Curso de DNS

Instalación de BIND 3
Ejecución 3
El archivo de arranque 3
Servidor de solo caché 4
El registro SOA 6
El registro A 7
El registro NS 7
El registro PTR 7
El registro MX 7
El registro CNAME 8
Configuración del resolvedor de nombres 8
Servidor de nombres para el dominio domaindns 8
Uso de nslookup 10

Instalación de BIND

La instalación en una máquina con Linux RedHat, o distribuciones basadas en él, es muy sencilla. Basta utilizar el siguiente comando en el directorio que contiene los paquetes del software RedHat (RPMS):
rpm -i bind-4.9.3-3.i386.rpm

Los números de versión del paquete, así como el especificador de arquitectura (i386) pueden variar: lo mejor es verificar el nombre exacto del paquete mediante el comando ls.

Ejecución

El sistema operativo debería arrancar por sí solo el demonio named al terminar su propia secuencia de arranque. En los sistemas UNIX BSD (Linux Slackware, por ejemplo), esto se logra incluyendo en el archivo rc.local la línea:

named &

Los sistemas que, por el contrario, siguen la norma System V para los archivos de arranque, contienen directorios especiales con scripts de shell que levantan los programas necesarios en cada runlevel. El caso de Linux RedHat, es el más sencillo: la misma instalación mediante el comando rpm agrega en el directorio correspondiente el script necesario para levantar el demonio.

El archivo de arranque

El primer archivo en la configuración de un servidor de nombres es el archivo de arranque, que es leído por el demonio named cuando arranca para saber a qué dominios va a servir y dónde encuentra las tablas de máquinas y direcciones IP, entre otras cosas. Este archivo es generalmente /etc/named.conf. Un ejemplo típico de este archivo, configurado como un servidor de sólo caché, es el siguiente:

```
options {
directory "/var/named";
};

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

zone "0.0.127.in-addr.arpa" {
   type master;
   file "named.local";
};
```

La línea 'directory' indica el directorio donde named debe buscar los archivos que aparecen en las líneas siguientes. Si named no encuentra esta línea, buscará los archivos en el directorio /etc.

Los paquetes de distribución de Linux pueden usar diferentes nombres para los archivos mencionados aquí; ellos contendrán aún las mismas cosas.

Servidor de solo caché

Por defecto, la configuración de named es como un servidor de solo caché, el cual es muy útil para los usuarios de conexiones telefónicas. Este servidor obtendrá las respuestas a solicitudes de nombre provenientes de su red preguntando a servidores externos, recordando la respuesta para la próxima vez que lo necesite. Un servidor de nombres de este tipo es útil porque disminuye el tráfico de peticiones de resolución de nombres en la red.

/etc/named.ca

El archivo named.ca describe los servidores de nombre raíz en el mundo y cambiará a lo largo del tiempo por lo que tiene que ser mantenido y actualizado con cierta regularidad. Básicamente su contenido es el siguiente:

```
.                       3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     128.9.0.107
;
; formerly C.PSI.NET
;
.                       3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     3600000      A     192.33.4.12
;
; formerly TERP.UMD.EDU
;
.                       3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.     3600000      A     128.8.10.90
;
; formerly NS.NASA.GOV
;
.                       3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.     3600000      A     192.203.230.10
;
; formerly NS.ISC.ORG
;
.                       3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     3600000      A     192.5.5.241
;
; formerly NS.NIC.DDN.MIL
;
```

```
.                       3600000     NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.     3600000     A     192.112.36.4
;
; formerly AOS.ARL.ARMY.MIL
;
.                       3600000     NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.     3600000     A     128.63.2.53
;
; formerly NIC.NORDU.NET
;
.                       3600000     NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.     3600000     A     192.36.148.17
;
; temporarily housed at NSI (InterNIC)
;
.                       3600000     NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.     3600000     A     198.41.0.10
;
; housed in LINX, operated by RIPE NCC
;
.                       3600000     NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.     3600000     A     193.0.14.129
;
; temporarily housed at ISI (IANA)
;
.                       3600000     NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.     3600000     A     198.32.64.12
;
; housed in Japan, operated by WIDE
;
.                       3600000     NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.     3600000     A     202.12.27.33
; End of File
```

/etc/named.conf

En el archivo named.conf se declara la zona 0.0.127.in-addr.arpa, el cual está guardado en un archivo llamado named.local. Este contiene:

```
@            IN   SOA   domaindns.   root.domaindns. (
                 2001031705 ; serial
                 28800      ; tasa de refresco, en segundos
                 14400      ; tasa de reintento, en segundos
                 3600000    ; caducidad para secundario, en segundos
                 86400      ; validez para clientes
                 )
@            IN   NS    domaindns.
1            IN   PTR   localhost.
```

Este tipo de archivo es llamado archivo de zona y a su dominio asociado, origen. Cada nombre de dominio o de máquina que aparezca en estos archivos es considerado relativo a este origen a menos que termine con un punto. Esta regla no debe ser

tomada a la ligera: todos los nombres en un archivo de zona son expandidos agregándoles el origen a menos que terminen en un punto. Para hacer referencia al origen en sí es necesario usar el símbolo "@''.

Los archivos de zonas están hechos de RRs (resource records) y tienen un tipo asociado. Por ejemplo, un registro para asociar un nombre de máquina con una dirección IP tiene el tipo A, y uno para asociar un nombre corto o alias a una máquina a la que ya se le asoció un IP es de tipo CNAME. En general, los registros o RRs tienen la forma siguiente:

[dominio] [ttl] [clase] tipo datos

Cada campo del registro se separa mediante espacios o tabuladores. Los campos entre corchetes son opcionales. Un campo puede ocupar más de una línea siempre y cuando aparezca un paréntesis antes del primer salto de línea y otro paréntesis cierre después del último campo del registro en la última línea. Al igual que en el archivo de arranque, en el named.conf, es posible introducir comentarios en un archivo de zona mediante un punto y coma: todo lo que aparece después de este signo es ignorado.

El registro SOA

SOA significa Start Of Authority e informa que todos los registros de recursos que le siguen están autorizados a dicho dominio. Los datos asociados con un registro SOA son los siguientes:
origin : Es el nombre canónico del servidor de nombres primario para este dominio, y generalmente se da como absoluto, es decir, con un punto al final.

contact : Es el nombre de la persona responsable para este dominio. Es parecido a una dirección de correo electrónico normal, a excepción que la arroba se remplaza con un punto. También termina con un punto.

serial : Es un número que indica la versión del archivo de zona, y debe ser incrementado cada vez que el archivo se modifique. Es importante porque los servidores secundarios solicitan el registro SOA en ciertos intervalos (ver refresh, más abajo), para verificar el serial. Si éste ha cambiado, entonces transfieren el archivo completo para actualizarse. Una práctica muy común es utilizar la fecha en el formato aammdd y agregarle dos dígitos más para los cambios que se hacen al archivo en el mismo día. De tal manera, un serial típico podría ser 2001032201.

refresh : Es el intervalo, en segundos, para las revisiones que hacen los servidores secundarios del registro SOA, con el fin de verificar si la información del dominio ha cambiado. El valor típico es de una hora (3600).

retry : Es el tiempo, en segundos, que un servidor secundario debe esperar para reintentar una conexión por refresh que ha fallado. El valor recomendado es de 10 minutos, o sea 600.

expire : Si un servidor secundario no ha podido comunicarse con su servidor primario para verificar que no haya habido cambios a la zona (mediante su registro SOA), descartará la información que tiene después de este periodo dado en segundos. El valor típico es de 42 días, o sea 3600000.

minimum : Este es el número de segundos empleado en los registros del archivo que no especifican su campo ttl (time to live).

El registro A

Este registro sirve para asociar un nombre de máquina con una dirección IP. El único dato para este tipo de registro es la dirección IP en su forma estándar:

xxx.xxx.xxx.xxx. Debe haber sólo un registro A por cada dirección IP en el archivo, aunque es posible asignarle a una máquina más de una dirección mediante varios registros A.

El registro NS

Mediante un registro NS es posible designar un servidor que deberá responder para todas las peticiones que involucren un determinado subdominio. Esto es importante porque permite delegar la asignación de nombres y facilita el manejo de dominios complejos.

Designar un servidor de nombres, sin embargo, no basta. Se necesita definir en alguna parte del archivo la dirección de este servidor, mediante un registro A, por supuesto. A este registro se le llama en inglés glue record.

El registro PTR

Un registro PTR se utiliza para relacionar una dirección IP con un nombre de máquina, exactamente al revés que un registro tipo A. Estos registros aparecen en los archivos de zonas para la resolución inversa, los que en named.conf aparecen en una línea zone. con el dominio IN-ADDR.ARPA.

Nótese que en cada registro sólo aparece una fracción de la dirección IP: la dirección se completa porque, como se dijo más arriba, a cada nombre que no termina en un punto se le agrega el origen.

Los nombres de máquinas aparecen siempre en los registros PTR en su forma canónica, es decir, con el dominio completo. El punto es necesario porque de no aparecer se le agregaría erróneamente el origen.

El registro MX

Los registros MX sirven para anunciar a los programas de intercambio de correo (Sendmail, por ejemplo), una máquina que se encarga de administrar el correo de un determinado dominio.

El registro CNAME

Este registro sirve para asignarle un nombre alternativo o alias a una máquina.

HOME

Configuración del resolvedor de nombres

En el directorio /etc se encuentran dos archivos, los cuales se emplean para configurar la biblioteca del resolutor de la máquina.

/etc/host.conf

Probablemente contiene varias líneas, una de ellas debe comenzar con order, indicando el orden en que se prueban los distintos mecanismos de resolución de nombres. Si aparece lo siguiente:

order hosts,bind

Indica a las rutinas de resolución de nombres que busquen primero en /etc/hosts y pregunte luego al servidor de nombres.

/etc/resolv.conf

Este archivo controla la forma en la que el resolutor utiliza DNS para resolver nombres de servidor. Indica los servidores de nombre DNS que deben contactarse y el orden en que se debe contactarlos. resolv.conf puede lucir así:

search domaindns
nameserver 10.20.30.2

La línea search especifica en qué dominios se buscaría para cualquier nombre de máquina a la que se quiera conectar. La línea nameserver especifica la dirección del servidor de nombres. Si se quiere una lista de varios servidores se debe poner una línea nameserver para cada uno. Es importante saber que named nunca lee este archivo, lo hace el resolutor que usa named

Servidor de nombres para el dominio domaindns

Para definir el dominio domaindns, es necesario agregar los archivos de zona correspondientes a él en named.conf; que queda de la siguiente manera:

```
options {
directory "/var/named";
};
zone "." {
    type hint;
    file "named.ca";
```

```
};
zone "domaindns" {
    type master;
    file "zona/domaindns";
};
zone "0.0.127.in-addr.arpa" {
    type master;
    file "named.local";
};
zone "30.20.10.in-addr.arpa" {
    type master;
    file "zona/10.20.30";
};
```

Aquí se nombran el archivo domaindns, el cual define la zona, y 10.20.30, que es usado para efectuar la resolución inversa. La configuración indica que dichos archivos están ubicados en el directorio zona creado en /var/named. La resolución inversa se usa para encontrar el nombre de la máquina a partir de su dirección IP.

/var/named/zona/domaindns

En él se dispone de un servidor de nombres secundario de seguridad (domain2) y están enunciadas las diferentes máquinas dentro de la red.

```
@       IN  SOA  domaindns.  root.domaindns. (
        2001031812 ; serial
        28800 ; tasa de refresco, en segundos
        14400 ; tasa de reintento, en segundos
        3600000 ; caducidad para secundario, en segundos
        86400 ; validez para clientes, en segundos
        )
@       IN  NS   domaindns.
@       IN  NS   domain2.
@       IN  MX   10   mail.domaindns.
@       IN  MX   20   mail.localdomain2.
@       IN  TXT   "SERVIDOR DNS"

localhots     IN   A   127.0.0.1
tarea         IN   A   10.20.30.5
tarea2        IN   A   10.20.30.3
ns     IN   A   10.20.30.4
linux01      IN   A   10.20.30.2
```

/var/named/zona/10.20.30

Este es el archivo de resolución inversa.

```
@       IN  SOA  domaindns.  root.domaindns. (
        2001031801 ; serial
        28800      ; tasa de refresco, en segundos
        14400      ; tasa de reintento, en segundos
        3600000    ; caducidad para secundario, en segundos
        86400      ; validez para clientes, en segundos
```

```
        )
@       IN   NS   domaindns.
@       IN   NS   domain2.

2        IN   PTR   linux01.domaindns
5        IN   PTR   tarea.
3        IN   PTR   tarea2.
4        IN   PTR   ns.
```

Luego de configurar los archivos del servidor o cada vez que cambie el archivo named.conf, se debe reinicializar el demonio named, empleando el comando ndc restart.

Uso de nslookup

Esta es una utilería sumamente provechosa que se utiliza comúnmente para verificar la instalación de un servidor de nombres. Esta herramienta puede utilizarse interactivamente o como un comando cualquiera. Esto último se hace de la siguiente manera: nslookup maquina

nslookup cuestionará al servidor de nombres especificado en el archivo /etc/resolv.conf acerca de la máquina que se desea encontrar y devolverá su dirección IP.

En modo interactivo, nslookup puede hacer mucho más que sólo encontrar direcciones IP: puede preguntarle al servidor de nombres por cualquier clase de registros (no sólo A) e incluso puede mostrar la información referente a una zona entera.

Para entrar en el modo interactivo sólo es necesario teclear nslookup. El programa contestará con un signo de menor que ``>'' indicando que está listo para ejecutar comandos. Es posible entonces indicarle cualquier nombre de dominio y nslookup buscará por registros de tipo A. Para cambiar el tipo de registro que queremos encontrar es posible indicar set type=tipo, donde tipo puede ser cualquiera de los que ya mencionamos en la sección 3 o incluso any, que indica cualquier tipo de registro.

Si se usa nslookup para indagar por la máquina linux02, el programa entrega lo siguiente:

```
$nslookup
Server:  linux01.domaindns
Address:  10.20.30.2

>linux02
Name:    linux02.domaindns
Address:  10.20.30.3
```

En algunas ocasiones aparece la línea "Non-authoritative answer"; esto significa que named no sale de la red para preguntar por un equipo, en su lugar mira en su caché y lo encuentra allí.