Security Manual for Bind DNS

DNS Hardening by Security Enrichment and Performance Enhancement of Recursive Resolver

Centre of Excellence in

DNS SECURITY

System Requirements

1) A Recursive Resolver setup using Bind.
2) Internet connection.
3) A valid IP address.

Manual at Glance:

I. Configure the named.conf file for basic performance and security

1) Navigate to the following location

```
# cd /usr/local/var
```

2) create a directory by name 'named' as shown below

```
# mkdir named
```

3) Navigate to the named directory created as shown below

```
# cd named
```

4) Create a directory by name 'data' as shown below

```
# mkdir data
```

5) Create a directory by name 'dynamic' as shown below

```
# mkdir dynamic
```

6) Navigate to the following location

```
# cd /usr/local/etc
```

7) Use an editor to open the named.conf file and all the boxed/highlighted content to the named.conf file.

```
# nano named.conf
```

```
options {
        listen-on port 53 { 127.0.0.1; 192.168.3.106;};
//      listen-on-v6 port 53 {  };
    directory         "/usr/local/var/named";
    dump-file         "data/cache_dump.db";
    statistics-file    "data/named_stats.txt";
    memstatistics-file  "data/named_mem_stats.txt";
    recursing-file   "data/named.recursing";
    secroots-file   "data/named.secroots";
    allow-query     { any; };
    memstatistics yes;
    dnssec-validation auto;
    /* Path to ISC DLV key */
    bindkeys-file "/usr/local/etc/bind.keys";
    managed-keys-directory "dynamic/";
```

```
        pid-file "/usr/local/var/run/named/named.pid";
        session-keyfile "/usr/local/var/run/named/session.key";
};
include "/usr/local/etc/rndc.key";
```

8) Run the following command to verify the correctness of configuration file

```
# named-checkconf
```

9) For the changes made above in the named.conf file to get into effect follow the following steps :

a) Kill the named process as shown below

```
# pkill  named
```

b) Start the Bind Server as shown below

```
# named –c /usr/local/etc/named.conf
```

10) For verification of the start of the DNS Server run the following command as shown below

```
# ps -eaf |grep named
```

If the DNS Server is successfully started, it should display the following information.

```
# ps -eaf |grep named
root       9024    1991  1 13:39 ?       00:00:00 named -c /usr/local/etc/named.conf
```

11) If you want to check dump.db files, run the command as shown below

```
# rndc dumpdb
```

12) If you want to check statistics file, run the command shown below

```
# rndc stats
```

13) If you want to see the recursing file, run the command as shown below

```
# rndc recursing
```

14) If you want to see the secroots file, run the command as shown below

```
# rndc secroots
```

15) If you want to validate, whether DNSSEC is enabled or not, run the command as shown below

```
# rndc validation status
```

II. Implement the RFC 7706 [1] [2]

1) Use an editor to open the named.conf file

```
 # nano named.conf
```

2) Copy the following information into the named.conf file before options section

```
view root {
    match-destinations { 127.0.0.1; };
    zone "." {
       type slave;
       file "rootzone.db";
       notify no;
       masters {
          192.228.79.201;  # b.root-servers.net
```

```
            192.33.4.12;    # c.root-servers.net
            192.5.5.241;    # f.root-servers.net
            192.112.36.4;   # g.root-servers.net
            193.0.14.129;   # k.root-servers.net
            192.0.47.132;   # xfr.cjr.dns.icann.org
            192.0.32.132;   # xfr.lax.dns.icann.org
            2001:500:84::b;  # b.root-servers.net
            2001:500:2f::f;   # f.root-servers.net
            2001:7fd::1;    # k.root-servers.net
            2620:0:2830:202::132;  # xfr.cjr.dns.icann.org
            2620:0:2d0:202::132;  # xfr.lax.dns.icann.org
        };
    };
};
view recursive {
    dnssec-validation auto;
    allow-recursion { any; };
    recursion yes;
    zone "." {
        type static-stub;
        server-addresses { 127.0.0.1; };
    };
};
```

3) Run the following command to verify the correctness of configuration file

```
#  named-checkconf
```

4) For the changes made above in the named.conf file to get into effect follow the following steps:

a) Kill the named process as shown below

```
# pkill  named
```

b) Start the Bind Server as shown below

```
# named –c /usr/local/etc/named.conf
```

5) To verify the implementation of RFC 7706 follow the following steps

a) Navigate to the following location

```
# cd /usr/local/var/named
```

b) Run the following command

```
# ls
```

The list of files should contain rootzone.db as shown below

```
data  dynamic  rootzone.db
```

6) For verification of the start of the DNS Server run the following command as shown below

```
# ps -eaf |grep named
```

If the DNS Server is successfully started, it should display the following information.

```
# ps -eaf |grep named
root       9024    1991  1 13:39 ?       00:00:00 named -c /usr/local/etc/named.conf
```

III. Configure the named.conf file for further performance improvements

1) Navigate to the following directory as shown below

```
# cd  /usr/local/etc
```

2) Use an editor to open the named.conf file

```
# nano named.conf
```

3) Copy the following lines into the options section of named.conf file and change the default values of some properties as per your requirements.

```
    minimal-any yes;
    querylog yes;
    zone-statistics yes;
    minimal-responses yes;
    answer-cookie no;
    qname-minimization relaxed;
    stale-answer-enable  yes;
    stale-cache-enable  no;

    clients-per-query  10;      //default value
    max-clients-per-query 100;  //default value

    allow-transfer {none;};
    allow-update {none;};
    allow-notify {none;};
```

```
allow-update-forwarding {none;};

lame-ttl 600;       // default value
servfail-ttl 1;     // default value
max-stale-ttl 0;  // default value

min-cache-ttl 0;  // default value
min-ncache-ttl 0;  // default value

max-cache-ttl  604800;  // default value
max-ncache-ttl 10800;  // default value

version  "Forbidden";
rate-limit {
        responses-per-second  0; //default value
};
```

4) Run the following command to verify the correctness of configuration file

```
#  named-checkconf
```

5) For the changes made above in the named.conf file to get into effect follow the following steps :

a) Kill the named process as shown below

```
# pkill  named
```

b) Start the Bind Server as shown below

```
# named –c /usr/local/etc/named.conf
```

6) For verification of the start of the DNS Server run the following command as shown below

```
# ps -eaf |grep named
```

If the DNS Server is successfully started, it should display the following information.

```
# ps -eaf |grep named
root       9024    1991  1 13:39 ?        00:00:00 named -c /usr/local/etc/named.conf
```

IV. Add zone details of Authoritative Server

1) Use an editor to open the named.conf file

```
# nano named.conf
```

2) Copy the following lines into the named.conf file after the options section.

```
view options{
zone "cdac.in" IN {
        type static-stub;
        zone-statistics yes;
        server-addresses {196.1.113.248; 196.1.113.249; };
   };
};
```

If you want to add another Authoritative Server, you can add so as shown below

```
view options{
zone "cdac.in" IN {
        type static-stub;
        zone-statistics yes;
        server-addresses {196.1.113.248; 196.1.113.249; };
```

```
  };
zone "domainName" IN {
        type static-stub;
        zone-statistics yes;
        server-addresses { IPAddresses of Authoritative Server; };
  };
};
```

3) Run the following command to verify the correctness of configuration file

```
#  named-checkconf
```

4) For the changes made above in the named.conf file to get into effect follow the following steps :

a) Kill the named process as shown below

```
# pkill  named
```

b) Start the Bind Server as shown below

```
# named –c /usr/local/etc/named.conf
```

5) For verification of the start of the DNS Server run the following command as shown below

```
# ps -eaf |grep named
```

If the DNS Server is successfully started, it should display the following information.

```
# ps -eaf |grep named
root       9024    1991  1 13:39 ?        00:00:00 named -c /usr/local/etc/named.conf
```

V. Add Statistics Channels details

1) Use an editor to open the named.conf file

```
# nano named.conf
```

2) Copy the following lines into the named.conf file after the view options section

```
statistics-channels {
  inet 127.0.0.1 port 8053 allow { 127.0.0.1; };
};
```

3) Execute the following command:

```
# setenforce 0
```

Note: If the system reboots, then execute the above command immediately after reboot.

4) Run the following command to verify the correctness of configuration file

```
#  named-checkconf
```

5) For the changes made above in the named.conf file to get into effect follow the following steps :

a) Kill the named process as shown below

```
# pkill  named
```

b) Start the Bind Server as shown below

```
# named –c /usr/local/etc/named.conf
```

6) For verification of the start of the DNS Server run the following command as shown below

```
# ps -eaf |grep named
```

If the DNS Server is successfully started, it should display the following information.

```
# ps -eaf |grep named
root      9024    1991  1 13:39 ?       00:00:00 named -c /usr/local/etc/named.conf
```

7) For seeing the statistics of the DNS Server open the URL in your browser:

```
http: //127.0.0.1:8053
```

VI. Add Logging facilities [3] [4]

1) Navigate to the following location

```
# cd /usr/local/var/named
```

2) Create a directory by name 'log' as shown below

```
# mkdir log
```

3) Navigate to the following location

```
# cd  /usr/local/etc
```

4) Use an editor to open the named.conf file

```
# nano named.conf
```

5) Copy the following details in the options section after statistics channel

```
logging {
   channel default_log {
        file "log/default" versions 3 size 20m;
        print-time yes;
        print-category yes;
        print-severity yes;
```

```
    severity info;
};
channel auth_servers_log {
    file "log/auth_servers" versions 100 size 20m;
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
     channel dnssec_log {
    file "log/dnssec" versions 3 size 20m;
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;

};
channel zone_transfers_log {
    file "log/zone_transfers" versions 3 size 20m;
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
channel ddns_log {
    file "log/ddns" versions 3 size 20m;
    print-time yes;
    print-category yes;
    print-severity yes;
```

```
    severity info;
};
channel client_security_log {
    file "log/client_security" versions 3 size 20m;
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
channel rate_limiting_log {
    file "log/rate_limiting" versions 3 size 20m;
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
channel dnstap_log {
    file "log/dnstap" versions 3 size 20m;
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
channel queries_log {
    file "log/queries" versions 600 size 200m;
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
```

```
};
channel query_errors_log {
    file "log/query_errors" versions 6 size 20m;
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
channel default_debug {
        file "data/named.run";
        severity dynamic;
};
  category default {
        default_log;
        default_debug;
  };
  category resolver {
        auth_servers_log;
        default_debug;
  };
  category delegation-only {
        auth_servers_log;
        default_debug;
  };
  category lame-servers {
        auth_servers_log;
        default_debug;
  };
  category dnssec {
```

```
        dnssec_log;
        default_debug;
};
category xfer-in {
        zone_transfers_log;
        default_debug;
};
category xfer-out {
        zone_transfers_log;
        default_debug;
};
category update {
        ddns_log;
        default_debug;
};
category update-security {
        ddns_log;
        default_debug;
};
category client {
        client_security_log;
        default_debug;
};
category security {
        client_security_log;
        default_debug;
};
category rate-limit {
        rate_limiting_log;
```

```
        default_debug;
    };
    category spill {
        rate_limiting_log;
        default_debug;
    };
    category database {
        rate_limiting_log;
        default_debug;
    };
    category dnstap {
        dnstap_log;
        default_debug;
    };
    category queries {
        queries_log;
    };
    category query-errors {
        query_errors_log;
        default_debug;
    };
```

6) Run the following command to verify the correctness of configuration file

```
# named-checkconf
```

7) For the changes made above in the named.conf file to get into effect follow the following steps :

a) Kill the named process as shown below

```
# pkill named
```

b) Start the Bind Server as shown below

```
# named –c /usr/local/etc/named.conf
```

8) Navigate to the following location

```
# cd  /usr/local/var/named/log
```

9) Run the following command to verify the correctness of configuration file

```
#  ls
```

If the logging is configured correctly, it will list the following details

```
auth_servers    ddns    dnssec  queries     rate_limiting
client_security  default  dnstap  query_errors  zone_transfers
```

References:

(1) https://coednssecurity.in/pdf/RFC7706.pdf
(2) https://tools.ietf.org/html/rfc7706
(3) https://kb.isc.org/docs/aa-01526
(4) https://www.isc.org/docs/BIND_Logging.pdf
(5) https://downloads.isc.org/isc/bind9/9.16.6/doc/arm/Bv9ARM.pdf

Acknowledgements:

We express our sincere thanks to Internet Governance Division of Ministry of Electronics & Information Technology (MeitY) and National Internet Exchange of India (NIXI).