTEN 10170/httpd]

2. Install nginx

`sudo yum install nginx`

3. Configure nginx for apache

- **Create a file wordpress.conf**

  `vi /etc/nginx/conf.d/wordpress.conf`

- **Add the below block of code**

```
server {
    listen 80;
       location / {
            proxy_pass http://127.0.0.1:8080/;    #add you IP of apche server
                 proxy_set_header Host $host;
                 proxy_set_header X-Real-IP $remote_addr;
                 proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
            proxy_set_header X-Forwarded-Proto $scheme;
        }
}
```

4. Do a configuration test

```
sudo service nginx configtest
```

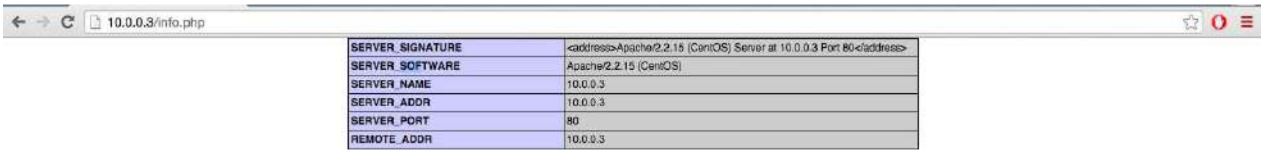
5. Disable Default Host Config for Nginx

mv /etc/nginx/conf.d/default.conf /etc/nginx/conf.d/default.conf.bak

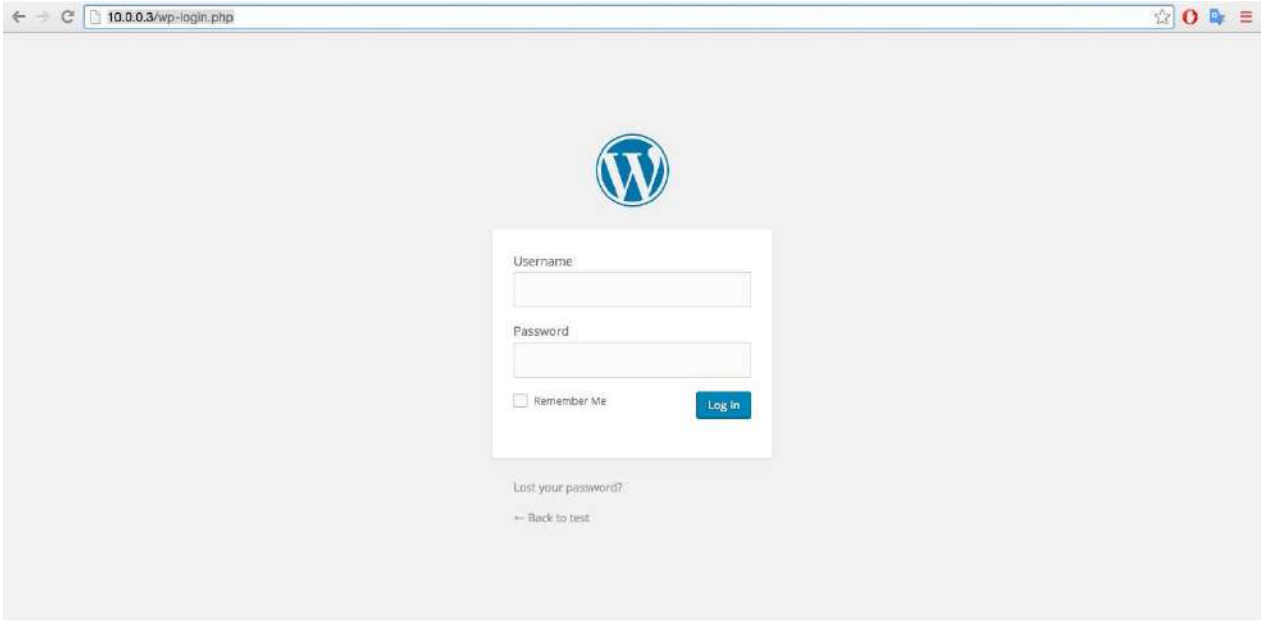
6. Reload the nginx config

```
sudo service nginx reload
```

7. visit the info.php page and check the variabe value



SERVER_SIGNATURE	<address>Apache/2.2.15 (CentOS) Server at 10.0.0.3 Port 80</address>
SERVER_SOFTWARE	Apache/2.2.15 (CentOS)
SERVER_NAME	10.0.0.3
SERVER_ADDR	10.0.0.3
SERVER_PORT	80
REMOTE_ADDR	10.0.0.3



10.0.0.3/wp-login.php
Username
Password
□ Remember Me
Log In
Lost your password?
← Back to test

Create and attach ssl certificate to nginx

1. create ssl certificate

Use this labe to create ssl certificate

2. edit the wordpress.conf file (/etc/nginx/conf.d/wordpress.conf)

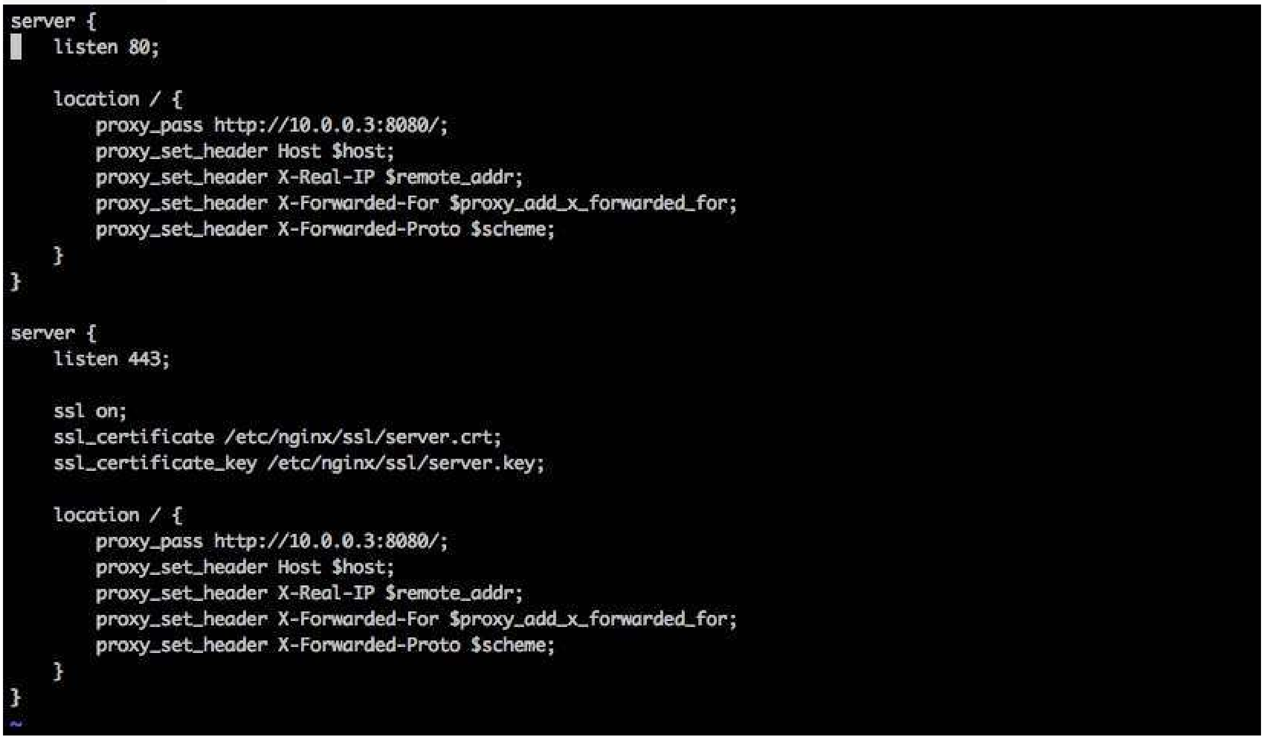
`vi /etc/nginx/conf.d/wordpress.conf`

3. Append the block of code below to existing configurations

```
    server {
            listen 443;

            ssl on;
            ssl_certificate /etc/httpd/ssl/server.crt;
            ssl_certificate_key /etc/httpd/ssl/server.key;

            location / {
                proxy_pass http://127.0.0.1:8080/;
                proxy_set_header Host $host;
                proxy_set_header X-Real-IP $remote_addr;
                proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                proxy_set_header X-Forwarded-Proto $scheme;
            }
        }
```

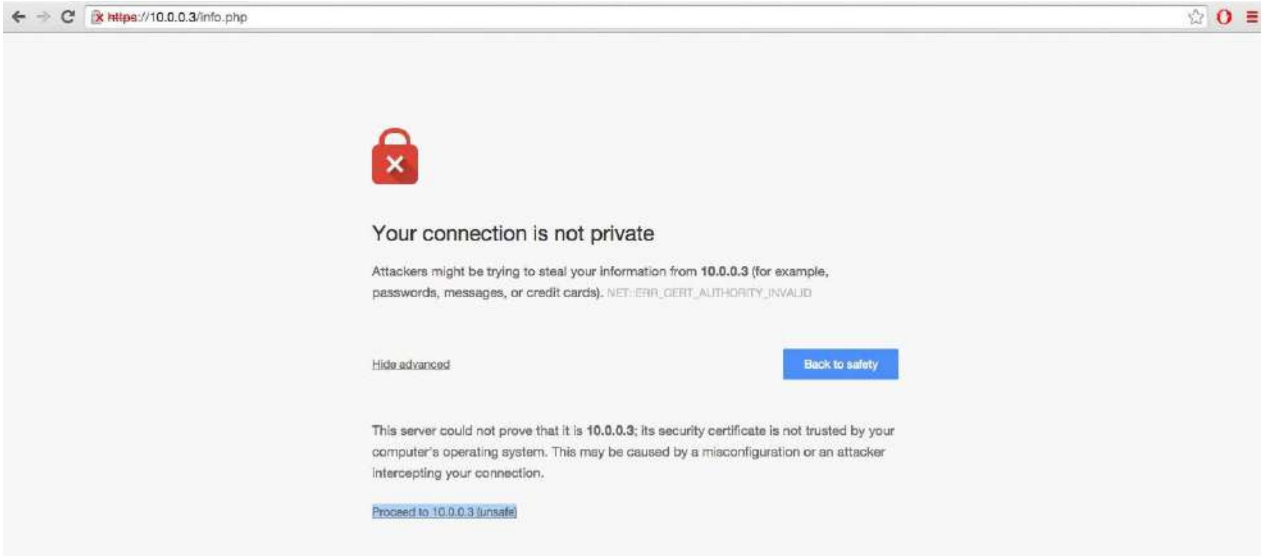
Note:- if you are using 443 port on apache then change the port to something else like

`listen 445`



```
server {
    listen 80;

    location / {
        proxy_pass http://10.0.0.3:8080/;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
}

server {
    listen 443;

    ssl on;
    ssl_certificate /etc/nginx/ssl/server.crt;
    ssl_certificate_key /etc/nginx/ssl/server.key;

    location / {
        proxy_pass http://10.0.0.3:8080/;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
}
~
```

4. Visit the info.php (https://your-ip-address/info.php)



Your connection is not private

Attackers might be trying to steal your information from **10.0.0.3** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **10.0.0.3**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Install and configure tomcat

1. install java

```
sudo yum install java-1.7.0-openjdk
```

2. install tomcat

```
sudo yum install tomcat
```

```
sudo yum install tomcat-webapps tomcat-admin-webapps
```

3. configure the tomcat

- ## open tomcat.conf file

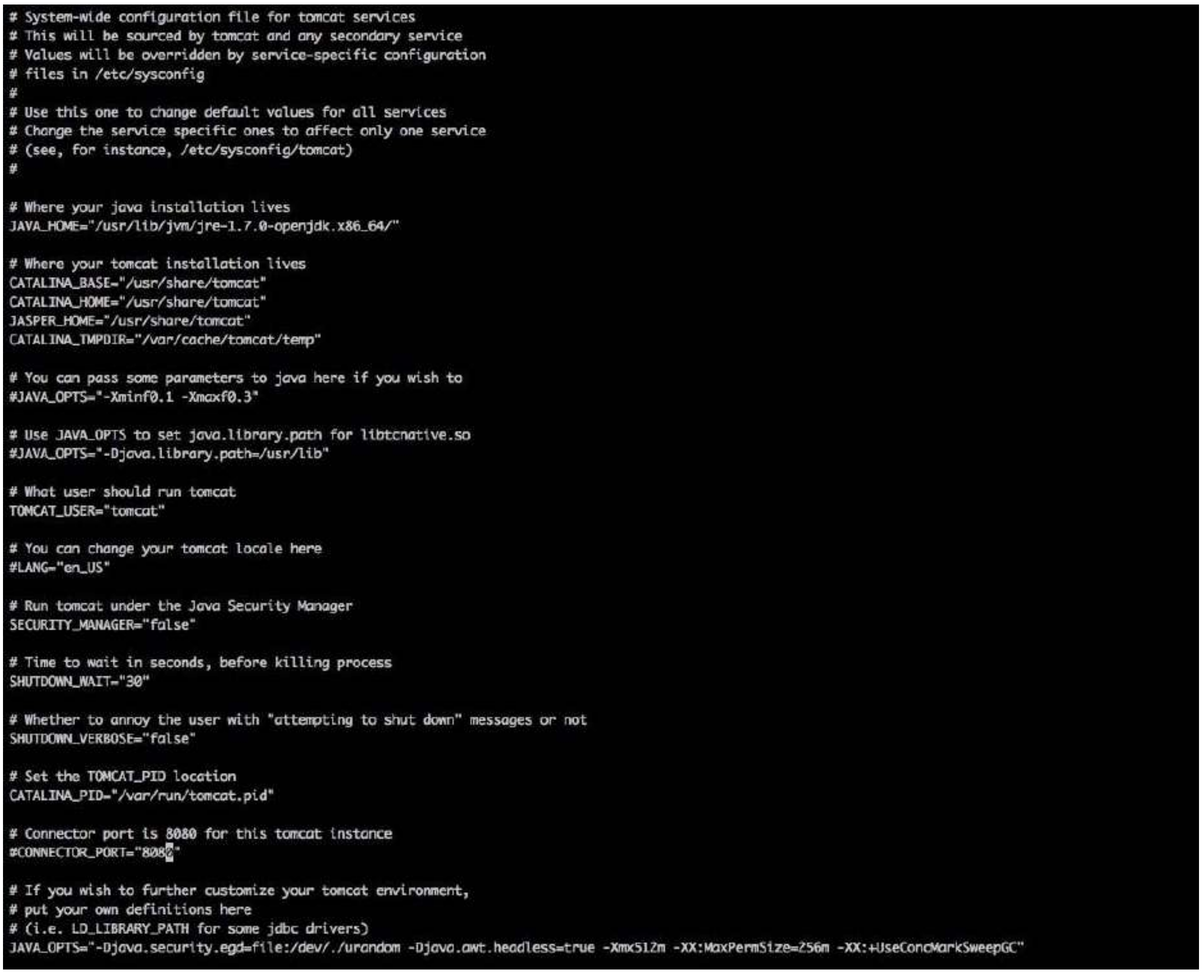
  ```
  sudo vi /etc/tomcat/tomcat.conf
  ```

- ## add the below JAVA_OPTS line

  ```
  JAVA_OPTS="-Djava.security.egd=file:/dev/./urandom -Djava.awt.headless=true -Xmx512m -XX:MaxPermSize=256m -XX:+UseConcMarkSweepGC"
  ```

- ## Put the appropriate value of JAVA_HOME

  ```
  JAVA_HOME="/usr/lib/jvm/jre-1.7.0-openjdk.x86_64/"
  ```



```
# System-wide configuration file for tomcat services
# This will be sourced by tomcat and any secondary service
# Values will be overridden by service-specific configuration
# files in /etc/sysconfig
#
# Use this one to change default values for all services
# Change the service specific ones to affect only one service
# (see, for instance, /etc/sysconfig/tomcat)
#

# Where your java installation lives
JAVA_HOME="/usr/lib/jvm/jre-1.7.0-openjdk.x86_64/"

# Where your tomcat installation lives
CATALINA_BASE="/usr/share/tomcat"
CATALINA_HOME="/usr/share/tomcat"
JASPER_HOME="/usr/share/tomcat"
CATALINA_TMPDIR="/var/cache/tomcat/temp"

# You can pass some parameters to java here if you wish to
#JAVA_OPTS="-Xminf0.1 -Xmaxf0.3"

# Use JAVA_OPTS to set java.library.path for libtcnative.so
#JAVA_OPTS="-Djava.library.path=/usr/lib"

# What user should run tomcat
TOMCAT_USER="tomcat"

# You can change your tomcat locale here
#LANG="en_US"

# Run tomcat under the Java Security Manager
SECURITY_MANAGER="false"

# Time to wait in seconds, before killing process
SHUTDOWN_WAIT="30"

# Whether to annoy the user with "attempting to shut down" messages or not
SHUTDOWN_VERBOSE="false"

# Set the TOMCAT_PID location
CATALINA_PID="/var/run/tomcat.pid"

# Connector port is 8080 for this tomcat instance
#CONNECTOR_PORT="8080"

# If you wish to further customize your tomcat environment,
# put your own definitions here
# (i.e. LD_LIBRARY_PATH for some jdbc drivers)
JAVA_OPTS="-Djava.security.egd=file:/dev/./urandom -Djava.awt.headless=true -Xmx512m -XX:MaxPermSize=256m -XX:+UseConcMarkSweepGC"
```

4. Change the tomcat's default port from 8080 to 9090 (skip these step if you are not running anything on port 8080)

Note:- default port on which tomcat run is 8080 but we are alresay running apache on that port.

- ## Open file server.xml

  ```
  sudo vi /etc/tomcat/server.xml
  ```

- ## find the below line

  ```
  <Connector port="8080" protocol="HTTP/1.1"
  ```

- ## Change the port from 8080 to 9090

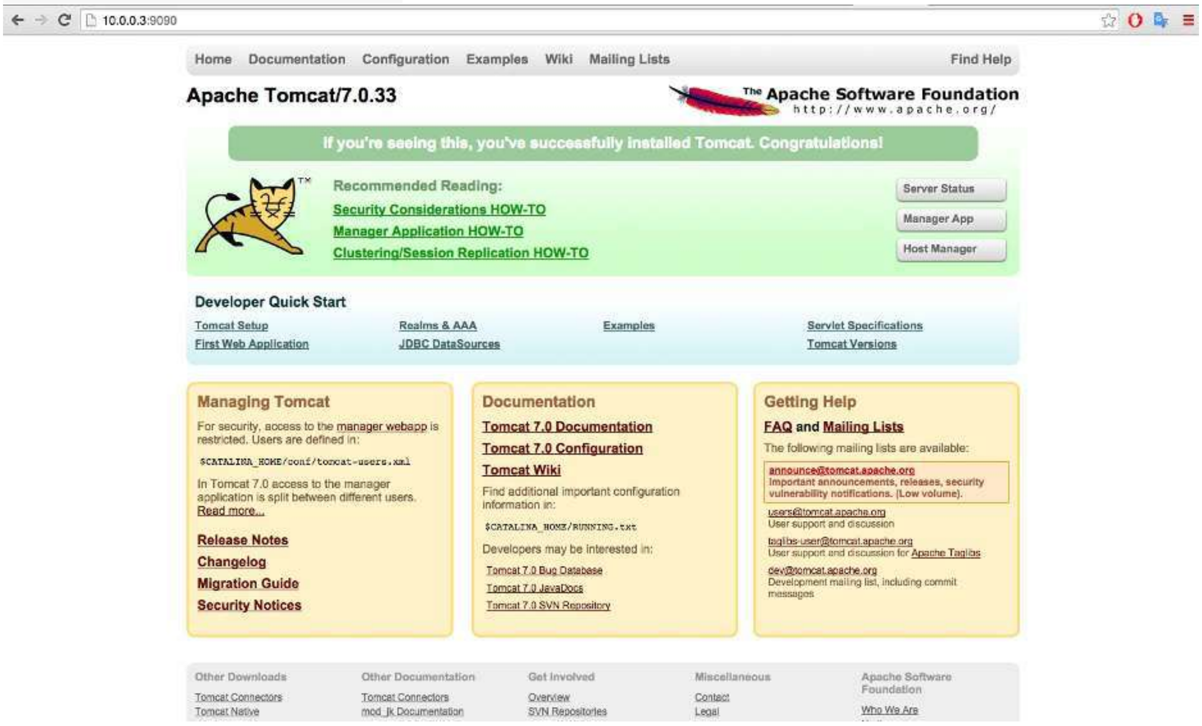
  ```
  <Connector port="9090" protocol="HTTP/1.1"
  ```

- **restart the tomcat service**

```
sudo service tomcat restart
```

5. open the tomcat management console

```
http://serveripaddress:9090
```



10.0.0.3:9090

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/7.0.33

The Apache Software Foundation
http://www.apache.org/

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:
Security Considerations HOW-TO
Manager Application HOW-TO
Clustering/Session Replication HOW-TO

Server Status
Manager App
Host Manager

Developer Quick Start
Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

Managing Tomcat
For security, access to the manager webapp is restricted. Users are defined in:
$CATALINA_HOME/conf/tomcat-users.xml
In Tomcat 7.0 access to the manager application is split between different users. Read more...
Release Notes
Changelog
Migration Guide
Security Notices

Documentation
Tomcat 7.0 Documentation
Tomcat 7.0 Configuration
Tomcat Wiki
Find additional important configuration information in:
$CATALINA_HOME/RUNNING.txt
Developers may be interested in:
Tomcat 7.0 Bug Database
Tomcat 7.0 JavaDocs
Tomcat 7.0 SVN Repository

Getting Help
FAQ and Mailing Lists
The following mailing lists are available:
announce@tomcat.apache.org
Important announcements, releases, security vulnerability notifications. (Low volume).
users@tomcat.apache.org
User support and discussion
taglibs-user@tomcat.apache.org
User support and discussion for Apache Taglibs
dev@tomcat.apache.org
Development mailing list, including commit messages

Other Downloads
Tomcat Connectors
Tomcat Native

Other Documentation
Tomcat Connectors
mod_jk Documentation

Get Involved
Overview
SVN Repositories

Miscellaneous
Contact
Legal

Apache Software Foundation
Who We Are

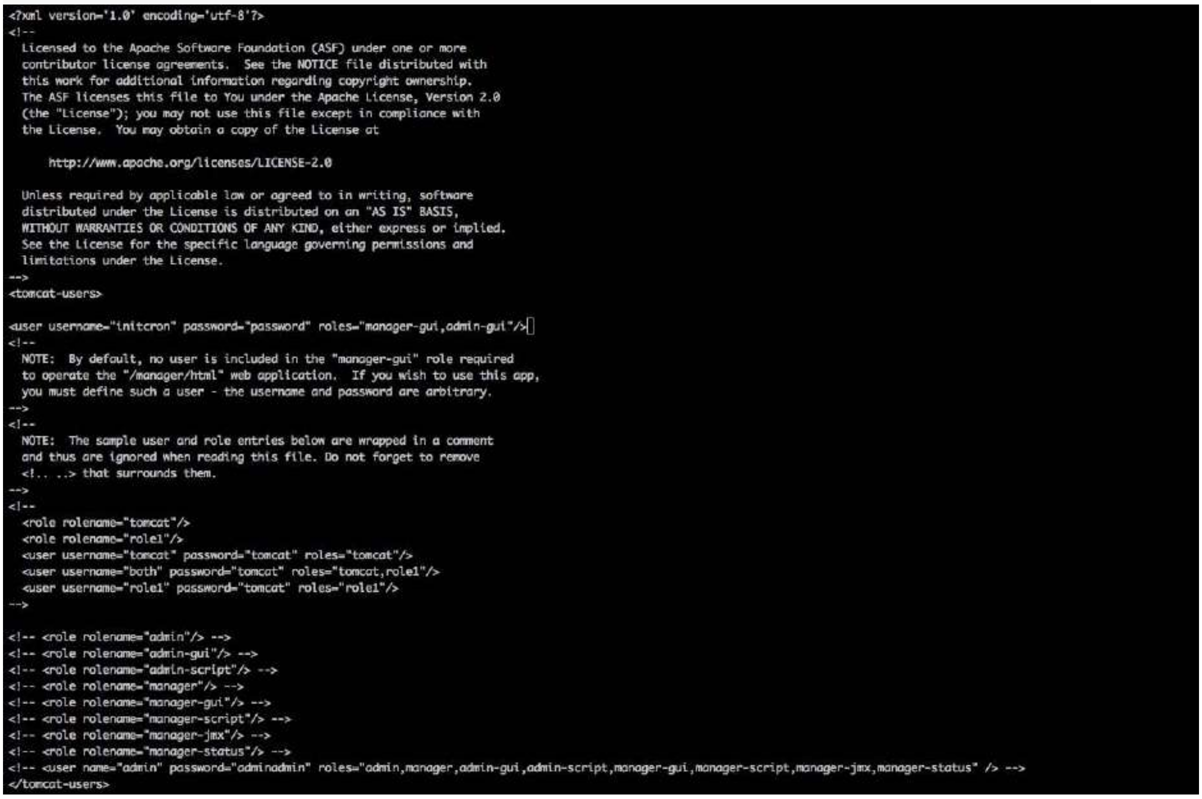
6. Configure Tomcate Web Mangment Interface

- **open tomcat-users.xml file**

```
sudo vi /opt/tomcat/conf/tomcat-users.xml
```

- **add the below line between `<tomcat-users>...</tomcat-users>` (change the username and password accordingly)**

```
<user username="initcron" password="password" roles="manager-gui,admin-gui"/>
```



```
<?xml version='1.0' encoding='utf-8'?>
<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<tomcat-users>

<user username="initcron" password="password" roles="manager-gui,admin-gui"/>
<!--
  NOTE:  By default, no user is included in the "manager-gui" role required
  to operate the "/manager/html" web application.  If you wish to use this app,
  you must define such a user - the username and password are arbitrary.
-->
<!--
  NOTE:  The sample user and role entries below are wrapped in a comment
  and thus are ignored when reading this file. Do not forget to remove
  <!.. ..> that surrounds them.
-->
<!--
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <user username="tomcat" password="tomcat" roles="tomcat"/>
  <user username="both" password="tomcat" roles="tomcat,role1"/>
  <user username="role1" password="tomcat" roles="role1"/>
-->

<!-- <role rolename="admin"/> -->
<!-- <role rolename="admin-gui"/> -->
<!-- <role rolename="admin-script"/> -->
<!-- <role rolename="manager"/> -->
<!-- <role rolename="manager-gui"/> -->
<!-- <role rolename="manager-script"/> -->
<!-- <role rolename="manager-jmx"/> -->
<!-- <role rolename="manager-status"/> -->
<!-- <user name="admin" password="adminadmin" roles="admin,manager,admin-gui,admin-script,manager-gui,manager-script,manager-jmx,manager-status" /> -->
</tomcat-users>
```

- # Restart the tomcat service

```
sudo service tomcat restart
```

Note:- now if you click on server setup or other option it you will have to pass the above credential

7. setup sample application

- ## Download sample application

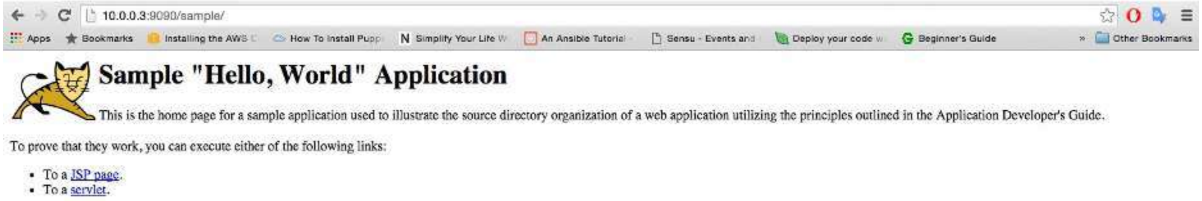
```
wget https://tomcat.apache.org/tomcat-6.0-doc/appdev/sample/sample.war
```

- ## move the sample application to CATALINA_HOME/webapps directory (/usr/share/tomcat/webapps)

Note:- you can see CATALINA_HOME variable value in /etc/tomcat/tomcat.conf file

```
mv sample.war /usr/share/tomcat/webapps
```

- **visit sample apllication by http://ip-address:9090/sample**



Sample "Hello, World" Application

This is the home page for a sample application used to illustrate the source directory organization of a web application utilizing the principles outlined in the Application Developer's Guide.

To prove that they work, you can execute either of the following links:

- To a JSP page.
- To a servlet.

Placeholder

placeholder

Lab

ping, ping6:-

send ICMP ECHO_REQUEST to network hosts. It is use to find connectivity between two nodes. Ping uses ICMP protocol. ping6 is IPv6 version of ping, and can also send Node Information Queries (RFC4620).

Usage:-

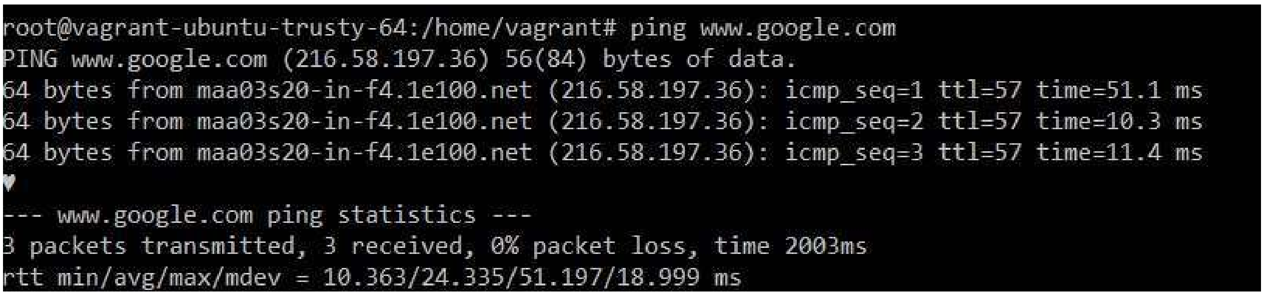
ping [-aAbBdDfhLnOqrRUvV] [-c count] [-F flowlabel] [-i interval] [-I interface] [-l preload] [-m mark] [-M pmtudisc_option] [-N node-info_option] [-w deadline] [-W timeout] [-p pattern] [-Q tos] [-s pack- etsize] [-S sndbuf] [-t ttl] [-T timestamp option] [hop ...] destination

---

Options:-

1. ping IP_addr/domain_name

By default ping without any option uses to check network connection between two nodes by sending & receiving packet to & from nodes.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# ping www.google.com
PING www.google.com (216.58.197.36) 56(84) bytes of data.
64 bytes from maa03s20-in-f4.1e100.net (216.58.197.36): icmp_seq=1 ttl=57 time=51.1 ms
64 bytes from maa03s20-in-f4.1e100.net (216.58.197.36): icmp_seq=2 ttl=57 time=10.3 ms
64 bytes from maa03s20-in-f4.1e100.net (216.58.197.36): icmp_seq=3 ttl=57 time=11.4 ms
♥
--- www.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 10.363/24.335/51.197/18.999 ms
```

---

2. ping –a IP_addr/domain_name

Ex. ping –a www.google.com

Audiable ping, it gives beep after every packet transmittion & reception.

---

3. ping domain_name

Ex. ping www.google.com

Use to find out ip address of specified domain name.

4. ping [–i interval] IP_addr/domain_name

Ex. ping –i 5 www.google.com

This is used to ping increase/decrese time interval, as mention in command. By default ping takes 1sec interval to send packets but with this utility we can increase/decrease its time interval.

5. ping [-c count] IP_addr/domain_name

Ex. ping –c 4 www.google.com

command cannot stop automatically we have to terminate it with CTRL+c. But with this utility we can specify no. of packet count ping can send , once it done it stop automatically.

6. ping –f IP_addr/domain_name

Ex. ping –f www.google.com

Flood ping. here it send "." For every ECHO_REQUEST & received backspace for every ECHO_REPLY. So increases output, ping can send thousands of packets in few seconds.

7. ping [-l preload] IP_addr/domain_name

Ex.ping –l 4 www.google.com

If preload option is specified then ping sends that many packets only not waiting for reply. Preload value more than 3 sudo privileges requires.

8. ping [-p pattern] IP_addr

Ex. ping –p aa 127.0.0.1

You may specify up to 16 ``pad'' bytes to fill out the packet you send. This is useful for diagnosing data-dependent problems in a network. For example, -p ff will cause the sent packet to be filled with all ones.

9. Ping [-m mark] IP_addr

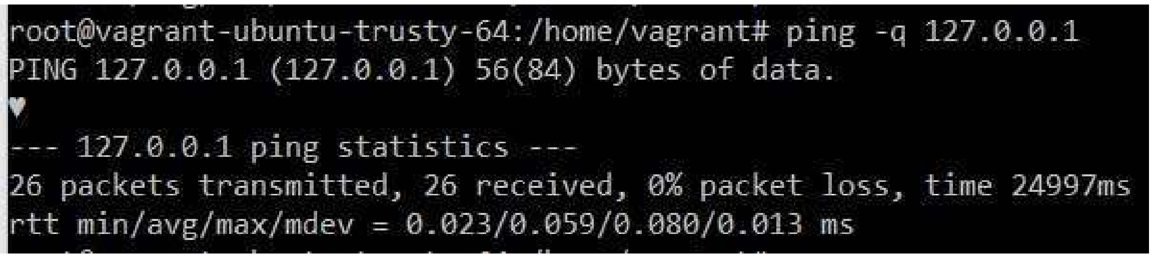
Ex. ping –m 10 127.0.0.1

This extends ping to send a packet out based on a given mark using -m option. Useful with policy routing to take different paths to same destination.

10. ping –q IP_addr

Ex. ping –q 127.0.0.1

Ping specified with q option nothing print on screen when we terminate command it prints only ping statistics summary.

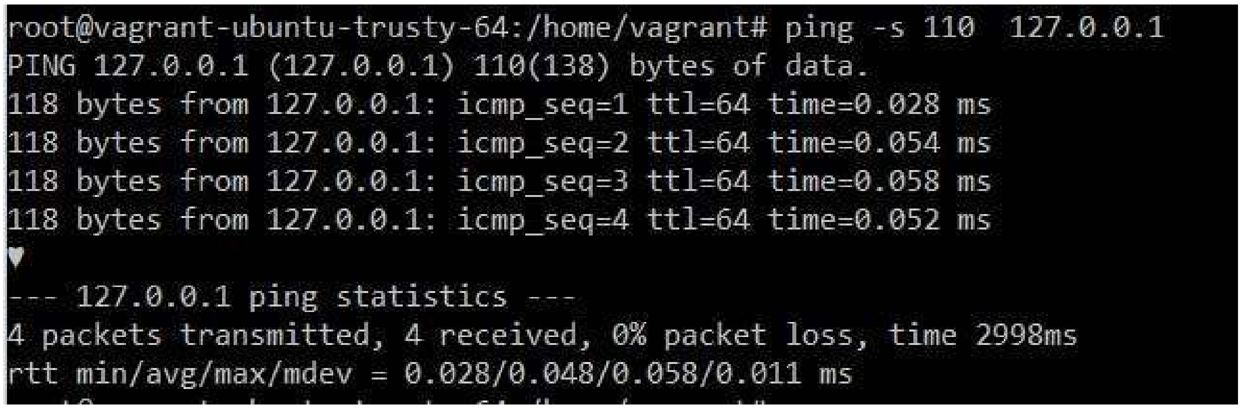


```
root@vagrant-ubuntu-trusty-64:/home/vagrant# ping -q 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
♥
--- 127.0.0.1 ping statistics ---
26 packets transmitted, 26 received, 0% packet loss, time 24997ms
rtt min/avg/max/mdev = 0.023/0.059/0.080/0.013 ms
```

11. ping [-s pack- etsize] IP_addr

Ex. ping –s 110 1270.0.01

Ping with s option , we can modify packet size of ping command. By default its range between 56 to 100. Ping has header size is ‘28’ so packet bytes send by ping in total is = ping packet size + ping header size.



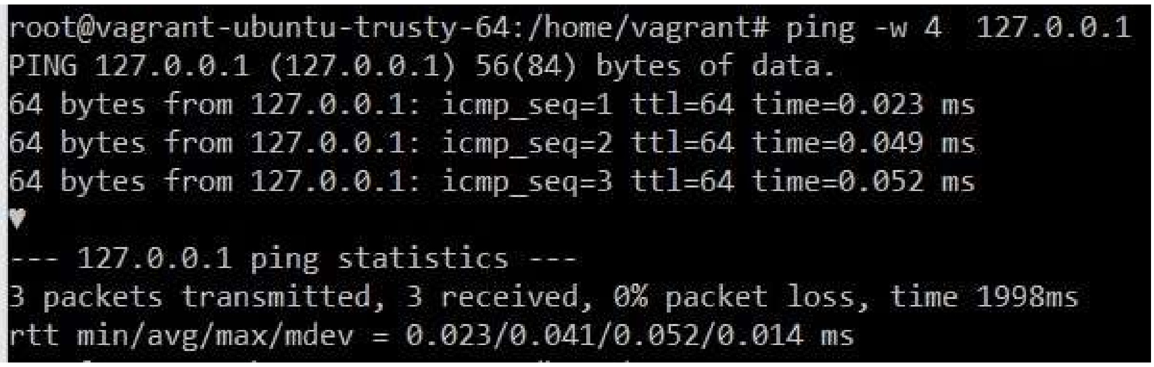
```
root@vagrant-ubuntu-trusty-64:/home/vagrant# ping -s 110  127.0.0.1
PING 127.0.0.1 (127.0.0.1) 110(138) bytes of data.
118 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.028 ms
118 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.054 ms
118 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.058 ms
118 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.052 ms
♥
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.028/0.048/0.058/0.011 ms
```

Here total byte send = 110 + 28 = 138

12. ping [-w deadline] IP_addr

Ex. ping –w 4 127.0.0.

Ping by default gives continuous output ,it cannot terminate itself , if we specify ‘w’ g with time then ping will stop automatically after specified time interval given in command.



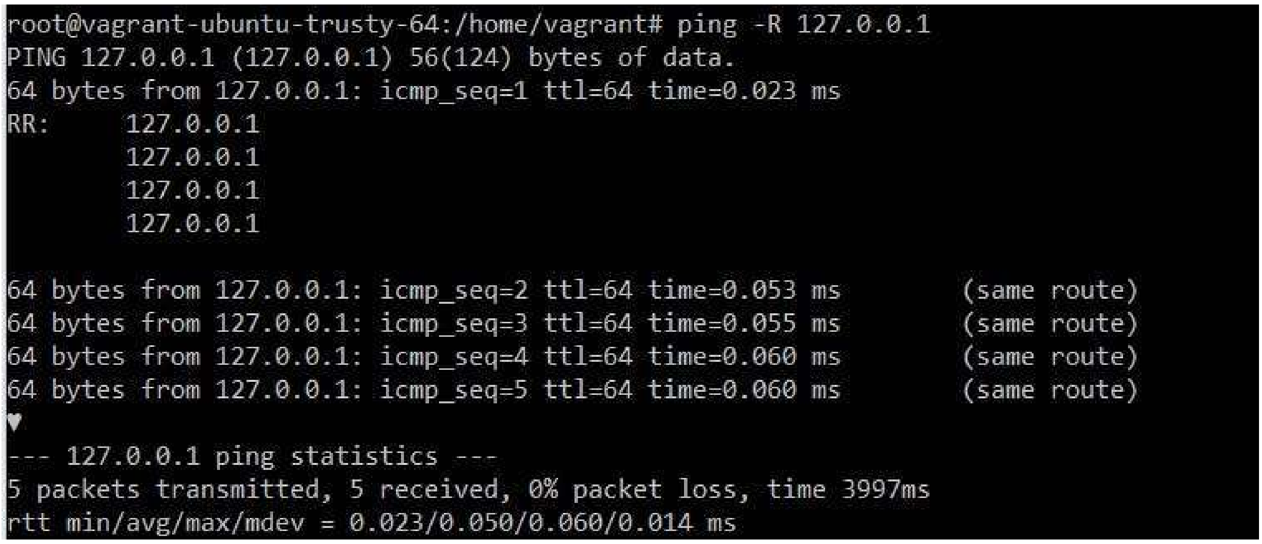
```
root@vagrant-ubuntu-trusty-64:/home/vagrant# ping -w 4  127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.049 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.052 ms
♥
--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.023/0.041/0.052/0.014 ms
```

Time =3998ms(@4sec)

13. ping –R IP_addr

Ex. ping –R 127.0.0.1

Ping with option ‘R’ we can record & prints the network routes through which packets is sent & received.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# ping -R 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(124) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.023 ms
RR:     127.0.0.1
        127.0.0.1
        127.0.0.1
        127.0.0.1

64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.053 ms        (same route)
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.055 ms        (same route)
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.060 ms        (same route)
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.060 ms        (same route)
♥
--- 127.0.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.023/0.050/0.060/0.014 ms
```

14. ping [-M pmtudisc_option] IP_addr

Ex .ping –M do 127.0.0.1

Select Path MTU Discovery strategy. Their are three parameter provided with MTU discovery do/don’t/want. These are use along with packet size ,if packet size is greater than maximum data payload depend on MTU parameter specified it takes decision to fragment packet or not.

15. ping IP IP_addr IP_addr

Ex. ping 192.168.2.3 192.168.33.1 192.168.64.1

We can specify path to reach ping packet to destination address. But here its important if any one path is not reachable then the ping fails to send packet to destination address.

16. Ping –D IP_addr

Ex . ping –D 127.0.0.1

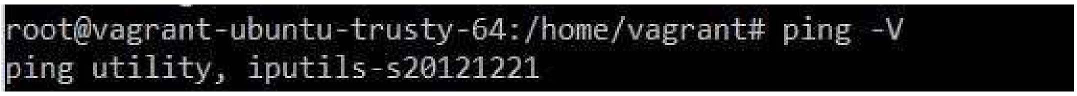
It prints time stamp before each line in format (unix time + microseconds as in gettimeofday)

17. ping localhost/127.0.0.1/0

These are the way we can ping to localhost.

18. ping –V

This show the the current version of ping on your machine.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# ping -V
ping utility, iputils-s20121221
```

Lab

Tenlet:-

User interface to the TELNET protocol. telnet command belongs to DAPRA command set, allow you to log on to remote machine. It is used for interactive communication with remote host. When telnet command with host IP address hit on command line it open telnet command prompt & require a password to login to another host machine. As long as we logged in with remote machine your machine is act like dumb terminal it just provide interface to logged in to remote machine.

With escape character there is facility we can switch between remote machine & local machine .**Default Escape character : " Ctrl +] "** Once you press this you can **work with your local machine** just at start of every command you have to press exclamatory mark **'!'** . we can end remote session with **exit** command after that we bacl to our local machine.

Telnet not secure - everything is sent in plain text be it over a local network or over the Internet. So any one can hack your information including your password. It is old - text based only, there are no graphics provided.

telnet is not in built functionality we have to install it from yum or apt repository.

Yum install telnet

Apt-get install telnet.

Usage:-

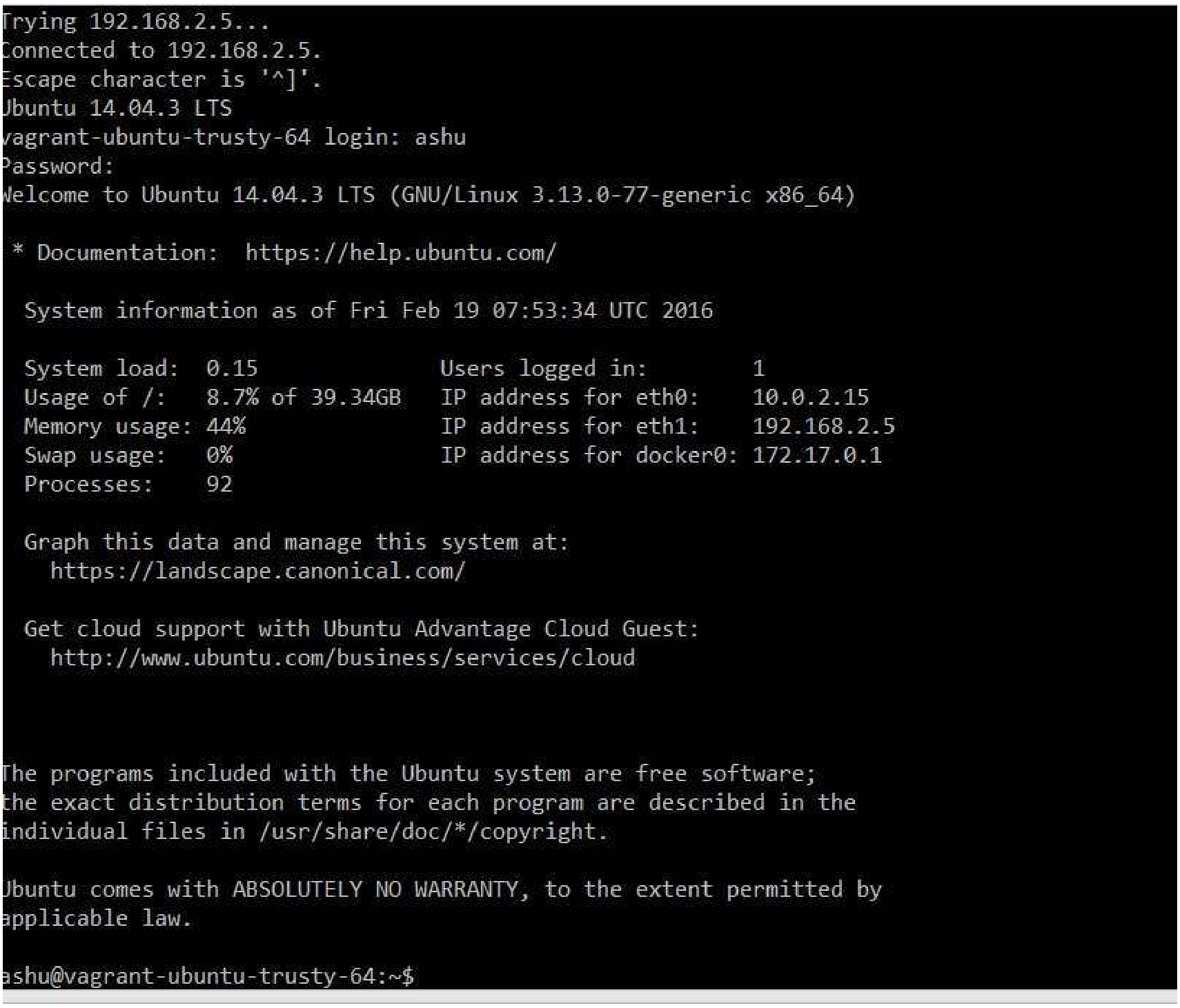
telnet [-468ELadr] [-S tos] [-b address] [-e escapechar] [-l user] [-n tracefile] [host [port]]

---

1. telnet IP_addr

ex. telnet 192.168.2.5

with this command your able to login to remote machine provided login infirmation & password. your local machine provide a terminal to work on remote machine using telnet command.



```
Trying 192.168.2.5...
Connected to 192.168.2.5.
Escape character is '^]'.
Ubuntu 14.04.3 LTS
vagrant-ubuntu-trusty-64 login: ashu
Password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.13.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Fri Feb 19 07:53:34 UTC 2016

  System load:  0.15               Users logged in:        1
  Usage of /:   8.7% of 39.34GB    IP address for eth0:    10.0.2.15
  Memory usage: 44%                IP address for eth1:    192.168.2.5
  Swap usage:   0%                 IP address for docker0: 172.17.0.1
  Processes:    92

  Graph this data and manage this system at:
    https://landscape.canonical.com/

  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ashu@vagrant-ubuntu-trusty-64:~$
```

2. telnet -4/6 IP_addr

Force IPv4/IPv6 address resolution.

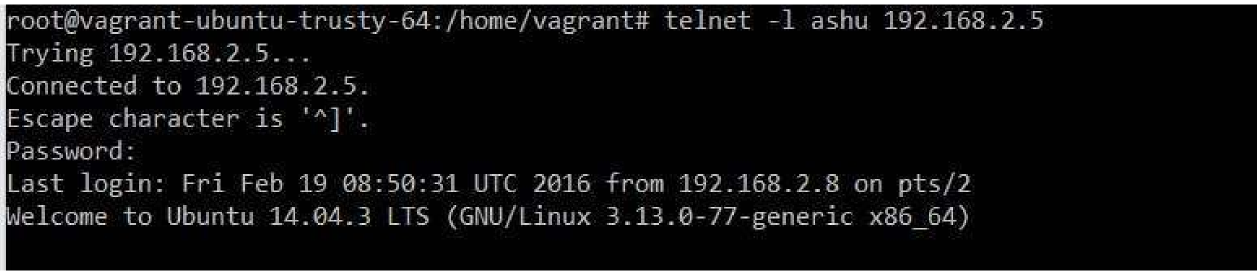
3. telnet -E IP_addr

it disables the escape character functionality.If ths functionality removes it is not possible to swich between remote machine & local machine.

4. telnet -l [user_name] IP_addr

ex. telnet -l ashu 192.168.2.5

with this "-l" option we can login to remote host with specific user name which must me present at remote machine. with this command it directly promt you for password as it already have user name with it.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# telnet -l ashu 192.168.2.5
Trying 192.168.2.5...
Connected to 192.168.2.5.
Escape character is '^]'.
Password:
Last login: Fri Feb 19 08:50:31 UTC 2016 from 192.168.2.8 on pts/2
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.13.0-77-generic x86_64)
```

5. telnet -e [escapechar] IP_addr

with this we can change the default escape character with new one as you specifies in command.

6. telnet -r IP-addr

Emulate rlogin(1). In this mode, the default escape character is a tilde. Also, the interpretation of the escape character is changed: an escape character followed by a dot causes telnet to disconnect from the remote host. A ^Z instead of a dot suspends telnet, and a ^] (the default telnet escape character) generates a normal telnet prompt. These codes are accepted only at the beginning of a line.

7. telnet IP_addr port [port_no]

By default telnet uses port 23. we can change port or service by this command as we want.

8. telnet -n tracefile IP_addr

It is used to record trace information in file we specified on command line. but to record trace information it is neccesary to set trace file first.

Lab

Nmap :-

Nmap (“Network Mapper”) is an open source tool for network exploration and security auditing. Namp determine what hosts are available on the network, what services offering by host, what type of operating system running, type of firewall in use. It is useful uitility for network & system administrators. The output from Nmap is a list of scanned targets, with information on each depending on the options used. **nmap command line tool to scan a host / network, security scanning, finding open port.** Nmap is available in package repository of most of linux distributions. We have to install it.

apt-get install nmap

yum install nmap

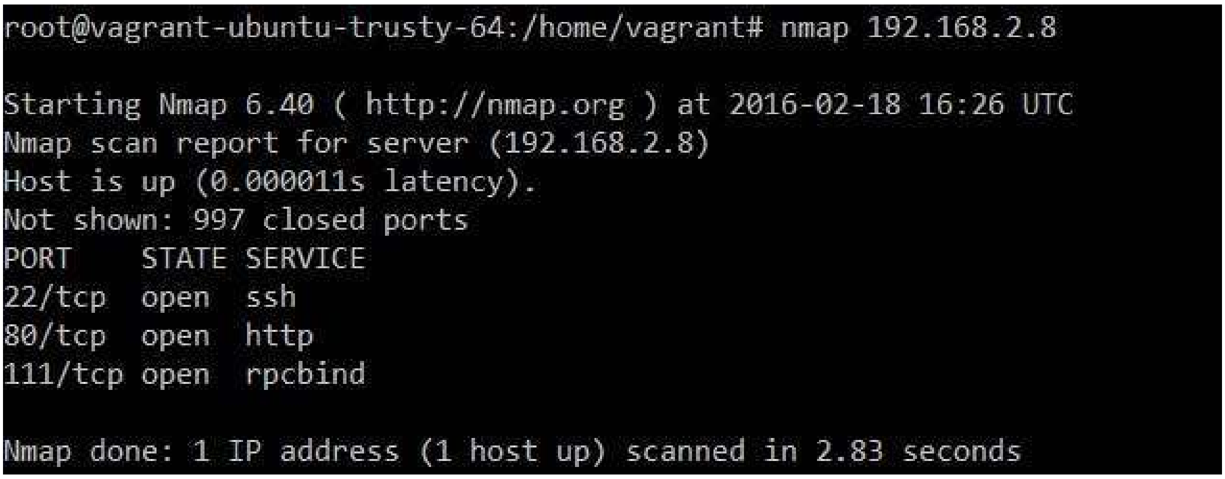
---

options:-

1. nmap IP_addr.

Ex. nmap 192.168.2.8

Namp with IP address scan IP address & gives you information of services, open port, mac address.



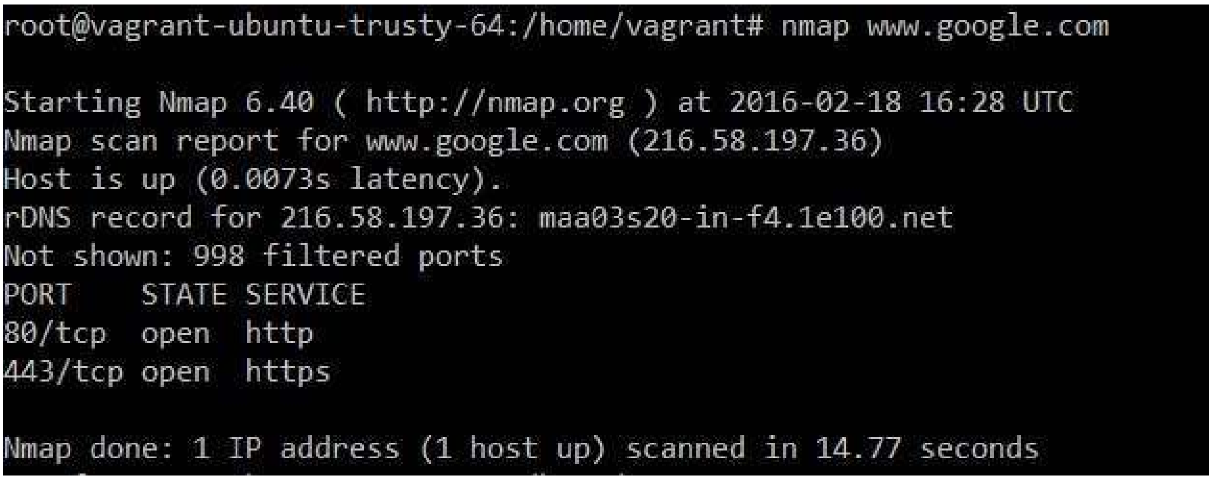
```
root@vagrant-ubuntu-trusty-64:/home/vagrant# nmap 192.168.2.8

Starting Nmap 6.40 ( http://nmap.org ) at 2016-02-18 16:26 UTC
Nmap scan report for server (192.168.2.8)
Host is up (0.000011s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 2.83 seconds
```

---

2. nmap domain_name

ex. nmap www.google.com

nmap scan server name & gives you IP address, list out services, open port information, mac address.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# nmap www.google.com

Starting Nmap 6.40 ( http://nmap.org ) at 2016-02-18 16:28 UTC
Nmap scan report for www.google.com (216.58.197.36)
Host is up (0.0073s latency).
rDNS record for 216.58.197.36: maa03s20-in-f4.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 14.77 seconds
```

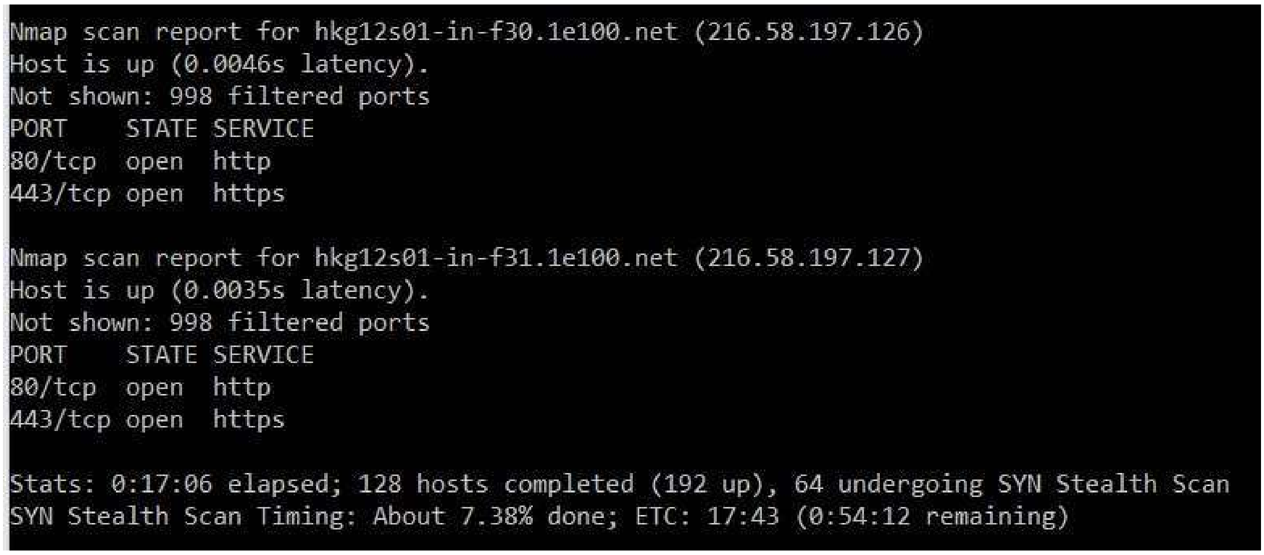
3. nmap -v IP_addr/domain_name

Gives details information of remote host.verbose dispaly.

4. nmap IP_addr with wildcard character ‘*’

Ex. nmap 192.168.2.* or nmap 192.168.2.0/24

With the wildcard character enter we can scan entire IP address range & subnet. gives all information of hosts which are up & down.

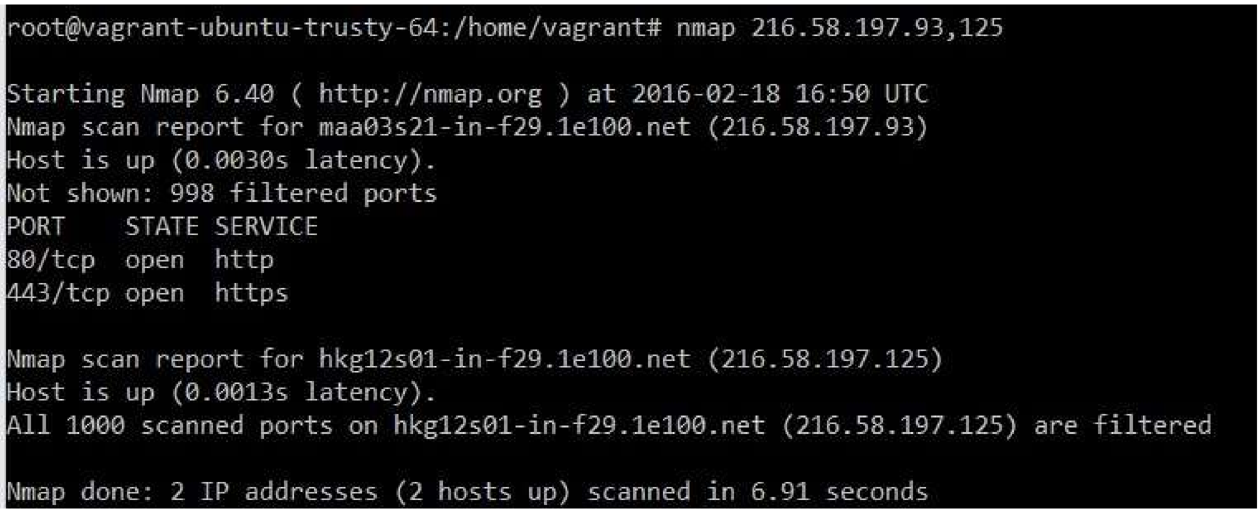


```
Nmap scan report for hkg12s01-in-f30.1e100.net (216.58.197.126)
Host is up (0.0046s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for hkg12s01-in-f31.1e100.net (216.58.197.127)
Host is up (0.0035s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Stats: 0:17:06 elapsed; 128 hosts completed (192 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 7.38% done; ETC: 17:43 (0:54:12 remaining)
```

5. nmap IP_addr with last octet

Ex. nmap 216.58.197.93,125

With nmap we can scan multiple IP address just by specifying last octect as shown in example.

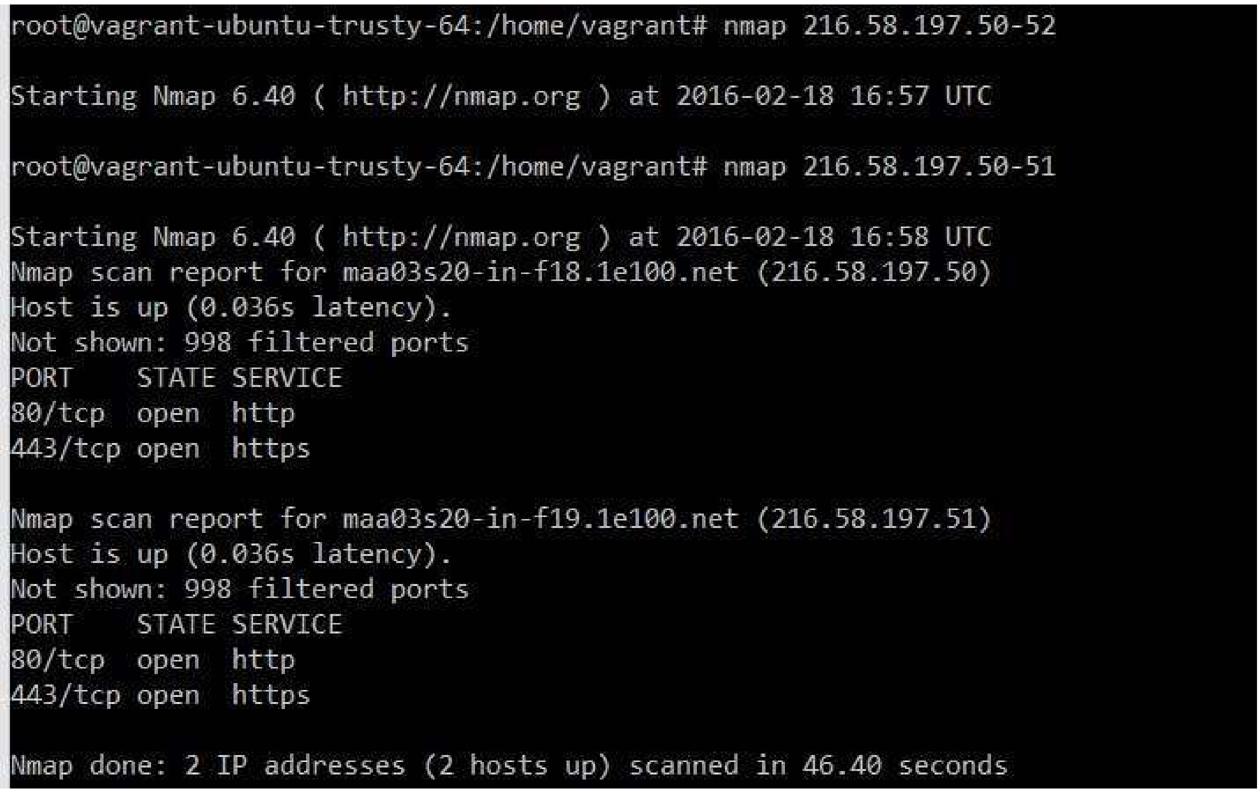


```
root@vagrant-ubuntu-trusty-64:/home/vagrant# nmap 216.58.197.93,125

Starting Nmap 6.40 ( http://nmap.org ) at 2016-02-18 16:50 UTC
Nmap scan report for maa03s21-in-f29.1e100.net (216.58.197.93)
Host is up (0.0030s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for hkg12s01-in-f29.1e100.net (216.58.197.125)
Host is up (0.0013s latency).
All 1000 scanned ports on hkg12s01-in-f29.1e100.net (216.58.197.125) are filtered

Nmap done: 2 IP addresses (2 hosts up) scanned in 6.91 seconds
```

6. nmap IP_addr range

Ex nmap 216.58.197.90-93

With nmap command we can scan IP address range as specified in above example.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# nmap 216.58.197.50-52

Starting Nmap 6.40 ( http://nmap.org ) at 2016-02-18 16:57 UTC

root@vagrant-ubuntu-trusty-64:/home/vagrant# nmap 216.58.197.50-51

Starting Nmap 6.40 ( http://nmap.org ) at 2016-02-18 16:58 UTC
Nmap scan report for maa03s20-in-f18.1e100.net (216.58.197.50)
Host is up (0.036s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for maa03s20-in-f19.1e100.net (216.58.197.51)
Host is up (0.036s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 2 IP addresses (2 hosts up) scanned in 46.40 seconds
```

7. nmap –A IP_addr

With option "A" menstion along with nmap it gives script scanning output, traceroute, OS version of provided host

---

8. nmap -O IP_addr

[O =-osscan guess]

With option 'O' it gives OS information & its version of remote host.

---

9. nmap IP_addr wildcard[*] --exclude IP_addr

Ex. nmap 192.168.2.* --exclude 192.168.2.8

With this command as shown in example we can exclude the IP address from scanning as we used wildcard character to scan all 256 host in last octect.

---

10. nmap example.txt**

Cat > example.txt

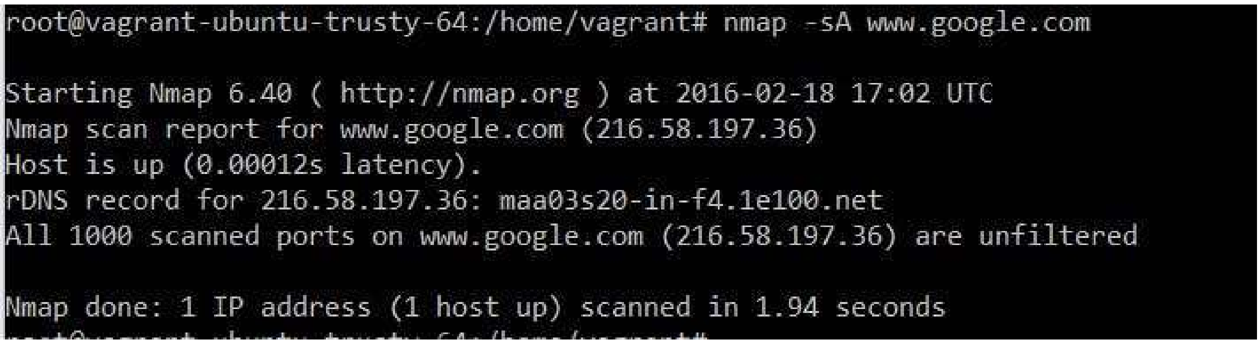
```
Localhost

192.168.2.2

192.168.22.1
```

With file menstion along with nmap command we can scan all the IP address server host names included in that .

---

11. nmap -sA IP_addr/ domain_name

With this 's' option along with nmap command we can determine is host is protected by firewall.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# nmap -sA www.google.com

Starting Nmap 6.40 ( http://nmap.org ) at 2016-02-18 17:02 UTC
Nmap scan report for www.google.com (216.58.197.36)
Host is up (0.00012s latency).
rDNS record for 216.58.197.36: maa03s20-in-f4.1e100.net
All 1000 scanned ports on www.google.com (216.58.197.36) are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 1.94 seconds
```

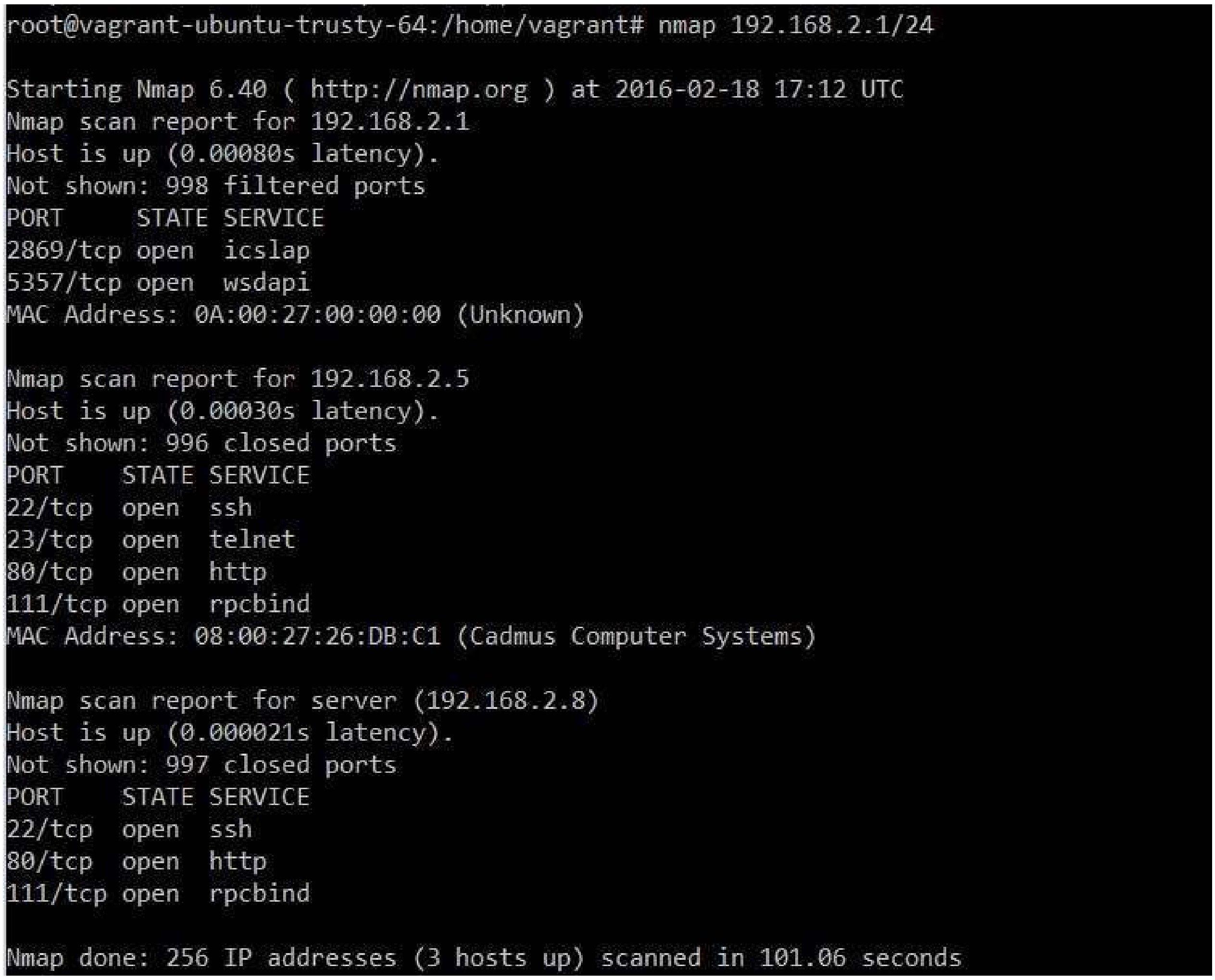
12. nmap –PN IP_addr/domain_name

Nmap along with this option we can scap host protected by firewall.

13. nmap -sP IP_addr/subnet mask

Ex. nmap -sP 192.168.2.2/24

With this we can scan which host are up, it find only running hosts. Its like ping utility.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# nmap 192.168.2.1/24

Starting Nmap 6.40 ( http://nmap.org ) at 2016-02-18 17:12 UTC
Nmap scan report for 192.168.2.1
Host is up (0.00080s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
2869/tcp open  icslap
5357/tcp open  wsdapi
MAC Address: 0A:00:27:00:00:00 (Unknown)

Nmap scan report for 192.168.2.5
Host is up (0.00030s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
80/tcp  open  http
111/tcp open  rpcbind
MAC Address: 08:00:27:26:DB:C1 (Cadmus Computer Systems)

Nmap scan report for server (192.168.2.8)
Host is up (0.000021s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind

Nmap done: 256 IP addresses (3 hosts up) scanned in 101.06 seconds
```

14. nmap -F IP_addr

To perform fast scan “-F” option is used.

15. nmap -r IP_addr

It is used to scan sequentially.

16. nmap –p IP_addr

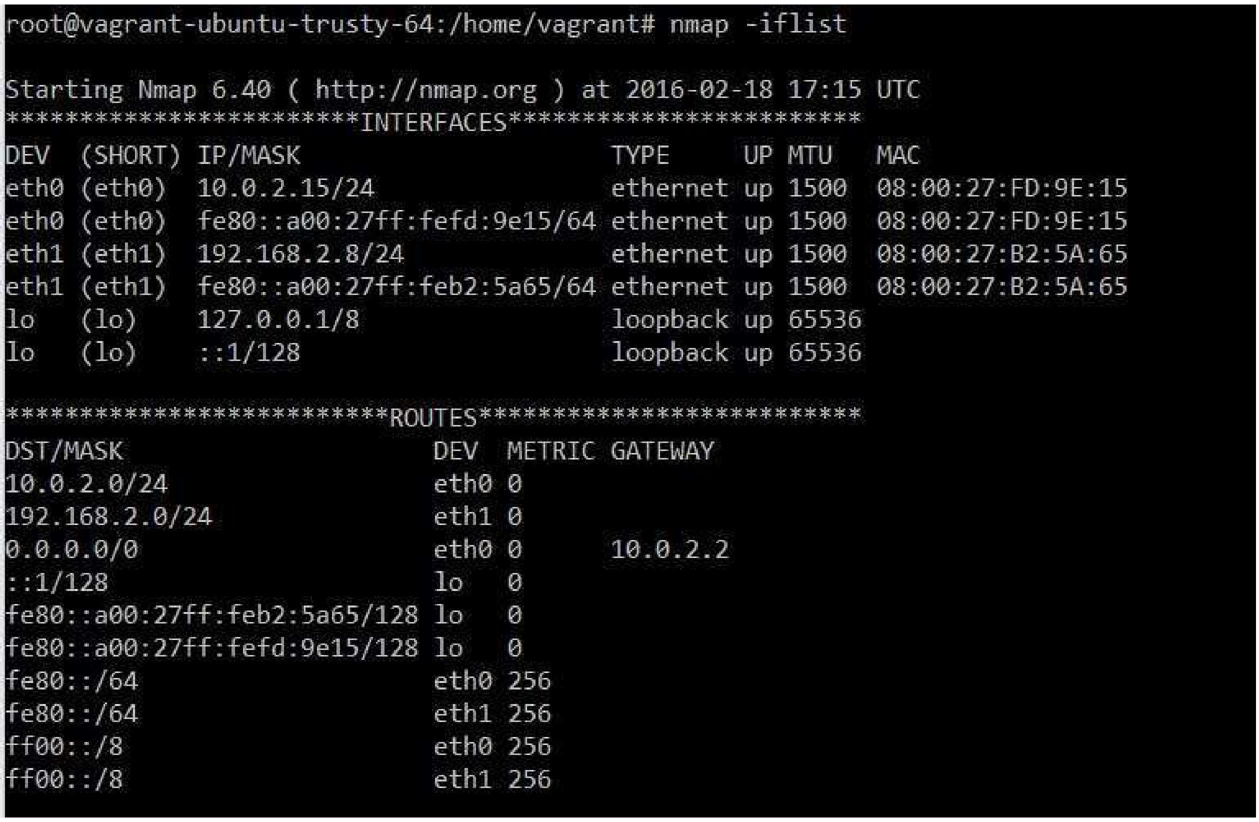
Ex. nmap –p 80 192.168.2.2

```
nmap  –p  T:80  192.168.2.2

nmap –p U:54   192.168.2.2

nmap –p  80,22  192.168.2.2

nmap –p 80-443   192.168.2.2
```

with “-p” option we scan fot a specific port . we cam menstioned port no directly inside command or we can also find along with port type AS TCP,UDP, multiple port also scan on single command line

17. nmap –iflist

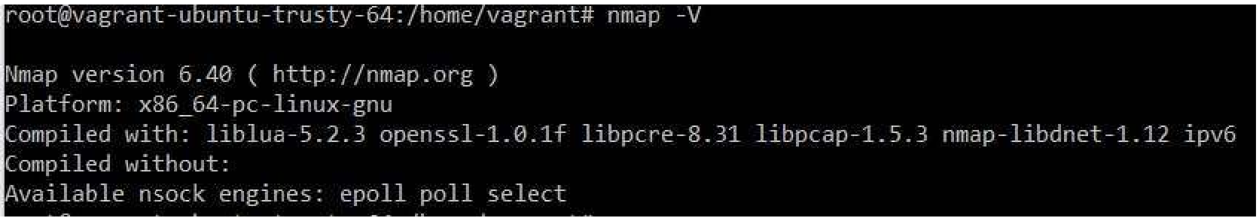
With this command we can find out network interfaces & route information. It is useful during debugging.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# nmap -iflist

Starting Nmap 6.40 ( http://nmap.org ) at 2016-02-18 17:15 UTC
************************INTERFACES************************
DEV  (SHORT) IP/MASK                      TYPE     UP MTU   MAC
eth0 (eth0)  10.0.2.15/24                 ethernet up 1500  08:00:27:FD:9E:15
eth0 (eth0)  fe80::a00:27ff:fefd:9e15/64 ethernet up 1500  08:00:27:FD:9E:15
eth1 (eth1)  192.168.2.8/24               ethernet up 1500  08:00:27:B2:5A:65
eth1 (eth1)  fe80::a00:27ff:feb2:5a65/64 ethernet up 1500  08:00:27:B2:5A:65
lo   (lo)    127.0.0.1/8                  loopback up 65536
lo   (lo)    ::1/128                      loopback up 65536

**************************ROUTES**************************
DST/MASK                     DEV  METRIC GATEWAY
10.0.2.0/24                  eth0 0
192.168.2.0/24               eth1 0
0.0.0.0/0                    eth0 0      10.0.2.2
::1/128                      lo   0
fe80::a00:27ff:feb2:5a65/128 lo   0
fe80::a00:27ff:fefd:9e15/128 lo   0
fe80::/64                    eth0 256
fe80::/64                    eth1 256
ff00::/8                     eth0 256
ff00::/8                     eth1 256
```

18. nmap -V IP_addr

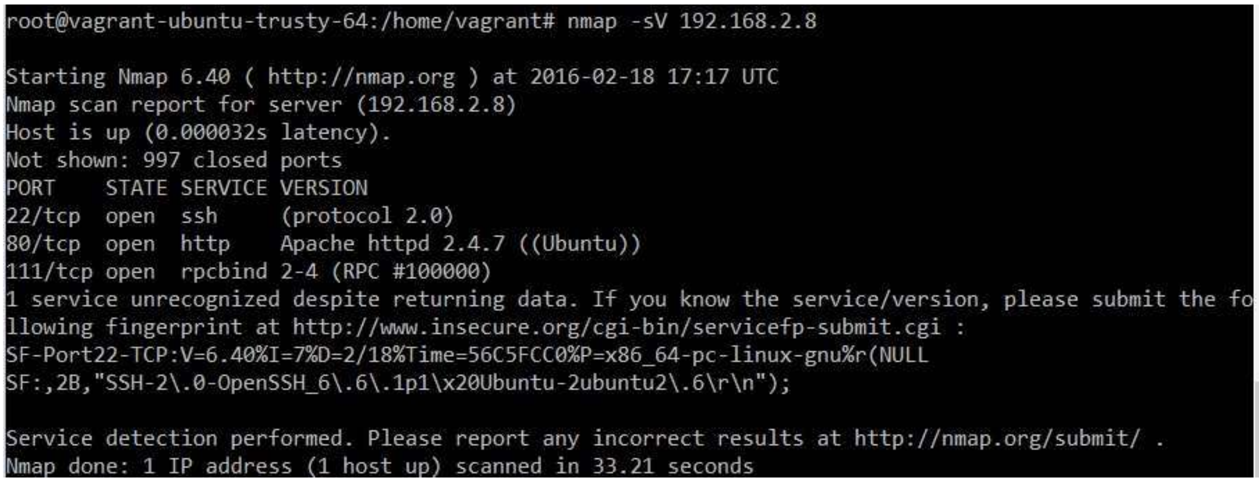
With “-V” option we can find out current install version of nmap on local machine.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# nmap -V

Nmap version 6.40 ( http://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.2.3 openssl-1.0.1f libpcre-8.31 libpcap-1.5.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

19. nmap –sV IP_addr

if we combine it as “-sV” then we can find service versions running on host.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# nmap -sV 192.168.2.8

Starting Nmap 6.40 ( http://nmap.org ) at 2016-02-18 17:17 UTC
Nmap scan report for server (192.168.2.8)
Host is up (0.000032s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     (protocol 2.0)
80/tcp  open  http    Apache httpd 2.4.7 ((Ubuntu))
111/tcp open  rpcbind 2-4 (RPC #100000)
1 service unrecognized despite returning data. If you know the service/version, please submit the fo
llowing fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:V=6.40%I=7%D=2/18%Time=56C5FCC0%P=x86_64-pc-linux-gnu%r(NULL
SF:,2B,"SSH-2\.0-OpenSSH_6\.6\.1p1\x20Ubuntu-2ubuntu2\.6\r\n");

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.21 seconds
```

20. scanning using ping protocol:

- Ping by host discovery method(when ICMP protocol blocks) for TCP protocol:

```
      Ex.    nmap -PS 192.168.2.2
             nmap -PS 80,21,443 ,22  192.168.1.2
             nmap -PA 192.168.1.1
             nmap -PA 80,21,200-512  192.168.2.8
```

- ping using IP protocol:

```
                nmap –PO   192.168.2.2
```

- ping using UDP protocol:

```
                nmap PU 192.168.2.
```

21. scan services using ports :

- scan for UDP services:

```
          nmap -sU www.google.com
          nmap -sU 192.168.1.1
```

- scan for TCP services:

```
        nmap -sS 192.168.1.1    ( stealthy scan)

        nmap -sT 192.168.1.1   (no stealth scan)

        nmap -sA 192.168.1.1   (ACK scan)

        nmap -sW 192.168.1.1  (window scan)

        nmap -sM 192.168.1.1   (maimon scan)
```

- scan fot IP services:

```
        namp  -sO 192.168.2.1
```

- scan for firewall check:

```
        nmap -sN 192.168.1.2
        nmap -sF 192.168.1.5
        nmap -sX 192.168.1.
```

---

22. we can save nmap output to a file using:

```
ex:-

    nmap 192.168.1.5 > nmap_soutput.txt

    nmap -oN /home/test/file_name 192.168.1.5

    nmap -oN nmap_output.txt 192.168.1.5
```

Lab

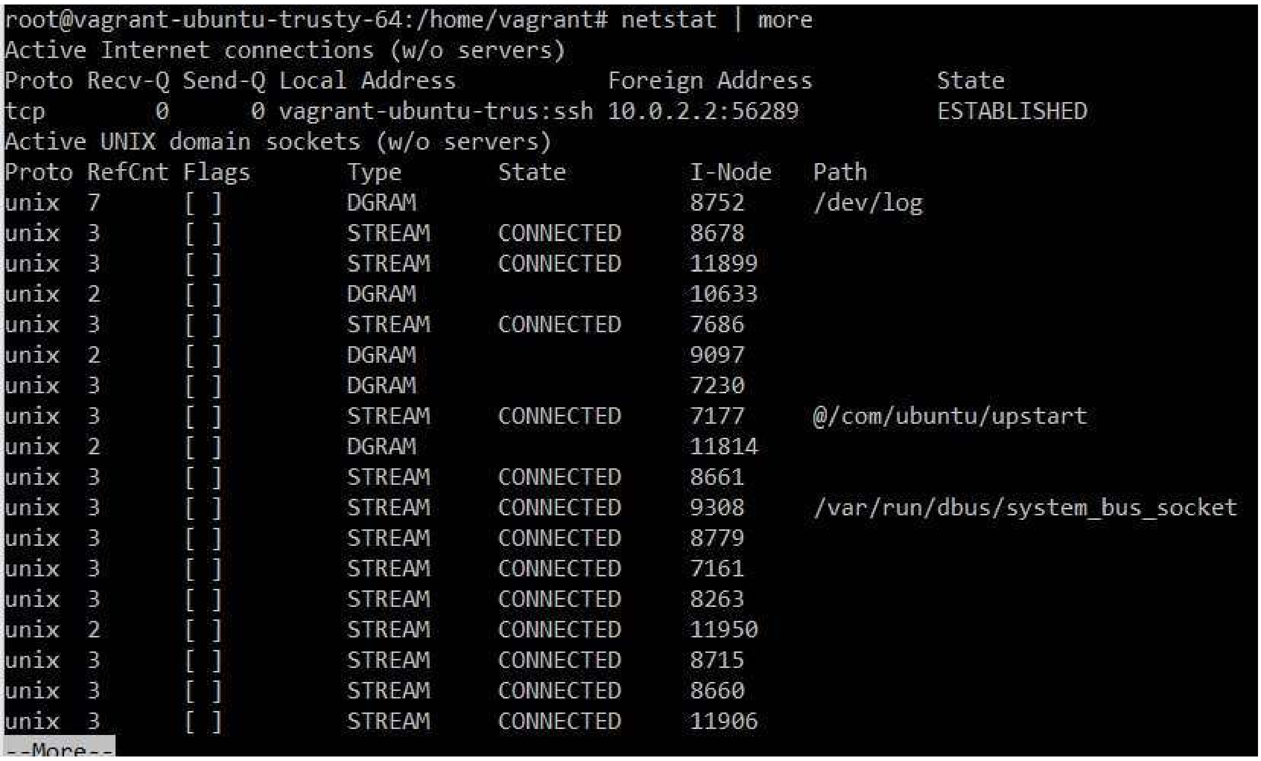
Netstat:-

Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. It prints the information related to Linux networking subsystem. It shows which ports are open & close, it is most useful command for network troubleshooting. This command is useful for network administration & system administration people.

Option:-

1. netstat

netstat displays a list of open sockets. If you don't specify any address families, then the active sockets of all configured address families it listed

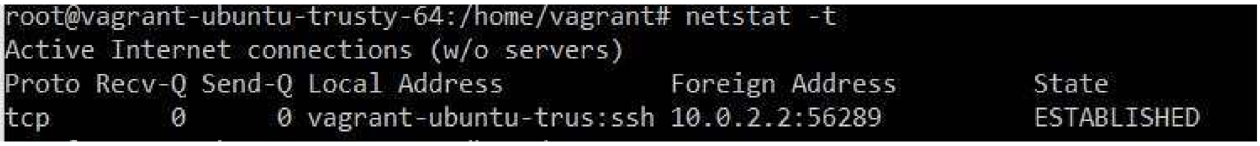


```
root@vagrant-ubuntu-trusty-64:/home/vagrant# netstat | more
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 vagrant-ubuntu-trus:ssh 10.0.2.2:56289          ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  7      [ ]         DGRAM                    8752     /dev/log
unix  3      [ ]         STREAM     CONNECTED     8678
unix  3      [ ]         STREAM     CONNECTED     11899
unix  2      [ ]         DGRAM                    10633
unix  3      [ ]         STREAM     CONNECTED     7686
unix  2      [ ]         DGRAM                    9097
unix  3      [ ]         DGRAM                    7230
unix  3      [ ]         STREAM     CONNECTED     7177     @/com/ubuntu/upstart
unix  2      [ ]         DGRAM                    11814
unix  3      [ ]         STREAM     CONNECTED     8661
unix  3      [ ]         STREAM     CONNECTED     9308     /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     8779
unix  3      [ ]         STREAM     CONNECTED     7161
unix  3      [ ]         STREAM     CONNECTED     8263
unix  2      [ ]         STREAM     CONNECTED     11950
unix  3      [ ]         STREAM     CONNECTED     8715
unix  3      [ ]         STREAM     CONNECTED     8660
unix  3      [ ]         STREAM     CONNECTED     11906
--More--
```

Its output like that but much big in length so just pipe it with more so you can go thgough all the list.

2. netstat –t

it shows list of programs which already have established TCP connection but, not those which are waiting for TCP connection



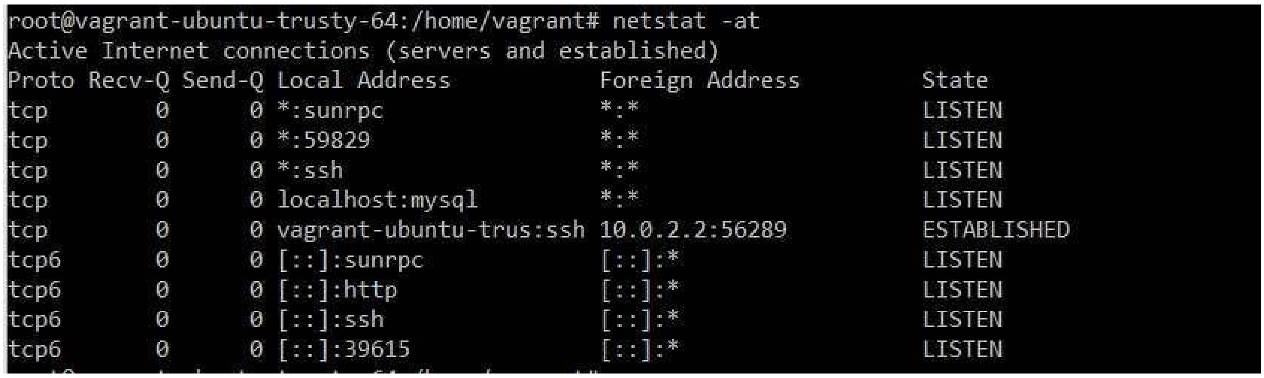
```
root@vagrant-ubuntu-trusty-64:/home/vagrant# netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 vagrant-ubuntu-trus:ssh 10.0.2.2:56289          ESTABLISHED
```

3. netstat –a

it shows list of listening & non listening sockets.

4. netstat –at

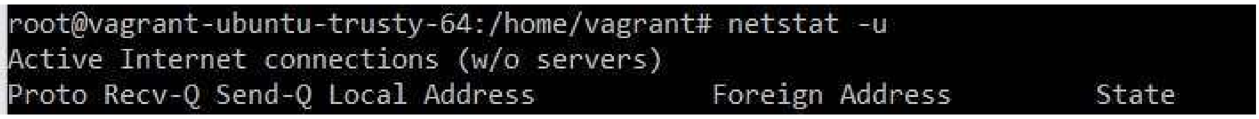
it list out all the programs which are listening & established TCP connection only.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:sunrpc                *:*                     LISTEN
tcp        0      0 *:59829                 *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 localhost:mysql         *:*                     LISTEN
tcp        0      0 vagrant-ubuntu-trus:ssh 10.0.2.2:56289          ESTABLISHED
tcp6       0      0 [::]:sunrpc             [::]:*                  LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 [::]:39615              [::]:*                  LISTEN
```

5. netstat –u

it list out all the programs which have already established UDP connection only not listening one.

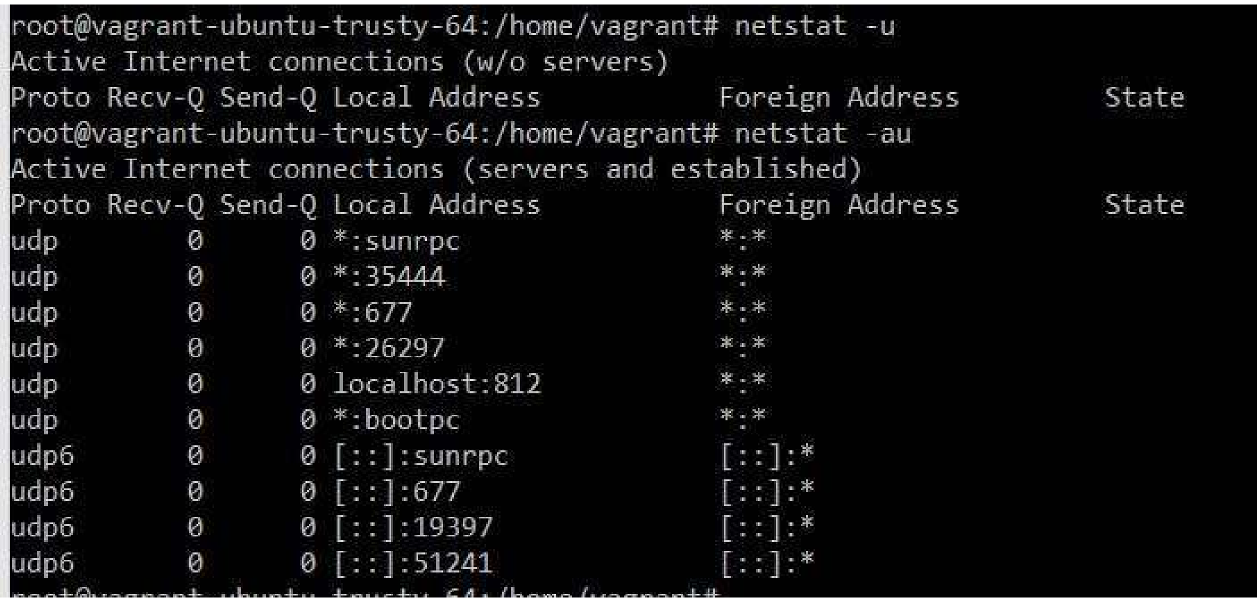


```
root@vagrant-ubuntu-trusty-64:/home/vagrant# netstat -u
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

Right now i don’t have any established UDP connection on my machine.

6. netstat –au

it list out all the programs which are listening & established UDP connection only.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# netstat -u
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
root@vagrant-ubuntu-trusty-64:/home/vagrant# netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 *:sunrpc                *:*
udp        0      0 *:35444                 *:*
udp        0      0 *:677                   *:*
udp        0      0 *:26297                 *:*
udp        0      0 localhost:812           *:*
udp        0      0 *:bootpc                *:*
udp6       0      0 [::]:sunrpc             [::]:*
udp6       0      0 [::]:677                [::]:*
udp6       0      0 [::]:19397              [::]:*
udp6       0      0 [::]:51241              [::]:*
root@vagrant-ubuntu-trusty-64:/home/vagrant#
```

7. netstat –l

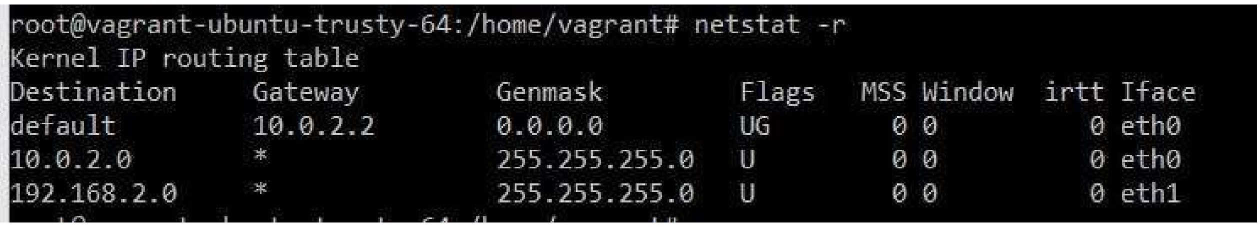
it shows all listening sockets.(whose which are omitted by default)

8. netstat -s

Display summary statistics for each protocol. Default protocol list are TCP,UDP,ICMP & IP.

9. netstat –r

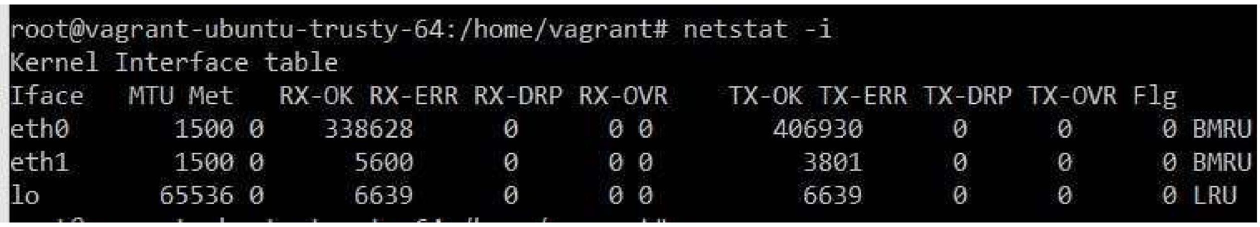
Dispaly kernel IP routing table.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         10.0.2.2        0.0.0.0         UG        0 0          0 eth0
10.0.2.0        *               255.255.255.0   U         0 0          0 eth0
192.168.2.0     *               255.255.255.0   U         0 0          0 eth1
```

10. netstat –i

Display kernel interface table. It shows network interface packet usage with MTU size.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# netstat -i
Kernel Interface table
Iface   MTU Met   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0      1500 0    338628      0      0 0       406930      0      0      0 BMRU
eth1      1500 0      5600      0      0 0         3801      0      0      0 BMRU
lo       65536 0      6639      0      0 0         6639      0      0      0 LRU
```

11. netstat –c

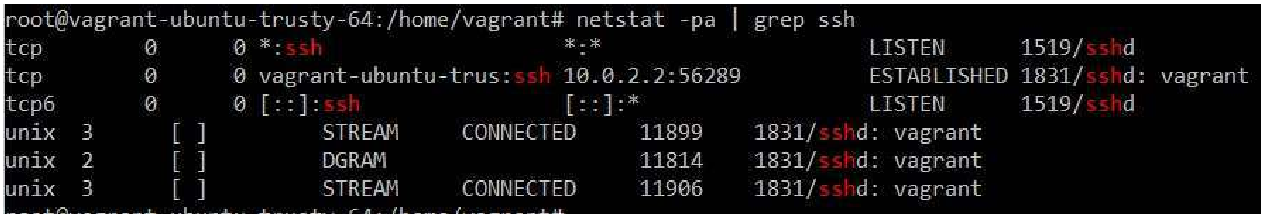
It print the netstat information continuously. If we menstion no along with then it print after that much duration of time

12. netstat –p

IT shows the list of services with their PID no which uses network sockets.

13. netstat –pa | grep ssh

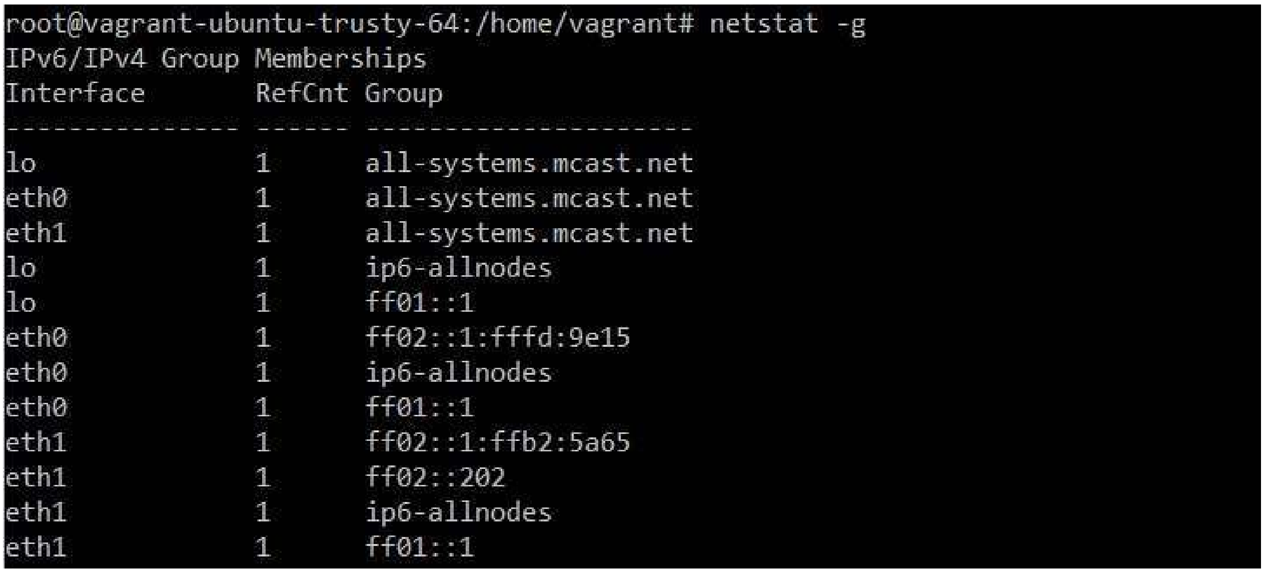
It displays the which programs are listening on specified port.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# netstat -pa | grep ssh
tcp        0      0 *:ssh                   *:*                     LISTEN      1519/sshd
tcp        0      0 vagrant-ubuntu-trus:ssh 10.0.2.2:56289          ESTABLISHED 1831/sshd: vagrant
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN      1519/sshd
unix  3      [ ]         STREAM     CONNECTED     11899    1831/sshd: vagrant
unix  2      [ ]         DGRAM                    11814    1831/sshd: vagrant
unix  3      [ ]         STREAM     CONNECTED     11906    1831/sshd: vagrant
```

14. netstat –g

It displays the multicast gropup membership information for IPv4/IPv6



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# netstat -g
IPv6/IPv4 Group Memberships
Interface       RefCnt Group
--------------- ------ ---------------------
lo              1      all-systems.mcast.net
eth0            1      all-systems.mcast.net
eth1            1      all-systems.mcast.net
lo              1      ip6-allnodes
lo              1      ff01::1
eth0            1      ff02::1:fffd:9e15
eth0            1      ip6-allnodes
eth0            1      ff01::1
eth1            1      ff02::1:ffb2:5a65
eth1            1      ff02::202
eth1            1      ip6-allnodes
eth1            1      ff01::1
```

15. netstat –F

Print routing information from the FIB. (This is the default.)

16. netstat –n

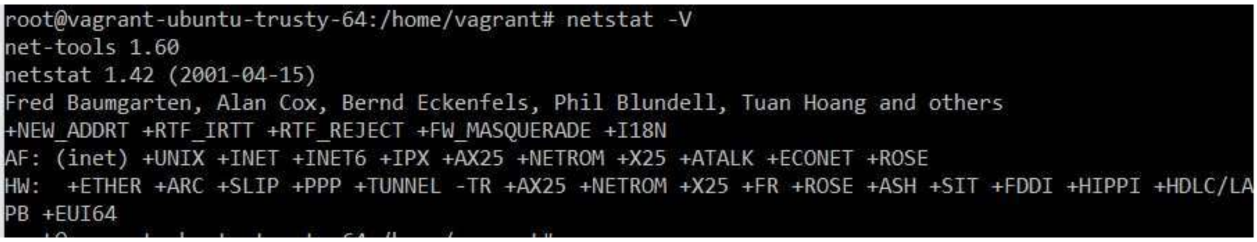
Show numerical addresses instead of trying to determine symbolic host, port or user names.

17. Netstat –M

Display a list of masqueraded connections.

18. netstat –V

shows the current version of netstat on system.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# netstat -V
net-tools 1.60
netstat 1.42 (2001-04-15)
Fred Baumgarten, Alan Cox, Bernd Eckenfels, Phil Blundell, Tuan Hoang and others
+NEW_ADDRT +RTF_IRTT +RTF_REJECT +FW_MASQUERADE +I18N
AF: (inet) +UNIX +INET +INET6 +IPX +AX25 +NETROM +X25 +ATALK +ECONET +ROSE
HW:  +ETHER +ARC +SLIP +PPP +TUNNEL -TR +AX25 +NETROM +X25 +FR +ROSE +ASH +SIT +FDDI +HIPPI +HDLC/LA
PB +EUI64
```

Lab

Traceroute:-

Print the route packets trace to network host.

It provides information number of routes presents between source to destination. It is important command to understand network flow. It takes maimum 30 hops to traceoute route,it does not means that their is only 30 routers/intermediate routers , it estimated & takes only main ISP & forwared information.

Usage:-

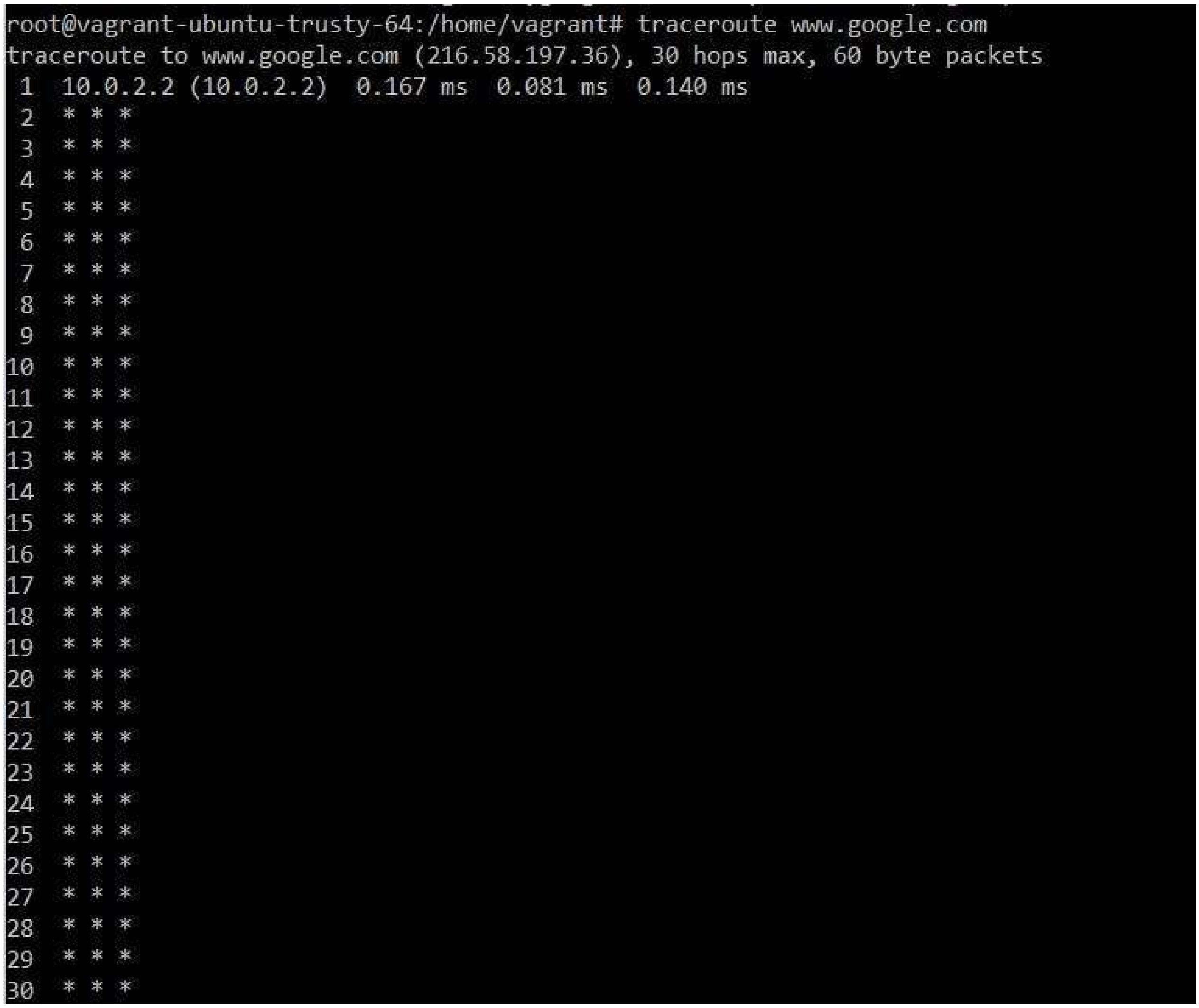
```
traceroute [-46dFITUnreAV] [-f first_ttl] [-g gate,...]
  [-i device] [-m max_ttl] [-p port] [-s src_addr]
  [-q nqueries] [-N squeries] [-t tos]
  [-l flow_label] [-w waittime] [-z sendwait] [-UL] [-D]
  [-P proto] [--sport=port] [-M method] [-O mod_options]
  [--mtu] [--back]
  host [packet_len]
traceroute6  [options]
tcptraceroute  [options]
lft  [options]
```

Options:-

1. traceroute domain_name/IP_addr

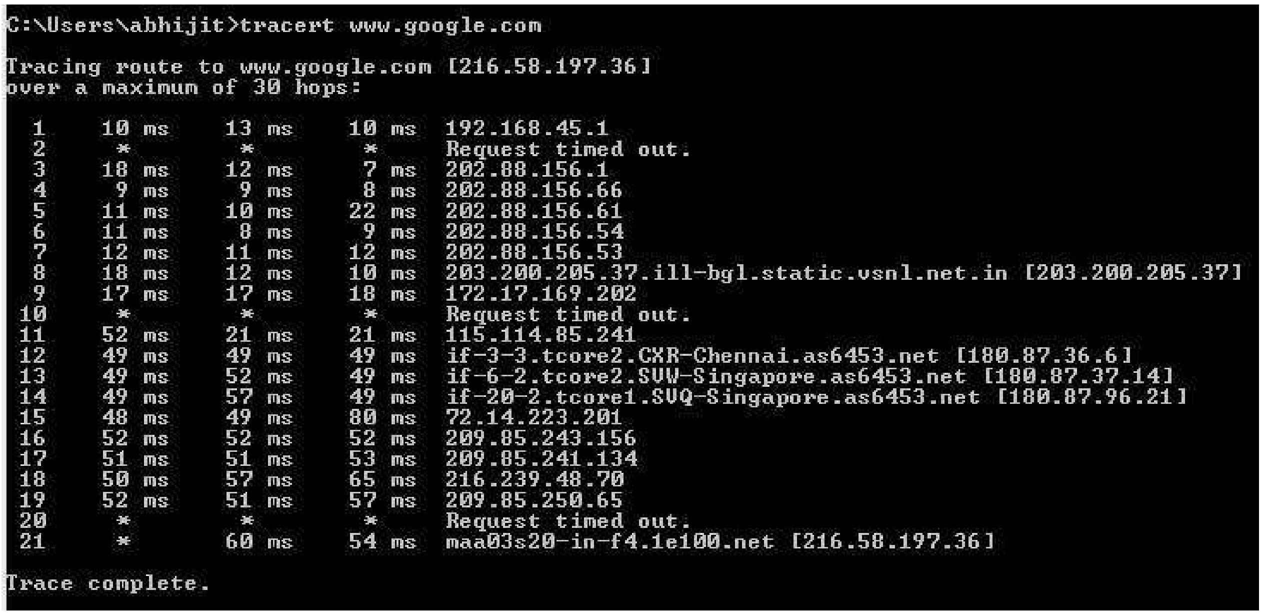
ex. traceroute www.google.com

It gives the route information to reach destination address. Maximum 30 hops are their whin that limit only it provide route information. If we get asterisks * signs its because some ICMP packets block by firewall or not respond in timely manner.(here its because i use virtualbox).



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# traceroute www.google.com
traceroute to www.google.com (216.58.197.36), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.167 ms  0.081 ms  0.140 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

same command i run on my local machine it gives me full path as shown below:-



```
C:\Users\abhijit>tracert www.google.com

Tracing route to www.google.com [216.58.197.36]
over a maximum of 30 hops:

  1    10 ms    13 ms    10 ms  192.168.45.1
  2     *        *        *     Request timed out.
  3    18 ms    12 ms     7 ms  202.88.156.1
  4     9 ms     9 ms     8 ms  202.88.156.66
  5    11 ms    10 ms    22 ms  202.88.156.61
  6    11 ms     8 ms     9 ms  202.88.156.54
  7    12 ms    11 ms    12 ms  202.88.156.53
  8    18 ms    12 ms    10 ms  203.200.205.37.ill-bgl.static.vsnl.net.in [203.200.205.37]
  9    17 ms    17 ms    18 ms  172.17.169.202
 10     *        *        *     Request timed out.
 11    52 ms    21 ms    21 ms  115.114.85.241
 12    49 ms    49 ms    49 ms  if-3-3.tcore2.CXR-Chennai.as6453.net [180.87.36.6]
 13    49 ms    52 ms    49 ms  if-6-2.tcore2.SVW-Singapore.as6453.net [180.87.37.14]
 14    49 ms    57 ms    49 ms  if-20-2.tcore1.SVQ-Singapore.as6453.net [180.87.96.21]
 15    48 ms    49 ms    80 ms  72.14.223.201
 16    52 ms    52 ms    52 ms  209.85.243.156
 17    51 ms    51 ms    53 ms  209.85.241.134
 18    50 ms    57 ms    65 ms  216.239.48.70
 19    52 ms    51 ms    57 ms  209.85.250.65
 20     *        *        *     Request timed out.
 21     *       60 ms    54 ms  maa03s20-in-f4.1e100.net [216.58.197.36]

Trace complete.
```

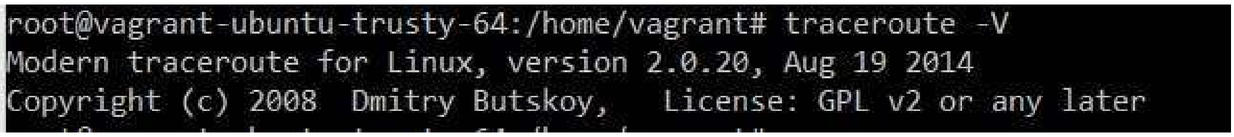
2. tracerout –mtu domain_name/IP_addr

ex. traceroute --mtu www.google.com

It gives information of mtu(maximum trasmistion unit) for hop, if firewall settings not blocking it. In the form of F=number.

3. traceroute –V

It tells the version traceroute used on your local machine.



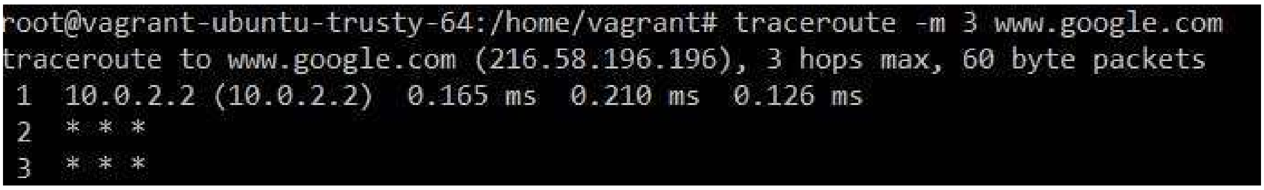
```
root@vagrant-ubuntu-trusty-64:/home/vagrant# traceroute -V
Modern traceroute for Linux, version 2.0.20, Aug 19 2014
Copyright (c) 2008  Dmitry Butskoy,   License: GPL v2 or any later
```

4. traceroute –m count domain_name/IP_addr

ex. traceroute -m count 3 www.google.com

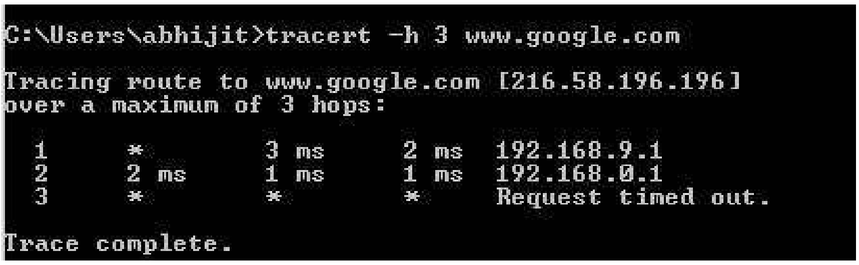
We know maximunm hop count is 30 we can limit that with this command with option m & providing count along with it,so it only show that no of hops. It count from starting incremental manner.

as shown below it just look upto first 3 hosts.(its virtual machine so its unable to dermine path)



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# traceroute -m 3 www.google.com
traceroute to www.google.com (216.58.196.196), 3 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.165 ms  0.210 ms  0.126 ms
 2  * * *
 3  * * *
```

same output on my local machine (as its windows so "-h" oprion used with traceoute)



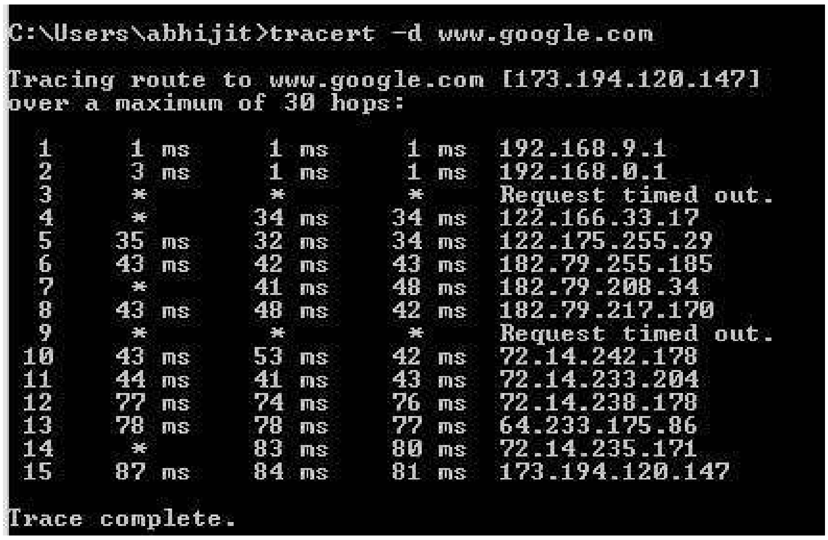
```
C:\Users\abhijit>tracert -h 3 www.google.com

Tracing route to www.google.com [216.58.196.196]
over a maximum of 3 hops:

  1     *        3 ms     2 ms  192.168.9.1
  2     2 ms     1 ms     1 ms  192.168.0.1
  3     *        *        *     Request timed out.

Trace complete.
```

5. traceroute –n domain_name/IP_addr

ex. traceroute -n www.google.com

With –n option it eliminates FKDN only shows ip address, only shows output in numerical form.

as its output on windows machine "d" option i used , as shown below its just show IP address No FKDN .



```
C:\Users\abhijit>tracert -d www.google.com

Tracing route to www.google.com [173.194.120.147]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.9.1
  2     3 ms     1 ms     1 ms  192.168.0.1
  3     *        *        *     Request timed out.
  4     *       34 ms    34 ms  122.166.33.17
  5    35 ms    32 ms    34 ms  122.175.255.29
  6    43 ms    42 ms    43 ms  182.79.255.185
  7     *       41 ms    48 ms  182.79.208.34
  8    43 ms    48 ms    42 ms  182.79.217.170
  9     *        *        *     Request timed out.
 10    43 ms    53 ms    42 ms  72.14.242.178
 11    44 ms    41 ms    43 ms  72.14.233.204
 12    77 ms    74 ms    76 ms  72.14.238.178
 13    78 ms    78 ms    77 ms  64.233.175.86
 14     *       83 ms    80 ms  72.14.235.171
 15    87 ms    84 ms    81 ms  173.194.120.147

Trace complete.
```

6. traceroute -4 /-6 domain_name

ex.traceroute -4 www.google.com

traceroute -6 www.google.com

Explicitly force to use IPv4 or IPv6 addressing scheme for tracerouting. By default it automatically choose protocol & resolve name.

7. traceroute -I domain_name/IP_addr

ex. traceroute -I www.google.com

It forces to choose ICMP_ECHO method for tracerouting.

8. traceroute -T domain_name/IP_addr

ex. traceroute -T www.google.com

It forces to choose TCP_SYN method for tracerouting.

9. traceroute -q domain_name/IP_addr

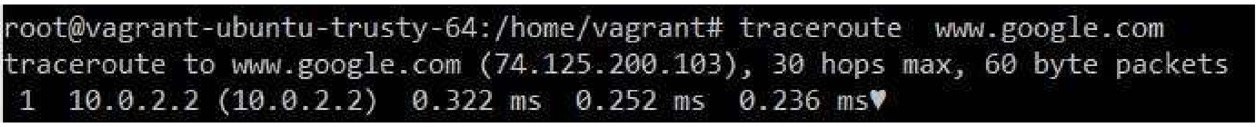
ex. traceroute -q www.google.com

option '-q' allows to change number of retries (default is 3).

10. traceroute domain_name/IP_addr packet_len

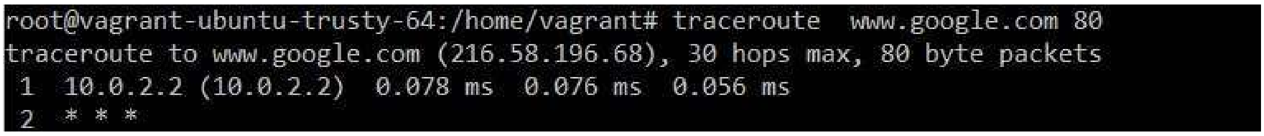
ex. traceroute www.google.com 80 It is use to modify original packet length using this command.

length of treaceroute packet here is 60 byte.as you can see below:



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# traceroute  www.google.com
traceroute to www.google.com (74.125.200.103), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.322 ms  0.252 ms  0.236 ms♥
```

modified lenth of packet:



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# traceroute  www.google.com 80
traceroute to www.google.com (216.58.196.68), 30 hops max, 80 byte packets
 1  10.0.2.2 (10.0.2.2)  0.078 ms  0.076 ms  0.056 ms
 2  * * *
```

11. traceroute –F domain_name/IP_addr

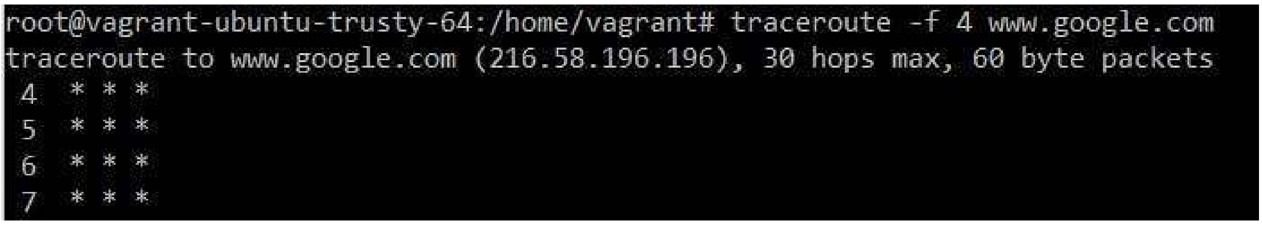
ex. traceroute -F www,google.com

It means do not fragments or splits the original probes packet.

12. traceroute –f [first_ttl] domain_name/IP_addr

ex. traceroute -f 4 www.google.com

It specifies from which ttl to start routing , by default it start from 1.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# traceroute -f 4 www.google.com
traceroute to www.google.com (216.58.196.196), 30 hops max, 60 byte packets
 4  * * *
 5  * * *
 6  * * *
 7  * * *
```

13. traceroute -g [gateway] domain_name/IP_addr

Tells traceroute to add an IP source routing option to the outgoing packet that tells the network to route the packet through the specified gateway (most routers have disabled source routing for security reasons).

14. traceroute –i [interface] domain_name/IP_addr

We can mention interface so that from which interface traceroute should send packets. By default it is selected according to routing table.

15. traceroute [–N squeries] domain_name/IP_addr

With this we can specify maximum no. of prob packets send simultaneously. Maximum vaue is 16. But if we incease size their is chances of packet get lost. Same side it is speed up response

16. traceroute [-s source_addr] domain_name/IP_addr

With this we can choose alternative souce address from interfaces, default outgoing interface address used.

17. traceroute [-p port] domain_name/IP_addr

Used for UDP port

18. traceroute [-w timeout_time] domain_addr/IP_addr

It is used to set time to respond for each probe . by default it is 3 sec.

Lab

Tcptraceroute:-

Is a traceroute implementation using TCP packets. Normal traceroute command uses ICMP or UDP protocol ECHO packet with TTL. But now a days most modern machine has firewall configured which blocks the ICMP & UDP protocol , so its not possible to trace out destination path. However firewall allowes inbound TCP packets , so with tcptraceroute utility it is possible to trace destination path.

It is worth noting that tcptraceroute never completely establishes a TCP connection with the destination host. If the host is not listening for incoming connections, it will respond with an RST indicating that the port is closed. If the host instead responds with a SYN|ACK, the port is known to be open, and an RST is sent by the kernel tcptraceroute is running on to tear down the connection without completing three-way handshake. This is the same half-open scanning technique.

Usage:-

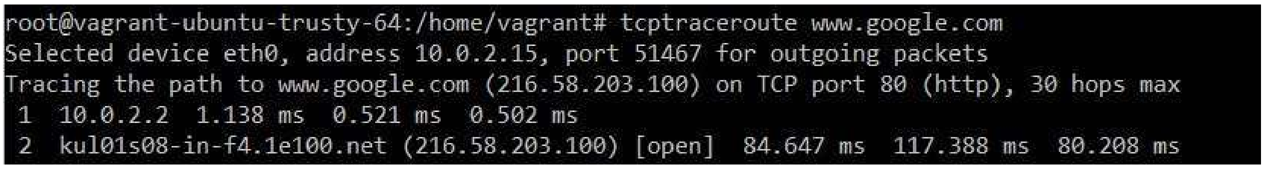
tcptraceroute [-nNFSAE] [-i] [-f] [-l] [-q] [-t] [-m] [-pP]] [-s] [-w] [destination port] [packet length]

Options:-

1. tcptreaceroute IP_addr/domain_server

ex. tcptraceroute www.google.com

It gives the route information to reach destination address using TCP packets.



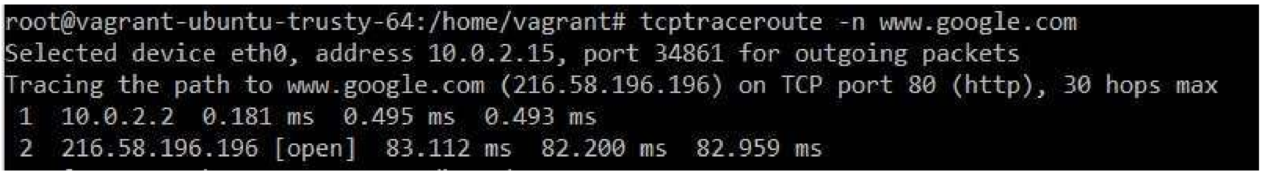
```
root@vagrant-ubuntu-trusty-64:/home/vagrant# tcptraceroute www.google.com
Selected device eth0, address 10.0.2.15, port 51467 for outgoing packets
Tracing the path to www.google.com (216.58.203.100) on TCP port 80 (http), 30 hops max
 1  10.0.2.2  1.138 ms  0.521 ms  0.502 ms
 2  kul01s08-in-f4.1e100.net (216.58.203.100) [open]  84.647 ms  117.388 ms  80.208 ms
```

---

2. tcptraceroute -n IP_addr/domain_name

ex. tcptraceroute -n www.google.com

It gives information in numerical form it dont display FQDN information associated with hosts.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# tcptraceroute -n www.google.com
Selected device eth0, address 10.0.2.15, port 34861 for outgoing packets
Tracing the path to www.google.com (216.58.196.196) on TCP port 80 (http), 30 hops max
 1  10.0.2.2  0.181 ms  0.495 ms  0.493 ms
 2  216.58.196.196 [open]  83.112 ms  82.200 ms  82.959 ms
```

3. tcptraceroute –f [first_ttl] domain_name/IP_addr

ex. tcptraceroute -f 4 www.google.com

It specifies from which ttl to start routing , by default it start from 1.

4. tcptraceroute -s [source_addr] domain_name/IP_addr

ex. tcptraceroute -s 192.168.2.5 www.google.com

we can set source address from which packets send to destination address to trace route from.

5. tcptraceroute –m count domain_name/IP_addr

ex. tcptraceroute -m count 3 www.google.com

We know maximunm hop count is 30 we can limit that with this command with option m & providing count along with it,so it only show that no of hops. It count from starting incremental manner.

6. tcptraceroute –i [interface] domain_name/IP_addr

We can mention interface so that from which interface tcptraceroute should send packets. By default it is selected according to routing table.

7. tcptraceroute [-w timeout_time] domain_addr/IP_addr

It is used to set time to respond for each probe . By default it is 3 sec.

8. tcptraceroute –F domain_name/IP_addr

ex. tcptraceroute -F www,google.com

It means do not fragments or splits the original probes packet.

9. tcptraceroute domain_name/IP_addr

ex. tcptraceroute www.google.com 110

Set the total packet length to be used in outgoing packets. If the length is greater than the minimum size required to assemble the necessary probe packet headers, this value is automatically increased.

10. tcptraceroute -S domain_name/IP_addr

Set the TCP SYN flag in outgoing packets. This is the default, if neither -S or -A is specified.

11. tcptraceroute -A domain_name/IP_addr

Set the TCP ACK flag in outgoing packets. By doing so, it is possible to trace through stateless firewalls which permit out- going TCP connections.

12. tcptraceroute -E domain_name/IP_addr

Send ECN SYN packets, as described in RFC2481.

Lab

Whois:-

client for the whois directory service. it provide owner,technical contact of virtually any public domain name. whois is protocol use for searching server of specified object. whois searches for an object in a RFC 3912 database.If no guess can made then it will connect to whois.networksolutions.com for NIC handles or whois.arin.net for IPv4 addresses and network names.

Usage:-

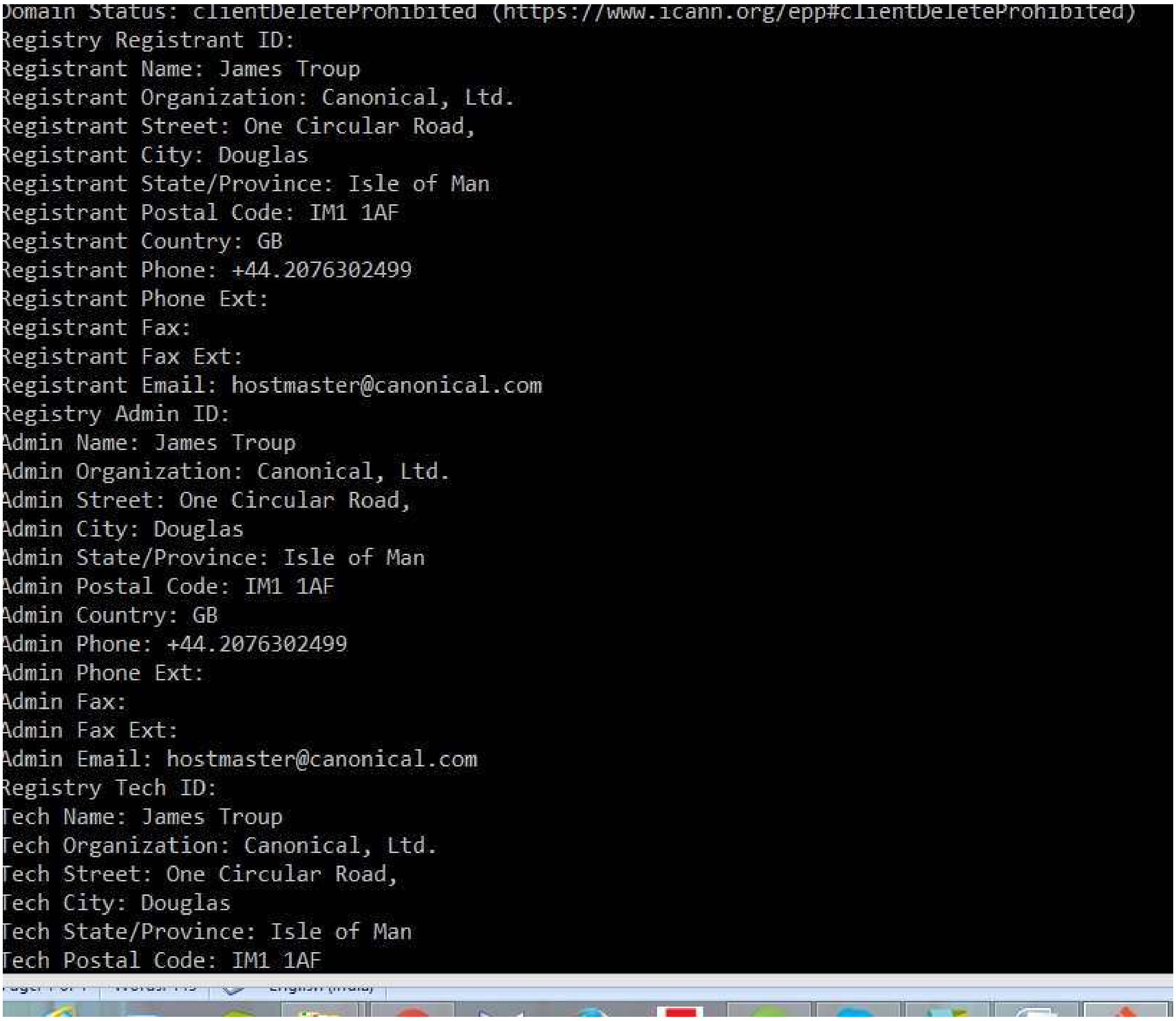
whois [OPTION]... OBJECT..[-h host] [-p port] [-alLMmcxbBGdKrR] [-i ATTR] [-T type]

Options:-

1. whois domain_name/IP_addr

ex. whois ubuntu.com

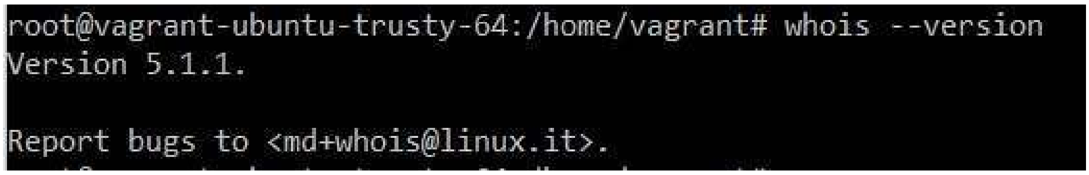
It gives register domain information owner ,technical contacts.



```
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Registry Registrant ID:
Registrant Name: James Troup
Registrant Organization: Canonical, Ltd.
Registrant Street: One Circular Road,
Registrant City: Douglas
Registrant State/Province: Isle of Man
Registrant Postal Code: IM1 1AF
Registrant Country: GB
Registrant Phone: +44.2076302499
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: hostmaster@canonical.com
Registry Admin ID:
Admin Name: James Troup
Admin Organization: Canonical, Ltd.
Admin Street: One Circular Road,
Admin City: Douglas
Admin State/Province: Isle of Man
Admin Postal Code: IM1 1AF
Admin Country: GB
Admin Phone: +44.2076302499
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: hostmaster@canonical.com
Registry Tech ID:
Tech Name: James Troup
Tech Organization: Canonical, Ltd.
Tech Street: One Circular Road,
Tech City: Douglas
Tech State/Province: Isle of Man
Tech Postal Code: IM1 1AF
```

2. whois --version

Gives version information.



```
root@vagrant-ubuntu-trusty-64:/home/vagrant# whois --version
Version 5.1.1.

Report bugs to <md+whois@linux.it>.
```

3. whois [-p port] domain_name

This command allow to used specified port as menstion in command.By default it uses port 43.

4. whois –v domain_name

Verbose display. It display output in detailed manner , what is being done.

5. whois –H domain_name

It use to hide legal disclaimers information.

6. whois --help

Use for online help.

Reading List

- Command Line Fu: http://www.commandlinefu.com/commands/browse
- Command Line Cookbook: https://www.gitbook.com/book/minhhh/command-line-cookbook
- Ops School : http://www.opsschool.org/en/latest/
- The Linux Cookbook : http://dsl.org/cookbook/cookbook_toc.html
- Kernel and Systems Programming: https://www.gitbook.com/book/0xax/linux-insides/details