ACTIVIDAD DNS[1]

1. Configuración de un servidor de nombres

1. Instalación del servicio

   `$ sudo apt-get install bind9 bind9utils dnsutils`

2. Los valores que debemos tener claros antes de comenzar son los siguientes:

   Dominio que vamos a crear [2]: *srdsi.lab*

   Nombre del servidor: *dns1.srdsi.lab*

   Dirección IP del servidor: *dirIP_dns1_ns* [p.e.: *172.16.0.136*]

3. En el servidor de nombres

   - Cambiar nombre en `/etc/hostname`
     dns1
   - En `/etc/hosts`
     127.0.0.1 localhost
     127.0.1.1 dns1.srdsi.lab dns1
   - Actualizar nombre

     `$ sudo hostnamectl set-hostname` *dns1*
   - Al ejecutar: `$ hostname --`*fqdn*
     dns1.srdsi.lab
   - Configurar el servidor como local en `/etc/resolv.conf`
     `domain` *srdsi.lab*
     `nameserver 127.0.0.1`
     Ejecutar: `$ sudo chattr +i /etc/resolv.conf`

4. Relanzar servicio

   `$ sudo systemctl restart bind9`

[Con esta configuración el servidor `dns1` actua como un servidor caché]
23-24: red UPV/EHU no permite consultas a servidores DNS externos

- Comando `rndc` (name server control utility)
  - `$ sudo rndc status`

[1] Recomendación: reducir las características de las máquinas virtuales a 1GB RAM y 1 CPU

[2] Utilizad el nombre del grupo como base para el nombre del dominio

  - Descarga la caché RAM en el fichero `/var/cache/bind/named_dump.db`
    `$ sudo rndc dumpdb -cache`
  - Borrar la caché
    `$ sudo rndc flush`

- Monitorizar ejecución y posibles errores: `$ tail /var/log/daemon.log`
- Cliente DNS / resolver: `$ dig @dirIPserver nameDNS typeRR`

Configuración de un cliente (*resolver*)

- Configurar el servidor local para el cliente en `/etc/resolv.conf`
  `domain srdsi.lab`
  `search srdsi.lab`
  `nameserver dirIP_dns1_ns`
  Ejecutar: `$ sudo chattr +i /etc/resolv.conf`
- Sin cambiar configuración del cliente
  `$ dig @dirIP_dns1_ns srdsi.lab. [tipoRR]`

2. Configuración de un servidor autorizado para la zona "*srdsi.lab*"

1. Configurar una nueva zona. Añadir en `/etc/bind/named.conf.local`:

```
// zona de resolución directa "srdsi.lab"
zone "srdsi.lab" {
    type primary;
    file "/etc/bind/db.srdsi.lab";
};
// zona de resolución inversa "0.16.172.in-addr.arpa"
zone "0.16.172.in-addr.arpa" {
    type primary;
    file "/etc/bind/db.0.16.172";
};
```

2. Crear el fichero de la zona `/etc/bind/db.srdsi.lab`

```
$ORIGIN     srdsi.lab.
$TTL        2h
@           IN          SOA     dns1.srdsi.lab. admin.srdsi.lab. (
            20140401                ; Serial
            604800                  ; Refresh
            86400                   ; Retry
            2419200                 ; Expire
            604800      )           ; Negative Cache TTL
;
srdsi.lab.  IN          NS      dns1.srdsi.lab.
;
dns1        IN          A       172.16.0.136
host1       IN          A       172.16.0.138
www         IN          CNAME   host1
```

3. Crear el fichero de la zona de resolución inversa `/etc/bind/db.0.16.172`

```
$TTL   604800
@      IN       SOA   dns1.srdsi.lab. admin.srdsi.lab. (
       20140401         ; Serial
       604800           ; Refresh
       86400            ; Retry
       2419200          ; Expire
       604800    )      ; Negative Cache TTL
;
@      IN       NS    dns1.srdsi.lab.
;
136    IN       PTR   dns1.srdsi.lab.
138    IN       PTR   host1.srdsi.lab.
```

4. Verificar configuración y zonas

   `$ sudo named-checkconf /etc/bind/named.conf`

   `$ sudo named-checkzone srdsi.lab /etc/bind/`*`db.srdsi.lab`*

   `$ sudo named-checkzone `*`0.16.172`*`.in-addr.arpa /etc/bind/`*`db.0.16.172`*

5. Lanzar *named*, verificar estado y funcionamiento

   `$ sudo systemctl restart bind9 [# sudo rndc reload]`

   `$ sudo rndc status`

   `$ dig `*`@dirIP_dns1_ns`*` dns1.srdsi.lab`

   `$ dig @localhost -x 172.16.0.136`

3. Configurar servidor de nombres secundario

1. Instalación servicio
2. Configurar el servidor con los siguientes valores:

   Dominio que vamos a crear: *srdsi.lab*

   Nombre del servidor: *dns2.srdsi.lab*

   Dirección IP del servidor: *dirIP_dns2_ns* [p.e.: *172.16.0.137*]
3. Configurar el servidor como local en `/etc/resolv.conf`

   `domain` *srdsi.lab*

   `nameserver 127.0.0.1`

   `nameserver` *dirIP_dns1_ns*

   Ejecutar: `$ sudo chattr +i /etc/resolv.conf`
4. Añadir en `/etc/bind/named.conf.local`

```
zone "srdsi.lab" {
    type secondary;
    file "/var/cache/bind/secondary/db.srdsi.lab";
    masterfile-format text;
    masters { dirIP_dns1_ns; };
};
zone "0.16.172.in-addr.arpa" {
    type secondary;
    file "/var/cache/bind/secondary/db.0.16.172";
    masterfile-format text;
    masters { dirIP_dns1_ns; };
};
```

5. Crear directorio que contendrá los ficheros transferidos desde el servidor primario, con los pemisos adecuados:

   `$ sudo chown bind:bind /var/cache/bind/secondary`
6. No permitir transferencias a otros NS, añadiendo en `/etc/bind/named.conf.options`

   `allow-transfer { none; };`
7. Verificar configuración y relanzar *named*

   `$ sudo systemctl restart bind9`

8. En el servidor primario `dns1` hay que configurar las declaraciones de zonas para que permitan las transferencias de zona al secundario, y también que le nofitifiquen los cambios (modificación valor `serial`)

   a) Añadir en cada zona, en el fichero `/etc/bind/named.conf.local`
   `allow-transfer { dirIP_dns2_ns ; };`
   `also-notify { dirIP_dns2_ns ; };`

   b) Reiniciar servidor primario

9. Comprobar con el resolver las transferencias de zona

   `$ dig @dirIP_dns1_ns srdsi.lab axfr`

   `$ dig @dirIP_dns2_ns srdsi.lab axfr`

10. En caso de errores, comprobar *logs*:

    `$ sudo tail /var/log/syslog`

    `$ sudo tail /var/log/daemon.log`

11. Incorporar este nuevo servidor en las BDs del servidor maestro (recomendable cambiar `serial`)

```
srdsi.lab.   IN   NS   dns1.srdsi.lab.
             IN   NS   dns2.srdsi.lab.
dns2         IN   A    172.16.0.137
```

    - Recargar la nueva configuración de `dns1`

    `$ sudo rndc reload`

12. Comprobar las transferencias de zonas entre los servidores con *Wireshark*

    a) en *dns1*: `$ sudo systemctl stop bind9`

    b) lanzar *Wireshark* (filtro: `ipaddr==`*dirIP_dns2_ns*)

    c) en *dns1*: `$ sudo systemctl start bind9`

    Otra opción, en *dns1*:

    `$ sudo rndc notify nombre-zona`

4. Transaction Signature (TSIG)

A. Configurar servidor primario(maestro)

1. Generar claves TSIG en el servidor primario (en `/etc/bind`)

   ```
   $ sudo tsig-keygen dns1-dns2_tsigkey > Kdns1-dns2_tsigkey
   key "dns1-dns2_tsigkey" {
       algorithm hmac-sha256;
       secret "Ok1qR5IW1ROAzOn21Ju==";
   };
   ```

2. Incorporarlo a la configuración del servidor en `/etc/bind/named.conf`

   ```
   include "/etc/bind/Kdns1-dns2_tsigkey";
   ```

3. Indicar que zonas utilizarán TSIG (`/etc/bind/named.conf.local`)

   ```
   zone "srdsi.lab" {
       type primary;
       file "/etc/bind/db.srdsi.lab";
       also-notify { dirIP_dns2_ns; };
       allow-transfer { key dns1-dns2_tsigkey;};
   };
   ```

4. Reiniciar servidor

   ```
   $ sudo systemctl restart bind9
   ```

B. Configurar servidor secundario

1. Distribuir la clave a los servidores secundarios (*off-line*, `ssh`)

2. Crear un fichero `/etc/bind/Kdns1-dns2_tsigkey`

   ```
   key "dns1-dns2_tsigkey" {
       algorithm hmac-sha256;
       secret "Ok1qR5IW1ROAzOn21Ju==";
   };
   server dirIP_dns1-ns {
       keys { dns1-dns2_tsigkey; };
   };
   ```

3. Incorporarlo a la configuración del servidor en `/etc/bind/named.conf`

   ```
   include "/etc/bind/Kdns1-dns2_tsigkey";
   ```

4. Modificar la definición de las zonas en `/etc/bind/named.conf.local`

   `masters { dirIP_dns1_ns key dns1-dns2_tsigkey; };`

5. Recargar configuración [Reiniciar servidor]

   `$ sudo rndc reload [systemctl restart bind9]`

6. Comprobar con el resolver las transferencias de zona

   `$ dig @dirIP_dns1-ns srdsi.lab axfr`

   - Al no indicar la clave fallará, hay que proporcionársela al resolver (un fichero que solo incluya la clave)

   `$ sudo dig @dirIP_dns1-ns srdsi.lab axfr`
   `-k Kdns1-dns2_tsigkey_only`

7. Ambas máquinas deben estar sincronizadas, mediante servidores explícitos (Network Time Protocol- NTP). En nuestro caso, podemos sincronizarlas lanzando las dos máquinas virtuales a la vez (sino puede cambiarse la hora con `date --set HH:MM:SS`)

8. Probar las transferencias de zonas entre servidores con *Wireshark*. ¿Qué cambia al usar TSIG?

5. DNSSEC

Pasos para firmar una zona (forma manual)

1. Generar claves para la zona (en `/etc/bind`)

   a) KSK (*Key-Signing Key*)
   `$ sudo dnssec-keygen -a RSASHA256 -b 1024 -f KSK -n ZONE srdsi.lab.`

   b) ZSK (*Zone-Signing Key*)
   `$ sudo dnssec-keygen -a RSASHA256 -b 1024 -n ZONE srdsi.lab.`

2. Añadir los registros DNSKEY de las claves ZSK y KSK al fichero de la zona `/etc/bind/db.srdsi.lab` (actualizar `serial`)

   `$INCLUDE Ksrdsi.lab.+005+39015.key`

   `$INCLUDE Ksrdsi.lab.+005+57448.key`

3. Firmar la zona

   `$ sudo dnssec-signzone -t -o srdsi.lab. [-k KSK-file] db.srdsi.lab [ZSK-file]`

4. [Habilitado por defecto]
   Habilitar en el servidor el uso de DNSSEC, en `/etc/bind/named.conf.options`

```
options {
    ...
    dnssec-enable yes;
};
```

5. Actualizar la declaración de la zona. Añadir en `/etc/bind/named.conf.local`:

```
zone "srdsi.lab" {
    type primary;
    file "/etc/bind/db.srdsi.lab.signed";
};
```

6. Verificar y recargar configuración del servidor.

7. Comprobación
   `$ dig @localhost srdsi.lab. [{dnskey, rrsig, nsec}] +dnssec [+multi]`

8. Validación cadena de confianza:

   a) Especificar un ***trust anchor.*** Añadir nuestra KSK en un fichero, `/etc/bind/trustanchor.key` :

```
trust-anchors {
srdsi.lab. static-key 257 3 8 "AwE ... Wi5";
};
```

b) Ejecutar el comando indicándole el fichero anterior como punto de partida de la cadena de confianza:

```
$ delv @localhost srdsi.lab. -a /etc/bind/trustanchor.key
+root=srdsi.lab srdsi.lab SOA [+multiline]
```

9. Quedaría pendiente enviar nuestra KSK (`dsset-srdsi.lab`) al administrador de nuestra zona-padre.

- Cada vez que se cambien los datos de la zona, hay que volver a firmarla, pero no será necesario generar nuevas claves. Re-firmar la zona ejecutando `dnssec-signzone` sobre la zona firmada:

```
$ sudo dnssec-signzone -o srdsi.lab. -f db.srdsi.lab.signed.new
    db.srdsi.lab.signed
$ sudo mv db.srdsi.lab.signed db.srdsi.lab.signed.bak
$ sudo mv db.srdsi.lab.signed.new db.srdsi.lab.signed
$ sudo rndc reload srdsi.lab
```

Ref.: https://bind9.readthedocs.io/en/stable/chapter5.html

6. Ejercicio: Delegación segura

- Crear subzona delegada (o zona hija) en vuestro dominio, por ejemplo *sub.srdsi.lab*[3]

  Nota: esta subzona puede estar definida en otro servidor (p.e. en el secundario) o como otra zona gestionada por el propio servidor `dns1.srdsi.lab`

- Firmar la subzona.
- Guardar los registros para la subzona en la base de datos de la zona padre (NS, A y DS). Re-firmar zona padre.
- Probar con/sin DNSSEC (si queremos validar la respuesta (flag ad), debemos realizar las pruebas desde un servidor no autorizado para el dominio).

6.1. Crear subzona delegada

- Configurar la nueva zona.
- Añadir en la zona padre los registros relativos a la subzona delegada.

  `sub IN NS` *`dns1.srdsi.lab.`*

  `sub IN A` *`172.16.0.136`*

- Crear el fichero de la zona. Por ejemplo:

```
$TTL 2h
@ IN SOA dns1.srdsi.lab. admin.srdsi.lab. (
        20140407 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
sub.srdsi.lab. IN NS dns1.srdsi.lab.
;
host1 IN A 172.16.145.45
host2 IN A 172.16.145.46
```

- Testar y recargar la configuración
- Pruebas con el *resolver*

[3] Utilizad el nombre del grupo como base para el nombre del dominio

6.2. Firmar subzona

- Generar claves para la subzona
- Añadir claves al fichero de subzona
- Firmar la subzona
- [Habilitar `dnssec` en `named.conf.options`]
- Actualizar la declaración de la subzona
- Comprobar y recargar configuración
- Testar con/sin verificación `dnssec`

6.3. Agregar DS-RR de la subzona a la DB de la zona padre.

- "Remitir de forma segura" el registro DS de la subzona al servidor padre.
- Añadir el registro DS a la DB de la zona padre.
- Re-firmar la zona padre y reiniciar servidor
- Testar

7. Ejercicio: `NSEC3`

Firmar la zona de resolución inversa. En la base de datos firmada deberán aparecer los registros relativos a la verificación de respuesta negativa válida, `NSEC3` y `NSEC3PARAM`.

Testar funcionamiento.

Documentación a entregar

Resolución de los ejercicios propuestos, documentados con ejemplos de configuración, pruebas realizadas, y análisis de los resultados obtenidos. Indicar tiempo requerido para su realización.

Ref.: https://bind9.readthedocs.io/en/latest/chapter6.html