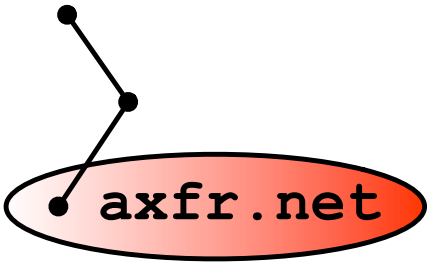


Los ejercicios de laboratorio para el Curso Especial DNSSEC*

Version v5.98 (**axfr.net**, v1.16)

Johan Ihrén
dns-training@axfr.net

19 de septiembre de 2016

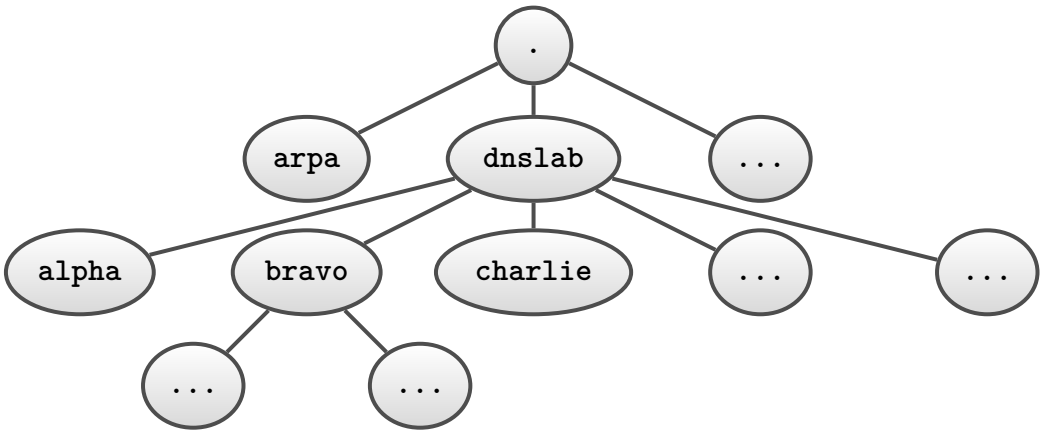
* main.tex, revision: 1.16 on 19 de septiembre de 2016 by johani

Índice

1 Los ejercicios de laboratorio

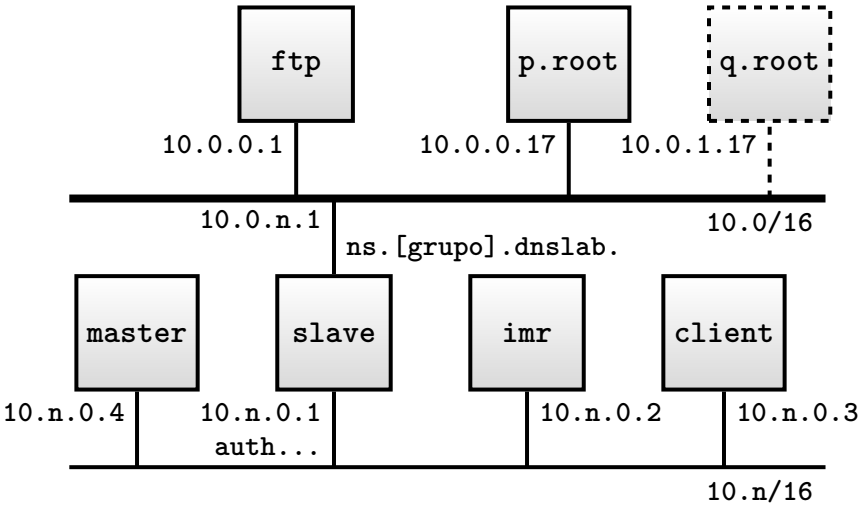
Estos ejercicios tienen por objeto dar una formación práctica en las distintas técnicas y opciones que se han cubierto en las clases. El curso se divide en distintas partes con la intención de intercalar clases teóricas y ejercicios trabajando sólo un aspecto en cada momento. Por favor consulte con un profesor antes de pasar a la siguiente parte.

Todos los ejercicios de laboratorio se llevarán a cabo en un espacio de nombres local, donde el dominio de nivel superior más importante es **dnslab** y cada grupo de laboratorio es un hijo (sudbomindio) de **dnslab**:



Los equipos del laboratorio están configurados individualmente tres cada grupo. La máquina "**slave**" está equipada con dos interfaces de red. La primera está conectada al entorno de laboratorio de base, que es compartido con otros grupos de laboratorio y también proporciona acceso a servicios como el servicio de nombres DNS raíz, **ftp**, **web**, etc. La segunda interfaz se conecta a una red privada "interna" que conecta las diferentes máquinas del grupo de laboratorio (ver dibujo).

Como **slave** tiene varias interfaces de red también tiene varias direcciones y varios nombres. El nombre de dominio para la interfaz externa será **ns.[grupo].dnslab**, mientras que el nombre de dominio de la interfaz interna será **fw.[grupo].dnslab**. **slave** será utilizado primordialmente como nombre del servidor autoritativo.



Conectado con la red "interna" hay también un segundo servidor, conocido como el **imr**. Se puede utilizar para proporcionar servicio DNS recursivo.

El siguiente servidor, llamado "**master**", será utilizado como un servidor "maestro escondido" ("hidden master"), o sea un servidor donde se guardan los datos pero que no es visible en ningún registro **NS**.

Por último, hay una máquina conocida como **cliente** conectada a la red "interna". Algunos de los ejercicios, en particular los laboratorios de DHCP y Actualización Dinámica en el Curso Avanzado, se llevarán a cabo aquí.

1.1 Plan de direccionamiento

Este es el plan de direccionamiento local (véase también el dibujo de la topología en la página anterior). La "red **10.0/16**" se utiliza para conectar los grupos individuales de laboratorio entre sí y a la infraestructura común. La red **10.n/16** es la red interna de cada grupo de laboratorio (donde **n** denota el número del grupo de laboratorio).

#	Máquina	Nombre de la zona	Prefijo IP	Dirección IP	Dirección IPv6
1	ns [slave] imr master fw [slave] client	alpha.dnslab	10.1.0.0/16	10.0.1.1 10.1.0.2 10.1.0.4 10.1.0.1 10.1.0.3	3ffe:b80:1:bb::1 3ffe:b80:1:1::2 3ffe:b80:1:1::4 3ffe:b80:1:1::1 3ffe:b80:1:1::3
2	ns [slave] imr master fw [slave] client	bravo.dnslab	10.2.0.0/16	10.0.2.1 10.2.0.2 10.2.0.4 10.2.0.1 10.2.0.3	3ffe:b80:1:bb::2 3ffe:b80:1:2::2 3ffe:b80:1:2::4 3ffe:b80:1:2::1 3ffe:b80:1:2::3
3	ns [slave] imr master fw [slave] client	charlie.dnslab	10.3.0.0/16	10.0.3.1 10.3.0.2 10.3.0.4 10.3.0.1 10.3.0.3	3ffe:b80:1:bb::3 3ffe:b80:1:3::2 3ffe:b80:1:3::4 3ffe:b80:1:3::1 3ffe:b80:1:3::3
...	...	...	...	...	...
26	ns [slave] imr master fw [slave] client	zulu.dnslab	10.26.0.0/16	10.0.26.1 10.26.0.2 10.26.0.4 10.26.0.1 10.26.0.3	3ffe:b80:1:bb::1a 3ffe:b80:1:1a::2 3ffe:b80:1:1a::4 3ffe:b80:1:1a::1 3ffe:b80:1:1a::3

El resto de los grupos de laboratorio son:

4=delta, **5=echo**, **6=foxtrot**, **7=golf**, **8=hotel**, **9=india**, **10=juliet**, **11=kilo**, **12=lima**, **13=mike**, **14=november**, **15=oscar**, **16=papa**, **17=quebec**, **18=romeo**, **19=sierra**, **20=tango**, **21=uniform**, **22=victor**, **23=whisky**, **24=x-ray**, **25=yankee**.

1.2 Estructura de directorios

La configuración de NSD, normalmente **nsd.conf**, se encuentra en **/usr/pkg/etc/nsd**. La configuración de Unbound, **unbound.conf**, se encuentra en **/usr/pkg/etc/unbound**.

Los ficheros de zona, los archivos de log y similar se pueden poner casi en cualquier lugar, pero la recomendación es mantener todo en un mismo directorio, es decir, normalmente en **/usr/pkg/etc/nsd**.

`/etc/resolv.conf` se encuentra en **`/etc`** (que es utilizado por aplicaciones externas y, por lo tanto, **debe estar siempre en `/etc`).**

Tenga en cuenta que debido a que algunos ejercicios de laboratorio se llevarán a cabo en un equipo y otros en otro distinto, habrá alguna alternancia entre las dos máquinas.

2 El entorno de prácticas

El entorno de prácticas, el Laboratorio, se divide en dos partes: las máquinas en sus mesas (que sólo se usan como pantallas, para acceder a la web y a las máquinas remotas) y un conjunto de máquinas de "laboratorio" que están alojadas en otro lugar (a las que accede de forma remota desde las máquinas en su mesa). Los ejercicios se hacen prácticamente todos en las máquinas de laboratorio, **no** en las que tiene en la mesa.

Como hemos dicho, cada grupo de laboratorio tiene que configurar varias máquinas. La máquina que va a usar para empezar se llama "**`imr.[groupname].dnslab`**" y la primera tarea es acceder a ella.

- Conéctese a la máquina que tiene delante. El nombre de usuario y la contraseña para cada una de estas máquinas se la darán en la clase.
- La **contraseña** para las máquinas de laboratorio le será facilitada por el profesor.
- Abra una nueva ventana de Terminal. La forma de hacerlo depende del tipo de máquina de la que disponga: Preguntele al profesor. Normalmente el escritorio tiene un icono para el terminal o la opción está en un menú.
- En la ventana de Terminal, conéctese a la máquina **`imr.[group].dnslab`** con el comando **`ssh`**. Necesitará usar el *puerto* especial reservardo para su grupo. El servidor proxy que va a utilizar para el acceso remoto es (normalmente) **`lacnic-proxy.axfr.net`** y el *número de puerto* para el **`imr`** es $7000 + n$ donde n es el número de su grupo. Veamos un ejemplo para el grupo **5**, o sea el grupo **`echo`**, con el puerto $7000 + 5 = 7005$:

```
desktop-machine# ssh -X root@lacnic-proxy.axfr.net -p 7005
...
desktop-machine# ssh -X root@lacnic-proxy.axfr.net -p 7005
...
Welcome to the AXFR.NET lab and training environment
imr.echo.dnslab#
```

números de puerto:	
master	5000+n
slave	6000+n
imr	7000+n

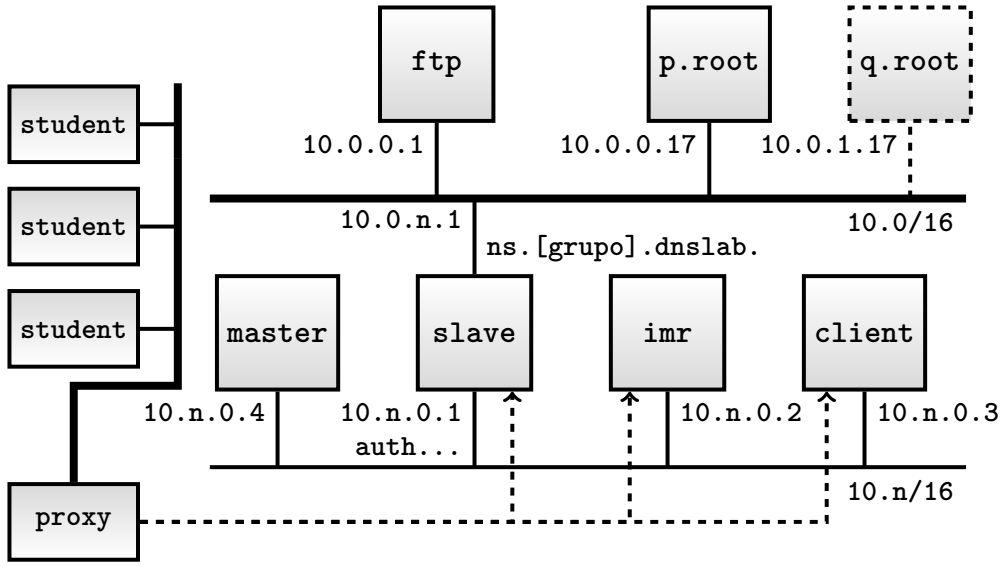
  - Utilice la contraseña suministrada por el profesor.
  - El argumento "**-X**" (X mayúscula) en el **ssh** ayuda a tener autenticatión para X11 sobre las conexiones remotas y es necesario para poder ejecutar aplicaciones X en la máquina remota y ver sus ventanas en la máquina que tiene delante de si.
  - El argumento "**-p**" se usa para indicar a que puerto conectarse.

- Una vez conectado a la máquina de laboratorio **imr**, abra un editor de textos. Si su preferencia es **emacs**, teclee "**emacs &**". Si prefiere **vi**, "**vim**" o "**gvim**", teclee "**vi**". Si está disponible el sistema de ventanas X11 entonces la version de **emacs** llamada "**xemacs**" y la versión de **vim** llamada "**gvim**" tienen la ventaja de que abran sus ventanas en el escritorio local. Aunque esto está bien, no es una función crucial. Por ejemplo:

  ```
  imr.echo.dnslab# emacs &
  ```

  Si no tiene ninguna preferencia, le recomendamos que pruebe la versión con ventanas de **emacs** o los editores más sencillos como "**joe**". Evite "**vi**" a no ser que ya lo conozca...

Vea el diagrama para obtener más detalles de la topología de red y el direccionamiento.



2.1 Buscando las herramientos web y la documentación

Hay varias herramientas Web que vamos a utilizar durante el curso. Entre ellas se encuentra un "evaluador del estado" de su laboratiorio y un servicio de correo web. A estos se accede a través de un **proxy web**.

Además de las herramientas, le puede resultar útil leer la documentación que viene con cada servidor de nombres. Está disponible en varios formatos, y el que aquí adjuntamos via Web está en mismo sitio que las herramientas.

2.1.1 Configurando el navegador para usar el proxy

Una vez que el navegador (en la máquina que tiene delante de si) ha arrancado debe configurarlo para usar un proxy en la **misma dirección usada para el acceso remoto**, o sea normalmente "`lacnic-proxy.axfr.net`", y el puerto `4128` (el proxy también acepta conexiones en los puertos `3128` y `4129` que pueden ser usados si es necesario, pregúntele a uno de los profesores si tiene problemas.)

A través del proxy debería ser posible acceder a una página web usando el nombre o la dirección IP incluso antes de que haya configurado su propio servidor DNS recursivo.

`http://10.0.0.1/` *o* `http://www.dnslab/`

Lamentablemente se ha hecho necesario proteger a este proxy con una contraseña. El nombre de usuario es **"axfr"** y la contraseña es **"net"**.

3 Instalacíon

Debido a que todas las implementaciones de servidores de nombres que utilizamos son código abierto es posible compilarlas desde el código fuente antes de la instalación. Hoy en día, sin embargo, lo más frecuente es instalar un paquete binario con la ayuda de un "administrador de paquetes". En NetBSD este sistema se llama "**pkg**" y el comando para la instalación de paquetes se llama "**pkg_add**".

Como existen varios servidores de nombres, tanto autoritativos como recursivos, en varias máquinas, hay que instalar el servidor de nombres adecuado en cada máquina. Instalar un servidor recursivo en "imr" y uno o más servidores autoritativos en los servidores "slave" y "master"

3.1 Instrucciones de instalación para Unbound

Instale la versión más reciente del paquete binario de **unbound** en el servidor recursivo. No se preocuper por los mensajes de aviso.

```
imr.echo.dnslab:/root# pkg_add unbound
unbound-1.5.7: Creating group "unbound"
unbound-1.5.7: Creating user "unbound"
useradd: Warning: home directory ‘/nonexistent’ doesn’t exist,
and -m was not specified
unbound-1.5.7: copying /usr/pkg/share/examples/unbound/unbound.conf
to /usr/pkg/etc/unbound/unbound.conf
=====================================================================
The following files should be created for unbound-1.5.7:
    /etc/rc.d/unbound (m=0755)
        [/usr/pkg/share/examples/rc.d/unbound]
=====================================================================
```

3.1.1 Configure la autenticación de "unbound-control"

Para poder usar la utilidad de control de Unbound, **unbound-control**, es necesario crear un certificado que **unbound-control** usará para autenticarse a si mismo con Unbound. El certificado se crea fácilmente con el comando:

```
imr.whisky.dnslab# unbound-control-setup
```

La instalación de Unbound está completa.

3.2 Instrucciones de instalación para NSD

Instale la versión más reciente del paquete binario de NSD4 en las máquinas autoritativas que desee. No se preocupero por los mensajes de aviso

```
ns.echo.dnslab:/root# pkg_add nsd
nsd-4.1.9: Creating group "nsd"
nsd-4.1.9: Creating user "nsd"
useradd: Warning: home directory ‘/nonexistent’ doesn’t exist,
and -m was not specified
nsd-4.1.9: copying /usr/pkg/share/examples/nsd/nsd.conf to
/usr/pkg/etc/nsd/nsd.conf
==========================================================
The following files should be created for nsd-4.1.9:
    /etc/rc.d/nsd (m=0755)
        [/usr/pkg/share/examples/rc.d/nsd]
==========================================================
```

3.2.1 Configure la auteticación para "nsd-control"

Para poder usar la utilidad de control de NSD4, **nsd-control**, es necesario crear un certificado que **nsd-control** usará para autenticarse a si mismo con NSD4. El certificado se crea fácilmente con el comando:

```
ns.whisky.dnslab# nsd-control-setup
```

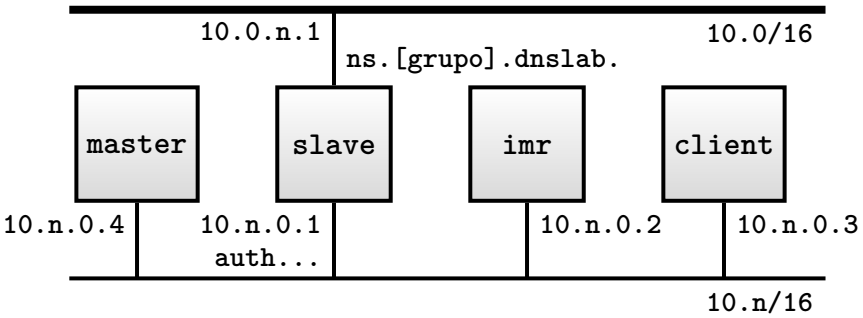
La instalación de NSD4 está ahora completa

4 Configuración de un Servidor Recursivo

Nota: Este ejercicio de laboratorio entero se llevará a cabo en la máquina **IMR**. Sólo debe usar una implementación de servidor recursivo por lo que será necesario elegir que parte de las instrucciones seguir.

- Asegurese de que el software para el servidor recursivo que desea está instalando (con "**pkg_add**"). (Vea la sección 3 si hace falta.)

Antes de continuar es necesario que tenga funcionando un llamado **resolver iterativo**, también llamado **servidor de nombres recursivo**. Para esto le hará falta un fichero **root.hints** con información sobre los servidores raíz (root).



4.1 root.hints

Encontrará um fichero **root.hints** que funciona en el directorio de configuración del servidor de nombres.

4.2 Unbound configuración: unbound.conf

El fichero principal de configuración se llama **unbound.conf** y deberia estar en el directorio **/usr/pkg/etc/unbound**.

```
imr.whisky.dnslab# cd /usr/pkg/etc/unbound
```

Deberá editar el fichero **/usr/pkg/etc/unbound/unbound.conf** (creelo si es necesario). Configure Unbound para que use el fichero **root.hints** para encontrar

los servidores de nombres de raiz. Además hay algunos detalles importantes más a tener en cuenta:

- Añade atributos **interface:** para las direcciones (IPv4 e IPv6) en las que el servidor recursivo debe escuchar. No se olvide de las direcciones **localhost**.
- Por defecto Unbound sólo responde a preguntas de **localhost**. Relaje el control de acceso (con el atributo **access-control:**) para que responda a preguntas de los clientes en las redes **10.0.0.0/8** y **3ffe:b80:1::/48**.
- Para poder utilizar la herramienta **unbound-control** recuerde añadir también un atributo "**remote-control:**" a la configuración.

La configuración resultante deberia estar estructurada de forma similar a la plantilla siguiente

```
server:
    directory:       /usr/pkg/etc/unbound
    username:        unbound
    interface:       ... # global addr v4 + v6
    interface:       ... # localhost v4 + v6
    access-control: 10.0.0.0/8 allow     access-control:
3ffe:b80:1::/48 allow
    root-hints: root.hints

remote-control:
    control-enable: yes
```

Cuando esto esté hecho arranque el servidor de nombres con el comando:

```
imr.whisky.dnslab# unbound-control start
```

4.3 Configuración del Stub Resolver

Hace falta un último paso para que las aplicaciones empiecen a usar el servidor reursivo que hemos configurado. Hay que indicarlo en la configuración del resolver local, que está en el fichero

/etc/resolv.conf

- Edite el fichero **/etc/resolv.conf** en **imr** para que haga referencia al servidor recursivo de la máquina local
- Edite también el fichero **/etc/resolv.conf** en **master** y **slave**. ¿Qué dirección IP debe usar?

Cuando haya acabado debe comprobar que todo funciona como debe haciendo preguntas sobre algo que exista en el espacio de nombre disponible en el entorno de laboratorio. Por ejemplo preguntando por la dirección IPv6 de la máquina

ftp.dnslab

deberia darle una respuesta válida. Intente también preguntar por algo que **no** existe, como el registro **MX** para

blahongasprongaj.grungelgroubledork.humbolkargatom.com

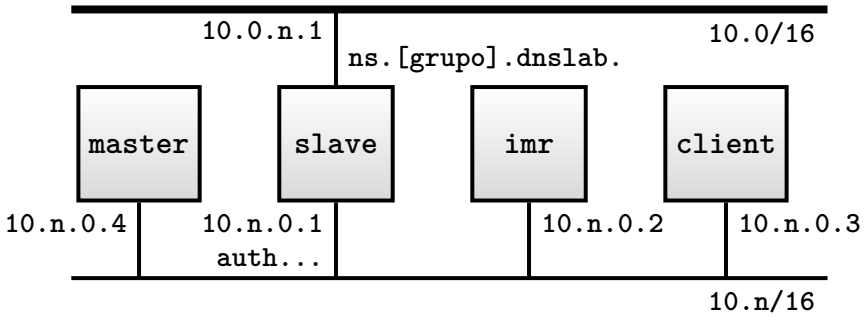
por lo que sabemos este nombre de dominio no debería existir en el espacio de nombres.

5 Configuración de un servidor Autoriativo

Nota: este ejercicio de laboratorio involucra tanto al servidor **maestro** como al **esclavo**.

Lo que queremos es que el servidor **maestro** se configure como un llamado "maestro oculto", o sea que debe ser autoritativo y tener el fichero de zona, pero no ser visible en ningún registro **NS**. En su lugar, la máquina **esclava** debe de ser el servidor autoritativo visible, para el que si existe un registro **NS**. El **esclavo no debe** de tener el fichero de zona de forma que se pueda editar sino recibirlo por transferencia de zona desde el **maestro**.

Vea a continuación la descripción de su topologia local e su plan de direccionamiento (el mismo dibujo que antes).



Ha llegado el momento de configurar los servidores autoritativos, o sea **maestro** y **esclavo**, para que sean autoritativos para la zona "directa" de la que es usted responsable. La tabla con nombres de zona y prefijos de red la repetimos a continuación (la misma información que en 1.1).

#	Máquina	Nombre de la zona	Prefijo IP	Dirección IP	Dirección IPv6
1	ns [slave] imr master fw [slave] client	alpha.dnslab	10.1.0.0/16	10.0.1.1 10.1.0.2 10.1.0.4 10.1.0.1 10.1.0.3	3ffe:b80:1:bb::1 3ffe:b80:1:1::2 3ffe:b80:1:1::4 3ffe:b80:1:1::1 3ffe:b80:1:1::3
2	ns [slave] imr master fw [slave] client	bravo.dnslab	10.2.0.0/16	10.0.2.1 10.2.0.2 10.2.0.4 10.2.0.1 10.2.0.3	3ffe:b80:1:bb::2 3ffe:b80:1:2::2 3ffe:b80:1:2::4 3ffe:b80:1:2::1 3ffe:b80:1:2::3
3	ns [slave] imr master fw [slave] client	charlie.dnslab	10.3.0.0/16	10.0.3.1 10.3.0.2 10.3.0.4 10.3.0.1 10.3.0.3	3ffe:b80:1:bb::3 3ffe:b80:1:3::2 3ffe:b80:1:3::4 3ffe:b80:1:3::1 3ffe:b80:1:3::3
...	...	...	...	...	...
26	ns [slave] imr master fw [slave] client	zulu.dnslab	10.26.0.0/16	10.0.26.1 10.26.0.2 10.26.0.4 10.26.0.1 10.26.0.3	3ffe:b80:1:bb::1a 3ffe:b80:1:1a::2 3ffe:b80:1:1a::4 3ffe:b80:1:1a::1 3ffe:b80:1:1a::3

Empieze por conectarse a su servidor **maestro** usando **ssh** desde una ventana de

terminal. Para conectarse al **maestro** tiene que usar el puerto $5000+n$. Por ejemplo, para el grupo número **3**, "**charlie**", el número de puerto es $5000 + 3 = 5003$. La contraseña es la misma que para el servidor **imr**.

```
desktop-machine# ssh -X root@lacnic-proxy.axfr.net-p 5003
...
Welcome to the AXFR.NET lab and training environment
master.charlie.dnslab#
```

números de puerto:	
master	$5000 + n$
slave	$6000 + n$
imr	$7000 + n$

5.1 Preparación del Maestro Oculto

- Asegurese de que el paquete (pkg) de software para el servidor autoritativo que desea está instalando (con "**pkg_add**"). (Vea la sección 3 si hace falta.)
- Modifique la configuración en **/etc/resolv.conf** (si existe) para que apunte a su propio **imr** como servidor recursivo. ¿Cuál es la dirección de **imr**?

5.2 Contenido de la zona

En este curso, los ficheros de zona para las tres zonas para las que será autoritativo ya han sido creados. Uno para la "zona directa" "**[nombredegrupo].dnslab**" y dos para las "zonas inversas", una para IPv4 y otra para IPv6. Los ficheros de zona tienen nombres correspondientes a sus respectivas zonas y se encuentran en el directorio config del servidor de nombres.

Si usa NSD los ficheros de zona estarán en:

master:/usr/pkg/etc/nsd/

Antes de arrancar el servidor autoritativo debe verificar el contenido de estos ficheros de zona.

5.3 Configuración del servidor Maestro

5.3.1 Configuracíon principal de NSD

Cree y edite el fichero de configuración principal de NSD

master:/usr/pkg/etc/nsd/nsd.conf

- Necesitará un atributo **server:** en la configuración global. Asegurese de que el atributo **server:** tiene sub-atributos "**ip-address:**" configurados para escuchar en las direcciones IPv4 e IPv6.
- NSD será un servidor maestro para la zona **whisky.dnslab**. Para hacer esto hay que añadir un atributo **zone:** que contenga al menos los sub-atributos **name:**. **zonefile:**, **provide-xfr:** y **notify:**.

Por lo general es buena idea verificar que el fichero es sintácticamente correcto antes de arrancar (o rearrancar) el servidor de nombres. Cuando el fichero **nsd.conf** esté completo deberia reconstruir la base de datos del espacio de nombres y después arrancar NSD:

```
master.whisky# nsd-checkconf nsd.conf
master.whisky# nsd-control start
```

5.4 Comprobación de mensajes de error

Use **dig** o **host** para verificar que su servidor autoritativo está respondiendo correctamente. Vea los ejemplos a continuación.

```
ns.whisky# dig @10.23.0.4 whisky.dnslab soa

; «» DiG 9.6.0 «» whisky.dnslab soa
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13567
;; flags: qr aa rd; QUERY: 1, ANS: 1, AUTH: 1, ADD'L: 2

;; QUESTION SECTION:
;whisky.dnslab. IN SOA

;; ANSWER SECTION:
whisky.dnslab.    3600 IN SOA ns.whisky.dnslab.
            hm.whisky.dnslab. 2016032301 7200 1800 604800 600
```

```
;; AUTHORITY SECTION:
whisky.dnslab.    3600 IN NS ns.whisky.dnslab.

;; ADDITIONAL SECTION:
ns.whisky.dnslab. 3600 IN A 10.0.23.1

;; Query time: 11 msec
;; SERVER: 10.23.0.4#53(master.whisky.dnslab)
;; WHEN: Sun Apr 12 13:09:29 2016
;; MSG SIZE rcvd: 182
```

5.5 Añada a su servidor autoritativo público a la zona

Empiece por conectarse a su máquina **slave** con **ssh** desde una ventana de terminal. El puerto a usar para **slave** es el $6000 + n$. Como ejemplo, para el grupo **3**, "**charlie**", el número de puerto es $6000 + 3 = 6003$. La contraseña es la misma que para **imr**.

```
desktop-machine# ssh -X root@lacnic-proxy.axfr.net-p 6003
...
Welcome to the AXFR.NET lab and training environment
ns.charlie.dnslab#
```

5.5.1 Preparando el Servidor Autoritativo

- Asegurese de que el paquete (pkg) de software para el servidor autoritativo que desea está instalando (con "**pkg_add**"). (Vea la sección 3 si hace falta.)
- Modifique la configuración en **/etc/resolv.conf** (si existe) para que use su propio **imr** como servidor recursivo. ¿Cuál es la dirección del **imr**?

5.5.2 Configuración de NSD como esclavo

Cree y edite el fichero de configuración principal de NSD

slave:/usr/pkg/etc/nsd/nsd.conf

- Necesitará un atributo **server:** en los ajustes globales. Asegurese de que el atributo **server:** tiene sub-atributos "**ip-address:**" que configuren la escucha en las direcciones IPv4 e IPv6 (tanto de las interfaces internas como externas) del servidor autoritativo.
- NSD será un servidor esclavo para la zona **whisky.dnslab**. Para que esto sea así tendrá que añadir un atributo **zone:**.

```
server:
    ip-address: 3ffe:b80:1:bb::17
    ...

zone:
    name:          whisky.dnslab
    zonefile:      ...
    request-xfr:   [address of master] NOKEY
    allow-notify:  [address of master] NOKEY
```

Por lo general es buena idea verificar que el fichero es sintácticamente correcto antes de arrancar (o rearrancar) el servidor de nombres. Cuando el fichero **nsd.conf** esté completo deberia arrancar NSD:

```
ns.whisky# nsd-checkconf nsd.conf
ns.whisky# nsd-control start
```

5.5.3 Compruebe que funciona la transferencia de zona

Compruebe, usando **dig**, que la máquina **slave** ha conseguido transferir la zona del **maestro**. ¿Cómo hacer esto? Compruebe también que si lleva a cabo una modificación del contenido de la zona en el **maestro** y **recarga** la zona el cambio se propaga hasta el servidor **slave**.

5.6 Solicitar una delegación del padre

Tiene ahora servicio DNS autoritativo en su propio servidor pero nadie más que usted lo sabe. Ha llegado el momento de solicitar una delegación a la zona padre.

Averigüe el nombre de su zona padre y el la dirección de correo electrónico del administrador. Escriba una solicitud (dirigida al administrador de la zona padre) para que le sea delegada la zona a su servidor.

Le sugerimos que use el sistema de webmail del laboratorio para esto. Su nombre de usuario de webmail es el mismo que su nombre de grupo y la contraseña es la misma que para conectarse a los servidores
De forma alternativa, es posible utilizar un trozo de papel dirigido al adminsitrador de la zona padre.

La solicitud **debe** contener los **registros DNS exactos** que sean necesarios. No se puede hacer demasiado hicapié en lo importante que es esto : el contenido debe incluir los **registros DNS exactos**.

La delegación no habrá tenido lugar hasta que no haya recibido contestación de la zona padre.

Cuando la haya recibido debe comprobar que la referencia funciona "desde arriba". La mejor manera de comprobarlo es preguntarle sobre su zona al servidor recursivo de otro grupo de laboratorio. Hacerlo es fácil con el comando **`dig`** (en el ejemplo usamos **`10.8.0.2`**, o sea **`imr.hotel.dnslab`**, para examinar el servidor autoritativo desde "fuera"):

```
ns.whisky# dig @10.8.0.2 client.whisky.dnslab a
```

5.7 Comprobar que las preguntas de DNS en la zona funcionan

Cuando la delegación se haya completado debe verificar que funciona. Debe comprobarlo examinando registros en la zona y comprobando que las aplicaciones pueden acceder a los registros (a través de su *stub resolver*).

- Compruebe que es posible extraer registros de la zona desde el servidor recursivo.
- Compruebelo con alguna aplicación que sea capaz de utilizar transporte IPv6, por ejemplo:
  - **`ping6 ns.whisky.dnslab`**
  - **`ssh -6 imr.whisky.dnslab`**

5.8 Añadir un Servidor Autoritativo Externo a su zona

Llegados a este punto tiene servicio de DNS funcional para sus zonas pero no redundancia. Es el momento de añadir un servidor esclavo externo. Para esto necesitará la ayuda de otro grupo. Hay varios pasos para la configuración y **hay que hacerlo en el orden correcto**:

- Pongase de acuerdo con alguién para que le dé servicio de esclavo para su zona. ¿Desde qué dirección IP deben transferir su zona?
- Compruebe que el otro servidor de nombres ha tenido éxito transfiriendo la zona y que está dando respuestas autoritativas.
- Cree un registro `NS` adicional para el nuevo servidor.
- Solicite una actualización de la información de delegación en la zona padre.

Ahora tiene varios servidores disponibles en su zona, pero el mundo sigue usando sólo el incial. Debe pedir una actualización de la delegación desde la zona padre. Piense que cambios serán necesarios, actualice el pedido de delegación (o escriba uno nuevo) y envíelo al administrador de la zona padre. No se olvide de esperar la respuesta.

Si alguién le pide que le dé servicio de esclavo para una o más de sus zonas tendrá que añadir las necesarias directivas de zona en el fichero el fichero de configuración del servidor de nombres autoritativo (`nsd.conf`).

Una vez hecho esto, recargue la configuración del servidor.

Es fácil comprobar si todo está correcto buscando el fichero de zona que ha especificado en la configuración y comprobando que el contenido es una copia del fichero de zona del servidor maestro. Puede que el formato del fichero sea algo diferente ya que se reformatea durante la transferencia de zona para ser todo lo compacto que se pueda, pero la esencia del contenido debe ser la misma.

Cuando su servidor esté funcionando como debe ser, debe comunicárselo al dueño de la zona o sea a quien le pidió que fuera esclavo para la zona. Entonces ellos podrán solicitar una actualización de la delegación a la zona padre para que su servidor esclavo sea incluido en las referencias futuras desde el padre.

6 DNSSEC

Este ejercicio es bastante complejo. El objetivo es que la zona publicada por el servidor "**slave**" sea *firmada* con DNSSEC y ligada de forma segura a la infraestructura DNSSEC existente en la zona padre, o sea que tenga lo que se llama una "delegación segura"). Además, el servidor recursivo debe configurarse para que *valide* las firmas DNSSEC para poder saber si los datos de DNS son auténticos. El ejercicio involucra al "**imr**" para la parte de validación y a los "**maestro**" y "**slave**" para el firmado y la publicación. El laboratorio consta de los siguientes pasos:

1. Instale las "*claves fiables*" para el "*ápex de seguridad*" (en este caso la zona de la raíz, "**.**") en el servidor recursivo, o sea en el **imr** (Unbound o BIND9).
2. Compruebe que la validación de datos fuera de su zona funciona.
3. Genere claves DNSSEC, una clave para firmar claves (key-signing key, KSK) y una clave para firmar la zona (zone-signing key, ZSK).
4. Firme la zona
5. Compruebe que la validación de datos de su propia zona se realiza con éxito.

Además de estos pasos iniciales hay ejercicios adicionales que cubren la "rotación de claves" y la utilización del registro **NSEC3** para la prueba de no-existencia autenticada.

6.1 Validación DNSSEC: Claves fiables

Este ejercicio debe hacerse en imr.

Para que su servidor recursivo pueda verificar las respuestas recibidas necesitará al menos una clave en la que pueda confiar "**um punto de anclaje para la confianza o ancla de confianza**", también llamada "**clave fiable**".

Los puntos de anclaje de la confianza se tienen que incluir en la configuración del servidor de nombres. La clave que hay que usar para "**.**" tiene este aspecto:

```
. 257 3 8
  AwEAAaQUID6/Px6EACdpe+eDCEwbkjWqchjhKWcnirPWEQxHquIrVes3
  4ah2q4dQ3PuXtFoGYxgePqc2tq5H0+tMUtSLU8ygwg2KWYT7iUOE3q+B
  /g5zaXLwNY41lHTyGAGkiO4XwVLyv3F5SU/hCq7/dVSkGNlS5zDAbxlS
  /EiO9Ppt
```

La clave **no** deberia copiarse a mano sino bajada de un servidor FTP. El método más cómodo es:

```
imr.whisky# ftp ftp://ftp.dnslab/pub/root.trusted-keys
imr.whisky# ls -l root.trusted-keys
-rw-r--r-- 1 root wheel 357 Nov 20 18:16 root.trusted-keys
```

6.1.1 Método alternativo para conseguir la "clave fiable"

Un método alternativo cómodo (pero no autenticado...), en lugar de usar FTP, es poner la clave pública en un fichero externo tal como se muestra abajo (el filtro para "**257**" hace que sólo se extraiga la **KSK**) y después utilizar el atributo **auto-trust-anchor-file:** para referenciar este fichero.

```
imr.whisky# dig . dnskey | grep 257 > root.trusted-keys
```

- Hay varias alternativas de configuración, porque Unbound puede usar tanto un registro **DS** como un registro **DNSKEY** como ancla de confianza. Unbound puede además usar los registros enteros o extraer la sintáxis para **trusted-keys** que BIND9 usa (esto se hizo para facilitar la interoperabilidad con BIND9). Compruebe la documentación de **trust-anchor:**, **trust-anchor-file:** y **trusted-keys-file:**.

- Para generar los registros **DS** a partir de las claves públicas puede usar **dnssec-dsfromkey** o **ldns-key2ds** (el "**-2**" fuerza SHA256 como hash para el **DS**):

  ```
  imr.whisky# dnssec-dsfromkey -2 root.key
  ```

  Nota: **dnssec-dsfromkey** es un poco simplón. Por ejemplo, dará por supuesto, sin avisar, que la clave estará en el fichero "*zona*.**key**" si se le invoca con el argumento "*zona*" (que no acaba en "**.key**") o sea que es muy importante que el nombre del fichero sea exactamente "**root.key**".

6.1.2 Compruebe que la validación DNSSEC funciona

Si su profesor ha hecho su trabajo todas piezas deberian ahora estar en su sitio. Por ejemplo deberia ser posible preguntar por el registro **A** de **www.dnslab**, y el registro **A** de su grupo. No se olvide de incluir la opción **+dnssec** en **dig**. Compruebe que el bit de estado **AD** (Authenticated Data) está puesto a 1 en las respuestas. Pruebe también a validar preguntas en otras partes del árbol, como el registro **SOA** de **in-addr.arpa**. ¿Está el bit **AD** puesto a 1?

```
imr.whisky# dig www.dnslab a +dnssec
...
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ...
...
;; ANSWER SECTION:
www.dnslab.     600    IN    A     10.0.0.1
www.dnslab.     600    IN    RRSIG   A 5 3 600 ...
...
```

esto es lo que queremos ver

Intente también buscar algo que no exista para ver como es una respuesta negativa firmada con DNSSEC.

6.1.3 Pruebe una validación de DNSSEC fallida

Para completar las pruebas con la validación DNSSEC ha llegado el momento de estudiar lo que pasa cuando las firmas **no** son se pueden validar.

- Dañe la trusted-key para **dnslab** en el servidor recursivo, por ejemplo intercambiando dos caracteres en la clave. **Esto no debe hacerse en los primeros caracteres, ya que estos se usan para codificar la keyid**, intercambie mejor caracteres que estén alrededor de uno de los espacios en blanco.
- Vacie la cache y recargue la configuración. La validación de firmas ya no deberia funcionar.
- Intente usar **dig** para buscar algo que no exista y que esté firmado. Esto no deberia funcionar. ¿Qué pasa?

- Haga la misma pregunta de nuevo, pero esta vez añada la opción "**+cd**" al final del la linea de comandos. Esto pondrá a 1 el bit **CD** ("checking disabled") en la pregunta. Este bit le dice al servidor recursivo que **no** intente llevar a cabo la validación. ¿Qué ocurre?

- Termine restableciendo la **trusted-key** a su versión original para que la validación funcione de nuevo. Si está usando BIND9 entonces borre también el fichero **managed-keys.bind** (otra vez) para forzar al servidor de nombres a validar con la clave que está en la directiva **managed-keys**.

6.2 Firmado de Zonas con DNSSEC

6.2.1 Generar claves de DNSSEC para la zona

Este ejercicio debe llevarse a cabo en el servidor "master"

La siguiente fase es conectar su zona a esta infraestructura firmada que acaba de probar. A esto se le llama crear una **delegación segura**. Una delegación firmada es el pegamento que une una zona padre firmada con una zona hijo firmada y que posibilita que un validador pueda seguir la cadena de confianza a través del corte de zona. El primer paso, obviamente, es firmar la zona hijo. Hay varios detalles que hay que recordar:

- Es necesario crear dos pares de claves, uno para la Clave de Firmado de Claves (KSK, Key Signing Key) y otro para la Clave de Firmado de Zonas (ZSK, Zone Signing Key). La forma más fácil de generar claves es usando el comando **dnssec-keygen**. En este ejercicio debe utilizar claves con el algoritmo y tamaño indicados en las especificaniones siguientes. Asegurese de que las claves están guardadas en el directorio de configuración del servidor de nombres autoritativo.

  KSK: 2048 bit **RSA/SHA256** (SPANISH MISSING)

  ZSK: 1024 bit **RSA/SHA256** (recomendado)

- A continuación se generan dos claves, una **KSK** y una **ZSK**, para la zona **whisky.dnslab**.

- Además debe tener cuidado al especificar el argumento "**-f KSK**" en la linea de comandos para **dnssec-keygen** cuando cree la **KSK**, como se muestra en el primero ejemplo a continuación.

```
master.whisky# cd /usr/pkg/etc/nsd    ()
master.whisky# dnssec-keygen -a RSASHA256 -b 2048 -n ZONE \
          -f KSK whisky.dnslab.
Kwhisky.dnslab.+008+39290
master.whisky# dnssec-keygen -a RSASHA256 -b 1024 -n ZONE \
          whisky.dnslab.
Kwhisky.dnslab.+008+24275
master.whisky# ls K*
Kwhisky.dnslab.+008+24275.key
Kwhisky.dnslab.+008+24275.private
Kwhisky.dnslab.+008+39290.key
Kwhisky.dnslab.+008+39290.private
```

Ahora ya posee las claves necesarias para firmar la zona. Asegurese de recordar cual de ellas es la **KSK** y cual es la **ZSK**. Es posible indentificarlas mirando el contenido del fichero **.key**-file pero es mejor anotarlo.

6.2.2 Firme la zona!

dnssec-signzone tiene más opciones de linea de comandos que las que cualquiera pudiera imaginar. Afortunamdamente la mayoria de ellos tienen valores por defecto sensatos y normalmente no hace falta usarlos. A continuación presentamos algunas de las opciones más interesantes para las que no hay valores por defecto o para las que los valores por defecto no son suficientes.

`-N soa-serial-format`

Hay tres formas diferentes por las que **dnssec-signzone** puede generar automáticamente el número de serie SOA para una zona firmada.

"**keep**" significa "no cambiar", "**increment**" signfica incrementar en uno y "**unix-time**" indica que usará la hora actual expresada en segundos.

`-S`	Utilice la llamada "firma inteligente" de **`dnssec-signzone`**. Esto hace que **`dnssec-signzone`** busque automáticamente las claves correctas para incluir en la zona y firmarla. Si **no** lo hace de esta forma, las claves tendrán que ser introducidas de forma manual en la zona.
`-v 9`	Verbosity level. Controla cuanto de hablador será el programa durante la ejecución. 9 = *muchísimo!*

A continuación viene el nombre del fichero de zona que será firmado.

Un ejemplo completo:

```
master.whisky# dnssec-signzone -S whisky.dnslab
Fetching KSK 39290/RSASHA256 from key repository.
Fetching ZSK 24275/RSASHA256 from key repository.
Zone signing complete:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 0 stand-by, 0 revoked
whisky.dnslab.signed
master.whisky#
```

- Actualice la configuración del servidor de nombres para que lea la zona firmada en vez de la zona sin firmar.
- Compruebe que esto es así mediante preguntas al servidor de nombres con "**`dig`**" usando las opciones "**`+dnssec +multi`**".

Ahora tiene no solamente una zona firmada sino que además la herramiento de firmado también ha creado un fichero "**`dsset`**". Contiene exactamente la información que necesita para mandar al padre (o sea el hash **`DS`** de su **`KSK`**) para que el padre puede añadir los registros **`DS`** correspondientes a su **`KSK`** a la zona padre.

6.3 Una Delegación Segura

6.3.1 Compruebe que la validación DNSSEC de sus datos funciona correctamente.

Tan pronto como el registro **DS** (firmado) sea generado y publicado en la zona padre todas los elementos deberian estar listos. Por ejemplo deberia ser posible buscar los registros **A** de su grupo. No se olvide de usar la opción **+dnssec** en **dig**. Compruebe que el bit de estado **AD** (Authenticated Data, Datos autenticados) está marcado en las respuestas. Además compruebe también la validación en otras partes del árbol.

```
ns.whisky# dig www.whisky.dnslab a +dnssec
...
;; flags: qr rd ra ad; QUERY: 1, ANS: 2, AUTH: 0, ...
...
;; ANSWER SECTION:
www.whisky.dnslab.   7200  IN  A     10.x.y.z
www.whisky.dnslab.   7200  IN  RRSIG A 5 3 600 ...
...
```

Nota: Dependiendo de como haya diseñado su anterior configuración puede que esto no funcione, o sea que no esté marcado el bit **AD** en la respuesta. Reflexione sobre cual podria ser la causa y propongale una solución a su profesor.

6.4 NSEC3

Ahora modificará su zona directa para que use semántica **NSEC3** en lugar de **NSEC**.

6.4.1 Algoritmos para las claves NSEC3

Si se va a firmar la zona con semántica **NSEC3** habrá que emplear claves con un algoritmo suficientemente moderno (porque el algoritmo se usa como una señal de forma que la validación sólo sea realizada por servidores que entienden los algoritmos modernos). Al haver usado el algoritmo **RSASHA256**, que también funciona con **NSEC3**, no necesitará reemplazar las claves.

6.4.2 Firme la zona con semántica NSEC3

Cuando se usa **NSEC3** hay varias opciones adicionales de la herramienta de firmado de zonas que se vuelven importantes:

ldns-signzone -n -s "salt" **dnssec-signzone -3 "salt"**	La sal es una cadena hexadecimal que se puede elegir libremente. La cadena vacia, "", es una elección válida. La sal se usa para dificultar los llamadas ataques de diccionario.
ldns-signzone -t num **dnssec-signzone -H num**	Número de iteraciones de la función hash. La intención es hacer los ataques más costosos (incrementando las necesidades de cálculo), a costa de aumentar también el tiempo de cálculo necesario en el servidor autoritativo.
ldns-signzone -p **dnssec-signzone -A**	Marca la opción **OPTOUT** en todos los registros **NSEC3** y no genera registros **NSEC3** para las delegaciones inseguras. Normalmente esto **no** es lo que queremos porque al usar OPTOUT no es posible validar las respuestas negativas.

Veamos un ejemplo de como firmar una zona con **NSEC3** (y como siempre esto es **un solo** comando, escrito en **una única** linea de comandos):

```
master.whisky# ldns-signzone -n -s "" -t 1 whisky.dnslab \
       Kwhisky.dnslab.+008+1234 Kwhisky.dnslab.+008+5678
```

```
master.whisky# dnssec-signzone -S -3 "" -H 1 whisky.dnslab
```

No se olvide de asegurarse de recargar la zona en el servidor.

Cuando haya completado todo hay que comprobarlo. Si todos los cambios han sido correctos entonces podrá obtener respuestas autenticadas (o sea, con el bit **AD** marcado) cuando realice búsquedas con su servidor recursivo (o con otro). Es posible que haga falta vaciar la caché con "**rndc flush**" para que la validación funcione correctamente.

6.5 SPANISH MISSING

Una zona firmada puede tener zonas hijas que pueden estar firmadas o no. Desde el punto de vista del padre esto se determina dependiendo de si la zona hijo solicita

un registro **DS** o no. Si la zona hijo tiene una KSK **y** el hijo solicita que se cree un registro **DS** entonces el padre debe hacerlo usando la KSK suministrada. Sin la KSK la delegación será una delegación normal, no segura, independientemente de que el hijo o el padre estén firmados.

- Cree dos zonas hijas de la zona **whisky.dnslab**. Llamelas "**secure.whisky.dnslab**" y "**unsecure.whisky.dnslab**" respectivamente. Puede servir las zonas usted mismo o pedirle a alguien que las aloje.
- Cree claves (una KSK y una ZSK) para la zona **secure.whisky.dnslab** e firme la zona de forma similar a lo que hizo anteriormente para **whisky.dnslab**.
- Asegurese de que el fichero **dsset** creado para **secure.whisky.dnslab** está en el mismo directorio que la zona padre (o sea "**whisky.dnslab**").
- Delegue las dos zonas hijas (o sea, añada registros **NS** para las zonas hijas en la zona **whisky.dnslab**.)
- Vuelva a firmar **whisky.dnslab**. Fijese en que se crea automáticamente un registro **DS** para **secure.whisky.dnslab** (y la correspondiente RRSIG. Sin embargo, no se crea ningún registro **DS** para **unsecure.whisky.dnslab**.

7 Usar un motor de firma DNSSEC

Para que el DNSSEC funcione de manera robusta y estable hace falta soporte del software, particularmente como ayuda durante los momentos de rotación de claves. Introducimos ahora herramientas que le pueden ayudar.

Interacción con el padre cuando se modifica la estrategia de firma DNSSEC

Es posible pasar de firmado "manual" DNSSEC como el que hemos usado hasta ahora al uso de herramientas más automáticas sin romper la cadena de firmas. Sin embargo, es necesario algún cuidado ya que las nuevas claves deben publicarse en la zona estando firmadas por las claves antiguas, etc
Para simplificar, durante este ejercicio haremos un reinicio, borraremos cualquier vestigio de las claves en la zona hija (los registros `DS` y el "autenticador de delegación" de CADR) para la `KSK` antigua y después cuando se firme la zona con el nuevo sistema solicitaremos una nueva delegación firmada pidiendo que se añadan nuevos registros `DS` a la zona padre.

El objetivo del ejercicio es pasar del firmado "manual" de DNSSEC a utilizar algunas de las herramientas disponibles, ambas diseñadas para operar según el modelo bump-on-the-wire (inserción en el cable):

- usará el motor de firma de OpenDNSSEC para generar claves de forma automática y para firmar su zona directa según una "política de claves y firmado" ("key and signing policy", KASP en Inglés). OpenDNSSEC se encargará de mantener la zona firmada de acuerdo con esta política.

7.1 Configurar Transferencias de Zona desde el Maestro al Motor de Firmado

El primer paso es actualizar la configuración del maestro oculto para que el motor de firmado pueda conseguir la zona. Para esto el maestro oculto tiene permitir transferencias de zona de salida y debe enviar Notifies al puerto 5353 en la dirección del maestro (`10.n.0.4`).

7.1.1 NSD4:

- Suponiendo que esté utilizando `pattern:` en NSD4 para múltiples zonas de las que sólo una deba ser publicada a través del motor de firmado, será necesario dejar de usar el antiguo `pattern:` para la zona directa (para evitar romper la configuración de las otras zonas).

```
# nsd.conf on the hidden master:
zone:
    name:           whisky.dnslab
    zonefile:       whisky.dnslab
    provide-xfr:    10.23.0.4 NOKEY
    notify:         10.23.0.4@5353 NOKEY
```

- Seleccione los cambios de la configuración con el comando:

  `master.whisky.dnslab:etc/nsd# nsd-control reconfig`

7.2 Configure las Transferencias de Zonas desde el Motor de Firma al Esclavo

El siguiente paso es actualizar la configuración del esclavo público para que obtenga la zona por transferencia de zona desde el motor de firmado **en el puerto 5353** en lugar de directamente del maestro oculto. También hará falta configurar el motor de firma para que Notifique al esclavo público y permita transferencias de zona, pero esto lo haremos más adelante.

Esto es, claramente, muy similar a lo que acaba de hacer en el maestro oculto.

7.2.1 NSD4:

- Actualice el atributo **`zone:`** de la zona directa para permitir notificaciones y solicitar transferencias de zona desde el motor de firmado.

```
zone:
    name:           whisky.dnslab
    zonefile:       whisky.dnslab
    request-xfr:    10.23.0.4@5353 NOKEY
    allow-notify:   10.23.0.4 NOKEY
```

7.3 Verificando la propagación de los datos cuando se usa un Motor de Firmado

Cuando hagamos pruebas con la propagación de las zonas para asegurarnos de que los NOTIFY funcionam correctamente es bastante fácil confundirse. En particular un número de serie nuevo en la zona en el **maestro** provocará **otros** números de serie tanto en el **signer** como en el (si todo funciona) **esclavo**.

Aunque siempre hay riesgo de confusión, hay un par de scripts de ayuda en el laboratorio que puede usar para simplificar un poco las pruebas.

- El primer script, `fixserial.sh`, solamente aumenta el número de serie para que no tenga que editar el fichero a mano sólo para esto. El requisito, no obstante, es que la cadena "**serial**" esté presente como un comentario después del número de serie del SOA (à la "`... 12345 ; serial`") en el fichero de zona para poder encontrar el número de serie.

  ```
  master.whisky:etc/nsd# ./fixserial.sh whisky.dnslab
  Serial in whisky.dnslab is changed from 2013091107 to 2013091108
  ```

  Fijese en el que el script no recarga el servidor de nombres. Eso hay que hacerlo aparte (dependiendo de que servidor de nombres esté utilizando).

- El segundo script, `checkserials.sh`, comprueba el número de serie en el **maestro**, **firma** y **esclavo** y los presenta para que se puedan compara fácilemente:

  ```
  master.whisky.dnslab:etc/nsd#./checkserials.sh whisky.dnslab
  master serial: 2016090811
  signer serial: 2016091123
  slave  serial: 2016091123
  ```

  Si hay más de un servidor esclavo es fácil modificar el script para verificar el número de serie de la zona en los servidores adicionales.

7.4 OpenDNSSEC

OpenDNSSEC está diseñado para ser una solución completa de DNSSEC para el responsable de una zona. Es un conjunto de oftware relativamente complejo y sólo trataremos parte de la funcionalidad.

Las ideas generales detrás de OpenDNSSEC son:

- Para aumentar la seguridad, las claves deben guardarse en HSMs (Hardware Security Modules, Módulos de Seguridad Hardware). Como no todo el mundo tiene acceso a HSMs hay un paquete de softwre adicional llamado "SoftHSM" que implementa un HSM en software.
- El firmado de las zonas está sujeto a una *política*. O sea, zonas diferentes necesitarán diferentes políticas (longitud de claves, algoritmos utilizados, calendario de rotación, etc).
- El signer (el software que firma) debe ejecutarse como un daemon (servidor) para que pueda firmar los **`RRsets`** cuando sea necesario.

7.4.1 Instalación de SoftHSM y OpenDNSSEC

Los paquetes de SoftHSM y OpenDNSSEC ya están instalados en la máquina "**`master`**".

7.4.2 Ajustando los ficheros de configuración de OpenDNSSEC

OpenDNSSEC guarda sus ficheros de configuración y *políticas* en formato XML en los ficheros **`conf.xml`**, **`kasp.xml`** y **`addns.xml`** que nornalmente están en el directorio **`/etc/opendnssec/`**.

Antes de que funcionen en el entorno de laboratorio, hay que hacer unos pequenhos ajustes en estos ficheros de configuración. Debido al tiempo disponible será necesario acortar algunas de las constantes de tiempo de forma significativa. Esto es sólo consecuencia del tiempo disponible para completar el laboratorio; en uso normal los valores por defecto son bastante razonables y no suele hacer falta ajustarlos.

Copie los ficheros **`conf.xml kasp.xml`** modificados que están en el directorio **`/etc/dnslab/`** al lugar correcto, **`/etc/opendnssec/`**. Esto reemplazará los ficheros estándar que estaban allí. Esto es intencional.

```
master.whisky# cp /etc/dnslab/*.xml /etc/opendnssec/
```

7.5 SoftHSM

Antes de hacer nada con **SoftHSM** hay que crear el directorio donde **SoftHSM** guarda su base de datos. Esto ya está hecho como parte del proceso automático de creación de este laboratorio. Si no hubiera sido asi, se puede crear con el comando "**mkdir -p /var/lib/softhsm**". **SoftHSM** también necesita un fichero de configuración para poder saber donde está la base de datos. Deberia tener este aspecto:

/usr/pkg/etc/softhsm.conf:

```
# softHSM configuration file
#
0:/var/lib/softhsm/slot0.db
```

SoftHSM es capaz de guardar muchas claves pero antes hay que inicializarlo. Los números "PIN" se pueden escoger de forma arbitraria pero asegurese de **anotarlos** ya que necesitará recordarlos para acceder a las claves. El "SO PIN" es para el "security officer", una especie de "PIN maestro".

- Inicialice el **SoftHSM** con el siguiente comando:

```
master.whisky# softhsm --init-token --slot 0 --label "OpenDNSSEC"
The SO PIN must have a length between 4 and 255 characters.
Enter SO PIN:
The user PIN must have a length between 4 and 255 characters.
Enter user PIN:
The token has been initialized.
```

- Para que OpenDNSSEC pueda utilizar **SoftHSM** para la generación y almacenamiento de claves tiene que saber el PIN para acceder al **SoftHSM**.

  Edite **/etc/opendnssec/conf.xml** y añada el **PIN de usuario** que acaba de definir en la sección de **SoftHSM**. Deberia parecerse a esto:

```
...
<Repository name="SoftHSM">
    <Module>/usr/pkg/lib/softhsm/libsofthsm.so</Module>
    <TokenLabel>OpenDNSSEC</TokenLabel>
    <PIN>4711</PIN>
</Repository>
```

El **SoftHSM** se usará por debajo del sistema para el almacenamiento de claves por parte de OpenDNSSSEC. Cuando se añadan zonas para que sean gestionadas por OpenDNSSEC todas las operaciones con claves serán completamente automáticas, incluida la generación de nuevas claves cuando sea necesario (dentro de **SoftHSM**), utilizandolas para el firmado de los datos de la zona durante la vida activa de la clave y finalmente retirando y borrando la clave.

Todas las operaciones se llevan a cabo de acuerdo con las políticas y por lo tanto el siguiente paso es inicializar la llamada base de datos de KASP ("Key and Signing Policy"). La utilidad **ods-enforcer** se usa para todo lo que se refiere a las diferentes políticas y que política se aplica a cada zona.

```
master.whisky# ods-enforcer-db-setup
*WARNING* This will erase all data in the database;
are you sure? [y/N] y
...
```

7.6 Ejecutar el componente de firma de OpenDNSSEC (signer)

Ahora arranque el motor de firmado. La zona que ha añadido deberia ser detectada y programada para ser firmada. Pero, como (al principio) no hay claves, todas las claves necesarias serán generada antes.

```
master.whisky# ods-control start
```

Como el motor de firmado está ahora en marcha, funcionará de forma automática. Las claves se generarán y las zonas se volverán a firmar según haga falta.

7.7 Modifcar la Clave de OpenDNSSEC y la Política de Firmado

OpenDNSSEC guarda todas las definiciones de las "políticas de firmado" en el fichero **/etc/opendnssec/kasp.xml** y en este fichero ya hay definidas tres políticas: "**default**", "**dnslab-nsec**" y "**dnslab-nsec3**". Puede usar cualquiera de estas dos últimas dependiendo de si quiere usar semántica **NSEC** o **NSEC3** en la zona.

- **Antes de continuar por favor decida si quiere utilizar una política que use NSEC o una que use NSEC3.** Tenga en cuenta que la política

"**dnslab-nsec3**" usa "**OPTOUT**". A continuacíon sólo debe cambiar la política que haya decidido usar.

- La "*vida útil*" de las claves (o sea el tiempo que queremos utililzarlas para firmar antes de comenzar una rotación de claves) deberia modificarse a un valor más pequeño. La **KSK** deberia tener una vida útil de **P6D** (esto es una forma de decir "6 días") y la **ZSK** deberia tener una vida útil de **PT3H** (o sea, "3 horas"). Cambie el valor entre los elementos **<Lifetime>** y **</Lifetime>** de la **KSK** a seis dias:

  Extracto de **/etc/opendnssec/kasp.xml**:

```
<Policy name="dnslab-nsec">
    ...
        <KSK>
            <Algorithm length="2048">8</Algorithm>
            <Lifetime>P6D</Lifetime>
            ...
        </KSK>
    ...
```

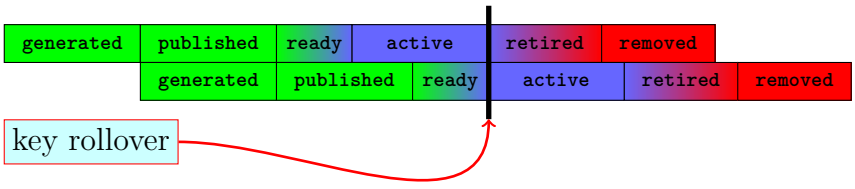
  De manera similar, cambie la vida útil de la **ZSK** a tres horas, o sea "**PT3H**".

Cuando haya realizado todos los cambios, digale a OpenDNSSEC que recargue la base de datos de KASP:

```
master.whisky# ods-enforcer policy import
master.whisky# ods-enforcer enforce
```

7.7.1 Observe el OpenDNSSEC en funcionamiento

Una de las razones principales para usar OpenDNSSEC es obviamente para automatizar las "rotaciones de claves", o sea las claves deberian pasar automáticamente de un estado al siguiente en el momento adecuado. El diagrama siguiente resume el conjunto de estados de clave para una ZSK:



No es obvio cual es la forma más fácil de observar la maquinaria de firmado y rotación en funcionamiento, pero cosas que puede hacer incluyen el filtrado de mensajes de log (bitácoras) buscando mensajes que incluyan la cadena "**ods-**" (OpenDNSSEC es bastante hablador, asi que con esto verá un montón de información sobre lo que está haciendo). Es una buena idea mantener este log visible en una ventana de terminal dedicada:

```
master.whisky# tail -f /var/log/messages | grep ods-
```

Otra cosa a observar es, por supuesto, el cambio en las claves durante un evento de rotación:

```
master.whisky# ods-enforcer key list
master.whisky# dig @10.0.23.1 whisky.dnslab dnskey +short
```

Nota: Ahora mismo no hay ninguna clave que observar ya que todavia no le hemos dicho a OpenDNSSEC que gestione nuestra zona. Esto se hará en el paso siguiente.

7.8 Añadir zonas a OpenDNSSEC

Ahora que la política está como queremos es el momento de añadir su zona directa al sistema. Como OpenDNSSEC asumirá la responsabilidad de la gestión de claves y el firmado primero hay que:

- borrar los registros **DNSKEY** de la zona sin firmar (no deberia haber ninguno).
- solicitar al padre que borre cualquier registro **DS** para la zona.

El siguiente paso es preparar el llamado "DNS Adapter (Adaptador de DNS)" para su uso. Es un fichero de configuración que especifica de que servidor de nombres transferir la zona sin firmar y hacia que servidores permitir las transferencias de salida de la zona firmada resultante. Usaremos el nombre **addns.xml** (de "**AD**apter **DNS**") para este fichero.

En el fichero **addns.xml** hay una sección **Inbound** para definir de donde hacer la transferencia de la zona sin firmar.

```
<Inbound>
  <RequestTransfer>
    <Remote><Address>10.23.0.4</Address></Remote>
  </RequestTransfer>
  <AllowNotify>
    <Peer><Prefix>10.23.0.4</Prefix></Peer>
  </AllowNotify>
```

address of hidden master

Aqui tendrá que especificar la dirección IP del servidor maestro oculto (tanto en la sección **RequestTransfer** para la transferencia de zona como en la sección **AllowNotify** para las notificaciones (Notify)).

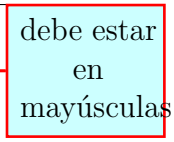
También hay una sección **Outbound** donde indicar hacia donde permitir las transferencias de zona y enviar las notificaciones. Añada la dirección del servidor autoritativo esclavo en la sección **ProvideTransfer** y en la sección **Notify**:

```
  <ProvideTransfer>
    <Peer><Prefix>10.23.0.0/16</Prefix></Peer>
    <Peer><Prefix>::1</Prefix></Peer>
    <Peer><Prefix>127.0.0.1</Prefix></Peer>
  </ProvideTransfer>
  <Notify>
    <Remote><Address>10.23.0.1</Address></Remote>
  </Notify>
```

SPANISH MISSING

SPANISH MISSING

Cuando esto esté hecho, use la utilidad **ods-enforcer** para añadir la zona a OpenDNSSEC. Fijese en que el siguiente comando es **un único** comando y debe de teclearse en **una única linea**.




```
master.whisky# ods-enforcer zone add --zone whisky.dnslab
               --in-type DNS --out-type DNS
               --input /etc/opendnssec/addns.xml
               --output /etc/opendnssec/addns.xml
               --policy dnslab-nsec
zonelist filename set to /etc/opendnssec/zonelist.xml.
Imported zone: whisky.dnslab
master.whisky# ods-enforcer policy import
master.whisky# ods-enforcer enforce

master.whisky# ods-enforcer zone list
zonelist filename set to /etc/opendnssec/zonelist.xml.
Found Zone: whisky.dnslab; on policy dnslab-nsec
```

7.9 Ejecutar el componente de firma de OpenDNSSEC (signer)

Las claves se generarán y las zonas se volverán a firmar según haga falta. Compruebe que las claves para la zona se han generado usando **ods-enforcer**:

```
master.whisky# ods-enforcer key list
Keys:
Zone:          Keytype:  State:  Date of next transition:
whisky.dnslab  KSK       publish 2016-07-27 14:35:21
whisky.dnslab  ZSK       active  2016-07-27 15:30:21
whisky.dnslab  ZSK       publish 2016-07-27 14:35:21
```

Otra utilidad, **ods-signer**, puede usarse para obtener información sobre que zonas está gestionando el el motor de firmado, ver la cola de tareas pendientes, etc. También es posible usarla para tomar control manual los tiempos de la política de firmado y solicitar una nueva firma de la zona. `master.whisky# ods-signer zones`

```
There are 2 zones configured
- 23.10.in-addr.arpa
- whisky.dnslab

master.whisky# ods-signer queue
```

```
It is now Thu Jul 28 01:45:41 2016

There are 2 tasks scheduled.
On Thu Jul 28 01:27:05 2016 I will [sign] zone 23.10.in-addr.arpa
On Thu Jul 28 01:31:05 2016 I will [sign] zone whisky.dnslab

master.whisky# ods-signer sign whisky.dnslab
Zone whisky.dnslab scheduled for immediate re-sign.
```

7.10 Una Delegación Firmada para una Zona Utilizando OpenDNSSEC

Ahora que tenemos la zona de nuevo firmada es el momento de solicitar añadir un nuevo registro **DS** en la zona padre. Por supuesto es de importancia vital que el **DS** represente la nueva **KSK** y no la antigua. Asegurese de que está publicando la nueva zona, con firmas generadas por las claves creadas por OpenDNSSEC.

- Pare completamente el servidor autoritativo y re-arrancolo inmediatamente para que se cargue la zona firmada generada por OpenDNSSEC en lugar de la antigua zona, la firmada manualmente.

- Compruebe que esto es asi mirando la **keyid** de las nuevas claves:

  ```
  master.whisky# ods-enforcer key list --zone whisky.dnslab --verbose
  SQLite database set to: /var/opendnssec/kasp.db
  Keys:
  Zone:          Keytype:  State:  CKA_ID    ... Repo:   Keytag:
  whisky.dnslab  KSK       active  3406jv... ... SoftHSM 30646
  whisky.dnslab  ZSK       retire  fj50dd... ... SoftHSM 61423
  whisky.dnslab  ZSK       active  5kf9sh... ... SoftHSM 46068
  ```

  Fijese en que el campo "**CKA_ID**" de arriba **no** representa el registro **DS** de la clave. Es solamente una referencia interna para el HSM y no muy útil.

- Una vez conozca la **keyid** de la **KSK**, asegurese de que es realmente la **KSK** utilizada para firmar el RRSET **DNSKEY** que está siendo publicado (compruebe el campo **keyid** en el registro **RRSIG**):

```
master.whisky# dig @::1 -p 5353 whisky.dnslab dnskey +dnssec +multi

...
;; ANSWER SECTION:
whisky.dnslab.  3600  IN  DNSKEY 257 3 8 AwEW8ly...6pL0c920xN8=
whisky.dnslab.  3600  IN  DNSKEY 256 3 8 AwE9rX0...cgGpBehsvOtD
whisky.dnslab.  3600  IN  DNSKEY 256 3 8 AwE4zww...2PEgRcI37fuH
whisky.dnslab.  3600  IN  RRSIG DNSKEY 8 2 3600 20160906093133
                          20160906072415 30646 whisky.dnslab.
                          VnXc/OJ4GbdSBgQWE5jKT+...pjXgpM7qIg==
```

este es el **keyid** de la KSK

Si los keyids coinciden la zona está lista de nuevo para tener una delegación firmada y esto se hace de la misma manera que antes, o sea, creando una "cuenta hijo" en CADR y desde esa cuenta solicitando que se genere un registro **DS**.

Para poder comprobar la validez del registro **DS** en la zona padre es posible pedirle a OpenDNSSEC que genere el **DS** directamente:

```
master.whisky# ods-enforcer key export --zone whisky.dnslab --ds
```

7.11

El estado actual de la zona es que OpenDNSSEC gestiona automáticamente las rotaciones de **ZSK** de acuerdo con la política seleccionada. Las rotaciones de **KSK**, sin embargo, no se completan sin una pequeña intervención manual, ya que se requiere interacción con la zona padre.

Lo que hace falta es publicar el registro **DS** de la **KSK** cuando la **KSK** esté "**lista**", o sea cuando haya estado publicada durante suficiente tiempo para que su utilización sea segura.

```
master.whisky# ods-ksmutil key list
Keys:
Zone:          Keytype:  State:     Date of next transition:
whisky.dnslab  KSK       ready      waiting for ds-seen
whisky.dnslab  ZSK       active     2016-07-27 19:35:14
whisky.dnslab  ZSK       publish    2016-07-27 18:40:14
```

El objetivo, como antes, es ser capaz de validar las búsquedas en la zona a partir de un ancla de confianza de una zona superior (la zona padre o posiblemente la

zona raiz). Es de nuevo necesario conseguir que el registro **DS** sea añadido a la zona padre.

- Para simplificar la comunicación con el padre es conveniente ser capaz de exportar la parte pública de la **KSK** del **softhsm**, lo que se consigue con el comando "**ods-ksmutil key export**":

  ```
  master.whisky# ods-ksmutil key export --zone whisky.dnslab

  ;active KSK DNSKEY record:
  whisky.dnslab. 3600   IN    DNSKEY  257 3 8 AwEAAdSN9ACmeBxF...
  4uP7ayffR4Z6pMldmk42PGIVBRo358xTQdjJZRTnKHDZEGHDSNOH38sr3Aoz...
  ...t0hIawd+/4hCeo6KevOWpCZvU= ;{id = 30646 (ksk), size = 2048b}
  ```

  Sólo las **KSK**s que están en estado "**ready**" serán exportadas. Si hace falta es posible forzar la exportación de otras claves con el argumento "**--keystate publish**" (por ejemplo).

  Ahora utilice el interfaz de CADR como antes para solicitar un registro **DS** para la zona y espera que aparezca el registro **DS**. Asegurese de **haber visto** el registro antes de continuar.

- Una vez que haya visto el registro **DS** en la zona padre es el momento de informar de esto a OpenDNSSEC para que el proceso de rotación de la **KSK** pueda continuar (esto es **un** comando, en una sola linea):

  ```
  master.whisky# ods-ksmutil key ds-seen
          --zone whisky.dnslab --keytag 30646
  ```

  El "**keytag**" que hay que usar se muestra en la salida de "**key export**" arriba como "**id = ... (ksk)**". Esto permite que la clave pase al estado "**active**":

- Compruebe que la **KSK** está ahora "**active**":

  ```
  master.whisky# ods-enforcer key list
  Keys:
  Zone:          Keytype:  State:     Date of next transition:
  whisky.dnslab  KSK       active     2016-07-27 21:49:50
  whisky.dnslab  ZSK       active     2016-07-27 19:35:14
  whisky.dnslab  ZSK       publish    2016-07-27 18:40:14
  ```

  Nota: Para poder comprobar la validez del registro **DS** en la zona padre es posible hacer que OpenDNSSEC gener el registro **DS** directamente:

  ```
  master.whisky# ods-enforcer key export --zone whisky.dnslab --ds
  ```

La delegación está (ahora) firmada y deberia ser posible validar las búsquedas en la zona a partir de un ancla de confianza para "`.`". Compruebe que ve el bit **`AD`** cuando testee en un resolver que valide.

8 Guardando ficheros de configuración para más adelante

Al completar este curso guardaremos los contenidos de:

- **`/usr/pkg/etc/nsd`** (para quien haya usado NSD)
- **`/usr/pkg/etc/unbound`** (para quien haya usado Unbound)
- **`/usr/pkg/etc/opendnssec`** para todas las configuraciones de OpenDNSSEC

para cada grupo de laboratorio y ponerlo a disposición para bajarse desde

```
http://www.axfr.net/student-data/dnssec-lacnic-sep2016/
```

(el URL exacto es único para cada curso y no está enlazado desde la página principal).

Los ficheros se combinan en archivos "**`tar`**" que se pueden desempaquetar con varias utilidades comunes, incluyendo el programa "**`tar`**" que se usó en el ejercicio de instalación del software.