3. Network Services Involved in the Deployment of a Web Application

Miquel Àngel París i Peñaranda

Web Application Deployment

2nd C-VET Web Application Development

Index

DNS Practice

Environment we will simulate:

The enterprise 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 DIA 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

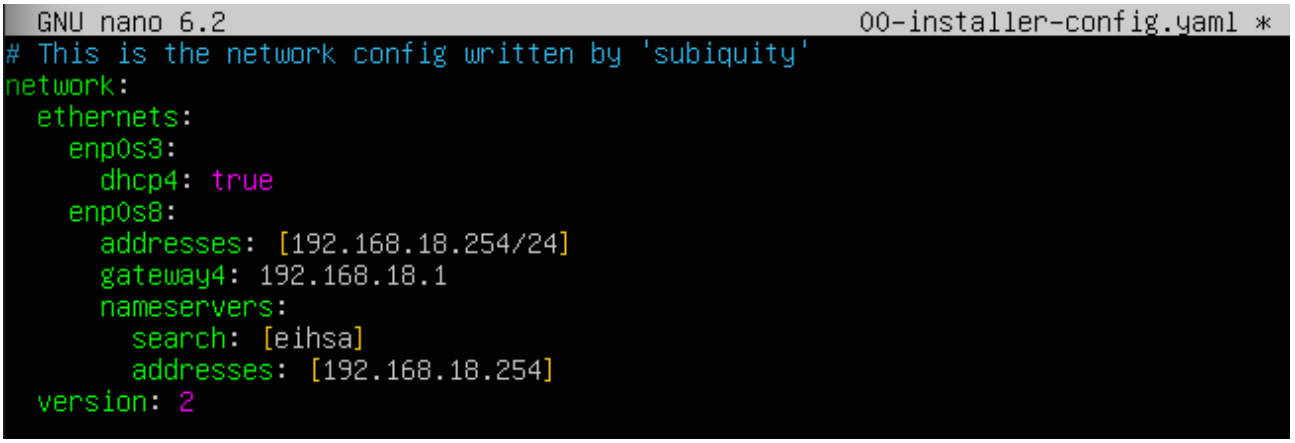
A.3. Indicate which registers will be required to configure the reverse resolution zone and the values of the configuration parameters for each register.

Indicate the required registers and the value of the different configuration parameters

B. DNS Server Installation and Forwarder Operation

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

Insert screenshot



B.2. Install the bind9 DNS server software.

Insert screenshot and answer, if applicable, the question

```
root@server:/etc/netplan# dpkg -l | grep bind9
ii  bind9                                1:9.18.28-0ubuntu0.22.04.1              amd64        Internet Domain Name Ser
ii  bind9-dnsutils                       1:9.18.28-0ubuntu0.22.04.1              amd64        Clients provided with BI
ii  bind9-doc                            1:9.18.28-0ubuntu0.22.04.1              all          Documentation for BIND 9
ii  bind9-host                           1:9.18.28-0ubuntu0.22.04.1              amd64        DNS Lookup Utility
ii  bind9-libs:amd64                     1:9.18.28-0ubuntu0.22.04.1              amd64        Shared Libraries used by
ii  bind9-utils                          1:9.18.28-0ubuntu0.22.04.1              amd64        Utilities for BIND 9
ii  dnsutils                             1:9.18.28-0ubuntu0.22.04.1              all          Transitional package for
nsutils
root@server:/etc/netplan# 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 Mon 2024-09-23 13:51:36 UTC; 42min ago
       Docs: man:named(8)
   Main PID: 1745 (named)
      Tasks: 5 (limit: 2204)
     Memory: 5.6M
        CPU: 163ms
     CGroup: /system.slice/named.service
             └─1745 /usr/sbin/named -u bind

Sep 23 13:51:36 server named[1745]: FORMERR resolving './NS/IN': 202.12.27.33#53
Sep 23 13:51:36 server named[1745]: resolver priming query complete: failure
Sep 23 14:28:23 server named[1745]: no longer listening on 10.0.2.15#53
Sep 23 14:28:23 server named[1745]: no longer listening on 192.168.18.254#53
Sep 23 14:28:23 server named[1745]: listening on IPv4 interface enp0s3, 10.0.2.15#53
Sep 23 14:28:23 server named[1745]: listening on IPv4 interface enp0s8, 192.168.18.254#53
Sep 23 14:28:23 server named[1745]: no longer listening on 192.168.18.254#53
Sep 23 14:28:23 server named[1745]: no longer listening on 10.0.2.15#53
Sep 23 14:28:23 server named[1745]: listening on IPv4 interface enp0s8, 192.168.18.254#53
Sep 23 14:28:23 server named[1745]: listening on IPv4 interface enp0s3, 10.0.2.15#53
root@server:/etc/netplan# _
```

B.3. 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

```
 GNU nano 6.2                                                named.conf
// 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";
```

B.4. 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 6.2                                          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";
};
```

B.5. Configure forwarders to the `named.conf.options` file.

Insert screenshot

```
 GNU nano 6.2                                          named.conf.options
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 {
                8.8.8.8;
         };

        //========================================================================
        // 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. Configure your server and a client so that they have the DNS server you are configuring. Check the result of the resolve status command to check the configuration of the Name Resolution System (DNS).

Insert screenshot

```
root@user-virtualbox:/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
Current DNS Server: 192.168.18.254
       DNS Servers: 192.168.18.254
        DNS Domain: eihsa
root@user-virtualbox:/etc/netplan#
```

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

Insert screenshot

```
root@server:/etc# dig eihsa

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> eihsa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63038
;; 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 15:26:08 UTC 2024
;; MSG SIZE  rcvd: 50

root@server:/etc# nslookup eihsa
Server:         127.0.0.53
Address:        127.0.0.53#53

Name:   eihsa
Address: 192.168.18.254

root@server:/etc# host eihsa
eihsa has address 192.168.18.254
Host eihsa not found: 3(NXDOMAIN)
root@server:/etc# _
```

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

```
 GNU nano 6.2                                          named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "eihsa.com" {
        type master;
        file "/etc/bind/db.eihsa.com";
        allow-query{ any; };
        allow-transfer { none; };
};
```

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

```
root@server:/etc/bind# systemctl restart bind9
Job for named.service failed because the control process exited with error code.
See "systemctl status named.service" and "journalctl -xeu named.service" for details.
root@server:/etc/bind#
```

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

Insert screenshot

```
 GNU nano 6.2                                                db.eihsa.com
;
; BIND data file for broadcast zone
;
$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       192.168.18.254
ns2     IN      A       192.168.18.253
www     IN      A       192.168.18.252
ftp     IN      A       192.168.18.252
mail    IN      MX      10      mail.eihsa.com
mail.eihsa.com  IN      A       192.168.18.251
management      IN      A       192.168.18.2
inf     IN      A       192.168.18.3
```

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@server:/etc/bind# named-checkzone eihsa.com /etc/bind/db.eihsa.com
zone eihsa.com/IN: loaded serial 2
OK
root@server:/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@server:/etc/bind# nslookup eihsa
Server:         127.0.0.53
Address:        127.0.0.53#53

Name:   eihsa
Address: 192.168.18.254

root@server:/etc/bind# dig eihsa

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> eihsa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50258
;; 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 17:01:00 UTC 2024
;; MSG SIZE  rcvd: 50

root@server:/etc/bind# host eihsa
eihsa has address 192.168.18.254
Host eihsa not found: 3(NXDOMAIN)
root@server:/etc/bind#
```

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

```
  GNU nano 6.2                                                named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";


zone "eihsa.com" {
        type master;
        file "/etc/bind/db.eihsa.com";
        allow-query{ any; };
        allow-transfer { none; };
};


zone "18.168.192.in-addr.arpa"{
        type master;
        file "/etc/bind/db.18.168.192.in-addr.arpa";
        allow-query{ any;};
        allow-transfer{ none; };
}
```

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

```
 GNU nano 6.2                                          db.18.168.192.in-addr.arpa
;
; 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.
254     IN      PTR     ns1.eihsa.
253     IN      PTR     ns2.eihsa.
252     IN      PTR     www.eihsa
252     IN      PTR     ftp.eihsa
251     IN      PTR     mail.eihsa.
2       IN      PTR     managment.eihsa.
3       IN      PTR     inf.eihsa.
```

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

```
root@server:/etc/bind# systemctl status bind9
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-09-30 14:19:51 UTC; 44s ago
       Docs: man:named(8)
    Process: 567 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 635 (named)
      Tasks: 5 (limit: 2204)
     Memory: 13.3M
        CPU: 172ms
     CGroup: /system.slice/named.service
             └─635 /usr/sbin/named -u bind

Sep 30 14:20:16 server named[635]: network unreachable resolving 'api.snapcraft.io/AAAA/IN': 2801:1b8:10::b#53
Sep 30 14:20:17 server named[635]: network unreachable resolving 'api.snapcraft.io/A/IN': 2001:7fd::1#53
Sep 30 14:20:17 server named[635]: network unreachable resolving 'api.snapcraft.io/AAAA/IN': 2001:7fd::1#53
Sep 30 14:20:19 server named[635]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
Sep 30 14:20:19 server named[635]: network unreachable resolving './NS/IN': 2001:500:1::53#53
Sep 30 14:20:20 server named[635]: network unreachable resolving 'api.snapcraft.io/A/IN': 2001:500:12::d0d#53
Sep 30 14:20:20 server named[635]: network unreachable resolving 'api.snapcraft.io/AAAA/IN': 2001:500:12::d0d#53
Sep 30 14:20:20 server named[635]: network unreachable resolving 'api.snapcraft.io/A/IN': 2001:500:1::53#53
Sep 30 14:20:20 server named[635]: network unreachable resolving 'api.snapcraft.io/AAAA/IN': 2001:500:1::53#53
Sep 30 14:20:23 server named[635]: resolver priming query complete: timed out
root@server:/etc/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

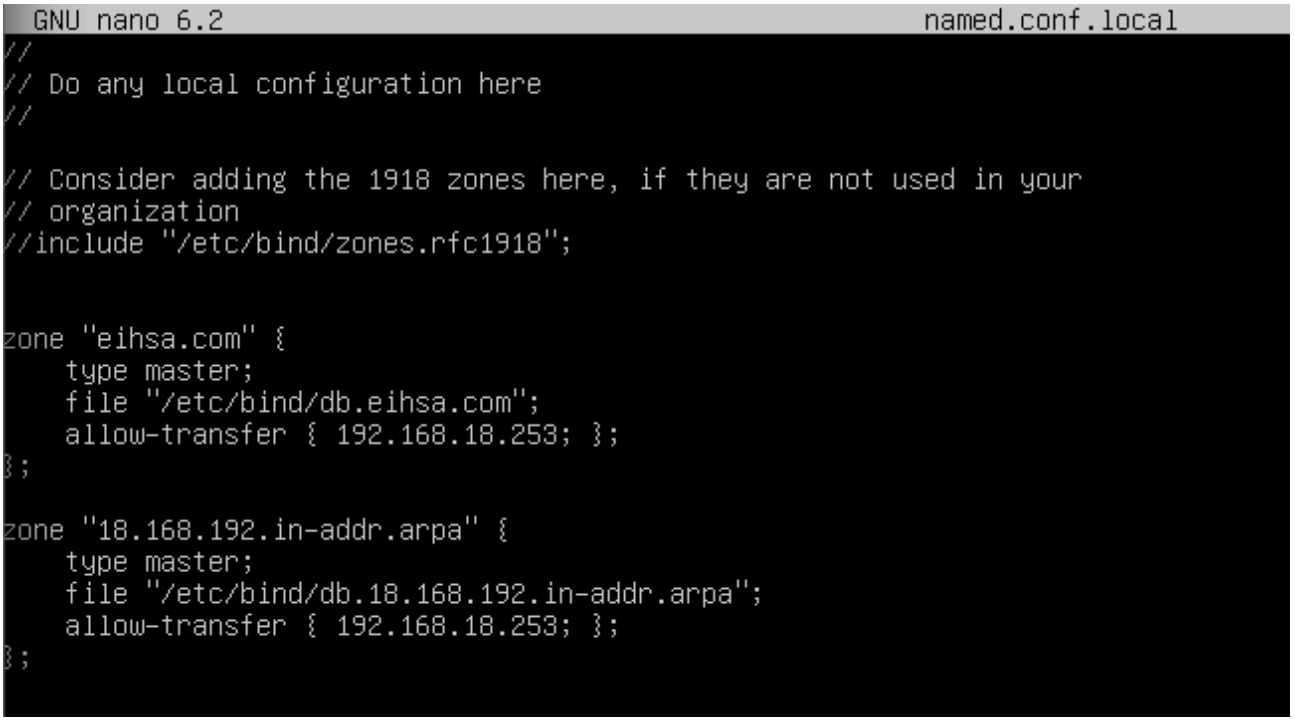
```
root@server:/etc/bind# named-checkzone 192.168.18.254 db.18.168.192.in-addr.arpa
zone 192.168.18.254/IN: loaded serial 1
OK
root@server:/etc/bind# _
```

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

```
root@server:/etc/bind# nslookup 192.168.18.254
254.18.168.192.in-addr.arpa     name = eihsa.

root@server:/etc/bind# 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: 56952
;; 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 14:22:34 UTC 2024
;; MSG SIZE  rcvd: 75

root@server:/etc/bind# host 192.168.18.254
254.18.168.192.in-addr.arpa domain name pointer eihsa.
root@server:/etc/bind#
```

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



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

```
  GNU nano 6.2                                  named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

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 { 192.168.18.254; };
};
```

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

- primary

```
root@server:/var/log/journal# ls
4d4f462bfe4048c5abfb3747f0445687
root@server:/var/log/journal# cd 4d4f462bfe4048c5abfb3747f0445687/
root@server:/var/log/journal/4d4f462bfe4048c5abfb3747f0445687# ls
system.journal                                  system@0006236a92438626-cddce6e1d67c5e93.journal~
system@000622f2d6500680-487c1f322d6f6d55.journal~  system@0006237022f1bfca-e09d1b44b50ca2d2.journal~
system@000622f2db8005f9-26d57cedbf3613bc.journal~  system@000623813db8d1d0-a2cae7e617c953ba.journal~
system@000623569c085ae2-e52a6fcf08bbd4f9.journal~  user-1000.journal
system@00062356a89e3249-ff6f79c401b31dd5.journal~  user-1000@000622f2ddd09708-ea543751e63960ea.journal~
system@00062356e47cd1fd-f77877508d2bd740.journal~  user-1000@00062356aa857ea9-986f159bf5236b1f.journal~
system@00062357ad0b2939-9df0b19a33ce0129.journal~  user-1000@00062356e6b5eb63-25c40b2dcc43f040.journal~
system@000623679d5348b2-8c946bc2a979a543.journal~  user-1000@0006236a94a98300-dd71beb0fc3d87cc.journal~
system@00062367d7cfefc5-28ab8bf7c300574e.journal~  user-1000@0006238140ddad77-5c54adcde80e42d1.journal~
root@server:/var/log/journal/4d4f462bfe4048c5abfb3747f0445687# _
```

- secondary

```
root@user2:/home/user2# cd /var/log/journal/
root@user2:/var/log/journal# ls
fc01dc0397fd4e079e2ee52319d9d866
root@user2:/var/log/journal# cd fc01dc0397fd4e079e2ee52319d9d866/
root@user2:/var/log/journal/fc01dc0397fd4e079e2ee52319d9d866# ls
system.journal
system@00062367a9053e35-bc621afb6e8d1a3e.journal~
system@00062367d1009067-93f2474be5632f49.journal~
system@0006236a92ab989d-fb5b9479e91036ce.journal~
system@00062370282f4924-e78ad8eea2802293.journal~
system@000623813db91e49-19283382643d843c.journal~
user-1000.journal
user-1000@0006236a973eae3e-5a7d271d65a6447f.journal~
user-1000@00062381553cdb6c-779d2bfaaf65405d.journal~
root@user2:/var/log/journal/fc01dc0397fd4e079e2ee52319d9d866# _
```

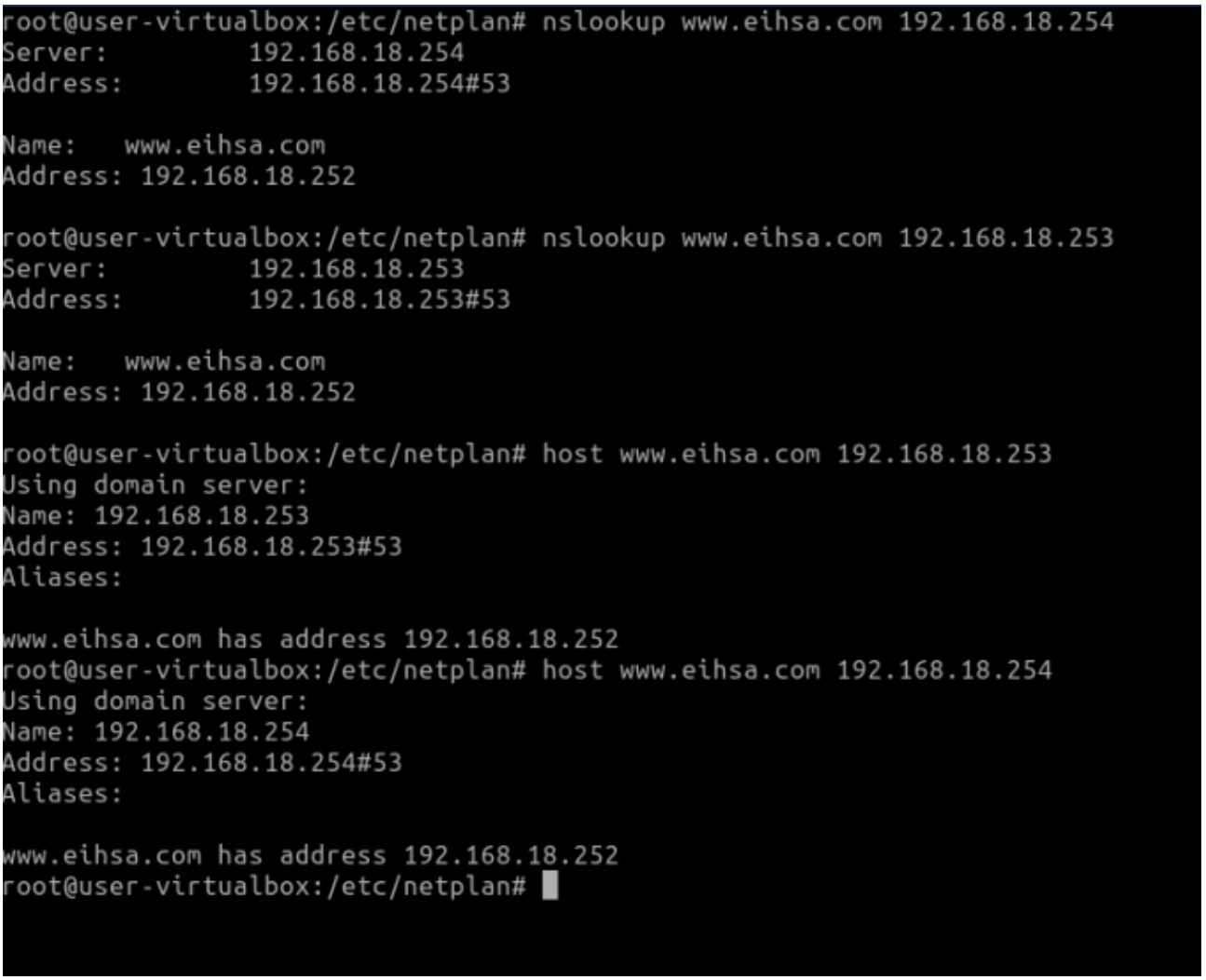
E.4. A zone transfer is performed only if the serial number of the primary server is larger than the serial number of the secondary server. Add the also-notify directive to the `/etc/bind/named.conf.local` configuration file on the primary server to notify the secondary server of the changes made. Insert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

```
 GNU nano 6.2                                          named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";


zone "eihsa.com" {
        type master;
        file "/etc/bind/db.eihsa.com";
        allow-transfer { 192.168.18.253; };
        also-notify { 192.168.18.253; };
};

zone "18.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.18.168.192.in-addr.arpa";
        allow-transfer { 192.168.18.253; };
        also-notify{ 192.168.18.253; };
};
```

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



```
root@user-virtualbox:/etc/netplan# dig @192.168.18.254 www.eihsa.com

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> @192.168.18.254 www.eihsa.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35147
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: af531704967f55dd0100000066fdb41ab0ebb3b67cbf87d8 (good)
;; QUESTION SECTION:
;www.eihsa.com.                 IN      A

;; ANSWER SECTION:
www.eihsa.com.          604800  IN      A       192.168.18.252

;; Query time: 3 msec
;; SERVER: 192.168.18.254#53(192.168.18.254) (UDP)
;; WHEN: Wed Oct 02 22:59:21 CEST 2024
;; MSG SIZE  rcvd: 86

root@user-virtualbox:/etc/netplan# dig @192.168.18.253 www.eihsa.com

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> @192.168.18.253 www.eihsa.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27103
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d456f445134666e50100000066fdb41d64c964ec641aede7 (good)
;; QUESTION SECTION:
;www.eihsa.com.                 IN      A

;; ANSWER SECTION:
www.eihsa.com.          604800  IN      A       192.168.18.252

;; Query time: 4 msec
;; SERVER: 192.168.18.253#53(192.168.18.253) (UDP)
;; WHEN: Wed Oct 02 22:59:24 CEST 2024
;; MSG SIZE  rcvd: 86

root@user-virtualbox:/etc/netplan#
```