DNS Notes

Monday, November 11, 2024 6:16 PM

Install Bind DNS in machine B
sudo dnf install bind bind-utils

<u>Create a secret key for both for internal view and external view:</u>

```
[root@dns0 ~]# tsig-keygen -a HMAC-MD5 internal-view-tsig
key "internal-view-tsig" {
        algorithm hmac-md5;
        secret "N53z8M6Hcu03Ksw0NhYO4Q==";
};
[root@dns0 ~]# tsig-keygen -a HMAC-MD5 external-view-tsig
key "external-view-tsig" {
        algorithm hmac-md5;
        secret "N343sQLGCRw+OKlnQ12NqQ==";
};
[root@dns0 ~]#
```

we have to edit the /etc/named.conf file:

```
[root@dns0 ~]# cat /etc/named.conf
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
options {
        listen-on port 53 { any; };
#       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";
        secroots-file   "/var/named/data/named.secroots";
        recursing-file  "/var/named/data/named.recursing";
        allow-query     { any; };
        allow-recursion {10.21.32.0/24; 100.64.28.0/24; };
        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;
        dnssec-validation no;
        managed-keys-directory "/var/named/dynamic";
        geoip-directory "/usr/share/GeoIP";
        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
        /* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
```

```
        include "/etc/crypto-policies/back-ends/bind.config";
};
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
key "external-key" {
   algorithm hmac-md5;
   secret "N343sQLGCRw+OKlnQ12NqQ==";
};
key "internal-key" {
   algorithm hmac-md5;
   secret "N53z8M6Hcu03Ksw0NhYO4Q==";
};
/* INTERNAL VIEW - LAN and DMZ */
view "internal" {
   match-clients { key internal-key; !key external-key; 10.21.32.0/24; 100.64.28.0/24; };  # LAN and DMZ
networks
   recursion yes;
   server 100.64.28.6 { keys internal-key; };
   // Root hints for internal view
   zone "." IN {
      type hint;
      file "named.ca";
   };
   // Internal zones
   zone "dundermifflin.com" {
      type primary;
      file "/var/named/db.dundermifflin.com.internal";
      allow-update { none; };
   };
   zone "28.64.100.in-addr.arpa" {
      type primary;
      file "/var/named/db.100.64.28.internal";
      allow-update { none; };
   };
   zone "32.21.10.in-addr.arpa" {
      type primary;
      file "/var/named/db.10.21.32.internal";
      allow-update { none; };
   };
};
/* EXTERNAL VIEW - Public Access */
view "external" {
   match-clients { key external-key; !key internal-key; any; };  # All other networks
   recursion no;
   server 100.64.28.6 { keys external-key; };
   // Root hints for external view
   zone "." IN {
      type hint;
      file "named.ca";
   };
   // External zones
   zone "dundermifflin.com" {
      type primary;
      file "/var/named/db.dundermifflin.com.external";
```

```
    allow-update { none; };
  };
  zone "28.64.100.in-addr.arpa" {
    type primary;
    file "/var/named/db.100.64.28.external";
    allow-update { none; };
  };
};
include "/etc/named.root.key";
```

After doing this we have to create zone files for the dundermifflin.com. domain, reverse DNS for the DMZ and LAN networks and recursive for everything else:

Create these files in ***/var/named/***

db.dundermifflin.com.internal

db.dundermifflin.com.external

db.100.64.28.internal

db.100.64.28.external

db.10.21.32.internal

```
[root@dns0 ~]# cat /var/named/db.dundermifflin.com.external
@   IN  SOA dns0.dundermifflin.com. arma2040.dundermifflin.com. (
            2024110918 ; Serial yyyymmddhh
            1d         ; Refresh
            1h         ; Retry
            7d         ; Expire
            1h         ; Negative Cache TTL
        )
; NS Records
    IN  NS  dns0.dundermifflin.com.
    IN  NS  dns1.dundermifflin.com.

; A Records
router             1h  IN  A   100.64.0.28
dmz                1h  IN  A   100.64.28.1
dns0               1h  IN  A   100.64.28.2
web0               1h  IN  A   100.64.28.3
web1               1h  IN  A   100.64.28.4
dns1               1h  IN  A   100.64.28.6
bsd                1h  IN  A   100.64.28.7
dundermifflin.com. 5m  IN  A   100.64.28.3

; CNAME Records
machinea   7d IN  CNAME  router.dundermifflin.com.
machineb   7d IN  CNAME  dns0.dundermifflin.com.
machinec   7d IN  CNAME  web0.dundermifflin.com.
machined   7d IN  CNAME  web1.dundermifflin.com.
machinef   7d IN  CNAME  dns1.dundermifflin.com.
machinex   7d IN  CNAME  bsd.dundermifflin.com.
;dundermifflin.com           5m IN  CNAME  web0.dundermifflin.com.
www        5m IN  CNAME  web0.dundermifflin.com.
www1       5m IN  CNAME  web1.dundermifflin.com.
dns        5m IN  CNAME  dns0.dundermifflin.com.
[root@dns0 ~]#
```

```
[root@dns0 ~]# cat /var/named/db.dundermifflin.com.internal
@   IN  SOA dns0.dundermifflin.com. arma2040.dundermifflin.com. (
            2024110918 ; Serial yyyymmddhh
            1d         ; Refresh
            1h         ; Retry
            7d         ; Expire
            1h         ; Negative Cache TTL
        )
; NS Records
    IN  NS  dns0.dundermifflin.com.
    IN  NS  dns1.dundermifflin.com.

; A Records
router             1h  IN  A   100.64.0.28
dmz                1h  IN  A   100.64.28.1
dns0               1h  IN  A   100.64.28.2
web0               1h  IN  A   100.64.28.3
web1               1h  IN  A   100.64.28.4
lan                1h  IN  A   10.21.32.1
nfs                1h  IN  A   10.21.32.2
dns1               1h  IN  A   100.64.28.6
bsd                1h  IN  A   100.64.28.7
dundermifflin.com. 5m  IN  A   100.64.28.3

; CNAME Records
machinea   7d IN  CNAME  router.dundermifflin.com.
machineb   7d IN  CNAME  dns0.dundermifflin.com.
machinec   7d IN  CNAME  web0.dundermifflin.com.
machined   7d IN  CNAME  web1.dundermifflin.com.
machinee   7d IN  CNAME  nfs.dundermifflin.com.
machinef   7d IN  CNAME  dns1.dundermifflin.com.
machinex   7d IN  CNAME  bsd.dundermifflin.com.
;dundermifflin.com           5m IN  CNAME  web0.dundermifflin.com.
www        5m IN  CNAME  web0.dundermifflin.com.
www1       5m IN  CNAME  web1.dundermifflin.com.
dns        5m IN  CNAME  dns0.dundermifflin.com.
files      7d IN  CNAME  nfs.dundermifflin.com.
[root@dns0 ~]#
```

```
[root@dns0 ~]# cat /var/named/db.100.64.28.internal
@   IN  SOA dns0.dundermifflin.com. arma2040.dundermifflin.com. (
            2024110918 ; Serial
            1d         ; Refresh
            1h         ; Retry
            7d         ; Expire
            1h         ; Negative Cache TTL
        )
; NS Records
    IN  NS  dns0.dundermifflin.com.
    IN  NS  dns1.dundermifflin.com.

; PTR Records
1  1h IN  PTR  dmz.dundermifflin.com.
2  1h IN  PTR  dns0.dundermifflin.com.
3  1h IN  PTR  web0.dundermifflin.com.
4  1h IN  PTR  web1.dundermifflin.com.
6  1h IN  PTR  dns1.dundermifflin.com.
7  1h IN  PTR  bsd.dundermifflin.com.
[root@dns0 ~]#
```

```
[root@dns0 ~]# cat /var/named/db.100.64.28.external
@   IN  SOA dns0.dundermifflin.com. arma2040.dundermifflin.com. (
            2024110918 ; Serial
            1d         ; Refresh
            1h         ; Retry
            7d         ; Expire
            1h         ; Negative Cache TTL
        )
; NS Records
    IN  NS  dns0.dundermifflin.com.
    IN  NS  dns1.dundermifflin.com.

; PTR Records
1  1h IN  PTR  dmz.dundermifflin.com.
2  1h IN  PTR  dns0.dundermifflin.com.
3  1h IN  PTR  web0.dundermifflin.com.
4  1h IN  PTR  web1.dundermifflin.com.
6  1h IN  PTR  dns1.dundermifflin.com.
7  1h IN  PTR  bsd.dundermifflin.com.
[root@dns0 ~]#
```

```
[root@dns0 ~]# cat /var/named/db.10.21.32.internal
@   IN  SOA dns0.dundermifflin.com. arma2040.dundermifflin.com. (
            2024110918 ; Serial
            1d         ; Refresh
            1h         ; Retry
            7d         ; Expire
            1h         ; Negative Cache TTL
        )
; NS Records
    IN  NS  dns0.dundermifflin.com.
    IN  NS  dns1.dundermifflin.com.

; PTR Records
1  1h IN  PTR  lan.dundermifflin.com.
2  1h IN  PTR  nfs.dundermifflin.com.
[root@dns0 ~]#
```

After creating the zone files we have to restart the DNS server
systemctl restart named

In machine F
install BIND DNS server by using:
sudo apt install bind9 bind9utils bind9-doc

After installing we have to edit the ***/etc/bind/named.conf and /etc/bind/named.conf.options***

```
root@dns1:~# cat /etc/bind/named.conf.options
options {
        listen-on port 53 { any; };
        directory "/var/cache/bind";
        allow-query { any; };
        recursion no;
        // 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 no;

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

```
root@dns1:~# cat /etc/bind/named.conf
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

// Root hints for resolving outside the local domain

key "external-key" {
        algorithm hmac-md5;
        secret "N343sQLGCRw+OKlnQ12NqQ==";
};

key "internal-key" {
        algorithm hmac-md5;
        secret "N53z8M6Hcu03Ksw0NhYO4Q==";
};

view "internal" {
    match-clients { key internal-key; !key external-key; 10.21.32.0/24; 100.64.28.0/24; };
    recursion yes;
    server 100.64.28.2 { keys internal-key; };
    // Internal zone files - synchronized as secondary from Machine B
    zone "dundermifflin.com" {
        type secondary;
        file "/var/cache/bind/db.dundermifflin.com.internal";
        primaries { 100.64.28.2; };
    };

    zone "28.64.100.in-addr.arpa" {
        type secondary;
        file "/var/cache/bind/db.100.64.28.internal";
        primaries { 100.64.28.2; };
    };

    zone "32.21.10.in-addr.arpa" {
        type secondary;
        file "/var/cache/bind/db.10.21.32.internal";
        primaries { 100.64.28.2; };
    };
};

view "external" {
        match-clients { key external-key; !key internal-key; any; };
        recursion no;
        server 100.64.28.2 { keys external-key; };
    // External zone files - synchronized as secondary from Machine B
    zone "dundermifflin.com" {
        type secondary;
        file "/var/cache/bind/db.dundermifflin.com.external";
        primaries { 100.64.28.2; };
    };

    zone "28.64.100.in-addr.arpa" {
        type secondary;
        file "/var/cache/bind/db.100.64.28.external";
        primaries { 100.64.28.2; };
    };
};

include "/etc/bind/named.conf.options";
// include "/etc/bind/named.conf.local";
// include "/etc/bind/named.conf.default-zones";
root@dns1:~#
```

After doing these configurations restart the service
systemctl restart named

To verify the configuration
if I do nslookup outside the VPN for LAN machine it will throw error

```
C:\Users\ARAVINDH GOUTHAM M>nslookup nfs.dundermifflin.com 100.64.28.6
Server:  dns1.dundermifflin.com
Address:  100.64.28.6

*** dns1.dundermifflin.com can't find nfs.dundermifflin.com: Non-existent domain

C:\Users\ARAVINDH GOUTHAM M>nslookup nfs.dundermifflin.com 100.64.28.2
Server:  dns0.dundermifflin.com
Address:  100.64.28.2

*** dns0.dundermifflin.com can't find nfs.dundermifflin.com: Non-existent domain

C:\Users\ARAVINDH GOUTHAM M>
```

For DMZ machine it will show:

```
C:\Users\ARAVINDH GOUTHAM M>nslookup web0.dundermifflin.com 100.64.28.2
Server:  dns0.dundermifflin.com
Address:  100.64.28.2

Name:    web0.dundermifflin.com
Address:  100.64.28.3


C:\Users\ARAVINDH GOUTHAM M>nslookup web0.dundermifflin.com 100.64.28.6
Server:  dns1.dundermifflin.com
Address:  100.64.28.6

Name:    web0.dundermifflin.com
Address:  100.64.28.3
```

After doing these we have to change the DHCP configurations for the Machine's name server:

```
option domain-name "dundermifflin.com";
option domain-name-servers 100.64.28.2, 100.64.28.6;
default-lease-time 600;
max-lease-time 600;
```

And change the resolv.conf in machine A manually

```
[root@router dhcp]# cd ~
[root@router ~]# cat /etc/resolv.conf
search dundermifflin.com
nameserver 100.64.28.2
nameserver 100.64.28.6
[root@router ~]#
```