

INSTALACIÓN Y CONFIGURACIÓN:

SERVICIO DNS BIND9
UBUNTU SERVER 20.04

.int

.edu

.en

VENTAJAS DE UTILIZAR SERVIDOR DNS

La utilización de un servidor DNS local tiene ciertas ventajas:

- **Agilizar el acceso a Internet:** Al tener un servidor de nombres en nuestra propia red local (que acceda al DNS de nuestro proveedor o directamente a los *root servers*) se agiliza el mecanismo de resolución de nombres; manteniendo en caché los nombres recientemente usados en la red contribuimos a disminuir el tráfico hacia/desde Internet. Si estamos en una red con varios equipos mayor beneficio.
- **Simplificar la administración de la red local:** Al contar con un DNS propio es posible definir zonas locales (no válidas ni accesibles desde Internet) para asignar nombres a cada uno de los ordenadores de la red. De esta forma es posible, por ejemplo, referirnos al servidor web como `www.aulaSMR.com` en vez de `192.168.1.1` y a nuestra impresora de red como `impresora.aulaSMR.com` en vez de `192.168.1.141`. Pensemos, por ejemplo, que ocurriría con las configuraciones de las aplicaciones si un día decidimos cambiar el esquema de direcciones IP de nuestra red.

CONFIGURACIÓN DE RED DEL SERVIDOR

El servidor DNS debería tener una IP fija o estática.

- Configura mediante el fichero de configuración de red correspondiente a esa IP estática.
- Otro método sugerido es obtener una IP fija por medio de una reserva de IP en algún servicio DHCP instalado en tu red.
- En VB tendremos una tarjeta de red en red interna y la otra en modo NAT para poder disponer de conexión a internet.



INSTALAR SERVICIO DNS – ACTUALIZAR REPOSITARIOS

Como primer paso para instalar el paquete de servicios DNS en nuestro sistema debemos cerciorarnos que nuestro sistema este actualizado para descargar e instalar el paquete.

Usaremos el gestor de paquetes apt (Herramienta Avanzada de Empaquetamiento), el cual nos ofrece un modo fácil, rápido y eficiente de instalar programas.

Ejecutamos el comando `apt-get update` e inmediatamente el sistema buscará en los repositorios actualizaciones para nuestro sistema.

INSTALAR BIND9

BIND (*Berkeley Internet Name Domain*) es el servidor de DNS más comúnmente usado en Internet, especialmente en sistemas Unix, en los cuales es un estándar de facto.

La configuración del servidor DNS Bind en Linux requiere la instalación de los paquetes siguientes (como root):

```
# apt-get install bind9 bind9utils bind9-doc
```

Los archivos de configuración están en el directorio `/etc/bind`.

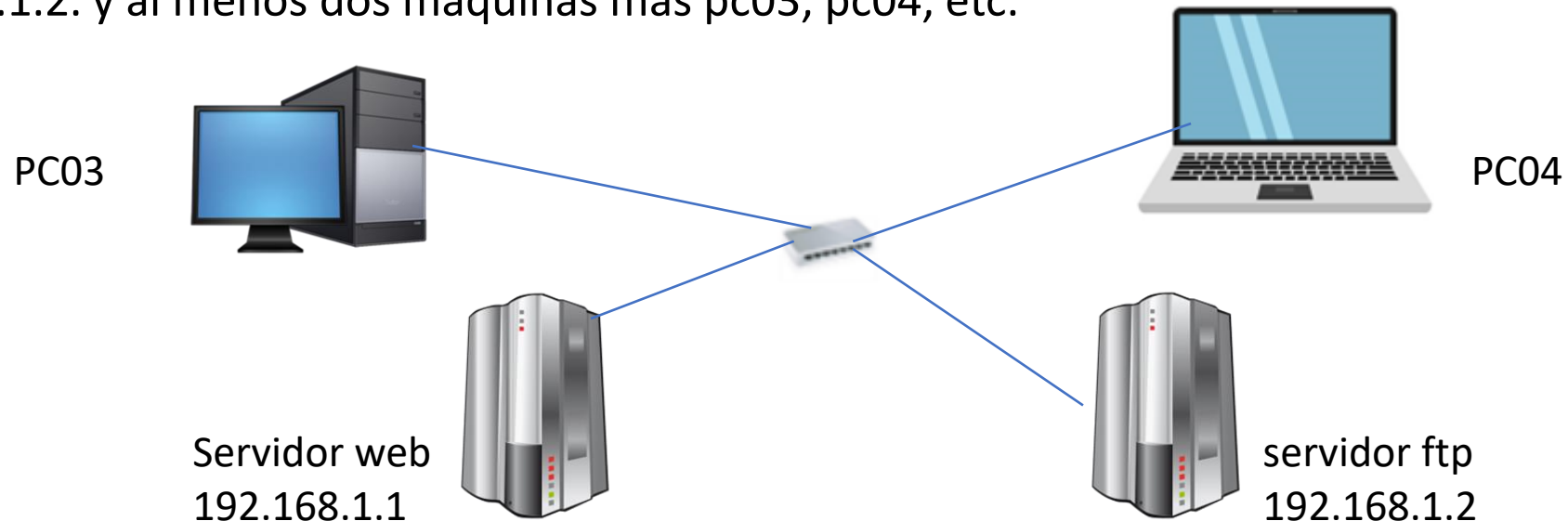
- Revisa el contenido de estos archivos.
- Busca donde se encuentra el archivo con la información de los root servers y compara el contenido con el de la imagen del mismo archivo en los apuntes.

ESCENARIO EJEMPLO

El dominio que vamos a crear para realizar esta práctica lo vamos a llamar aulaSMR.com. Instalaremos un servidor DNS. La máquina que hace de servidor de nombres, cuyo nombre será servidor tiene la IP 192.168.1.1, y hace también la función de servidor web.

De esta forma, desde cualquier ordenador de nuestra red interna podemos poner www.aulaSMR.com en el navegador para que aparezca la página web almacenada en el servidor.

En la red del ejemplo hay también un servidor FTP, cuyo nombre es servidor2 y tiene dirección IP 192.168.1.2. y al menos dos máquinas más pc03, pc04, etc.



CONFIGURACIÓN BIND9

Los archivos de configuración que tendremos que modificar en el servidor DNS son los siguientes:

- /etc/bind/named.conf.options
- /etc/bind/named.conf.local

Estos dos siguientes **los crearemos nosotros** ya que no existen, y corresponden a las características de nuestro dominio.

- /etc/bind/db.aulaSMR.com
- /etc/bind/db.192.168.1

FICHERO NAMED.CONF.OPTIONS

En primer lugar modificamos el fichero **/etc/bind/named.conf.options**.

Por defecto, al instalar el paquete *bind* está preconfigurado como servidor caché DNS.

Tan solo será necesario editar el archivo `/etc/bind/named.conf.options` y en la sección *forwarders* añadir las IP de dos servidores DNS donde redirigir las peticiones DNS (en nuestro caso dará igual pues estamos en red interna, en entornos reales será imprescindible una correcta configuración). Por ejemplo los DNS de nuestro proveedor de servicios, o los que se estén usando en la red en la que nos encontremos.

FICHERO NAMED.CONF.LOCAL

Las zonas específicas del servidor DNS que se configura se definen en /etc/bind/named.conf.local.

```
#Esta sería la definición de zona, con el nombre escogido
zone "aulaSMR.com"{
    type master;
    file "/etc/bind/db.aulaSMR.com";
};
```

```
#Esta sería la definición de zona de resolución inversa.
Cambia 1.168.192 por la dirección de tu red.
zone "1.168.192.in-addr.arpa"{
    type master;
    file "/etc/bind/db.192.168.1";
};
```

FICHERO DB.AULASMR.COM

Ahora tenemos que crear el fichero de definición de zona /etc/bind/db.aulaSMR.com

En este fichero es donde pondremos todos los nombres de máquinas y direcciones IP que conocerá nuestro servidor DNS.

Al principio del documento añadiremos el SOA.

FICHERO DB.192.168.1

A continuación, creamos el archivo de zona de resolución inversa /etc/bind/db.192.168.1

```
@ IN SOA servidor.aulaSMR.com. admin.aulaSMR.com. (  
2022101001 ;  
86400      ;  
60         ;  
360000     ;  
172800     );  
;  
  
@ IN NS  servidor.aulaSMR.com.  
@ IN NS  secundario.aulaSMR.com.  
1 IN PTR servidor.aulaSMR.com.  
2 IN PTR servidor2.aulaSMR.com.  
3 IN PTR pc03.aulaSMR.com.  
10 IN PTR secundario.aulaSMR.com.
```

COMANDO NAMED-CHECKCONF

Cuando hayamos creado cada uno de los archivos tendremos que reiniciar BIND con el siguiente comando:

/etc/init.d/bind9 restart o también **# service bind9 restart**

A partir de la versión 9 de BIND se incluyen dos herramientas software para comprobar la sintaxis y semántica de los archivos que describen las zonas y el archivo de configuración principal *named.conf*.

Dichas herramientas son: *named-checkzone* y *named-checkconf*.

Una vez configurado el servidor DNS, si se quiere hacer una comprobación sintáctica del archivo de configuración *named.conf* hay que ejecutar: *named-checkconf*. La salida muestra los errores que genera. Si no genera salida, está todo correcto. Algunas son simplemente advertencias.

COMANDO NAMED-CHECKZONE

Si lo que queremos comprobar son los archivos de zona entonces el comando a ejecutar es:

```
named-checkzone dominioacomprobar ficherozonadeldominio
```

Por ejemplo,

```
named-checkzone aulaSMR.com /etc/bind/db.aulaSMR.com
```

Este comando genera la siguiente salida si todo está correcto:

```
zone aulaSMR.com/IN: loaded serial 1 OK
```

Esta comprobación también la tendremos que realizar para el archivo de zona inversa.

```
named-checkzone 1.168.192.in-addr.arpa /etc/bind/db.192.168.1
```

COMPROBANDO LOS LOGS

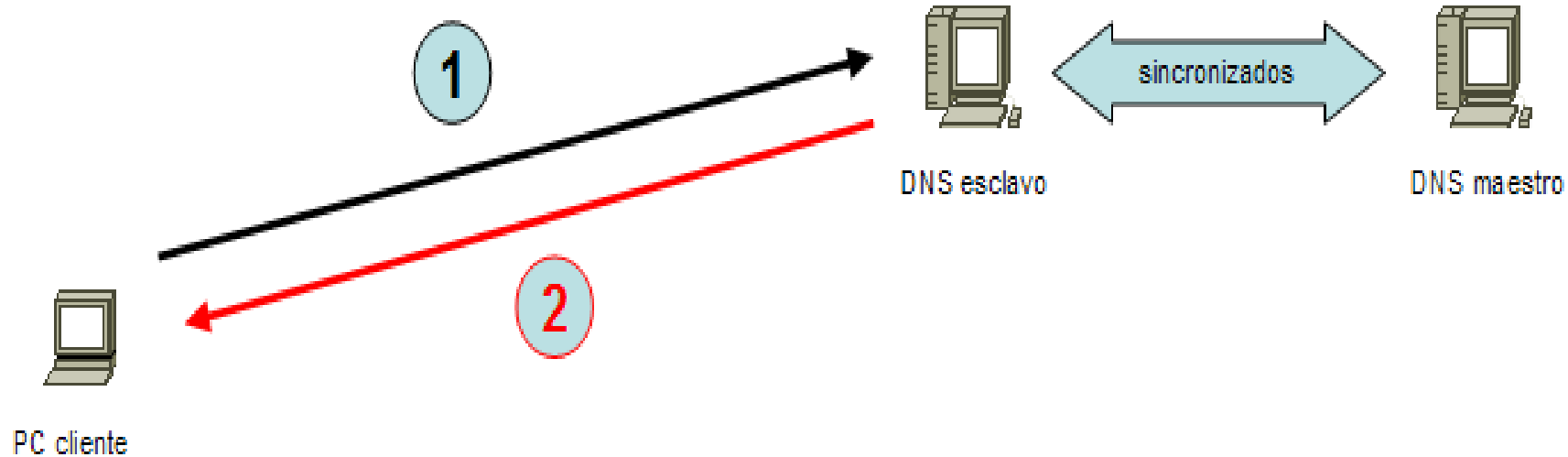
Para analizar posibles fallos en el funcionamiento del servidor DNS conviene visualizar el contenido del archivo de logs `/var/log/syslog`.

```
Oct 16 07:37:58 servidorsr named[1383]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
Oct 16 07:37:58 servidorsr named[1383]: network unreachable resolving './NS/IN': 2001:7fe::53#53
Oct 16 07:37:58 servidorsr named[1383]: network unreachable resolving './NS/IN': 2001:500:2::c#53
Oct 16 07:37:58 servidorsr named[1383]: network unreachable resolving './NS/IN': 2001:7fd::1#53
Oct 16 07:37:58 servidorsr named[1383]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
Oct 16 07:37:58 servidorsr named[1383]: resolver priming query complete
Oct 16 07:41:14 servidorsr dhcpd[653]: DHCPREQUEST for 192.168.1.63 from 08:00:27:15:81:d6 (alumnoVB) via enp0s3
Oct 16 07:41:14 servidorsr dhcpd[653]: DHCPACK on 192.168.1.63 to 08:00:27:15:81:d6 (alumnoVB) via enp0s3
Oct 16 07:46:14 servidorsr dhcpd[653]: DHCPREQUEST for 192.168.1.63 from 08:00:27:15:81:d6 (alumnoVB) via enp0s3
Oct 16 07:46:14 servidorsr dhcpd[653]: DHCPACK on 192.168.1.63 to 08:00:27:15:81:d6 (alumnoVB) via enp0s3
```

INSTALAR UN SERVIDOR SECUNDARIO DNS

En la máquina que hayamos decidido que haga de servidor secundario instalaremos el servicio **bind9**.

Para continuar con nuestro ejemplo, vamos a suponer la instalación de un nuevo servidor secundario en nuestro escenario del dominio aulaSMR.com. El nuevo servidor se llamará secundario.aulaSMR.com y se encontrará en la máquina con IP 192.168.1.10



AÑADIR DNS SECUNDARIO AL PRIMARIO (ZONA DIRECTA)

Si deseamos configurar nuestro servidor DNS para que actúe como esclavo de un servidor DNS maestro, la configuración es mucho más sencilla que en el caso anterior ya que únicamente será necesario indicar en el DNS esclavo quién es el servidor DNS maestro, y en el DNS maestro la IP del DNS esclavo.

Recordemos que el nombre del DNS maestro era servidor.aulaSMR.com. con IP 192.168.1.1.

Supongamos que el nombre del DNS esclavo es secundario.aulaSMR.com.

En el archivo db.aulaSMR.com de zona directa que se encuentra en la máquina que hace de maestro añadiremos la línea del segundo DNS justo debajo de donde está la del primero:

```
aulaSMR.com. IN NS servidor.aulaSMR.com.  
aulaSMR.com. IN NS secundario.aulaSMR.com.
```


AÑADIR DNS SECUNDARIO AL PRIMARIO (ZONA INVERSA)

Lo mismo haremos en el archivo db.192.168.1 de la zona inversa en el servidor primario.

Por tanto, habrá que añadir unas líneas en /etc/bind/db.192.168.1 del maestro.

```
1.168.192.in-addr.arpa. IN NS servidor.aulaSMR.com.
```

```
1.168.192.in-addr.arpa. IN NS secundario.aulaSMR.com.
```

FICHERO NAMED.CONF.LOCAL DEL PRIMARIO

En el archivo `/etc/bind/named.conf.local` del servidor DNS maestro añadimos las directivas *allow-transfer* y *also-notify* en cada una de las zonas para mantener los DNS sincronizados.

Debemos meter estas 2 directivas dentro de cada una de las secciones de zona declaradas en el fichero

```
allow-transfer {ip_del_secundario};  
also-notify {ip_del_secundario};
```

FICHERO NAMED.CONF.LOCAL DEL SECUNDARIO

En el archivo */etc/bind/named.conf.local* del servidor DNS **secundario** debemos indicar que se trata de un servidor esclavo y también debemos indicar quién es el maestro:

En este caso cambia al ser tipo esclavo (secundario).

El archivo no contiene una ruta y hay una directiva masters con la IP privada del servidor maestro (primario).

```
zone "aulaSMR.com"{
    type slave;
    file "db.aulaSMR.com";
    masters {192.168.1.1;};
};
```

```
zone "1.168.192.in-addr.arpa"{
    type slave;
    file "db.192.168.1";
    masters {192.168.1.1;};
};
```

FICHEROS DE ZONA DEL SERVIDOR SECUNDARIO

Por defecto, el directorio donde se guardan los archivos de zona es */var/cache/bind*.

Dicho directorio se declara en el archivo */etc/bind/named.conf.options* con la directriz ***directory "/var/cache/bind";***

REINICIAR LOS SERVICIOS

Por último, reiniciaremos el servicio bind en el servidor primario antes que en el secundario.

Después de reiniciar el servicio verificamos en el syslog que nuestro servidor DNS secundario está copiando la zona de DNS para aulaSMR.com. (tail -f /var/log/syslog)

Encontraremos un registro similar a este:

```
Oct 16 10:12:42 servidorsr named[1455]: transfer of '1.168.192.in-addr.arpa/IN' from 192.168.1.1#53:
Transfer completed: 1 messages, 7 records, 240 bytes, 0.001 secs (240000 bytes/sec)
Oct 16 10:12:42 servidorsr named[1455]: zone 1.168.192.in-addr.arpa/IN: sending notifies (serial 202
2101001)
Oct 16 10:12:43 servidorsr named[1455]: zone aulaSMR.com/IN: Transfer started.
Oct 16 10:12:43 servidorsr named[1455]: transfer of 'aulaSMR.com/IN' from 192.168.1.1#53: connected
using 192.168.1.10#51567
Oct 16 10:12:43 servidorsr named[1455]: zone aulaSMR.com/IN: transferred serial 2022101201
Oct 16 10:12:43 servidorsr named[1455]: transfer of 'aulaSMR.com/IN' from 192.168.1.1#53: Transfer s
tatus: success
Oct 16 10:12:43 servidorsr named[1455]: transfer of 'aulaSMR.com/IN' from 192.168.1.1#53: Transfer c
ompleted: 1 messages, 11 records, 286 bytes, 0.008 secs (35750 bytes/sec)
```

Y ya podemos hacer la prueba de configurar un cliente para que use como DNS los servidores DNS configurados, y comprobar que si alguna de las dos están apagadas, la otra es la que resuelve.

INSTALACIÓN Y CONFIGURACIÓN BIND9 UBUNTU SERVER 20.04

FIN