

Práctica 3.2: Servidor DNS Maestro con chroot y apparmor

Cristina Díaz García

Noviembre 2018

Índice

Índice general	1
1. Modificación de <i>/etc/default/bind9</i>	2
2. Creación de directorios necesarios para bind9	2
3. Movemos los ficheros de definición de zonas	2
4. Creamos el enlace simbólico	2
5. Creamos <i>/dev/null</i> y <i>/dev/random</i>	2
6. Cambiamos el propietario	2
7. Cambiamos los permisos	2
8. Editamos el archivo <i>rsyslog</i>	3
9. Iniciamos bind y comprobamos su estado	3
10. Comprobamos su funcionamiento	3

1. Modificación de */etc/default/bind9*

```
GNU nano 2.9.3 /etc/default/bind9
# run resolvconf?
RESOLVCONF=no

# startup options for the server
OPTIONS="-u bind -t /chroot/bind9/"
```

2. Creación de directorios necesarios para bind9

```
ladynightmare@ladynightmare-E5-522-4154:~$ mkdir -p /chroot/bind9/etc
ladynightmare@ladynightmare-E5-522-4154:~$ mkdir /chroot/bind9/dev
ladynightmare@ladynightmare-E5-522-4154:~$ mkdir -p /chroot/bind9/var/cache
ladynightmare@ladynightmare-E5-522-4154:~$ mkdir -p /chroot/bind9/var/run/bind/run
```

3. Movemos los ficheros de definición de zonas

```
ladynightmare@ladynightmare-E5-522-4154:~$ mv /etc/bind /chroot/bind9/etc
ladynightmare@ladynightmare-E5-522-4154:~$ mv /var/cache/bind /chroot/bind9/var/cache
```

4. Creamos el enlace simbólico

```
ladynightmare@ladynightmare-E5-522-4154:~$ sudo ln -s /chroot/bind9/etc/bind /etc/bind
```

5. Creamos */dev/null* y */dev/random*

```
ladynightmare@ladynightmare-E5-522-4154:~$ mknod /chroot/bind9/dev/null c 1 3
ladynightmare@ladynightmare-E5-522-4154:~$ mknod /chroot/bind9/dev/random c 1 8
```

6. Cambiamos el propietario

```
ladynightmare@ladynightmare-E5-522-4154:~$ sudo chown -R bind:bind /chroot/bind9/etc/bind
ladynightmare@ladynightmare-E5-522-4154:~$ sudo chown -R bind:bind /chroot/bind9/var/cache/bind
```

7. Cambiamos los permisos

```
ladynightmare@ladynightmare-E5-522-4154:~$ sudo chmod 666 /chroot/bind9/dev/{null,random}
```

8. Editamos el archivo *rsyslog*

```
GNU nano 2.9.3 /etc/default/rsyslog
# Options for rsyslogd
# -x disables DNS lookups for remote messages
# See rsyslogd(8) for more details
RSYSLOGD_OPTIONS="-a /chroot/bind9/dev/log"
```

9. Iniciamos bind y comprobamos su estado

```
ladynightmare@ladynightmare-E5-522-4154:~$ /etc/init.d/bind9 start
[ ok ] Starting bind9 (via systemctl): bind9.service.

ladynightmare@ladynightmare-E5-522-4154:~$ /etc/init.d/bind9 status
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2018-11-20 18:24:01 CET; 1h 16min ago
     Docs: man:named(8)
    Main PID: 28559 (named)
      Tasks: 7 (limit: 4915)
    CGroup: /system.slice/bind9.service
            └─28559 /usr/sbin/named -f -u bind -t /chroot/bind9/

nov 20 18:24:03 ladynightmare-E5-522-4154 named[28559]: network unreachable r...53
nov 20 18:24:03 ladynightmare-E5-522-4154 named[28559]: managed-keys-zone: Ke...ed
nov 20 18:24:03 ladynightmare-E5-522-4154 named[28559]: managed-keys-zone: Ke...ed
nov 20 18:24:03 ladynightmare-E5-522-4154 named[28559]: resolver priming quer...te
nov 20 18:24:03 ladynightmare-E5-522-4154 named[28559]: checkhints: b.root-se...ts
nov 20 18:24:03 ladynightmare-E5-522-4154 named[28559]: checkhints: b.root-se...ts
nov 20 18:24:03 ladynightmare-E5-522-4154 named[28559]: checkhints: b.root-se...ts
nov 20 18:24:03 ladynightmare-E5-522-4154 named[28559]: checkhints: b.root-se...ts
nov 20 18:24:03 ladynightmare-E5-522-4154 named[28559]: checkhints: l.root-se...ts
nov 20 18:24:03 ladynightmare-E5-522-4154 named[28559]: checkhints: l.root-se...ts
Hint: Some lines were ellipsized, use -l to show in full.
```

10. Comprobamos su funcionamiento

```
ladynightmare@ladynightmare-E5-522-4154:~$ host dijkstra.org
dijkstra.org has address 185.53.178.8
dijkstra.org mail is handled by 5 mail.h-email.net.
ladynightmare@ladynightmare-E5-522-4154:~$ host pc7.dijkstra.org
pc7.dijkstra.org has address 185.53.178.8
pc7.dijkstra.org mail is handled by 5 mail.h-email.net.
```