# DNS Server

## 1) What Version the DNS Server it is and Run Status

### a) BIND (Linux) Version

$ /usr/sbin/named -v

### b) BIND Status

$ service named status

### c) Update BIND

patch -Np1 -i ../bind-9.11.2-use\_iproute2-1.patch

## 2) Change BIND configuration files (CentOS)

Now the named.conf file, which is the main file for BIND, must be configured for safer authorizations.. Open the file with any program you favor. For this example, I will be using vim.

vim /etc/named.conf

This is also where one can determine if the server is a slave or master. Normally you define one master server and all others are slave servers:

zone "example.com"{   
 type master;   
 file "example.com";   
 notify yes; // Add this line to enable Notifications }

The following will be what should be on the named.conf file should look like. **Pay attention to the underlined and bolded text**. This text will be comments for what the highlighted configuration should be and why:

options {

# change ( listen all )

listen-on port 53 { any; };  **change ‘any’ to specific host (IP)**

# change if not use IPv6

listen-on-v6 { none; }; **if not explicitly stated or nothing there, assume it’s any**

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";

# query range ( set internal server and so on )

allow-query { localhost; 10.0.0.0/24; }; **Only allow authorized IPs to query**

# transfer range ( set it if you have secondary DNS )

**For the DNS servers in your network that are exposed to the Internet, if zone transfer must be enabled, restrict DNS zone transfers to either DNS servers identified in the zone by name server (NS) resource records or to specific DNS servers in your network.**

allow-transfer { localhost; 10.0.0.0/24; };

**By default, recursion is not disabled for the DNS Server service. This makes it possible for the DNS server to perform recursive queries on behalf of its DNS clients and DNS servers that have forwarded DNS client queries to it. Recursion may be used by attackers to deny the DNS Server service. Therefore, if a DNS server in your network is not intended to receive recursive queries, it should be disabled.**

recursion no;

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";

pid-file "/run/named/named.pid";

session-keyfile "/run/named/session.key";

};

logging {

channel default\_debug {

file "data/named.run";

severity dynamic;

};

};

# change all from here

view "internal" {

match-clients {

localhost;

10.0.0.0/24;

};

zone "." IN {

type hint;

file "named.ca"; };

zone "srv.world" IN {

type master;

file "srv.world.lan";

allow-update { none; }; **ensure that zones are not allowed to be updated by other servers or zones**

};

zone "0.0.10.in-addr.arpa" IN {

type master;

file "0.0.10.db";

allow-update { none; };**ensure that zones are not allowed to be updated by other servers or zones**

};

## 2) Restart Service

The service MUST be restarted after any changes have been made in order for the changes to apply:

systemctl restart named

## 3) CentOS DNS Troubleshooting

If the DNS server does not seem to be running, here is a checklist of some commands you can run to update/see what possible errors there may be:

1. sudo ntpdate time.nist.gov
   1. Sometimes DNS server times are out of whack, this command will update the time
2. sudo named-checkconf
   1. This allows one to see if there are any errors
3. service named status
   1. Shows if service is running, and brief overview if there is an error
4. dig [ip or address]
   1. Shows where the information came from
   2. Shows who the system was looking for
   3. Shows IP to name or reverse
5. If you have edited the files, but you get a failure or you are not able to resolve anything, remember your First, confirm configurations! Take a hard look at the documents you created and ensure you have the right “.” or space or ip address where they should be. Look for little misspellings. Errors messages can help you narrow the search. Try the following command right after your server fails to restart:  
     
   tail -f /var/log/syslog  
     
   This command should give you the last fews lines of errors in your syslog file, which should capture what went wrong and give you a hint as to what to fix. Often there will be a line number of the db file that has the issue! Second, if it is not clear what the issue is from tracing through the configs, it is time to confirm the network from layer 1 and up. Is layer 1 and layer 2 properly configured, i.e. are your interface cards correct and connected to the virtual infrastructure? Do you have layer 3 connectivity? Can you ping end-to-end? A layer 7 protocol, like DNS, cannot work if the lower layers are broken! Often, one link in the chain is broken, causing issues.

## 4) Secure Windows DNS Server Checklist

Windows DNS is more of a GUI. Below will be how to secure your DNS server and zones.

### a) Restrict DNS server to listen only on selected addresses

1. Open DNS Manager.
   1. To open DNS Manager, click **Start**, point to **Administrative Tools**, and then click **DNS**.
2. In the console tree, click the applicable DNS server. Where?
   1. DNS/*applicable DNS server*
3. On the **Action** menu, click **Properties**.
4. On the **Interfaces** tab, click **Only the following IP addresses**.
5. In **IP address**, type an IP address to be enabled for this DNS server , and then click **Add**.
6. Repeat the previous step as necessary to specify other server IP addresses to be enabled for this DNS server. To remove an IP address from the list, click it, and then click **Remove**.

### b) Secure the Server Cache Against Names Pollution

1. Open DNS Manager.
2. In the console tree, click the applicable DNS server. **Where?**
   * DNS/*applicable DNS server*
3. On the **Action** menu, click **Properties**.
4. Click the **Advanced** tab.
5. In **Server options**, select the **Secure cache against pollution** check box, and then click **OK**.

### c) Disable Recursion

1. Open DNS Manager.
2. In the console tree, right-click the applicable DNS server, then click **Properties**. **Where?**
   1. DNS/*applicable DNS server*
3. Click the **Advanced** tab.
4. In **Server options**, select the **Disable recursion** check box, and then click **OK**.

### d) Disable Root Hints

This ensures that if you have an internal DNS root infrastructure, that root hints only point to the DNS root in the internal network not hosts in the internet root domain.

1. Open DNS Manager.
2. In the console tree, click the applicable DNS server. **Where?**
   * DNS/*applicable DNS server*
3. On the **Action** menu, click **Properties**.
4. Click the **Root Hints** tab.
5. Modify server root hints as follows:
   * To add a root server to the list, click **Add**, and then specify the name and IP address of the server to be added to the list.
   * To modify a root server in the list, click **Edit**, and then specify the name and IP address of the server to be modified in the list.
   * To remove a root server from the list, select it in the list, and then click **Remove**.
   * To copy root hints from a DNS server, click **Copy from server**, and then specify the IP address of the DNS server from which you want to copy a list of root servers to use in resolving queries. These root hints will not overwrite any existing root hints.