Nombre _____

Práctica 3.2: Servidor DNS Maestro con chroot y apparmor

En esta práctica se cambiará la configuración del servidor DNS maestro de la práctica 3.1, para que el usuario "bind", usuario ligado al servicio bind9, tenga como raíz del árbol de directorios el directorio real "/chroot/bind9" (es un directorio nuevo que tendrá que ser creado).

Para ello deberemos modificar el fichero /etc/default/bind9, y cambiar la línea:

OPTIONS="-u bind"

Por lo siguiente:

OPTIONS="-u bind -t /chroot/bind9/"

Esta nueva opción "–t <ruta>" indica el nuevo directorio raíz para el usuario bind y por lo tanto estará confinado en ese directorio y no tendrá acceso al resto del sistema de ficheros.

A continuación, tendremos que recrear a partir del nuevo directorio raíz del usario "bind" todo aquello que el servidor bind9 necesita, tanto directorios, como ficheros, como dispositivos.

Primero creamos todos los directorios necesarios:

Creamos una serie de directorio necesarios:

Creamos una serie de directorio necesarios:

mkdir –p /chroot/bind9/etc

mkdir /chroot/bind9/dev

mkdir –p /chroot/bind9/var/cache

mkdir –p /chroot/bind9/var/run/bind/run

Ahora, movemos los ficheros de definición de las zonas a su nueva ubicación, o sean a /chroot/bind9/etc/bind:

mv /etc/bind /chroot/bind9/etc

También podemos mover los ficheros con la base de datos temporal (los archivos que guardan la información del DNS local) a su nueva ubicación /chroot/bind9/var/cache/bind:

mv /var/cache/bind /chroot/bind9/var/cache

Para que el bind se actualice correctamente y otras aplicaciones que necesiten acceder al directorio /etc/bind funcionen bien es necesario crear un enlace simbólico en la carpeta /etc/bind que apunte a la nueva ubicación:

ln -s /chroot/bind9/etc/bind   /etc/bind

También es imprescindible crear (usando el comando nknod) los dispositivo /dev/null y /dev/random… para el nuevo bind y a partir de la ubicación en el nuevo entorno (no se pueden copiar):

mknod /chroot/bind9/dev/null c 1 3

mknod /chroot/bind9/dev/random c 1 8

Además, tenemos que cambiar el propietario de los ficheros movidos :

chown -R bind:bind /chroot/bind9/etc/bind

chown -R bind:bind /chroot/bind9/var/cache/bind

Cambiamos los permisos de los dispositivos creados:

chmod 666 /chroot/bind9/dev/{null,random}

Finalmente, configuramos el registro de eventos para que capture los eventos de bind9 en su nueva ubicación. Editamos /etc/deafult/rsyslog, y cambiamos RSYSLOGD_OPTIONS=“ ” por RSYSLOGD_OPTIONS=“-a /chroot/bind9/dev/log”

Al final del proceso tenemos que iniciar el demonio bind …

/etc/init.d/bind9 start
[ok] Starting bind9 (via systemctl): bind9.service.

Para comprobar que bind está funcionando introducimos:

/etc/init.d/bind9 status

Active: **Active (running)**

Si lo anterior no funciona, es muy posible que haya un conflicto con la aplicación de seguridad “apparmor”. Esto puede solucionarse si se le indica a apparmor la nueva ubicación de los ficheros de bind. Para ello tenemos que modificar el fichero /etc/apparmor.d/usr.sbin.named y hacer los siguientes cambios:

Donde aparezca	/etc/bind	reemplazar por	/chroot/bind9/etc/bind
Donde aparezca	/var/lib/bind	reemplazar por	/chroot/bind9/var/lib/bind
Donde aparezca	/var/cache/bind	reemplazar por	/chroot/bind9/var/cache/bind

Finalmente, reiniciamos apparmor y comprobar que funciona correctamente:

service apparmor reload

El servidor DNS también debería funcionar_

service bind9 status