Lab Exercise 5 – Remote NDC

Objective:
Be able to use Remote NDC (RNDC) to securely send control messages to a nameserver either remotely or locally.

Steps:

1. Use RNDC for the lab master name server. Under /var/named/master, generate the RNDC key using rndc-confgen and update named.conf to use it.

```
rndc-confgen
```

   This command requires a source of randomness. If it hangs, specify the source, which in normal case is /dev/urandom or /dev/random.

```
rndc-confgen –r /dev/urandom
```

   If you add the option –a, it will only generate the rndc.key.

   Note: By default named will look for the rndc.conf in /etc. You can create a symlink to the current location of your rndc.conf.

2. Cut the first part of the statement to rndc.conf and the second part, which has a comment (hash), to named.conf.

   Example:

   This is what goes to rndc.conf.

```
# Start of rndc.conf
key "rndc-key" {
      algorithm hmac-md5;
      secret "yVhKO3ioVnaMwyob39yAvw==";
};

options {
      default-key "rndc-key";
      default-server 127.0.0.1;
      default-port 953;
};
# End of rndc.conf
```

This goes to named.conf. Make sure to remove the comment starting from the "key" statement before using it.

```
# Use with the following in named.conf, adjusting the allow list as
needed:
# key "rndc-key" {
#     algorithm hmac-md5;
#     secret "yVhKO3ioVnaMwyob39yAvw==";
# };
#
# controls {
#     inet 127.0.0.1 port 953
#           allow { 127.0.0.1; } keys { "rndc-key"; };
# };
# End of named.conf
```

You could also place the second part to a file then use "include" statement in your named.conf to specify that file.

Example:

```
include "/var/named/master/<serverX>-rndc-key.txt";
```

3. Test RNDC. From your server, try the command below.

rndc status

If not successful, the error shows as:

```
rndc: connection to remote host closed
```

4. Add an access list that allows only specific servers (or IP addresses) who can use run rndc.

```
acl rndc-users {
    192.168.101.2; 192.168.102.1;
      };
```

Then edit your myrndc-key.txt to reflect the allowed hosts. The controls options should look as follows:

```
controls {
   inet 127.0.0.1 allow { 127.0.0.1; };
   inet 10.32.1.7 port 953 allow { "rndc-users"; } keys { "ns-rndc-
key"; };
```

```
};
```

5. Copy rndc.conf from server to one of the “rndc-users” access list. You may want to rename this to a more descriptive one if you rndc to different DNS servers. Now try following the command.

Ex:

rndc –s <server-ip> -c rndc.conf status

rndc –s 192.168.101.1 –c server1-rndc.conf status (for Server1)

RNDC is the recommended way of controlling a server’s named. Run the commands below as needed.

```
rndc -s <server ip>  -c rndc.conf reload  (reload config & all
zones)
rndc -s <server ip>  -c rndc.conf reload pcx.net (reload single
zone)
rndc -s <server ip>  -c rndc.conf status
rndc -s <server ip>  -c rndc.conf stop
rndc -s <server ip>  -c rndc.conf trace [level] (activate
debugging)
rndc -s <server ip>  -c rndc.conf flush (flushes the server’s
cache)

rndc -s <server ip>  -c rndc.conf   freeze   (suspend dynamic
updates)
rndc -s <server ip>  -c rndc.conf   unfreeze (Resume dynamic
updates)
```