

Universidad del País Vasco

FACULTAD DE INFORMÁTICA

**SEGURIDAD, RENDIMIENTO Y
DISPONIBILIDAD DE SERVICIOS E
INFRAESTRUCTURAS**

Ejercicios DNS

Autores:
Gorka Álvarez
Jon Gámiz
Asier Zubia

Donostia, a 18 de Abril de 2021

Índice

1. Descripción de la práctica	2
2. Desarrollo de la práctica	2
2.1. Delegación Segura	2
2.1.1. Creación de la subzona delegada	2
2.1.2. Firma de la subzona	3
2.1.3. DS-RR	7
2.2. NSEC3	8

Comandos de Bash

1. Comandos de generación de claves de la subzona	3
2. Comando para firmar la subzona	4
3. Comandos de generación aleatoria de claves	8

Índice de figuras

1. Contenido de la nueva zona <i>grupotr3s.srdsi.lab</i>	2
2. Actualización de los registros de la zona padre	2
3. Contenido del nuevo fichero <i>db.grupotr3s.srdsi.lab</i>	3
4. Generación de claves de la subzona <i>grupotr3s.srdsi.lab</i>	3
5. Actualización del fichero de la subzona	4
6. Actualización del fichero <i>named.conf.local</i>	4
7. Actualización del fichero <i>named.conf.options</i>	5
8. Captura de Wireshark de la transferencia de la nueva zona	6
9. Contenido del fichero <i>syslog</i>	6
10. Registro DS para la zona <i>srdsi.lab</i>	7
11. Registro DS utilizando el <i>resolver</i>	7
12. Error al ejecutar el comando <i>loadkeys</i>	8
13. Linea relativa al comando en <i>syslog</i>	8
14. Resultado en <i>syslog</i> tras ejecutar el comando	8
15. Resultado en consola tras ejecutar el comando	8

1. Descripción de la práctica

Durante esta práctica se trabajarán los conceptos trabajados en clase sobre la seguridad en los servidores DNS¹. Un DNS es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP². El tiempo estimado dedicado a la realización total de la práctica ha sido de **5 horas** aproximadamente.

2. Desarrollo de la práctica

En esta sección se describirán cada uno de los apartados del laboratorio así como la resolución de cada uno de ellos. Cabe destacar que previamente a la realización de los ejercicios se ha realizado la configuración de dos servidores DNS, uno primario y otro secundario, utilizando DNSSEC para firmar las zonas.

El objetivo principal de la práctica será crear una subzona delegada en el dominio *srdsi.lab*, firmarla y comprobar su correcto funcionamiento. Así mismo, se pide firmar y comprobar el correcto funcionamiento de la zona de resolución inversa.

2.1. Delegación Segura

Durante los próximos apartados se realizará la creación y configuración de una subzona delegada de nuestro dominio. La subzona que se creará será *grupotr3s.srdsi.lab* y estará gestionada por el servidor *dns1.srdsi.lab*. Así mismo, se realizará la configuración necesaria para que se pueda utilizar DNSSEC con esta nueva subzona.

2.1.1. Creación de la subzona delegada

El primer paso a realizar para poder crear nuestra nueva zona será agregarla al fichero de zonas de nuestro servidor, es decir, al fichero *named.conf.local*. El contenido a añadir será el siguiente.

```
zone "grupotr3s.srdsi.lab" IN {
    type master;
    file "/etc/bind/db.grupotr3s.srdsi.lab";
    allow-update{none;};
};
```

Figura 1: Contenido de la nueva zona *grupotr3s.srdsi.lab*

A continuación, se deberán añadir en la zona padre los registros relativos a la subzona delegada. Para ello, se añadirán las siguientes líneas en el fichero *db.srdsi.lab*.

```
user1@dns1:/etc/bind$ cat db.srdsi.lab
$ORIGIN srdsi.lab.
$TTL 2h
@   IN      SOA   dns1.srdsi.lab. admin.srdsi.lab (
    20140408          ; Serial
    604800            ; Refresh
    86400             ; Retry
    2419200           ; Expire
    604800            ; Negative Cache TTL
;
srdsi.lab.   IN      NS      dns1.srdsi.lab.
              IN      NS      dns2.srdsi.lab.
grupotr3s  IN      NS      dns1.srdsi.lab.
grupotr3s  IN      A       192.168.118.137
dns2        IN      A       192.168.118.139
;
dns1        IN      A       192.168.118.137
host1       IN      A       192.168.118.138
www         IN      CNAME  host1
$INCLUDE Ksrdsi.lab.+005+55903.key
$INCLUDE Ksrdsi.lab.+005+36945.key
user1@dns1:/etc/bind$
```

Figura 2: Actualización de los registros de la zona padre

¹Domain Name System

²Internet Protocol

Cabe destacar que la dirección IP que se utiliza (192.168.118.137) se corresponde con la dirección del servidor *dns1*, que en este caso es la misma maquina. Tras ello, firmaremos de nuevo el fichero de la zona padre para posteriormente realizar las pruebas. `sudo dnssec-signzone -N INCREMENT -t -o srdsi.lab. db.srdsi.lab`

Si nos fijamos en la figura 1, el *file* al que se hace referencia, es decir, el fichero de la subzona, no esta creado, por lo que se creara un nuevo fichero con el siguiente contenido.

```
user1@dns1:/etc/bind$ cat db.grupotr3s.srdsi.lab
$TTL 2h
@ IN SOA dns1.srdsi.lab. admin.srdsi.lab. (
    20140407
    604800
    86400
    2419200
    604800 )
;
@ IN NS dns1.srdsi.lab.
@ IN A 192.168.118.137
;
host1 IN A 192.168.118.138
host2 IN A 192.168.118.141
```

Figura 3: Contenido del nuevo fichero *db.grupotr3s.srdsi.lab*

Con esta configuración ya tendríamos lista nuestra nueva subzona. En los siguientes apartados se mostrará la configuración extra a realizar para poder utilizar esta nueva zona utilizando DNSSEC.

testar ?

2.1.2. Firma de la subzona

Ahora que ya se tiene la nueva subzona creada y correctamente configurada, se procederá a firmarla para poder utilizarla junto a DNSSEC. Por tanto, el primer paso a realizar será generar las claves KSK y ZSK de la subzona que se había creado. Para ello, ejecutaremos los siguientes comandos.

```
sudo dnssec-keygen -a RSASHA1 -b 512 -f KSK -r /dev/urandom -n ZONE grupotr3s.srdsi.lab.
sudo dnssec-keygen -a RSASHA1 -b 512 -r /dev/urandom -n ZONE grupotr3s.srdsi.lab.
```

Comando 1: Comandos de generación de claves de la subzona

```
user1@dns1:/etc/bind$ sudo dnssec-keygen -a RSASHA1 -b 512 -f KSK -r /dev/urandom -n ZONE grupotr3s.srdsi.lab.
[sudo] password for user1:
Generating key pair.....+++++Kgrupotr3s.srdsi.lab.+005+00003
user1@dns1:/etc/bind$ sudo dnssec-keygen -a RSASHA1 -b 512 -r /dev/urandom -n ZONE grupotr3s.srdsi.lab.
Generating key pair.....+++++Kgrupotr3s.srdsi.lab.+005+05670
user1@dns1:/etc/bind$
```

Figura 4: Generación de claves de la subzona *grupotr3s.srdsi.lab*

Ahora que se tienen las claves generadas han de añadirse al fichero de la subzona creado previamente (*db.grupotr3s.srdsi.lab*). Simplemente se realizaran los *INCLUDE* de las claves correspondientes al final del fichero.

```

user1@dns1:/etc/bind$ cat db.grpotr3s.srdsi.lab
$TTL 2h
@ IN SOA dns1.srdsi.lab. admin.srdsi.lab. (
    20140407
    604800
    86400
    2419200
    604800 )
;
@ IN NS dns1.srdsi.lab.
@ IN A 192.168.118.137
;
host1 IN A 192.168.118.138
host2 IN A 192.168.118.141
$INCLUDE Kgrpotr3s.srdsi.lab.+005+00003.key
$INCLUDE Kgrpotr3s.srdsi.lab.+005+05670.key
user1@dns1:/etc/bind$ 

```

Figura 5: Actualización del fichero de la subzona

El siguiente paso será firmar la subzona para que pueda ser verificada correctamente utilizando DNSSEC. Para firmar la subzona se ha utilizado el comando mostrado a continuación.

```
sudo dnssec-signzone -N INCREMENT -t -o grpotr3s.srdsi.lab. db.grpotr3s.srdsi.lab
```

Comando 2: Comando para firmar la subzona

Cabe destacar que en este comando se hace uso del parámetro “-N”, con valor *INCREMENT*. Gracias a este parámetro no tendremos que preocuparnos por el valor serial de nuestro fichero de zona, ya que incrementará automáticamente el valor del serial. De manera que si en el fichero original el valor del serial era “1000”, en el fichero firmado será “1001”, pero en el original se mantendrá igual.

Con el fichero de zona firmado, lo único que queda es asegurarse de que los ficheros *named.conf.local* y *named.conf.options* están correctamente actualizados y listos para utilizar DNSSEC.

```

user1@dns1:/etc/bind$ cat named.conf.local
// 
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "srdsi.lab" {
    type master;
    file "/etc/bind/db.srdsi.lab.signed";
    also-notify {192.168.118.139;};
    allow-transfer {127.0.0.1;};
};

zone "118.168.192.in-addr.arpa"{
    type master;
    file "/etc/bind/db.118.168.192";
    allow-transfer {192.168.118.139;};
    also-notify {192.168.118.139;};
};

zone "grpotr3s.srdsi.lab" IN {
    type master;
    file "/etc/bind/db.grpotr3s.srdsi.lab.signed";
    allow-update{none;};
};

user1@dns1:/etc/bind$ 

```

Figura 6: Actualización del fichero *named.conf.local*

```

user1@dns1:/etc/bind$ cat named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //========================================================================
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //================================================================

    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside auto;

    listen-on-v6 { any; };

};

user1@dns1:/etc/bind$ █

```

Figura 7: Actualización del fichero *named.conf.options*

Para probar que nuestra configuración es correcta se utilizará el *resolver* para comprobar las transferencias de zona. Para ello, se ejecutará el comando `dig @localhost +dnssec +multiline`. Siendo la respuesta obtenida la siguiente.

```

; <>> DiG 9.11.5-P4-5.1+deb10u3-Debian <>> @localhost grupotr3s.srdsi.lab. +dnssec
→ +multiline
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45494
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
; COOKIE: e0fb655dbe8097a11ea4d77560797ac6843de7ed1e9f21e7 (good)
;; QUESTION SECTION:
;grupotr3s.srdsi.lab.      IN A

;; ANSWER SECTION:
grupotr3s.srdsi.lab.      7200 IN      A 192.168.118.137
grupotr3s.srdsi.lab.      7200 IN      RRSIG A 5 3 7200 (
                           20210516091621 20210416091621 5670 grupotr3s.srdsi.lab.
                           1c4fNPSy9vr9dJb874100vUyNvrQsjmTlpGHnq1iY9Gn
                           9pVONzqmn693kj3hxARbzonZM3PjC9DfYqXv1Z0tkw== )

;; AUTHORITY SECTION:
grupotr3s.srdsi.lab.      7200 IN      NS dns1.srdsi.lab.
grupotr3s.srdsi.lab.      7200 IN      RRSIG NS 5 3 7200 (
                           20210516091621 20210416091621 5670 grupotr3s.srdsi.lab.
                           i9BaHV5KPWYqGc+022hCsHWk9eljRfv6ccTx13vuzm/n
                           fTOHyw+W4n2oUJesy20wNdM8byCefuuKms4o68LZyA== )

;; ADDITIONAL SECTION:
dns1.srdsi.lab.           7200 IN      A 192.168.118.137

```

```

dns1.srdsi.lab.          7200 IN      RRSIG A 5 3 7200 (
20210516103440 20210416103440 36945 srdsi.lab.
V1+a9g0NYVowCFPZGc3zDsXFIQrZ/IPt32yGkd9T1IgW
ZH2En/rScM13x/1z41GdCuGp91d/citt5V3s4scd3w== )

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: vie abr 16 13:53:42 CEST 2021
;; MSG SIZE rcvd: 462

```

Como se puede observar al comienzo de la respuesta obtenida, el estado esta ha sido *NOERROR*. Tras capturar la transferencia utilizando Wireshark, la captura obtenida es la siguiente.

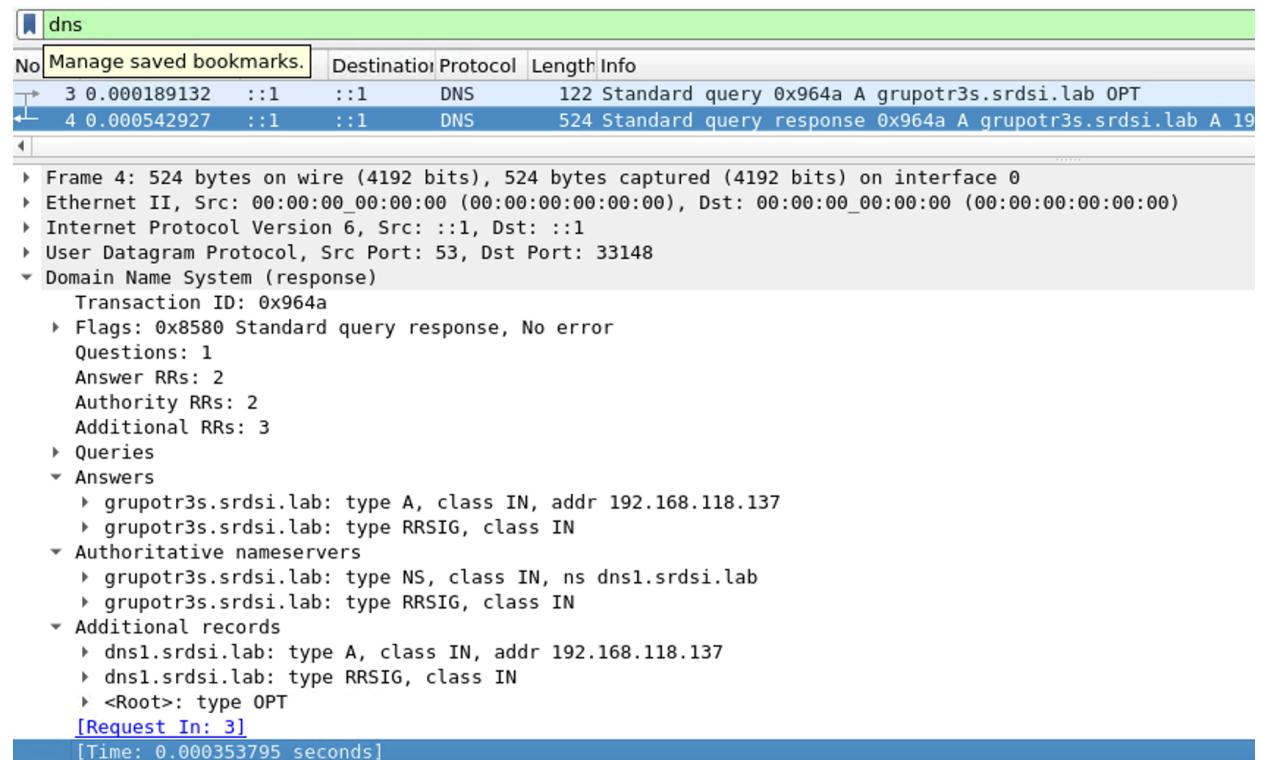


Figura 8: Captura de Wireshark de la transferencia de la nueva zona

Así mismo, si se quiere asegurar que efectivamente la transferencia de zona se ha hecho utilizando DNSSEC, se puede comprobar el contenido del fichero */var/log/syslog*. Buscando la linea correspondiente del *log* se encontrará lo siguiente.

```

Apr 16 12:18:03 dns1 named[10774]: zone srdsi.lab/IN: loaded serial 20140408 (DNSSEC signed)
Apr 16 12:18:03 dns1 named[10774]: zone grupotr3s.srdsi.lab/IN: sig-re-signing-interval less than 3 * refresh.
Apr 16 12:18:03 dns1 named[10774]: zone grupotr3s.srdsi.lab/IN: loaded serial 20140408 (DNSSEC signed)
Apr 16 12:18:03 dns1 named[10774]: zone localhost/IN: loaded serial 2
Apr 16 12:18:03 dns1 named[10774]: all zones loaded

```

Figura 9: Contenido del fichero *syslog*

2.1.3. DS-RR

Al realizar la firma de las zonas de forma manual, el registro DS se genera automáticamente. Para la zona `srdsi.lab` el fichero que se genera es `dsset-srdsi.lab.`, cuyo contenido es el siguiente.

```
user1@dns1:/etc/bind$ cat dsset-srdsi.lab.
srdsi.lab.           IN DS 55903 5 1 1107FA4E3A892B3CC1D108899287F2D1B198BFB0
srdsi.lab.           IN DS 55903 5 2 24CE196835C054F28EBA70CC92F18B5563CDD5E136A0C1BC0F73D6C1 FAB3B6A0
user1@dns1:/etc/bind$
```

Figura 10: Registro DS para la zona `srdsi.lab`

No obstante, este registro también se puede obtener utilizando el comando `dig @localhost dnskey srdsi.lab.`, cuyo resultado es el siguiente.

```
user1@dns1:/etc/bind$ dig @localhost dnskey srdsi.lab

; <>> DiG 9.11.5-P4-5.1+deb10u3-Debian <>> @localhost dnskey srdsi.lab
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44906
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: f838713f62c750e3e4bf35026079ab96c762825ab1cf2b55 (good)
;; QUESTION SECTION:
;srdsi.lab.          IN      DNSKEY

;; ANSWER SECTION:
srdsi.lab.        7200    IN      DNSKEY  256 3 5 AwEAAcLWci3b9NncbLwBkLT8pZogUvZeU4n6s=
srdsi.lab.        7200    IN      DNSKEY  257 3 5 AwEAAdRK3ZSz0W7FdTS35RFUudsw08pd5dhYk=>

;; Query time: 2 msec
;; SERVER: ::1#53(::1)
;; WHEN: vie abr 16 17:21:58 CEST 2021
;; MSG SIZE  rcvd: 234

user1@dns1:/etc/bind$
```

Figura 11: Registro DS utilizando el *resolver*

Y cómo lo incorporáis a la BD de la zona padre? refirmar y testar?

2.2. NSEC3

Para este último ejercicio se pide firmar la zona de resolución inversa utilizando NSEC3. El objetivo de NSEC3 es saber cuando existe un nombre dentro de una zona determinada. De esta manera se trata de evitar que tras un ataque se envíen respuestas falsas a las consultas. Para realizar la configuración se han seguido los pasos del blog publicado en <https://blog.apnic.net/2019/05/23/how-to-deploying-dnssec-with-bind-and-ubuntu-server/>.

Por tanto, siguiendo los pasos, lo primero ha realizar es generar un nuevo par de claves utilizando los comandos.

```
sudo dnssec-keygen -r /dev/urandom -a RSASHA256 -3 -b 1024 -n ZONE srdsi.lab
sudo dnssec-keygen -r /dev/urandom -f KSK -a RSASHA256 -b 2048 -3 -n ZONE srdsi.lab
```

Comando 3: Comandos de generación aleatoria de claves

Tras ello, se ha tratado de ejecutar el comando `sudo rndc loadkeys srdsi.lab`, sin embargo, al hacerlo se obtiene un error de permisos que no se ha podido solucionar. Si se comprueba el contenido del fichero `/var/log/syslog` no se muestra nada que permita solucionar el error, simplemente la linea que se muestra a continuación.

```
user1@dns1:/etc/bind$ sudo rndc loadkeys srdsi.lab
rndc: 'loadkeys' failed: permission denied
```

Figura 12: Error al ejecutar el comando *loadkeys*

```
Apr 16 16:59:56 dns1 named[11830]: received control channel command 'loadkeys srdsi.lab.'
```

Figura 13: Línea relativa al comando en *syslog*

Si a continuación se ejecuta el siguiente comando mostrado en el *blog* antes mencionado, `sudo rndc signing -nsec3param 1 0 10 auto srdsi.lab.`, obtenemos la siguiente respuesta por consola y resultado en el fichero *syslog*.

```
Apr 16 16:58:47 dns1 named[11830]: received control channel command 'signing -nsec3param 1 0 10 auto
srdsi.lab.'
Apr 16 16:58:47 dns1 named[11830]: generated salt: D9A86343CB522A6F
Apr 16 16:58:47 dns1 named[11830]: /etc/bind/db.srdsi.lab.signed.jnl: create: permission denied
Apr 16 16:58:47 dns1 named[11830]: zone srdsi.lab/IN: setnsec3param:dns_journal_open -> unexpected e
rror
Apr 16 16:58:47 dns1 kernel: [355410.918128] audit: type=1400 audit(1618585127.993:17): apparmor="DE
NIED" operation="mknod" profile="/usr/sbin/named" name="/etc/bind/db.srdsi.lab.signed.jnl" pid=11830
comm="isc-worker0003" requested_mask="c" denied_mask="c" fsuid=113 ouid=113
Apr 16 16:59:56 dns1 named[11830]: received control channel command 'loadkeys srdsi.lab.'
```

Figura 14: Resultado en *syslog* tras ejecutar el comando

```
user1@dns1:/etc/bind$ sudo rndc signing -NSEC3PARAM 1 0 10 auto srdsi.lab.
nsec3param request queued
user1@dns1:/etc/bind$
```

Figura 15: Resultado en consola tras ejecutar el comando

Como os comenté en clase bastaba con haber mirado la ayuda “man” de esos comandos para realizar este ejercicio, repitiendo los mismos pasos que en el ejercicio anterior pero incluyendo las opciones correspondientes a NSEC3