Response Policy Zones

Response Policy Zones (or RPZ's) are special bind9 zones that can be used to mask or rewrite some DNS responses. Typical uses include specifc name blocking, website redirection or offline operation of zones outside an organization's administrative reach.

Steps to configure an RPZ

1. In named.conf, include the 'response policy' statement:

```
options {
        directory "/opt/bbsigner";
        allow-recursion {127.0.0.1; ::1;};
        listen-on port 5301 { any; };
        listen-on-v6 port 5301 { none; };

        response-policy {
                zone "dpol" policy given;
        } recursive-only no;
};

zone "dpol" {
        type master;
        file "/v/dfiles/rpz/dpol.policy.db";
};
```

1. Configure the rpz zone, file dpol.policy.db:

```
$TTL 10
$ORIGIN dpol.
;

@        IN     SOA dpol. Hostmaster.LACNIC.NET. (
                                106        ; serial
                                7200       ; refresh (2 hours)
                                3600       ; retry (1 hour)
                                648736     ; expire (1 week 12 hours 12
minutes 16 seconds)
                                600        ; minimum (10 minutes)
                                )

;; AUTHORITY SECTION:
@       IN      NS localhost.

;; policy sections
;; note that the policy record DOES NOT END on a dot
eventos.yahoo.com       IN      CNAME   10
eventos.lanacion.com.ar IN      CNAME   10
eventos.lacnic.net      IN      CNAME   10
networking.lacnic.net   IN      CNAME   10
nuc1.lacnic.net         IN      CNAME   10
10                      IN      A       192.168.1.10

;;
;;
```

Note that the left-side names (eventos.yahoo.com) are not terminated in a dot, meaning that they are names relative to $ORIGIN. This is key for the correct operatio of the policy zone.

This policy zone actually points the names "eventos.yahoo.com", "networking.lacnic.net" to a CNAME record which in turn points them to the IP address 192.168.1.10.

The zone itself is a normal zone. It can be slaved from other servers, etc.

Verifying the operation of the RPZ

Using dig, a check similar to this can be performed:

```
carlos@potomac ~> dig @192.168.1.10 eventos.lacnic.net.

; <<>> DiG 9.8.3-P1 <<>> @192.168.1.10 eventos.lacnic.net
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;eventos.lacnic.net.            IN      A

;; ANSWER SECTION:
eventos.lacnic.net.     5       IN      CNAME   10.dpol.
10.dpol.                10      IN      A       192.168.1.10

;; AUTHORITY SECTION:
dpol.                   10      IN      NS      localhost.

;; Query time: 2 msec
;; SERVER: 192.168.1.10#53(192.168.1.10)
```

Note how the absolute (including a finishing dot) query for "eventos.lacnic.net." is nevertheless transformed into a query inside the rpz, the 'dpol' zone in this example.