

Instalación e configuración dun servidor DNS en Linux

Introdución

Nesta actividade realizaremos a instalación do servizo de nomes de dominio (DNS) nunha máquina Debian sen contorno gráfico. A distribución do sistema operativo que empregaremos é a testing. Esta distribución caracterízase por estar en continuo desenvolvemento e porque se converterá na próxima distribución estable. A razón do seu uso é simple: desta maneira poderemos empregar as versións máis recentes do software dispoñible a través dos repositorios.

Ó longo da actividade trataremos a instalación do servidor DNS BIND 9 (ou bind9) e a súa configuración básica. Veremos como preparar o servidor para almacenar respostas dun servidor DNS dunha rede pública e como engadir rexistros de nomes correspondentes a unha nova zona, con opcións de servidores de correo e alias.

Unha vez feito isto, aprenderemos a realizar transferencias de zona entre 2 ou máis servidores e a comprobar o correcto funcionamento do servizo.

Actividade

Que é bind9?

O servidor DNS que imos a empregar é BIND 9.

BIND (Berkeley Internet Name Domain, anteriormente: Berkeley Internet Name Daemon) é o servidor de DNS máis empregado en Internet, especialmente en sistemas Unix.

Unha nova versión de BIND (BIND 9) foi escrita desde cero para mellorar a arquitectura do seu código e permitir a súa auditoría, así como para incorporar DNSSEC (DNS Security Extensions).

Pódese consultar máis información sobre BIND 9 no seguinte enderezo web:
<https://wiki.debian.org/Bind9>

Instalación de bind9

Para instalar o servidor DNS bind9 no noso sistema (neste caso Debian), deberemos introducir no terminal o seguinte comando:

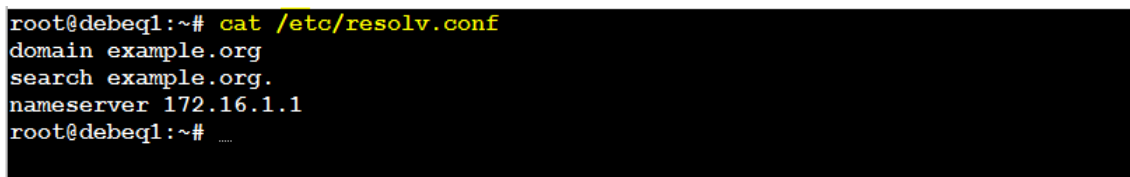
```
# apt-get install bind9
```

No caso de que queiramos, tamén podemos instalar a documentación de bind9 co comando:

```
# apt-get install bind9-doc
```

Configuración dos servidores DNS a empregar en equipos Linux

O servidor ou servidores DNS empregados polo sistema para resolver as consultas DNS nun equipo Linux están especificados no ficheiro */etc/resolv.conf* (ademais pode que se especifiquen outros aspectos como o dominio ou o sufixo de busca).



```
root@debeql:~# cat /etc/resolv.conf
domain example.org
search example.org.
nameserver 172.16.1.1
root@debeql:~# .....
```

Figura 1 – Exemplo de contido dun ficheiro resolv.conf

Para realizar cambios nos servidores DNS empregados debemos ter en conta dous casos:

Cando o software *resolvconf* **non está instalado** (non confundir co nome do ficheiro *resolv.conf*):

Este é o caso dos equipos Debian. En principio podemos editar a man este ficheiro e modificar os servidores DNS a empregar.

Cando todas as interfaces de rede do equipo teñen unha configuración estática esta solución é válida. O problema radica en que no caso de que algunha das nosas interfaces de rede obteña a configuración automaticamente dun servidor DHCP, cada vez que se renove a concesión obtida (cosa que pode ocorrer cada pouco tempo), o ficheiro */etc/resolv.conf* sobrescribírase e perderanse os cambios que tiveramos feitos nel.

Este inconveniente pode solucionarse editando o ficheiro `/etc/dhcp/dhclient.conf` para configurar os parámetros que se lle solicitan ó servidor DHCP e fixar a un valor determinado aqueles que queiramos.

Para non solicitar servidor DNS, no apartado *request* debemos borrar o parámetro *domain-name-servers* e mediante a directiva *supersede* fixámolo a un valor predeterminado:

```
nano 2.6.3      Ficheiro: /etc/dhcp/dhclient.conf

#
option rfc3442-classless-static-routes code 121 = array of unsigned integer 8;

send host-name = gethostname();
request subnet-mask, broadcast-address, time-offset, routers,
       domain-name, domain-name-servers, domain-search, host-name,
       dhcp6.name-servers, dhcp6.domain-search, dhcp6.fqdn, dhcp6.sntp-servers,
       netbios-name-servers, netbios-scope, interface-mtu,
       rfc3442-classless-static-routes, ntp-servers;

#send dhcp-client-identifier 1:0:a0:24:ab:fb:9c;
#send dhcp-lease-time 3600;
#supersede domain-name "fugue.com home.vix.com";
#prepend domain-name-servers 127.0.0.1;
#require subnet-mask, domain-name-servers;
#timeout 60;
#retry 60;
#reboot 10;
```

Figura 2 – Edición do ficheiro `/etc/dhcp/dhclient.conf` para evitar a solicitude de servidor DNS.

```
nano 2.6.3      Ficheiro: /etc/dhcp/dhclient.conf      Modificado

#
option rfc3442-classless-static-routes code 121 = array of unsigned integer 8;

send host-name = gethostname();

supersede domain-name-servers 8.8.8.8;

request subnet-mask, broadcast-address, time-offset, routers,
       domain-name, domain-search, host-name,
       dhcp6.name-servers, dhcp6.domain-search, dhcp6.fqdn, dhcp6.sntp-servers,
       netbios-name-servers, netbios-scope, interface-mtu,
       rfc3442-classless-static-routes, ntp-servers;

#send dhcp-client-identifier 1:0:a0:24:ab:fb:9c;
#send dhcp-lease-time 3600;
#supersede domain-name "fugue.com home.vix.com";
#prepend domain-name-servers 127.0.0.1;
#require subnet-mask, domain-name-servers;
```

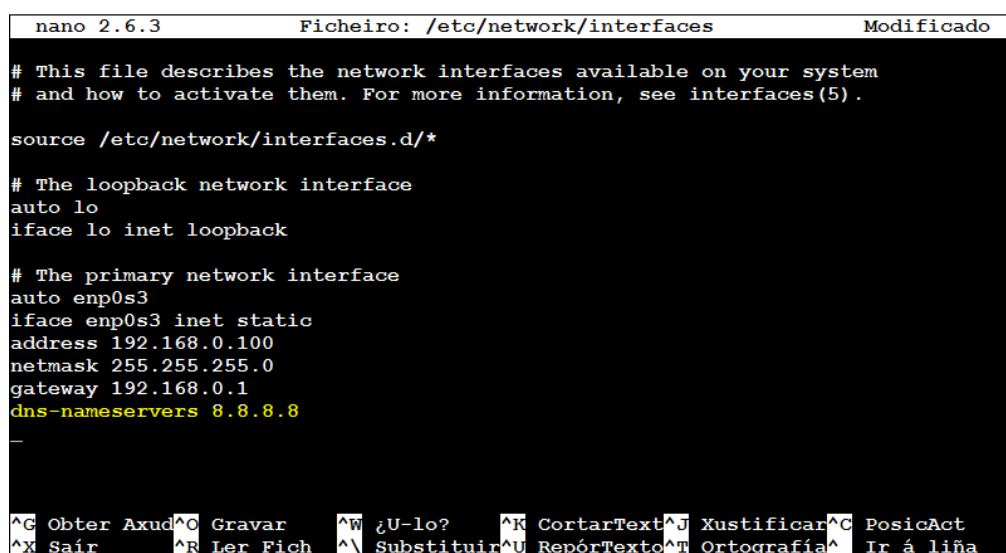
Figura 3 – Establecemento do servidor DNS a empregar por medio da directiva *supersede*.

Cando o software *resolvconf* **está instalado** (non confundir co nome do ficheiro *resolv.conf*):

Outra posible solución (é a que se emprega por defecto en equipos Ubuntu) é empregar o software *resolvconf*. En Debian, como xa se comentou, non se utiliza por defecto polo que habería que instalalo mediante o comando:

```
# apt-get install resolvconf
```

A partir do momento en que se instala este software xa non se pode editar o ficheiro *resolv.conf* á man. Para fixar os valores dos servidores DNS debemos editar o ficheiro de configuración de rede (*/etc/network/interfaces*) e, mediante a directiva *dns-nameservers* darlle o valor que queiramos:



```
nano 2.6.3      Ficheiro: /etc/network/interfaces      Modificado

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet static
address 192.168.0.100
netmask 255.255.255.0
gateway 192.168.0.1
dns-nameservers 8.8.8.8
--
^G Obter Axuda  ^O Gravar      ^W ¿U-lo?     ^K CortarText ^J Xustificar  ^C PosicAct
^X Saír        ^R Ler Fich   ^\ Substituir ^U RepórTexto ^T Ortografía ^_ Ir á liña
```

Figura 4 – Configuración dos servidores DNS no ficheiro de configuración de rede */etc/network/interfaces*.

A directiva *dns-nameservers* só funciona se *resolvconf* está instalado. Para que os cambios se apliquen, deberemos reiniciar o equipo.

Cando algunha das interfaces de rede do equipo se configura automaticamente, o servidor DNS que especificamos mediante a directiva *dns-nameservers* engadiríase detrás dos obtidos do servidor DHCP, polo que só se empregaría se os outros non responden.

Para poder empregar o que nós queiramos, cando algunha interface se configura por DHCP, hai que configurar o cliente DHCP para que non solicite servidores DNS (como xa se explicou anteriormente).

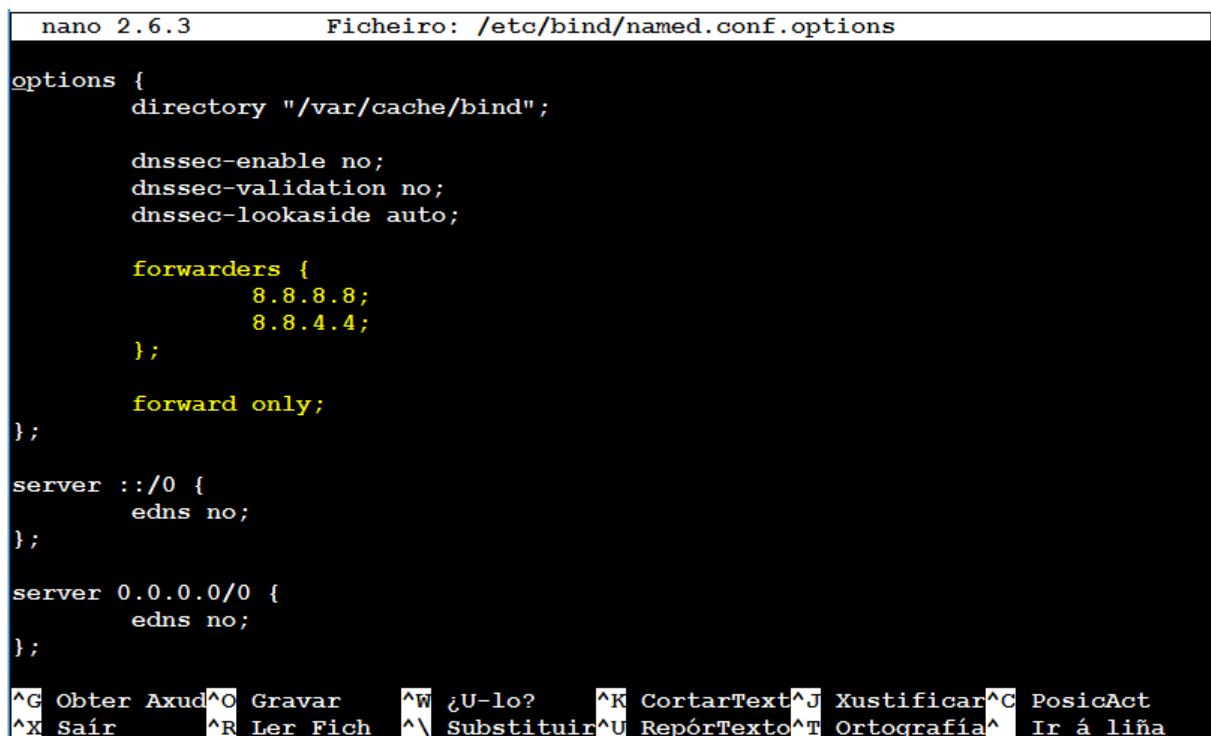
Configuración por defecto

Rematado o proceso de instalación e antes de realizar ningún cambio na configuración, o servidor bind9 funciona como un Caching DNS Server. Isto é un servidor DNS que atende ás consultas recursivas dos clientes e que posúe unha memoria caché onde almacena os resultados obtidos por un período determinado de tempo, conseguindo desta maneira aumentar a velocidade das respostas e diminuír o número de consultas iterativas precisas para resolver unha determinada petición.

Configuración como Forwarding DNS Server

Para configurar o servidor Bind9 para que reenvíe as peticións a outro/s servidor/es DNS debemos de editar o ficheiro `/etc/bind/named.conf.options`

Neste arquivo imos engadir a opción *forwarders* cos enderezos IP dos servidores ós que se reenviarán as peticións DNS e a opción *forward only*; que implica que o servidor DNS vai reenviar todas as peticións sen tentar resolvelas el mesmo.



```
nano 2.6.3      Ficheiro: /etc/bind/named.conf.options

options {
    directory "/var/cache/bind";

    dnssec-enable no;
    dnssec-validation no;
    dnssec-lookaside auto;

    forwarders {
        8.8.8.8;
        8.8.4.4;
    };

    forward only;
};

server ::/0 {
    edns no;
};

server 0.0.0.0/0 {
    edns no;
};
```

Figura 5 – Configuración do servidor bind9 como Forwarding DNS Server.

Unha vez feito isto, deberemos reiniciar o servizo bind9 co comando:

```
# /etc/init.d/bind9 restart
```

Creación dunha zona mestra de resolución inversa

O primeiro que debemos facer é engadir a definición de zona ó ficheiro `/etc/bind/named.conf.local`. Dos catro bytes que conforman o enderezo dunha rede, só se deben poñer no identificador da zona aqueles que identifican a rede. Por exemplo, para 10.15.0.0/16 poríase como identificador de zona `"15.10.in-addr.arpa"`, e para 10.15.0.0/24 poríase `"0.15.10.in-addr.arpa"`.



```
nano 2.6.3      Ficheiro: /etc/bind/named.conf.local      Modificado

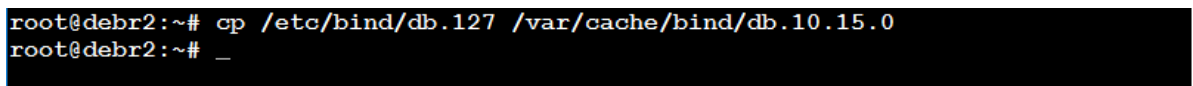
zone "0.15.10.in-addr.arpa" {
    type master;
    file "/var/cache/bind/db.10.15.0";
};

_

^G Obter Axuda ^O Gravar      ^W ¿U-lo?      ^K CortarText ^J Xustificar ^C PosicAct
^X Saír      ^R Ler Fich  ^\ Substituir ^U RepórTexto ^T Ortografía ^_ Ir á liña
```

Figura 6 – Definición de zona mestra de resolución inversa.

Para crear o arquivo de zona partiremos doutro xa existente para a rede de loopback.



```
root@debr2:~# cp /etc/bind/db.127 /var/cache/bind/db.10.15.0
root@debr2:~# _
```

Figura 7 – Copia do ficheiro de zona da rede de loopback para crear a nova zona mestra de resolución inversa.

Neste ficheiro debemos cambiar localhost. polo FQDN do noso servidor, deixando o "." adicional ao final.

Tamén cambiaremos 1.0.0 polo contido dos bytes de host do enderezo IP do noso servidor de nomes DNS (hai que ter coidado xa que debemos poñelos ó revés, é dicir, de xeito semellante a como para 127.0.0.1/8 se poñen os tres últimos bytes en sentido inverso: 1.0.0).

Ademais, deberemos substituír tamén root.localhost por un enderezo de correo electrónico válido como, por exemplo, root.example.com deixando tamén o "." ó final. Por outra parte, tamén incluiremos o rexistro correspondente ó glue record.

Aclaración

Un glue record é un rexistro A/AAAA adicional que permite a correcta resolución no enderezo IP do servidor DNS. Os glue records son necesarios para previr referencias circulares que se forman cando os servidores de nomes para un dominio non poden ser resoltos sen resolver o dominio para o cal eles son responsables

Sen o/os rexistro/s glue record a resolución de nomes para o DNS non funcionaría.

```
nano 2.6.3                               Ficheiro: /var/cache/bind/db.10.15.0          Modificado
$TTL      604800
@         IN      SOA      debr2.example.com. root.example.com. (
                                1          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@         IN      NS       debr2.example.com.
2         IN      PTR      debr2.example.com.
```

Figura 8 – Edición do ficheiro de zona mestra de resolución inversa.

Cada vez que fagamos cambios neste ficheiro debemos de incrementar o número de serie (*Serial*) nunha unidade (veremos a importancia deste dato posteriormente).

Por último, para que os cambios sexan aplicados, deberemos reiniciar bind9 co comando:

```
# /etc/init.d/bind9 restart
```

Creación dunha zona mestra de resolución directa

O proceso é análogo ó de creación dunha zona mestra de resolución inversa. O primeiro paso é engadir a definición da zona no ficheiro */etc/bind/named.conf.local*.

O proceso é análogo ao anterior. O primeiro é engadir a definición de zona.

Neste caso só hai que poñer o nome do ficheiro, xa que o directorio onde se vai gardar, por defecto, é */var/cache/bind*. Na zona mestra de resolución inversa si que se pon a ruta completa, pero neste caso, aínda que non é incorrecto, si que resulta redundante.

```

nano 2.6.3                               Ficheiro: /etc/bind/named.conf.local          Modificado
zone "0.15.10.in-addr.arpa" {
    type master;
    file "/var/cache/bind/db.10.15.0";
};

zone "example.com" {
    type master;
    file "db.example.com";
};

```

Figura 9 – Definición de zona mestra de resolución directa.

Ó igual que no apartado anterior, empregarase un modelo para crear o arquivo de zona */etc/bind/db.example.com*:

Empregamos un modelo para crear o arquivo de zona */etc/bind/db.example.com*:

```

root@debr2:~# cp /etc/bind/db.local /var/cache/bind/db.example.com
root@debr2:~# _

```

Figura 10 – Copia do ficheiro de zona que servirá de modelo para crear a nova zona mestra de resolución directa.

Neste ficheiro debemos cambiar *localhost*. polo FQDN do noso servidor, deixando o "." adicional ó final. Tamén substituiremos *root.localhost* por un email válido (por exemplo, *root.example.com*. deixando tamén o "." ó final).

Nesta ocasión tamén se inclúe o rexistro correspondente ó glue record.

```

nano 2.6.3                               Ficheiro: /var/cache/bind/db.example.com      Modificado
$TTL      604800
@          IN      SOA      debr2.example.com. root.example.com. (
                                1          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@          IN      NS       debr2.example.com.
debr2     IN      A         10.15.0.2

```

Figura 11 – Edición do ficheiro de zona mestra de resolución directa.

Ó igual que na zona mestra de resolución inversa, cada vez que fagamos cambios neste ficheiro debemos de incrementar o *Serial* nunha unidade. Para que os cambios sexan aplicados, tamén teremos que reiniciar bind9 co comando:

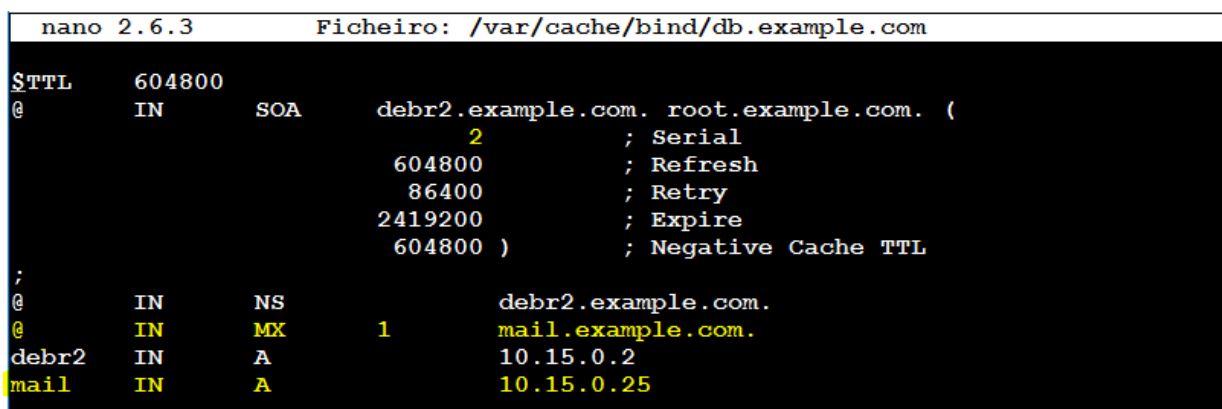
```
# /etc/init.d/bind9 restart
```

Especificación do servidor de correo

O rexistro MX permite definir cal é o enderezo IP da/s máquina/s encargada/s de xestionar o correo para o dominio ou subdominio correspondente. Estes rexistros a maiores inclúen un número que indica a prioridade (no caso de que houbera máis dunha máquina servidor de correo). Os rexistros MX só se poden atopar nas zonas de resolución directa.

É moi habitual introducir o símbolo @ no lugar do nome dun recurso ou do nome da zona. Este @ substituirase polo valor introducido na directiva *\$ORIGIN*. Esta directiva adóitase poñer ó inicio do ficheiro, antes do rexistro SOA, ou pode omitirse e nese caso tomará o nome da zona.

Ademais, introdúcese un rexistro de tipo A para a máquina que fai de Mail Exchanger e, igual que nos apartados anteriores, debe incrementarse o *Serial*.



```
nano 2.6.3      Ficheiro: /var/cache/bind/db.example.com

$TTL      604800
@          IN      SOA      debr2.example.com. root.example.com. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@          IN      NS       debr2.example.com.
@          IN      MX       1      mail.example.com.
debr2      IN      A        10.15.0.2
mail       IN      A        10.15.0.25
```

Figura 12 – Edición dos rexistros relacionados co servidor de correo ou Mail Exchanger (MX).

Unha vez máis, para aplicar os cambios, teremos que reiniciar bind9 co comando:

```
# /etc/init.d/bind9 restart
```

Outros rexistros

Os rexistros tipo *CNAME* empréganse para crear un "alias" doutro nome definido por outro rexistro tipo *CNAME* ou tipo *A*.

Os rexistros *TXT* permiten introducir calquera información arbitraria, como pode ser unha frase, un comentario ou calquera outro texto.

```
nano 2.6.3      Ficheiro: /var/cache/bind/db.example.com      Modificado
$TTL      604800
@          IN      SOA      debr2.example.com. root.example.com. (
                        2          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
@          IN      NS       debr2.example.com.
@          IN      MX       1   mail.example.com.
debr2      IN      A        10.15.0.2
mail       IN      A        10.15.0.25
other      IN      CNAME    debr2.example.com.
word       IN      TXT      "some text"
```

Figura 13 – Edición dos rexistros relacionados co servidor de correo ou Mail Exchanger (MX).

Creación dunha zona de reenvío

Se queremos que para unha zona determinada se reenvíen as consultas a un servidor DNS determinado, indistintamente de se xa se configurou o servidor como Forwarding DNS Server, debemos editar o ficheiro */etc/bind/named.conf.local* e engadir o seguinte:

```
nano 2.6.3      Ficheiro: /etc/bind/named.conf.local      Modificado

zone "xunta.es" {
    type forward;
    forward only;
    forwarders {7.7.7.7};
};_
^G Obter Axuda ^O Gravar      ^W ¿U-lo?    ^K CortarText ^J Xustificar ^C PosicAct
^X Saír      ^R Ler Fich  ^\ Substituir ^U RepórTexto ^T Ortografía ^ Ir á liña
```

Figura 14 – Edición do ficheiro */etc/bind/named.conf.local* para engadir unha zona de reenvío.

Evidentemente, deberemos modificar o nome da zona e o enderezo IP do servidor DNS para adaptalos ós datos que nos interesen.

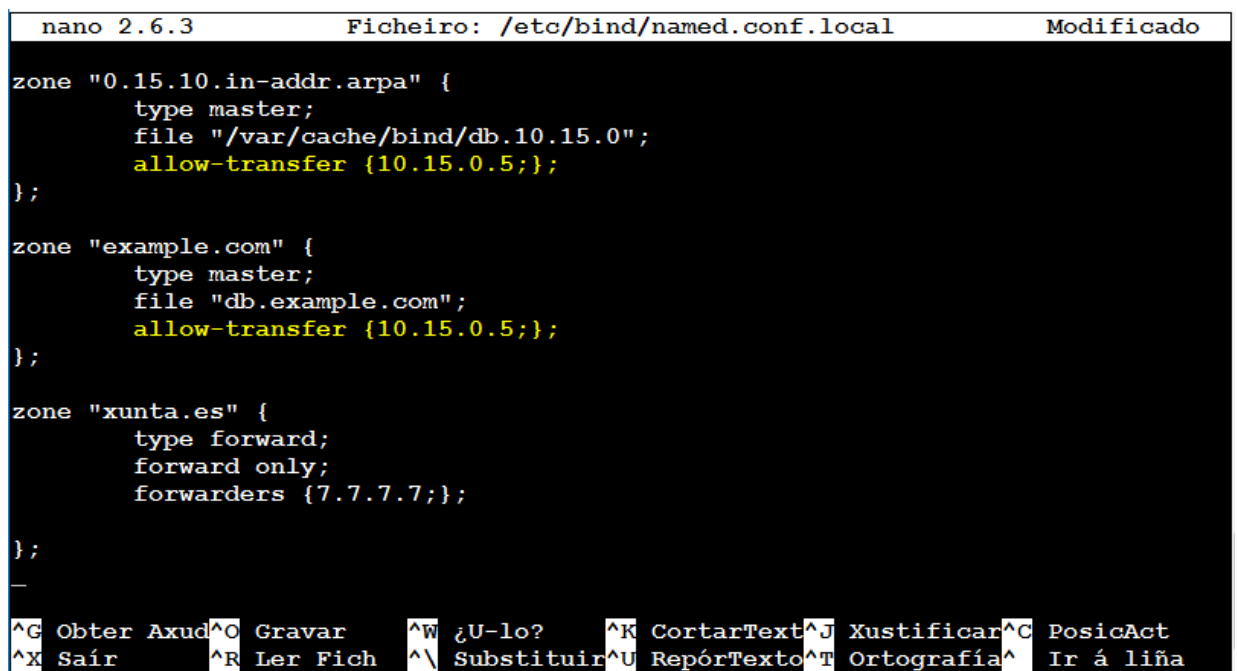
Configuración de zonas subordinadas ou secundarias

Unha vez que o servidor mestre primario foi configurado, é aconsellable ter polo menos un servidor secundario por motivos de dispoñibilidade, balanceo de carga, etc.

A transferencia de zona é o proceso polo cal os servidores subordinados ou secundarios copian o contido dos ficheiros de zona do servidor primario (no caso de que o *Serial* cambiara desde a última transferencia de zona).

No servidor mestre primario debemos permitir unicamente as transferencias de zona ós servidores subordinados xa que senón, desde calquera equipo, poderían copiar os ficheiros de zona, o que suporía unha grave vulnerabilidade grave da seguridade.

A continuación, amósanse as modificacións que teremos que introducir na configuración do servidor DNS primario para autorizar a transferencia de zona a un determinado servidor DNS secundario.



```
nano 2.6.3      Ficheiro: /etc/bind/named.conf.local      Modificado

zone "0.15.10.in-addr.arpa" {
    type master;
    file "/var/cache/bind/db.10.15.0";
    allow-transfer {10.15.0.5};
};

zone "example.com" {
    type master;
    file "db.example.com";
    allow-transfer {10.15.0.5};
};

zone "xunta.es" {
    type forward;
    forward only;
    forwarders {7.7.7.7};
};

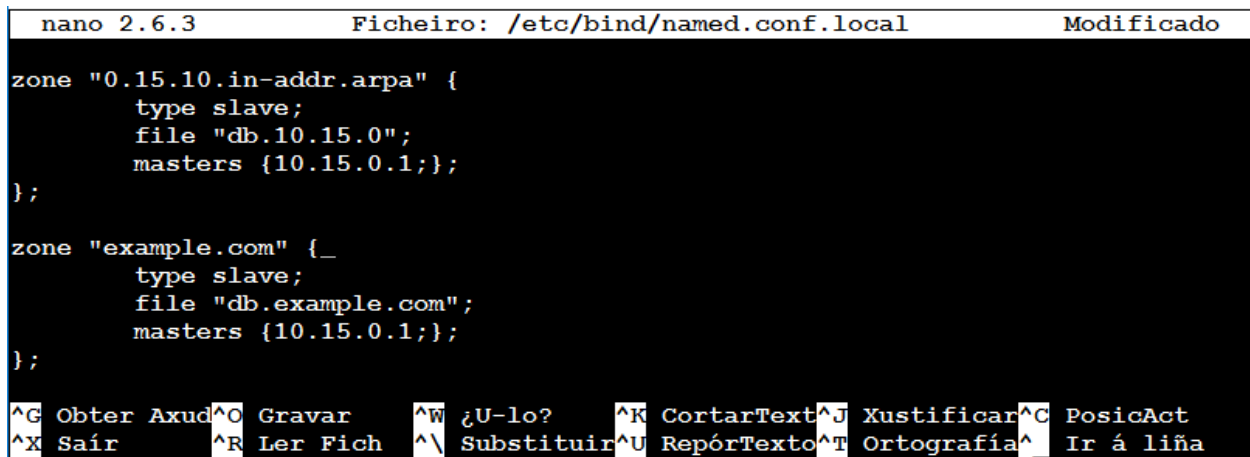
-
^G Obter Axuda ^O Gravar      ^W ¿U-lo?      ^K CortarText ^J Xustificar ^C PosicAct
^X Sair        ^R Ler Fich    ^_ Substituir  ^U RepórTexto ^T Ortografía  ^_ Ir á liña
```

Figura 15 – Autorización da transferencia de zona a un determinado servidor secundario con IP 10.15.0.5.

De novo, para aplicar os cambios, no servidor DNS primario teremos que reiniciar o servizo bind9 co comando:

```
# /etc/init.d/bind9 restart
```

No equipo que actuará como servidor DNS secundario, editaremos o ficheiro `/etc/bind/named.conf.local` e engadiremos as seguintes declaracións para as zonas de resolución inversa e directa. É importante notar que o tipo destas zonas é *slave* (escrava ou, neste caso, secundaria) e que coa directiva *masters* identifícase ó enderezo IP do servidor DNS primario do que hai que copiar a información da zona.



```
nano 2.6.3      Ficheiro: /etc/bind/named.conf.local      Modificado

zone "0.15.10.in-addr.arpa" {
    type slave;
    file "db.10.15.0";
    masters {10.15.0.1};
};

zone "example.com" {
    type slave;
    file "db.example.com";
    masters {10.15.0.1};
};

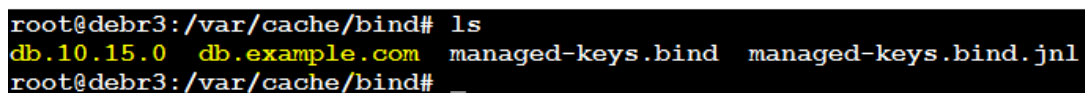
^G Obter Axuda  ^O Gravar      ^W ¿U-lo?      ^K CortarText ^J Xustificar  ^C PosicAct
^X Saír        ^R Ler Fich    ^\ Substituir  ^U RepórTexto ^T Ortografía  ^_ Ir á liña
```

Figura 16 – Configuración das zonas directa e inversa no servidor DNS secundario.

Para aplicar estes cambios, debemos reiniciar no servidor DNS secundario o servizo bind9 por medio do comando:

```
# /etc/init.d/bind9 restart
```

Podemos comprobar que os ficheiros de zona están en `/var/cache/bind`, aínda que a diferenza do servidor DNS primario, no secundario estarán nun formato para facilitar a súa transferencia na rede e que non se pode visualizar cun editor de texto convencional.



```
root@debr3:/var/cache/bind# ls
db.10.15.0  db.example.com  managed-keys.bind  managed-keys.bind.jnl
root@debr3:/var/cache/bind# _
```

Figura 17 – Ficheiros de definición de zona no servidor DNS secundario.

Notificación de cambios ós servidores subordinados ou secundarios

Cando se faga un cambio na zona mestra, este deberá propagarse ós servidores secundarios. Para que isto se produza, ó introducir algún cambio na definición da zona ou nos seus rexistros, hai que lembrar sempre que se debe aumentar o *Serial* nos ficheiros de zona afectados.

Así mesmo, no servidor mestre primario debemos asegurarnos de que se propagan os cambios ós secundarios. Para iso teremos que comprobar que en cada servidor DNS (tanto o primario como o/s secundario/s) exista un rexistro NS definido na zona correspondente.

```
nano 2.6.3 Ficheiro: /var/cache/bind/db.example.com
$TTL 604800
@ IN SOA debr2.example.com. root.example.com. (
    3 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS debr2.example.com.
@ IN NS debr3.example.com.
@ IN MX 1 mail.example.com.
debr2 IN A 10.15.0.1
debr3 IN A 10.15.0.5
mail IN A 10.15.0.25
other IN CNAME debr2.example.com.
word IN TXT "some text"
```

```
nano 2.6.3 Ficheiro: /var/cache/bind/db.10.15.0
$TTL 604800
@ IN SOA debr2.example.com. root.example.com. (
    3 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS debr2.example.com.
@ IN NS debr3.example.com.
1 IN PTR debr2.example.com.
5 IN PTR debr3.example.com.
25 IN PTR mail.example.com.
```

Figura 18 – Ficheiros de definición de zona dos servidores DNS primario e secundario, respectivamente.

No caso de que o apartado anterior non se cumpra, debemos incluír o seguinte na declaración da zona primaria:

```
nano 2.6.3 Ficheiro: /etc/bind/named.conf.local Modificado
zone "0.15.10.in-addr.arpa" {
    type master;
    notify yes;
    file "/var/cache/bind/db.10.15.0";
    allow-transfer {10.15.0.5;};
    also-notify {10.15.0.5;};
};

zone "example.com" {
    type master;
    notify yes;
    file "db.example.com";
    allow-transfer {10.15.0.5;};
    also-notify {10.15.0.5;};
};
```

Figura 19 – Modificación das definicións de zona do servidor DNS primario para notificar forzosamente ó servidor DNS secundario cando se produce algún cambio.

Como de costume, para aplicar estes cambios será preciso reiniciar o servidor DNS primario co comando:

```
# /etc/init.d/bind9 restart
```