



tux.cl
sitio de tux en chile

[Historia](#)

[TuxTips](#)

[Artículos](#)

[Eventos](#)

[Screenshots](#)

[Info](#)

[Links](#)

[Contacto](#)

100% Libre de M\$

[Principal](#) > [Artículos](#) > [Redes](#)

Configuración de Multiple Views en BIND 9.x

Juan Pablo Tamayo L. jtamayo@tux.cl
Viernes, 11 de Enero del 2002.

Introducción

Multiple Views, o Vistas Múltiples, es una de las nuevas características de la versión 9 de **BIND**, y es una mejora a la opción conocida como **Split DNS**, disponible en la versión 8 de BIND, y que permiten mantener DNS duales.

Un DNS dual significa que la información de la zona interna y la zona externa para un determinado dominio se encuentra en el mismo servidor de nombres. Es decir, podemos mantener el DNS interno, con datos de zona direccionados a IP's privadas, y el DNS externo, con los datos de zona apuntando a direcciones IP públicas, en una única máquina física.

Típicamente el Split DNS opera en el gateway de la red privada hacia la Internet, levantando dos programas (**daemons**), llamados **named**. Un primer **named** configurado con la información de la zona externa y dicha zona enlazada a la tarjeta de red externa (eth0), con la opción **listen-on**. Y el segundo **named** configurado con la información de la zona interna y dicha zona enlazada a la tarjeta de red interna (eth1).

De manera que si la consulta entra por la interfaz de red externa, desde la Internet por ejemplo, el **named** escuchando en esa interfaz devolverá información relativa a la zona externa (www.dominio.cl = IP pública), mientras que si la consulta entra por la interfaz de red interna, desde la LAN, el **named** escuchando en esa interfaz devolverá información relativa a la zona interna (www.dominio.cl = IP privada).

Con el uso de la declaración **view** en **/etc/named.conf**, BIND 9.x permite configurar un servidor de nombres para que conteste las consultas de algunos clientes de una manera diferente a como les contesta a otros, esto es sobre todo útil si se quiere que los clientes externos a la red local no puedan realizar una consulta DNS en particular o ver un tipo determinado de información, mientras que al mismo tiempo permitir que los clientes internos si puedan hacerlo.

La declaración **view** utiliza la opción **match-clients** para identificar direcciones IP o redes enteras y entregarles opciones y datos de zona especiales.

Las ventajas en comparación a Split DNS es que Multiple Views levanta un único **daemon**, por lo que consume menos recursos, y la información de la zona no se amarra a una dirección IP del servidor sino que dependerá de la dirección IP del cliente. Con esto ya no necesitamos ejecutar el DNS en la máquina que hace de gateway, típicamente un firewall GNU/Linux, hacia la Internet (lo cual es altamente inapropiado IMHO). Ni tampoco necesitamos que la máquina DNS posea dos interfaces de red (física o virtual).

Escenario del ejemplo

En el ejemplo a continuación se muestran los archivos de configuración para el programa **named** que representan el siguiente escenario:

Red Interna (clientes): 192.168.0.0/24 (segmento de direcciones privadas)
Red DMZ (servidores): 192.168.10.0/24 (segmento de direcciones privadas)
Red Externa (Internet): 172.30.30.128/28 (segmento de direcciones públicas)

Todos los servidores en la red privada DMZ son accedados desde la Internet gracias a NAT estáticos configurados en el Firewall.

Los servidores en la red DMZ son accedados desde la red Interna directamente a su dirección DMZ sin NAT, ruteados eso si por el FireWall.

Nombre de Máquina	Dirección pública (NAT)	Dirección privada
-------------------	-------------------------	-------------------

ns.mi-dominio.cl	172.30.30.130	192.168.10.130
correo.mi-dominio.cl	172.30.30.131	192.168.10.131
mail.mi-dominio.cl	172.30.30.132	192.168.10.132
webmail.mi-dominio.cl	172.30.30.133	192.168.10.133
www.mi-dominio.cl	172.30.30.134	192.168.10.134

Archivos de configuración de ejemplo

/etc/named.conf

```

options {
    directory "/var/named";
    version "surely you must be joking";
    query-source address * port 53;
    auth-nxdomain yes;
    allow-query { any; };
    recursion no;
};

view "internal" {
    match-clients { 192.168.0.0/16; 127.0.0.0/8; };
    recursion yes;
    zone "mi-dominio.cl" IN {
        type master;
        file "int.mi-dominio.cl";
        allow-transfer { any; };
        allow-update { none; };
    };

    zone "10.168.192.in-addr.arpa" IN {
        type master;
        file "int.mi-dominio.rev";
        allow-transfer { any; };
        allow-update { none; };
    };

    zone "." IN {
        type hint;
        file "named.ca";
    };

    zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
    };

    zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
    };
};

view "external" {
    match-clients { any; };

```

```

recursion no;
zone "mi-dominio.cl" IN {
    type master;
    file "ext.mi-dominio.cl";
    allow-transfer { none; };
    allow-update { none; };
};

zone "30.30.172.in-addr.arpa" IN {
    type master;
    file "ext.mi-dominio.rev";
    allow-transfer { none; };
    allow-update { none; };
};

zone "." IN {
    type hint;
    file "named.ca";
};

};

key "key" {
    algorithm hmac-md5;
    secret "GpD0LTIdSetvjBSgLramNOEEsjglVuiAckhEcnhiykGLEEiZAQvzYjSogcDT";
};

```

Actualización: En las zonas externas se ha dejado la línea:

```
allow-transfer { none; };
```

como una medida de seguridad para bloquear las transferencias de zonas desde la Internet. En caso de necesitar que algún servidor de nombres externo sea nuestro DNS secundario, deberemos cambiar las líneas necesarias desde el `/etc/named.conf` a:

```
allow-transfer { ip.dns.externo.cl; };
```

además de agregar las líneas:

```
IN      NS      dns.externo.cl.
```

en los respectivos `/var/named/ext.mi-dominio.cl` y `/var/named/ext.mi-dominio.rev`

Gracias a [Carlos Jara](#) por el comentario ;-)

Observación: La sentencia `key "key" ...` **no** debe ser copiada y esta solo a modo de ejemplo, la key o llave será distinta en cada servidor DNS, y es la autenticación utilizada para administrar remotamente servidores de nombres utilizando **rndc(8)** y **rndc.conf(5)**. [pero eso es materia para otro artículo :-p]

```
-----
/var/named/int.mi-dominio.cl
-----
```

```

$ORIGIN mi-dominio.cl.
@      IN      SOA      mi-dominio.cl. root.mi-dominio.cl. (
                                2001120401 ; Serial
                                28800      ; Refresh
                                14400      ; Retry
                                3600000    ; Expire
                                86400 )    ; Minimum
                                IN      NS      ns.mi-dominio.cl.
                                IN      NS      correo.mi-dominio.cl.

```

```

                IN      MX      5 correo
                IN      MX      10 mail

ns              IN      A       192.168.10.130
correo         IN      A       192.168.10.131
mail          IN      A       192.168.10.132
webmail       IN      A       192.168.10.133
www           IN      A       192.168.10.134

```

/var/named/int.mi-dominio.rev

```

@              IN      SOA      mi-dominio.cl. root.mi-dominio.cl. (
                2001101701 ; Serial
                28800     ; Refresh
                14400     ; Retry
                3600000   ; Expire
                86400    ) ; Minimum

                IN      NS      ns.mi-dominio.cl.
                IN      NS      correo.mi-dominio.cl.

130            IN      PTR      ns.mi-dominio.cl.
131            IN      PTR      correo.mi-dominio.cl.
132            IN      PTR      mail.mi-dominio.cl.
133            IN      PTR      webmail.mi-dominio.cl.
134            IN      PTR      www.mi-dominio.cl.

```

/var/named/ext.mi-dominio.cl

```

$ORIGIN mi-dominio.cl.
@              IN      SOA      mi-dominio.cl. root.mi-dominio.cl. (
                2001120401 ; Serial
                28800     ; Refresh
                14400     ; Retry
                3600000   ; Expire
                86400    ) ; Minimum

                IN      NS      ns.mi-dominio.cl.
                IN      NS      ns.isp.net.
                IN      MX      5 correo
                IN      MX      10 mail

ns             IN      A       172.30.30.130
correo        IN      A       172.30.30.131
mail         IN      A       172.30.30.132
webmail      IN      A       172.30.30.133
www          IN      A       172.30.30.134

```

/var/named/ext.mi-dominio.rev

```

@              IN      SOA      mi-dominio.cl. root.mi-dominio.cl. (
                2001120401 ; Serial
                28800     ; Refresh
                14400     ; Retry
                3600000   ; Expire
                86400    ) ; Minimum

                IN      NS      ns.mi-dominio.cl.
                IN      NS      ns.isp.net.

130            IN      PTR      ns.mi-dominio.cl.
131            IN      PTR      correo.mi-dominio.cl.
132            IN      PTR      mail.mi-dominio.cl.
133            IN      PTR      webmail.mi-dominio.cl.
134            IN      PTR      www.mi-dominio.cl.

```

En la practica esto debería ser suficiente para empezar a utilizar la característica de "Multiple Views" disponible en BIND 9.x.

Notar que el orden en que son definidas las vistas en la configuración del archivo `/etc/named.conf` si es relevante. Por ejemplo, si la vista externa es definida antes que la interna todas las consultas caeran en ella debido a la opción **match-clients { any; }** que calza con todas las direcciones IP de clientes DNS, por lo que no alcanza a pasar a la siguiente vista.

Otro comportamiento interesante es el hecho de cerrar nuestro DNS a clientes externos que consulten por dominios externos, es decir cerrar el relay de DNS en analogía al relay de SMTP. Por ejemplo, si eliminamos la definición de la zona de tipo **hint** de la vista externa, en este caso la zona ".", nos aseguramos de que ningún cliente externo pueda usar nuestro servidor de nombres para resolver direcciones de otros dominios que no sean los explicitamente definidos en la vista externa, esto porque el conjunto inicial de servidores de nombres raíz se especifica usando una zona indirecta o **hint**. Cuando el servidor DNS arranca, utiliza las zonas raices indirectas para encontrar un servidor de nombres raíz y conseguir la lista más reciente de los servidores de nombres raíz. Sin los servidores raiz se quiebra desde el principio toda la jerarquia de árbol del servicio de nombres de dominio dejando dicho sistema inoperante.

Espero que esta lectura sea tan instructiva para ustedes como lo fue para mi su escritura.

