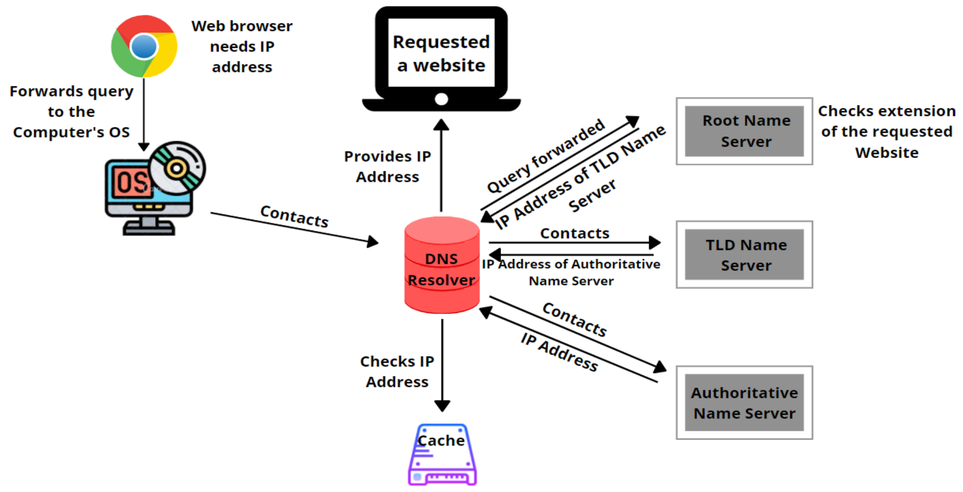
DNS CONFIGURATION

DNS SERVER:

A DNS server is a computer that translates human-readable domain names (like www.google.com) into the numerical IP addresses that computers use to communicate on the internet.

WORKING:

- When we type a website like www.google.com in our browser, our computer tries to find the IP address.
- First, it checks the local cache (our browser, operating system, or router) to see if it already knows the IP address.
- If the local cache doesn't have the IP, the query is sent to a DNS resolver to find it.
- The DNS recursor (also referred to as the DNS resolver) is a server that receives the query from the DNS client, and then interacts with other DNS servers to hunt down the correct IP. Once the resolver receives the request from the client, the resolver then actually behaves as a client itself, querying the other three types of DNS servers in search of the right IP.
- Resolver sends the query to a Root DNS server, which doesn't know the exact IP address. The root server then responds to the resolver with the address of a top-level domain (TLD) DNS server (such as .com or .net) that stores the information for its domains .(e.g., .com server for this example).
- TLD server then directs the resolver to the authoritative nameserver for google.com
- Authoritative nameserver knows the exact IP address for google.com and sends it back to the resolver.
- Resolver passes the IP address to our computer.


Web browser needs IP address
Requested a website
Forwards query to the Computer's OS
OS
Provides IP Address
Contacts
Query forwarded
IP Address of TLD Name Server
Root Name Server
Checks extension of the requested Website
Contacts
IP Address of Authoritative Name Server
TLD Name Server
DNS Resolver
Contacts
IP Address
Authoritative Name Server
Checks IP Address
Cache

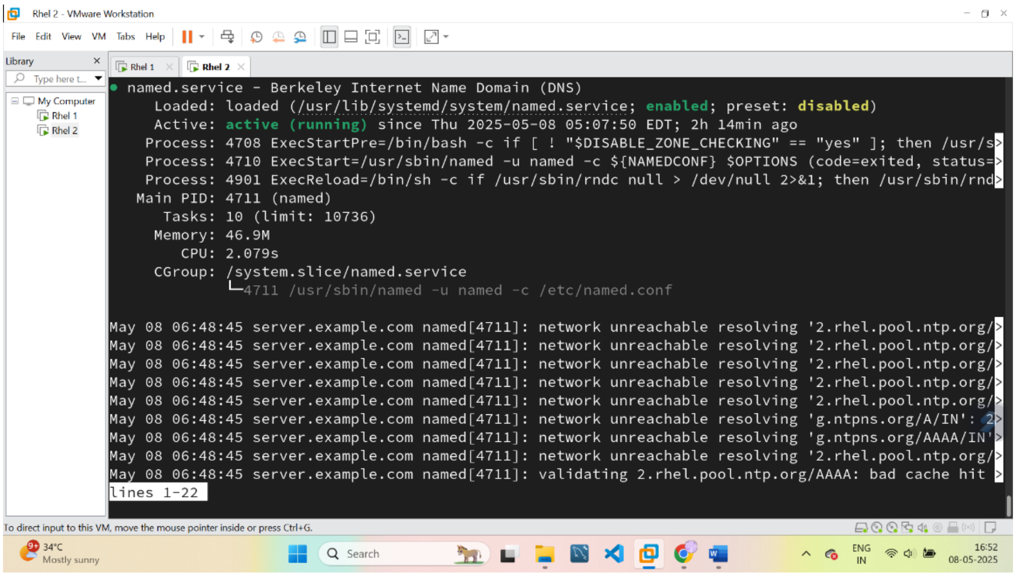
Caching:

Resolvers can also resolve DNS queries using cached data. After retrieving the correct IP address for a given website, the resolver will then store that information in its cache for a limited amount of time. During this time period, if any other clients send requests for that domain name, the resolver can skip the typical DNS lookup process and simply respond to the client with the IP address saved in the cache.

CONFIGURATION:

SERVER:

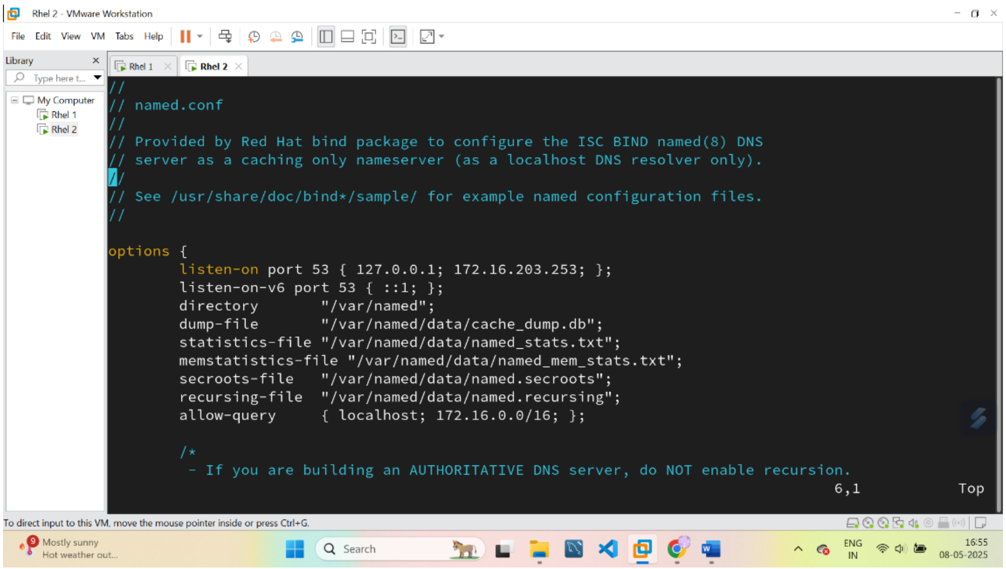
1. Install the bind and bind-utils package
   yum install bind bind-utils
2. Start and enable the service
   systemctl enable - -now named



Rhel 2 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Rhel 1
Rhel 2
Rhel 1
Rhel 2
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
34°C
Mostly sunny
Search
ENG
IN
16:52
08-05-2025

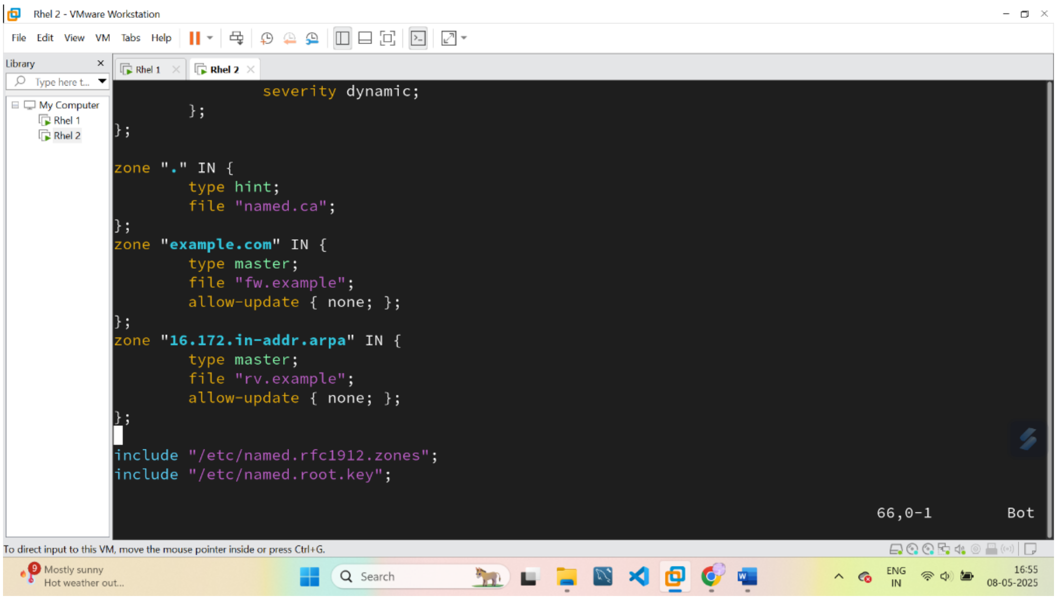
```
● named.service - Berkeley Internet Name Domain (DNS)
     Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: disabled)
     Active: active (running) since Thu 2025-05-08 05:07:50 EDT; 2h 14min ago
    Process: 4708 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then /usr/s>
    Process: 4710 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exited, status=>
    Process: 4901 ExecReload=/bin/sh -c if /usr/sbin/rndc null > /dev/null 2>&1; then /usr/sbin/rnd>
   Main PID: 4711 (named)
      Tasks: 10 (limit: 10736)
     Memory: 46.9M
        CPU: 2.079s
     CGroup: /system.slice/named.service
             └─4711 /usr/sbin/named -u named -c /etc/named.conf

May 08 06:48:45 server.example.com named[4711]: network unreachable resolving '2.rhel.pool.ntp.org/>
May 08 06:48:45 server.example.com named[4711]: network unreachable resolving '2.rhel.pool.ntp.org/>
May 08 06:48:45 server.example.com named[4711]: network unreachable resolving '2.rhel.pool.ntp.org/>
May 08 06:48:45 server.example.com named[4711]: network unreachable resolving '2.rhel.pool.ntp.org/>
May 08 06:48:45 server.example.com named[4711]: network unreachable resolving '2.rhel.pool.ntp.org/>
May 08 06:48:45 server.example.com named[4711]: network unreachable resolving 'g.ntpns.org/A/IN': 2>
May 08 06:48:45 server.example.com named[4711]: network unreachable resolving 'g.ntpns.org/AAAA/IN'>
May 08 06:48:45 server.example.com named[4711]: network unreachable resolving '2.rhel.pool.ntp.org/>
May 08 06:48:45 server.example.com named[4711]: validating 2.rhel.pool.ntp.org/AAAA: bad cache hit >
lines 1-22
```

3. Edit the /etc/named.conf file



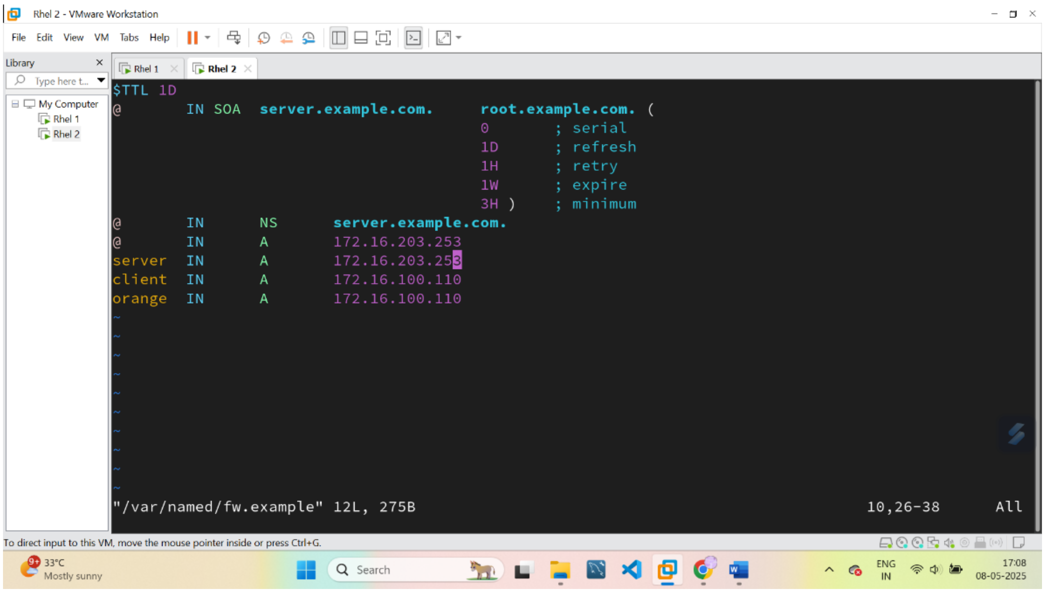
Rhel 2 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Rhel 1
Rhel 2
Rhel 1
Rhel 2
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Mostly sunny
Hot weather out...
Search
ENG
IN
16:55
08-05-2025

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
        listen-on port 53 { 127.0.0.1; 172.16.203.253; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        secroots-file   "/var/named/data/named.secroots";
        recursing-file  "/var/named/data/named.recursing";
        allow-query     { localhost; 172.16.0.0/16; };

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
                                                                    6,1           Top
```


Rhel 2 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Rhel 1
Rhel 2
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Mostly sunny
Hot weather out...
Search
ENG
IN
16:55
08-05-2025

```
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};
zone "example.com" IN {
        type master;
        file "fw.example";
        allow-update { none; };
};
zone "16.172.in-addr.arpa" IN {
        type master;
        file "rv.example";
        allow-update { none; };
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

                                                              66,0-1        Bot
```

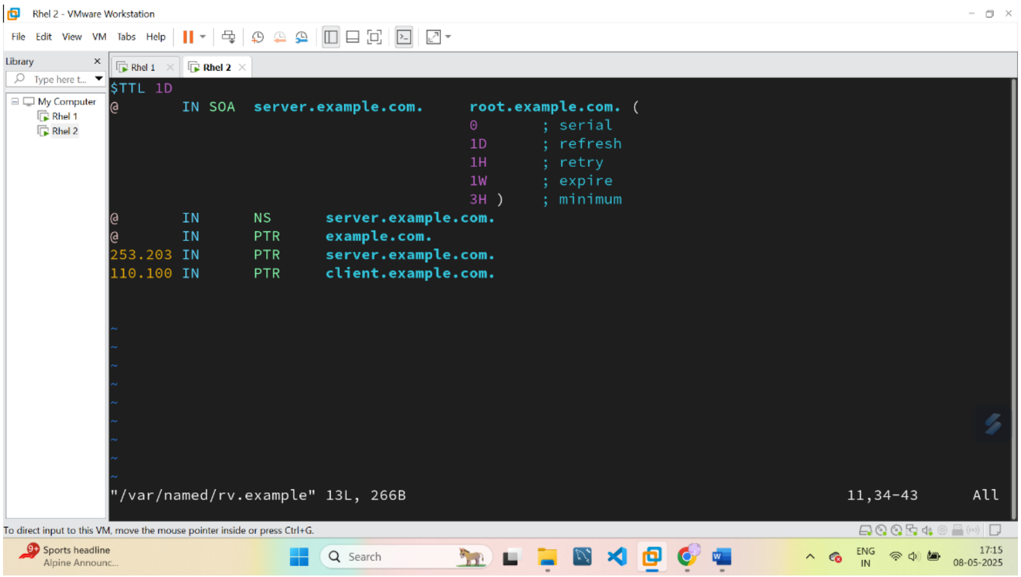
4. Create a forward zone file (maps domain names to their corresponding IP addresses) named fw.example in /var/named and add the information about the machines


Rhel 2 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Rhel 1
Rhel 2
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
33°C
Mostly sunny
Search
ENG
IN
17:08
08-05-2025

```
$TTL 1D
@       IN SOA  server.example.com.     root.example.com. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      server.example.com.
@       IN      A       172.16.203.253
server  IN      A       172.16.203.253
client  IN      A       172.16.100.110
orange  IN      A       172.16.100.110
~
~
~
~
~
~
~
~
~
~
"/var/named/fw.example" 12L, 275B                               10,26-38      All
```

- SOA (start of authority)-identifies the authoritative name server for this domain
- TTL(time to live) -determines how long DNS records should be stored in the local DNS cache before they need to be refreshed, helps improve performance by reducing the no. of requests to DNS servers
- A records map to IPv4 addresses , AAAA records map to IPv6 addresses

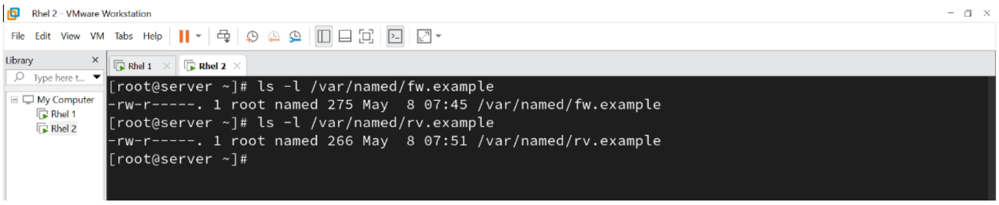
5. Create a reverse zone file (maps IP addresses to their corresponding domain names) named rv.example in /var/named


Rhel 2 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Rhel 1
Rhel 2
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Sports headline
Alpine Announc...
Search
ENG IN
17:15
08-05-2025

```
$TTL 1D
@       IN SOA  server.example.com.     root.example.com. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      server.example.com.
@       IN      PTR     example.com.
253.203 IN      PTR     server.example.com.
110.100 IN      PTR     client.example.com.


~
~
~
~
~
~
~
~
~
"/var/named/rv.example" 13L, 266B                             11,34-43      All
```

6. Change the group ownership of both /var/named/fw.example and /var/named/rv.example from root to named.

    - chown :named /var/named/fw.example
    - chown :named /var/named/rv.example



```
[root@server ~]# ls -l /var/named/fw.example
-rw-r-----. 1 root named 275 May  8 07:45 /var/named/fw.example
[root@server ~]# ls -l /var/named/rv.example
-rw-r-----. 1 root named 266 May  8 07:51 /var/named/rv.example
[root@server ~]#
```

7. Restart the named service

    systemctl restart named

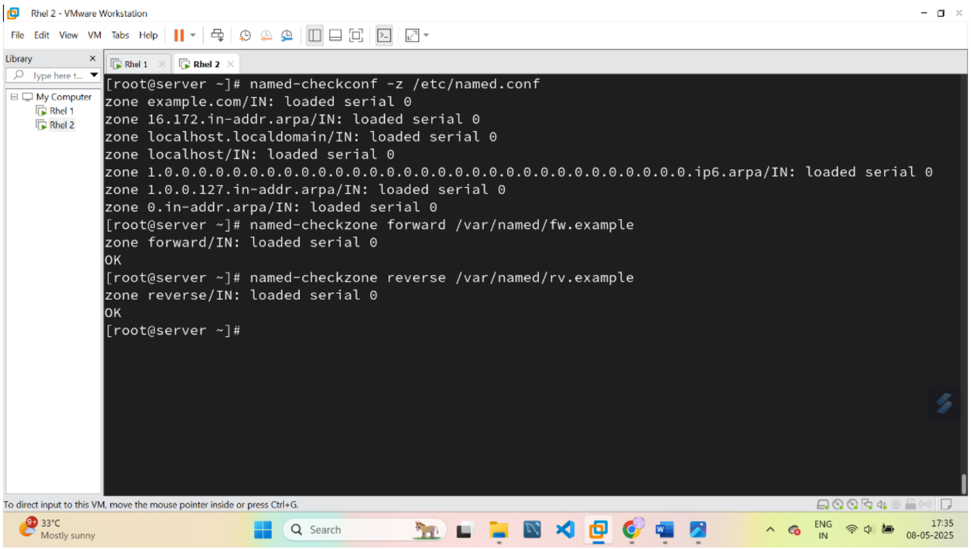
8. Add the service to firewall

    firewall-cmd - -permanent - -add-service=dns - -zone=public

    firewall-cmd - -permanent - - add-port=53/tcp

9. Check whether the changes in the configuration file are correct or not using the following commands.

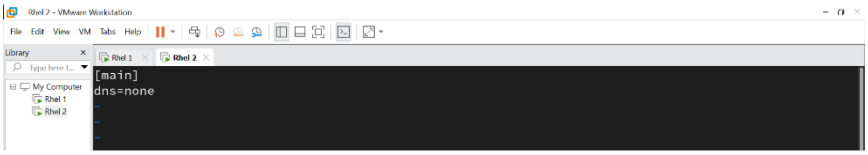
    - named-checkconf -z /etc/named.conf
    - named-checkzone forward /var/named/fw.example
    - named-checkzone reverse /var/named/rv.example


Rhel 2 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Rhel 1
Rhel 2
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
33°C
Mostly sunny
Search
ENG
IN
17:35
08-05-2025

```
[root@server ~]# named-checkconf -z /etc/named.conf
zone example.com/IN: loaded serial 0
zone 16.172.in-addr.arpa/IN: loaded serial 0
zone localhost.localdomain/IN: loaded serial 0
zone localhost/IN: loaded serial 0
zone 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa/IN: loaded serial 0
zone 1.0.0.127.in-addr.arpa/IN: loaded serial 0
zone 0.in-addr.arpa/IN: loaded serial 0
[root@server ~]# named-checkzone forward /var/named/fw.example
zone forward/IN: loaded serial 0
OK
[root@server ~]# named-checkzone reverse /var/named/rv.example
zone reverse/IN: loaded serial 0
OK
[root@server ~]#
```

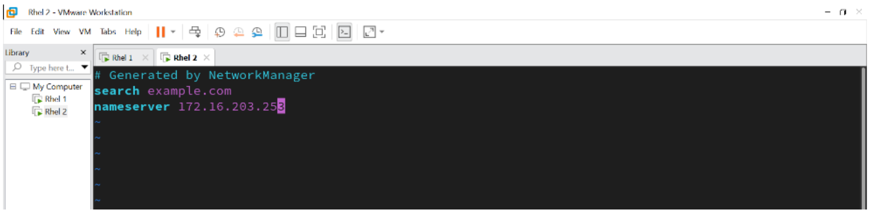
10. Disable DNS processing by NetworkManager because it dynamically updates the /etc/resolv.conf file with DNS settings from its active connection profiles. To disable this and allow manual editing of /etc/resolv.conf, create a file 90-dns-none.conf as root in the /etc/NetworkManager/conf.d/ directory

    - 90-dns-none.conf - configuration file used to prevent NetworkManager from managing DNS settings, thereby allowing you to manually configure DNS settings in the /etc/resolv.conf file without interference.



```
[main]
dns=none
~
~
~
```

11. After reload NetworkManager, it won't update /etc/resolv.conf. Now, we can manually add the nameserver's IP address to the /etc/resolv.conf



```
# Generated by NetworkManager
search example.com
nameserver 172.16.203.253
~
~
~
~
~
~
```

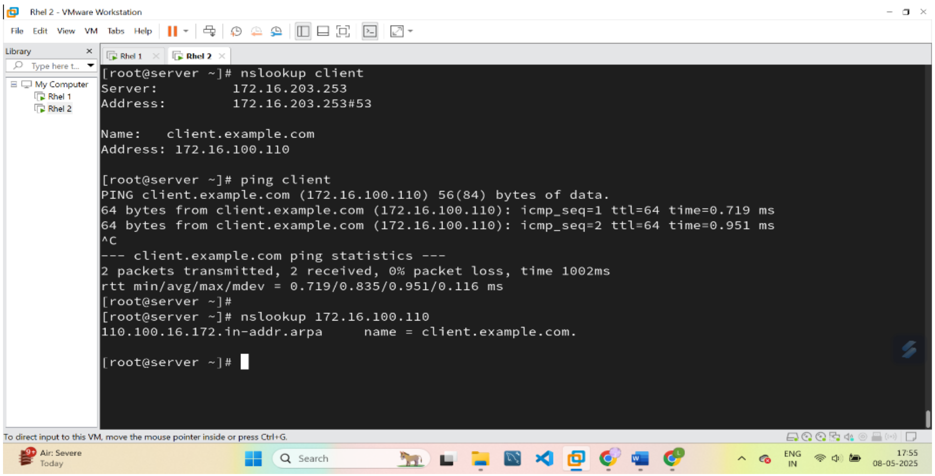
12. Verify whether DNS is working properly by using nslookup, dig, ping commands

    dig – Domain information groper -command line tool to query DNS servers

    nslookup – to query DNS servers to obtain domain name or IP address mapping

    - nslookup orange (another name for client machine)
    - nslookup client
    - nslookup 172.16.100.110
    - dig example.com

- dig orange.example.com
- dig -x 172.16.100.110 (reverse DNS lookup)



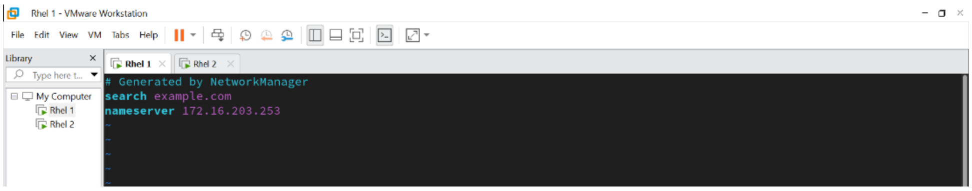
Rhel 2 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Rhel 1
Rhel 2
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Air: Severe
Today
Search
ENG
IN
17:55
08-05-2025

```
[root@server ~]# nslookup client
Server:         172.16.203.253
Address:        172.16.203.253#53

Name:   client.example.com
Address: 172.16.100.110

[root@server ~]# ping client
PING client.example.com (172.16.100.110) 56(84) bytes of data.
64 bytes from client.example.com (172.16.100.110): icmp_seq=1 ttl=64 time=0.719 ms
64 bytes from client.example.com (172.16.100.110): icmp_seq=2 ttl=64 time=0.951 ms
^C
--- client.example.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.719/0.835/0.951/0.116 ms
[root@server ~]#
[root@server ~]# nslookup 172.16.100.110
110.100.16.172.in-addr.arpa     name = client.example.com.

[root@server ~]# 
```

CLIENT :

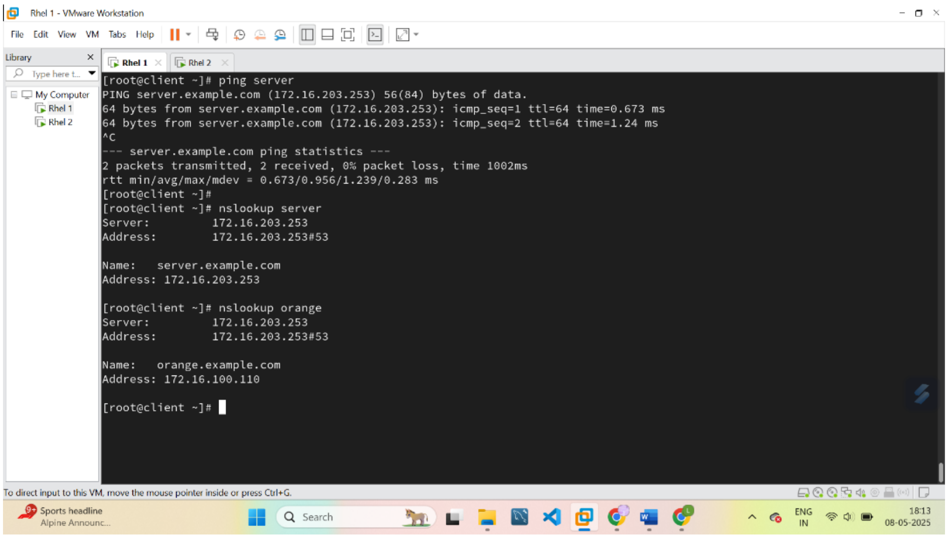
1. Disable DNS processing by NetworkManager because it dynamically updates the /etc/resolv.conf file with DNS settings from its active connection profiles. To disable this and allow manual editing of /etc/resolv.conf, create a file 90-dns-none.conf as root in the /etc/NetworkManager/conf.d/ directory

2. After reload NetworkManager, it won't update /etc/resolv.conf. Now, we can manually add the nameserver's IP address to the /etc/resolv.conf



```
# Generated by NetworkManager
search example.com
nameserver 172.16.203.253
~
~
~
~
```

3. Verify the working of DNS by nslookup, dig, ping commands



Rhel 1 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Rhel 1
Rhel 2
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Sports headline
Alpine Announc...
Search
ENG
IN
18:13
08-05-2025

```
[root@client ~]# ping server
PING server.example.com (172.16.203.253) 56(84) bytes of data.
64 bytes from server.example.com (172.16.203.253): icmp_seq=1 ttl=64 time=0.673 ms
64 bytes from server.example.com (172.16.203.253): icmp_seq=2 ttl=64 time=1.24 ms
^C
--- server.example.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.673/0.956/1.239/0.283 ms
[root@client ~]#
[root@client ~]# nslookup server
Server:         172.16.203.253
Address:        172.16.203.253#53

Name:   server.example.com
Address: 172.16.203.253

[root@client ~]# nslookup orange
Server:         172.16.203.253
Address:        172.16.203.253#53

Name:   orange.example.com
Address: 172.16.100.110

[root@client ~]# 
```