

# DNS SERVER

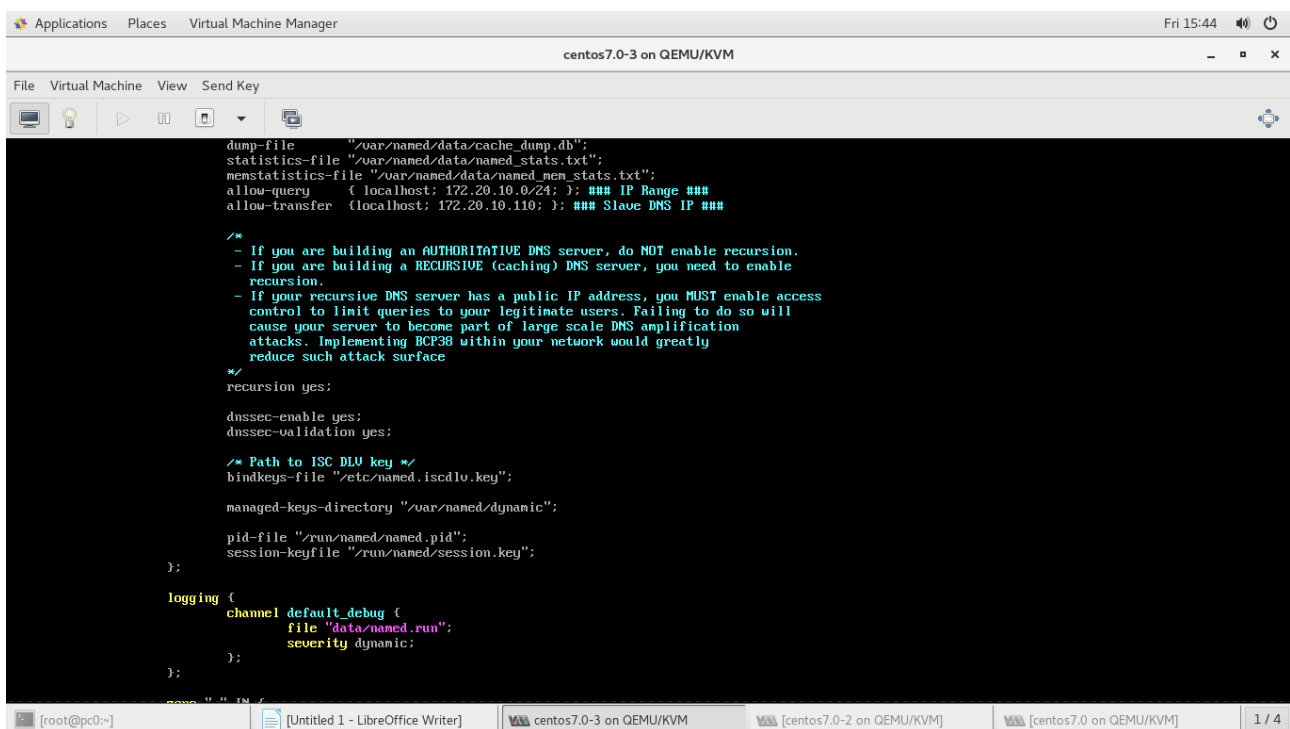
step1 :

#yum install bind\*

step2 :

#vim /etc/named.conf

edit file as below



```
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; 172.20.10.0/24; }; ### IP Range ###
allow-transfer { localhost; 172.20.10.110; }; ### 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;

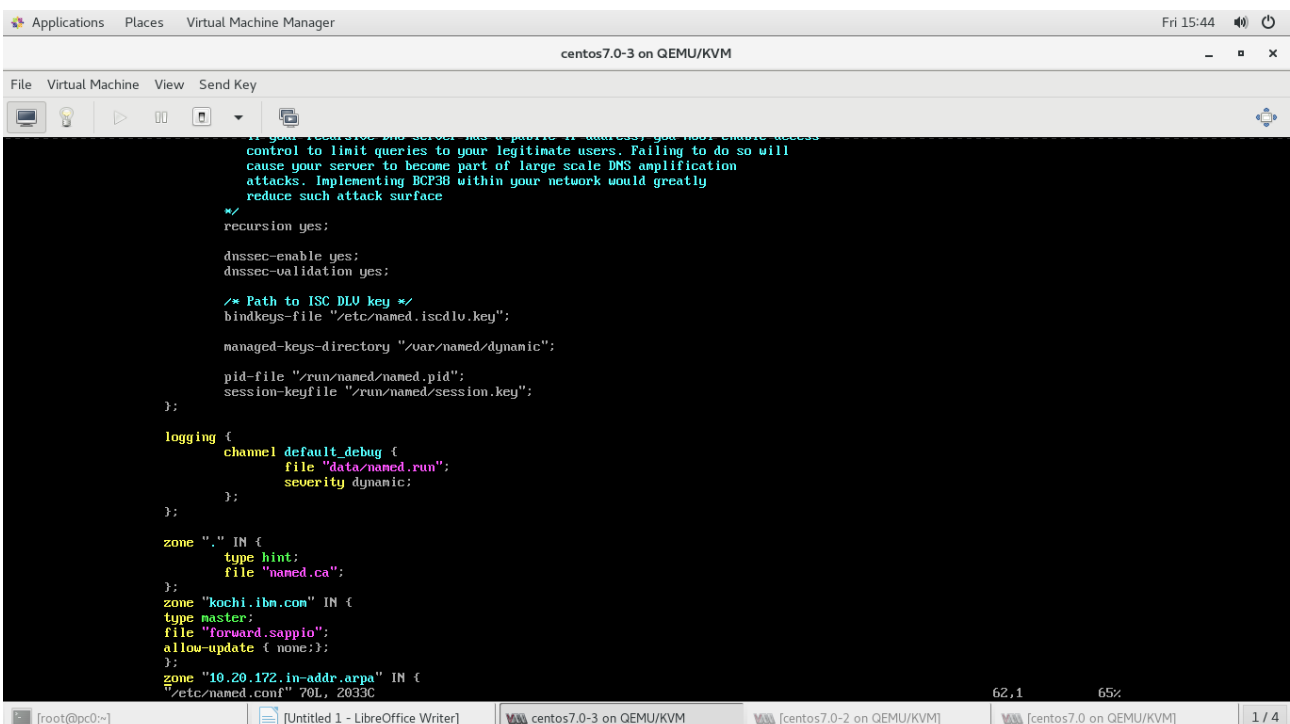
/* Path to ISC DLV key */
bindkeys-file "/etc/named.iscdlv.key";

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 "kochi.ibm.com" IN {
type master;
file "forward.sappio";
allow-update { none; };
};
zone "10.20.172.in-addr.arpa" IN {
type reverse;
file "reverse.map";
};
```



```
/*
- 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;
};
};

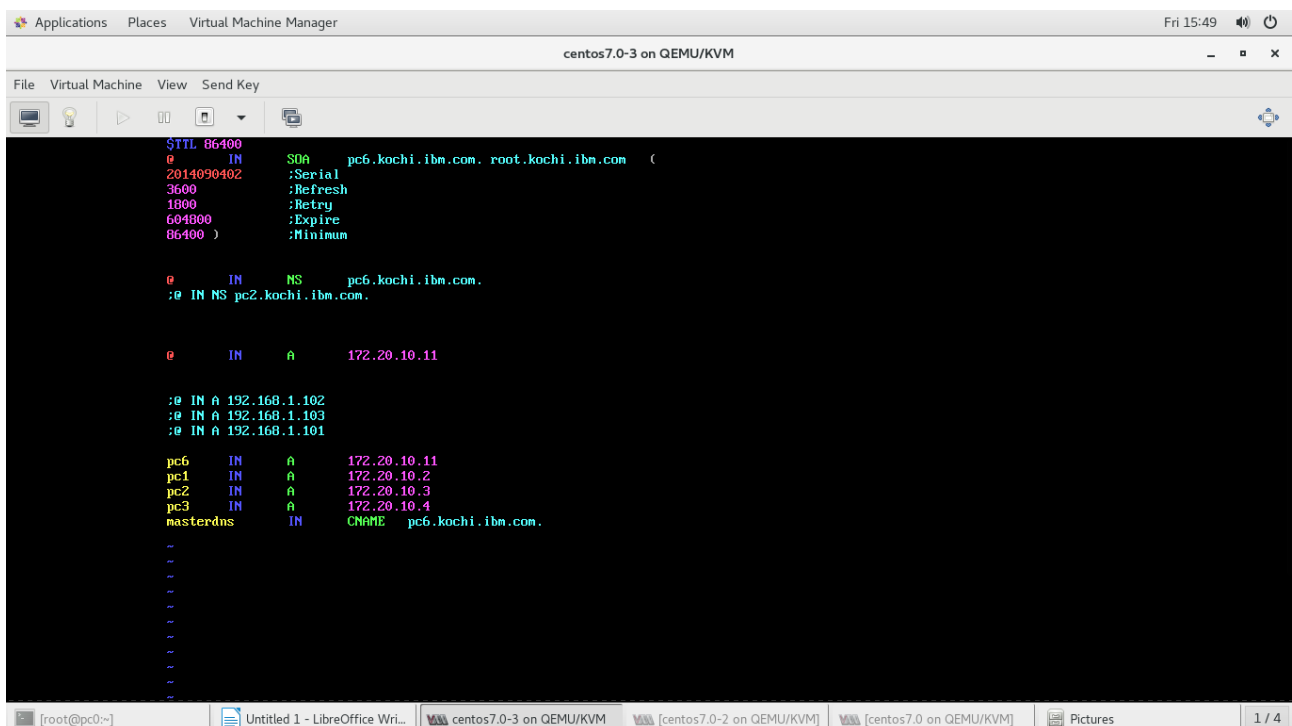
zone "." IN {
type hint;
file "named.ca";
};
zone "kochi.ibm.com" IN {
type master;
file "forward.sappio";
allow-update { none; };
};
zone "10.20.172.in-addr.arpa" IN {
type reverse;
file "reverse.map";
};
```

we need to add two files in path /var/named/

Forward file and reverse file in the above scenario files are

forward.sappio and reverse.sappio

#vim /var/named/forward.sappio



```
$TTL 86400
@ IN SOA pc6.kochi.ibm.com. root.kochi.ibm.com. (
2014090402 :Serial
3600 :Refresh
1800 :Retry
604800 :Expire
86400 ) :Minimum

@ IN NS pc6.kochi.ibm.com.
;@ IN NS pc2.kochi.ibm.com.

@ IN A 172.20.10.11

;@ IN A 192.168.1.102
;@ IN A 192.168.1.103
;@ IN A 192.168.1.101

pc6 IN A 172.20.10.11
pc1 IN A 172.20.10.2
pc2 IN A 172.20.10.3
pc3 IN A 172.20.10.4
masterdns IN CNAME pc6.kochi.ibm.com.

~
~
~
~
~
~
~
~
~
~
```

#vim /var/named/reverse.sappio

Here both the files created are in root users & group ownership, so we need to change the group should be under in named group . Change the group to named on both files using following commands.

The screenshot shows a Virtual Machine Manager window titled "centos7.0-3 on QEMU/KVM". The terminal window displays the output of the command `cat /etc/passwd`. The output lists system users and their details:

```

root@pc6 ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/bash
daemon:x:2:2:daemon:/sbin:/sbin/bash
named:x:35:35:Named:/usr/sbin/named:/usr/sbin/named
dnsmasq:x:415:415:dnsmasq:/var/lib/ntp:/usr/sbin/named
forward:x:2281:2281:forward.sappio:/var/lib/ntp:/usr/sbin/named
empty:x:152:152:empty:/var/lib/ntp:/usr/sbin/named
localhost:x:152:152:localhost:/var/lib/ntp:/usr/sbin/named
loopback:x:168:168:loopback:/var/lib/ntp:/usr/sbin/named
reverse:x:408:408:reverse.sappio:/var/lib/ntp:/usr/sbin/named
slaves:x:6:6:slaves:/var/lib/ntp:/usr/sbin/named

```

The window also shows the standard Linux terminal prompt `root@pc6 ~]#` and the file manager interface at the bottom.

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

```
#named-checkzone pc6.kochi.ibm.com /var/named/reverse.sappio
```

## finally, test the DNS using dig & nslookup tools

The screenshot shows a Kali Linux desktop with the following elements:

- Top Panel:** Applications, Places, Virtual Machine Manager. System clock: Fri 16:06.
- Virtual Machine Manager Window:** Title bar: centos7.0-3 on QEMU/KVM. Menu bar: File, Virtual Machine, View, Send Key. Toolbar: icons for VM, power, play, pause, shutdown, and a dropdown menu.
- Terminal Window:** Prompt: [root@pc6 ~]#. It shows the execution of two dig commands and their outputs.

**Terminal Output:**

```
[root@pc6 ~]# dig 172.20.10.11

;<<>> DiG 9.9.4-RedHat-9.9.4-61.el7 <<>> 172.20.10.11
;; global options: +cmd
;; Got answer:
;;->HEADER<<- opcode: QUERY, status: SERVFAIL, id: 53886
;; flags: qr rd ra: QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

;; Query time: 21 msec
;; SERVER: 172.20.10.11#53(172.20.10.11)
;; WHEN: Fri Mar 06 16:05:35 IST 2020
;; MSG SIZE rcvd: 41

[root@pc6 ~]# dig -x 172.20.10.11

;<<>> DiG 9.9.4-RedHat-9.9.4-61.el7 <<>> -x 172.20.10.11
;; global options: +cmd
;; Got answer:
;;->HEADER<<- opcode: QUERY, status: NOERROR, id: 14413
;; flags: qr aa rd ra: QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:: udp: 4096
;; QUESTION SECTION:
;;11.10.20.172.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
11.10.20.172.in-addr.arpa. 86400 IN    PTR    pc6.kochi.ibn.com.

;; AUTHORITY SECTION:
10.20.172.in-addr.arpa. 86400 IN    NS     pc6.kochi.ibn.com.
```

**Taskbar:** Shows the following open applications: root@pc0:~, Untitled 1 - LibreOffice Wri..., centos7.0-3 on QEMU/KVM, centos7.0-2 on QEMU/KVM, centos7.0 on QEMU/KVM, [Pictures], and 1 / 4.

**Client side**

**edit the /etc/resolv.conf**

**Add name server as 172.20.10.11 on client**

**To add DNS server permanent make a entry in connection file**

**eg of connection file : /etc/sysconfig/network-script/ifcfg-eth0**