

Installing Bind9 (System D)

Made by: Aaron Sierra

date created: 02/17/2022

Bind9 version: 1:9.11.5

Note: any text after a box is the command you type.

Overview:

overall steps to install bind9 and get the service up and running.

Note: this is currently in no particular order

- apt install bind9
 - modify the config file to allow forwarders
 - create a local zone
 - create a DB file to manage said zone
 - set DNS to yourself (127.0.0.1)
 - disable dns sec validation
-

Installing bind9

- ☐ apt install bind9

```
root@Communications:/home/cybears# sudo apt install bind9
```

Changing your hostname

First, change your hostname (name of computer) as this is best practice

- ☐ sudo hostnamectl set-hostname {whatever-you-name-box}

```
root@Communications:/home/cybears# hostnamectl set-hostname Communications
```

Then check to see if the command worked

☐ hostname

```
root@Communications:/home/cybears# hostname
Communications
```

Now we are going to change the /etc/hosts file to match

☐ sudo nano /etc/hosts

```
root@Communications:/home/cybears# sudo nano /etc/hosts
```

Here is what the file should look like normally

```
cybears@Communications: ~
File Edit View Search Terminal Help
GNU nano 3.2 /etc/hosts
127.0.0.1 localhost
172.0.0.1 debian
```

Change part A to {your-ip-address} and part B to {your-hostname}

```
cybears@Communications: ~
File Edit View Search Terminal Help
GNU nano 3.2 /etc/hosts
127.0.0.1 A localhost
172.0.0.1 B debian
```

Here is what it should look like after

```
cybears@Communi
File Edit View Search Terminal Help
GNU nano 3.2 /etc/ho
127.0.0.1 localhost
192.168.7.224 Communications
```

Changing /etc/resolv.conf

We are going to change the nameserver

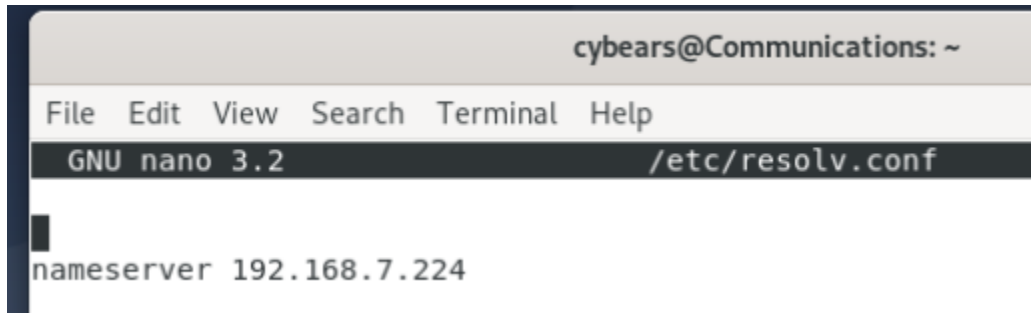
☐ `sudo nano /etc/resolv.conf`

```
root@Communications:/home/cybears# sudo nano /etc/resolv.conf
```

here is the default file:

```
cybears@Communications: ~
File Edit View Search Terminal Help
GNU nano 3.2 /etc/resolv.conf
# Generated by NetworkManager
nameserver 129.62.148.40
```

Change the nameserver to your machines IP address



```
cybears@Communications: ~
File Edit View Search Terminal Help
GNU nano 3.2 /etc/resolv.conf
nameserver 192.168.7.224
```

Note: if you are having an issue with the /etc/resolv.conf folder rewriting itself, you can fix this by deleting the file, recreating it, and naming the file read-only. Usually, you will not have this problem.

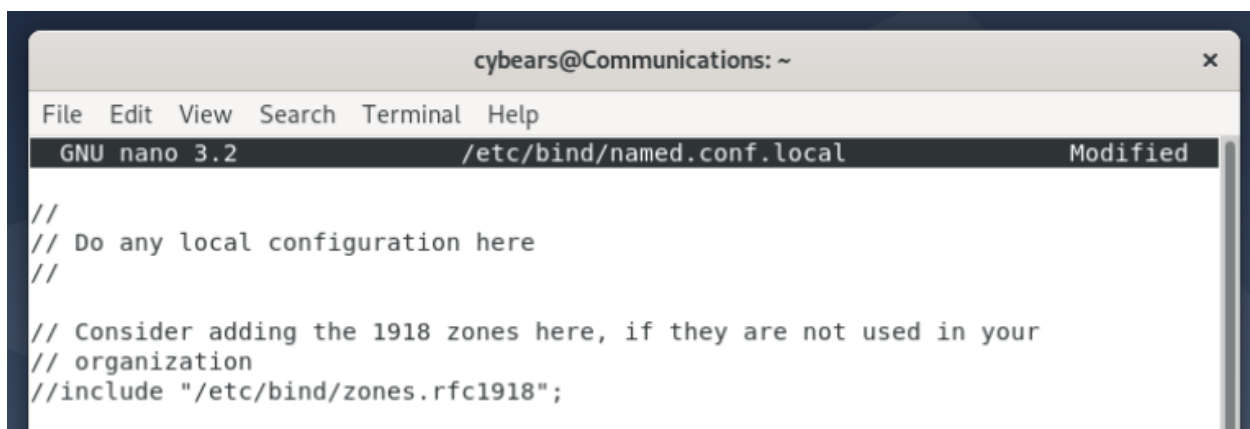
Adding zones

Go into your /etc/bind/named.conf.local file

☐ `sudo nano /etc/bind/named.conf.local`

```
root@Communications:/home/cybears# sudo nano /etc/bind/named.conf.local
```

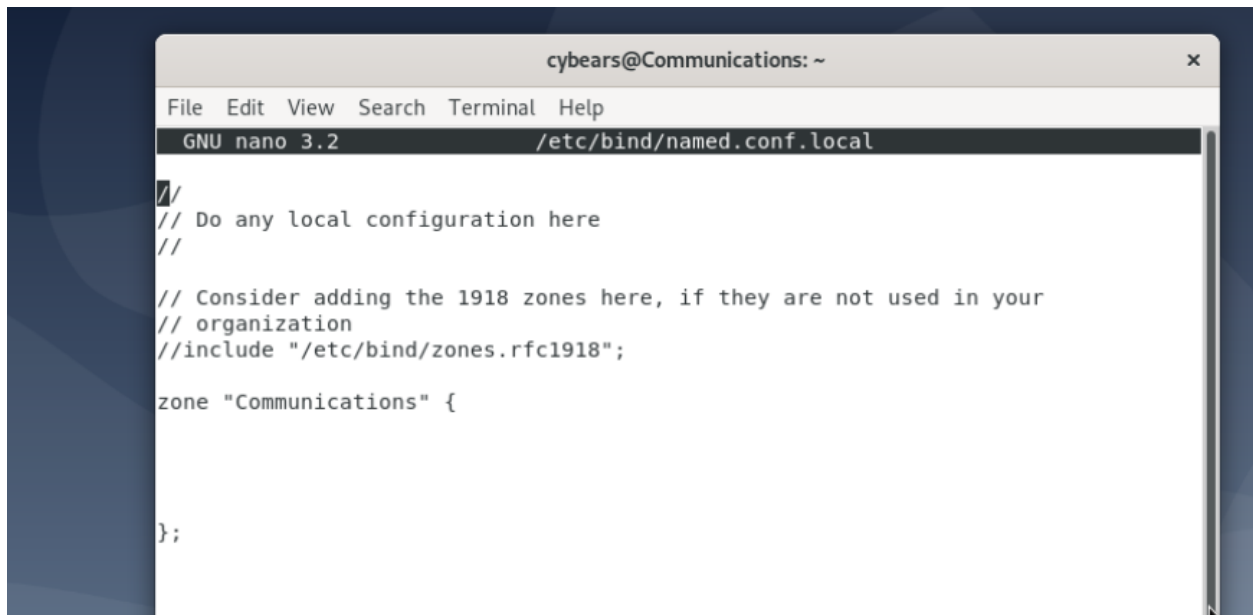
Here is what the file will look like before you edit it



```
cybears@Communications: ~
File Edit View Search Terminal Help
GNU nano 3.2 /etc/bind/named.conf.local Modified
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

We are going to add a zone

☐ `zone "{name-of-zone}" {"};`



```
cybears@Communications: ~
File Edit View Search Terminal Help
GNU nano 3.2 /etc/bind/named.conf.local

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "Communications" {

};
```

Now we are going to specify what exactly we want the zone to be

- ☐ type master;
- ☐ file {filename};

```
zone "Communications" {
    type master;
    file "/etc/bind/zones/db.Communications";
};
```

we specified what the type of DNS was, and where it could find information.

Now we are going to create a zone directory, where we will place a folder

- ☐ `sudo mkdir /etc/bind/zones`

```
root@Communications:/home/cybears# sudo mkdir /etc/bind/zones
```

We are going to copy bind9s local zone folder so that we do not have to write a new one from scratch

☐ `sudo cp /etc/bind/db.local /etc/bind/zones/db.{filename}`

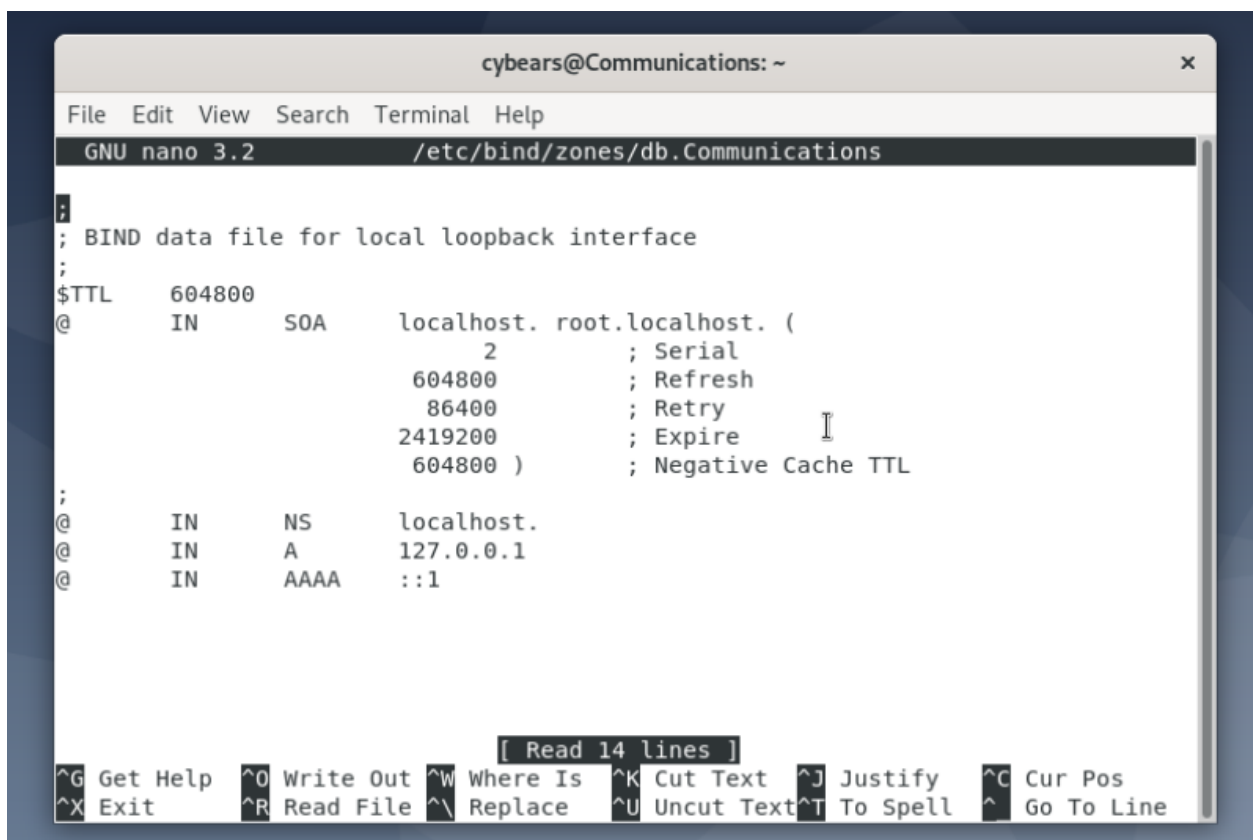
```
root@Communications:/home/cybears# sudo cp /etc/bind/db.local /etc/bind/zones/db.Communications
```

Now we are going to open it and customize the server

☐ `sudo nano /etc/bind/zones/db.{filename}`

```
root@Communications:/home/cybears# sudo nano /etc/bind/zones/db.Communications
```

Here is what the default file looks like



The screenshot shows a terminal window titled "cybears@Communications: ~". Inside, the GNU nano 3.2 editor is open, editing the file "/etc/bind/zones/db.Communications". The file content is as follows:

```
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      localhost. root.localhost. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       localhost.
@         IN      A        127.0.0.1
@         IN      AAAA     ::1
```

At the bottom of the terminal, there is a status bar showing "[Read 14 lines]" and a list of keyboard shortcuts: ^G Get Help, ^O Write Out, ^W Where Is, ^K Cut Text, ^J Justify, ^C Cur Pos, ^X Exit, ^R Read File, ^\ Replace, ^U Uncut Text, ^T To Spell, ^_ Go To Line.

First and foremost, UPDATE THE SERIAL, so bind knows it must update the settings

```
localhost. root.localhost. (
  2 ; Serial
  604800 ; Refresh
  86400 ; Retry
  2419200 ; Expire
  604800 ) ; Negative Cache TTL
```

nunication
/hosts

After

```
3 ; Serial
```

Next you are going to change everything in the list below, notice the differences between the before and after images:

- Change the localhost and root.localhost to your {computername/domainName} (A)
- Change the @ IN to {yourcomputer/DomainName} (B)
- Add any machines you want running through the DNS (C)
- Add Arecords if necessary (D) (*Arecords are assigning a name to an ip, very simple explanation, its not that simple*)

```
cybears@Communications: ~
File Edit View Search Terminal Help
GNU nano 3.2 /etc/bind/zones/db.Communications Modified

;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      Communications. root.Communications. (
                                4               ; Serial
                                604800          ; Refresh
                                86400           ; Retry
                                2419200        ; Expire
                                604800 )      ; Negative Cache TTL
;
@         IN      NS       Communications.
;
@         IN      A        192.168.7.224
Box1      In      A        192.168.7.152
;Are cords
Communications IN      A        192.168.7.224

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

Now we check to see if everything worked properly

- ☐ `sudo named-checkzone {computername/domain} /etc/bind/zones/db.{computer/domain}`

```
root@Communications:/home/cybears# sudo named-checkzone Communications /etc/bind/zones/db.Communications
zone Communications/IN: loaded serial 4
OK
```

NOTE: IF YOU HAVE AN ERRO AND MUST FIX FILE, DO NOT FORGET TO INCREMENT SERIAL NUMBER

Restart the service

- ☐ `sudo systemctl restart bind9.service`

```
root@Communications:/home/cybears# systemctl restart bind9.service
```


☐ `sudo systemctl status bind9.service`

```
root@Communications:/home/cybeares# systemctl status bind9.service
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: en
   Active: active (running) since Fri 2022-02-18 00:07:43 CST; 6s ago
     Docs: man:named(8)
   Process: 1953 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCE
 Main PID: 1954 (named)
    Tasks: 7 (limit: 4915)
   Memory: 15.7M
   CGroup: /system.slice/bind9.service
           └─1954 /usr/sbin/named -u bind

Feb 18 00:07:43 Communications named[1954]: network unreachable resolving './DNS
Feb 18 00:07:43 Communications named[1954]: network unreachable resolving './NS/
Feb 18 00:07:43 Communications named[1954]: network unreachable resolving './DNS
Feb 18 00:07:43 Communications named[1954]: network unreachable resolving './NS/
Feb 18 00:07:43 Communications named[1954]: network unreachable resolving './DNS
Feb 18 00:07:43 Communications named[1954]: network unreachable resolving './NS/
Feb 18 00:07:43 Communications named[1954]: network unreachable resolving './DNS
Feb 18 00:07:43 Communications named[1954]: network unreachable resolving './NS/
Feb 18 00:07:43 Communications named[1954]: managed-keys-zone: Unable to fetch D
Feb 18 00:07:43 Communications named[1954]: resolver priming query complete
lines 1-21/21 (END)
```

NOTE: ANOTHER WAY TO TEST, IS AN NS LOOKUP

From a different computer, type this

☐ `nslookup {computer/domain} {DNS IP address}`

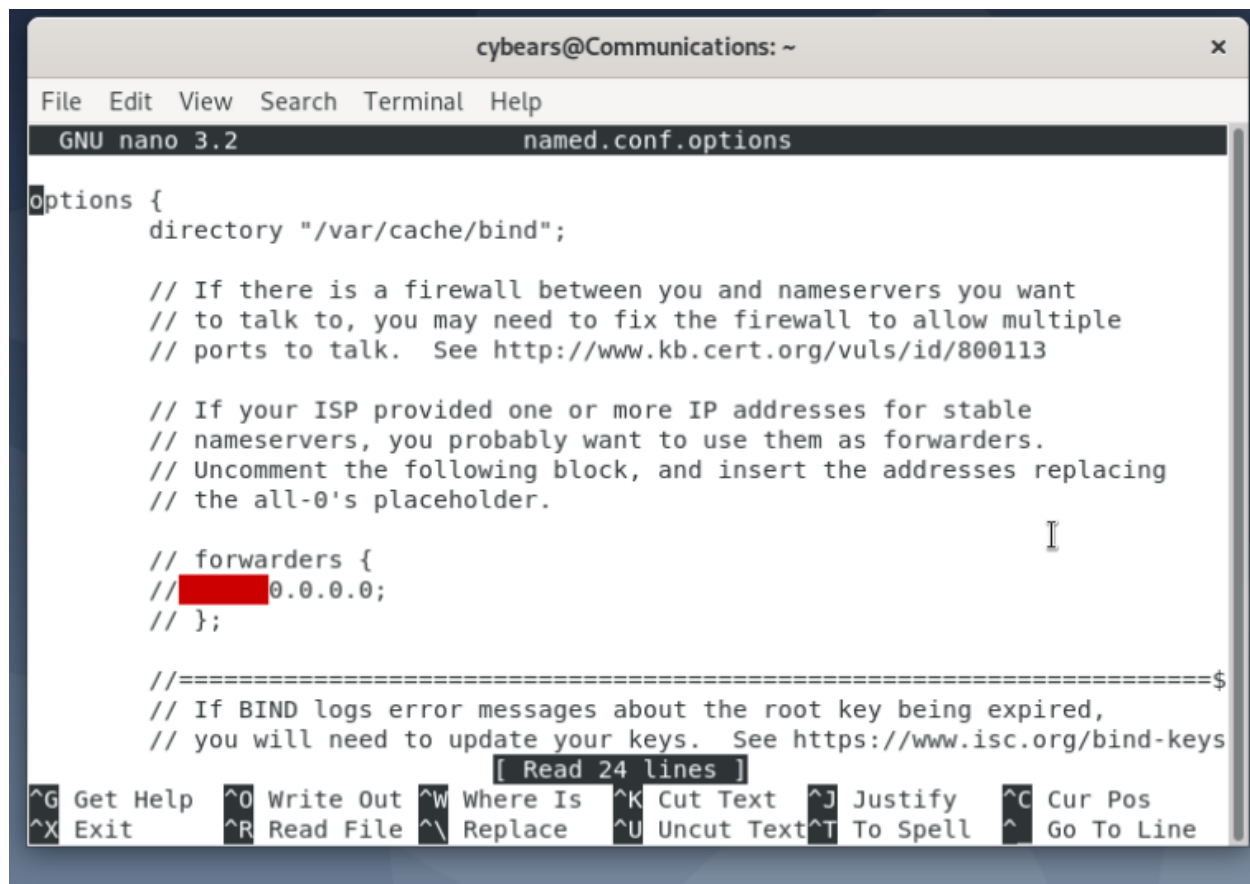
Ensure you keep your internet

The last step is to disable dnssec validation

☐ `nano /etc/bind/named.conf.options`

```
|root@Communications:/etc/bind# nano named.conf.options
```

Here is the file



```
cybears@Communications: ~
File Edit View Search Terminal Help
GNU nano 3.2 named.conf.options

options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    // 0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;

    listen-on-v6 { any; };
};
```

[Read 24 lines]

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

Scroll to this option

```
    // };

    //=====
    // If BIND logs error messages about
    // you will need to update your key
    //=====
    dnssec-validation auto;

    listen-on-v6 { any; };
};
```

Change this to no

```
// you will need to update your key  
//=====  
dnssec-validation no;  
  
listen-on-v6 { any; };
```

NOTE: any box you attach to the dns, must have a fixed ip address. This means you have to disable DHCP



End