|  |  |
| --- | --- |
|  | |
| Titel  Ondertitel | |
| **Naam** | IT factory |
|  |
| Campus Geel, Kleinhoefstraat 4, BE-2440 Geel |

8865

Content

[Content 3](#_Toc41298628)

[DNS 4](#_Toc41298629)

[Install and configure DNS on Ubuntu 5](#_Toc41298630)

[1.1 Update System 5](#_Toc41298631)

[1.2 Install DNS package 5](#_Toc41298632)

[1.3 Install DNS Utilities 5](#_Toc41298633)

[2.1 Configuring the Options File 5](#_Toc41298635)

[2.2 Configuring the Local File 6](#_Toc41298636)

[2.3 Creating the Forward Zone File 7](#_Toc41298637)

[2.4 Creating the Reverse Zone File(s) 8](#_Toc41298638)

[2.5 Restarting BIND 9](#_Toc41298639)

# DNS

Each website has its own IP number, a number like 72.121.183.70. Such numbers are not really easy to remember. That's why a name is attached to them, think of www.bol.com. Domain Name Servers (DNS) keep track of which website name belongs to which IP number. A DNS service translates a requested web address into the IP address of the server on which the website runs.

Therefore we will install and configure DNS on Ubuntu in this documentation. Through this documentation we will use one of the most commonly used programs to handle the name server BIND (abbreviation of Berkley Internet Naming Daemon) on Ubuntu.

# Install and configure DNS on Ubuntu

Before starting the installation process, make sure the system is updated by performing the following three commands.

## Update System

* sudo apt-get update
* sudo apt-get upgrade
* sudo reboot

## Install DNS package

Once you execute the previous command it will suggest some other packages to be installed, press y to confirm downloading and installing those packages.

* sudo apt-get install bind9

## Install DNS Utilities

Another useful package that will help you a lot in troubleshooting and testing the DNS issues is the dnsutils package that can be installed using the next command.

* sudo apt-get install dnsutils



**Configuring the DNS Server**

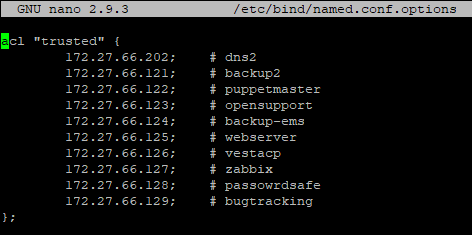
The BIND configuration contains several files that are included in the main configuration file named .conf. These file names start with named because this is the name of the process that BIND performs (abbreviation of "domain name daemon"). We first configure the option file.

## Configuring the Options File

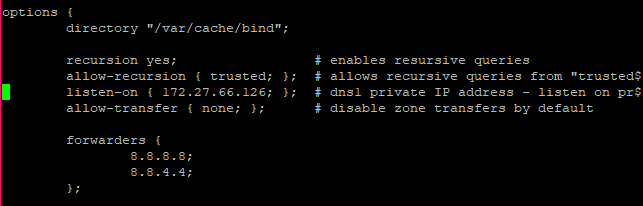
Open the named.conf.options file for editing:

* sudo nano /etc/bind/named.conf.options

Create a new ACL block (Access Control List) called "Trusted" above the existing option block. Here we will define a list of clients to allow recursive DNS queries.



Now that we have our list of trusted DNS clients, we will want to edit the options block. Below the directory directive, add the highlighted configuration lines so it looks something like this:



When you're done, save the file named.conf.options and close it. The above configuration shows that only your own server ("trusted" server) can query the external domain in the DNS server.

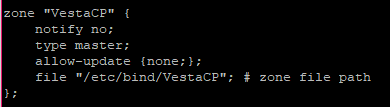
## Configuring the Local File

Open the named.conf.local file for editing:

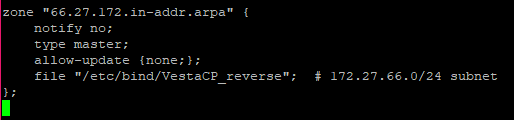
* nano /etc/bind/named.conf.local

Except for a few comments, the file should be empty. Here we will specify the forward and backward areas. The DNS zone specifies a specific space for managing and defining DNS records. Since our domains all belong to the "VestaCP" subdomain, we use it as the forwarding area. Since the special IP addresses of our servers are located in the 172.27.66.0/24-IP space, we will set up a reverse zone so that we can define reverse lookups within this range.

Add the forward zone with the following lines:



Assuming that our private subnet is 172.27.66.0/24, add the reverse zone by with the following lines:



Now that our zones are specified in BIND, we need to create the corresponding forward and reverse zone files.

## Creating the Forward Zone File

In the forward zone file we define DNS records for forward DNS lookup. That is, when DNS receives a name query, e.g. "webserver.VestaCP", it will search the forward zone file to resolve the corresponding host 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 commands:

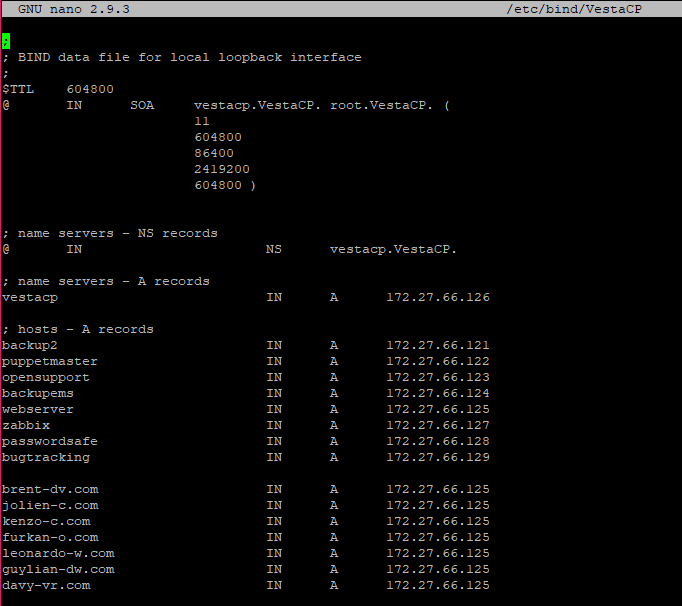
* sudo cp /etc/bind/db.local /etc/bind/VestaCP
* sudo nano /etc/bind/VestaCP

First, you will want to edit the SOA record. Replace the first “localhost” with vestacp FQDN, then replace “root.localhost” with “root.vestacp.”.

Next, delete the three records at the end of the file (after the SOA record).

At the end of the file, use the following lines to add a name server record (replace the name with your own). Keep in mind that the second column indicates that these are "NS" records:

Now add A records for the hosts belonging to the zone. This includes all the servers we want to terminate with "vestacp.VestaCP.". (Replace the name and special IP address).



Save and close the file.

## Creating the Reverse Zone File(s)

In the reverse zone file, we define DNS PTR records for reverse DNS lookups. That is, when DNS receives a query for each IP address, such as "172.27.66.125", it will look in the reverse zone file to resolve the corresponding FQDN (in this case, "webserver.VestaCP") .

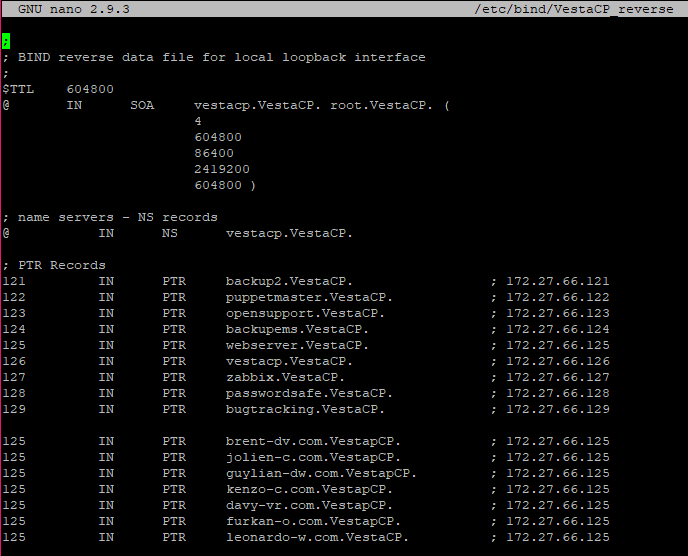
On dns1 , create a reverse zone file for each reverse zone specified in the named.conf.local file. We build a reverse zone file based on the example db.127 zone file. Use the following command to copy it to the correct location (replace the target file name to match your reverse zone definition):

* sudo cp /etc/bind/db.127 /etc/bind/VestaCP\_reverse
* sudo nano /etc/bind/VestaCP\_reverse

In the same manner as the forward zone file, you will want to edit the SOA record.

Now delete the two records at the end of the file (after the SOA record). Use the following lines at the end of the file to add a name server record. Keep in mind that the second column indicates that these are "NS" records:

Then add PTR records for all servers whose IP addresses are in the subnet of the zone file you are editing. In our example, this includes all our hosts because they are all in the subnet 172.27.66.0/24. Please note that the first column consists of the last octet of the server's private IP address, in reverse order.



Save and close the reverse zone file.

## Restarting BIND

Restart BIND:

* sudo systemctl restart bind9

If you have the UFW firewall configured, open up access to BIND by typing:

* sudo ufw allow Bind9

Your DNS server is now setup and ready to respond to DNS queries.