Install and Configure Caching-Only DNS Server in CentOS 7

1. Install BIND DNS Servers

```
[root@server1 ~]# yum install bind bind-utils -y
```

2. Configure the BIND DNS Servers

```
[root@server1 ~]# vi  /etc/named.conf

//

// 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.

//

// See the BIND Administrator's Reference Manual (ARM) for details about the

// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html


options {

        listen-on port 53 { 127.0.0.1; 172.25.1.200; };

        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; any; };

        allow-query-cache {localhost; any; };
        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;

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

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

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};

logging {
    channel default_debug {
        file "data/named.run";
```

```
            severity dynamic;
        };
};

zone "." IN {
            type hint;
            file "named.ca";
};
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

These directives instruct the DNS server to listen on **UDP** port **53**, and to allow queries and caches responses from **localhost** and any other machine that reaches the server.

1. **listen-on port 53** – This say that Cache server want to use the port 53 for query.
2. **allow-query** – This Specifies which ip address may query the server, here I have defined for localhost, from anywhere anyone can send query.
3. **allow-query-cache** – This will add the query request to the bind.
4. **recursion** – This will query the answer and give back to us, during query it may send query to other DNS server over the internet and pull back the query.

3. Firewall Configuration For BIND DNS Servers

```
# firewall-cmd --add-port=53/udp
# firewall-cmd --add-port=53/udp -permanent

# firewall-cmd --add-port 53/udp -permanent

# firewall-cmd -reload

# firewall-cmd --list-port
```

4. Config Check for BIND DNS Servers

```
[root@server1 ~]# named-checkconf /etc/named.conf
```

5. Start BIND DNS Service

```
[root@server1 ~]# systemctl start named

[root@server1 ~]# systemctl status named

[root@server1 ~]# systemctl enable named
```

DNS Server Cache

```
#cat /etc/named.conf

        "/var/named/data/cache_dump.db";


# ls /var/named/data/

# man rndc

# rndc dumpdb  –cache

# ls –l /var/named/data/

# cat /var/named/data/cache_dump.db
```

Clear DNS Server Cache

```
# rndc flush

# rndc reload
```

To show DNS Root Hint

```
# ls /var/named
# cat /var/named/named.ca
```

How To Configure BIND as a Private Network DNS Server on CentOS 7

1. Install BIND DNS Servers

```
sudo yum install bind bind-utils
```

2. Configure Primary DNS Server

BIND's configuration consists of multiple files, which are included from the main configuration file, `named.conf`. These filenames begin with "named" because that is the name of the process that BIND runs. We will start with configuring the options file.

```
sudo vi /etc/named.conf
```

At the end of the file, add the following line:

```
include "/etc/named/named.conf.local";
```

Now save and exit `named.conf`. The above configuration specifies that only your own servers (the "trusted" ones) will be able to query your DNS server.

Next, we will configure the local file, to specify our DNS zones.

3. Configure Local File

On *server3*, open the `named.conf.local` file for editing:

```
sudo vi /etc/named/named.conf.local
```

```
zone "achnetworklab.com" {
      type master;
      file "/etc/named/zones/db.achnetworklab.com";
};
zone "1.25.172.in-addr.arpa" {
      type master;
      file "/etc/named/zones/db.1.25.172";
};
```

4. Create Forward Zone File

The forward zone file is where we define DNS records for forward DNS lookups. That is, when the DNS receives a name query, "host1.achnetworklab.com" for example, it will look in the forward zone file to resolve *host1*'s corresponding private IP address.

Let's create the directory where our zone files will reside. According to our *named.conf.local* configuration, that location should be `/etc/named/zones`:

```
sudo chmod 755 /etc/named
sudo mkdir /etc/named/zones
```

```
sudo vi /etc/named/zones/db.achnetworklab.com
```

```
$TTL    604800
@       IN      SOA     server3.achnetworlab.com. admin.achnetworklab.com. (
              3         ; Serial
             604800     ; Refresh
              86400     ; Retry
            2419200     ; Expire
             604800 )   ; Negative Cache TTL

; name servers - NS records
                IN      NS      server3.achnetworklab.com.
                IN      NS      server2.achnetworklab.com.

; host A Record - A records
server3.achnetworklab.com.              IN      A       172.25.1.200
server2.achnetworklab.com.              IN      A       172.25.1.201
pc1.achnetworklab.com.                  IN      A       172.25.1.1
pc2.achnetworklab.com.                  IN      A       172.25.1.2
```

Creating CNAME Record

```
www             IN              CNAME           server3
```

```
# systemctl restart named
```

5. Create Reverse Zone File(s)

```
sudo vi  cat /etc/named/zones/db.1.25.172
```

```
$TTL    604800
@       IN      SOA     server3.achnetworklab.com. admin.achnetworklab.com. (
                        3       ; Serial
                   604800       ; Refresh
```

```
                    86400        ; Retry
                   2419200        ; Expire
                    604800 )      ; Negative Cache TTL

; name servers - NS records
     IN      NS      server3.achnetworklab.com.
     IN      NS      server2.achnetworklab.com.

; PTR Records
200   IN      PTR     server3.achnetworklab.com.
201   IN      PTR     server2.achnetworklab.com.
1   IN      PTR     pc1.achnetworklab.com.
2   IN       PTR     pc2.achnetworklab.com.
```