NCS 490:
DNS

By: Tony Perez

November 14, 2014

Abstract

For this lab we learned how to setup a DNS server. We had two DNS servers a master and a slave for redundancy. Although for our purpose we did not need two DNS servers it is a good practice to usually have two setup up for load balancing, as a backup, and in some cases for better routing. Domain Name Service (DNS) is used to translate an IP address to a host name or a host name to an IP address. Although our ISP or Google have a DNS server in which we could use we wanted a local DNS so we could use domain names instead of IP address on our LAN. There are other benefits to having your own DNS like caching and blocking unwanted websites or certain IP addresses.

1 Introduction

For our DNS servers we setup a primary and a secondary. They are each on one VM. We needed out DNS servers to cache the domain names we have already used and need to be able to talk to our machines using domain names and not our IP addresses. We also needed our primary, master, DNS server to replicate its zone files to our secondary, slave, DNS server.

2 Installation of BIND

BIND is an open source software that we will use to implement DNS on our servers.
To do this we installed BIND:

```
# yum install bind bind-utils -y
```

Once installed we needed to configure the **/etc/named.conf** file and make two zone files, one is our forward zone file and the other is our reverse zone file. I called the forward zone file: **tonyDNS.com.zone** and the reverse zone file: **tonyDNS.com.rr.zone**. We make these in our primary DNS server and in the location: **/var/named/**.

```
10 options {
11         listen-on port 53 { 127.0.0.1; 10.103.67.80; };
12         listen-on-v6 port 53 { ::1; };
13         directory       "/var/named";
14         dump-file       "/var/named/data/cache_dump.db";
15         statistics-file "/var/named/data/named_stats.txt";
16         memstatistics-file "/var/named/data/named_mem_stats.txt";
17         allow-query     { localhost; 10.103.67.80; };
18         allow-transfer  { localhost; 10.103.67.81; };
19         recursion yes;
20
21         dnssec-enable yes;
22         dnssec-validation yes;
23         dnssec-lookaside auto;
24
25         forwarders {
26                 8.8.8.8;
27                 8.8.4.4;
28         };
29         forward only;
30
31         /* Path to ISC DLV key */
32         bindkeys-file "/etc/named.iscdlv.key";
33
34         managed-keys-directory "/var/named/dynamic";
35 };
```

Figure 1: Option configuration in named.conf file

As we can see in Figure 1 We edited lines 11, 17, 18, and 25-29. Lines 25-29 is where we want our DNS server to search if our DNS server does not have the domain names being looked up.

Figure 2: Zone configuration in named.conf

Figure 2 shows the zone entries we made. This is what we had to add to tell our DNS server where our zone files are located. Our zone files is where we insert the domain name and its matching IP address. Here we can also see that it is our master DNS server.

Our Forward zone file contains the domain names we want to use and matched them to an IP address. In my case I wanted to use dns1 as the domain name of my Primary DNS server and dns2 as the domain name of my secondary DNS server.

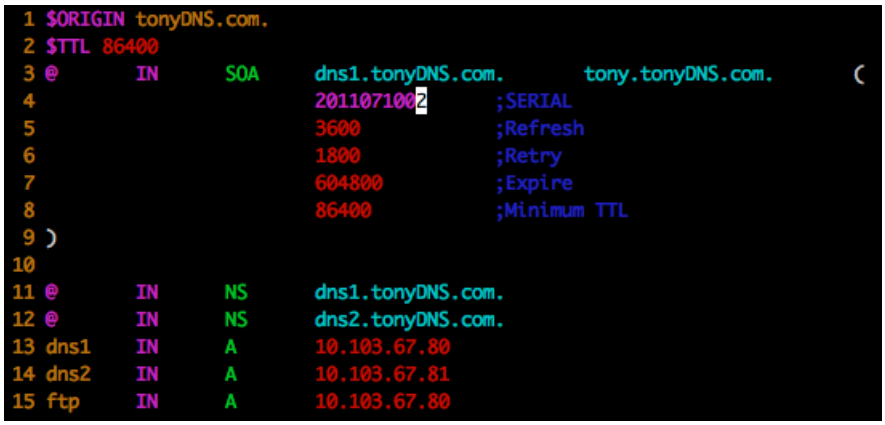

Figure 3: Forward Zone file

Our reverse zone file contains the same information but in reverse. Here we have an IP address matching the domain name in case we knew the IP address of a machine and wanted to find out its domain name.

```
1 $ORIGIN 67.103.10.in-addr.arpa.
2 $TTL 86400
3 @       IN      SOA     dns1.tonyDNS.com.       tony.tonyDNS.com. (
4                         2011071002      ;Serial
5                         3600            ;Refresh
6                         1800            ;Retry
7                         604800          ;Expire
8                         86400           ;Minimum TTL
9 )
10 @      IN      NS      dns1.tonyDNS.com.
11 @      IN      NS      dns2.tonyDNS.com.
12 80     IN      PTR     dns1.tonyDNS.com.
13 81     IN      PTR     dns2.tonyDNS.com.
14 80     IN      PTR     ftp.tonyDNS.com.
```

Figure 4: Reverse Zone file

On our secondary machine we only had to install BIND and edit the **/etc/named.conf** file. We had to use a slightly different configuration since it is a slave DNS server.

```
options {
        listen-on port 53 { 127.0.0.1; 10.103.67.81; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; 10.103.67.0/16; };
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;

        forwarders {
                8.8.8.8;
                8.8.4.4;
        };
        forward only;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";

        managed-keys-directory "/var/named/dynamic";
};
```

Figure 5: Machine 2 option section

Figure 6 shows that this DNS server is a slave and will gets its configuration file the master at **10.103.67.80**. This also tells where it will save its configuration files.

```
zone "tonyDNS.com" IN {
        type slave;
        masters { 10.103.67.80; };
        file "slaves/tonyDNS.com.zone";
};

zone "67.103.10.in-addr.arpa" IN {
        type slave;
        masters { 10.103.67.80; };
        file "slaves/tonyDNS.com.rr.zone";
};
```

Figure 6: Machine 2 zone seciton

Now on both machines we need to edit our **iptables** and allow DNS.

```
# iptables -A INPUT -p udp -m state --state NEW -m udp --dport 53 -j ACCEPT
# iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 53 -j ACCEPT
# iptables-save
```

We then restart our named service on both machines and then check our second machine to see if the zone files were replicated.

```
# service named restart
```

```
root@pereztr-2 ~ $ cat /var/named/slaves/tonyDNS.com.zone
$ORIGIN .
$TTL 86400      ; 1 day
tonyDNS.com             IN SOA  dns1.tonyDNS.com. tony.tonyDNS.com. (
                                2011071003 ; serial
                                3600       ; refresh (1 hour)
                                1800       ; retry (30 minutes)
                                604800     ; expire (1 week)
                                86400      ; minimum (1 day)
                                )
                        NS      dns1.tonyDNS.com.
                        NS      dns2.tonyDNS.com.
$ORIGIN tonyDNS.com.
dns1                    A       10.103.67.80
dns2                    A       10.103.67.81
ftp                     A       10.103.67.80
```

Figure 7: Machine 2 Forward zone file

```
root@pereztr-2 ~ $ cat /var/named/slaves/tonyDNS.com.rr.zone
$ORIGIN .
$TTL 86400      ; 1 day
67.103.10.in-addr.arpa  IN SOA  dns1.tonyDNS.com. tony.tonyDNS.com. (
                                2011071002 ; serial
                                3600       ; refresh (1 hour)
                                1800       ; retry (30 minutes)
                                604800     ; expire (1 week)
                                86400      ; minimum (1 day)
                                )
                        NS      dns1.tonyDNS.com.
                        NS      dns2.tonyDNS.com.
$ORIGIN 67.103.10.in-addr.arpa.
80                      PTR     dns1.tonyDNS.com.
                        PTR     ftp.tonyDNS.com.
81                      PTR     dns2.tonyDNS.com.
```

Figure 8: Machine 2 Reverse file

We did not need to create these files and input that information. It was copied from our master DNS server.

Now we change the DNS server address we use on our client machines to test to see if our DNS server work. I will use our first machine as the client and have it point to our second machine. We edit the **/etc/resolv.conf** file like so:

```
1 ; generated by /sbin/dhclient-script
2 ;search cs.sunyit.edu
3 search tonyDNS.com
4 ;nameserver 10.103.67.80
5 nameserver 10.103.67.81
6 nameserver 10.102.0.32
```

Next to test our DNS servers we ping to **dns1** and **dns2** to see if we can rech them.

```
root@pereztr-1 tony $ ping -c 5 dns1
PING dns1.tonyDNS.com (10.103.67.80) 56(84) bytes of data.
64 bytes from ftp.tonyDNS.com (10.103.67.80): icmp_seq=1 ttl=64 time=0.029 ms
64 bytes from ftp.tonyDNS.com (10.103.67.80): icmp_seq=2 ttl=64 time=0.075 ms
64 bytes from ftp.tonyDNS.com (10.103.67.80): icmp_seq=3 ttl=64 time=0.079 ms
64 bytes from ftp.tonyDNS.com (10.103.67.80): icmp_seq=4 ttl=64 time=0.075 ms
64 bytes from ftp.tonyDNS.com (10.103.67.80): icmp_seq=5 ttl=64 time=0.078 ms

--- dns1.tonyDNS.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.029/0.067/0.079/0.019 ms
root@pereztr-1 tony $ ping -c 5 dns2
PING dns2.tonyDNS.com (10.103.67.81) 56(84) bytes of data.
64 bytes from dns2.tonyDNS.com (10.103.67.81): icmp_seq=1 ttl=64 time=1.72 ms
64 bytes from dns2.tonyDNS.com (10.103.67.81): icmp_seq=2 ttl=64 time=0.543 ms
64 bytes from dns2.tonyDNS.com (10.103.67.81): icmp_seq=3 ttl=64 time=0.580 ms
64 bytes from dns2.tonyDNS.com (10.103.67.81): icmp_seq=4 ttl=64 time=0.282 ms
64 bytes from dns2.tonyDNS.com (10.103.67.81): icmp_seq=5 ttl=64 time=0.263 ms

--- dns2.tonyDNS.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.263/0.679/1.728/0.540 ms
```

Figure 9: Successful pings

Now we use the **nslookup** tool to query our DNS server for information on the domain name like so:

```
root@pereztr-1 tony $ nslookup dns1
Server:         10.103.67.81
Address:        10.103.67.81#53

Name:   dns1.tonyDNS.com
Address: 10.103.67.80

root@pereztr-1 tony $ nslookup dns2
Server:         10.103.67.81
Address:        10.103.67.81#53

Name:   dns2.tonyDNS.com
Address: 10.103.67.81
```

Figure 10: Looking up information on dns1

Now we will try and get information on Google's domain name:

```
root@pereztr-1 tony $ nslookup google.com
Server:         10.103.67.81
Address:        10.103.67.81#53

Non-authoritative answer:
Name:   google.com
Address: 74.125.225.32
Name:   google.com
Address: 74.125.225.33
Name:   google.com
Address: 74.125.225.40
Name:   google.com
Address: 74.125.225.46
Name:   google.com
Address: 74.125.225.39
Name:   google.com
Address: 74.125.225.41
Name:   google.com
Address: 74.125.225.34
Name:   google.com
Address: 74.125.225.37
Name:   google.com
Address: 74.125.225.35
Name:   google.com
Address: 74.125.225.36
Name:   google.com
Address: 74.125.225.38
```

3 Conclusion

In this lab we learn how to install and setup a DNS server. We will be using our DNS server to input domain names we will to use instead of the IP address.