esprit
Se former autrement
HONORIS UNITED UNIVERSITIES

Install & Configure Bind DNS Server on Ubuntu

Services et Administration des Réseaux

2024-2025

Introduction :

A DNS (Domain Name Service) is used for domain name resolution into an IP address. This means that a domain name is associated with an IP address. DNS servers allow the transformation of complicated IP addresses into easily memorable domain names. For example, the IP address 172.217.22.131 corresponds to the domain name google.fr, which is much easier to remember.

Goals :

In this lab, we will install and configure a DNS server using Bind 9, which will manage the "esprit1.com" zone along with with its reverse zone.

Additionally, we will cover the integration between the DNS server and a web server.

Step 1- Install the latest updates

Before we install any packages, we will first update download and install the latest updates with the apt update and apt upgrade commands :

```
sudo su

apt update -y && apt upgrade -y
```

Step 2- Disable firewall

```
sudo systemctl stop ufw
```

Step 3- Install BIND 9 on the DNS server

Download the necessary packages from Ubuntu base :

Next, we're going to install three packages on our DNS server :

• bind9 - The BIND 9 DNS server software.

• bind9utils - Utilities that make working with BIND 9 easier.

• bind9-doc - A documentation package for BIND 9.

```
sudo apt install -y bind9 bind9utils bind9-doc dnsutils
```

After installation, the BIND 9 service should be running. We check the status with this command :

```
sudo systemctl status bind9
```

Step 4- Edit the named.conf.options file

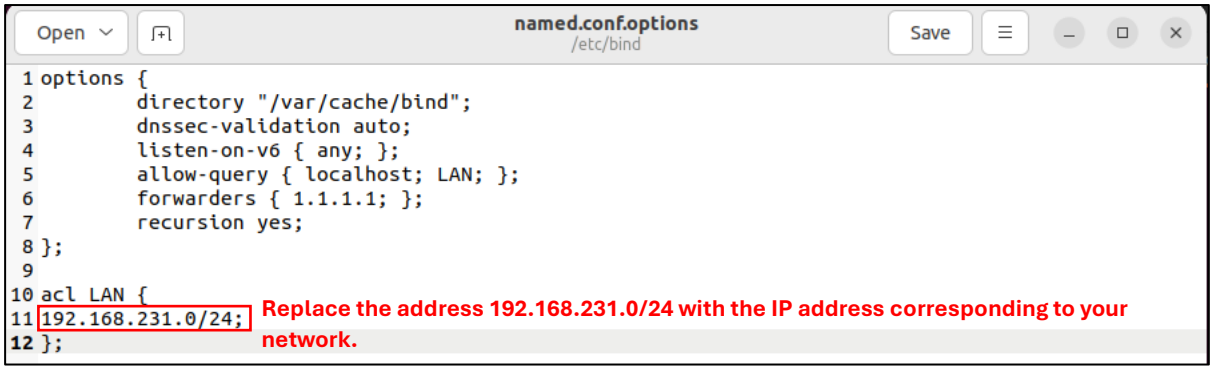
The named.conf file is BIND 9's main configuration file.

You'll make four modifications to the /etc/bind/named.conf.options file :

- An **acl** directive that defines our local area network (LAN).
- An **allow-query** directive that defines what IP addresses can send DNS queries to the server.
- A **forwarders** directive that defines what DNS servers this server will forward recursive queries to.
- A **recursion** directive that allows recursive DNS queries to the server.

To make those changes, open /etc/bind/named.conf.options in a text editor and modify the files to look similar to this:

sudo gedit /etc/bind/named.conf.options



After you make the changes, check the syntax of the file with the named-checkconf command :

sudo named-checkconf /etc/bind/named.conf.options

➔ **Note : If the syntax is correct, the command should not return any output.**

Now update named service

sudo named -V

sudo ss -lnptu | grep named

sudo systemctl restart named

sudo systemctl enable named

Step 5- Edit the named.conf.local file

The named.conf.local is typically used to define local DNS zones for a private domain. We will update this file to include our forward and reverse DNS zones.

To make the changes, open /etc/bind/named.conf.local in a text editor :

```
sudo gedit /etc/bind/named.conf.local
```

The named-checkconf command is used to check if the syntax is okay or if there is any error.

The command should return to shell if there is no error.

```
sudo named-checkconf
```

Step 6- Create a directory for your zone files

Next, we'll create a directory to store the zone files we specified in the previous step.

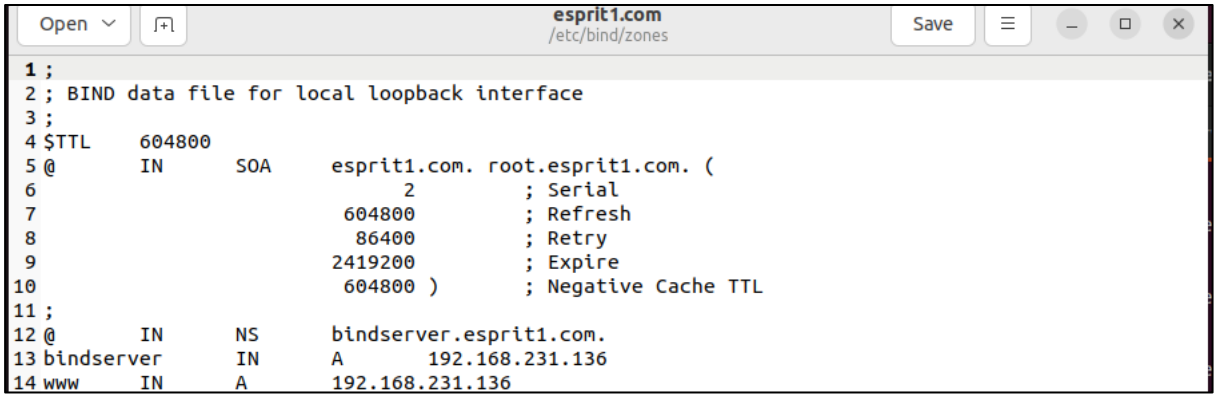
```
sudo mkdir /etc/bind/zones
```

Step 7- Create the forward zone file

First, copy the default db.local zone file to /etc/bind/zones/db.esprit1.com

```
sudo cp /etc/bind/db.local /etc/bind/zones/esprit1.com

sudo gedit /etc/bind/zones/esprit1.com
```



The acronyms on the file have the following description :

• SOA – Start of Authority

• NS – Name Server

• A – A record

• MX – Mail for Exchange

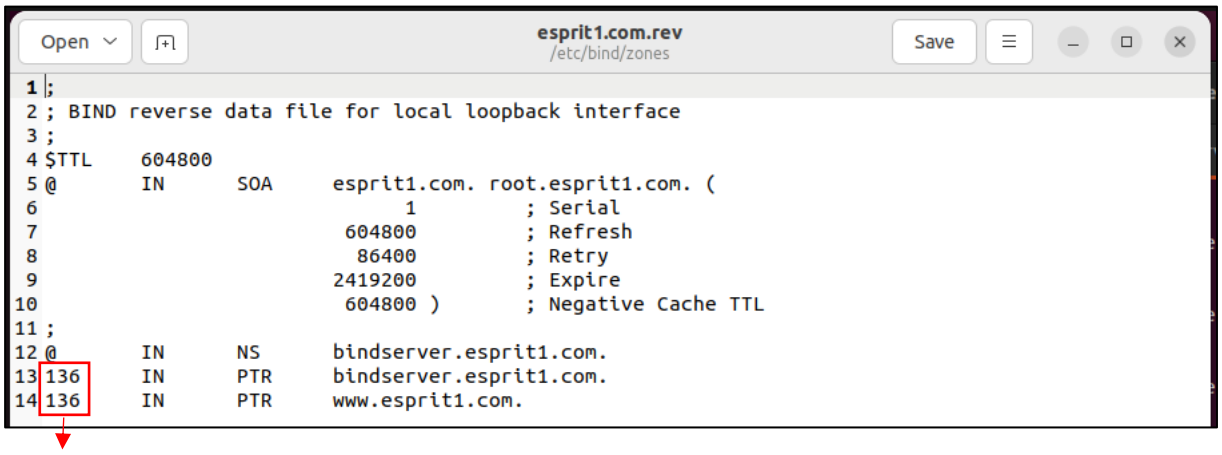
• CN – Canonical Name

Step 8- Create the reverse zone file

First, copy the default db.127 zone file to /etc/bind/zones/esprit1.com.rev

sudo cp /etc/bind/db.127 /etc/bind/zones/esprit1.com.rev

sudo gedit /etc/bind/zones/esprit1.com.rev



136 corresponds to the last octet of the server's IP address. Replace it with the one from your own IP address.

Note : The acronyms in the revese zone file are :

• PTR – Pointer

• SOA – Start of Authority

Step 9- Check BIND DNS syntax

The named-checkzone command is used to check the syntax of the forward and reverse zone files :

- Forward zone file

sudo named-checkzone esprit1.com /etc/bind/zones/esprit1.com

You should see output similar to :

```
server@server-virtual-machine:~/Desktop$ sudo named-checkzone esprit1.com /etc/bind/zones/esprit1.com
zone esprit1.com/IN: loaded serial 2
OK
```

- Reverse zone file

sudo named-checkzone esprit1.com.rev /etc/bind/zones/esprit1.com.rev

```
server@server-virtual-machine:~/Desktop$ sudo named-checkzone esprit1.com.rev /etc/bind/zones/esprit1.com.rev
zone esprit1.com.rev/IN: loaded serial 1
OK
```

Step 10- Restart BIND 9

To make the BIND DNS server use the new configuration, restart the restart the BIND 9 and named services the following commands :

sudo systemctl restart named

sudo systemctl restart bind9

Step 11- Testing the DNS Server

The dig command followed by the FQDN of our server allows us to test its proper functioning :

```
server@server-virtual-machine:~/Desktop$ sudo dig a www.esprit1.com @192.168.231.136

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> a www.esprit1.com @192.168.231.136
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7278
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 7265091c56e05ede0100000066f48e74c02f00f5e1e04fe5 (good)
;; QUESTION SECTION:
;www.esprit1.com.               IN      A

;; ANSWER SECTION:
www.esprit1.com.        604800  IN      A       192.168.231.136

;; Query time: 0 msec
;; SERVER: 192.168.231.136#53(192.168.231.136) (UDP)
;; WHEN: Wed Sep 25 23:28:04 CET 2024
;; MSG SIZE  rcvd: 88
```

You need to add the -x option to test the resolution from the reverse DNS zone :

```
server@server-virtual-machine:~/Desktop$ sudo dig -x 192.168.231.136 @192.168.231.136

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> -x 192.168.231.136 @192.168.231.136
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21446
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: e32d833fe56da3ae0100000066f48f5f0eaa59745158cccb (good)
;; QUESTION SECTION:
;136.231.168.192.in-addr.arpa.  IN      PTR

;; ANSWER SECTION:
136.231.168.192.in-addr.arpa. 604800 IN PTR     www.esprit1.com.

;; Query time: 0 msec
;; SERVER: 192.168.231.136#53(192.168.231.136) (UDP)
;; WHEN: Wed Sep 25 23:31:59 CET 2024
;; MSG SIZE  rcvd: 114
```

Step 12- Client configuration & Test

The /etc/resolv.conf file is a configuration file used to specify the DNS servers the system should query to resolve domain names into IP addresses.

Each line represents a DNS server that the system can use for name resolution. The DNS server listed on the first line is considered the priority, meaning the system will attempt to contact this server first. If it doesn't respond, the system will try the next server listed, and so on.

That’s why we will add our BIND9 DNS server at the top of the list.

1. To make the changes, open /etc/resolv.conf in a text editor and and modify the file :

sudo gedit /etc/resolv.conf

```
18 # See man:systemd-resolved.service(8) for details about the supported modes of
19 # operation for /etc/resolv.conf.
20
21 nameserver 192.168.231.136
22 nameserver 127.0.0.53
23 options edns0 trust-ad
24 search localdomain
```

2. Edit the /etc/hosts file and remove the entry for www.esprit1.com.

sudo gedit /etc/hosts

3. Run the web browser to test esprit1.com web site.