

Update AlmaLinux and install Bind

Run the following commands after installing almalinux

```
1 sudo yum update -y
2 sudo firewall-cmd --permanent --add-service=dns
3 sudo firewall-cmd --permanent --add-port=53/udp
4 sudo firewall-cmd --reload
5 sudo dnf update -y
6 sudo dnf install bind bind-utils -y
7 sudo systemctl start named
8 sudo systemctl enable named
9 sudo systemctl status named #Should show active
```

Update Ubuntu and install Bind9

Run the following commands after installing ubuntu

```
1 sudo apt update -y
2 sudo apt install firewalld
3 sudo systemctl stop ufw && systemctl disable ufw
4 sudo firewall-cmd --permanent --add-service=dns
5 sudo firewall-cmd --permanent --add-port=53/udp
6 sudo firewall-cmd --reload
7 sudo apt install bind9 bind9-utils -y
8 sudo systemctl start named
9 sudo systemctl enable named
sudo systemctl status named #Should show active
```

AlmaLinux Bind

Ok next step is to make a few changes to the /etc/named.conf file.

```
1 vi /etc/named.conf
2
3 Comment these lines out:
4 // listen-on port 53 { 127.0.0.1; };
5 // listen-on-v6 port 53 { ::1; };
6
7 Add your home lab subnets to this param:
8 allow-query { localhost;192.168.0.0/16;10.0.0.0/8; }
9
10 Add these blocks of code at the bottom (Modify the 'home.lab' if you are using
11 something different. Also adjust the IP address below. My home subnet is
12 192.168.3.0):
13 //Forward Zone
14 zone "home.lab" IN {
15     type master;
16     file "home.lab.db";
17     allow-update { none; };
18 };
19 //Reverse Zone
20 zone "3.168.192.in-addr.arpa" IN {
21     type master;
22     file "192.168.3.db";
23     allow-update { none; };
24 };
25
26
```

Next step we're going to create the forward zone file. Every time you add a new A record, you will update this file and the reverse zone file, then bounce named. I'll provide an example below.

```

1 vi /var/named/home.lab.db
2 Paste the following code and save (I'm calling my DNS server 'ns1.home.lab'
3 modify it as you please):
4 $TTL 86400
5 @ IN SOA  jellyfin.home.lab. root.home.lab. (
6                                     3      ;Serial
7                                     3600   ;Refresh
8                                     1800   ;Retry
9                                     604800 ;Expire
10                                    86400   ;Minimum
11 TTL
12 )
13
14 ;Name Server Information
15 @      IN  NS      jellyfin.home.lab.
16
17 ;A - Record HostName To Ip Address
    jellyfin      IN  A      192.168.3.6

```

And finally we create the reverse zone file. This allows for reverse DNS lookups (IP Address to FQDN)

```

1 vi /var/named/192.168.3.db
2
3 Paste the following code and save (I'm calling my DNS server 'ns1.home.lab'
4 modify it as you please, and my dns server IP is 192.168.3.6):
5 $TTL 86400
6 @ IN SOA  jellyfin.home.lab. root.home.lab. (
7                                     3      ;Serial
8                                     3600   ;Refresh
9                                     1800   ;Retry
10                                    604800 ;Expire
11                                    86400   ;Minimum TTL
12 )
13
14 ;Name Server Information
15 @      IN  NS      jellyfin.home.lab.
16
17 ;Reverse lookup for Name Server
18 6      IN  PTR      jellyfin.home.lab.

```

Ubuntu Bind9

Ok next step is to make a few changes to the following files

Named.conf.options

Named.conf.local

Named.conf.resolv.conf

```
forwarders {  
# Give here your ISP DNS IP's  
192.168.0.1; # gateway or router  
1.1.1.1;  
8.8.8.8;  
9.9.9.9;  
};
```

vi /etc/bind/named.conf.local

```
//Add your home lab subnets to this param:  
allow-query { localhost;192.168.0.0/16;10.0.0.0/8; }  
  
// Our forward zone  
zone "home.lab" {  
type master;  
file "/etc/bind/zones/home.lab.db";  
allow-update { none; };  
};  
  
// Our reverse Zone  
zone "0.168.192.in-addr.arpa" {  
type master;  
file "/etc/bind/zones/0.168.192.db";  
allow-update { none; };  
};
```

```
mkdir -p /etc/bind/zones
cp /etc/bind/db.local /etc/bind/zones/home.lab.db
vi /etc/bind/zones/home.lab.db
```

```
; BIND data file for local loopback interface
;
$TTL 86400
@ IN SOA  jellyfin.home.lab. root.home.lab. (
        3      ;Serial
        3600   ;Refresh
        1800   ;Retry
        604800 ;Expire
        86400  ;Minimum TTL
)

;Name Server Information
@ IN NS  jellyfin.home.lab.

;A - Record HostName To Ip Address
jellyfin IN A  192.168.0.6
```

```
cp /etc/bind/db.127 /etc/bind/zones/0.168.192.db
vi /etc/bind/zones/0.168.192.db
; BIND reverse data file for local loopback interface
```

```
;
$TTL 86400
@ IN SOA  jellyfin.home.lab. root.home.lab. (
        3      ;Serial
        3600   ;Refresh
        1800   ;Retry
        604800 ;Expire
        86400  ;Minimum TTL
)

;Name Server Information
@ IN NS  jellyfin.home.lab.

;Reverse lookup for Name Server
6 IN PTR jellyfin.home.lab.
```

It's that simple. You can even validate the code for typos, by running the following commands.

```
1sudo named-checkconf /etc/named.conf
2sudo named-checkzone home.lab /var/named/home.lab.db
3sudo named-checkzone 3.168.192.in-addr.arpa /var/named/192.168.3.db
```

```
[root@ns1 named]# sudo named-checkzone home.lab /var/named/home.lab.db
zone home.lab/IN: loaded serial 3
OK
```

Finally, restart named to set it all up.

```
1sudo systemctl restart named
```

Add an A record and test

To add a new record, you will modify both of the zone files, then restart named.

```
1vi /var/named/home.lab.db
2
3Add these lines:
4esxi2  IN A    192.168.3.4
5esxi1  IN A    192.168.3.5
6
7
8vi /var/named/192.168.3.db
9
9Add these lines:
105  IN PTR    esxi1.home.lab.
114  IN PTR    esxi2.home.lab.
12
13Then restart named:
14sudo systemctl restart named
15
```

Testing is just as easy. After you can test locally, I would test from various other machines to make sure it responds to all queries. If it fails, check firewall rules, check allowed subnets, reachability, routes, etc.

```
1Test forward lookup:
2dig esxi1.home.lab +short
3
4Test reverse lookup:
5dig -x 192.168.3.5 +short
```

```
[root@ns1 named]# dig esxi1.home.lab +short
192.168.3.5
[root@ns1 named]# dig -x 192.168.3.5 +short
esxi1.home.lab.
```

Optional: Fix Forwarding

If you're running into an issue where you can only resolve local domains, but not public domains like google.com, then you might try the following steps to see if it resolves your issue.

```
1 vi /etc/named.conf
2
3 Add your extra DNS servers here, or public servers like google.com:
4     forwarders {
5         8.8.8.8;
6         x.x.x.x;
7     };
8     forward only;
9
10 Also modify the dnssec lines below:
11     dnssec-enable no;
12     dnssec-validation no;
```