Sri Lanka Institute of Information Technology

Faculty of Computing

Network Design & Management - IT3010

Practical 4 – Part 2

Main objective of this lab is to equip the students with knowledge on how to install and configure a DNS server in a Linux environment. In parallel students will gain knowledge on using yum install to install a package in Linux. Important that you have completed up to the last lab to perform the rest of the lab sheet.

STEP 01----------

. 1) Open the configuration files of the dns server.

[root@server ~]# vi /etc/named.conf

. Note: Root privilege is needed for the terminal.

. 2) Add two zone, one forward lookup zone and one reverse lookup zone for the named.conf file.

```
. //
. // named.conf
. //
. // Provided by Red Hat bind package to configure the ISC
  BIND named(8) DNS
. // server as a caching only nameserver (as a localhost
  DNS resolver only).
. //
. // See /usr/share/doc/bind*/sample/ for example named
  configuration files.
. //
. options {
. listen-on port 53 { 127.0.0.1; 10.0.1.5 };
. 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; 10.0.1.0/24 };
. recursion yes;
.
. dnssec-enable yes;
```

```
. dnssec-validation yes;
. dnssec-lookaside auto;
.
. /* Path to ISC DLV key */
. bindkeys-file "/etc/named.iscdlv.key";
.
. managed-keys-directory "/var/named/dynamic";
. };
. logging {
. channel default_debug {
. file "data/named.run";
. severity dynamic;
. };
. };
.
. zone "." IN {
. type hint;
. file "named.ca";
. };
.
. //forward look up zone
. zone"ns" IN {
. type master;
. file "forward.csa.lk";
. allow-update { none; };
. };
.
. //reverse look up zone
. zone"1.0.10.in-addr.arpa" IN {
. type master;
. file "reverse.csa.lk";
. allow-update { none; };
. };
.
. include "/etc/named.rfc1912.zones";
. include "/etc/named.root.key";
```

3) Save and close the file.

Note: You should be in your own network at this point.

STEP 02----------

. 4) To create the zone files change your directory as follows.

[root@server etc]# cd /var/named

. 5) Open a new file named forward.csa.lk in the named directory as follows to create the forward zone file for the DNS server.

[root@server named]# vi forward.csa.lk

. 6) Add the following lines of coding for the file

```
$TTL 86400
@       IN      SOA     mlb-dc1-centos7.csa.lk.         root.csa.lk.    (
                2011071001              ;Serial
                3600                    ;Refresh
                1800                    ; Retry
                604800                  ; Expire
                86400           )       ;Minimum TTL

@       IN      NS      mlb-dc1-centos7.csa.lk.
@       IN      A       10.0.1.5  //provide your server IP address
@       IN      A       10.0.1.10  //provide your client IP address
mlb-dc1-centos7         IN      A       10.0.1.5        //provide your server IP
address
<client hostname>       IN      A       10.0.1.6        //provide your client IP address
```

. 7) Save and close the file.

. 8) Open a new file named reverse.csa.lk in the named directory as follows to create the forward zone file for the DNS server.

[root@server named]# vi reverse.csa.lk

. 9) Add the following lines of coding for the file

```
. $TTL 86400
. @       IN      SOA     mlb-dc1-centos7.csa.lk.         root.csa.lk.    (
.               2011071001              ;Serial
.               3600                    ;Refresh
.               1800                    ; Retry
.               604800                  ; Expire
.               86400           )       ;Minimum TTL
.
. @ IN NS mlb-dc1-centos7.csa.lk.
. @ IN PTR csa.lk.
. server IN A 10.0.1.5 <-provide your server IP address
. client IN A 10.0.1.10 <-provide your server IP address
. 5 IN PTR mlb-dc1-centos7.csa.lk.
. 10 IN PTR <client hostname>.
```

10) Save and close the file

. 11) Read the following information and understand what the commands given, the configurations are being done for the zone files.

$TTL 86400

Sets the default Time to Live (TTL) value for the zone. This is the length of time, in seconds, that a zone resource record is valid. Each resource record can contain its own TTL value, which overrides this directive. Increasing this value allows remote nameservers to cache the zone information for a longer period of time, reducing the number of queries for the zone and lengthening the amount of time required to proliferate resource record changes. Zone File Resource Records The primary component of a zone file is its resource records. There are many types of zone file resource records. The following are used most frequently:

A - [mlb-dc1-centos7 IN A 10.0.1.5]

. This refers to the Address record, which specifies an IP address to assign to a name, as in this example: <host> IN A <IP-address>

If the <host> value is omitted, then an A record points to a default IP address for the top of the namespace. This system is the target for all non-FQDN requests.

Consider the following A record examples for the example.com zone file:

server1 IN A 10.0.1.3

IN A 10.0.1.5

Requests for example.com are pointed to 10.0.1.3 or 10.0.1.5.

NS – [@ IN NS mlb-dc1-centos7.csa.lk.]

This refers to the NameServer record, which announces the authoritative nameservers for a particular zone.

The following illustrates the layout of an NS record:

IN NS <nameserver-name>

Here, <nameserver-name> should be an FQDN.

Next, two nameservers are listed as authoritative for the domain. It is not important whether these nameservers are slaves or if one is a master; they are both still considered authoritative.

IN NS dns1.example.com.

IN NS dns2.example.com.

PTR - [5 IN PTR mlb-dc1-centos7.csa.lk.]

This refers to the PoinTeR record, which is designed to point to another part of the

namespace.

PTR records are primarily used for reverse name resolution, as they point IP addresses back to a particular name.

A reverse name resolution zone file is used to translate an IP address in a particular namespace into an FQDN. It looks very similar to a standard zone file, except that PTR resource records are used to link the IP addresses to a fully qualified domain name.

The following illustrates the layout of a PTR record:

<last-IP-digit> IN PTR <FQDN-of-system>

The <last-IP-digit> is the last number in an IP address which points to a particular system's FQDN.

```
SOA@IN      SOA    mlb-dc1-centos7.csa.lk.      root.csa.lk.    (
        2011071001              ;Serial
        3600                    ;Refresh
        1800                    ; Retry
        604800                  ; Expire
        86400           )       ;Minimum TTL
```

This refers to the Start Of Authority resource record, which proclaims important authoritative information about a namespace to the nameserver.

Located after the directives, an SOA resource record is the first resource record in a zone file.

The following shows the basic structure of an SOA resource record:

@ IN SOA <primary-name-server> <hostmaster-email> (

<serial-number>

<time-to-refresh>

<time-to-retry>

<time-to-expire>

<minimum-TTL>)

The @ symbol places the $ORIGIN directive (or the zone's name, if the $ORIGIN directive is not set) as the namespace being defined by this SOA resource record. The hostname of the primary nameserver that is authoritative for this domain is the <primary-name-server> directive, and the email of the person to contact about this namespace is the <hostmaster-email> directive.

The <serial-number> directive is a numerical value incremented every time the zone file is altered to indicate it is time for named to reload the zone. The <time-to-refresh> directive is the numerical value slave servers use to determine how long to wait before asking the master nameserver if any changes have been made to the zone. The <serial-number> directive is a numerical value used by the slave servers to determine if it is using outdated zone data and should therefore refresh it.

The <time-to-retry> directive is a numerical value used by slave servers to determine the length of time to wait before issuing a refresh request in the event that the master nameserver is not answering. If the master has not replied to a refresh request before the amount of time specified in the <time-to-expire> directive elapses, the slave servers stop responding as an authority for requests concerning that namespace.

The <minimum-TTL> directive is the amount of time other nameservers cache the zone's information.

5

STEP 03----------

12) Stop your name server service and dhcp service if they are runing

```
[root@server ~]#service dhcpd stop
[root@server ~]#service named stop
```

13) Open and edit dhcpd.conf file,

```
vi /etc/dhcp/dhcpd.conf
```

14) Make the changes as shown below(the highlighted area).

a. Set the domain name and domain-name servers:

```
[...]
```

```
# option definitions common to all supported networks...

option domain-name "csa.lk";

option domain-name-servers mlb-dc1-centos7.csa.lk;

[...]
```

b. Define the sunbet, range of ip addresses, domain and domain name servers like below:

```
[...]

A slightly different configuration for an internal subnet. subnet 10.0.1.0 netmask
255.255.255.0 {

#

. .

option domain-name-servers mlb-dc1-centos7.csa.lk;

. .

} [...]
```

Note: Keep the other original coding the same and just change the given area.

15) Save and close the file

STEP 04----------

16) You'll have to allow the DNS communication via the firewall of CentOS. For this you'll have add a firewall rule allowing UDP port 53. Change to root account and issue the command;

```
Firewall-cmd --permanent --add-port=53/udp
```

17) Load the new firewall rules to the CentOS firewall by issuing the command;

```
Firewall-cmd –reload
```

6

18) Test DNS configuration and zone files for any syntax errors as follows,

```
[root@server ~]# named-checkconf /etc/named.conf
```

Note: You should get the prompt back if there are no errors.

[root@server ~]# named-checkzone csa.lk /var/named/forward.csa.lk
Note: If there are no errors you should get zone csa.lk/IN: loaded serial 2011071001 OK

[root@server ~]# named-checkzone csa.lk /var/named/reverse.csa.lk
Note: If there are no errors you should get zone csa.lk/IN: loaded serial 2011071001 OK

19) Restart your dhcp service and dns services.

[root@server ~]#service dhcpd start
[root@server ~]]#service named start
Or
[root@server ~]#service dhcpd restart
[root@server ~]#service named restart

Note: If there are no errors in the zone files and the dhcp and dns configuration files both the operations should run smoothly.

STEP 05----------

20) Test DNS Server by using the following commands and check whether the input gets resolved correctly.

[root@server ~]# dig csa.lk
[root@server ~]# dig mlb-dc1-centos7.csa.lk
[root@server ~]# nslookup mlb-dc1-centos7.csa.lk
[root@server ~]# nslookup csa.lk

Note: You should get your server IP address resolved from the tests if the server is configured correctly.

7

STEP 06----------

21) Go to the Fedora client.

Note: Should be given the root privilege to perform any changes or configurations and you should be in your own network (vmNet2).

. 22) Restart its Network services as follows.

. [root@server ~]# service network restart

. 23) Use the hostname command, what is the hostname of the machine?

[root@localhost ~]# hostname

. 24) In order to change the hostname of the Fedora machine as client you have to follow up the same procedure as the server name changing that you performed in the DNS-Part 01 (Practical 5). Reopen the lab sheet and follow-up the same procedure except whenever we used the key word server at the server side you have to use the word client.

Note: Do not install DNS at the client side as well.

. 25) After changing the machine name add DNS server details on the client side resolv.conf file. [root@server ~]# vi /etc/resolv.conf

. # Generated by NetworkManager
. search mlb-dc1-centos7.csa.lk
. nameserver 10.0.1.5
.

. 26) Restart its Network services as follows.

. [root@server ~]# service network restart

. 27) Again, test DNS Server from the client side by using the following commands and check whether the input gets resolved correctly.

. [root@server ~]# dig csa.lk

. [root@server ~]# dig mlb-dc1-centos7.csa.lk
. [root@server ~]# nslookup mlb-dc1-centos7.csa.lk
. [root@server ~]# nslookup csa.lk
. Note: You should get your server IP address resolved from the tests if the server is configured correctly.

STEP 08 – DO THIS BY YOUR SELF----------

28) Try to specify new zones. forward look up zone. reverse lookup zone.

29) Try to start a service using the GUI options available.