DNS Server Configuration on Centos-7

Scenario:

Here in this document One will be acting as Master DNS server, the second system will be acting as Secondary DNS, and the third will be our DNS client. Here are my three systems details.

Primary(Master)DNS Server Details:

Operating System : Centos 7 Minimal Server
Hostname : masterdns.gurubhat.lab
IP Address : 192.168.2.101/24

```
[root@materdns ~]# uname -a
Linux materdns.gurubhat.lab 3.10.0-123.el7.x86_64 #1 SMP Mon Jun 30 12:09:22 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
[root@materdns ~]# hostname
materdns.gurubhat.lab
[root@materdns ~]# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eno16777728: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:4c:d5:cc brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.101/24 brd 192.168.2.255 scope global eno16777728
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe4c:d5cc/64 scope link
       valid_lft forever preferred_lft forever
[root@materdns ~]#
```

Secondary (Slave) DNS Server Details:

Operating System : Centos 7 Minimal Server
Hostname : secondarydns.gurubhat.lab
IP Address : 192.168.2.102/24

```
[root@secondarydns ~]# uname -a
Linux secondarydns.gurubhat.local 3.10.0-123.el7.x86_64 #1 SMP Mon Jun 30 12:09:22 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
[root@secondarydns ~]# hostname
secondarydns.gurubhat.local
[root@secondarydns ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eno16777728: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:48:04:96 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.102/24 brd 192.168.2.255 scope global eno16777728
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe48:496/64 scope link
       valid_lft forever preferred_lft forever
[root@secondarydns ~]#
```

Client Details:

Operating System : Centos 7 with GUI
Hostname : client.gurubhat.lab
IP Address : 192.168.2.103/24

```
[root@client ~]# uname -a
Linux client.gurubhat.lab 3.10.0-123.el7.x86_64 #1 SMP Mon Jun 30 12:09:22 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
[root@client ~]# hostname
client.gurubhat.lab
[root@client ~]# ifconfig
eno16777728: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.103  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::20c:29ff:fe4c:890b  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:4c:89:0b  txqueuelen 1000  (Ethernet)
        RX packets 5121  bytes 383000 (374.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 372  bytes 39377 (38.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 973  bytes 83858 (81.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 973  bytes 83858 (81.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@client ~]#
```

Set Up Primary(Master)DNS Server Details:

Install bind Packages on your server.

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

Configure DNS Server:
Edit **"/etc/named.conf"** file

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

Edit the file as below.

```
//
// 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; 192.168.2.101;}; ### Master DNS IP ###
#       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; 192.168.1.0/24; }; ### IP Range ###
        allow-transfer{ localhost; 192.168.2.102; }; ### Slave DNS IP ###
        /*
         - 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";
};

zone "gurubhat.lab" IN {
type master;
file "forward.gurubhat";
allow-update { none; };
};
zone "1.168.192.in-addr.arpa" IN {
type master;
file "reverse.gurubhat";
allow-update { none; };
};


include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

Create Zone Files:
Create forward and reverse zone files which we mentioned in the **'/etc/named.conf'** file.

Create Forward Zone:

Create **forward.gurubhat** file in the **'/var/named'** directory.

```
[root@materdns ~]# vi /var/named/forward.gurubhat
```

Edit the file as below,

```
$TTL 86400
@   IN  SOA     masterdns.gurubhat.lab. root.gurubhat.lab. (
        2011071001  ;Serial
        3600        ;Refresh
        1800        ;Retry
        604800      ;Expire
        86400       ;Minimum TTL
)
@       IN  NS          masterdns.gurubhat.lab.
@       IN  NS          secondarydns.gurubhat.local.
@       IN  A           192.168.2.101
@       IN  A           192.168.2.102
@       IN  A           192.168.2.103
masterdns       IN  A   192.168.2.101
secondarydns    IN  A   192.168.2.102
client          IN  A   192.168.2.103
[root@materdns ~]#
```

Create Reverse Zone:

Create **reverse.gurubhat** file in the **'/var/named'** directory.

```
[root@materdns ~]# vi /var/named/reverse.gurubhat
```

Add the following lines.

```
$TTL 86400
@   IN  SOA     masterdns.gurubhat.lab. root.gurubhat.lab. (
        2011071001  ;Serial
        3600        ;Refresh
        1800        ;Retry
        604800      ;Expire
        86400       ;Minimum TTL
)
@       IN  NS          masterdns.gurubhat.lab.
@       IN  NS          secondarydns.gurubhat.local.
@       IN  PTR         gurubhat.local.
masterdns       IN  A   192.168.2.101
secondarydns    IN  A   192.168.2.102
client          IN  A   192.168.2.103
101     IN  PTR         masterdns.gurubhat.lab.
102     IN  PTR         secondarydns.gurubhat.local.
103     IN  PTR         client.gurubhat.local.

~
```

Start the DNS Service:

Enable and start DNS service:

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

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

Firewall Configuration:

```
[root@materdns ~]# firewall-cmd --permanent --add-port=53/tcp
```

```
[root@materdns ~]# firewall-cmd --permanent --add-port=53/udp
```

Restart Firewall:

```
[root@materdns ~]# firewall-cmd --reload
```

Configuring Permissions, Ownership, and SELinux:

Run the following commands one by one:

```
[root@materdns ~]# chgrp named -R /var/named
[root@materdns ~]# chown -v root:named /etc/named.conf
ownership of ‘/etc/named.conf’ retained as root:named
[root@materdns ~]# restorecon -rv /var/named
[root@materdns ~]# restorecon /etc/named.conf
```

Test DNS configuration and zone files for any syntax errors:

Check DNS default configuration file:

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

If it returns nothing, your configuration file is valid.

Check Forward zone:

```
[root@masterdns ~]# named-checkzone gurubhat.lab /var/named/forward.gurubhat
zone gurubhat.lab/IN: loaded serial 2011071001
OK
```

Check reverse zone:

```
[root@masterdns ~]# named-checkzone gurubhat.lab /var/named/reverse.gurubhat
zone gurubhat.lab/IN: loaded serial 2011071001
OK
[root@masterdns ~]#
```

Add the DNS Server details in your network interface config file.

```
[root@masterdns ~]# cd /etc/sysconfig/network-scripts/
[root@masterdns network-scripts]#
```

```
[root@masterdns network-scripts]# ls
ifcfg-eno16777728  ifdown-ppp       ifup-eth     ifup-sit
ifcfg-lo           ifdown-routes    ifup-ippp    ifup-Team
ifdown             ifdown-sit       ifup-ipv6    ifup-TeamPort
ifdown-bnep        ifdown-Team      ifup-isdn    ifup-tunnel
ifdown-eth         ifdown-TeamPort  ifup-plip    ifup-wireless
ifdown-ippp        ifdown-tunnel    ifup-plusb   init.ipv6-global
ifdown-ipv6        ifup             ifup-post    network-functions
ifdown-isdn        ifup-aliases     ifup-ppp     network-functions-ipv6
ifdown-post        ifup-bnep        ifup-routes
```

```
[root@masterdns network-scripts]# vi ifcfg-eno16777728
```

```
HWADDR=00:0C:29:4C:D5:CC
TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=eno16777728
UUID=005574b1-48e4-482a-9792-93d79c3249dc
ONBOOT=yes
IPADDR=192.168.2.101
NETMASK=255.255.255.0
GATEWAY=192.168.2.1
DNS1=192.168.2.101
DNS2=8.8.8.8
```

Edit file **/etc/resolv.conf**,

```
[root@masterdns /]# vi /etc/resolv.conf
```

Add the name server ip address:

Nameserver 192.168.2.101

Save and close the file.

Restart network service:

```
[root@masterdns /]# service network restart
```

Check for nameserver details.

```
[root@masterdns /]# cat /etc/resolv.conf
```

```
[root@masterdns /]# cat /etc/resolv.conf
# Generated by NetworkManager
search gurubhat.lab
nameserver 192.168.2.101
nameserver 8.8.8.8
[root@masterdns /]#
```

Test DNS Server:

```
[root@masterdns /]# dig masterdns.gurubhat.lab
```

```
; <<>> DiG 9.9.4-RedHat-9.9.4-51.el7_4.2 <<>> masterdns.gurubhat.lab
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60328
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;masterdns.gurubhat.lab.                IN      A

;; ANSWER SECTION:
masterdns.gurubhat.lab. 86400   IN      A       192.168.2.101

;; AUTHORITY SECTION:
gurubhat.lab.           86400   IN      NS      secondarydns.gurubhat.local.
gurubhat.lab.           86400   IN      NS      masterdns.gurubhat.lab.

;; Query time: 2 msec
;; SERVER: 192.168.2.101#53(192.168.2.101)
;; WHEN: Tue Mar 20 08:17:34 EDT 2018
;; MSG SIZE  rcvd: 122

[root@masterdns /]#
```

```
[root@masterdns /]# nslookup gurubhat.lab
Server:         192.168.2.101
Address:        192.168.2.101#53

Name:   gurubhat.lab
Address: 192.168.2.102
Name:   gurubhat.lab
Address: 192.168.2.101
Name:   gurubhat.lab
Address: 192.168.2.103

[root@masterdns /]#
```

Now the Primary DNS server is ready to use.

It is time to configure our Secondary DNS server.

Setup Secondary(Slave) DNS Server:

Install bind packages using the following command:

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

Configure Slave DNS Server:

Edit file **`/etc/named.conf'**:

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

Edit the file as below,

```
//
// 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; 192.168.2.102; };
        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; 192.168.2.0/24; };

        /*
         - 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";
};
zone "gurubhat.lab" IN {
type slave;
file "slaves/gurubhat.fwd";
masters { 192.168.2.101; };
};
zone "1.168.192.in-addr.arpa" IN {
type slave;
file "slaves/gurubhat.rev";
masters { 192.168.2.101; };
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

[root@secondarydns slaves]#
```

Start the DNS Service:

```
[root@secondarydns ~]# systemctl enable named
[root@secondarydns ~]# systemctl start named
```

Now the forward and reverse zones are automatically replicated from Master DNS server to ‘/var/named/slaves/’ in Secondary DNS server.

```
[root@secondarydns /]# ls /var/named/slaves/
```

```
[root@secondarydns slaves]# ls
gurubhat.fwd  gurubhat.rev
[root@secondarydns slaves]#
```

Add the DNS Server details:

Add the DNS Server details in your network interface config file.

```
[root@secondarydns ~]# cd /etc/sysconfig/network-scripts/
```

```
[root@secondarydns network-scripts]# ls
ifcfg-eno16777728  ifdown-eth   ifdown-post    ifdown-Team      ifup-aliases  ifup-ipv6   ifup-post    ifup-Team      init.ipv6-global
ifcfg-lo           ifdown-ippp  ifdown-ppp     ifdown-TeamPort  ifup-bnep     ifup-isdn   ifup-ppp     ifup-TeamPort  network-functions
ifdown             ifdown-ipv6  ifdown-routes  ifdown-tunnel    ifup-eth      ifup-plip   ifup-routes  ifup-tunnel    network-functions-ipv6
ifdown-bnep        ifdown-isdn  ifdown-sit     ifup             ifup-ippp     ifup-plusb  ifup-sit     ifup-wireless
[root@secondarydns network-scripts]#
```

```
[root@secondarydns network-scripts]# vi ifcfg-eno16777728
```

```
HWADDR=00:0C:29:48:04:96
TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=eno16777728
UUID=fcc769ae-207a-4618-8d1e-77efc5ea6e28
ONBOOT=yes
IPADDR=192.168.2.102
NETMASK=255.255.255.0
GATEWAY=192.168.2.1
DNS1=192.168.2.101
DNS2=192.168.2.102
~
~
~
~
~
```

Save and close the file.

Restart network service.

```
[root@secondarydns /]# systemctl restart network
```

Firewall Configuration:

```
[root@secondarydns /]# firewall-cmd --permanent --add-port=53/tcp
success
[root@secondarydns /]# firewall-cmd --reload
success
[root@secondarydns /]#
```

Configuring Permissions, Ownership, and SELinux:

```
[root@secondarydns /]# chgrp named -R /var/named
[root@secondarydns /]# chown -v root:named /etc/named.conf
ownership of ‘/etc/named.conf’ retained as root:named
[root@secondarydns /]# restorecon -rv /var/named
[root@secondarydns /]# restorecon /etc/named.conf
[root@secondarydns /]#
```

Test DNS Server:

```
[root@masterdns ~]# dig masterdns.gurubhat.lab

; <<>> DiG 9.9.4-RedHat-9.9.4-51.el7_4.2 <<>> masterdns.gurubhat.lab
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16303
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;masterdns.gurubhat.lab.                IN      A

;; ANSWER SECTION:
masterdns.gurubhat.lab. 86400   IN      A       192.168.2.101

;; AUTHORITY SECTION:
gurubhat.lab.           86400   IN      NS      secondarydns.gurubhat.local.
gurubhat.lab.           86400   IN      NS      masterdns.gurubhat.lab.

;; Query time: 1 msec
;; SERVER: 192.168.2.101#53(192.168.2.101)
;; WHEN: Wed Mar 21 01:44:53 EDT 2018
;; MSG SIZE  rcvd: 122

[root@masterdns ~]#
```

```
[root@masterdns ~]# dig secondarydns.gurubhat.lab

; <<>> DiG 9.9.4-RedHat-9.9.4-51.el7_4.2 <<>> secondarydns.gurubhat.lab
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48650
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;secondarydns.gurubhat.lab.     IN      A

;; ANSWER SECTION:
secondarydns.gurubhat.lab. 86400 IN     A       192.168.2.102

;; AUTHORITY SECTION:
gurubhat.lab.           86400   IN      NS      masterdns.gurubhat.lab.
gurubhat.lab.           86400   IN      NS      secondarydns.gurubhat.local.

;; ADDITIONAL SECTION:
masterdns.gurubhat.lab. 86400   IN      A       192.168.2.101

;; Query time: 0 msec
;; SERVER: 192.168.2.101#53(192.168.2.101)
;; WHEN: Wed Mar 21 01:45:21 EDT 2018
;; MSG SIZE  rcvd: 151

[root@masterdns ~]#
```

```
[root@secondarydns ~]# nslookup gurubhat.lab
;; Got recursion not available from 192.168.2.101, trying next server
Server:         192.168.2.102
Address:        192.168.2.102#53

Name:   gurubhat.lab
Address: 192.168.2.103
Name:   gurubhat.lab
Address: 192.168.2.102
Name:   gurubhat.lab
Address: 192.168.2.101

[root@secondarydns ~]#
```

Client Side Configuration:

Add the DNS server details in **'/etc/resolv.conf'** file in all client systems

```
[root@client ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search gurubhat.lab
nameserver 192.168.2.101
nameserver 192.168.2.102
[root@client ~]#
```

Restart network service or reboot the system.

Test DNS Server:

Now, you can test the DNS server using any one of the following commands:

dig masterdns.gurubhat.lab
dig secondarydns.gurubhat.lab
dig client.gurubhat.lab

That's all about now. The primary and secondary DNS servers are ready to use.

--Guru Bhat