**Configure a master name server.**

**Presentation**

Installing a master **DNS** server will bring you several advantages:

* you define machine names one for all in a centralized way, you can then better organize your workshops, build machines dedicated to a specific task (**NFS** server, **LDAP** server, etc),
* you don’t need to regularly edit the **/etc/hosts** file of each of them,
* you can use the machine names everywhere in an efficient way,
* you can now test postfix labs through **MX** records (**M**ail e**X**change).

Besides making conversion between IP address and names, the **DNS** service provides the infrastructure necessary for mail management through the **MX** records: for a given domain name, mails coming are sent to servers owning a **MX** record.

Let’s install a **DNS** server for the **example.com** domain. Here, the **DNS** service is installed on a server called **dns.example.com** with an IP address of **192.168.1.5**.

**Procedure**

Install the **bind** package:

# **yum install -y bind**

Edit the **/etc/named.conf** file and change the **listen-on** option from **127.0.0.1** to **any**:

**listen-on port 53 { any; };**

In the same file, change the **allow-query** option from **localhost** to **any**:

**allow-query { any; };**

In the same file, disable the **dnssec-validation** option:

**dnssec-validation no;**

Still in the same file, below the **recursion** option, add the two following lines (with **192.168.1.1** being the **DNS** IP address of your Internet provider):

**forward only;**

**forwarders { 192.168.1.1; };**

After the **logging** stanza and still in the **/etc/named.conf** file, add the following lines (**example.com** is supposed to be your domain name):

**zone "example.com" {**

**type master;**

**file "example.com.zone";**

**allow-update { none; };**

**};**

**zone "1.168.192.in-addr.arpa" {**

**type master;**

**file "example.com.revzone";**

**allow-update { none; };**

**};**

Create the **/var/named/example.com.zone** file and insert the following lines (where **gateway** is your gateway to Internet, **dns** your **DNS** server, **mail** your mail server and **client** a simple client):

**$TTL 86400**

**@ IN SOA dns.example.com. root.example.com. (**

***2014080601* ; Serial**

**1d ; refresh**

**2h ; retry**

**4w ; expire**

**1h ) ; min cache**

**IN NS dns.example.com.**

**IN MX 10 mail.example.com.**

**gateway IN A 192.168.1.1**

**dns IN A 192.168.1.5**

**master IN CNAME dns.example.com.**

**mail IN A 192.168.1.10**

**client IN A 192.168.1.15**

Note1: **IN NS** indicates a name server, **IN MX** a mail server.  
Note2: It is a good practice to put the date in the **Serial** field and increase it (only the last two digits) when changes are required (if you don’t increase them, no changes will be taken into account even after restarting the **named** service).  
Note3: It is possible to assign the same IP address to several names by using a **CNAME** record (**C**anonical **NAME**). However, only one name, the canonical name, will be sent back for this IP address. This feature allows a lot of flexibility when setting up service configuration: here the same server can be called **dns.example.com** or **master.example.com** according to the situation. The services may be later spread over two different machines if needed without any changes on the client side.

Create the **/var/named/example.com.revzone** file and insert the following lines:

**$TTL 86400**

**@ IN SOA dns.example.com. root.example.com. (**

***2014080601* ; Serial**

**1d ; refresh**

**2h ; retry**

**4w ; expire**

**1h ) ; min cache**

**IN NS dns.example.com.**

**1 IN PTR gateway.example.com.**

**5 IN PTR dns.example.com.**

**10 IN PTR mail.example.com.**

**15 IN PTR client.example.com.**

Check the configuration files:

# **named-checkconf**

**Alternatively**, you can check your zone files:

# **named-checkzone example.com /var/named/example.com.zone**

**zone example.com/IN: loaded serial 2014080601**

**OK**

# **named-checkzone 1.168.192.in-addr.arpa /var/named/example.com.revzone**

**zone 1.168.192.in-addr.arpa/IN: loaded serial 2014080601**

**OK**

If **Firewalld** is running, add the new service to the firewall and reload the configuration:

# **firewall-cmd --permanent --add-service=dns**

Success

# **firewall-cmd --reload**

Success

Note: For performance reasons, when protecting a **production** master **DNS** server, it is recommended to use **Iptables** rather than **Firewalld** (see details [here](https://www.spinics.net/lists/centos/msg165363.html)).

Activate the **DNS** service at boot and start it:

# **systemctl enable named && systemctl start named**

Check the configuration:

# **nslookup cnn.com 127.0.0.1**

Server:        127.0.0.1

Address:    127.0.0.1#53

Non-authoritative answer:

Name:    cnn.com

Address: 157.166.226.25

Name:    cnn.com

Address: 157.166.226.26

# **dig @127.0.0.1 cnn.com**

; <<>> DiG 9.9.4-RedHat-9.9.4-14.el7 <<>> @127.0.0.1 cnn.com

; (1 server found)

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41414

;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 13, ADDITIONAL: 13

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 4096

;; QUESTION SECTION:

;cnn.com.            IN    A

;; ANSWER SECTION:

cnn.com.        152    IN    A    157.166.226.26

cnn.com.        152    IN    A    157.166.226.25

;; AUTHORITY SECTION:

com.            125267    IN    NS    c.gtld-servers.net.

com.            125267    IN    NS    i.gtld-servers.net.

com.            125267    IN    NS    a.gtld-servers.net.

com.            125267    IN    NS    k.gtld-servers.net.

com.            125267    IN    NS    f.gtld-servers.net.

com.            125267    IN    NS    m.gtld-servers.net.

com.            125267    IN    NS    l.gtld-servers.net.

com.            125267    IN    NS    d.gtld-servers.net.

com.            125267    IN    NS    j.gtld-servers.net.

com.            125267    IN    NS    e.gtld-servers.net.

com.            125267    IN    NS    g.gtld-servers.net.

com.            125267    IN    NS    b.gtld-servers.net.

com.            125267    IN    NS    h.gtld-servers.net.

;; ADDITIONAL SECTION:

i.gtld-servers.net.     9799    IN    A    192.43.172.30

m.gtld-servers.net.     5154    IN    A    192.55.83.30

f.gtld-servers.net.    11700    IN    A    192.35.51.30

d.gtld-servers.net.    16095    IN    A    192.31.80.30

g.gtld-servers.net.     5325    IN    A    192.42.93.30

h.gtld-servers.net.     5345    IN    A    192.54.112.30

j.gtld-servers.net.     5108    IN    A    192.48.79.30

c.gtld-servers.net.    13522    IN    A    192.26.92.30

l.gtld-servers.net.     6529    IN    A    192.41.162.30

e.gtld-servers.net.     6040    IN    A    192.12.94.30

k.gtld-servers.net.    10294    IN    A    192.52.178.30

b.gtld-servers.net.     3807    IN    AAAA 2001:503:231d::2:30

;; Query time: 70 msec

;; SERVER: 127.0.0.1#53(127.0.0.1)

;; WHEN: Wed Aug 06 13:00:29 CEST 2014

;; MSG SIZE  rcvd: 496