LABORATORY 2
UNIT 03: DOMAIN NAME SERVER

0 How to install bind9 DNS server.

In order to install DNS server in your Ubuntu server, run the following command:

```
sudo apt install bind9
```

After the installation, the service will be running. There are specific commands to start, stop, restart and check the status of the DNS service:

```
sudo service bind9 start
sudo service bind9 stop
sudo service bind9 restart
sudo service bind9 status
```

To manage network devices easily (we wil use it often) you can install Network Manager graphical interface with the following command (**not needed on Ubuntu MATE**):

```
sudo apt install network-manager-gnome
```

And to run it, if you don't restart your computer :

```
nm-connection-editor
```

1 Virtual Machine

The network configuration of both VM, server and client, must be "Bridged networking", so that the VM are going to work as independent hosts in the network with an IP address of the network each one.

2 Configuration files.

A setting of the DNS server must be done before it works properly.

The main bind9 configuration file is **/etc/bind/named.conf.** Other files related to bind9 configuration are:

- **named.conf.options**: it contains general options
- **named.conf.local**: this file contains the forward and reverse zones definition
- **db.root:** this file holds the information about root name servers.

3. Good practice

It is good practice to make a copy of configuration files before changing them. The name of the copied files could finish ".old", so if necessary we could retrieve them later. The files we have to copy are:

- named.conf.option
- named.conf.local

4. DNS record types

There are lots of different DNS record types, but some of the most common types are covered below.

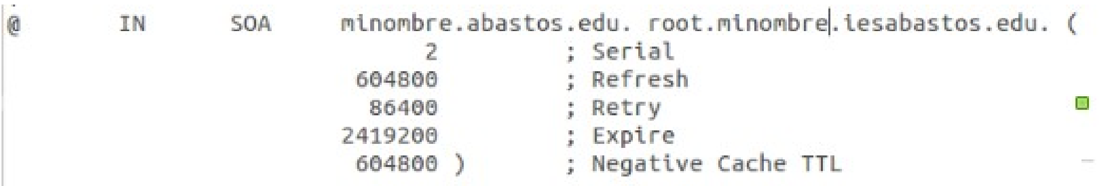
- A (Address records). The most commonly used type of record. This record maps an IP Address to a hostname.

- MX (Mail eXchange records). Used to define where email should be sent to and at what priority. Must point to an A record, not a CNAME. Multiple MX records can exist if multiple mail servers are responsible for that domain.

- CNAME (Canonical Name). Used to create an alias from an existing A record. You can create a CNAME record pointing to another CNAME record. But it doubles the number of requests made to the name server, thus making it an inefficient way to do so.

- NS (Name Server records). Used to define which servers serve copies of this zone. It must point to an A record, not a CNAME. This is where Primary and Secondary servers are defined.

- SOA (Start Of Authority Resource Record). The SOA defines the global parameters for the zone (domain). Only one SOA resource record (RR) is allowed in a zone file and it must be the first RR in the zone. The most complex and most critical record in the zone file.



```
@       IN      SOA     minombre.abastos.edu. root.minombre.iesabastos.edu. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
```

In the first line:

- @: It is the 'root name' or the apex of the zone. Most commonly written as @ but can be the explicit base Domain Name in FQDN format.

- IN: Defines the class of record and normally takes the value IN = Internet

- SOA: DNS record type

- minombre.abastos.edu.: Any name server that will respond authoritatively for the domain. Called the *Primary Master* in the context of DNS. To mimimise confusion this is most commonly written as a Fully-qualified Domain Name (FQDN - ends with a dot).

- root.minombre.abastos.edu.: Email address of the person responsible for this zone and to which email may be sent to report errors or problems

Other information:

- Serial: This value MUST increment when any resource record in the zone file is updated. A slave (Secondary) DNS server will read the master DNS SOA record periodically, either on expiry of *refresh* (defined below) or when it receives a NOTIFY and compares, arithmetically, its current value of *sn* with that received from the master. If the *sn* value from the master is arithmetically HIGHER than that currently stored by the slave then a zone transfer (AXFR/IXFR) is initiated by the slave. If the value of *sn* from the master DNS SOA is the same or LOWER then no zone transfer is initiated. The convention is to use a date based *sn* value to simplify the task of incrementing the *sn* - the most popular convention being yyyymmddss where yyyy = year, mm = month and dd = day ss = a sequence number in case you update it more than once in the day!

- Refresh: Signed 32 bit time value in seconds. Indicates the time when the slave will try to refresh the zone from the master (by reading the master DNS SOA RR). RFC 1912 recommends 1200 to 43200 seconds, low (1200) if the data is volatile or 43200 (12 hours) if it's not. If you are using NOTIFY you can set it to much higher values, for instance, 1 or more days.

- Retry: Signed 32 bit value in seconds. Defines the time between retries if the slave (secondary) fails to contact the master when *refresh* (above) has expired or a NOTIFY message is received. Typical values would be 180 (3 minutes) to 900 (15 minutes) or higher

- Expire: Signed 32 bit value in seconds. Indicates when the zone data is no longer authoritative. Used by Slave (Secondary) servers only. BIND9 slaves stop responding authoritatively to queries for the zone when this time has expired and no contact has been made with the master.. It is recommended 1209600 to 2419200 seconds (2-4 weeks) to allow for major outages of the zone master.

- Negative cache TL: It is the time a NAME ERROR = NXDOMAIN result may be cached by any resolver. The maximum value allowed by RFC 2308 for this parameter is 3 hours (10800 seconds).

5. Caching server

In this configuration BIND9 will find the answer to name queries and remember the answer for the next query. This can be useful for a slow internet connection. By caching DNS queries, you will reduce bandwidth and (more importantly) latency.

The default configuration is setup to act as a caching server.
All that is required is simply adding the IP numbers of your ISP's DNS servers.

Simply uncomment and edit the following in /etc/bind/named.conf.options:

```
[ . . . ]
forwarders {
8.8.8.8;
8.8.4.4;
};
[ . . . ]
```

Before testing your caching server don't forget to restart the bind daemon, running the following command:

```
sudo service bind9 restart
```

6. Setting up the DNS client

Click on the network icon on the top right side and select “Edit connections” → ”Wired connection1” → Select IPv4 Settings tab → Select Automatic(DHCP) addresses only Method. And finally, find out your Ubuntu Server ip address and write it into DNS server text box.

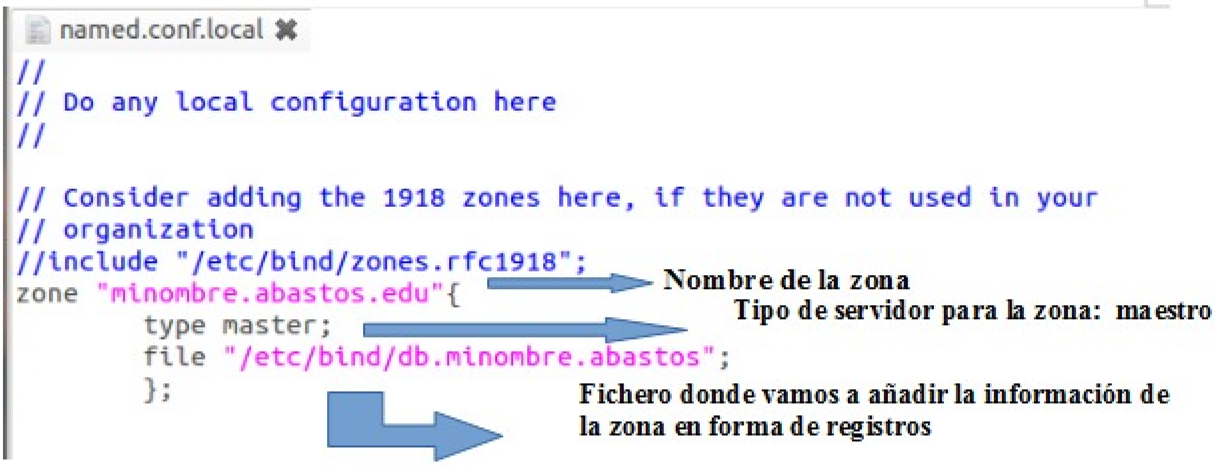
You can use your host machine just using “nslookup” putting the DNS address at the end of the request: “nslookup pc1.minombre.abastos.edu 192.168.1.111” for example.

7. Setting up a master DNS server

Imagine that we wan to to set up a private DNS server authoritative for “yourname.abastos.edu” domain. This DNS won't be only able to performance resolutions but also reverse resolutions.

First of all, you must edit /etc/bind/named.conf.local. Aside from a few comments, the file should be empty. Here, we will specify our forward and reverse zones.

Add the forward zone with the following lines:



```
//
// 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 "minombre.abastos.edu"{
        type master;
        file "/etc/bind/db.minombre.abastos";
        };
```

Nombre de la zona

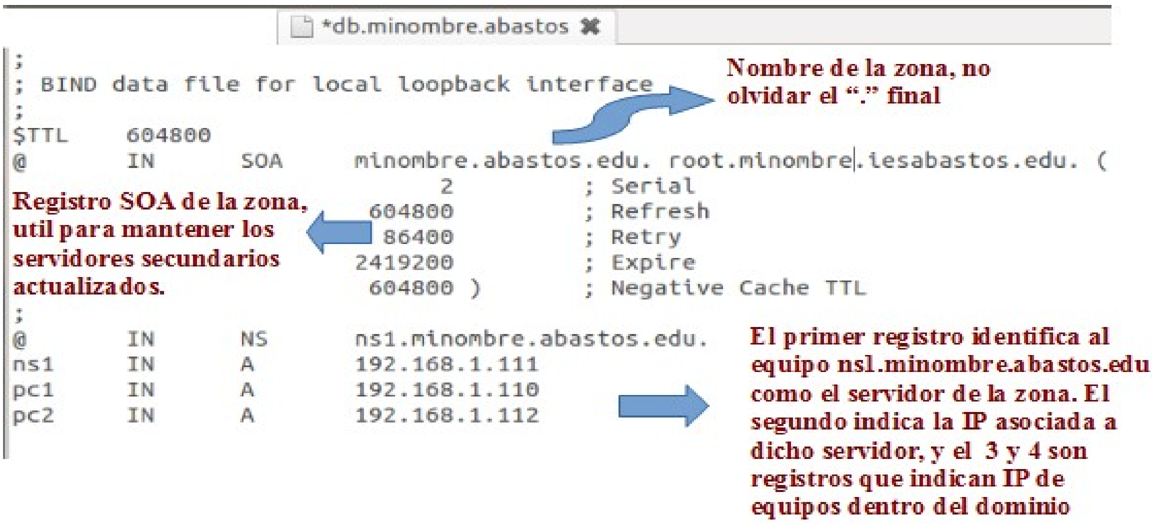
Tipo de servidor para la zona: maestro

Fichero donde vamos a añadir la información de la zona en forma de registros

Now that our zones are specified in BIND, we need to create the corresponding forward file. The forward zone file is where we define DNS records for forward DNS lookups. That is, when the DNS receives a name query, "pc1.minombre.abastos.edu" for example, it will look in the forward zone file to resolve *pc1*'s corresponding private IP address.

We will base our forward zone file on the sample db.local zone file. Copy it to the proper location with the following command: cp db.local /etc/bind/db.minombre.abastos
Now let's edit our forward zone file :

- First, you will want to edit the SOA record. Replace the first "localhost" with “yourname.abastos.edu.” FQDN, then replace "root.localhost" with "root.yourname.abastos.edu.". Also, every time you edit a zone file, you should increment the *serial* value before you restart the DNS.
- Now exchange the last three lines with the lines of your own zone. Add NS records and A records.



```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     minombre.abastos.edu. root.minombre.iesabastos.edu. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns1.minombre.abastos.edu.
ns1     IN      A       192.168.1.111
pc1     IN      A       192.168.1.110
pc2     IN      A       192.168.1.112
```

Nombre de la zona, no olvidar el “.” final

Registro SOA de la zona, util para mantener los servidores secundarios actualizados.

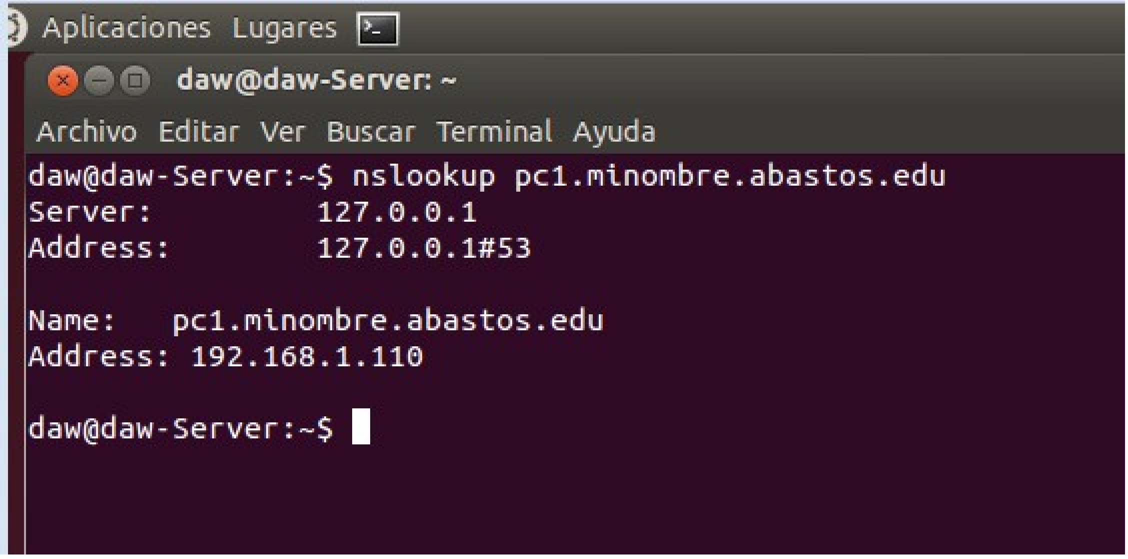
El primer registro identifica al equipo nsl.minombre.abastos.edu como el servidor de la zona. El segundo indica la IP asociada a dicho servidor, y el 3 y 4 son registros que indican IP de equipos dentro del dominio

When you finish, you must restart the service

sudo service bind9 restart

You can check the DNS service by running the nslookup command from the client VM:

nslookup pc1.minombre.abastos.edu



```
daw@daw-Server:~$ nslookup pc1.minombre.abastos.edu
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   pc1.minombre.abastos.edu
Address: 192.168.1.110

daw@daw-Server:~$ 
```

If there is something wrong, there are two commands:

- **named-checkconf**
- **named-checkzone** *zone-name zone-file*

that could help you to find the errors.

ie

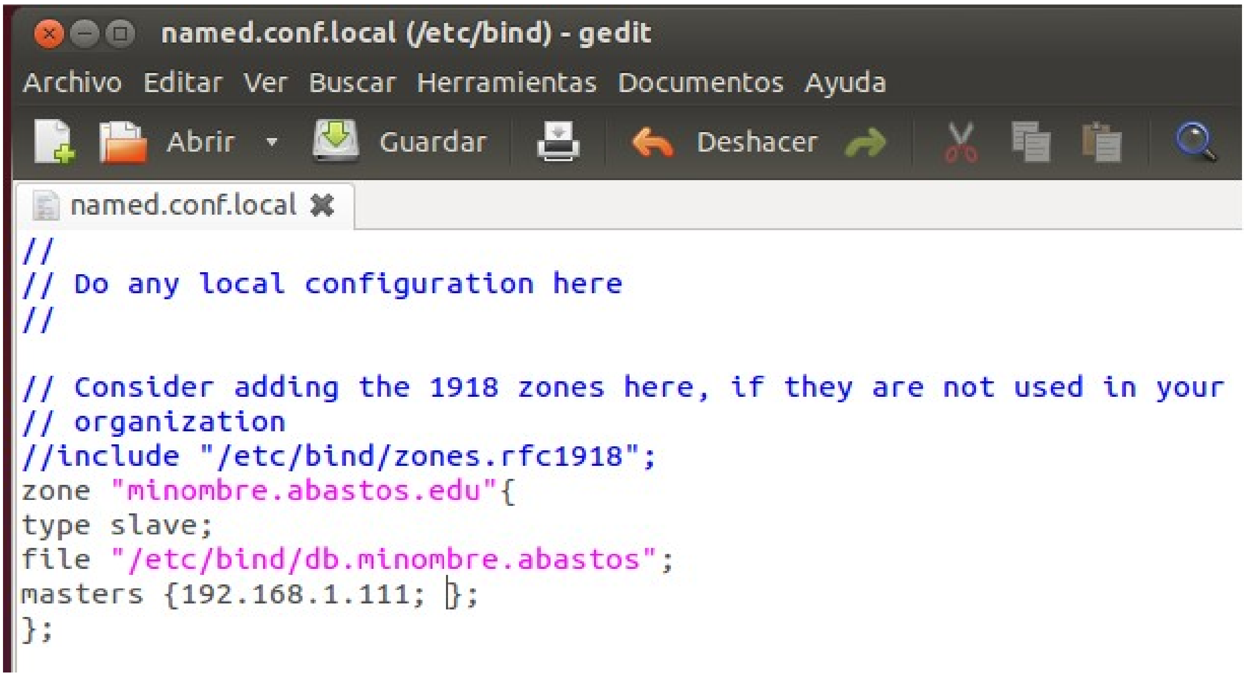
named-checkzone minombre.abastos.edu /etc/bind/db.minombre.abastos

8. Setting up a secondary DNS server

In most environments, it is a good idea to set up a secondary DNS server that will respond to requests if the primary becomes unavailable. A secondary DNS server is always up, and ready to serve. It can help balance the load on the network as there are now more than one authoritative place to get your information We are going to use our client VM as a secondary DNS server for our zone. So that, it is necessary to install bind9 on client VM.

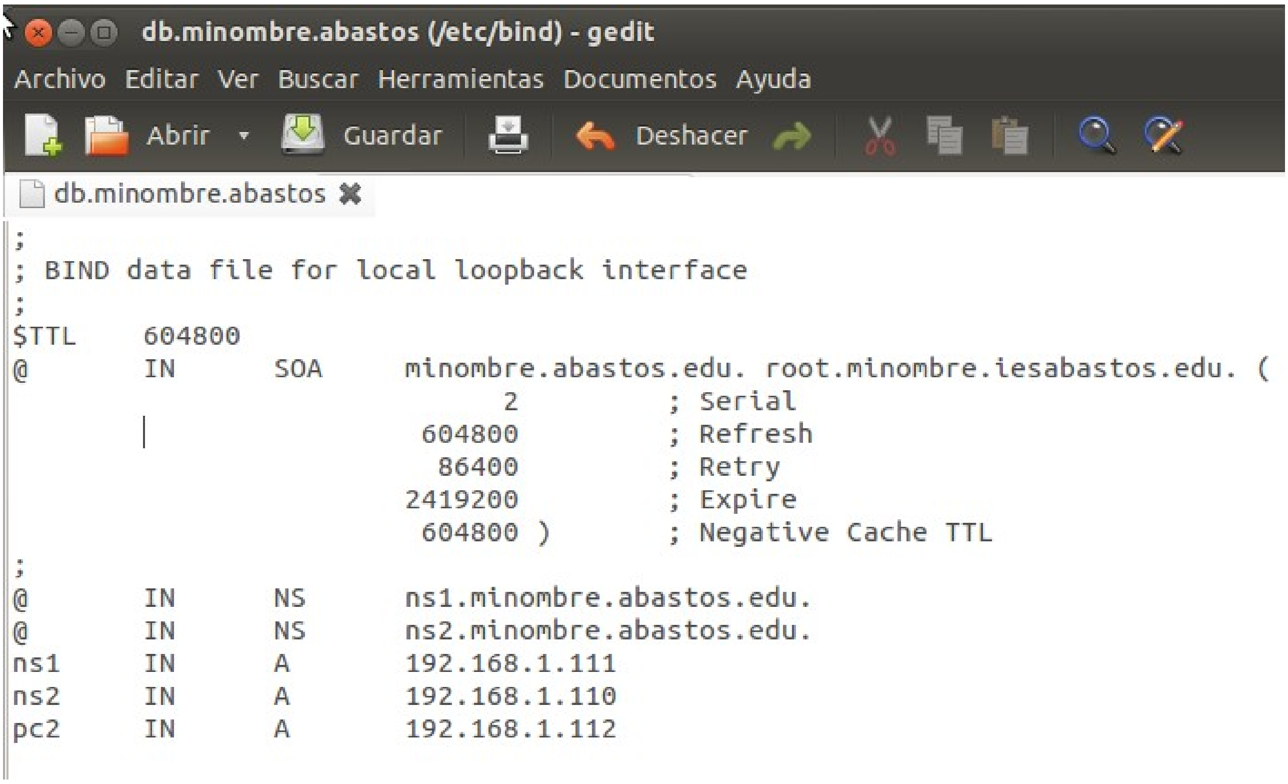
Luckily, the secondary DNS server is much easier to configure. We need to do some changes in both primary DNS server and secondary DNS server.

1. Client VM: Edit named.conf.local file and define slave zones that correspond to the master zones on the primary DNS server. Note that the type is "slave", the file, and there is a masters directive which should be set to the primary DNS server's private IP.


named.conf.local (/etc/bind) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Abrir
Guardar
Deshacer
named.conf.local

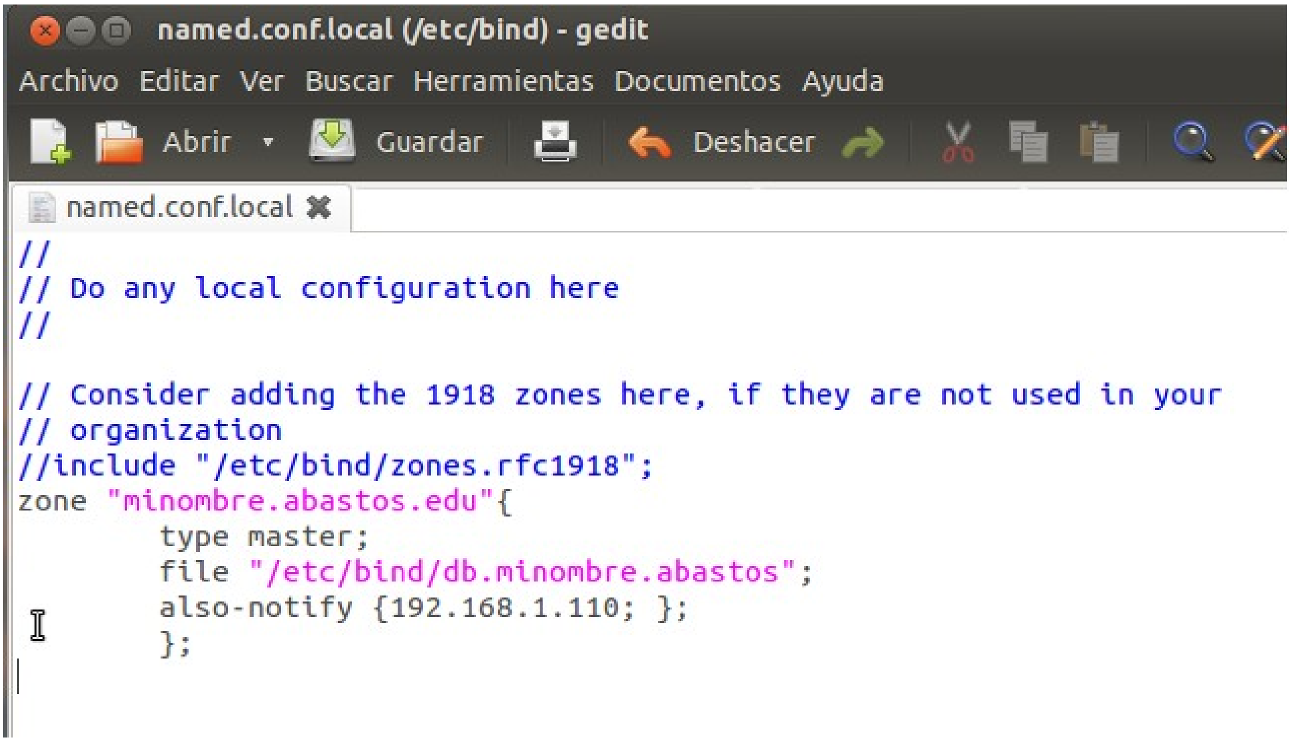
```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "minombre.abastos.edu"{
type slave;
file "/etc/bind/db.minombre.abastos";
masters {192.168.1.111; };
};
```

2. Server VM: add the new NS record in “db.minombre.abastos”. In this case pc1 is the secondary DNS server, we exchange the name “pc1” with the name “ns2”.


db.minombre.abastos (/etc/bind) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Abrir
Guardar
Deshacer
db.minombre.abastos

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     minombre.abastos.edu. root.minombre.iesabastos.edu. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns1.minombre.abastos.edu.
@       IN      NS      ns2.minombre.abastos.edu.
ns1     IN      A       192.168.1.111
ns2     IN      A       192.168.1.110
pc2     IN      A       192.168.1.112
```

Finally edit the /etc/bind/named.conf.local file in the master DNS server, use the also-notify directive which should be set to the secondary DNS server's private IP.


named.conf.local (/etc/bind) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Abrir
Guardar
Deshacer
named.conf.local

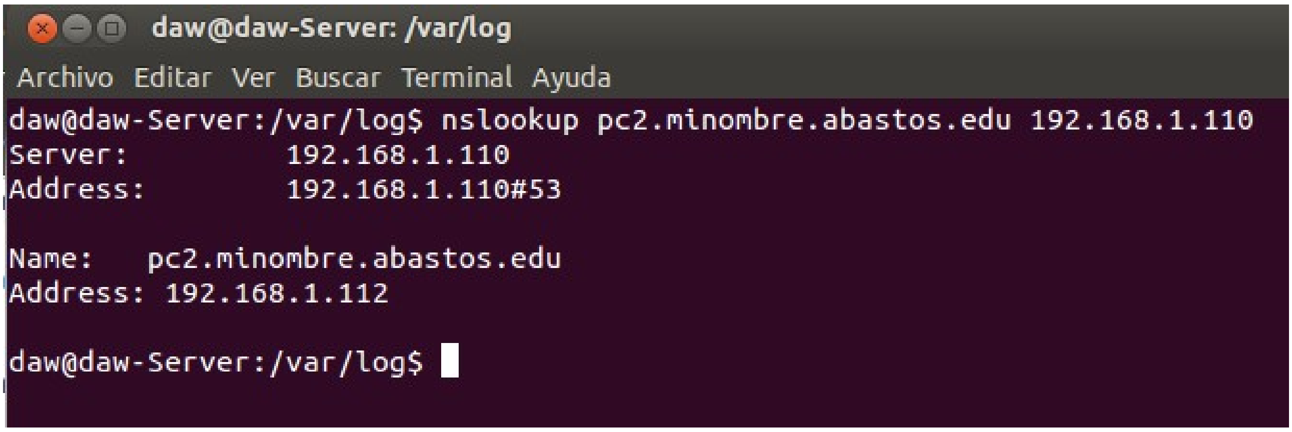
```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "minombre.abastos.edu"{
        type master;
        file "/etc/bind/db.minombre.abastos";
        also-notify {192.168.1.110; };
        };
```

Remember that whenever we make a change in /etc/bind/abastos.db we must increment the *serial* value before restarting the service.

Before checking the secondary DNS server, make sure the zone information has been transferred from primary to secondary dns server and stop the primary server.

ie Run the following command from a third party host.

nslookup pc2.minombre.abastos.edu 192.168.1.110

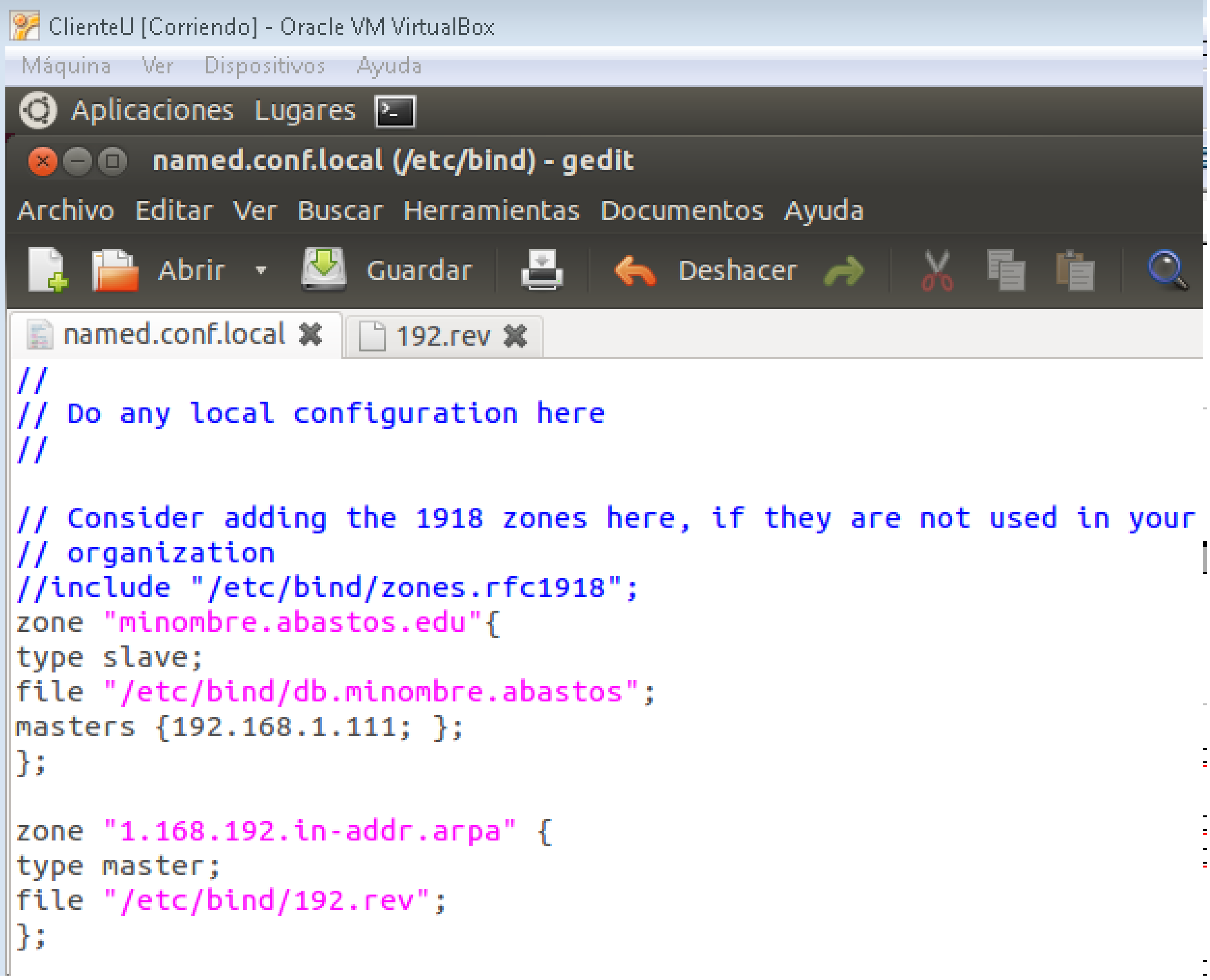


```
daw@daw-Server:/var/log$ nslookup pc2.minombre.abastos.edu 192.168.1.110
Server:         192.168.1.110
Address:        192.168.1.110#53

Name:   pc2.minombre.abastos.edu
Address: 192.168.1.112

daw@daw-Server:/var/log$
```

9. Create Reverse Zone File

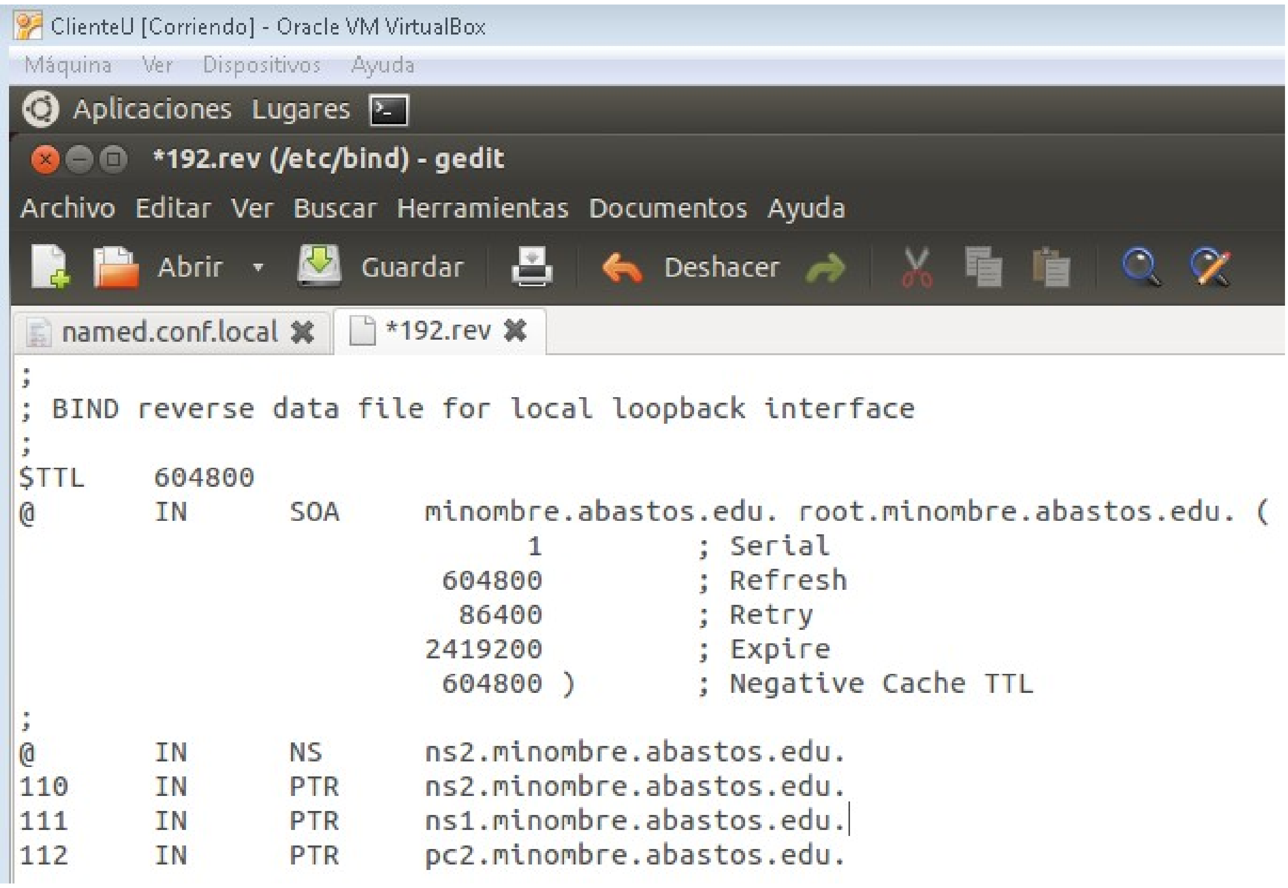
Reverse zone file are where we define DNS PTR records for reverse DNS lookups. That is, when the DNS receives a query by IP address, "192.168.1.112" for example, it will look in the reverse zone file(s) to resolve the corresponding FQDN, "pc2.minombre.abastos.edu" in this case.

The primary dns server for the reverse zone will be the client vm. For each reverse zone specified in the named.conf.local file, create a reverse zone file. The name of the reverse zone is “1.168.192.in-addr.arpa”.


ClienteU [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
Aplicaciones Lugares
named.conf.local (/etc/bind) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Abrir
Guardar
Deshacer
named.conf.local
192.rev

```
//
// 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 "minombre.abastos.edu"{
type slave;
file "/etc/bind/db.minombre.abastos";
masters {192.168.1.111; };
};

zone "1.168.192.in-addr.arpa" {
type master;
file "/etc/bind/192.rev";
};
```

We will base our reverse zone file(s) on the sample `db.127` zone file. Copy it to the proper location with the proper name, in this case “/etc/bind/191.rev”. We will add the NS record and the PTR records to it.

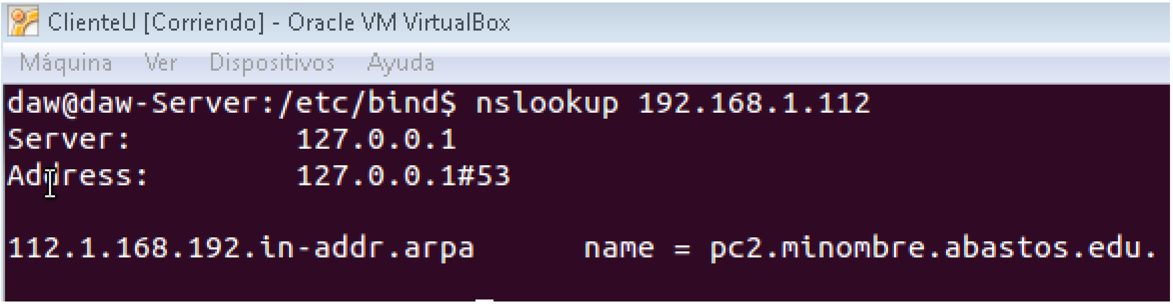

ClienteU [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
Aplicaciones Lugares
*192.rev (/etc/bind) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Abrir Guardar Deshacer
named.conf.local
*192.rev

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     minombre.abastos.edu. root.minombre.abastos.edu. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns2.minombre.abastos.edu.
110     IN      PTR     ns2.minombre.abastos.edu.
111     IN      PTR     ns1.minombre.abastos.edu.
112     IN      PTR     pc2.minombre.abastos.edu.
```

After these changes, restart the DNS servers and check the reverse resolution

ie

nslookup 192.168.1.112


ClienteU [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda

```
daw@daw-Server:/etc/bind$ nslookup 192.168.1.112
Server:         127.0.0.1
Address:        127.0.0.1#53

112.1.168.192.in-addr.arpa      name = pc2.minombre.abastos.edu.
```

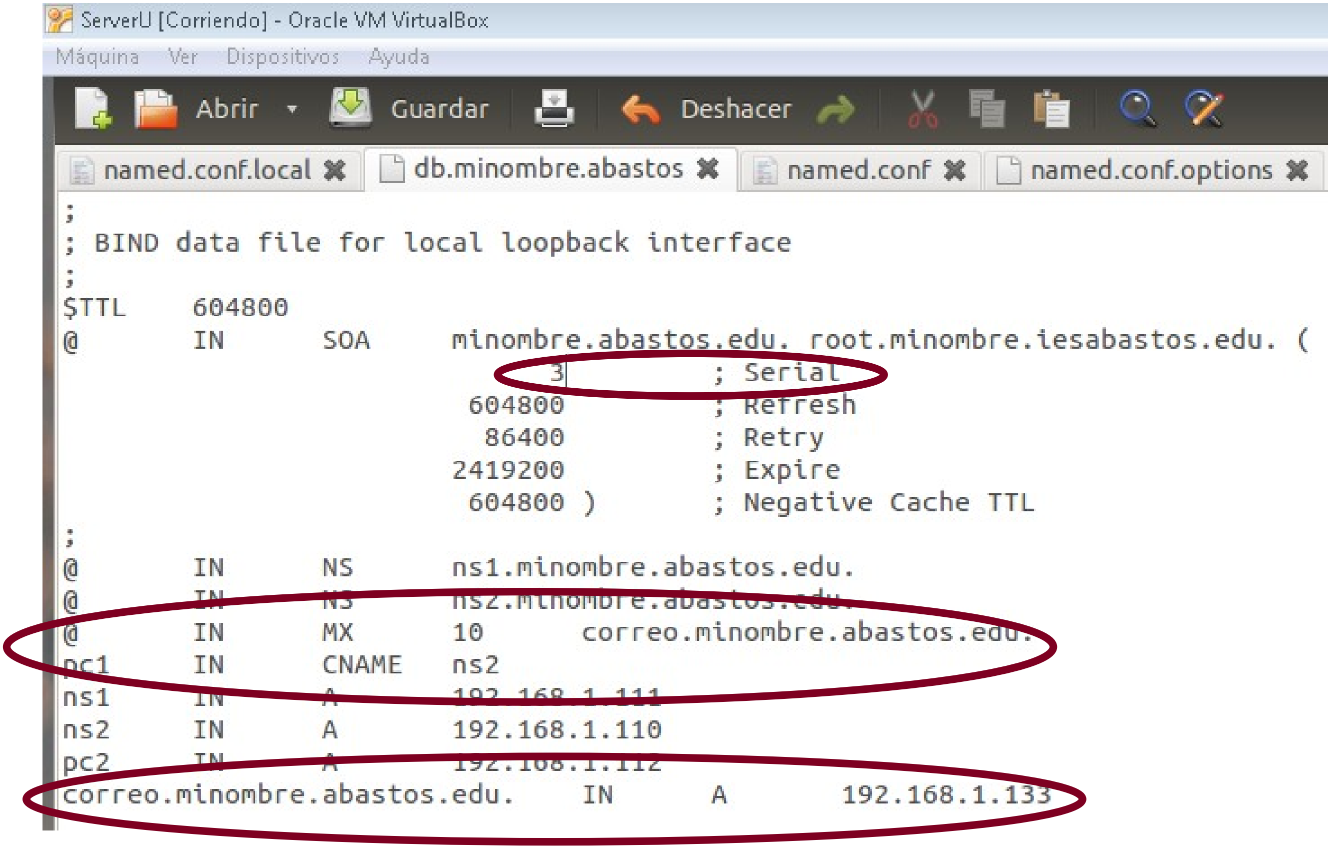
10. Maintaining DNS Records

We need to maintain our DNS records so that they accurately reflect our server environment.

Now we are going to modify the db.minombre.abastos file to add:

- a mail server, mail.minombre.abastos.edu with 192.168.1.133 ip address

- an alias from ns2.minombre.abastos.edu to pc1.minombre.abastos.edu.
- increment the value of "Serial"



```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     minombre.abastos.edu. root.minombre.iesabastos.edu. (
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns1.minombre.abastos.edu.
@       IN      NS      ns2.minombre.abastos.edu.
@       IN      MX      10      correo.minombre.abastos.edu.
pc1     IN      CNAME   ns2
ns1     IN      A       192.168.1.111
ns2     IN      A       192.168.1.110
pc2     IN      A       192.168.1.112
correo.minombre.abastos.edu.    IN      A       192.168.1.133
```

Check the resolution process for the new records in the secondary dns server

ie

nslookup correo.minombre.abastos.edu 192.168.1.110