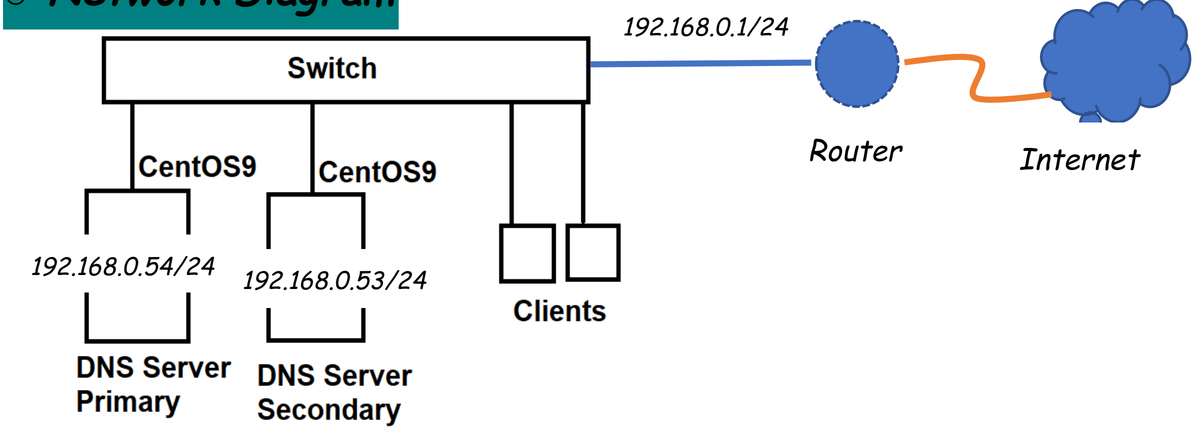
Lab (DNS)-Configure Primary DNS Server on Linux CentOS9

○ Network Diagram



Domain: lovekhmer.com

ជំហាន (Steps):

➢ Linux CentOS9 Machine (Primary DNS)

0. Update system before you install anything.

```
yum -y update
```

1. Install DNS Packages named "bind, bind-utils, bind-libs"

```
yum -y install bind bind-utils bind-libs
```

>> ពិនិត្យផ្ទៀងផ្ទាត់ដោយ

```
rpm -q bind bind-utils bind-libs
```

```
bind-9.16.23-24.el9.x86_64
bind-utils-9.16.23-24.el9.x86_64
bind-libs-9.16.23-24.el9.x86_64
```

បានដំឡើងរួច

2. Configure Bind Primary DNS Server

>> Backup configuration file

```
cp /etc/named.conf /etc/named.conf.backup
```

>> បើក Main Configuration File (named.conf) to see Default Setting

```
vim /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.
//
options {
            listen-on port 53 { 127.0.0.1; };
```

យើងពិនិត្យឃើញថា DNS ស្តាប់សំណើរលើ Port ៥៣ នៃ Loopback Interface ដែលមាន IP: 127.0.0.1

```
          listen-on-v6 port 53 { ::1; };
          directory      "/var/named";
```

ទីតាំងនៃ Zone Files

```
          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";
          secroots-file   "/var/named/data/named.secroots";
          recursing-file  "/var/named/data/named.recursing";
          allow-query     { localhost; };
```

ទទួលសំណើរដំណោះស្រាយតែពី localhost តែប៉ុណ្ណោះ

```
...
```

ប្រសិនបើយើងមិនទាន់កែប្រែអ្វីទាំងអស់ ដោយគ្រាន់តែចាកចេញរួច ហើយបើកដំណើរការ Service (named) និងពិនិត្យផ្ទៀងផ្ទាត់។

+បើកដំណើរការ Service

```
[root@linuxserver1 ~]# systemctl start named
[root@linuxserver1 ~]#
```

+ពិនិត្យមើលការស្តាប់សំណើររបស់ DNS

```
[root@linuxserver1 ~]# netstat -ltnp | grep named
tcp       0     0               127.0.0.1:953        0.0.0.0:*         LISTEN       12679/named
tcp       0     0               127.0.0.1:53         0.0.0.0:*         LISTEN       12679/named
tcp6      0     0               ::1:953              :::*              LISTEN       12679/named
tcp6      0     0               ::1:53               :::*              LISTEN       12679/named
```

Note:

Port	Protocol	Service	Details
953	tcp	rndc	BIND9 remote name daemon controller

```
[root@ inuxserver1 ~]# netstat -lunp | grep named
udp       0     0               127.0.0.1:53         0.0.0.0:*                   12679/named
udp       0     0               127.0.0.1:53         0.0.0.0:*                   12679/named
udp6      0     0     ::1:53             :::*                                    12679/named
udp6      0     0     ::1:53             :::*                                    12679/named
[root@linuxserver1 ~]#
```

>> កំណត់ Interface ឱ្យស្តាប់សំណើពី Clients

+ពិនិត្យមើល IP

```
[root@linuxserver1 ~]# ifconfig
Ens36: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
 inet 192.168.0.54  netmask 255.255.255.0  broadcast 192.168.0.255
```

```
     inet6 fe80::20b9:54de:ac9:9808  prefixlen 64  scopeid 0x20<link>
     ether 00:0c:29:dd:07:1c  txqueuelen 1000  (Ethernet)
     RX packets 23554  bytes 33339665 (31.7 MiB)
     RX errors 0  dropped 0  overruns 0  frame 0
     TX packets 6708  bytes 479372 (468.1 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 1000  (Local Loopback)
     RX packets 98  bytes 8059 (7.8 KiB)
     RX errors 0  dropped 0  overruns 0  frame 0
     TX packets 98  bytes 8059 (7.8 KiB)
     TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
[root@linuxserver1 ~]#
```

+បញ្ចូល IP: 192.168.0.54 របស់យើយទៅក្នុង Configuration File

```
vim /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.
//
options {
        listen-on port 53 { 127.0.0.1; 192.168.0.54; };
```

+Restart Service

```
[root@linuxserver1 ~]# systemctl restart named
[root@linuxserver1 ~]#
```

+ពិនិត្យមើលការស្តាប់សំណើររបស់ DNS ម្តងទៀត

```
[root@linuxserver1 ~]# netstat -ltnp | grep named
tcp      0     0  127.0.0.1:953           0.0.0.0:*          LISTEN     6180/named
tcp      0     0  127.0.0.1:53            0.0.0.0:*          LISTEN     6180/named
tcp      0     0  192.168.0.54:53         0.0.0.0:*          LISTEN     6180/named
(ស្តាប់លើ IP: 192.168.0.54 នៃ Server របស់យើង)
tcp6     0    0   ::1:53                  :::*               LISTEN     6180/named
tcp6     0    0   ::1:953                 :::*               LISTEN     6180/named
[root@linuxserver1 ~]#
```

» បញ្ចូល IP និង FQDN (fully qualified domain name) ទៅក្នុង hosts file.

- The Linux hosts file is a plain text file that maps hostnames to IP addresses. It's located in the /etc directory, which is owned by the root user.
- The hosts file was used on early computer networks for name resolution before DNS was developed.
- The hosts file is still present on computer systems (Windows, Linux, MAC), tablets etc and can be very useful for testing purposes.

```
vim /etc/hosts
#Add this
192.168.0.54    linuxserver1.lovekhmer.com      linuxserver1
```

+តេស្ត Hosts File ដោយ Ping

```
[root@linuxserver1 ~]# ping linuxserver1.lovekhmer.com
PING linuxserver1.lovekhmer.com (192.168.0.54) 56(84) bytes of data.
64 bytes from linuxserver1.lovekhmer.com (192.168.0.54): icmp_seq=1 ttl=64 time=0.104 ms
64 bytes from linuxserver1.lovekhmer.com (192.168.0.54): icmp_seq=2 ttl=64 time=0.056 ms
64 bytes from linuxserver1.lovekhmer.com (192.168.0.54): icmp_seq=3 ttl=64 time=0.056 ms
64 bytes from linuxserver1.lovekhmer.com (192.168.0.54): icmp_seq=7 ttl=64 time=0.054 ms
^Z
[2]+  Stopped                 ping linuxserver1.lovekhmer.com
[root@linuxserver1 ~]#
```

» និងង្កើត **Zones (Forward & Reverse)** ដើម្បីគ្រប់គ្រងដំណោះស្រាយបំណកប្រែពីឈ្មោះដូម៉េន ទៅអាសយដ្ឋានអាយភី និងអាសយដ្ឋានអាយភី ទៅឈ្មោះដូម៉េន។ ការនេះអាចប្រព្រឹត្តទៅបានដោយកែ Configuration File ឈ្មោះថា named.conf នៅក្រោម /etc ។ The BIND name server named server uses the /etc/named.conf file for configuration. All zone files are placed in the /var/named/ directory.

```
vim /etc/named.conf
options {
        listen-on port 53 { 127.0.0.1; 192.168.0.54; };
```

```
// Master DNS IPv4 to enable the DNS configuration to accept the
// request on DNS Server IPv4
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";
recursing-file  "/var/named/data/named.recursing";
secroots-file   "/var/named/data/named.secroots";
allow-query     { any; };
// any: Accept the request from all DNS Clients (Public)
allow-transfer  { 192.168.0.53; };
// allow-transfer: IPv4 of Secondary DNS Server
```

ទាញចុះក្រោម ដើម្បីបង្កើត **Zones**។ Zone "<Zone-name>" -Specifies particular zones for which this nameserver is authoritative. We will update the /etc/named.conf for the names of **forward** and **reverse lookup** files.

```
    zone "." IN {
    type hint;
    file "named.ca";
    };
// A zone statement on a primary nameserver hosting the
// domain lovekhmer.com may look like:
//1-Forward Lookup Zone (Name to IP)
   zone "lovekhmer.com" IN {
   type master;
   file "fwd.lovekhmer.com";
   allow-update { none; };
   };
```

//This zone statement names the zone lovekhmer.com, sets the type as master,
//tells named to read the /var/named/fwd.lovekhmer.com file to configure the
//zone, and to allow no updates by any other hosts.
//2-Reverse Lookup Zone (IP to Name)
*// Reverse DNS actually uses the same query methods as normal DNS, but uses a special zone called **in-addr.arpa**. Under **in-addr.arpa** the zones have numeric names corresponding to the numeric values of octets of IP addresses.*
// "IN-ADDR" stands for "INternet ADDRess".
// "ARPA" stands for "Address and Routing Parameter Area".

```
zone "0.168.192.in-addr.arpa" IN {
type master;
file "rev.lovekhmer.com";
allow-update      { none; };
};
```

⇨ ***SAVE and EXIT From named.conf file***

```
esc:wq
```

>> ង្កើត Zone Files (Forward & Reverse)

Zone files, which contain information about a particular namespace, are stored in the named working directory. By default, this is /var/named. Each zone file is named according to the file option data in the zone statement, usually in a way that relates to the domain in question and identifies the file as containing zone data, such as lovekhmer.com.zone. We should create forward and reverse zone files which we mentioned in the '/etc/named.conf' file.

+ Create Forward Zone file & Change ownership

- *Create 'fwd.lovekhmer.com' file in the '/var/named' directory and add the entries for forward zone as shown below.*

```
vim /var/named/fwd.lovekhmer.com
$TTL 1D
@      IN SOA  linuxserver1.lovekhmer.com.  root.lovekhmer.com. (
                         0      ; serial
```

```
                        1D      ; refresh
                        1H      ; retry
                        1W      ; expire
                        3H )    ; minimum
; Specify our two nameservers
IN  NS      linuxserver1.lovekhmer.com.
IN  NS      linuxserver2.lovekhmer.com.
; Resolve nameserver hostnames to IP, replace with your two droplet IP addresses.
Linuxserver1    IN  A   192.168.0.54
linuxserver2    IN  A   192.168.0.53
; Clients
it01  IN  A  192.168.0.10
it02  IN  A  192.168.0.11
; CNAME (canonical name): An alias for one name to another name that should have an A
or AAAA record.
; <alias-name>  IN CNAME <real-name>
www     IN      CNAME          cos9server
xyz     IN      CNAME          cos9server2
```

⇨ SAVE and EXIT From fwd.lovekhmer.com file

```
esc:wq
```

- Change ownership for named user 'fwd.lovekhmer.com' file

```
chown named:name fwd.lovekhmer.com
```

```
[root@linuxserver1 named]# chown named:named fwd.lovekhmer.com
[root@linuxserver1 named]# ls -l fwd.lovekhmer.com
-rw-r-----. 1 named named 684 Feb  9 17:30 fwd.lovekhmer.com
[root@linuxserver1 named]#
```

+ Create Reverse Zone & Change ownership

- Create 'rev.lovekhmer.com' file in the '/var/named' directory and add the entries for reverse zone as shown below.

```
vim /var/named/rev.lovekhmer.com
$TTL 1D
@    IN SOA  linuxserver1.lovekhmer.com.  root.lovekhmer.com. (
                    0      ; serial
                    1D     ; refresh
```

```
                1H     ; retry
                 1W     ; expire
                3H )   ; minimum
; Specify our two nameservers
        IN NS      linuxserver1.lovekhmer.com.
        IN NS      linuxserver2.lovekhmer.com.
; Resolve nameserver hostnames to IP, replace with your two droplet IP
addresses.
linuxserver1    IN A    192.168.0.54
linuxserver2    IN A   192.168.0.53
; Clients
it01  IN A  192.168.0.10
it02  IN A  192.168.0.11
; CNAME (canonical name): An alias for one name to another name that should
have an A or AAAA record.
; <alias-name> IN CNAME <real-name>
www    IN    CNAME           linuxserver1
xyz     IN      CNAME          linuxserver2
; Pointer Records
54     IN PTR   linuxserver1.lovekhmer.com.
53    IN PTR   linuxserver2.lovekhmer.com.
10    IN PTR   it01.lovekhmer.com.
11      IN PTR   it02.lovekhmer.com.
```

⇨ **Save and Exit From rev.lovekhmer.com**

- *Change ownership for named user 'rev.lovekhmer.com' file*

  chown named:name fwd.lovekhmer.com

```
[root@linuxserver1 named]# chown named:named rev.lovekhmer.com
[root@linuxserver1 named]# ls -l rev.lovekhmer.com
-rw-r-----. 1 named named 884 Feb  9 17:30 rev.lovekhmer.com
[root@linuxserver1 named]#
```

3. Test syntax errors of DNS configuration and zone files

>> Check DNS Config file

```
named-checkconf /etc/named.conf
```

អត់ឃើញអី មានន័យថាអត់ Error

>> Check zone files (Forward & Reverse)

```
named-checkzone lovekhmer.com /var/named/fwd.lovekhmer.com
```

```
          zone lovekhmer.com/IN: loaded serial 0
          OK (មានន័យថាអត់ Error)
named-checkzone lovekhmer.com /var/named/rev.lovekhmer.com
          zone lovekhmer.com/IN: loaded serial 0
          OK (មានន័យថាអត់ Error)
```

4. Restart and Enable Bind Service (named)

>> Retart Service

```
systemctl restart named
```

>> Enable Service (Start on boot)

```
systemctl enable named
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /usr/lib/systemd/system/named.service.
```

>> Verify DNS Status:

```
systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: disabled)
Active: active (running) since Sat 2025-02-08 10:21:43 +07; 2min 31s ago
```

5. Allow DNS Server through FireWall

Add a allow rule in firewall to let clients can connect to DNS server for name resolution.

```
firewall-cmd --add-port=53/udp --permanent
firewall-cmd --permanent --add-port=53/tcp
firewall-cmd --reload
```

>> Verify Firewall Table:

```
firewall-cmd --list-ports
53/tcp 53/udp
```

6. Test DNS Server

>> ពី Linux ខ្លួនឯង

+ Check the resolver library (DNS Client)

The resolver library queries the name servers listed in the /etc/resolv.conf file.

```
[root@linuxserver1 named]# cat /etc/resolv.conf
# Generated by NetworkManager
```

```
nameserver 192.168.0.54
[root@linuxserver1 named]#
```

+ តេស្តជាមួយ host –a ឬ host command

```
[root@linuxserver1 named]# host -a lovekhmer.com
Trying "lovekhmer.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48832
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2
;; QUESTION SECTION:
;lovekhmer.com.                    IN       ANY
;; ANSWER SECTION:
lovekhmer.com.          86400      IN       SOA      linuxserver1.lovekhmer.com. root.lovekhmer.com. 0 86400 3600 604800 10800
lovekhmer.com.          86400      IN       NS       linuxserver2.lovekhmer.com.
lovekhmer.com.          86400      IN       NS       linuxserver1.lovekhmer.com.
;; ADDITIONAL SECTION:
linuxserver1.lovekhmer.com. 86400 IN        A        192.168.0.54
linuxserver2.lovekhmer.com. 86400 IN        A        192.168.0.53

Received 158 bytes from 192.168.0.54#53 in 2 ms
[root@linuxserver1 named]#
```

```
[root@linuxserver1 network-scripts]# host www.lovekhmer.com
www.lovekhmer.com is an alias for linuxserver1.lovekhmer.com.
linuxserver1.lovekhmer.com has address 192.168.0.54
[root@linuxserver1 network-scripts]#
```

```
[root@linuxserver1 named]# host -a 192.168.0.54
Trying "54.0.168.192.in-addr.arpa"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52079
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;54.0.168.192.in-addr.arpa.        IN       PTR
;; ANSWER SECTION:
54.0.168.192.in-addr.arpa. 86400 IN         PTR      linuxserver1.lovekhmer.com.
Received 83 bytes from 192.168.0.54#53 in 2 ms
[root@linuxserver1 named]#
```

+ តេស្តជាមួយ dig command

```
[root@linuxserver1 named]# dig www.lovekhmer.com
; <<>> DiG 9.16.23-RH <<>> www.lovekhmer.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21194
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 0a3c1fcad03f0c760100000067a88f5e3856fc307460d6f3 (good)
;; QUESTION SECTION:
;www.lovekhmer.com.              IN       A
;; ANSWER SECTION:
www.lovekhmer.com.      86400    IN       CNAME linuxserver1.lovekhmer.com.
linuxserver1.lovekhmer.com. 86400 IN      A        192.168.0.54
```

```
;; Query time: 0 msec
;; SERVER: 192.168.0.54#53(192.168.0.54)
;; WHEN: Sun Feb 09 18:19:58 +07 2025
;; MSG SIZE  rcvd: 117
```

Others:

```
dig it01.lovekhmer.com
 dig –x 192.168.0.54
dig –x 192.168.0.10
```

+ តេស្តជាមួយ nslookup command

```
[root@linuxserver1 named]# nslookup www.lovekhmer.com
Server:             192.168.0.54
Address:  192.168.0.54#53
www.lovekhmer.com      canonical name = linuxserver1.lovekhmer.com.
Name:     linuxserver1.lovekhmer.com
Address: 192.168.0.54

[root@linuxserver1 named]# nslookup linuxserver1.lovekhmer.com
Server:             192.168.0.54
Address:  192.168.0.54#53
Name:     linuxserver1.lovekhmer.com
Address: 192.168.0.54

[root@linuxserver1 named]# nslookup 192.168.0.54
54.0.168.192.in-addr.arpa           name = linuxserver1.lovekhmer.com.
[root@linuxserver1 named]#
[root@linuxserver1 named]# nslookup 192.168.0.53
53.0.168.192.in-addr.arpa           name = linuxserver2.lovekhmer.com.
[root@linuxserver1 named]#
```

>> ពី Windows Clients (សំណើសុំដំណោះស្រាយពី DNS Server)

+មើល IP Configuration នៃ Client

```
Ipconfig /all
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network connection
   Physical Address. . . . . . . . . : 00-0C-29-4F-21-5F
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.0.10 (Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
   DNS Servers . . . . . . . . . . . : 192.168.0.54
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

- ping www.lovekhmer.com

- *nslookup www.lovekhmer.com*
- *nslookup 192.168.0.54*
- *nslookup 192.168.0.53*
- nslookup 192.168.0.10
- nslookup 192.168.0.11

›› លទ្ធផលនៃការធ្វើតេស្តបង្ហាញថា Primary DNS Server បំពេញការងារបានត្រឹមត្រូវ ដូចការរំពឹងទុក។