DNS PRACTICE – DAW2

Environment we will simulate:

The businessman Equipamientos Industriales Homero S.A. (EIHSA) has acquired a .com domain and has commissioned you to install and configure the primary and secondary servers of the domain authority.

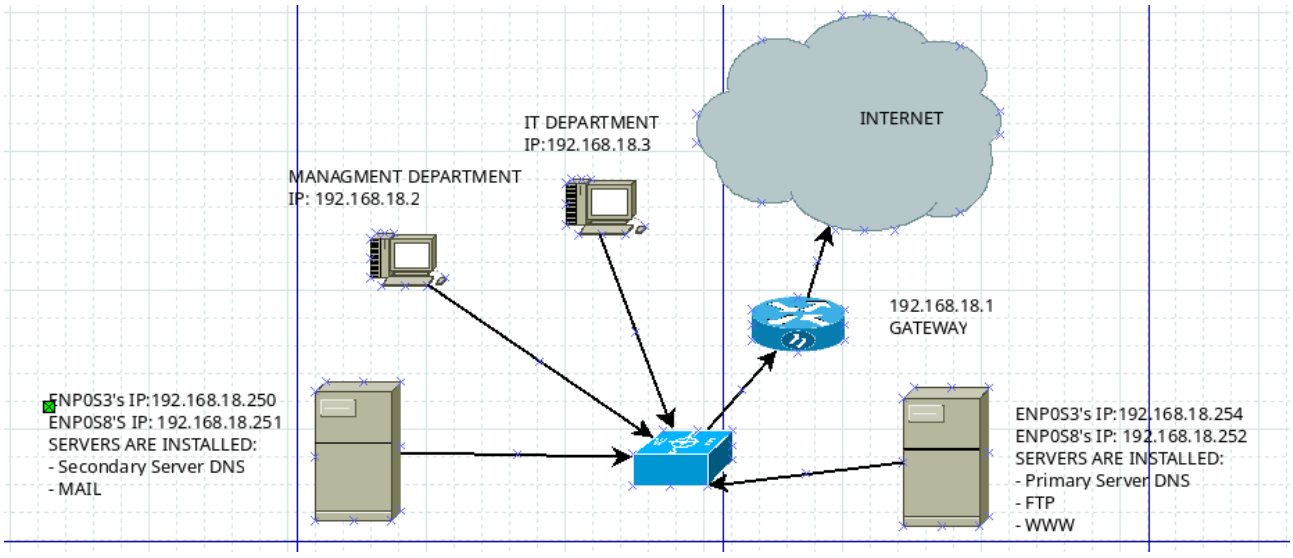
For the simulation, use the following relationship between machine names and IPs:

Name	IP	Description
router	192.168.x.1	Gateway
NS1	NS1 virtual Machine IP	Name Server 1 (Primary DNS Server)
NS2	NS2 virtual Machine IP	Name Server 2 (Secondary DNS Server)
www	192.168.x.252	Web server
FTP	192.168.x.252	FTP server (located on the same www machine) alias
mail	192.168.x.251	Mail Server
management	192.168.x.2	Management computer
Inf	192.168.x.3	Computer IT department

A. Installation planning

A.1. With the DÍA or similar software, you make a physical and logical diagram of the network where the different equipment and devices are shown, as well as their IPs and DNS names.

Insert physical/logical schematic of the network.



A.2. Indicate which registers will be required to configure the direct resolution zone and the values of the configuration parameters for each register. Indicate the required registers and the value of the different configuration parameters

DIRECT ZONE:

@ IN SOA eihsa. root.eihsa.

→ Determines the name of the DNS servers from which they respond

@ IN NS ns1.eihsa.
@ IN NS ns2.eihsa.

→ Determines the IP's to which NS1 and NS2 respond

ns1 IN A 192.168.18.252
ns2 IN A 192.168.18.251

→ Determines the IP's to which services to WWW, FTP(both have the same IP) and MAIL

www IN A 192.168.18.252
ftp IN A 192.168.18.252
mail IN MX 10 mail.eihsa.
mail.eihsa. IN A 192.168.18.251

→ Determines the IP's to which equipments for the departments(managment and inf)

inf IN A 192.168.18.3
managment IN A 192.168.18.2

A.3. Indicate which registers will be required to configure the reverse resolution zone and the values of the configuration parameters for each register. Indicate the required registers and the value of the different configuration parameters

INVERSE ZONE:

@ IN SOA eihsa. root.eihsa.

→ Determines the name of the DNS servers from which they respond

@ IN NS ns1.eihsa.
@ IN NS ns2.eihsa.

→ Determines the IP's to which NS1 and NS2 respond

252 IN PTR ns1.eihsa.
251 IN PTR ns2.eihsa.

→ Determines which services the IPs point to

252 IN PTR www.eihsa
252 IN PTR ftp.eihsa
251 IN PTR mail.eihsa.

→ Determines the IP's to which equipments for the departments(managment and inf)

3 IN PTR inf.eihsa
2 IN PTR managment.eihsa

B. DNS Server Installation and Forwarder Operation

From this section, the virtual machine network must be configured as a bridge adapter.

B.1. Assign a static network configuration to the NS1 server according to the IP that corresponds to your virtual machine

Insert screenshot

```
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    ethernets:
        enp0s3:
            dhcp4: true
        enp0s8:
            addresses: [192.168.18.252/24]
            gateway4: 192.168.18.1
            nameservers:
              search: [eihsa]
              addresses:
                - 192.168.18.252
                - 192.168.18.251
    version: 2
```

B.2. Install the bind9 DNS server software.
Insert screenshot and answer, if applicable, the question

```
user@ubntserver24:~$ sudo apt install bind9 bind9-doc dnsutils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bind9-dnsutils bind9-host bind9-libs bind9-utils dns-root-data liblmdb0 libmaxminddb0 libuv1
  linux-modules-extra-5.15.0-122-generic
Suggested packages:
  bind-doc resolvconf ufw mmdb-bin
The following NEW packages will be installed:
  bind9 bind9-dnsutils bind9-doc bind9-host bind9-libs bind9-utils dns-root-data dnsutils liblmdb0 libmaxminddb0 libuv1
The following packages will be upgraded:
  linux-modules-extra-5.15.0-122-generic
1 upgraded, 11 newly installed, 0 to remove and 4 not upgraded.
1 not fully installed or removed.
Need to get 5266 kB/69.2 MB of archives.
After this operation, 367 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://es.archive.ubuntu.com/ubuntu jammy/main amd64 liblmdb0 amd64 0.9.24-1build2 [47.6 kB]
Get:2 http://es.archive.ubuntu.com/ubuntu jammy/main amd64 libmaxminddb0 amd64 1.5.2-1build2 [24.7 kB]
Get:3 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libuv1 amd64 1.43.0-1ubuntu0.1 [92.7 kB]
Get:4 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 bind9-libs amd64 1:9.18.28-0ubuntu0.22.04.1 [1256 kB]
Get:5 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 bind9-utils amd64 1:9.18.28-0ubuntu0.22.04.1 [161 kB]
Get:6 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 dns-root-data all 2023112702~ubuntu0.22.04.1 [5136 B]
Get:7 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 bind9 amd64 1:9.18.28-0ubuntu0.22.04.1 [261 kB]
Get:8 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 bind9-host amd64 1:9.18.28-0ubuntu0.22.04.1 [52.6 kB]
Get:9 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 bind9-dnsutils amd64 1:9.18.28-0ubuntu0.22.04.1 [157 kB]
Get:10 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 bind9-doc all 1:9.18.28-0ubuntu0.22.04.1 [3205 kB]
Get:11 http://es.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 dnsutils all 1:9.18.28-0ubuntu0.22.04.1 [3924 B]
Fetched 5266 kB in 0s (13.7 MB/s)
debconf: delaying package configuration, since apt-utils is not installed
(Reading database ... 72883 files and directories currently installed.)
Preparing to unpack .../00-linux-modules-extra-5.15.0-122-generic_5.15.0-122.132_amd64.deb ...
Unpacking linux-modules-extra-5.15.0-122-generic (5.15.0-122.132) over (5.15.0-122.132) ...

Progress: [  2%] [##.....................................................................................................]
```

B.3. You show the contents of the configuration file /etc/bind/named.conf. What is the use of the include directive? What files are included?
Insert screenshot and answer the questions

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

The include directive means that when the named.conf file is executed it will include the consecutive execution of the files that are specified

B.4. You look for which file, within the configuration directory /etc/bind/ you find the IP addresses of the root servers and show their content.
Insert screenshot

```
 GNU nano 4.8                          named.conf.default-zones
// prime the server with knowledge of the root servers
zone "." {
        type hint;
        file "/usr/share/dns/root.hints";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};
```

In the folder of *bind*, the file is called named.conf.default-zones and you find all you need about the IP's root

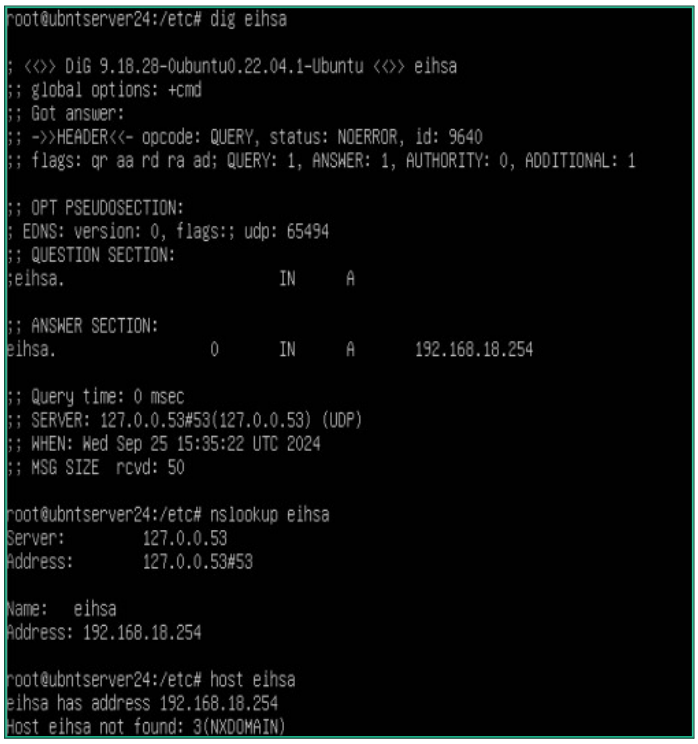
B.5. You configure forwarders to the named.conf.options file.
Insert screenshot

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

         forwarders {
         194.179.1.100;
         };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        //dnssec-validation auto;

        //listen-on-v6 { any; };
};
```

B.6. You configure your server and a client so that they have the DNS server you are configuring. You check the result of the *resolve status* command to check the configuration of the Name Resolution System (DNS).
Insert screenshot

```
root@user-client:/etc/netplan# resolvectl status
Global
       Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
resolv.conf mode: stub

Link 2 (enp0s3)
Current Scopes: DNS
     Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
   DNS Servers: 192.168.18.254
    DNS Domain: eihsa
```

B.7. Install the dnsutils package and check that your server performs the catching correctly by testing dig, nslookup and host requests
Insert screenshot



C. Direct Zone Configuration
C.1. Create a new direct zone for the domain eihsa.com to the /etc/bind/named.conf.local file. The file where the database of the zone will be saved will be the /etc/bind/db.eihsa.com
Insert screenshot

C.2. Create a new file called /etc/bind/db.eihsa.com and configure it taking into account the requirements of the statement for the direct zone.
Insert screenshot

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     eihsa. root.eihsa. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns1.eihsa.
@       IN      NS      ns2.eihsa.
ns1     IN      A       192.168.18.252
ns2     IN      A       192.168.18.251
www     IN      A       192.168.18.252
ftp     IN      A       192.168.18.252
mail    IN      MX 10   mail.eihsa.
mail.eihsa. IN  A       192.168.18.251
inf     IN      A       192.168.18.3
managment IN    A       192.168.18.2
```

C.3. Restart the service with the sudo systemctl restart bind9.service command for the changes to take effect.
Insert screenshot

```
root@ubntserver24:/etc/bind# systemctl status bind9.service
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2024-09-25 16:45:07 UTC; 45s ago
       Docs: man:named(8)
    Process: 1153 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 1154 (named)
      Tasks: 8 (limit: 4540)
     Memory: 5.9M
        CPU: 84ms
     CGroup: /system.slice/named.service
             └─1154 /usr/sbin/named -u bind
```

C.4. Check, using the named-checkzone command, that the syntax of the /etc/bind/db.eihsa.com file is correct. You can use the man named-checkzone command to check how the order works. If you have any syntax errors, correct them until the zone is correctly configured. Don't forget to restart the service and update the serial of the SOA record. Insert screenshot

```
root@ubntserver24:/etc/bind# named-checkzone eihsa.com db.eihsa.com
zone eihsa.com/IN: loaded serial 2
OK
root@ubntserver24:/etc/bind#
```

C.5. Using the nslookup, dig and host commands, verify that your DNS server has the direct zone correctly configured.
Insert screenshot

```
root@ubntserver24:/etc/bind# dig eihsa && nslookup eihsa && host eihsa

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> eihsa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31324
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
eihsa.                  0       IN      A       192.168.18.254

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Sep 25 17:06:46 UTC 2024
;; MSG SIZE  rcvd: 50

Server:         127.0.0.53
Address:        127.0.0.53#53

Name:   eihsa
Address: 192.168.18.254

eihsa has address 192.168.18.254
```

D. Reverse Zone Configuration
D.1. Create a new reverse zone for the domain eihsa.com to the /etc/bind/named.conf.local file. The file where the database of the zone will be saved will be the /etc/bind/db.x.168.192.in-addr.arpa.
Insert screenshot

```
zone "18.168.192.in-addr.arpa" {
type master;
file "db.18.168.192.in-addr.arpa";
allow-query { any; };
allow-transfer { 192.168.18.250; };
//allow-notify { 192.168.18.250; };
also-notify { 192.168.18.250; };
};
```

D.2. Create a new file called /etc/bind/db.x.168.192.in-addr.arpa. Set it up with the requirements of the statement for the inverse zone in mind.
Insert screenshot

```
;
; BIND reverse data file for broadcast zone
;
$TTL    604800
@       IN      SOA     eihsa. root.eihsa. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns1.eihsa.
@       IN      NS      ns2.eihsa.
252     IN      PTR     ns1.eihsa.
251     IN      PTR     ns2.eihsa.
252     IN      PTR     www.eihsa.
252     IN      PTR     ftp.eihsa.
251     IN      PTR     mail.eihsa.
3       IN      PTR     inf.eihsa.
2       IN      PTR     managment.eihsa.
```

D.3. Restart the service with the sudo systemctl restart bindS9 command for the changes to take effect. Insert screenshot

```
root@ubntserver24:/etc/bind# systemctl restart bind9.service
root@ubntserver24:/etc/bind# systemctl status bind9.service
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2024-09-25 17:33:00 UTC; 4s ago
       Docs: man:named(8)
    Process: 1311 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 1312 (named)
      Tasks: 6 (limit: 4540)
     Memory: 5.8M
        CPU: 81ms
     CGroup: /system.slice/named.service
             └─1312 /usr/sbin/named -u bind
```

D.4. Check, using the named-checkzone command, that the syntax of the /etc/bind/db.x.168.192.in-addr.arpa file is correct. You can use the man named-checkzone command to check how the order works. If you have any syntax errors, correct them until the zone is correctly configured. Don't forget to restart the service and update the serial of the SOA record. Insert screenshot

```
root@ubntserver24:/etc/bind# named-checkzone 192.168.18.254 db.18.168.192.in-addr.arpa
zone 192.168.18.254/IN: loaded serial 1
OK
```

D.5. Using the nslookup, dig and host commands, verify that your DNS server has the reverse zone correctly configured. Insert screenshot

```
root@ubntserver24:/home/user# nslookup 192.168.18.254
254.18.168.192.in-addr.arpa     name = eihsa.

root@ubntserver24:/home/user# dig -x 192.168.18.254

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> -x 192.168.18.254
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28306
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;254.18.168.192.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
254.18.168.192.in-addr.arpa. 0  IN      PTR     eihsa.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Sep 30 13:50:19 UTC 2024
;; MSG SIZE  rcvd: 75

root@ubntserver24:/home/user# host 192.168.18.254
254.18.168.192.in-addr.arpa domain name pointer eihsa.
```

E. Secondary Server Configuration

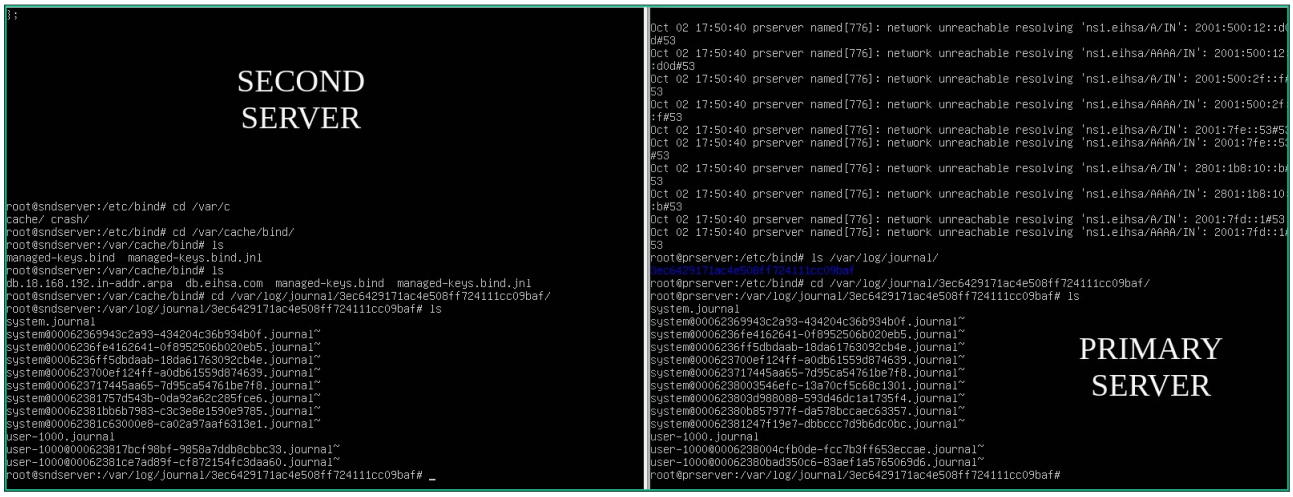
E.1. Allow the primary server to transfer the zone to the secondary server. Add the corresponding configuration options to the /etc/bind/named.conf.local file on the primary server. Don't forget to restart the service for the changes to take effect. Insert screenshot

```
zone "eihsa.com" {
    type master;
    file "/etc/bind/db.eihsa.com";
    allow-query { any; };
    allow-transfer { 192.168.18.250; };
};
zone "18.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.18.168.192.in-addr.arpa";
    allow-query { any; };
    allow-transfer { 192.168.18.250; };
};
```

E.2. Configure the /etc/bind/named.conf.local file of the secondary server to connect to the primary server and perform the corresponding zone transfer. You need to edit the /etc/bind/named.conf.local file. Don't forget to restart the service for the changes to take effect.
Insert screenshot

```
zone "eihsa.com" {
        type slave;
        file "/var/cache/bind/db.eihsa.com";
        masters { 192.168.18.254; };
};

zone "18.168.192.in-addr.arpa" {
        type slave;
        file "/var/cache/bind/db.18.168.192.in-addr.arpa";
        masters { 193.168.18.254; };
};
```

E.3. Check the /var/log/syslog file, both on the primary and secondary servers, that the transfer has been carried out correctly.
Insert screenshots

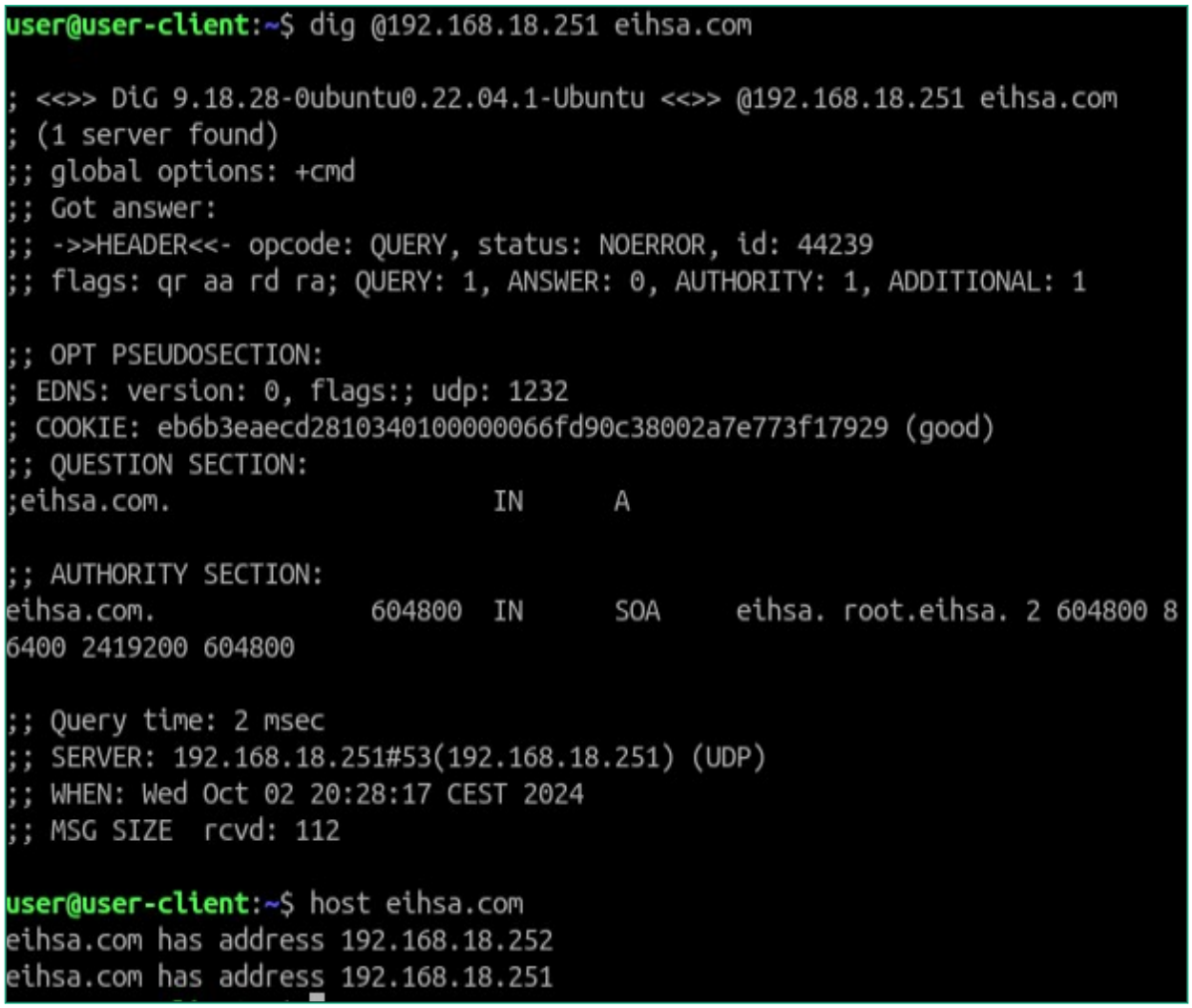


Previously, the transfer service for data connection activities in Bind, the route was located in /var/log/syslog, but currently this changed as it was adapted to another type of package called journel. This is located in /var/log/journel/

E.4. A zone transfer is performed only if the serial number of the primary server is larger than the serial number of the secondary server. Add the also-notify directive to the /etc/bind/named.conf.local configuration file on the primary server to notify the secondary server of the changes made. Insert screenshot

E.5. Access the files contained in the /var/cache/bind folder of the secondary server. What content is saved to this folder? Insert screenshot and answer the question

E.6. Configure a DNS client to connect to the secondary DNS server. Using the nslookup, dig and host commands, verify that your DNS server is correctly configured. Based on the results obtained, indicate whether the responses obtained from the secondary DNS server are authoritative or non-authoritative.
Insert screenshot and answer the question



In this case it tells us that it is authoritive since it is authorized by the primary DNS server, that is, it searches for it so that this server works