

A dark blue vertical bar runs along the left edge of the page. A blue arrow-shaped banner points to the right from this bar, containing the text 'DESPLIEGUE DE APLICACIONES WEB'. In the bottom-left corner, there are several thin, curved, light blue lines that sweep upwards and to the right.

DESPLIEGUE DE APLICACIONES WEB

CONFIGURACIÓN DE UN SERVIDOR DNS USANDO WEBMIN

AUTOR: Alberto Martínez Pérez

CURSO: 2º CFGS Desarrollo de Aplicaciones Web (DAW)

MÓDULO: Despliegue de Aplicaciones Web

FECHA DE ENTREGA: 25 de febrero de 2024

ÍNDICE

INTRODUCCIÓN	3
A. ¿QUÉ ES WEBMIN?	3
B. INSTALACIÓN DE WEBMIN EN EL SERVIDOR DNS	3
ACCESO A WEBMIN DESDE UN NAVEGADOR WEB.....	5
CREAR UNA ACL.....	7
CREAR UNA ZONA MAESTRA	8
A. EDITAR EL REGISTRO DE RECURSO SOA	9
B. VISUALIZAR Y EDITAR EL FICHERO DE ZONA	9
C. AÑADIR NUEVOS REGISTROS DE RECURSO A LA ZONA.....	10
1. Añadir un registro de recurso de tipo A (Address)	10
2. Añadir un registro de recurso de tipo MX (Mail Exchange)	11
3. Añadir un registro de recurso de tipo TXT (Plain Text)	12
D. COMPROBACIÓN DE FUNCIONAMIENTO EN UN CLIENTE	14
CREAR UNA ZONA DE RESOLUCIÓN INVERSA	15
A. AÑADIENDO REGISTROS PTR.....	16
B. COMPROBACIÓN DE FUNCINAMIENTO EN UN CLIENTE.....	16
CONFIGURACIÓN DE UNA TRANSFERENCIA DE ZONA	17
A. CONFIGURACIONES EN EL SERVIDOR DNS PRIMARIO.....	17
B. CONFIGURACIONES EN EL SERVIDOR DNS SECUNDARIO	19
C. LLEVAR A CABO LA TRANSFERENCIA DE ZONA	21
D. CONFIGURAR LA ACTUALIZACIÓN AUTOMÁTICA	23
CONFIGURACIÓN DE UNA DELEGACIÓN DE ZONA	25
A. CONFIGURACIONES EN EL DNS PRINCIPAL	25
B. CONFIGURACIONES EN EL DNS DELEGADO	25
C. COMPROBACIÓN DE FUNCIONAMIENTO DE LA ZONA DELEGADA	26
CUESTIONES FINALES.....	27

INTRODUCCIÓN

A. ¿QUÉ ES WEBMIN?

Webmin es una interfaz web de administración de sistemas basada en Unix. Permite a los administradores de sistemas gestionar de forma remota y simplificada la configuración y administración de servidores Unix-like, como Linux, FreeBSD y otros sistemas basados en Unix.



Webmin también proporciona funciones específicas para la administración del sistema de nombres de dominio (DNS). A través del módulo DNS de Webmin, los administradores pueden gestionar la configuración y la administración de servidores de nombres en un entorno DNS.

Con el módulo DNS de Webmin, puedes realizar tareas como:

1. **Configuración de zonas DNS:** Puedes crear y configurar zonas DNS para tus dominios, especificando registros como A (dirección IP), MX (servidor de correo), CNAME (alias), entre otros.
2. **Gestión de registros DNS:** Permite añadir, modificar o eliminar registros individuales en las zonas DNS. Esto es útil para actualizar la información de resolución de nombres.
3. **Configuración de servidores de nombres:** Puedes gestionar la configuración de los servidores de nombres, estableciendo opciones como la dirección IP del servidor, los puertos de escucha, y otras configuraciones relacionadas con el servicio DNS.
4. **Gestión de servidores de reenvío:** Webmin facilita la configuración de servidores de reenvío, permitiendo que tu servidor DNS utilice otros servidores para resolver nombres que no están en sus zonas.

En resumen, el módulo DNS de Webmin proporciona una interfaz gráfica para facilitar la configuración y administración de servicios DNS en sistemas basados en Unix, contribuyendo a simplificar tareas relacionadas con la resolución de nombres y la gestión de zonas DNS.

B. INSTALACIÓN DE WEBMIN EN EL SERVIDOR DNS

En esta práctica vamos a instalar webmin en una máquina virtual con BIND9 instalado y que ejercerá el rol de DNS principal.

Para instalar Webmin vamos a usar la utilidad wget para descargar archivos de la web a través de la línea de comandos. La URL que

utilizaremos es la que contiene el script setup-repos.sh del repositorio de GitHub de Webmin.

sudo wget

<https://raw.githubusercontent.com/webmin/webmin/master/setup-repos.sh>

```
albertom-servidor@dns1:~$ sudo wget https://raw.githubusercontent.com/webmin/webmin/master/setup-repos.sh
--2024-02-13 15:20:13-- https://raw.githubusercontent.com/webmin/webmin/master/setup-repos.sh
Resolviendo raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.110.133, 185.199.111.133, ...
Conectando con raw.githubusercontent.com (raw.githubusercontent.com)[185.199.109.133]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 5268 (5,1K) [text/plain]
Grabando a: «setup-repos.sh»

setup-repos.sh          100%[=====] 5,14K --.-KB/s en 0,001s

2024-02-13 15:20:13 (5,52 MB/s) - «setup-repos.sh» guardado [5268/5268]
```

Una vez completada la descarga se nos habrá descargado un fichero de nombre setup-repos.sh dentro del directorio donde hayamos ejecutado el comando anterior:

```
albertom-servidor@dns1:~$ ls -la
total 124
drwx----- 14 albertom-servidor albertom-servidor 4096 feb 13 15:20 .
drwxr-xr-x  3 root root 4096 dic 20 18:15 ..
-rw-----  1 albertom-servidor albertom-servidor 1215 feb 13 15:18 .bash_history
-rw-r--r--  1 albertom-servidor albertom-servidor 220 dic 20 18:15 .bash_logout
-rw-r--r--  1 albertom-servidor albertom-servidor 3526 dic 20 18:15 .bashrc
drwx----- 11 albertom-servidor albertom-servidor 4096 dic 20 18:28 .cache
drwx----- 11 albertom-servidor albertom-servidor 4096 dic 20 18:28 .config
drwxr-xr-x  2 albertom-servidor albertom-servidor 4096 dic 20 18:30 Descargas
drwxr-xr-x  2 albertom-servidor albertom-servidor 4096 dic 20 18:19 Documentos
drwxr-xr-x  2 albertom-servidor albertom-servidor 4096 dic 20 18:19 Escritorio
-rw-r--r--  1 albertom-servidor albertom-servidor 5290 dic 20 18:15 .face
lrwxrwxrwx  1 albertom-servidor albertom-servidor  5 dic 20 18:15 .face.icon -> .face
drwxr-xr-x  2 albertom-servidor albertom-servidor 4096 dic 20 18:19 Imágenes
drwx-----  4 albertom-servidor albertom-servidor 4096 dic 20 18:19 .local
drwx-----  4 albertom-servidor albertom-servidor 4096 dic 20 18:28 .mozilla
drwxr-xr-x  2 albertom-servidor albertom-servidor 4096 dic 20 18:19 Música
drwxr-xr-x  2 albertom-servidor albertom-servidor 4096 dic 20 18:19 Plantillas
-rw-r--r--  1 albertom-servidor albertom-servidor 807 dic 20 18:15 .profile
drwxr-xr-x  2 albertom-servidor albertom-servidor 4096 dic 20 18:19 Público
-rw-r--r--  1 root root 5268 feb 13 15:20 setup-repos.sh
-rw-r-----  1 albertom-servidor albertom-servidor  5 feb 13 15:19 .vboxclient-clipboard-tid
-rw-r-----  1 albertom-servidor albertom-servidor  5 feb 13 15:19 .vboxclient-clipboard-tid
```

Podemos utilizar la nano para ver el aspecto de este fichero y, como podremos ver, se trata de un script de Shell:

```
GNU nano 7.2 ./setup-repos.sh
#!/bin/sh
# shellcheck disable=SC1090 disable=SC2059 disable=SC2164 disable=SC2181
# setup-repos.sh
# Configures Webmin repository for RHEL and Debian systems (derivatives)

webmin_host="download.webmin.com"
webmin_download="https://$webmin_host"
webmin_key="developers-key.asc"
webmin_key_download="$webmin_download/$webmin_key"
webmin_key_suffix="webmin-developers"
debian_repo_file="/etc/apt/sources.list.d/webmin.list"
rhel_repo_file="/etc/yum.repos.d/webmin.repo"
download_wget="/usr/bin/wget"
download="$download_wget -nv"

# Temporary colors
NORMAL=''
GREEN=''
RED=''
ITALIC=''
BOLD=''
if tty -s; then
    NORMAL="$(tput sgr0)"
    GREEN="$(tput setaf 2)"
    RED="$(tput setaf 1)"
    BOLD="$(tput bold)"
    ITALIC="$(tput sitm)"
fi

# Check user permission
if [ "${id -u}" -ne 0 ]; then
    echo "${RED}Error:${NORMAL} `setup-repos.sh` script must be run as root!" >&2
    exit 1
fi
```

Instalamos el script utilizando el siguiente comando:

```
sudo sh ./setup-repos.sh
```

```
albertom-servidor@dns1:~$ sudo sh ./setup-repos.sh
Setup repository? (y/N) y
Downloading Webmin key ..
.. done
Installing Webmin key ..
.. done
Setting up Webmin repository ..
.. done
Cleaning repository metadata ..
.. done
Downloading repository metadata ..
.. done
Webmin package can now be installed using apt-get install --install-recommends webmin command.
```

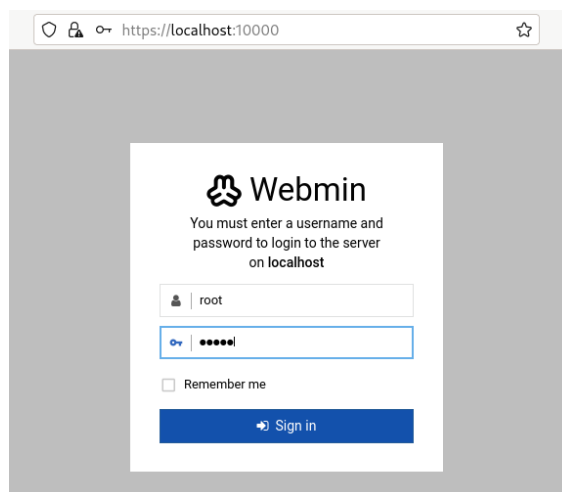
Por último, ejecutamos el comando que vemos en color verde en la imagen anterior y con ello conseguiremos instalar Webmin en el sistema:

```
sudo apt-get install --install-recommends webmin
```

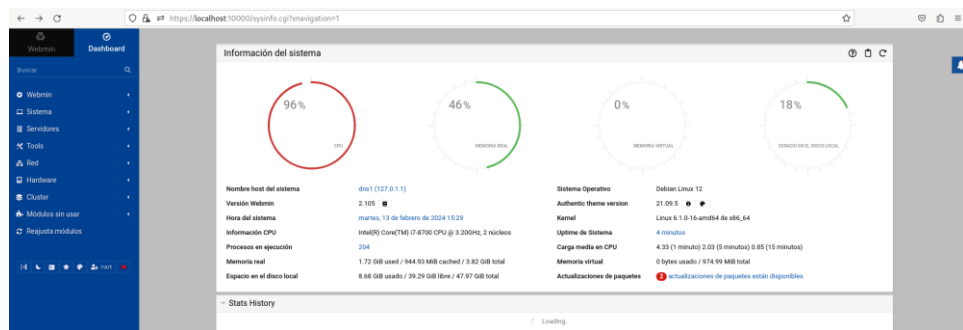
```
albertom-servidor@dns1:~$ sudo apt-get install --install-recommends webmin
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
libalgorithm-c3-perl libauthen-pam-perl libb-hooks-endofscope-perl libb-hooks-op-check-perl
libclass-c3-perl libclass-c3-xs-perl libclass-data-inheritable-perl libclass-inspector-perl
libclass-method-modifiers-perl libclass-singleton-perl libclass-xsaccessor-perl libdata-optlist-perl
libdatetime-locale-perl libdatetime-perl libdatetime-timezone-perl libdevel-callchecker-perl
libdevel-caller-perl libdevel-lexalias-perl libdevel-stacktrace-perl libdynaloader-functions-perl
libencode-detect-perl libeval-closure-perl libexception-class-perl libfile-sharedir-perl
libio-pty-perl libmodule-implementation-perl libmodule-runtime-perl libmro-compat-perl
libnamespace-autoclean-perl libnamespace-clean-perl libpackage-stash-perl libpackage-stash-xs-perl
libpadwalker-perl libparams-classify-perl libparams-util-perl libparams-validationcompiler-perl
libreadonly-perl libref-util-perl libref-util-xs-perl librole-tiny-perl libspecio-perl
libsub-exporter-perl libsub-exporter-progressive-perl libsub-identify-perl libsub-install-perl
libsub-name-perl libsub-quote-perl libvariable-magic-perl libxstring-perl
Paquetes sugeridos:
libscalar-number-perl libtest-fatal-perl
```

ACCESO A WEBMIN DESDE UN NAVEGADOR WEB

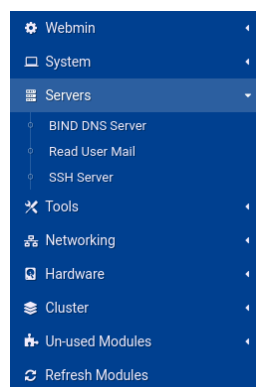
Para acceder a Webmin debemos de abrir un navegador web y escribir la URL localhost:10000, esto nos mostrará un formulario de login, debemos introducir los datos del administrador del sistema:



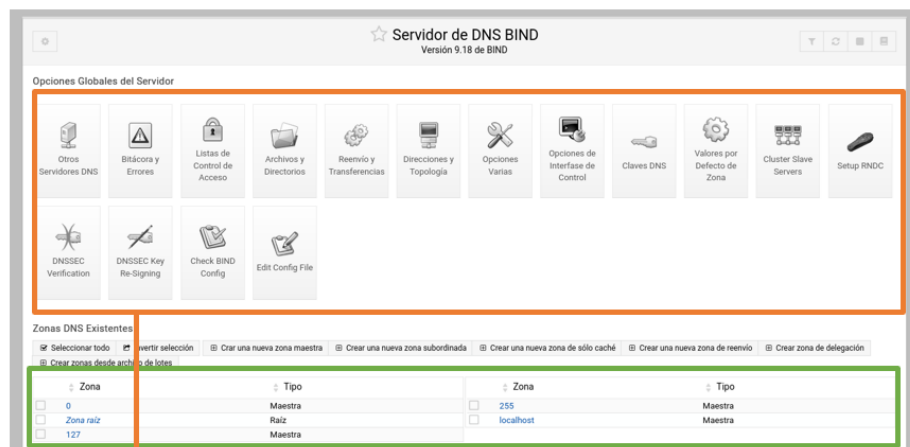
Una vez logados accederemos a la ventana de administración de Webmin donde podemos ver información de nuestra máquina virtual.



Lo que nos interesa es la sección servidores y concretamente la de BIND:



Hacemos clic sobre esta sección y podremos ver las diferentes opciones con las que contamos:



Opciones generales del servidor DNS.

Aquí podremos editar los ficheros de configuración entre otras cosas.

Zonas existentes en el DNS. En las opciones superiores podemos crear nuevas zonas, zonas delegadas, zonas secundarias, etc.

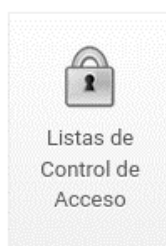
En las opciones inferiores podemos acceder a las zonas que tenemos definidas en el DNS.

CREAR UNA ACL

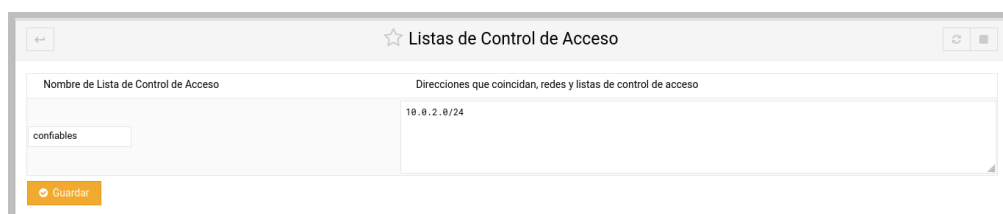
Lo primero que vamos a hacer es crear una ACL (*Access Control List*) o Lista de Control de Acceso. Una ACL en DNS se utiliza para especificar qué usuarios o sistemas tienen permiso para realizar ciertas acciones o acceder a ciertos recursos en un servidor DNS.

En el caso específico de DNS, las ACL pueden utilizarse para controlar el acceso a zonas específicas, restringir consultas de ciertos clientes o permitir el acceso solo a determinadas direcciones IP. Por ejemplo, puedes configurar una ACL para permitir solo consultas de resolución de nombres desde una red interna y bloquear consultas desde direcciones IP externas.

Para crear la ACL debemos de seleccionar la opción “Listas de Control de Acceso” del conjunto de opciones globales del servidor:

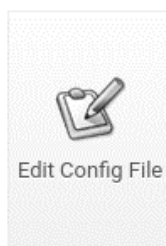


Una vez dentro se nos desplegará un formulario donde podremos crear una o varias ACL, en nuestro caso vamos a crear una ACL de nombre “confiables” y que afectará a todas aquellas IPs de la red 10.0.2.0/24 ya que vamos a conectar a nuestras máquinas dentro de una Red Nat que usa esta red.

A screenshot of a web-based configuration window titled 'Listas de Control de Acceso'. The window has a light gray border and a title bar. Inside, there are two input fields. The first field is labeled 'Nombre de Lista de Control de Acceso' and contains the text 'confiables'. The second field is labeled 'Direcciones que coincidan, redes y listas de control de acceso' and contains the text '10.0.2.0/24'. Below these fields is an orange button with a white plus icon and the text 'Guardar'.

Una vez que hayamos completado ambos campos debemos pulsar en “Guardar” y los cambios se harán efectivos.


Si queremos comprobar el cambio que se ha realizado podemos ir a la opción “Edit Config File”:



Y una vez dentro seleccionamos el fichero named.conf que almacena la configuración global del DNS y es el lugar donde Webmin coloca las diferentes ACL que podemos crear:

CREAR UNA ZONA MAESTRA

Vamos a crear una nueva zona maestra en nuestro servidor DNS, para ello debemos hacer clic sobre la opción “Crear una nueva zona maestra”:

 [Crar una nueva zona maestra](#)

Esto desplegará un formulario en una nueva ventana donde debemos crear la zona con los valores que decidamos. En nuestro caso:

- Será una zona de reenvío. Es decir, convertirá nombres de dominio en direcciones IP.
- El nombre de dominio será “albertom.es.”.
- El servidor maestro será el nombre de nuestra máquina. En nuestro caso “dns1”.
- La dirección de correo será “admini.albertom.es.”

El resto de los valores se dejarán por defecto.

Una vez completado pulsamos en “Crear” y se generará el nuevo fichero de zona, esto lo podemos comprobar volviendo a la ventana del servidor y veremos que en la parte inferior donde se muestran las zonas de nuestro DNS ha aparecido la nueva zona que hemos creado:

Zonas DNS Existentes

☒ Seleccionar todo
 ☒ Invertir selección
 ☐ Crear una nueva zona maestra
 ☐ Crear una nueva zona subordinada
 ☐ Crear una nueva zona de sólo caché
 ☐ Crear una nueva zona de reenvío
 ☐ Crear zona de delegación
 ☐ Crear zonas desde archivo de lotes

Zona	Tipo	Zona	Tipo
<input type="checkbox"/> 0	Maestra	<input type="checkbox"/> 255	Maestra
<input type="checkbox"/> Zona raiz	Raiz	<input type="checkbox"/> albertom.es	Maestra
<input type="checkbox"/> 127	Maestra	<input type="checkbox"/> localhost	Maestra

A. EDITAR EL REGISTRO DE RECURSO SOA

El siguiente paso será editar el SOA de nuestro fichero, para ello podemos acceder a esta edición desde la opción de “Editar Parámetros de Zona” que encontraremos dentro de la ventana de la zona.



Dentro podemos ver y editar los diferentes parámetros que tiene el registro SOA de nuestro fichero de zona que acabamos de crear:

☆ Parámetros de Zona
albertom.es

Parámetros de Zona

Servidor Maestro <input type="text" value="dns1."/>	Tiempo de expiración 1209600 segundos ▼
Dirección de correo <input type="text" value="admini@alberto.es"/>	Tiempo-que-está-viva por Defecto 3600 segundos ▼
Tiempo de refresco 3600 segundos ▼	Default time-to-live for records <input type="radio"/> Por defecto <input checked="" type="radio"/> 3600 segundos ▼
Tiempo de reintento de transferencia 600 segundos ▼	

B. VISUALIZAR Y EDITAR EL FICHERO DE ZONA

Si lo que queremos es visualizar el fichero de zona deberemos seleccionar la opción “Editar Archivo de Registros” disponible en la ventana de la zona:



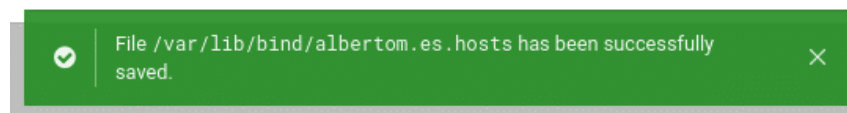
Dentro de esta opción podremos ver el fichero de zona:

De hecho, este fichero contiene una serie de errores:

- Nuestra máquina dns1 no tiene nuestro dominio “albertom.es.”.
- El correo tiene el dominio mal escrito, “alberto.es” en lugar de “albertom.es.”.

Para solucionar esto podemos modificar el fichero desde el propio editor:

Una vez modificado, hacemos clic en “Save” y los cambios se guardarán.



C. AÑADIR NUEVOS REGISTROS DE RECURSO A LA ZONA

1. *Añadir un registro de recurso de tipo A (Address)*

En el listado de tipos de registro de nuestra zona maestra debemos elegir “Dirección”:

Tipo	Registros	Tipo	Registros
Dirección	0	Localización	0
Servidor de nombre	1	Dirección del servicio	0
Nombre de Alias	0	Clave pública	0
Servidor de Correo	0	SSL Certificate	0
Información de Máquina	0	SSH Public Key	0
Texto	0	Certificate Authority	0
Sender Permitted From	0	Name Authority	0
DMARC	0	DNSSEC Parameters	0
Servicio Acreditado	0	Dirección IPv6	0
Persona Responsable	0	Todo	1
Dirección Inversa	0		

En el formulario que aparece rellenamos con los datos de nuestra máquina:

Añadir Registro Dirección

Nombre

Tiempo de vida
☒ Por defecto
☐ segundos ▼

Dirección

¿Actualizar Inversas?
☒ Si ☐ Sí (y reemplazar las existentes) ☐ No

+ Crear

Show records matching:

🔍 Search

Y pulsamos en “Crear” para crear el registro.

Nombre	TTL	Dirección
<input type="checkbox"/> dns1.albertom.es.	3600	10.0.2.7

2. Añadir un registro de recurso de tipo MX (Mail Exchange)

Ahora vamos a crear un registro de tipo MX, en este caso en el listado de tipos de registro debemos elegir el de “Servidor de Correo”:

Tipo	Registros	Tipo	Registros
Dirección	1	Localización	0
Servidor de nombre	1	Dirección del servicio	0
Nombre de Alias	0	Clave pública	0
Servidor de Correo	0	SSL Certificate	0
Información de Máquina	0	SSH Public Key	0
Texto	0	Certificate Authority	0
Sender Permitted From	0	Name Authority	0
DMARC	0	DNSSEC Parameters	0
Servicio Acreditado	0	Dirección IPv6	0
Persona Responsable	0	Todo	2
Dirección Inversa	0		

Y volvemos a completar el formulario con los datos del registro:

Añadir Registro Servidor de Correo

Nombre

Tiempo de vida
☒ Por defecto
☐ segundos ▼

Servidor de Correo

Prioridad

+ Crear

Show records matching:

🔍 Search

Y al igual que antes pulsamos en “Crear” y esto hará que se genere el registro:

Nombre	TTL	Prioridad	Servidor de Correo
<input type="checkbox"/> albertom.es.	3600	5	svrcorreo.albertom.es.

Para que este servidor funcione requiere de un registro de tipo A por lo que debemos crear un nuevo registro de dirección para que el dominio svrcorreo.albertom.es. pueda ser resuelto:

Añadir Registro Dirección

Nombre

Tiempo de vida

☒ Por defecto
 ☐ segundos ▼

Dirección

¿Actualizar Inversas?

☒ Si
 ☐ Sí (y reemplazar las existentes)
 ☐ No

Show records matching:


3. Añadir un registro de recurso de tipo TXT (Plain Text)

Por último, vamos a crear un registro de tipo TXT, para ello en el menú de selección de tipos de registro debemos seleccionar la opción “Texto”:

Tipo	Registros	Tipo	Registros
Dirección	1	Localización	0
Servidor de nombre	1	Dirección del servicio	0
Nombre de Alias	0	Clave pública	0
Servidor de Correo	1	SSL Certificate	0
Información de Máquina	0	SSH Public Key	0
Texto	0	Certificate Authority	0
Sender Permitted From	0	Name Authority	0
DMARC	0	DNSSEC Parameters	0
Servicio Acreditado	0	Dirección IPv6	0
Persona Responsable	0	Todo	3
Dirección Inversa	0		

En este registro vamos a crear un SPF que es un estándar de autenticación de correo electrónico diseñado para combatir la falsificación de direcciones de remitente en los correos electrónicos, lo que ayuda a reducir el riesgo de mensajes de spam o phishing.

Para ello podemos utilizar MxTool y crear nuestro TXT personalizado para nuestro dominio:

 **SPF Record Generator**

Domain Name or URL

albertom.es.

Check SPF Record

Solve Email Delivery Problems

☐ Pre-fill with record found

SPF WIZARD

Answer the questions below and we'll generate a record for you in the correct format. If you have questions, you can contact [MxToolbox Support](#)

Do you send email from your webserver?

No ▾

Do you send email from the same server in your MX records?

Yes ▾

Enter any other server hostname or domain that delivers email for your domain

Enter your domain's IPv4 Addresses / CIDR Ranges

10.0.2.4/24

Enter your domain's IPv6 Addresses / CIDR Ranges

Enter any 3rd party systems that may deliver emails for your domain (usually provided to you by the sending system)

Ex. Google Apps, Office 365, etc., This record is usually provided by the 3rd party.

How strict should the SPF Policy be?

Neutral ▾

Suggested Record:

Type: TXT

Host/Name: albertom.es.

Value: v=spf1 mx ip4:10.0.2.4/24 ?all

Dentro del formulario de Webmin para crear un registro TXT introducimos estos datos:

Añadir Registro Texto

Nombre

albertom.es.

Tiempo de vida

☒ Por defecto

☐ segundos ▾

Mensaje

v=spf1 mx ip4:10.0.2.4/24 ?all

+ Crear

Show records matching:

Q Search

Finalizamos la creación pulsando en “Crear”.

Para asegurarnos de que los cambios surgen efecto en los archivos de configuración pulsamos en “Apply Configuration” en el menú principal de nuestra zona maestra:



Y, a continuación, accedemos a la visualización en pantalla del fichero de zona para comprobar que realmente se han aplicado estos nuevos registros.

```
1 $ttl 3600
2 albertom.es.      IN  SOA dns1.albertom.es. admini.albertom.es. (
3                   2024021604
4                   3600
5                   600
6                   1209600
7                   3600 )
8 albertom.es.      IN  NS  dns1.albertom.es.
9 dns1.albertom.es. IN  A   10.0.2.7
10 albertom.es.      IN  MX  5 svrcorreo.albertom.es.
11 albertom.es.      IN  TXT "v=spf1 mx ip4:10.0.2.4/24 ?all"
12 svrcorreo.albertom.es. IN A 10.0.2.15
13
```

Hay que tener en cuenta que este fichero se está guardando localmente, concretamente Webmin lo está almacenando en el directorio /var/lib/bind/:

```
albertom-servidor@dns1:~$ ls -la /var/lib/bind/
total 12
drwxrwxr-x  2 root bind 4096 feb 16 16:34 .
drwxr-xr-x 56 root root 4096 feb 13 15:15 ..
-rwxrwxr-x  1 root bind  286 feb 16 16:34 albertom.es.hosts
```

D. COMPROBACIÓN DE FUNCIONAMIENTO EN UN CLIENTE

Vamos a utilizar una máquina virtual que tendrá el rol de un cliente que va a preguntar por los diferentes registros de nuestra zona maestra.

Esta máquina se debe encontrar en la misma Red Nat que nuestro servidor DNS y, además, debemos hacer que el servidor DNS sea el servidor de nombres de nuestro cliente.

```
nameserver 10.0.2.7
nameserver 127.0.0.53
options edns0 trust-ad
search home
```

Una vez hecho esto vamos a utilizar nslookup para realizar preguntas por los diferentes registros de nuestra zona maestra:

```
albertom-cliente@cliente:~$ nslookup -type=A dns1.albertom.es
Server:      10.0.2.7
Address:     10.0.2.7#53

Name:   dns1.albertom.es
Address: 10.0.2.7

albertom-cliente@cliente:~$ nslookup -type=MX albertom.es
Server:      10.0.2.7
Address:     10.0.2.7#53

albertom.es      mail exchanger = 5 svrcorreo.albertom.es.

albertom-cliente@cliente:~$ nslookup -type=A svrcorreo.albertom.es
Server:      10.0.2.7
Address:     10.0.2.7#53

Name:   svrcorreo.albertom.es
Address: 10.0.2.15

albertom-cliente@cliente:~$ nslookup -type=TXT albertom.es
Server:      10.0.2.7
Address:     10.0.2.7#53

albertom.es      text = "v=spf1 mx ip4:10.0.2.4/24 ?all"

albertom-cliente@cliente:~$ nslookup -type=NS albertom.es
Server:      10.0.2.7
Address:     10.0.2.7#53

albertom.es      nameserver = dns1.albertom.es.
```

CREAR UNA ZONA DE RESOLUCIÓN INVERSA

Una vez realizada nuestra zona de resolución directa, vamos a configurar nuestra zona de resolución inversa, esta zona se va a encargar de resolver direcciones IP a dominio.

Para crear una zona inversa debemos crear una nueva zona maestra, pero en este caso el tipo de zona que seleccionaremos en el formulario será “Inversas” en lugar de “Reenvío”.

La configuración base de nuestro fichero de zona inversa será el siguiente:

Crear Zona Maestra

Opciones de nueva zona maestra

Tipo de zona

☐ Reenvío (Nombres a Direcciones)

☒ Inversas (Direcciones a Nombres)

Nombre de Dominio/Red

10.0.2

Archivo de Registros

☒ Automático ☐ [Icono de archivo]

Servidor Maestro

dns1.albertom.es

☒ ¿Añadir registro NS para servidor maestro?

Dirección de correo

admini.alberto.es

¿Utilizar plantilla de zona?

☒ Si ☐ No

Dirección IP para registros de plantilla

[Campo de texto]

Add reverses for template addresses?

☒ Si ☐ No

Tiempo de refresco

3600 segundos

Tiempo de reintento de transferencia

600 segundos

Tiempo de expiración

1209600 segundos

Tiempo-que-está-viva por Defecto

3600 segundos


El nombre del fichero debe ser 10.0.2 representando los primeros tres octetos de la dirección IP de nuestro servidor DNS.

El aspecto final del archivo de zona inversa se puede ver entrando en el editor de archivos de registro de esta zona que hemos creado:

```
1 $ttl 3600
2 2.0.10.in-addr.arpa. IN SOA dns1.albertom.es. admini.alberto.es (
3     2024021600
4     3600
5     600
6     1209600
7     3600 )
8 2.0.10.in-addr.arpa. IN NS dns1.albertom.es.
9
```

A. AÑADIENDO REGISTROS PTR

Para añadir registros PTR (Pointer Record) a nuestra zona de resolución inversa podemos añadir registros de una manera similar a como hemos añadido registros a nuestra resolución directa o acudir a los diferentes registros de resolución directa y actualizar las inversas:



Una vez hecho esto si comprobamos el estado de nuestro fichero de zona inversa se deberían haber creado registros PTR correspondientes a los registros de nuestra zona de resolución directa:

```
1 $ttl 3600
2 2.0.10.in-addr.arpa. IN SOA dns1.albertom.es. admini.alberto.es (
3     2024021602
4     3600
5     600
6     1209600
7     3600 )
8 2.0.10.in-addr.arpa. IN NS dns1.albertom.es.
9 7.2.0.10.in-addr.arpa. IN PTR dns1.albertom.es.
10 15.2.0.10.in-addr.arpa. IN PTR svrcorreo.albertom.es.
11
```

Aplicamos cambios en la configuración de nuestro servidor DNS y con ello habremos terminado de crear la zona de resolución inversa.

B. COMPROBACIÓN DE FUNCIONAMIENTO EN UN CLIENTE

Volvemos a nuestra máquina virtual que cumple el rol de cliente y comprobamos el funcionamiento de la zona de resolución inversa.

```
albertom-cliente@cliente:~$ nslookup 10.0.2.7
7.2.0.10.in-addr.arpa    name = dns1.albertom.es.

albertom-cliente@cliente:~$ nslookup 10.0.2.15
15.2.0.10.in-addr.arpa  name = svrcorreo.albertom.es.
```


CONFIGURACIÓN DE UNA TRANSFERENCIA DE ZONA

Para la transferencia de zona necesitamos tener una segunda máquina virtual que haga de servidor DNS secundario.

El servidor en el que hemos configurado las zonas anteriores se encargará de ser el DNS primario y de llevar a cabo la transferencia de zona.

A. CONFIGURACIONES EN EL SERVIDOR DNS PRIMARIO

Primero vamos a configurar el servidor DNS primario para que en la zona se registre el servidor secundario. Para ello debemos añadir un nuevo registro de servidor de nombres:

Añadir Registro Servidor de nombres

Nombre de Zona

albertom.es.

Tiempo de vida

☒ Por defecto ☐ segundos ▼

Servidor de Nombres

esclavo.albertom.es.

(Los nombres absolutos deben de terminar con un .)

+ Crear

Show records matching:

Search

☒ Seleccionar todo ☒ Invertir selección

Nombre	TTL	Servidor de Nombres
<input type="checkbox"/> albertom.es.	3600	dns1.albertom.es.

☒ Seleccionar todo ☒ Invertir selección

Delete Selected

También deberemos crear un registro de dirección para que el nombre de dominio esclavo pueda ser resuelto:

Añadir Registro Dirección

Nombre

esclavo.albertom.es.

Tiempo de vida

☒ Por defecto ☐ segundos ▼

Dirección

10.0.2.8

¿Actualizar Inversas?

☒ Si ☐ Sí (y reemplazar las existentes) ☐ No

+ Crear

Show records matching:

Search

Con esto nuestro fichero de zona quedaría así:

```
1 $ttl 3600
2 albertom.es. IN SOA dns1.albertom.es. admini.albertom.es. (
3     2024021608
4     3600
5     600
6     1209600
7     3600 )
8 albertom.es. IN NS dns1.albertom.es.
9 dns1.albertom.es. IN A 10.0.2.7
10 albertom.es. IN MX 5 svrcorreo.albertom.es.
11 albertom.es. IN TXT "v=spf1 mx ip4:10.0.2.4/24 ?all"
12 svrcorreo.albertom.es. IN A 10.0.2.15
13 albertom.es. IN NS esclavo.albertom.es.
14 esclavo.albertom.es. IN A 10.0.2.8
15
```

Ahora debemos permitir las transferencias de la zona y las notificaciones, para ello dentro de las opciones de nuestra zona maestra debemos seleccionar la opción “Editar opciones de Zona”:



Y en el formulario correspondiente debemos añadir la dirección IP de nuestro servidor secundario para permitir la transferencia de zona hacia él:

Opciones de Zona

¿Revisar nombres?
☐ Aviso ☐ Fallo ☐ Ignorar ☒ Por defecto

¿Notificar los cambios a las subordinadas?
☐ Si ☐ No ☐ explicit ☒ Por defecto

Permitir actualizaciones desde...

Permitir transferencias desde...

10.0.2.8

Permitir consultas desde...

También notificar a subordinadas...

✓ Guardar

Ahora si comprobamos el fichero named.conf.local veremos que se han añadido la directiva allow-transfer:

```
Editing config file: /etc/bind/named.conf.local
1 zone "albertom.es" {
2     type master;
3     file "/var/lib/bind/albertom.es.hosts";
4     allow-transfer {
5         10.0.2.8;
6     };
7 };
8 zone "2.0.10.in-addr.arpa" {
9     type master;
10    file "/var/lib/bind/10.0.2.rev";
11 };
12
```

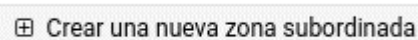
Realizamos los mismos pasos, pero en el fichero de resolución inversa para que también se transfiera esta zona:

```
Editing config file: /etc/bind/named.conf.local
1 zone "albertom.es" {
2     type master;
3     file "/var/lib/bind/albertom.es.hosts";
4     allow-transfer {
5         10.0.2.8;
6     };
7 };
8 zone "2.0.10.in-addr.arpa" {
9     type master;
10    file "/var/lib/bind/10.0.2.rev";
11    allow-transfer {
12        10.0.2.8;
13    };
14 };
15
```

Estas directivas allow-transfer se podrían poner también en el fichero named.conf.options para afectar al comportamiento general del servidor DNS pero es más seguro colocarlas dentro de las zonas para que en caso de un ataque de denegación de servicio (DDoS) el servidor DNS no se vea afectado. De hecho, es buena práctica el colocar la directiva allow-transfer con valor a none en el fichero de configuración general.

B. CONFIGURACIONES EN EL SERVIDOR DNS SECUNDARIO

En el servidor secundario debemos crear una zona subordinada o esclava, para ello en el menú principal de Webmin para el servidor DNS debemos seleccionar la opción “Crear una nueva zona subordinada”:

 Crear una nueva zona subordinada

En el formulario que nos aparecerá a continuación debemos rellenar el nombre del dominio y las IPs de los servidores maestros que en nuestro

caso será la IP del DNS primario que hemos configurado en el apartado anterior:

Opciones de nueva zona subordinada

Tipo de Zona
☒ Reenvío (Nombres a Direcciones) ☐ Inversas (Direcciones a Nombres)

Nombre de Dominio/Red
albertom.es.

Archivo de Registros
☐ Ninguno ☒ Automático

Servidores Maestros
10.0.2.7

Puerto de Servidor
☒ Por defecto ☐ puerto

+ Crear

Y creamos una más para la zona de resolución inversa:

Opciones de nueva zona subordinada

Tipo de Zona
☐ Reenvío (Nombres a Direcciones) ☒ Inversas (Direcciones a Nombres)

Nombre de Dominio/Red
10.0.2

Archivo de Registros
☐ Ninguno ☒ Automático

Servidores Maestros
10.0.2.7

Puerto de Servidor
☒ Por defecto ☐ puerto

+ Crear

Esto actualizará el fichero `named.conf.local` para añadir las zonas que hemos creado que será de tipo esclavo (slave) y contarán con la directiva `masters`:

Editing config file: `/etc/bind/named.conf.local`

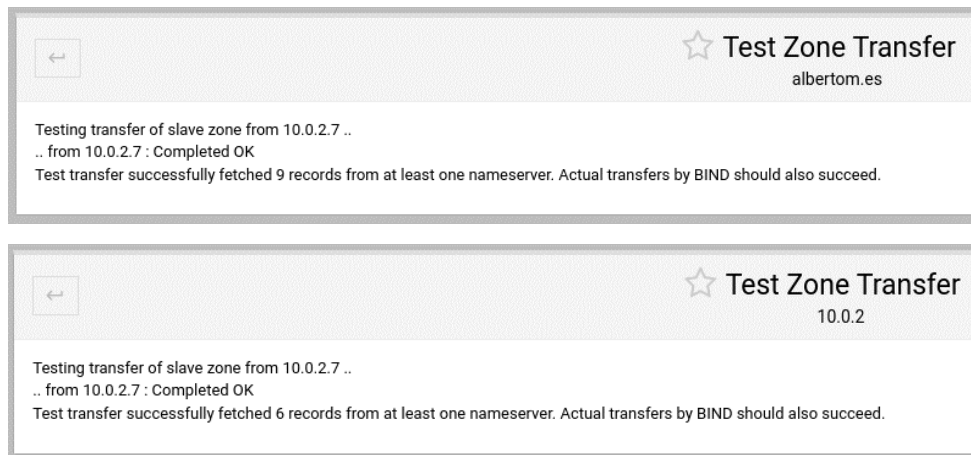
```
1 zone "albertom.es" {
2     type slave;
3     masters {
4         10.0.2.7;
5     };
6     file "/var/lib/bind/albertom.es.hosts";
7 };
8 zone "2.0.10.in-addr.arpa" {
9     type slave;
10    masters {
11        10.0.2.7;
12    };
13    file "/var/lib/bind/10.0.2.rev";
14 };
15
```

C. LLEVAR A CABO LA TRANSFERENCIA DE ZONA

Una vez hechas las configuraciones anteriores debemos llevar a cabo la transferencia de zona como tal, para ello dentro de las opciones de nuestras zonass subordinada (servidor secundario) debemos usar la opción “test zone transfer” para comprobar si se realiza la transferencia de zona:



Esto llevará a cabo una prueba de transferencia de zona:



Si esta prueba ha sido positiva, debemos llevar a cabo la transferencia reiniciando el servicio named tanto en la máquina secundaria como en la primaria:

```
albertom-servidor@dns1:~$ sudo systemctl restart named.service
albertom-servidor@dns1:~$ sudo systemctl status named.service
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Mon 2024-02-19 15:48:47 CET; 9s ago
     Docs: man:named(8)
    Main PID: 37269 (named)
      Status: "running"
        Tasks: 4 (limit: 4622)
       Memory: 33.2M
          CPU: 127ms
   CGroup: /system.slice/named.service
           └─37269 /usr/sbin/named -f -u bind -4

feb 19 15:48:47 dns1 named[37269]: zone albertom.es/IN: sending notifies (serial 2024021609)
feb 19 15:48:47 dns1 named[37269]: all zones loaded
feb 19 15:48:47 dns1 named[37269]: running
feb 19 15:48:47 dns1 systemd[1]: Started named.service - BIND Domain Name Server.
feb 19 15:48:47 dns1 named[37269]: resolver priming query complete: success
feb 19 15:48:47 dns1 named[37269]: checkhints: b.root-servers.net/A (170.247.170.2) missing from hints
feb 19 15:48:47 dns1 named[37269]: checkhints: b.root-servers.net/A (199.9.14.201) extra record in hints
feb 19 15:48:47 dns1 named[37269]: checkhints: b.root-servers.net/AAAA (2801:1b8:10::b) missing from hints
feb 19 15:48:47 dns1 named[37269]: checkhints: b.root-servers.net/AAAA (2001:500:200::b) extra record in hints
feb 19 15:48:47 dns1 named[37269]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
```

```

albertom-servidor@esclavo:~$ sudo systemctl restart named.service
albertom-servidor@esclavo:~$ sudo systemctl status named.service
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Mon 2024-02-19 15:53:44 CET; 4s ago
     Docs: man:named(8)
    Main PID: 24610 (named)
      Status: "running"
       Tasks: 6 (limit: 4622)
    Memory: 39.1M
       CPU: 45ms
    CGroup: /system.slice/named.service
            └─24610 /usr/sbin/named -f -u bind -4

feb 19 15:53:44 esclavo named[24610]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
feb 19 15:53:44 esclavo named[24610]: resolver priming query complete: success
feb 19 15:53:44 esclavo named[24610]: checkhints: b.root-servers.net/A (170.247.170.2) missing from hints
feb 19 15:53:44 esclavo named[24610]: checkhints: b.root-servers.net/A (199.9.14.201) extra record in hints
feb 19 15:53:44 esclavo named[24610]: checkhints: b.root-servers.net/AAAA (2801:1b8:10::b) missing from hints
feb 19 15:53:44 esclavo named[24610]: checkhints: b.root-servers.net/AAAA (2001:500:200::b) extra record in hints
feb 19 15:53:44 esclavo named[24610]: zone albertom.es/IN: transferred serial 2024021609
feb 19 15:53:44 esclavo named[24610]: transfer of 'albertom.es/IN' from 10.0.2.7#53: Transfer status: success
feb 19 15:53:44 esclavo named[24610]: transfer of 'albertom.es/IN' from 10.0.2.7#53: Transfer completed: 1 messages, 9 re
feb 19 15:53:44 esclavo named[24610]: zone albertom.es/IN: sending notifies (serial 2024021609)

```

Si se ha producido un error en la transferencia nos vendrá marcado al hacer el status de systemctl, puede ser debido a que la propiedad de los ficheros de zona no sea de bind sino de root. Para comprobar esto podemos usar el siguiente comando:

```
sudo ls -la /var/lib/bind/nombre_fichero_zona
```

Y comprobar si es propiedad de bind o de root, en caso de ser propiedad de root debemos cambiar la propiedad a bind con:

```
sudo chown bind:bind var/lib/bind/nombre_fichero_zona
```

Si todo ha ido correctamente se habrán transferido ambas zonas, para ello podemos de nuevo acceder a las zonas en Webmin y comprobar si se ha producido la transferencia de las zonas:

✪ Editar Zona Subordinada			
Last transferred : 19/02/24 15:53 albertom.es			
Tipo	Registros	Tipo	Registros
Dirección	3	Dirección Inversa	0
Servidor de nombre	2	Localización	0
Nombre de Alias	0	Dirección del servicio	0
Servidor de Correo	1	Clave pública	0
Información de Máquina	0	SSL Certificate	0
Texto	0	SSH Public Key	0
Sender Permitted From	1	Certificate Authority	0
DMARC	0	Name Authority	0
Servicio Acreditado	0	DNSSEC Parameters	0
Persona Responsable	0	Dirección IPv6	0

✪ Editar Zona Subordinada			
Last transferred : 19/02/24 15:52 10.0.2			
Tipo	Registros	Tipo	Registros
Dirección Inversa	3	Nombre de Alias	0
Servidor de nombre	1		

D. CONFIGURAR LA ACTUALIZACIÓN AUTOMÁTICA

Existen dos formas de funcionamiento para transferencias de zona:

- **AXFR (Transferencia Completa de Zona):** En este método, se transfiere la información completa de una zona DNS de un servidor DNS a otro.

Cuando se realiza una transferencia de zona completa, se envía todo el archivo de zona, que contiene la información completa sobre los registros de recursos (RR) para ese dominio.

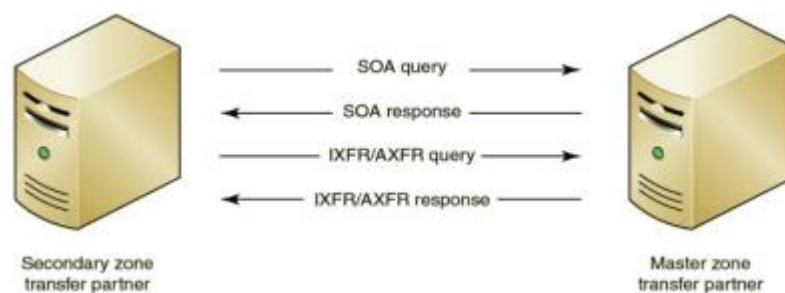
Este proceso es sencillo, pero puede consumir más ancho de banda y tiempo, especialmente en zonas con un gran número de registros.

- **IXFR (Transferencia Incremental de Zona):** En lugar de enviar toda la zona, la transferencia incremental (IXFR) se centra únicamente en las modificaciones realizadas desde la última transferencia.

El servidor DNS que solicita la información envía una solicitud indicando la última versión de la zona que posee. El servidor que tiene la zona compara esta versión con la versión actual y solo envía los cambios realizados desde la versión indicada hasta la versión más reciente.

Esto reduce significativamente la cantidad de datos transferidos, haciendo que las actualizaciones sean más eficientes en términos de ancho de banda y tiempo.

El funcionamiento paso a paso es el que se ve en la siguiente imagen:



1. Un servidor secundario inicia la transferencia de zona enviando una solicitud al servidor primario. Esta solicitud generalmente contiene una consulta SOA para obtener información sobre la zona.
2. El servidor primario responde proporcionando el registro SOA de la zona. El registro SOA contiene información crucial, incluyendo el número de serie de la zona, que se utiliza para determinar si la zona ha cambiado desde la última transferencia.

3. Si la transferencia incremental (IXFR) es compatible y se desea utilizar, el servidor secundario envía una solicitud IXFR al servidor primario. La solicitud IXFR incluirá el número de serie de la versión que posee el servidor secundario.

Si la transferencia completa (AXFR) es preferida o si el servidor primario no admite IXFR, entonces se envía una solicitud AXFR.

4. Si se solicitó IXFR, el servidor primario responde con las modificaciones realizadas desde el número de serie especificado por el servidor secundario.

Si se solicitó AXFR, el servidor primario responde enviando toda la zona.

Este proceso asegura que el servidor secundario tenga una copia actualizada de la zona DNS, ya sea transfiriendo solo las modificaciones (IXFR) o la zona completa (AXFR), según la configuración y las capacidades de los servidores involucrados. La utilización de IXFR es preferida cuando se busca eficiencia al transferir solo la información modificada en lugar de la zona completa.

Estos números de serie son el serial del SOA y en el caso de que el número sea más alto que el que tiene en su fichero de zona, el servidor secundario actualizará su fichero de zona con las modificaciones que le lleguen.

Se pueden comprobar las transferencias si se activa el registro mediante el fichero log.

Se configura en `/etc/bind/named.conf.options` añadiendo una sección logging.

```
options {
    directory "/var/cache/bind";

    dnssec-validation auto;

    listen-on-v6 { any; };
};

logging {
    channel transfers {
        file "var/log/bind/transfers" versions 3 size 10M;
        print-time yes;
        severity info;
    };
    channel notify {
        file "var/log/bind/notify" versions 3 size 10M;
        print-time yes;
        severity info;
    };
    channel general {
        file "var/log/bind/general" versions 3 size 10M;
        print-time yes;
        severity info;
    };
};
```


CONFIGURACIÓN DE UNA DELEGACIÓN DE ZONA

La configuración de la zona delegada se va a realizar a través de la modificación directa de los ficheros sin utilizar Webmin.

Para la delegación de zona necesitamos tener una nueva máquina virtual que haga de servidor DNS delegado.

El servidor primario que se ha utilizado hasta ahora será el encargado de llevar a cabo la delegación de zona.

A. CONFIGURACIONES EN EL DNS PRINCIPAL

En el fichero de zona del DNS principal tenemos que añadir dos registros:

- Un NS para asociar el subdominio que se va a delegar nombre de la máquina que ejercerá de DNS delegado
- Un A que resuelva el nombre de dominio de la máquina delegada asociándolo a su IP.

```
GNU nano 7.2 /var/lib/bind/albertom.es.hosts
$ttl 3600
albertom.es.                IN      SOA     dns1.albertom.es. admini.albertom.es. (
                               2024021609
                               3600
                               600
                               1209600
                               3600 )

albertom.es.                IN      NS      dns1.albertom.es.
dns1.albertom.es.           IN      A        10.0.2.7
albertom.es.                IN      MX       5 svrcorreo.albertom.es.
albertom.es.                IN      TXT      "v=spf1 mx ip4:10.0.2.4/24 ?all"
svrcorreo.albertom.es.       IN      A        10.0.2.15

; Transferencia de zona
albertom.es.                IN      NS      esclavo.albertom.es.
esclavo.albertom.es.         IN      A        10.0.2.8

; Delegación de zona
programacion.albertom.es.    IN      NS      delegado.albertom.es.
delegado.albertom.es.        IN      A        10.0.2.9
```

Con esto quedaría configurada la delegación de zona en el DNS principal.

B. CONFIGURACIONES EN EL DNS DELEGADO

En el DNS delegado debemos crear un fichero de zona que tenga la siguiente estructura:

- Un SOA con los datos correspondientes a esta nueva zona.
- Un NS que asocie el dominio con la máquina.
- Un A que resuelva el nombre de la máquina asociándolo a su IP.

```
$ttl 3600
programacion.albertom.es.    IN      SOA     delegado.programacion.albertom.es. admini.programacion.albertom.es. (
                               2024021609
                               3600
                               600
                               1209600
                               3600 )

programacion.albertom.es.    IN      NS      delegado.programacion.albertom.es.
delegado.programacion.albertom.es. IN      A        10.0.2.9
```

Además deberemos modificar el fichero `named.conf.local` para hacer maestro a este DNS sobre esta zona:

```
zone "programacion.albertom.es" {
    type master;
    file "/var/lib/bind/programacion.albertom.es.hosts";
};
```

Con esto ya tendremos configurada la delegación de zona.

Lo que tendremos que hacer a continuación es reiniciar el servicio `named` en ambas máquinas:

```
albertom-servidor@dns1:~$ sudo systemctl restart named.service
albertom-servidor@dns1:~$ sudo systemctl status named.service
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Tue 2024-02-20 15:27:46 CET; 1s ago
     Docs: man:named(8)
   Main PID: 2254 (named)
    Status: "running"
   Tasks: 6 (limit: 4622)
  Memory: 41.9M
     CPU: 46ms
   CGroup: /system.slice/named.service
           └─2254 /usr/sbin/named -f -u bind -4

feb 20 15:27:46 dns1 named[2254]: all zones loaded
feb 20 15:27:46 dns1 systemd[1]: Started named.service - BIND Domain Name Server.
feb 20 15:27:46 dns1 named[2254]: running
feb 20 15:27:46 dns1 named[2254]: zone albertom.es/IN: sending notifies (serial 2024021609)
feb 20 15:27:46 dns1 named[2254]: resolver priming query complete: success
feb 20 15:27:46 dns1 named[2254]: checkhints: b.root-servers.net/A (170.247.170.2) missing from hints
feb 20 15:27:46 dns1 named[2254]: checkhints: b.root-servers.net/A (199.9.14.201) extra record in hints
feb 20 15:27:46 dns1 named[2254]: checkhints: b.root-servers.net/AAAA (2801:1b8:10::b) missing from hints
feb 20 15:27:46 dns1 named[2254]: checkhints: b.root-servers.net/AAAA (2801:500:200::b) extra record in hints
feb 20 15:27:46 dns1 named[2254]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)

albertom-servidor@delegado:~$ sudo systemctl restart named.service
albertom-servidor@delegado:~$ sudo systemctl status named.service
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Tue 2024-02-20 15:30:12 CET; 4s ago
     Docs: man:named(8)
   Main PID: 2866 (named)
    Status: "running"
   Tasks: 6 (limit: 4622)
  Memory: 41.3M
     CPU: 57ms
   CGroup: /system.slice/named.service
           └─2866 /usr/sbin/named -f -u bind -4

feb 20 15:30:12 delegado named[2866]: all zones loaded
feb 20 15:30:12 delegado named[2866]: running
feb 20 15:30:12 delegado named[2866]: zone programacion.albertom.es/IN: sending notifies (serial 2024021609)
feb 20 15:30:12 delegado systemd[1]: Started named.service - BIND Domain Name Server.
feb 20 15:30:12 delegado named[2866]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
feb 20 15:30:12 delegado named[2866]: resolver priming query complete: success
feb 20 15:30:12 delegado named[2866]: checkhints: b.root-servers.net/A (170.247.170.2) missing from hints
feb 20 15:30:12 delegado named[2866]: checkhints: b.root-servers.net/A (199.9.14.201) extra record in hints
feb 20 15:30:12 delegado named[2866]: checkhints: b.root-servers.net/AAAA (2801:1b8:10::b) missing from hints
feb 20 15:30:12 delegado named[2866]: checkhints: b.root-servers.net/AAAA (2801:500:200::b) extra record in hints
```

C. COMPROBACIÓN DE FUNCIONAMIENTO DE LA ZONA DELEGADA

Para comprobar el funcionamiento de la zona delegada debemos usar la máquina virtual que creamos como cliente y realizar una consulta sobre el subdominio:

```
albertom-cliente@cliente:~$ nslookup delegado.programacion.albertom.es
Server:          10.0.2.7
Address:         10.0.2.7#53

Non-authoritative answer:
Name:   delegado.programacion.albertom.es
Address: 10.0.2.9
```

CUESTIONES FINALES

1. *¿Qué pasará si un cliente de una red diferente a la tuya intenta hacer uso de tu DNS de alguna manera, le funcionará? ¿Por qué, en qué parte de la configuración puede verse?*

No podrá acceder a nuestro DNS. Esto es debido a que en la configuración del DNS hemos hecho que sólo puedan realizar consultas los equipos de una red específica dentro de la ACL confiables.

Esto se ve en el archivo `named.conf.options` concretamente en la directiva `"allow-recursion"`. Dentro de este bloque hemos hecho referencia a una acl llamada `"confiables"` que engloba a las IPs de nuestra red.

2. *¿Por qué tenemos que permitir las consultas recursivas en la configuración?*

Permitir consultas recursivas en un servidor DNS es esencial para aprovechar la estructura jerárquica del DNS, reducir el tráfico de consultas, optimizar la experiencia del usuario y cumplir con los estándares del protocolo DNS, asegurando un funcionamiento eficiente y efectivo del sistema de resolución de nombres en Internet.

3. *El servidor DNS que acabáis de montar, ¿es autoritativo? ¿Por qué?*

Todos los DNS montados a lo largo de esta práctica son autoritativos ya que tienen acceso al fichero de zona del que son responsables.

4. *¿Dónde podemos encontrar la directiva `$ORIGIN` y para qué sirve?*

Se encuentra en los ficheros de zona y establece el dominio que debe ser añadido al final de los nombres de dominio que son relativos, es decir, todos aquellos que no son FQDN.

Un FQDN es todo aquel dominio que se considera completo, es decir, termina en `'.'`. Por ejemplo, en `dns1` sería un nombre relativo y una directiva `$ORIGIN` con valor `albertom.es.` añadiría ese dominio al final, convirtiéndolo en `dns1.albertom.es.` y, por tanto, en un FQDN.

5. *¿Una zona es idéntico a un dominio?*

No, una zona y un dominio no son idénticos, aunque están estrechamente relacionados en el contexto del sistema DNS.

Un dominio es una entidad en la estructura jerárquica del DNS, mientras que una zona es un conjunto de registros DNS que se gestiona y administra como una unidad. Aunque a menudo una zona se asocia directamente con un dominio, no son idénticos y puede haber casos donde una zona abarque solo una parte de un dominio o incluso múltiples dominios.

6. *¿Pueden editarse los archivos de zona de un servidor esclavo/secundario?*

No, estos ficheros no deben ser modificados por el administrador. En caso de necesitar alguna modificación, esta se realizará en el servidor primario y, una vez que ocurra la transferencia de zona, el servidor esclavo recibirá el fichero de zona modificado.

7. *¿Por qué podría querer tener más de un servidor esclavo para una misma zona?*

Hay diversas situaciones en las que sería conveniente tener más de un servidor esclavo para una misma zona. Por ejemplo:

- Reducir y repartir la carga entre varios servidores DNS.
- Favorecer la tolerancia a fallos.
- Ofrecer mayor rapidez.

En el caso de realizar esto, lo ideal es que los servidores DNS para una misma zona estén ubicados en redes y localizaciones diferentes para evitar que, si ocurre algún problema no les afecte simultáneamente y deje sin servicio de resolución a los nombres de esa zona.

8. *¿Cuántos servidores raíz existen?*

Existen un total de 13 servidores raíz en toda Internet y cada uno de ellos tiene múltiples copias distribuidas por todo el mundo. Cada conjunto de copias de uno de estos servidores se identifica por una misma IP.

El nombre de estos servidores tiene la forma letra.root-servers.net, donde la letra puede ser cualquiera entre la 'a' y la 'm'.

9. *¿Qué es una consulta iterativa de referencia?*

Una consulta iterativa de referencia es un tipo de consulta que se realiza a un servidor DNS para obtener la información asociada a un nombre de dominio o una dirección IP. En una consulta iterativa, el servidor DNS responde con la mejor información local que tiene, basada en los archivos de zona o la caché.

10. *En una resolución inversa, ¿a qué nombre se mapearía la dirección IP 172.16.34.56?*

Se mapearía a la dirección "56.34.16.172.in-addr.arpa." y para ello se utilizaría un RR de tipo PTR dentro de una zona de resolución inversa.