**DNS (Bind) Server**

## tep 1 – Install Bind Packages

Bind packages are available under default yum repositories. To install packages simple execute below command.

# yum install bind bind-chroot

## Step 2 – Edit Main Configuration File

Default bind main configuration file is located under /etc directory. But using chroot environment this file is located at /var/named/chroot/etc directory. Now edit main configuration file and update content as below.

# vim /var/named/chroot/etc/named.conf

Content for the named.conf file

// /var/named/chroot/etc/named.conf

options {

listen-on port 53 { 127.0.0.1; 192.168.1.0/24; 0.0.0.0/0; };

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; 0.0.0.0/0; };

recursion yes;

dnssec-enable yes;

dnssec-validation yes;

dnssec-lookaside auto;

/\* Path to ISC DLV key \*/

bindkeys-file "/etc/named.iscdlv.key";

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

};

logging {

channel default\_debug {

file "data/named.run";

severity dynamic;

};

};

zone "." IN {

type hint;

file "named.ca";

};

zone "demotecadmin.net" IN {

type master;

file "/var/named/demotecadmin.net.db";

};

zone"**0.168.192.in-addr.arpa**" IN {

type master;

file "**/var/named/**demotecadmin.net.db **.rev.zone**";

};

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

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

## Step 3 – Create Zone File for Your Domain

After creating bind main configuration file, create a zone file for you domain as per configuration, for example **demotecadmin.net.db** in this article.

# vim /var/named/chroot/var/named/demotecadmin.net.db

Content for the zone file

; Zone file for demotecadmin.net

$TTL 14400

@ 86400 IN SOA ns1.tecadmin.net. webmaster.tecadmin.net. (

3013040200 ; serial, todays date+todays

86400 ; refresh, seconds

7200 ; retry, seconds

3600000 ; expire, seconds

86400 ; minimum, seconds

)

demotecadmin.net. 86400 IN NS ns1.tecadmin.net.

demotecadmin.net. 86400 IN NS ns2.tecadmin.net.

demotecadmin.net. IN A 192.168.1.100

demotecadmin.net. IN MX 0 mail.demotecadmin.net.

mail IN CNAME demotecadmin.net.

www IN CNAME demotecadmin.net.

If you are having more domain, its required to create zone files for each domain individually.

## Step 4 – Add More Domains

To add more domains in dns, create zone files individually for all domain as above. After that add any entry for all zones in named.conf like below. Change **demotecadmin.net** with your domain name.

zone "demotecadmin.net" IN {

type master;

file "/var/named/demotecadmin.net.db";

};

## Step 5 – Start Bind Service

Start named (bind) service using following command.

# service named restart

Enable auto start on system boot.

# chkconfig named on

##### Step 6 – Test Your DNS Setup

Send query to your dns server directly using below command.  
Syntax: nslookup <domainname> <dns server name/ip>

# nslookup demotecadmin.net 192.168.1.254

Server: 192.168.1.254

Address: 192.168.1.254#53

Name: demotecadmin.net

Address: 192.168.1.100

Above output is showing that dns server has successfully resolved domain demotecadmin.net.

### Configure Bind

BIND's process is known as **named**. As such, many of the files refer to "named" instead of "BIND".

On ns1, open the named.conf file for editing:

* sudo vi /etc/named.conf

Above the existing options block, create a new ACL block called "trusted". This is where we will define list of clients that we will allow recursive DNS queries from (i.e. your servers that are in the same datacenter as ns1). Using our example private IP addresses, we will add ns1, ns2, host1, and host2 to our list of trusted clients:

/etc/named.conf — 1 of 4

acl "trusted" {

10.128.10.11; # ns1 - can be set to localhost

10.128.20.12; # ns2

10.128.100.101; # host1

10.128.200.102; # host2

};

Now that we have our list of trusted DNS clients, we will want to edit the options block. Add the private IP address of ns1 to the listen-on port 53 directive, and comment out the listen-on-v6 line:

/etc/named.conf — 2 of 4

options {

listen-on port 53 { 127.0.0.1; 10.128.10.11; };

# listen-on-v6 port 53 { ::1; };

...

Below those entries, change the allow-transfer directive to from "none" to **ns2**'s private IP address. Also, change allow-query directive from "localhost" to "trusted":

/etc/named.conf — 3 of 4

...

options {

...

allow-transfer { 10.128.20.12; }; # disable zone transfers by default

...

allow-query { trusted; }; # allows queries from "trusted" clients

...

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

/etc/named.conf — 4 of 4

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.

### Configure Local File

On ns1, open the named.conf.local file for editing:

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

The file should be empty. Here, we will specify our forward and reverse zones.

Add the forward zone with the following lines (substitute the zone name with your own):

/etc/named/named.conf.local — 1 of 2

zone "nyc3.example.com" {

type master;

file "/etc/named/zones/db.nyc3.example.com"; # zone file path

};

Assuming that our private subnet is 10.128.0.0/16, add the reverse zone by with the following lines (note that our reverse zone name starts with "128.10" which is the octet reversal of "10.128"):

/etc/named/named.conf.local — 2 of 2

zone "128.10.in-addr.arpa" {

type master;

file "/etc/named/zones/db.10.128"; # 10.128.0.0/16 subnet

};

If your servers span multiple private subnets but are in the same datacenter, be sure to specify an additional zone and zone file for each distinct subnet. When you are finished adding all of your desired zones, save and exit the named.conf.local file.

Now that our zones are specified in BIND, we need to create the corresponding forward and reverse zone files.

### 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.nyc3.example.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

Now let's edit our forward zone file:

* sudo vi /etc/named/zones/db.nyc3.example.com

First, you will want to add the SOA record. Replace the highlighted ns1 FQDN with your own FQDN, then replace the second "nyc3.example.com" with your own domain. Every time you edit a zone file, you should increment the serial value before you restart the named process--we will increment it to "3". It should look something like this:

/etc/named/zones/db.nyc3.example.com — 1 of 3

@ IN SOA ns1.nyc3.example.com. admin.nyc3.example.com. (

3 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

After that, add your nameserver records with the following lines (replace the names with your own). Note that the second column specifies that these are "NS" records:

/etc/named/zones/db.nyc3.example.com — 2 of 3

; name servers - NS records

IN NS ns1.nyc3.example.com.

IN NS ns2.nyc3.example.com.

Then add the A records for your hosts that belong in this zone. This includes any server whose name we want to end with ".nyc3.example.com" (substitute the names and private IP addresses). Using our example names and private IP addresses, we will add A records for ns1, ns2, host1, and host2 like so:

/etc/named/zones/db.nyc3.example.com — 3 of 3

; name servers - A records

ns1.nyc3.example.com. IN A 10.128.10.11

ns2.nyc3.example.com. IN A 10.128.20.12

; 10.128.0.0/16 - A records

host1.nyc3.example.com. IN A 10.128.100.101

host2.nyc3.example.com. IN A 10.128.200.102

Save and exit the db.nyc3.example.com file.

Our final example forward zone file looks like the following:

/etc/named/zones/db.nyc3.example.com — complete

* $TTL 604800
* @ IN SOA ns1.nyc3.example.com. admin.nyc3.example.com. (
* 3 ; Serial
* 604800 ; Refresh
* 86400 ; Retry
* 2419200 ; Expire
* 604800 ) ; Negative Cache TTL
* ;
* ; name servers - NS records
* IN NS ns1.nyc3.example.com.
* IN NS ns2.nyc3.example.com.
* ; name servers - A records
* ns1.nyc3.example.com. IN A 10.128.10.11
* ns2.nyc3.example.com. IN A 10.128.20.12
* ; 10.128.0.0/16 - A records
* host1.nyc3.example.com. IN A 10.128.100.101
* host2.nyc3.example.com. IN A 10.128.200.102

Now let's move onto the reverse zone file(s).

### Create Reverse Zone File(s)

Reverse zone file are where we define DNS PTR records for reverse DNS lookups. That is, when the DNS receives a query by IP address, "10.128.100.101" for example, it will look in the reverse zone file(s) to resolve the corresponding FQDN, "host1.nyc3.example.com" in this case.

On ns1, for each reverse zone specified in the named.conf.local file, create a reverse zone file.

Edit the reverse zone file that corresponds to the reverse zone(s) defined in named.conf.local:

* sudo vi /etc/named/zones/db.10.128

In the same manner as the forward zone file, replace the highlighted ns1 FQDN with your own FQDN, then replace the second "nyc3.example.com" with your own domain. Every time you edit a zone file, you should increment the serial value before you restart the named process--we will increment it to "3". It should look something like this:

/etc/named/zones/db.10.128 — 1 of 3

@ IN SOA ns1.nyc3.example.com. admin.nyc3.example.com. (

3 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

After that, add your nameserver records with the following lines (replace the names with your own). Note that the second column specifies that these are "NS" records:

/etc/named/zones/db.10.128 — 2 of 3

; name servers - NS records

IN NS ns1.nyc3.example.com.

IN NS ns2.nyc3.example.com.

Then add PTR records for all of your servers whose IP addresses are on the subnet of the zone file that you are editing. In our example, this includes all of our hosts because they are all on the 10.128.0.0/16 subnet. Note that the first column consists of the last two octets of your servers' private IP addresses in reversed order. Be sure to substitute names and private IP addresses to match your servers:

/etc/named/zones/db.10.128 — 3 of 3

; PTR Records

11.10 IN PTR ns1.nyc3.example.com. ; 10.128.10.11

12.20 IN PTR ns2.nyc3.example.com. ; 10.128.20.12

101.100 IN PTR host1.nyc3.example.com. ; 10.128.100.101

102.200 IN PTR host2.nyc3.example.com. ; 10.128.200.102

Save and exit the reverse zone file (repeat this section if you need to add more reverse zone files).

Our final example reverse zone file looks like the following:

/etc/named/zones/db.10.128 — complete

* $TTL 604800
* @ IN SOA nyc3.example.com. admin.nyc3.example.com. (
* 3 ; Serial
* 604800 ; Refresh
* 86400 ; Retry
* 2419200 ; Expire
* 604800 ) ; Negative Cache TTL
* ; name servers
* IN NS ns1.nyc3.example.com.
* IN NS ns2.nyc3.example.com.
* ; PTR Records
* 11.10 IN PTR ns1.nyc3.example.com. ; 10.128.10.11
* 12.20 IN PTR ns2.nyc3.example.com. ; 10.128.20.12
* 101.100 IN PTR host1.nyc3.example.com. ; 10.128.100.101
* 102.200 IN PTR host2.nyc3.example.com. ; 10.128.200.102

### Check BIND Configuration Syntax

Run the following command to check the syntax of the named.conf\* files:

* sudo named-checkconf

If your named configuration files have no syntax errors, you will return to your shell prompt and see no error messages. If there are problems with your configuration files, review the error message and the [Configure Primary DNS Server](https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-an-private-network-dns-server-on-centos-7#ConfigurePrimaryDNSServer) section, then try named-checkconf again.

The named-checkzone command can be used to check the correctness of your zone files. Its first argument specifies a zone name, and the second argument specifies the corresponding zone file, which are both defined in named.conf.local.

For example, to check the "nyc3.example.com" forward zone configuration, run the following command (change the names to match your forward zone and file):

* sudo named-checkzone nyc3.example.com /etc/named/zones/db.nyc3.example.com

And to check the "128.10.in-addr.arpa" reverse zone configuration, run the following command (change the numbers to match your reverse zone and file):

* sudo named-checkzone 128.10.in-addr.arpa /etc/named/zones/db.10.128

When all of your configuration and zone files have no errors in them, you should be ready to restart the BIND service.

### Start BIND

Start BIND:

* sudo systemctl start named

Now you will want to enable it, so it will start on boot:

* sudo systemctl enable named

Your primary DNS server is now setup and ready to respond to DNS queries. Let's move on to creating the secondary DNS server.

#named-checkconf Conf file

#named-checkzone domain name zone file

### dns tips while configuring

Just sharing some DNS tips, which needs to keep on mind while configuring your DNS server.  
  
1. An A Record must ALWAYS contain IP address (map host to IP)  
  
Whenever you specify A record it must contain IP address on the Right side. The A record is so important in DNS without which the meaning of mapping hostnames to IP would be absurd. So remember this!  
  
2. CNAME (Alias) must contain hostnames. No IPs here  
  
3. NS an MX records must contain host names. No IPs allowed.  
  
4. Use the DOT in the end, whenever you specify a domain name in the DNS zone file. This DOT is so important and if you forget this you will have nightmares with your dns configuration.  
For example  
example.com. IN NS ns1.example.com.  
  
Why DOT? simply because it tells to start query from root servers (denoted by dot)  
  
5. MX records (for mail servers) should contain hostnames NOT IPs.  
  
6. Allow Port 53 for both UDP and TCP connections  
If you use firewall make sure you do not block port 53 for DNS tcp and udp requests. By default dns lookups use UDP protocol while zone transfers and notifications use TCP protocol of port 53.  
-Port 53 UDP = Dns Requests  
-Port 53 TCP = Zone transfers  
  
7. CNAMEs cannot co-xist with MX hosts.  
Do not specify CNAME or aliases pointing to MX records.  
  
domain.com. IN MX 10 mail.domain.com.  
mail IN CNAME domain.com. ----------> WRONG  
  
Instead use A record to map directly to IP address.  
  
mail IN A 11.33.55.77 ---> CORRECT  
  
8. No duplicate MX records  
domain.com. IN MX mail.domain.com.  
domain.com. IN MX mail.domain.com ----> DUPLICATE  
  
In case if some information provided above is incorrect, please feel free to update me.  
Will surely add more tips & tricks in the coming future.

Command Syntax Checking

|  |  |
| --- | --- |
| **Daemon** | **Command** |
| OpenSSH | /usr/sbin/sshd -t && echo $? /usr/sbin/sshd -T |
| Apache | /usr/sbin/apache2 -t apachectl configtest |
| nginx | /usr/local/nginx/sbin/nginx -t /usr/local/nginx/sbin/nginx -t -c /usr/local/nginx/conf/nginx.conf |
| lighttpd | /usr/local/sbin/lighttpd -t -f /usr/local/etc/lighttpd/cyberciti.biz/lighttpd.conf |
| Bind (named server config) | named-checkconf /etc/named.conf |
| Bind (zone syntx) | named-checkzone cyberciti.biz /var/named/zone.cyberciti.biz |
| Squid proxy | /usr/sbin/squid -k check /usr/sbin/squid -k parse |
| MySQL server | mysqld --verbose --help /usr/libexec/mysqld --verbose --help 1>/dev/null |
| Postfix MTA | postfix check postfix -vvv |
| Samba SMB/CIFS | testparm -v |
| tcpd | tcpdchk tcpdchk -v |
| dhcpd (DHCP / BOOTP) server | dhcpd -t -cf /path/to/dhcpd.testing.conf |
| vsftpd server | vsftpd -olisten=NO /path/to/vsftpd.testing.conf |
| nagios | nagios -v /path/to/testing/nagios.cfg |
| Openntpd NTPD server | ntpd -d -f /usr/local/etc/ntpd.conf -n |
| Xorg (X11 Server) | Xorg -config /path/to/xorg.conf.new -retro |
| syslogd / rsyslogd | rsyslogd -c4 -f /etc/rsyslog.testing.conf -N 1 |
| CUPS Printing System | cupsd -f -c /path/to/cupsd.testing.conf -t |
| slapd (OpenLDAP) | slapd -Tt |
| varnishd | varnishd -C -f /path/to/wordpress.vlc |
| exim MTA | exim -bV |
| Bash/Ksh scripts | bash -n ./myscript ksh -n /path/to/script.ksh |
| BSD pf firewall | pfctl -nf /etc/pf.conf |
| proftpd | proftpd -t -c /path/to/proftpd.testing.conf |
| Perl scripts | perl -c /path/to/script.pl perl -wc /path/to/script.pl |

CentOS Find Out Latest Available Updated Package or Kernel Version