Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

BIND 9 Configure Views To Partition External and Internal DNS Information

Posted by Vivek Gite <vivek@nixcraft.com>

[1]

How do I configure Bind 9 dns server views to allow a single nameserver in my DMZ to make different sets of data available to different sets of clients? For example, I'd like to run recursion, some other data for LAN users (192.168.1.0/24), and for the Internet user I'd like to display limited DNS data without recursion. How do I configure views to partition external (Internet) and internal (LAN) DNS information?

[2]

You need to edit /etc/named.conf or /var/named/chroot/etc/named.conf file, run (the following configuration is tested on FreeBSD and RHEL 5.x BIND 9 servers):

```
# vi /var/named/chroot/etc/named.conf
```

Append the following and define internal subnet (192.168.1.0/24 and localhost with full access and recursion):

```
acl internal {
   192.168.1.0/24;
   localhost;
};
```

Define zone and other data as per your requirements:

```
//
// Lan zone recursion is the default
//
view "internal-view" {
  match-clients { internal; };
  zone "." IN {
    type hint;
    file "db.cache";
  };
  zone "internal.nixcraft.com " IN {
    type master;
    file "zones/lan.master.nixcraft.com";
    allow-transfer { key TRANSFER; };
  };
};
//
// external zone w/o recursion
//
view "external-view" {
  match-clients { any; };
  recursion no;
  zone "nixcraft.com " IN {
    type master;
    file "zones/internet.master.nixcraft.com";
    allow-transfer { key TRANSFER; };
  };
};
```

Make sure you configure TSIG as described here [3].

Create Zone Files

First, create required directories, enter:

```
# mkdir -p /var/named/chroot/var/named/zones
# chown named:named /var/named/chroot/var/named/zones
```

Create Internal Zone With LAN IP Data

Edit /var/named/chroot/var/named/zones/lan.master.nixcraft.com, run:

```
# vi /var/named/chroot/var/named/zones/lan.master.nixcraft.com
```

Append the data, enter:

```
$ORIGIN nixcraft.com.
$TTL 3h
@        IN SOA ns1.nixcraft.com. vivek.nixcraft.com. (
                        20080703328        ; Serial yyyymmddnn
                        3h                ; Refresh After 3 hours
                        1h                ; Retry Retry after 1 hour
                        1h                ; Expire after 1 week 1w
                        1h)             ; Minimum negative caching of 1 hour

@                           IN NS    ns1.nixcraft.com.
@                           IN NS    ns2.nixcraft.com.

@                       3600 IN MX 10 mail1.nixcraft.com.
@                       3600     IN MX 20 mail2.nixcraft.com.

@                       3600    IN A     208.43.79.236
ns1                     3600    IN A     208.43.138.52
ns2                     3600    IN A     75.126.168.152
mail1                   3600    IN A     208.43.79.236
mail2                   3600    IN A     67.228.49.229
out-router              3600    IN A     208.43.79.100
; lan data
wks1                    3600    IN A     192.168.1.5
wks2                    3600    IN A     192.168.1.5
wks3                    3600    IN A     192.168.1.5
in-router               3600    IN A     192.168.1.254
; add other lan specifc data below
```

Edit /var/named/chroot/var/named/zones/internet.master.nixcraft.com, run:

```
# vi /var/named/chroot/var/named/zones/internet.master.nixcraft.com
```

Same as above but no internal data:

```
$ORIGIN nixcraft.com.
$TTL 3h
@        IN SOA ns1.nixcraft.com. vivek.nixcraft.com. (
                        20080703328        ; Serial yyyymmddnn
                        3h                ; Refresh After 3 hours
                        1h                ; Retry Retry after 1 hour
                        1h                ; Expire after 1 week 1w
                        1h)             ; Minimum negative caching of 1 hour

@                           IN NS    ns1.nixcraft.com.
@                           IN NS    ns2.nixcraft.com.

@                       3600 IN MX 10 mail1.nixcraft.com.
@                       3600     IN MX 20 mail2.nixcraft.com.

@                       3600    IN A     208.43.79.236
ns1                     3600    IN A     208.43.138.52
ns2                     3600    IN A     75.126.168.152
mail1                   3600    IN A     208.43.79.236
```

```
mail2                   3600    IN A     67.228.49.229
out-router              3600    IN A     208.43.79.100
```

Finally, reload data:

```
# rndc reload
```

Test it, enter:

```
$ ping in-router.nixcraft.com
$ ping out-router.nixcraft.com
```

Recommend readings:

- Bind Security: Transaction [3] Signatures (TSIG) Configuration
- named.conf, and named man page
- BIND 9 Administrator Reference Manual