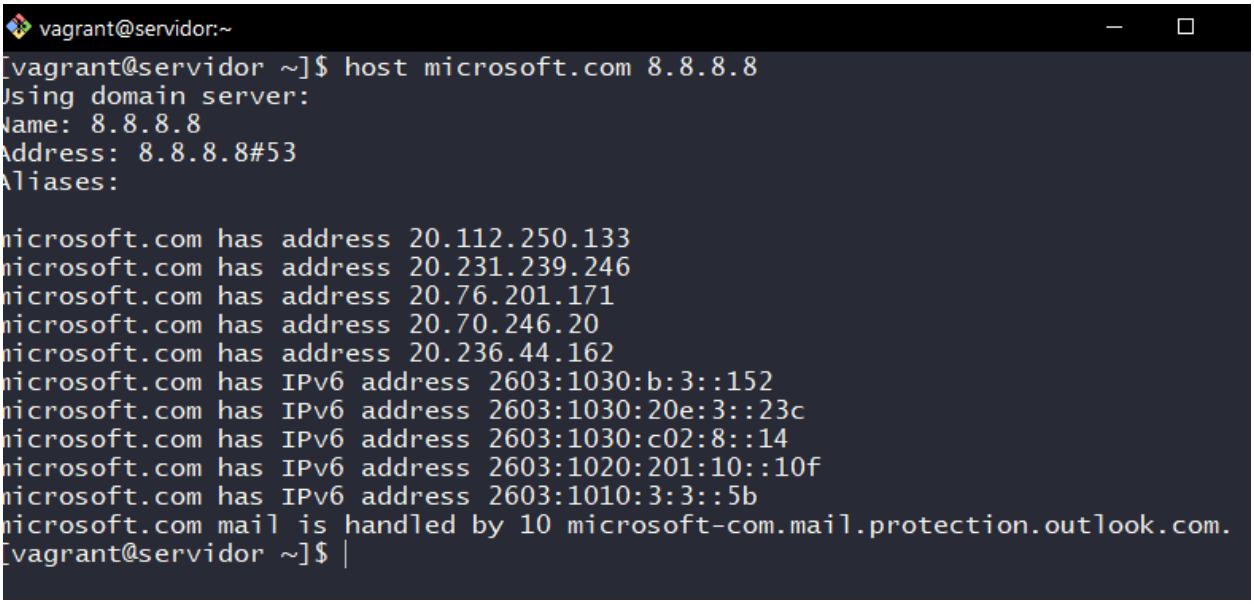
Práctica DNS
(Domain Name System)

1. **Uso de la herramienta** `host`:
   Para consultar información sobre distintos nombres de dominio:

```
host microsoft.com 8.8.8.8
host uao.edu.co 8.8.8.8
host elpais.com 8.8.8.8
```



```
[vagrant@servidor ~]$ host uao.edu.co 8.8.8.8
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

uao.edu.co has address 104.26.9.14
uao.edu.co has address 172.67.73.231
uao.edu.co has address 104.26.8.14
uao.edu.co has IPv6 address 2606:4700:20::681a:80e
uao.edu.co has IPv6 address 2606:4700:20::681a:90e
uao.edu.co has IPv6 address 2606:4700:20::ac43:49e7
uao.edu.co mail is handled by 1 aspmx.l.google.com.
uao.edu.co mail is handled by 10 alt3.aspmx.l.google.com.
uao.edu.co mail is handled by 20 alt4.aspmx.l.google.com.
uao.edu.co mail is handled by 5 alt1.aspmx.l.google.com.
uao.edu.co mail is handled by 5 alt2.aspmx.l.google.com.
[vagrant@servidor ~]$
```

```
[vagrant@servidor ~]$ host elpais.com 8.8.8.8
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

elpais.com has address 95.101.29.59
elpais.com has address 95.101.29.96
elpais.com has IPv6 address 2600:1419:5600:8::213:acc5
elpais.com has IPv6 address 2600:1419:5600:8::213:acc6
elpais.com mail is handled by 10 mail01.edicioneselpais.net.
elpais.com mail is handled by 20 mail02.edicioneselpais.net.
[vagrant@servidor ~]$
```

Para determinar la dirección IP de los servidores de correo de **www.uao.edu.co**:

```
host -t MX uao.edu.co 8.8.8.8
```

```
vagrant@servidor:~
[vagrant@servidor ~]$ host -t MX uao.edu.co 8.8.8.8
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

uao.edu.co mail is handled by 1 aspmx.l.google.com.
uao.edu.co mail is handled by 10 alt3.aspmx.l.google.com.
uao.edu.co mail is handled by 20 alt4.aspmx.l.google.com.
uao.edu.co mail is handled by 5 alt1.aspmx.l.google.com.
uao.edu.co mail is handled by 5 alt2.aspmx.l.google.com.
[vagrant@servidor ~]$
```

2.

dig @8.8.8.8 microsoft.com

```
vagrant@servidor:~

 <<>> DiG 9.16.23-RH <<>> @8.8.8.8 microsoft.com
 (1 server found)
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26191
; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
 EDNS: version: 0, flags:; udp: 512
; QUESTION SECTION:
microsoft.com.                 IN      A

; ANSWER SECTION:
microsoft.com.          1803    IN      A       20.112.250.133
microsoft.com.          1803    IN      A       20.231.239.246
microsoft.com.          1803    IN      A       20.76.201.171
microsoft.com.          1803    IN      A       20.70.246.20
microsoft.com.          1803    IN      A       20.236.44.162

; Query time: 84 msec
; SERVER: 8.8.8.8#53(8.8.8.8)
; WHEN: Tue Aug 15 21:42:03 UTC 2023
; MSG SIZE  rcvd: 122
```

`dig @8.8.8.8 uao.edu.co MX`

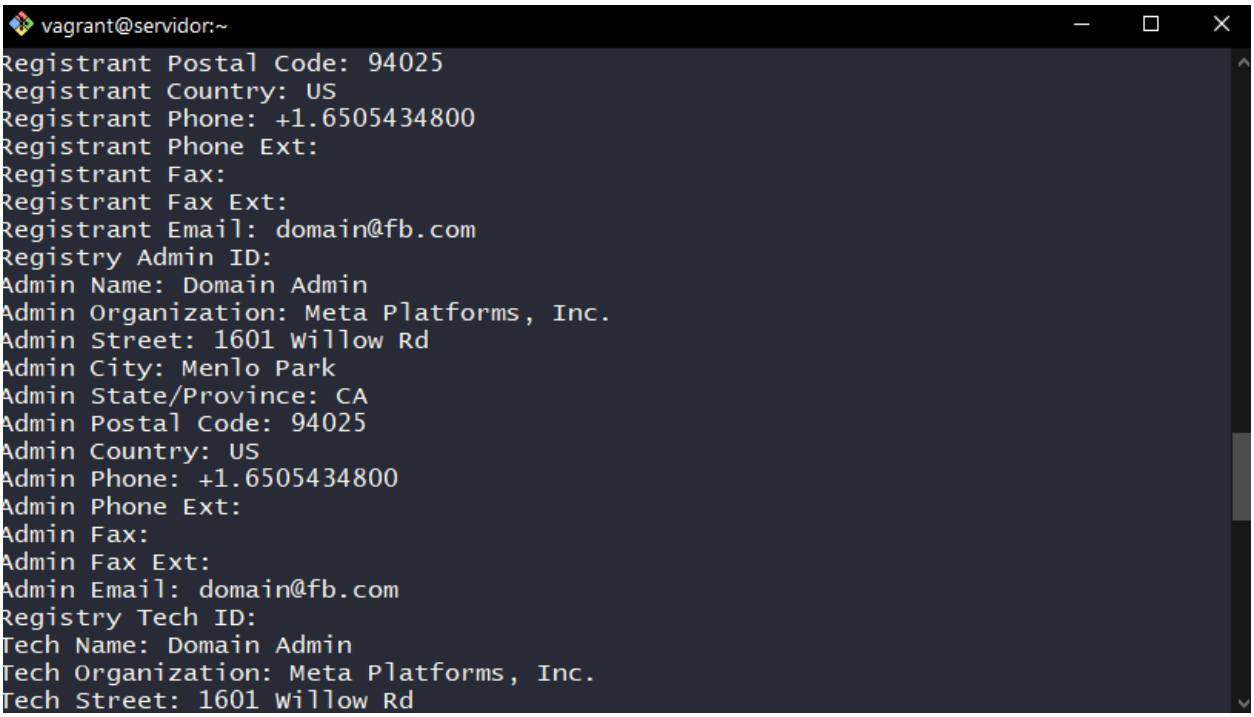
```
vagrant@servidor:~

[vagrant@servidor ~]$ dig @8.8.8.8 uao.edu.co MX

; <<>> DiG 9.16.23-RH <<>> @8.8.8.8 uao.edu.co MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17551
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;uao.edu.co.                    IN      MX

;; ANSWER SECTION:
uao.edu.co.             300     IN      MX      1 aspmx.l.google.com.
uao.edu.co.             300     IN      MX      10 alt3.aspmx.l.google.com.
uao.edu.co.             300     IN      MX      20 alt4.aspmx.l.google.com.
uao.edu.co.             300     IN      MX      5 alt1.aspmx.l.google.com.
uao.edu.co.             300     IN      MX      5 alt2.aspmx.l.google.com.

;; Query time: 102 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
```

3. Para obtener información administrativa:

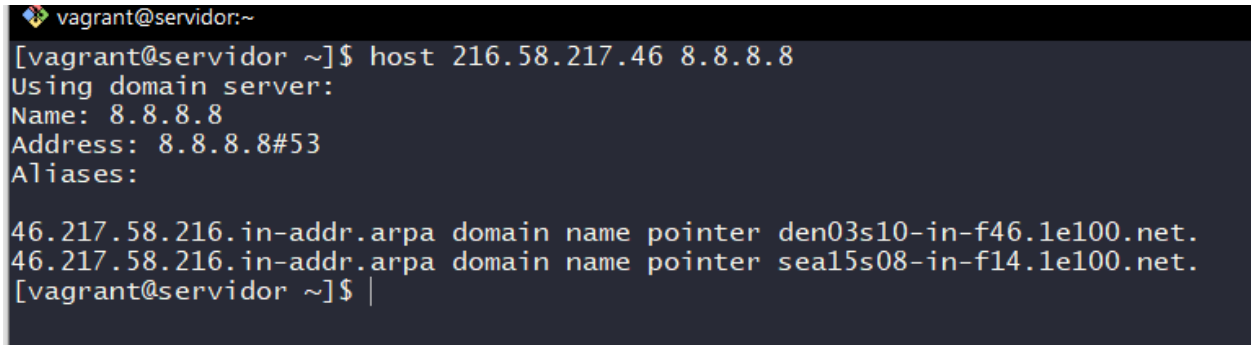
`whois google.com`

```
vagrant@servidor:~
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdatePro
hibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransfe
rProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeletePro
hibited)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/w
hois/google.com
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/
google.com
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/g
oogle.com
Name Server: ns3.google.com
Name Server: ns1.google.com
Name Server: ns2.google.com
```

`whois facebook.com`



4. Para obtener el nombre del host correspondiente a partir de una dirección IP:



El sistema DNS tiene un dominio especial `.in-addr.arpa` para estas consultas inversas.

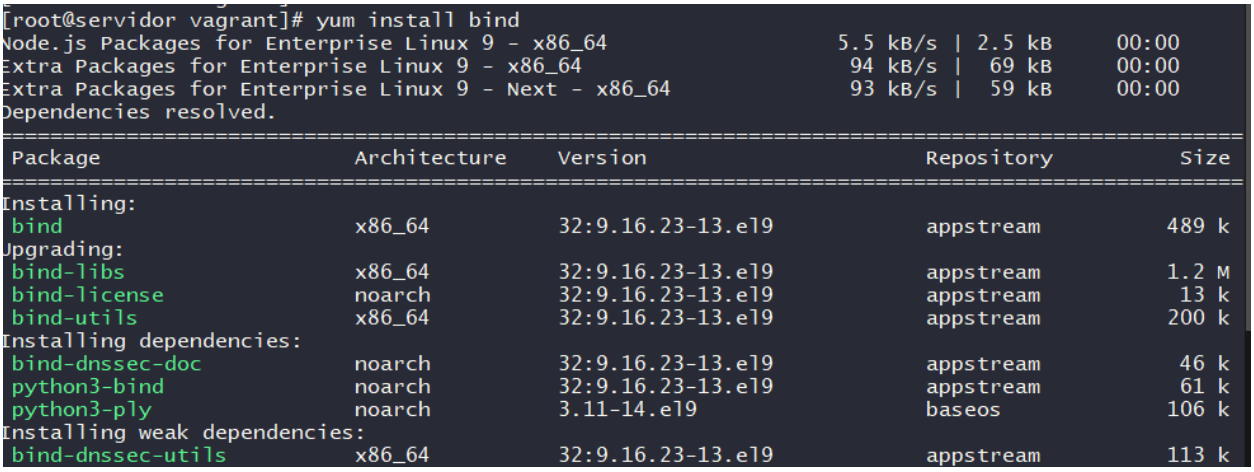
5. **Investigación sobre `nslookup`**:
   `nslookup` es similar a `dig` y `host` pero funciona en modo interactivo. Al ingresar `nslookup` en la línea de comandos sin argumentos, se entra en el modo interactivo, donde se pueden realizar múltiples consultas.

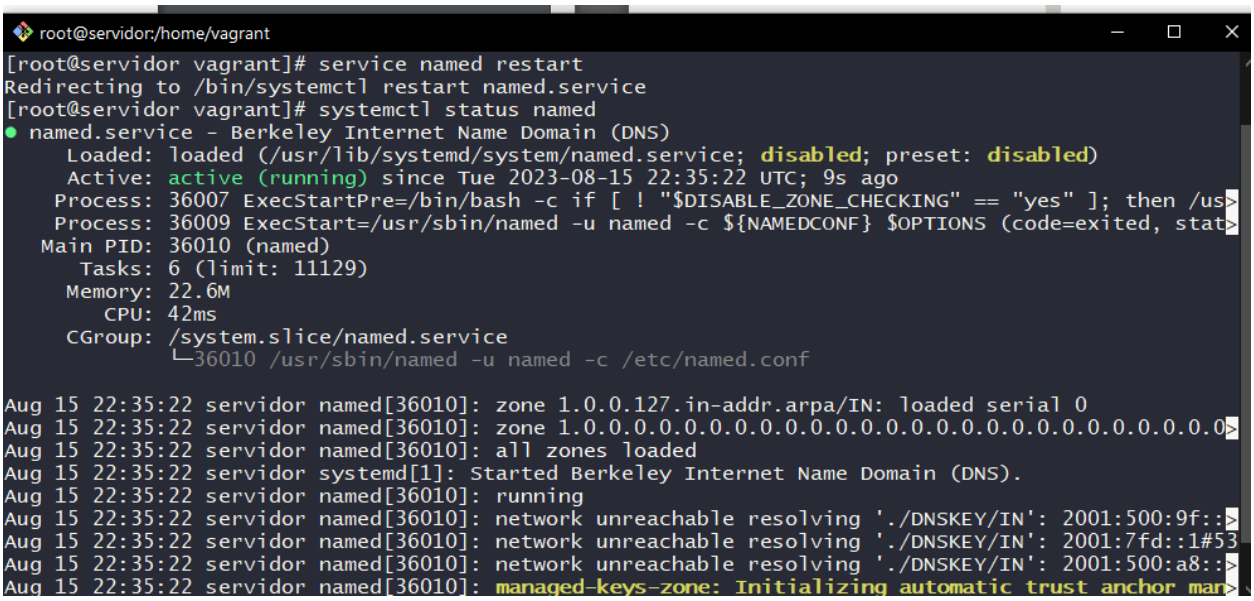
Parte 2. Monitorización de tráfico DNS

Parte 3 DNS y BIND

1. **Función principal de un servidor DNS**: El servidor DNS traduce los nombres de dominio legibles por humanos en direcciones IP que las máquinas pueden entender y viceversa.
2. **¿Qué es BIND?**:
   BIND es un software que implementa protocolos DNS. Se utiliza en servidores para traducir nombres de dominio o resolver consultas DNS.
3. **Archivos de configuración de BIND**:
   - `/etc/named.conf` es el archivo principal de configuración.
   - Los archivos de zonas, que contienen registros para dominios, generalmente están en `/var/named/`.
4. **Demonio y activación de BIND**:
   El demonio se llama `named`. Para iniciarlo:

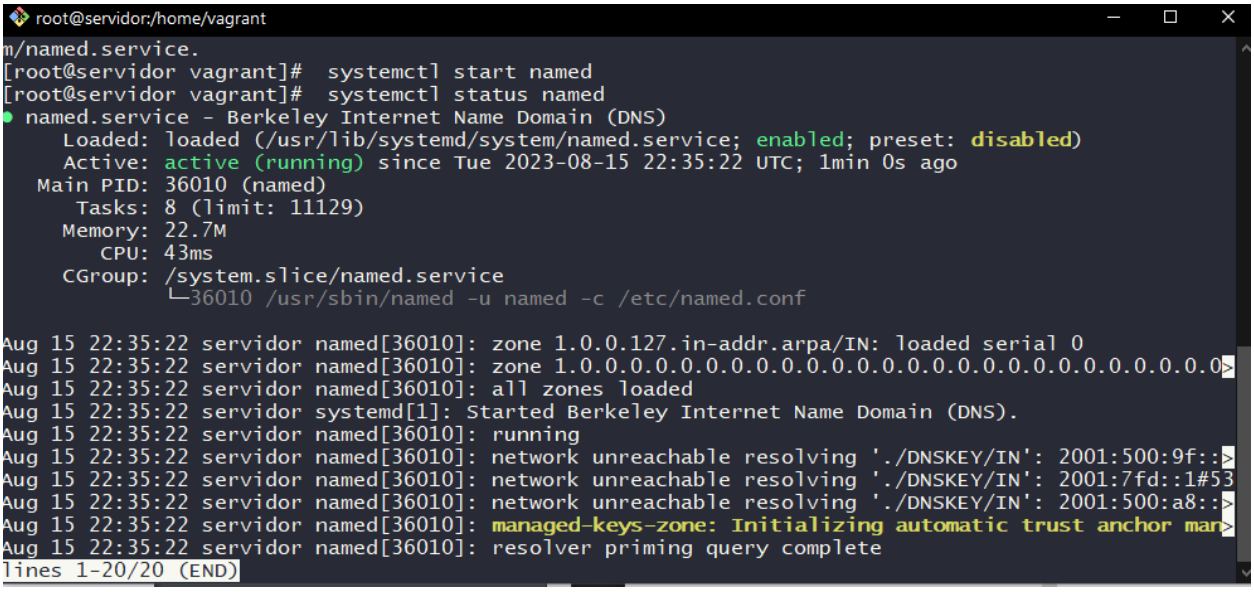
```
yum install bind
```





`systemctl enable named`

`systemctl start named`



5.

`sudo nano /etc/named.conf`

```
zone "urbano.com" IN {
        type master;
        file "forward.urbano";
        allow-update { none; };
};


zone “50.168.192.in-addr.arpa" IN {
    type master;
    file "reverse.urbano";
    allow-update { none; };
};
```

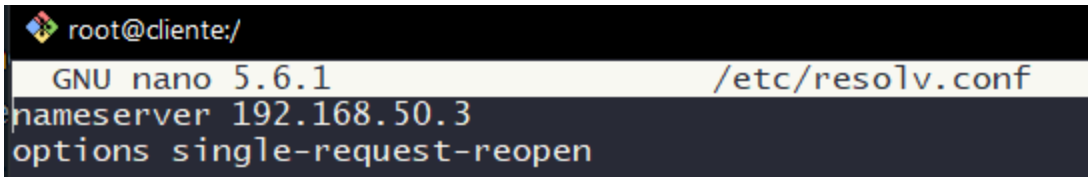
`sudo nano /var/named/urbano.com.fwd`

```
root@servidor:/var/named
  GNU nano 5.6.1                          /var/named/urbano.com.fwd
$ORIGIN urbano.com.
$TTL 3H
@       IN SOA  server.urbano.com root@urbano.com (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      server.urbano.com.
server  IN      A       192.168.50.3
cliente IN      A       192.168.50.2
www     IN      CNAME   server
```

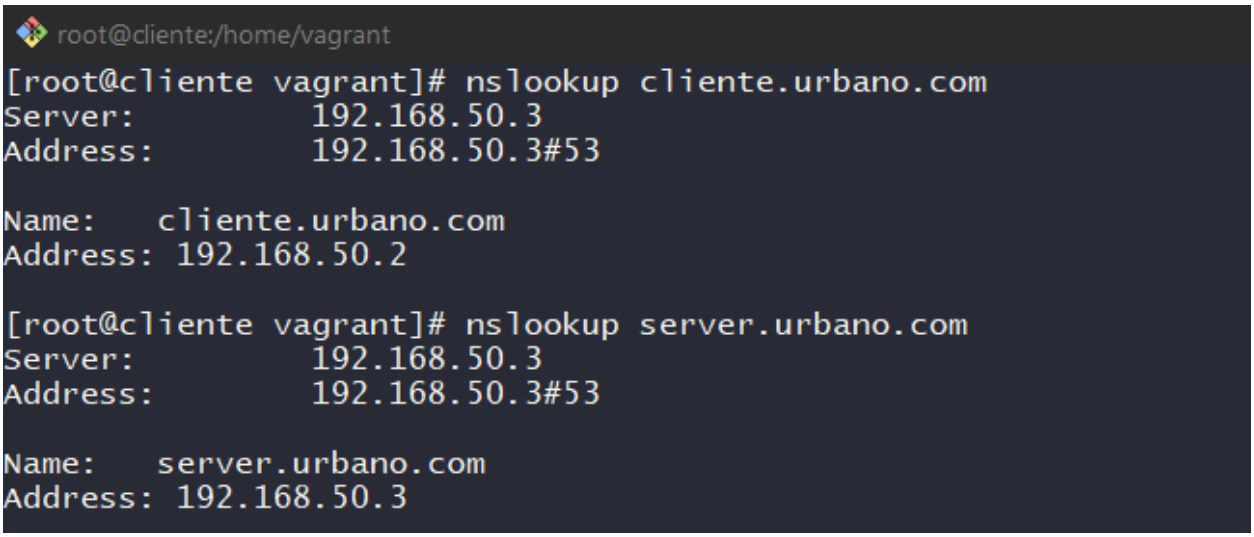
`sudo nano /var/named/urbano.com.rev`

```
root@servidor:/var/named
  GNU nano 5.6.1                          /var/named/urbano.com.re
$ORIGIN 50.168.192.in-addr.arpa.
$TTL 3H
@       IN SOA  server.urbano.com root@urbano.com. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      server.urbano.com.
3       IN      PTR     server.urbano.com.
```

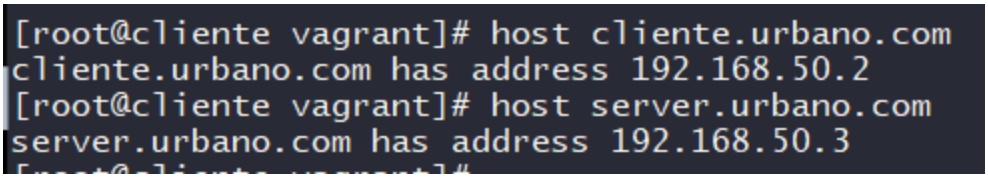
luego se configura en el cliente el /etc/resolv.conf



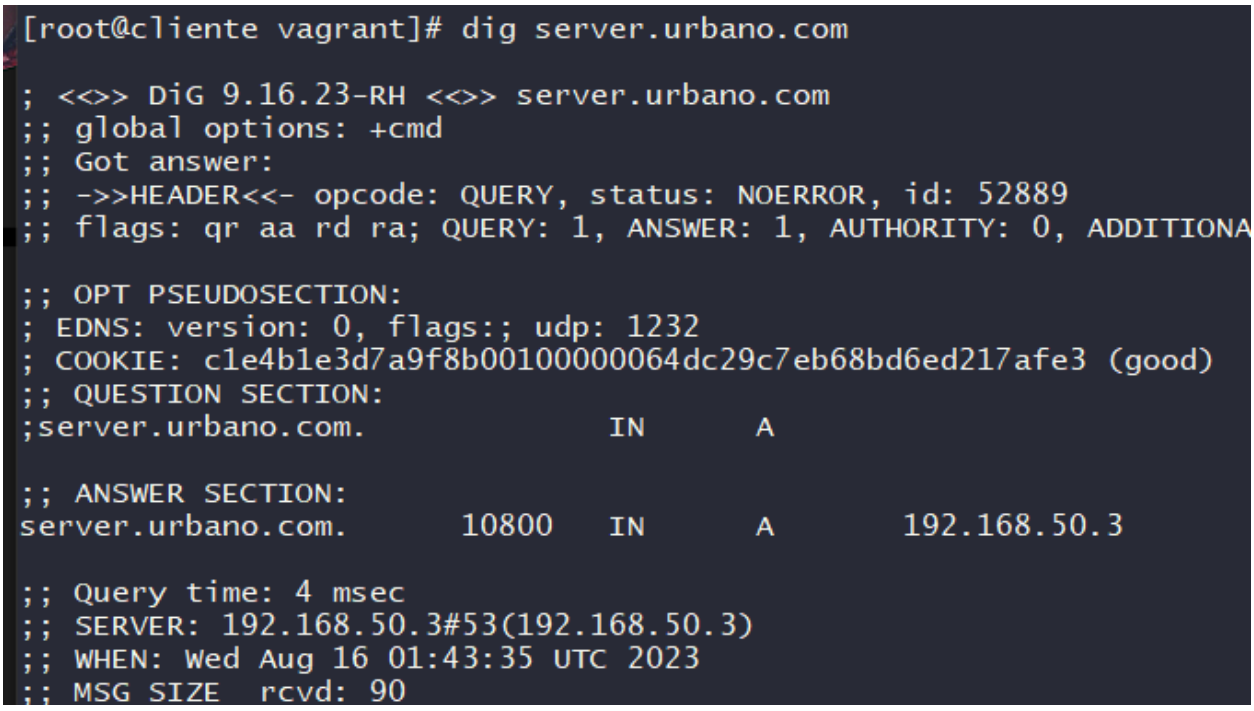
prueba con nslookup:



prueba con host:



prueba con dig:


[root@cliente vagrant]# dig server.urbano.com
; <<>> DiG 9.16.23-RH <<>> server.urbano.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52889
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONA
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c1e4b1e3d7a9f8b00100000064dc29c7eb68bd6ed217afe3 (good)
;; QUESTION SECTION:
;server.urbano.com. IN A
;; ANSWER SECTION:
server.urbano.com. 10800 IN A 192.168.50.3
;; Query time: 4 msec
;; SERVER: 192.168.50.3#53(192.168.50.3)
;; WHEN: Wed Aug 16 01:43:35 UTC 2023
;; MSG SIZE rcvd: 90