PRÁCTICA 5
Configuración de DNS en una Intranet.

Administración de Sistemas Informáticos
Acedo Legarre, Aitor.
Puértolas Rebollar, Cristina.
Curso 2002-2003.

OBJETIVO

Configurar DNS en una intranet.

ENUNCIADO

Suponer que el dominio global de las prácticas es `asi.cps.unizar.es`. Y que vosotros definiréis subdominios con el nombre que queráis.

REQUISITOS

1. Configurar tres máquinas correspondientes a tres grupos de la sesión de prácticas para que constituyan vuestro subdominio DNS (nombre de vuestra discreción) independiente de los demás, pero bajo `asi.cps.unizar.es`

2. Una de las máquinas funcionará como servidor primario de la zona.

3. El otro como servidor secundario.

4. El otro como servidor.

5. Y el tercero y último lo configuráis como resolver-only, y una vez que funciona el conjunto lo probáis como servidor cache-only.

MEMORIA

El subdominio DNS elegido para esta ocasión ha sido `eupla`, esto es, el nombre del dominio completo será `eupla.asi.cps.unizar.es.`

Comenzaremos configurando el servidor primario de la zona.

Lo primero es instalar el paquete bind9 en la máquina:

```
apt-get install bind9
```

Será útil instalar el paquete `dns-utils` para utilizar programas como el `'dig'` o el `'host'` para comprobar que la configuración de los dns que hagamos en nuestra zona es correcta.

Servidor primario DNS (Máquina GIZMO): `/etc/hosts`

Este fichero contendrá la resolución de nombres de modo estático, por lo que deberemos incluir la mínima información posible. Mas concretamente el nombre de nuestra máquina, y como no, la identidad localhost-127.0.0.1.

```
127.0.0.1         localhost
155.210.154.194   gizmo.eupla.asi.cps.unizar.es      gizmo
```

¿Por que es necesario configurar este fichero? Pues bien, en el fichero `/etc/nsswitch.conf` se indica qué recursos se utilizan para resolver según que cosas, en caso de que se disponga de más de uno, es decir, si fuera necesario resolver nombres, en este fichero tenemos que primero el sistema hará una búsqueda de la información en el fichero `"/etc/hosts"`, y si la búsqueda no ha sido exitosa, entonces se hará la petición al DNS:

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

hosts:          files dns
networks:       files
netgroup:       nis
```

Servidor primaro DNS (Máquina GIZMO): `/etc/resolv.conf`

Este fichero es necesario en el sistema para saber cuáles son los servidores de nombres de la máquina en concreto, junto con el orden de dominios sobre los que debe hacer las peticiones. En este caso el fichero contendrá las siguientes líneas:

```
# CAMBIADO PARA DNS
# Búsqueda en orden según dominios.
search eupla.asi.cps.unizar.es asi.cps.unizar.es cps.unizar.es

# COMENTADO PARA DNS
# Servidores de nombres de la universidad de Zaragoza
# nameserver 155.210.33.4
# nameserver 155.210.12.9

# Nuestro servidor de nombres, activo para la ocasión.
nameserver 127.0.0.1
```

Nótese cómo hemos comentado las líneas de los servidores de nombres por defecto del sistema (los servidores de nombres de la Universidad de Zaragoza), sin embargo el nuevo servidor de nombres para nuestra zona será la propia máquina, pues estamos configurando el servidor de nombres primario para la zona `eupla.asi.cps.unizar.es`.

Para ilustrar lo que hace este fichero, pongamos un ejemplo: Si un cliente intenta buscar `hendrix`, lo primero que se probaría sería `hendrix.eupla.asi.cps.unizar.es`, luego `hendrix.asi.cps.unizar.es` y finalmente `hendrix.cps.unizar.es`. No es muy recomendable añadir muchos dominios en esta línea, pues lleva bastante tiempo hacer la comprobación de todos.

Servidor primario DNS (Máquina GIZMO): `/etc/bind/named.conf`

Éste es el fichero principal de configuración para el DNS. Este fichero contendrá información sobre qué ficheros consultar para resolver nombres de forma inversa o directa. También contendrá restricciones sobre servicios a otras máquinas.

El contenido del fichero es el que sigue:

```
options {
      directory "/var/cache/bind";
      auth-nxdomain no;    # conform to RFC1035

};

// prime the server with knowledge of the root servers
zone "." {
      type hint;
      file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
      type master;
      file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
      type master;
      file "/etc/bind/db.127";
};
```

```
zone "0.in-addr.arpa" {
      type master;
      file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
      type master;
      file "/etc/bind/db.255";
};

// Aquí empieza la declaración de nuestras zonas.

//ZONAS DIRECTAS
zone "eupla.asi.cps.unizar.es" {
      type master;
      file "/etc/bind/db.eupla";
      allow-transfer { 155.210.154.192; };
};

// La línea de 'allow-transfer' se debe a la existencia de un servidor DNS
// secundario, al cual le transferiremos los ficheros necesarios para la
// resolución de nombres, por si acaso el servidor primario cae.
// La IP del servidor secundario al que se harán las transferencias de ficheros
// será la 155.210.154.192.
// El fichero clave para resolver nombres de modo directo será el db.eupla.
// Análogamente, para la resolución inversa de nombres , se consultará el
// fichero db.194, al que se hace referencia en las líneas que siguen.

//ZONAS INVERSAS
zone "154.210.155.in-addr.arpa" {
      type master;
      file "/etc/bind/db.194";
      allow-transfer { 155.210.154.192; };
};
```

Servidor primario DNS (Máquina GIZMO): "/etc/bind/db.eupla"

```
$TTL  604800
@     IN    SOA   eupla.asi.  root.eupla.asi. (
                  20030710    ; Serial
                   604800     ; Refresh
                    86400     ; Retry
                  2419200     ; Expire
                   604800 )   ; Negative Cache TTL
;
      IN    NS    gizmo       ; Nombre del servidor maestro
;
; Host's pertenecientes a nuestro dominio
;
gizmo       IN    A     155.210.154.194
gizmo2      IN    A     155.210.154.192
gizmo3      IN    A     155.210.154.198
```

Este es el fichero de resolución de nombres de modo directo. Las seis primeras líneas son de configuración de la zona. Estas líneas dicen cuál es la zona (eupla.asi.) y quién es el responsable (root@eupla.asi) junto con una serie de campos. Estos otros campos nos dan una pista sobre cuándo se ha actualizado, cada cuanto actualizar la base de datos, cada cuanto reintentar una transferencia de zona, cuándo caduca la información de zona, y un tiempo de vida por defecto.
IMPORTANTE en el momento en el que se hagan cambios en el fichero de zona, deberemos incrementar el número de serie. Si no lo hacemos, podrán existir incoherencias entre la información contenida por el servidor primario y el secundario.

El resto del fichero de la zona relaciona todos los hosts de la zona con sus IP's.

Servidor primario DNS (Máquina GIZMO): "/etc/bind/db.194"

```
$TTL 86400
@     IN    SOA   eupla.asi.  root.eupla.asi. (
                  20030710    ; Serial
                  604800      ; Refresh
                  86400       ; Retry
                  2419200     ; Expire
                  60480       ; Minimum TTL
                  )
      IN    NS    gizmo.eupla.asi.cps.unizar.es.
;
194   IN    PTR   gizmo.eupla.asi.cps.unizar.es.
192   IN    PTR   gizmo2.eupla.asi.cps.unizar.es.
198   IN    PTR   gizmo3.eupla.asi.cps.unizar.es.
```

Los ficheros de búsqueda inversa son casi iguales a los ficheros de dominio descritos anteriormente, pero con algunos pequeños cambios.

Cabe destacar en este fichero la finalización con punto al final de los los nombres completos de los dominios (gizmo.eupla.asi.). Este fichero de zona contiene tres registros fuentes, el SOA (Start Of Authority), NS y el PTR. La @ es un caracter especial que denota el origen, como la columna de dominio para este fichero dice "154.210.155.in-addr.arpa", en realidad significa :

```
      154.210.155.in-addr.arpa      IN    SOA
```

NS es el registro fuente del servidor de nombres. No existe @ pues está implícita en la línea anterior, por lo que la línea NS podría también ser escrita como sigue:

```
154.210.155.in-addr.arpa      IN    NS    gizmo.eupla.asi.cps.unizar.es
```

Esta línea le dice al DNS qué máquina es la servidora de nombres del dominio 154.210.155.in-addr.arpa, que es gizmo.eupla.asi.cps.unizar.es.

Finalmente el registro PTR (Domain Name Pointer), que indica que la dirección del host 194 dentro de la subred 155.210.154 se llama gizmo.eupla.asi.cps.unizar.es. Análogamente con el host 192 y el host 198 dentro de la misma subred.

El registro SOA es el preámbulo de todos los ficheros de zona, y debería haber exactamente uno (al menos) por zona. En este fichero existen unos campos muy especiales (refresh, retry, expire y minimum) que indican , entre otras cosas, el tiempo de validez de este fichero. Sin embargo cabe destacar el campo Serial, a través del cual se hará un control sobre la transferencia de estos ficheros a los servidores secundarios existentes en la zona. Es decir, si el serial number del servidor primario es MAYOR que el contenido por el secundario, entonces se realizará la transferencia del fichero de zona como actualización.

Servidor secundario DNS (Máquina GIZMO2): "/etc/hosts"

```
      127.0.0.1   localhost
      155.210.154.192 gizmo2.cps.unizar.es     gizmo2
```

Análogamente habrá que cuidar los ficheros de configuración del sistema en el servidor secundario de nombres. Sólo hará falta incluir la correspondencia entre IP y host de la propia máquina (referenciable de dos posibles maneras).

Servidor secundario DNS (Máquina GIZMO2) : "/etc/resolv.conf"

```
# CONFIGURACIÓN PARA SERVIDOR DNS Esclavo
search eupla.asi.cps.unizar.es asi.cps.unizar.es cps.unizar.es
nameserver 155.210.154.194
nameserver 155.210.154.192
```

Este fichero es ahora ligeramente distinto al anterior. Si nos fijamos ahora utilizaremos el servidor de nombres primario para resolver peticiones. En caso de que éste falle, entonces haremos la petición a nuestra propia máquina (155.210.154.192). Sería indiferente añadir como servidor de nombres secundario a la IP 127.0.0.1 pues corresponde a "localhost" (nuestra propia máquina que desempeña el papel de servidor de nombres secundario).

Servidor secundario DNS (Máquina GIZMO2): "/etc/bind/named.conf"

```
options {
      directory "/var/cache/bind";
      auth-nxdomain no;    # conform to RFC1035

};

// prime the server with knowledge of the root servers
zone "." {
      type hint;
      file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
      type master;
      file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
      type master;
      file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
      type master;
      file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
      type master;
      file "/etc/bind/db.255";
};

// add entries for other zones below here

// ZONA DIRECTA DEL SERVIDOR ESCLAVO
zone "eupla.asi.cps.unizar.es" {
      type slave;
      file "/etc/bind/db.euplaS";
      masters { 155.210.154.194; };
};
// ZONA INVERSA DEL SERVIDOR ESCLAVO
zone "154.210.155.in-addr.arpa" {
      type slave;
```

```
      file "/etc/bind/db.192";
      masters { 155.210.154.194; };
};
```

Como vemos en estas dos zonas de arriba, únicamente habrá que especificar que la máquina actual desempeña el papel de "esclavo" (type slave;), indicando qué máquina le servirá como servidor primario de nombres (masters { 155.210.154.194; };). Igualmente que en el servidor primario, definiremos la ruta de los ficheros de las zonas ("/etc/bind/db.euplaS" y "/etc/bind/db.192"), sin embargo , en el servidor secundario no hará falta editar y definir dichos ficheros, pues serán transferidos por el servidor primario en cuanto ambos estén funcionando al mismo tiempo. A continuación veremos los ficheros obtenidos por la transferencia del servidor primario.

Servidor secundario DNS (Máquina GIZMO2) : "db.euplaS"

```
$ORIGIN .
$TTL 604800 ; 1 week
eupla.asi.cps.unizar.es IN SOA      eupla.asi. root.eupla.asi. (
                        20030710   ; serial
                        604800     ; refresh (1 week)
                        86400      ; retry (1 day)
                        2419200    ; expire (4 weeks)
                        604800     ; minimum (1 week)
                        )
                    NS    gizmo.eupla.asi.cps.unizar.es.
$ORIGIN eupla.asi.cps.unizar.es.
gizmo               A     155.210.154.194
gizmo2              A     155.210.154.192
gizmo3              A     155.210.154.198
```

Servidor secundario DNS (Máquina GIZMO2) : "db.192"

```
$ORIGIN .
$TTL 86400  ; 1 day
154.210.155.in-addr.arpa IN SOA     eupla.asi. root.eupla.asi. (
                        20030710   ; serial
                        604800     ; refresh (1 week)
                        86400      ; retry (1 day)
                        2419200    ; expire (4 weeks)
                        60480      ; minimum (16 hours 48 minutes)
                        )
                    NS    gizmo.eupla.asi.cps.unizar.es.
$ORIGIN 154.210.155.in-addr.arpa.
198                 PTR   gizmo3.eupla.asi.cps.unizar.es.
192                 PTR   gizmo2.eupla.asi.cps.unizar.es.
194                 PTR   gizmo.eupla.asi.cps.unizar.es.
```

Máquina Resolver-Only (Máquina GIZMO3): "/etc/hosts"

```
      127.0.0.1         localhost
      155.210.154.198   gizmo3.cps.unizar.es    gizmo3
```

Una vez más añadiremos los dos posibles nombres por los que puede ser identificada la máquina (en este caso cliente DNS).

Máquina Resolver-Only (Máquina GIZMO3): "/etc/resolv.conf"

```
      search eupla.asi.cps.unizar.es asi.cps.unizar.es cps.unizar.es
      #SERVIDOR PRIMARIO DNS
      nameserver 155.210.154.194
      #SERVIDOR SECUNDARIO DNS
```

```
nameserver 155.210.154.192
```

Igualmente, le diremos al sistema qué servidores de nombres ha de utilizar al hacer peticiones de resolución de nombres.