7. Linux Networking Commands

TechData-Infinity-Devops with MultiCloud

Linux ifconfig –

The command ifconfig stands for interface configurator. This command enables us to initialize an interface, assign IP address, enable or disable an interface. It display route and network interface.

ifconfig

Hostname -i

```
root@ip-172-31-8-13:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 172.31.8.13  netmask 255.255.240.0  broadcast 172.31.15.255
        inet6 fe80::87b:4cff:fecb:da54  prefixlen 64  scopeid 0x20<link>
        ether 0a:7b:4c:cb:da:54  txqueuelen 1000  (Ethernet)
        RX packets 14055  bytes 2127912 (2.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12256  bytes 1374101 (1.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 130  bytes 14273 (14.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 130  bytes 14273 (14.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@ip-172-31-8-13:~# hostname -i
172.31.8.13
root@ip-172-31-8-13:~#
```

Get details of specific interface-

ifconfig eth0

```
root@ip-172-31-8-13:~# ifcofig eth0
Command 'ifcofig' not found, did you mean:
  command 'ifconfig' from deb net-tools (1.60+git20181103.0eebece-1ubuntu5)
Try: apt install <deb name>
root@ip-172-31-8-13:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 172.31.8.13  netmask 255.255.240.0  broadcast 172.31.15.255
        inet6 fe80::87b:4cff:fecb:da54  prefixlen 64  scopeid 0x20<link>
        ether 0a:7b:4c:cb:da:54  txqueuelen 1000  (Ethernet)
        RX packets 14186  bytes 2136033 (2.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12376  bytes 1386979 (1.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@ip-172-31-8-13:~#
```

TechData-Infinity-Devops with MultiCloud

Linux traceroute command-

Linux traceroute command is a network troubleshooting utility that helps us determine the number of hops and packets traveling path required to reach a destination. It is used to display how the data transmitted from a local machine to a remote machine. Loading a web page is one of the common examples of the traceroute. A web page loading transfers data through a network and routers. The traceroute can display the routes, IPaddresses, and hostnames of routers over a network. It can be useful for diagnosing network issues.

apt install inetutils-traceroute

apt install traceroute

The above commands will install the traceroute utility on our system. After the successful installation, the output will look like as follows:

traceroute ygminds.com

```
root@ip-172-31-8-13:~# traceroute ygminds.com
traceroute to ygminds.com (103.171.45.241), 64 hops max
  1    52.66.0.243   4.632ms   16.366ms   1.674ms
  2    100.65.19.64   4.743ms   8.162ms   8.114ms
  3    100.66.8.138   4.165ms   8.205ms   8.186ms
  4    100.66.11.160   6.260ms   8.085ms   8.509ms
  5    100.66.6.103   55.192ms   61.146ms   58.743ms
  6    100.66.4.157   6.818ms   8.171ms   7.938ms
  7    100.65.8.65   0.514ms   0.513ms   0.566ms
  8    99.83.77.25   6.368ms   1.425ms   1.114ms
  9    52.95.67.174   4.011ms   5.965ms   5.902ms
 10    52.95.65.224   0.651ms   1.131ms   0.766ms
 11    115.114.89.57   0.804ms   0.707ms   0.688ms
 12    *   *   *
 13    219.65.44.178   22.596ms   22.711ms   22.493ms
 14    180.179.197.214   22.594ms   22.699ms   22.628ms
 15    180.179.194.124   26.635ms   24.119ms   24.283ms
 16    *   *   *
```

Linux tracepath –

It is similar to traceroute command, but it doesn't require root privileges. By default, it is installed in Ubuntu but you may have to download traceroute on Ubuntu. It traces the network path of the specified destination and reports each hop along the path. If you have a slow network then tracepath will show you where your network is weak.

tracepath <destination>

```
ubuntu@ip-172-31-8-13:~$ tracepath ygminds.com
 1?: [LOCALHOST]                                         pmtu 1500
 1:  no reply
 2:  no reply
 3:  no reply
 4:  no reply
 5:  no reply
 6:  no reply
 7:  100.65.10.65                                      18.321ms asymm  8
 8:  99.83.77.31                                        0.654ms
 9:  99.83.76.242                                       1.495ms asymm 14
10:  52.95.65.230                                       0.599ms asymm 12
11:  115.114.89.57.static-Mumbai.vsnl.net.in            0.976ms asymm 13
12:  no reply
13:  219.65.44.178.static-delhi.vsnl.net.in            22.608ms asymm 18
14:  180.179.197.202                                   21.442ms asymm 19
15:  180.179.194.124                                   27.670ms asymm 20
16:  no reply
17:  no reply
```

TechData-Infinity-Devops with MultiCloud

Linux ping Command-

Linux ping command stands for (Packet Internet Groper). It checks connectivity between two nodes to see if a server is available. It sends ICMP ECHO_REQUEST packets to network hosts and displays the data on the remote server's response. It checks if a remote host is up, or that network interfaces can be reached. Further, it is used to check if a network connection is available between two devices. It is also handy tool for checking your network connection and verifying network issues.

Ping command keeps executing and sends the packet until you interrupt.

The ping command supports various command-line options. But, the basic syntax for the ping command is as follows:

ping <option> <destination>

```
root@ip-172-31-8-13:~# ping ygminds.com
PING ygminds.com (103.171.45.241) 56(84) bytes of data.
64 bytes from server.exabyteserver.com (103.171.45.241): icmp_seq=1 ttl=44 time=21.7 ms
64 bytes from server.exabyteserver.com (103.171.45.241): icmp_seq=2 ttl=44 time=21.8 ms
64 bytes from server.exabyteserver.com (103.171.45.241): icmp_seq=3 ttl=44 time=21.8 ms
64 bytes from server.exabyteserver.com (103.171.45.241): icmp_seq=4 ttl=44 time=21.6 ms
64 bytes from server.exabyteserver.com (103.171.45.241): icmp_seq=5 ttl=44 time=21.8 ms
64 bytes from server.exabyteserver.com (103.171.45.241): icmp_seq=6 ttl=44 time=21.7 ms
64 bytes from server.exabyteserver.com (103.171.45.241): icmp_seq=7 ttl=44 time=21.7 ms
64 bytes from server.exabyteserver.com (103.171.45.241): icmp_seq=8 ttl=44 time=21.7 ms
64 bytes from server.exabyteserver.com (103.171.45.241): icmp_seq=9 ttl=44 time=21.8 ms
64 bytes from server.exabyteserver.com (103.171.45.241): icmp_seq=10 ttl=44 time=21.7 ms
64 bytes from server.exabyteserver.com (103.171.45.241): icmp_seq=11 ttl=44 time=21.7 ms
```

We can limit the number of sent packets by using the ping command. To limit the packet, specify the 'c' option followed by the number of packets to be sent. It will be executed as:

ping -c <number> <destination>

Ping -c 5 ygminds.com

```
root@ip-172-31-8-13:~# ping -c 5 ygminds.com
PING ygminds.com (103.171.45.241) 56(84) bytes of data.
64 bytes from server.exabyteserver.com (103.171.45.241): icmp_seq=1 ttl=44 time=21.8 ms
64 bytes from server.exabyteserver.com (103.171.45.241): icmp_seq=2 ttl=44 time=21.8 ms
64 bytes from server.exabyteserver.com (103.171.45.241): icmp_seq=3 ttl=44 time=22.3 ms
64 bytes from server.exabyteserver.com (103.171.45.241): icmp_seq=4 ttl=44 time=21.8 ms
64 bytes from server.exabyteserver.com (103.171.45.241): icmp_seq=5 ttl=44 time=21.8 ms

--- ygminds.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 21.822/21.934/22.314/0.190 ms
root@ip-172-31-8-13:~#
```

Linux netstat Command-

Linux netstat command stands for **Network statistics**. It displays information about different interface statistics, including open sockets, routing tables, and connection information. Further, it can be used to displays all the socket connections (including TCP, UDP). Apart from connected sockets, it also displays the sockets that are pending for connections. It is a handy tool for network and system administrators.

apt install net-tools

netstat- a

```
root@ip-172-31-8-13:~# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:http            0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0    332 ip-172-31-8-13.ap-s:ssh 150.107.192.87:37514    ESTABLISHED
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 ip-172-31-8-13.a:bootpc 0.0.0.0:*
udp        0      0 localhost:323           0.0.0.0:*
udp        0      0 ip-172-31-8-13.ap:55740 ip-172-31-0-2.ap:domain ESTABLISHED
udp6       0      0 ip6-localhost:323       [::]:*
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (servers and established)
```

Linux dig Command (DNS Lookup)-

Linux dig command stands for **Domain Information Groper**. This command is used for tasks related to DNS lookup to query DNS name servers. It mainly deals with troubleshooting DNS related problems. It is a flexible utility for examining the DNS (Domain Name Servers). It is used to perform the DNS lookups and returns the queried answers from the name server. Usually, it is used by most DNS administrators to troubleshoot the DNS problems. It is a straightforward tool and provides a clear output. It is more functional than other lookups tools.

The dig command supports plenty of command-line options. Additionally, it facilitates batch mode, which is useful for accessing the lookup requests from a file. If it is not specified to the dig command to query a specific name server, it will access each of the servers from **"/etc/resolv.conf**." The dig without any command-line options will perform an NS query for "." (the root).

Query a Domain name

dig ygminds.com

```
ubuntu@ip-172-31-8-13:~$ dig ygminds.com

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> ygminds.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24936
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;ygminds.com.                   IN      A

;; ANSWER SECTION:
ygminds.com.            300     IN      A       103.171.45.241

;; Query time: 95 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Jul 09 07:29:34 UTC 2022
;; MSG SIZE  rcvd: 56
```

Linux nslookup –

This command is also used to find DNS related query.

nslookup <domainName>

```
root@ip-172-31-8-13:~# nslookup ygminds.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ygminds.com
Address: 103.171.45.241

root@ip-172-31-8-13:~#
```

```
root@ip-172-31-42-137:~# awk '/0$/' information.txt
Thomas          Shelby          30      Rio         400
Omega           Night           45      Ontario     600
Giorgos         Georgiou        35      London      300
root@ip-172-31-42-137:~#
```