INDOSYSADMIN

KONFIGURASI BIND RPZ

FROM ZERO TO HORE!

by Pujo Mulyono

indosysadmin.org

KONFIGURASI RECURSIVE

Recursive adalah usaha mendapatkan answer dari hirarki/external DNS

Sebetulnya default instalasi BIND adalah open recursive, dan sudah kita set tidak aktif sebelumnya saat sebagai authoritave only melalui **named.conf.option**

```
allow-recursion { none; };
```

Baris di atas itu dirubah menjadi misalnya

```
allow-recursion {
    192.168.0.0/16;
    172.16.0.0/12;
    10.0.0.0/8;
  };
```

yang mana ditambahkan 3 blok ip yang diperbolehkan untuk query recursive

```
recursive-clients 5000;
```

Default value recursive client 1000, ini adalah batas jumlah concurrent queries yg diijinkan untuk dihandle oleh BIND, pada server yang sibuk dan resourcesnya mencukupi batas ini bisa kita naikkan menjadi 5000 atau 10000, misalnya

max-udp-size 2048;

Default value untuk max-udp-size adalah 4096 bytes, nilai ini sebenarnya terlalu besar untuk sebuah record, 1 byte mewakili 1 character/huruf. Normalnya jarang sekali ukuran type record yang hingga lebih dari 2000 huruf, tetapi mungkin saja terjadi jika ada multiple TXT record atau Multiple CNAME dari suatu record hingga resolved. DNS Amplification Attack menggunakan kelemahan max-udp-size ini utk mengamplify query size yg umumnya berupa trafik ini dibawah 50 bytes mengakibatkan answer sebesar 4096 bytes, sehingga trafik out menjadi 100x lipat dari trafik in, itu yg disebut dengan istilah amplify.

max-cache-size 256M;

Default cache size adalah 32M, nilai ini mungkin terlalu kecil jadi perlu dinaikkan karena cache adalah penting bagi recursor, jika data ada di cache maka tidak dilakukan query ke luar, melainkan data yang ada di cache yang diberikan sebagai jawaban. Menaikkan nilai ini mengakibatkan DNS recursor lebih responsif. Setiap record yang TTL nya belum habis akan disimpan ke dalam cache, semakin banyak queries maka semakin cepat cache terisi. Perlu diketahui bahwa penggunaan RAM pada OS mungkin bisa mencapai 4x lipat dari nilai max cache size yang diset.

listen-on {127.0.0.1; 10.11.12.13; };

Pada server yang memiliki banyak ip address, mungkin perlu diset agar DNS server hanya listen di ip tertentu saja. By default BIND akan listen on any ip address yag ada di server

KONFIGURASI RPZ SLAVE ZONE

Untuk mengaktifkan slave rpz zone maka kita harus mengedit file **named.conf**

```
zone "trustpositifkominfo" {
        type slave;
        masters { 103.154.123.130; 139.255.196.202; };
        file "slave.trustpositifkominfo";
        notify explicit;
        masterfile-format text;
};
```

Selanjutnya, kita edit file **named.conf.options**

```
response-policy {
        zone "trustpositifkominfo"
           policy cname lamanlabuh.aduankonten.id
           max-policy-ttl 30
           log no;
        }
        recursive-only yes
        qname-wait-recurse no
        break-dnssec yes
        nsip-wait-recurse no;
```

Selanjutnya, kita cek dulu konfigurasi dengan perintah **named-checkconf /etc/bind/named.conf**
Lalu, jika tidak ada kesalahan, kita restart Bind dengan perintah **systemctl restart named**

CONFIGURATION REFFERENCE

Referensi untuk konfigurasi BIND bisa dipelajari di link di bawah ini

https://bind9.readthedocs.io/en/latest/reference.html

KNOWLEGDE BASE

Bahan bacaan BIND yang lebih lengkap tersedia pada knowledge base di link di bawah ini

https://kb.isc.org/v1/docs/aa-01310