DNS Lab

Purpose

In this lab you will explore the Domain Name System

Software Requirements

Linux Virtual Machine

References

- https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-ubuntu-16-04
- https://help.ubuntu.com/community/BIND9ServerHowto

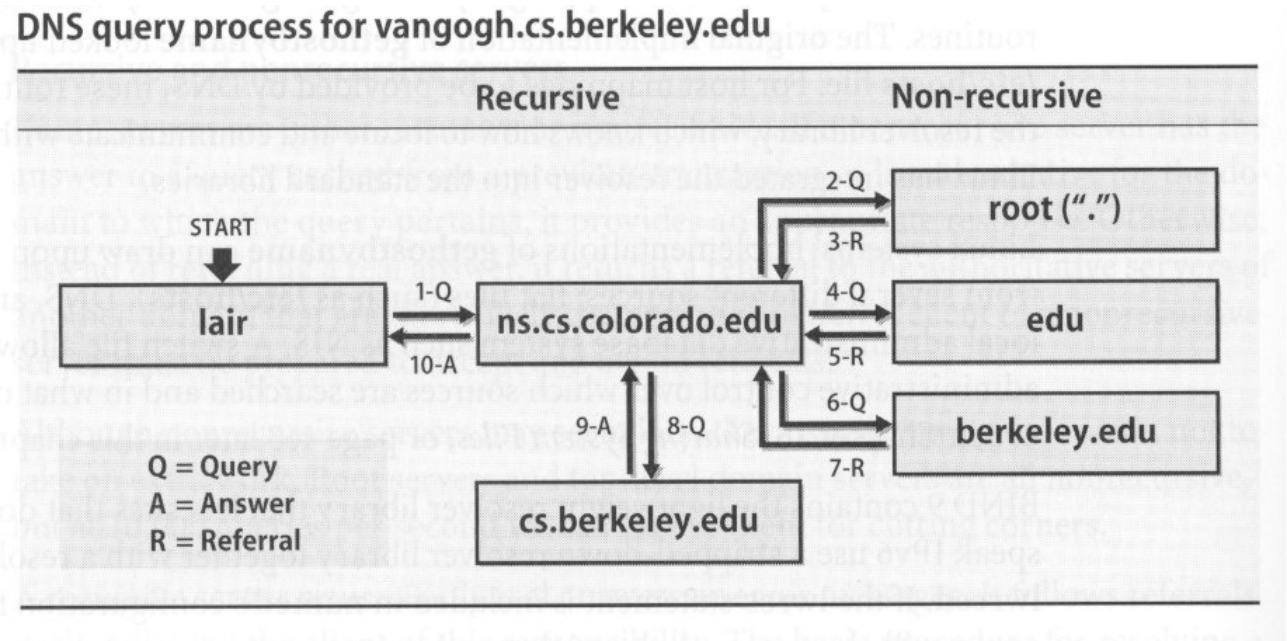
Background

How DNS works

https://www.youtube.com/watch?v=72snZctFFtA

DNS defines

- A hierarchical namespace for hosts and IP addresses
- A distributed database of hostname and address information
- A **"resolver"** to query this database
- Improved routing and sender authentication for email
- A mechanism for finding services on a network
- A protocol used by name servers to exchange information



Recursive query
When the name server of a host cannot resolve a query,
the server issues a query to resolve the query
!Iterative queries
When the name server of a host cannot resolve a query,
it sends a referral to another server to the resolver

Laboratory

Host	Role	FQDN	IP Address
ns1	Primary DNS Server	ns1.yourname.lk	192.168.100.100
ns2	Secondary DNS Server	ns2.yourname.lk	192.168.100.200
host1	Generic Host 1	host1.yourname.lk	192,168.100.50

Before continue this Lab make sure you logged into the system as root or continue with super user permissions

ex:

Installing BIND and Configure

```
bind9
bind9utils
bind9-docs
```

Enable BIND IPV4 only

```
systemctl edit –full bind9
```

Append -4 to the end of ExecStart

```
[Service]
ExecStart=/usr/sbin/named -f -u bind -4
```

Reload the systemd daemon to read the new configuration into the running system

```
systemctl daemon-reload
```

Restart Bind

“ Backup each and every configuration file before you make the changes “
“ Do not copy and paste”

Configure Primary DNS Server

Create an new ACL block called “trusted” to allow the recursive DNS queries from list of clients. (ex: ns2, host1, .. etc)

Add the below entry into the top of /etc/bind/named.conf.options.

```
acl “trusted"{
        192.168.100.50;
        192.168.100.100;
        192.168.100.200;
};
```

Make the highlighted changes into the “options” block in /etc/bind/named.conf.options

```
        directory "/var/cache/bind";

        recursion yes;
        allow-recursion { trusted; };
        listen-on { 192.168.100.128; 127.0.0.1;};
        allow-transfer { 192.168.100.130; };

        forwarders {
                8.8.8.8;
                8.8.4.4;
        };

//       dnssec-validation auto;
//       auth-nxdomain no;    # conform to RFC1035
//       listen-on-v6 { any; };
};
```

Add the below entry to /etc/bind/named.conf.local

```
include “/etc/bind/zones.nibm.lk";
```

Create a new file called zones.nibm.lk in /etc/bind/ directory

Insert the lines into the file

```
zone "yourname.lk" {
      type master;
      file “/etc/bind/zones/db.yourname.lk”;
      also-notify{ 192.168.100.200; };
      allow-transfer { 192.168.100.200; };
};

zone "100.168.192.in-addr.arpa" {
```

```
        type master;
        file "/etc/bind/zones/db.192.168.100";
        also-notify{ 192.168.100.200; };
        allow-transfer { 192.168.100.200; };
};
```

Check BIND Configurations

Checking the syntax of **/etc/bind/named.conf.***

```
named-checkconf
```

Create Forward Zone file

Go to **/etc/bind/zones**
copy /etc/bind/db.local into **/etc/bind/zones** as **db.yourname.lk**

Edit the **/etc/bind/zones/db.yourname.lk** as below

```
$TTL    604800
@       IN      SOA     ns1.yourname.lk. admin.yourname.lk. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;

;name servers
@       IN      NS      ns1.yourname.lk.
@       IN      NS      ns2.yourname.lk.

;name servers - A records
ns1.yourname.lk.        IN      A       192.168.100.128
ns2.yourname.lk.        IN      A       192.168.100.130

;192.168.100.0/24 - A records
host1                   IN      A       192.168.100.50
smallco                 IN      A       192.168.100.10
bigco                   IN      A       192.168.100.20
```

Check Forward Zone Configurations

```
named-checkzone yourname.lk db.yourname.lk
```

Create Reverse Zone file

Go to /etc/bind/zones
copy /etc/bind/db.127 into /etc/bind/zones as db.192.168.100

Edit the /etc/bind/zones/db.192.168.100 as below

```
$TTL    604800
@       IN      SOA     ns1.yourname.lk. admin.yourname.lk. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;

;name servers
@       IN      NS      ns1.yourname.lk.
@       IN      NS      ns2.yourname.lk.

;PTR Records
100     IN      PTR     ns1.yourname.lk.       ;
200     IN      PTR     ns2.yourname.lk.       ;
50      IN      PTR     host1.yourname.lk.     ;
10      IN      PTR     smallco.yourname.lk.   ;
20      IN      PTR     bigco.yourname.lk.     ;
```

Check Reverse Zone Configurations

```
named-checkzone 100.168.192.in-addr.arpa /etc/bind/zones/db.
192.168.100
```

Restart BIND

Configure UFW to Allow BIND

```
ufw allow Bind9
```

Check the system log (/etc/log/syslog) using below command.

```
tail -f /var/log/syslog
```

Configure Secondary DNS Server

Follow the instructions on below article and configure Secondary DNS Server. You might have to troubleshoot everything by yourself. :)

https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-ubuntu-16-04

Configure Client to resolve DNS using Primary and Secondary DNS Servers

Add the below lines into the **/etc/resolv.conf**

```
nameserver 192.168.100.100
nameserver 192.168.100.200
search     yourname.lk
```

Resolving DNS records

```
dig smallco.yourname.lk @192.168.100.100
dig bigco.yourname.lk   @192.168.100.200

dig -x 192.168.100.10 @192.168.100.100
dig -x 192.168.100.20 @192.168.100.200
```