Arsenia Suero

11/24/2021 original

12/12/2021 revised

Networking.

CentOS Server.

Current network configuration

- **System Ip address, and interfaces.**

```
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.44.128  netmask 255.255.255.0  broadcast 192.168.44.255
        inet6 fe80::20c:29ff:fe07:a5e2  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:07:a5:e2  txqueuelen 1000  (Ethernet)
        RX packets 19737  bytes 28085244 (26.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6230  bytes 406171 (396.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:a6:20:3b  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
```

TX packets 0 bytes 0 (0.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

- **Route table**

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	_gateway	0.0.0.0	UG	100	0	0	ens33
172.17.0.0	0.0.0.0	255.255.0.0	U	0	0	0	docker0
192.168.44.0	0.0.0.0	255.255.255.0	U	100	0	0	ens33
192.168.122.0	0.0.0.0	255.255.255.0	U	0	0	0	virbr0

- **Domain name**

localhost.localdomain

- **Current Users**

asuero tty2 tty2 01:35 1:10m 1:03 0.26s /usr/libexec/tr

- **Open Ports**

tcp	0	0	192.168.122.1:53	0.0.0.0:*	LISTEN	1659/dnsmasq
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	1152/sshd
tcp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN	1141/cupsd
tcp	0	0	0.0.0.0:111	0.0.0.0:*	LISTEN	1/systemd
tcp6	0	0	:::22	:::*	LISTEN	1152/sshd
tcp6	0	0	::1:631	:::*	LISTEN	1141/cupsd
tcp6	0	0	:::111	:::*	LISTEN	1/systemd

What is installed?

```
ID   | Command line                  | Date and time  | Action(s)  | Altered
-------------------------------------------------------------------------------
  19 | -y install libvirt qemu-k     | 2021-12-10 01:04 | Install      |  31
  18 | install -y kubelet kubead     | 2021-12-10 00:42 | Install      |  10
  17 | install docker-ce --nobes     | 2021-12-09 23:36 | E, I, O      |  12
  16 | install -y yum-utils          | 2021-12-09 22:04 | Install      |   1
  15 | update                        | 2021-12-09 21:47 | I, O, U      | 534 EE
  14 | install sendEmail             |  2021-12-05 23:27 | Install      |   3
  13 | install lynis                 | 2021-12-04 19:43 | Install      |   1
  12 |                               | 2021-12-03 21:24 | Install      |   2
  11 |  net-tools                    | 2021-12-03 21:22 | Install      |   1
  10 | install snapd                 | 2021-12-02 16:39 | Upgrade      |   5
   9 | install nload                 | 2021-11-30 00:50 | Install      |   1
   8 | install vim                   | 2021-11-24 00:33 | Upgrade      |   2
   7 | install snapd                 | 2021-11-24 00:03 | Install      |   3
   6 | install cowsay                | 2021-11-23 22:27 | Install      |   1
   5 | install fail2ban              | 2021-11-23 22:22 | Install      |   6
   4 | install emacs                 | 2021-11-23 18:33 | I, U         |   6
   3 | install epel-release          | 2021-11-23 09:57 | Install      |   1
   2 | update                        | 2021-10-23 14:10 | I, U         |  40 EE
   1 |
```

- **Last update of the apps:** **12/10/2021**
- **No Changes to the default network**

Executed Script Sample.

Bash Script that dump my network information

Ip Address.

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever preferred_lft forever 2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000 link/ether 00:0c:29:07:a5:e2 brd ff:ff:ff:ff:ff:ff inet 192.168.44.128/24 brd 192.168.44.255 scope global dynamic noprefixroute ens33 valid_lft 1546sec preferred_lft

1546sec inet6 fe80::20c:29ff:fe07:a5e2/64 scope link noprefixroute valid_lft forever preferred_lft forever 3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000 link/ether 52:54:00:a6:20:3b brd ff:ff:ff:ff:ff:ff inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0 valid_lft forever preferred_lft forever 4: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc fq_codel master virbr0 state DOWN group default qlen 1000 link/ether 52:54:00:a6:20:3b brd ff:ff:ff:ff:ff:ff 5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default link/ether 02:42:24:9a:6d:f7 brd ff:ff:ff:ff:ff:ff inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0 valid_lft forever preferred_lft forever

---

Information about my ports

Ip: Forwarding: 1 141 total packets received 1 with invalid addresses 0 forwarded 0 incoming packets discarded 95 incoming packets delivered 133 requests sent out 4 dropped because of missing route Icmp: 0 ICMP messages received 0 input ICMP message failed ICMP input histogram: 0 ICMP messages sent 0 ICMP messages failed ICMP output histogram: Tcp: 3 active connection openings 0 passive connection openings 0 failed connection attempts 0 connection resets received 0 connections established 40 segments received 42 segments sent out 0 segments retransmitted 0 bad segments received 3 resets sent Udp: 55 packets received 0 packets to unknown port received 0 packet receive errors 85 packets sent 0 receive buffer errors 0 send buffer errors UdpLite: TcpExt: 4 delayed acks sent 14 packet headers predicted 2 acknowledgments not containing data payload received 13 predicted acknowledgments TCPBacklogCoalesce: 3 TCPRcvCoalesce: 1 TCPAutoCorking: 1 TCPOrigDataSent: 18 TCPDelivered: 21 IpExt: InMcastPkts: 52 OutMcastPkts: 51 InBcastPkts: 8 InOctets: 27672 OutOctets: 12084 InMcastOctets: 5090 OutMcastOctets: 4767 InBcastOctets: 576 InNoECTPkts: 144 MPTcpExt:

Hostname

localhost.localdomain

Dns Name

; <<>> DiG 9.11.26-RedHat-9.11.26-6.el8 <<>> ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32523 ;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13 ;; QUESTION SECTION: ;. IN NS ;; ANSWER SECTION: . 5 IN NS d.root-servers.net. . 5 IN NS e.root-servers.net. . 5 IN NS f.root-servers.net. . 5 IN NS g.root-servers.net. . 5 IN NS h.root-servers.net. . 5 IN NS a.root-servers.net. . 5 IN NS

i.root-servers.net. . 5 IN NS j.root-servers.net. . 5 IN NS k.root-servers.net. . 5 IN NS l.root-servers.net. . 5 IN NS m.root-servers.net. . 5 IN NS b.root-servers.net. . 5 IN NS c.root-servers.net. ;; ADDITIONAL SECTION: m.root-servers.net. 5 IN A 202.12.27.33 m.root-servers.net. 5 IN AAAA 2001:dc3::35 b.root-servers.net. 5 IN A 199.9.14.201 b.root-servers.net. 5 IN AAAA 2001:500:200::b c.root-servers.net. 5 IN A 192.33.4.12 c.root-servers.net. 5 IN AAAA 2001:500:2::c d.root-servers.net. 5 IN A 199.7.91.13 d.root-servers.net. 5 IN AAAA 2001:500:2d::d e.root-servers.net. 5 IN A 192.203.230.10 e.root-servers.net. 5 IN AAAA 2001:500:a8::e f.root-servers.net. 5 IN A 192.5.5.241 f.root-servers.net. 5 IN AAAA 2001:500:2f::f g.root-servers.net. 5 IN A 192.112.36.4 ;; Query time: 20 msec ;; SERVER: 192.168.44.2#53(192.168.44.2) ;; WHEN: Sun Dec 12 03:58:30 EST 2021 ;; MSG SIZE rcvd: 508

Running Process

(Not all processes could be identified, non-owned process info

will not be shown, you would have to be root to see it all.)

Active Internet connections (only servers) Proto Recv-Q Send-Q Local Address Foreign Address State User Inode PID/Program name tcp 0 0 192.168.122.1:53 0.0.0.0:* LISTEN 0 46264 - tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 0 36593 - tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN 0 34802 - tcp 0 0 0.0.0.0:111 0.0.0.0:* LISTEN 0 23660 - tcp6 0 0 :::22 :::* LISTEN 0 36595 - tcp6 0 0 ::1:631 :::* LISTEN 0 34801 - tcp6 0 0 :::111 :::* LISTEN 0 23662 - udp 0 0 0.0.0.0:5353 0.0.0.0:* 70 34217 - udp 0 0 127.0.0.1:323 0.0.0.0:* 0 29640 - udp 0 0 192.168.122.1:53 0.0.0.0:* 0 46263 - udp 0 0 0.0.0.0:67 0.0.0.0:* 0 46260 - udp 0 0 0.0.0.0:59475 0.0.0.0:* 70 34219 - udp 0 0 0.0.0.0:111 0.0.0.0:* 0 23661 - udp6 0 0 :::5353 :::* 70 34218 - udp6 0 0 ::1:323 :::* 0 29641 - udp6 0 0 :::48530 :::* 70 34220 - udp6 0 0 :::111 :::* 0 23663 -

---

Logged users, log time etc

03:58:30 up 4 min, 1 user, load average: 1.25, 1.18, 0.57 USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT asuero tty2 tty2 03:54 4:25 38.24s 0.56s /usr/libexec/tracker-miner-fs

---

Date

Sun Dec 12 03:58:30 EST 2021

[asuero@localhost ~]$

[asuero@localhost ~]$ ./mm.shSUDO

bash: ./mm.shSUDO: No such file or directory

[asuero@localhost ~]$ sudo ./mm.sh

[sudo] password for asuero:

Bash Script that dump my network information

Ip Address.

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever preferred_lft forever 2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000 link/ether 00:0c:29:07:a5:e2 brd ff:ff:ff:ff:ff:ff inet 192.168.44.128/24 brd 192.168.44.255 scope global dynamic noprefixroute ens33 valid_lft 1515sec preferred_lft 1515sec inet6 fe80::20c:29ff:fe07:a5e2/64 scope link noprefixroute valid_lft forever preferred_lft forever 3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000 link/ether 52:54:00:a6:20:3b brd ff:ff:ff:ff:ff:ff inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0 valid_lft forever preferred_lft forever 4: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc fq_codel master virbr0 state DOWN group default qlen 1000 link/ether 52:54:00:a6:20:3b brd ff:ff:ff:ff:ff:ff 5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default link/ether 02:42:24:9a:6d:f7 brd ff:ff:ff:ff:ff:ff inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0 valid_lft forever preferred_lft forever

---

Information about my ports

Ip: Forwarding: 1 151 total packets received 1 with invalid addresses 0 forwarded 0 incoming packets discarded 102 incoming packets delivered 142 requests sent out 4 dropped because of missing route Icmp: 0 ICMP messages received 0 input ICMP message failed ICMP input histogram: 0 ICMP messages sent 0 ICMP messages failed ICMP output histogram: Tcp: 3 active connection openings 0 passive connection openings 0 failed connection attempts 0 connection resets received 0 connections established 40 segments received 42 segments sent out 0 segments retransmitted 0 bad segments received 3 resets sent Udp: 62 packets received 0 packets to unknown port received 0 packet receive errors 94 packets sent 0 receive buffer errors 0 send buffer errors UdpLite: TcpExt: 4 delayed acks sent 14 packet headers predicted 2 acknowledgments not containing data payload received 13 predicted acknowledgments TCPBacklogCoalesce: 3 TCPRcvCoalesce: 1 TCPAutoCorking: 1 TCPOrigDataSent: 18 TCPDelivered: 21 IpExt: InMcastPkts: 55 OutMcastPkts: 54 InBcastPkts: 9 InOctets: 28814

OutOctets: 12686 InMcastOctets: 5291 OutMcastOctets: 4968 InBcastOctets: 648 InNoECTPkts: 154 MPTcpExt:

Hostname

localhost.localdomain

Dns Name

; <<>> DiG 9.11.26-RedHat-9.11.26-6.el8 <<>> ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58365 ;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13 ;; QUESTION SECTION: ;. IN NS ;; ANSWER SECTION: . 5 IN NS j.root-servers.net. . 5 IN NS k.root-servers.net. . 5 IN NS l.root-servers.net. . 5 IN NS m.root-servers.net. . 5 IN NS b.root-servers.net. . 5 IN NS c.root-servers.net. . 5 IN NS d.root-servers.net. . 5 IN NS e.root-servers.net. . 5 IN NS f.root-servers.net. . 5 IN NS g.root-servers.net. . 5 IN NS h.root-servers.net. . 5 IN NS a.root-servers.net. . 5 IN NS i.root-servers.net. ;; ADDITIONAL SECTION: m.root-servers.net. 5 IN A 202.12.27.33 m.root-servers.net. 5 IN AAAA 2001:dc3::35 b.root-servers.net. 5 IN A 199.9.14.201 b.root-servers.net. 5 IN AAAA 2001:500:200::b c.root-servers.net. 5 IN A 192.33.4.12 c.root-servers.net. 5 IN AAAA 2001:500:2::c d.root-servers.net. 5 IN A 199.7.91.13 d.root-servers.net. 5 IN AAAA 2001:500:2d::d e.root-servers.net. 5 IN A 192.203.230.10 e.root-servers.net. 5 IN AAAA 2001:500:a8::e f.root-servers.net. 5 IN A 192.5.5.241 f.root-servers.net. 5 IN AAAA 2001:500:2f::f g.root-servers.net. 5 IN A 192.112.36.4 ;; Query time: 20 msec ;; SERVER: 192.168.44.2#53(192.168.44.2) ;; WHEN: Sun Dec 12 03:59:00 EST 2021 ;; MSG SIZE rcvd: 508

Running Process

Active Internet connections (only servers) Proto Recv-Q Send-Q Local Address Foreign Address State User Inode PID/Program name tcp 0 0 192.168.122.1:53 0.0.0.0:* LISTEN 0 46264 1689/dnsmasq tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 0 36593 1147/sshd tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN 0 34802 1140/cupsd tcp 0 0 0.0.0.0:111 0.0.0.0:* LISTEN 0 23660 1/systemd tcp6 0 0 :::22 :::* LISTEN 0 36595 1147/sshd tcp6 0 0 ::1:631 :::* LISTEN 0 34801 1140/cupsd tcp6 0 0 :::111 :::* LISTEN 0 23662 1/systemd udp 0 0 0.0.0.0:5353 0.0.0.0:* 70 34217 965/avahi-daemon: r udp 0 0 127.0.0.1:323 0.0.0.0:* 0 29640 951/chronyd udp 0 0 192.168.122.1:53 0.0.0.0:* 0 46263 1689/dnsmasq udp 0 0 0.0.0.0:67 0.0.0.0:* 0 46260 1689/dnsmasq udp 0 0 0.0.0.0:59475 0.0.0.0:* 70 34219 965/avahi-daemon: r udp 0 0 0.0.0.0:111 0.0.0.0:* 0 23661 1/systemd udp6 0 0 :::5353 :::* 70 34218 965/avahi-daemon: r

udp6 0 0 ::1:323 :::* 0 29641 951/chronyd udp6 0 0 :::48530 :::* 70 34220 965/avahi-daemon: r udp6 0 0 :::111 :::* 0 23663 1/systemd

---

Logged users, log time etc

03:59:00 up 5 min, 1 user, load average: 1.03, 1.13, 0.57 USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT asuero tty2 tty2 03:54 4:55 42.93s 0.56s /usr/libexec/tracker-miner-fs

---

Date

Sun Dec 12 03:59:00 EST 2021

Debian Server.

Current network configuration

- **System Ip address, and interfaces.**

br-3d1beedbc6f1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500

inet 192.168.49.1 netmask 255.255.255.0 broadcast 192.168.49.255

ether 02:42:9b:58:be:5e txqueuelen 0 (Ethernet)

RX packets 0 bytes 0 (0.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 0 bytes 0 (0.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500

inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255

```
        ether 02:42:b9:34:2f:95  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.44.130  netmask 255.255.255.0  broadcast 192.168.44.255
        inet6 fe80::20c:29ff:feef:c491  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ef:c4:91  txqueuelen 1000  (Ethernet)
        RX packets 319  bytes 106844 (104.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 185  bytes 19285 (18.8 KiB)
        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 50  bytes 3974 (3.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 50  bytes 3974 (3.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- **Route table**

Destination Gateway Genmask Flags Metric Ref Use Iface

default _gateway 0.0.0.0 UG 100 0 0 ens33

172.17.0.0 0.0.0.0 255.255.0.0 U 0 0 0 docker0

192.168.44.0 0.0.0.0 255.255.255.0 U 100 0 0 ens33

192.168.49.0 0.0.0.0 255.255.255.0 U 0 0 0 br-3d1beedbc6f1

- **Domain name**

Debian.alce

- **Current Users and load average**

03:15:54 up 15 min, 1 user, load average: 1.50, 0.92, 0.54

USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT

arsenias tty2 tty2 03:03 15:02 0.06s 0.05s /usr/libexec/gnome-session-binary –systemd

- **Open Ports**

tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 510/sshd: /usr/sbin

tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN 985/exim4

tcp6 0 0 :::22 :::* LISTEN 510/sshd: /usr/sbin

tcp6 0 0 ::1:25 :::* LISTEN 985/exim4

What is installed?

2021-12-01 21:47:29 install snapd:amd64 <none> 2.49-1+b5

2021-12-08 14:03:05 install curl:amd64 <none> 7.74.0-1.3+b1
2021-12-08 14:28:33 install conntrack:amd64 <none> 1:1.4.6-2
2021-12-08 14:28:33 install cri-tools:amd64 <none> 1.19.0-00
2021-12-08 19:06:39 install docker-ce:amd64 <none> 5:20.10.11~3-0~debian-buster
2021-12-08 19:06:42 install docker-ce-rootless-extras:amd64 <none> 5:20.10.11~3-0~debian-buster
2021-12-08 19:06:43 install docker-scan-plugin:amd64 <none> 0.9.0~debian-buster
2021-12-08 19:06:44 install libslirp0:amd64 <none> 4.4.0-1+deb11u2
2021-12-08 19:06:44 install slirp4netns:amd64 <none> 1.0.1-2
2021-12-08 19:47:38 install uidmap:amd64 <none> 1:4.8.1-1
2021-12-08 23:10:55 install python3-cffi-backend:amd64 <none> 1.14.5-1
2021-12-08 23:10:55 install python3-cryptography:amd64 <none> 3.3.2-1
2021-12-08 23:10:55 install python3-jinja2:all <none> 2.11.3-1
2021-12-08 23:10:55 install python3-pyparsing:all <none> 2.4.7-1
2021-12-08 23:10:55 install python3-packaging:all <none> 20.9-2
2021-12-08 23:10:55 install python3-yaml:amd64 <none> 5.3.1-5
2021-12-08 23:10:56 install python3-pycryptodome:amd64 <none> 3.9.7+dfsg1-1+b2
2021-12-08 23:10:57 install python3-lib2to3:all <none> 3.9.2-1
2021-12-08 23:10:57 install python3-distutils:all <none> 3.9.2-1
2021-12-08 23:10:57 install python3-dnspython:all <none> 2.0.0-1
2021-12-08 23:10:57 install ieee-data:all <none> 20210605.1
2021-12-08 23:10:57 install python3-netaddr:all <none> 0.7.19-5
2021-12-08 23:10:57 install ansible:all <none> 2.10.7+merged+base+2.10.8+dfsg-1
2021-12-08 23:11:06 install python3-argcomplete:all <none> 1.8.1-1.5
2021-12-08 23:11:06 install python3-jmespath:all <none> 0.10.0-1
2021-12-08 23:11:06 install python3-kerberos:amd64 <none> 1.1.14-3.1+b3
2021-12-08 23:11:06 install python3-lockfile:all <none> 1:0.12.2-2.2
2021-12-08 23:11:06 install python3-simplejson:amd64 <none> 3.17.2-1
2021-12-08 23:11:06 install python3-libcloud:all <none> 3.2.0-2
2021-12-08 23:11:07 install python3-ntlm-auth:all <none> 1.4.0-1
2021-12-08 23:11:07 install python3-requests-kerberos:all <none> 0.12.0-2
2021-12-08 23:11:07 install python3-requests-ntlm:all <none> 1.1.0-1.1
2021-12-08 23:11:07 install python3-requests-toolbelt:all <none> 0.9.1-1
2021-12-08 23:11:07 install python3-selinux:amd64 <none> 3.1-3
2021-12-08 23:11:07 install python3-xmltodict:all <none> 0.12.0-2
2021-12-08 23:11:07 install python3-winrm:all <none> 0.3.0-2
2021-12-08 23:14:53 install binutils-common:amd64 <none> 2.35.2-2
2021-12-08 23:14:53 install libbinutils:amd64 <none> 2.35.2-2
2021-12-08 23:14:53 install libctf-nobfd0:amd64 <none> 2.35.2-2
2021-12-08 23:14:53 install libctf0:amd64 <none> 2.35.2-2
2021-12-08 23:14:53 install binutils-x86-64-linux-gnu:amd64 <none> 2.35.2-2
2021-12-08 23:14:53 install binutils:amd64 <none> 2.35.2-2
2021-12-08 23:14:53 install libc-dev-bin:amd64 <none> 2.31-13+deb11u2
2021-12-08 23:14:53 install linux-libc-dev:amd64 <none> 5.10.70-1
2021-12-08 23:14:54 install libcrypt-dev:amd64 <none> 1:4.4.18-4

2021-12-08 23:14:54 install libtirpc-dev:amd64 <none> 1.3.1-1
2021-12-08 23:14:54 install libnsl-dev:amd64 <none> 1.3.0-2
2021-12-08 23:14:54 install libc6-dev:amd64 <none> 2.31-13+deb11u2
2021-12-08 23:14:54 install libcc1-0:amd64 <none> 10.2.1-6
2021-12-08 23:14:54 install libitm1:amd64 <none> 10.2.1-6
2021-12-08 23:14:54 install libatomic1:amd64 <none> 10.2.1-6
2021-12-08 23:14:54 install libasan6:amd64 <none> 10.2.1-6
2021-12-08 23:14:55 install liblsan0:amd64 <none> 10.2.1-6
2021-12-08 23:14:55 install libtsan0:amd64 <none> 10.2.1-6
2021-12-08 23:14:55 install libubsan1:amd64 <none> 10.2.1-6
2021-12-08 23:14:55 install libgcc-10-dev:amd64 <none> 10.2.1-6
2021-12-08 23:14:55 install gcc-10:amd64 <none> 10.2.1-6
2021-12-08 23:14:57 install gcc:amd64 <none> 4:10.2.1-1
2021-12-08 23:14:57 install libstdc++-10-dev:amd64 <none> 10.2.1-6

- **Last update of the apps:** **12/10/2021**
- **No Changes to the default network**

Executed Script Sample.

Bash Script that dump my network information

Ip Address.

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever preferred_lft forever 2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000 link/ether 00:0c:29:ef:c4:91 brd ff:ff:ff:ff:ff:ff altname enp2s1 inet 192.168.44.130/24 brd 192.168.44.255 scope global dynamic noprefixroute ens33 valid_lft 960sec preferred_lft 960sec inet6 fe80::20c:29ff:feef:c491/64 scope link noprefixroute valid_lft forever preferred_lft forever 3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default link/ether 02:42:0b:98:ee:ab brd ff:ff:ff:ff:ff:ff inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0 valid_lft forever preferred_lft forever 4: br-3d1beedbc6f1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default link/ether 02:42:5b:1f:02:74 brd ff:ff:ff:ff:ff:ff inet 192.168.49.1/24 brd 192.168.49.255 scope global br-3d1beedbc6f1 valid_lft forever preferred_lft forever

---

Information about my ports

Ip: Forwarding: 1 4260 total packets received 1 with invalid addresses 0 forwarded 0 incoming packets discarded 4257 incoming packets delivered 3897 requests sent out 40 dropped because of missing route Icmp: 0 ICMP messages received 0 input ICMP message failed ICMP input histogram: 0 ICMP messages sent 0 ICMP messages failed ICMP output histogram: Tcp: 97 active connection openings 0 passive connection openings 14 failed connection attempts 0 connection resets received 18 connections established 3467 segments received 3275 segments sent out 0 segments retransmitted 0 bad segments received 35 resets sent Udp: 763 packets received 0 packets to unknown port received 0 packet receive errors 746 packets sent 0 receive buffer errors 0 send buffer errors IgnoredMulti: 37 UdpLite: TcpExt: 45 TCP sockets finished time wait in fast timer 55 delayed acks sent 1280 packet headers predicted 290 acknowledgments not containing data payload received 1546 predicted acknowledgments TCPBacklogCoalesce: 8 TCPRcvCoalesce: 19 TCPAutoCorking: 19 TCPOrigDataSent: 1661 TCPHystartTrainDetect: 1 TCPHystartTrainCwnd: 24 TCPKeepAlive: 202 TCPDelivered: 1741 IpExt: InMcastPkts: 117 OutMcastPkts: 98 InBcastPkts: 37 OutBcastPkts: 9 InOctets: 2727094 OutOctets: 701564 InMcastOctets: 14237 OutMcastOctets: 11930 InBcastOctets: 2718 OutBcastOctets: 702 InNoECTPkts: 5321

Hostname

Debian.alce

Dns Name

; <<>> DiG 9.16.22-Debian <<>> ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51559 ;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13 ;; QUESTION SECTION: ;. IN NS ;; ANSWER SECTION: . 5 IN NS h.root-servers.net. . 5 IN NS a.root-servers.net. . 5 IN NS i.root-servers.net. . 5 IN NS j.root-servers.net. . 5 IN NS k.root-servers.net. . 5 IN NS l.root-servers.net. . 5 IN NS m.root-servers.net. . 5 IN NS b.root-servers.net. . 5 IN NS c.root-servers.net. . 5 IN NS d.root-servers.net. . 5 IN NS e.root-servers.net. . 5 IN NS f.root-servers.net. . 5 IN NS g.root-servers.net. ;; ADDITIONAL SECTION: m.root-servers.net. 5 IN A 202.12.27.33 m.root-servers.net. 5 IN AAAA 2001:dc3::35 b.root-servers.net. 5 IN A 199.9.14.201 b.root-servers.net. 5 IN AAAA 2001:500:200::b c.root-servers.net. 5 IN A 192.33.4.12 c.root-servers.net. 5 IN AAAA 2001:500:2::c d.root-servers.net. 5 IN A 199.7.91.13 d.root-servers.net. 5 IN AAAA 2001:500:2d::d e.root-servers.net. 5 IN A 192.203.230.10 e.root-servers.net. 5 IN AAAA 2001:500:a8::e f.root-servers.net. 5 IN A 192.5.5.241 f.root-servers.net. 5 IN AAAA 2001:500:2f::f g.root-servers.net. 5 IN A 192.112.36.4 ;; Query time: 32 msec ;; SERVER: 192.168.44.2#53(192.168.44.2) ;; WHEN: Sun Dec 12 03:47:17 EST 2021 ;; MSG SIZE rcvd: 508

Running Process

Active Internet connections (only servers) Proto Recv-Q Send-Q Local Address Foreign Address State User Inode PID/Program name tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 0 24657 505/sshd: /usr/sbin tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN 0 26252 1073/exim4 tcp6 0 0 :::22 :::* LISTEN 0 24659 505/sshd: /usr/sbin tcp6 0 0 ::1:25 :::* LISTEN 0 26253 1073/exim4 udp 0 0 0.0.0.0:48931 0.0.0.0:* 109 23484 433/avahi-daemon: r udp 0 0 0.0.0.0:5353 0.0.0.0:* 109 23482 433/avahi-daemon: r udp6 0 0 :::46947 :::* 109 23485 433/avahi-daemon: r udp6 0 0 :::5353 :::* 109 23483 433/avahi-daemon: r

----

Logged users, log time etc

03:47:17 up 14 min, 1 user, load average: 0.20, 0.23, 0.19 USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT arsenias tty2 tty2 03:33 14:01 0.02s 0.02s /usr/libexec/gnome-session-binary --systemd

---

Date

Sun 12 Dec 2021 03:47:17 AM EST

Steps to run the script

-To **run** the **script**, you must have the root privileges, if you run the script without having the root privileges you won't be able to see all the information.

-This script saves the file in my directory

At least one page of research on what you've chosen to add to your script and why. Remember to cite your sources and explain why you think these additions are valuable. Sources do not count towards the one page.

Ip address:

- I used this command to show my Ip address and my network configuration.
- It is important to see important configuration of my network.

Dig

- Dig (Domain Information Groper) is a command use to verify if our dns is working properly
- dig is a flexible tool for interrogating DNS name servers.
- I used it to see all the information of my dns.

Netstat -s

- It provides the connections, package received, the failed connection. I considered this command important to be on my script to keep tracking of the package.
- So, in that way we can see all the numbers of lost packages and the successful ones.

Netstat -tulpen

Netstat -tulpen is used to see the active process. When we can see the running process in our system we can check if there is something wrong, if there is a suspicious processes running in the system.

Date

I used this on my script to print the date of the system.

Sources:

https://www.cyberciti.biz/faq/linux-find-out-which-port-is-open-using-the-command-line/
https://www.fosslinux.com/42935/linux-networking-commands.htm
https://www.fosslinux.com/42935/linux-networking-commands.htm

A link to your GitHub where your script has been uploaded

https://github.com/elimelec19/Portafolio/blob/main/Network_inf_Script.sh