Manual for

Installation and Configuration of DNS Server Using Bind on CentOS

February 2024

BIND 9.18.*

System Requirements

1) Operating System: CentOS 9.x
2) Internet connection.
3) All the commands to be executed as "*root*" user.
4) A valid IP address.

Procedure at Glance:

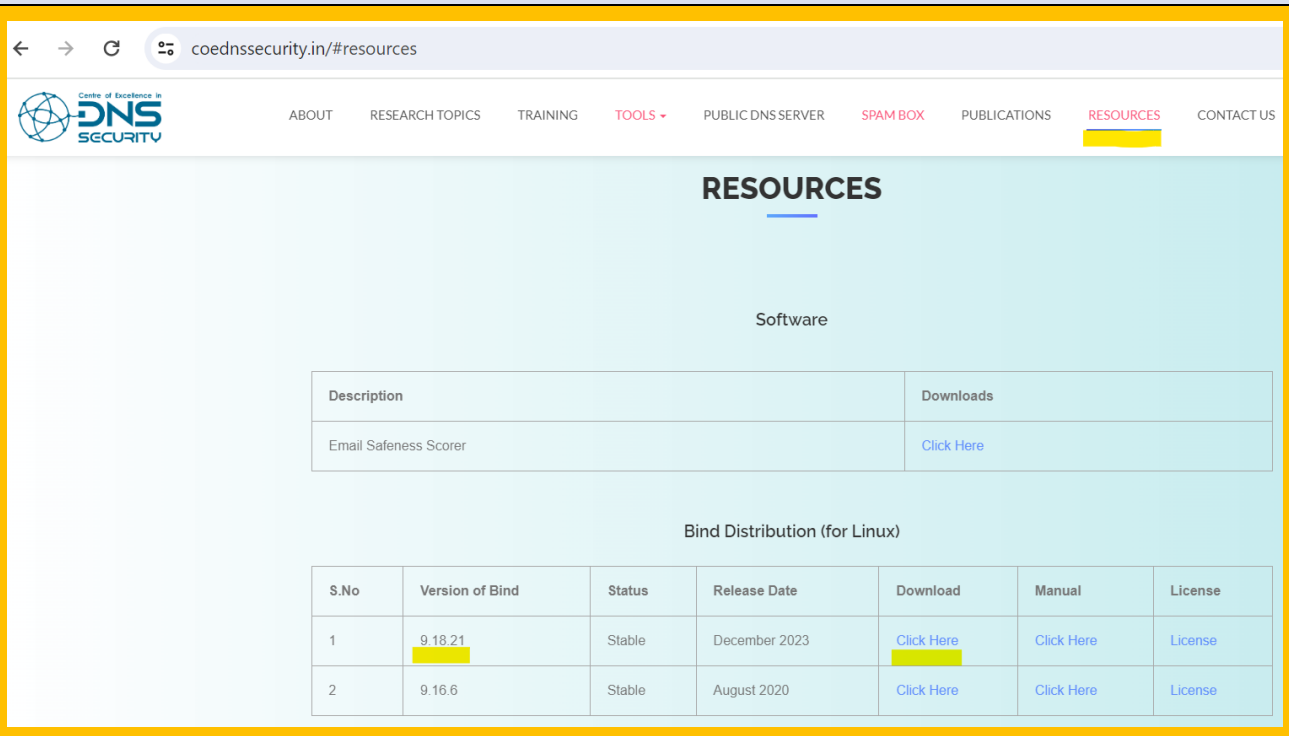
Overview of Steps:

Stepwise Procedure

Step 1: Download the latest stable Bind Software

Download the latest stable Bind Software from the Resources section of the following portal.

 # https://www.coednssecurity.in/



Step 2: Download and Install the prerequisite libraries for Bind Software

2.1) Install **epel release package** as show below:

```
# yum install epel-release -y
```

2.2) Install **gcc** package as shown below:

```
# yum install gcc
```

Install the **make** tool using the command as shown below:

```
# yum install make
```

2.3) Install the **libuv** package as shown below:

```
# yum install libuv -y
```

2.4) For installation of **libuv-devel** package follow the following step if Operating System is **CentOS 9**

```
# yum install https://dl.rockylinux.org/pub/rocky/9/CRB/x86_64/os/Packages/l/libuv-devel-1.42.0-1.el9.x86_64.rpm
```

2.5) Install the **openssl-devel** package as shown below:

```
# yum install openssl-devel -y
```

2.6) Install the libnghttp2 package as shown below:

```
# yum install libnghttp2
```

2.7) Install libnghttp2-devel package as shown below:

```
# yum install https://mirror.stream.centos.org/9-stream/CRB/x86_64/os/Packages/libnghttp2-devel-1.43.0-5.el9.x86_64.rpm
```

2.8) Install **libcap-devel** package as shown below:

```
# yum install libcap-devel -y
```

Step 3: Untar the Bind tar file

Navigate to the location where bind-*.tar.xz **is downloaded and run the following command. By default the downloaded files will be in** Downloads **folder.**

```
# tar -xvf bind-*.tar.xz
```

Step 4: Configure the libraries required for the Bind Software and Build, Install Bind

4.1) Navigate to the directory of the Bind Software installation as shown below:

```
# cd bind-9.18.*/
```

4.2) Configure the Bind Software with the libraries by running the command as shown below:

```
# ./configure
```

4.3) Run the make command as shown below:

```
# make
```

4.4) Run the **make install** as shown below:

```
# make install
```

Step 5: Verify the installation of Bind Software

For verifying the successful installation of the version of Bind Software run the following command as shown below:

```
# named -v
```

Step 6: Configure the named.conf file

6.1) Navigate to the directory as shown below:

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

6.2) Create a file **named.conf** file at the above location using the command as shown below:

```
# nano named.conf
```

6.3) Make the changes in the **named.conf** file by refering the sample given below. Replace the IP Address highlighted with machine's IP Address and port to 53.

```
options {
        Listen-on port 53 { 127.0.0.1; <IP Address> ;};
        allow-query     { any; };
        recursion yes;
        dnssec-validation auto;
};
```

7.4) Check for the correctness of the named configuration file use the following command.

```
# named-checkconf
```

For a correctly configured file, the command does not provide any output.

Step 7: Start the DNS Server

Start the DNS Server by running the command as shown below:

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

Step 8: Verification of the start the DNS Server

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

Step 9: Test the DNS Server

Test the DNS Server, by running the following command as shown below.
Give your DNS Server IP Address in the highlighted IP Address.

```
# dig @<IP Address> cdac.in
```

If it is successful, you can see the following kind of information:

```
; <<>> DiG 9.16.5 <<>> @<IP Address> cdac.in
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3966
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 7045cc7e5a12a93001000000626fb55261bf5d44cb63ab61 (good)
;; QUESTION SECTION:
;cdac.in.                       IN      A
;; ANSWER SECTION:
cdac.in.                300     IN      A       196.1.113.45
;; Query time: 3106 msec
```

```
;; SERVER: <IP Address>#53(<IP Address>)
;; WHEN: Fri Feb 9 13:40:48 IST 2024
;; MSG SIZE  rcvd: 83
```

Step 10: Trusted Domain Configuration in Recursive Resolver

10.1) Open the named.conf file using any editor like vim/nano or cat command as shown below

```
# nano named.conf
```

Add these lines in your named.conf file by seeing the sample given below after the options.

```
zone "coednssecurity.in"  {          #domain name
    type forward;
    forwarders {162.251.82.249; };  #Authoritative DNS Server IP Addresses
};
```

Change the Highlight Area according to your domain name.

10.2) Restart the DNS Server

For stop the DNS Server

```
# pkill named
```

And then start the DNS Server

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

References:

(1) https://downloads.isc.org/isc/bind9/9.18.21/doc/arm/html/requirements.html
(2) https://downloads.isc.org/isc/bind9/9.18.21/doc/arm/html/configuration.html

Acknowledgements:

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