

# GUÍA DE RESOLUCIÓN DE LA TAREA 04. DNS Y LDAP.

DESPLIEGUE DE APLICACIONES WEB  
CURSO 2023/2024

## Contenido

Ejercicio 1.- DNS y Dominios. (hasta 3 puntos) (RA5.a, RA5.g) .....	3
Actividad 1.1.- Jerarquía de dominios. Explica qué son los dominios TLD, cómo se clasifican y pon ejemplos de de varios tipos. ....	3
Actividad 1.2.- Ventajas del uso de DNS. Explica las ventajas que aporta el uso de un servicio como el DNS. ....	3
Actividad 1.3.- Tipos de registros DNS. Enumera y explica los tipos de registros DNS más habituales y su finalidad.....	3
Actividad 1.4.- Uso del servicio DNS. Utilizando los comandos vistos en la unidad, averigua la IP a la que responden los siguientes dominios: .....	5
EJERCICIO 2. SERVIDOR DNS. ....	7
Actividad 2.1. Instalación de bind9.....	7
Actividad 2.2. Creación de una zona directa e inversa.....	11
Actividad 2.3. Añadiendo registros DNS a las zonas. ....	14
Actividad 2.4. Comprobando que los registros funcionan. ....	17
EJERCICIO 3. SERVIDOR LDAP.....	24
Actividad 3.1. Instalación de LDAP.....	24
Actividad 3.2. Añadir una unidad organizativa el directorio LDAP.....	29
Actividad 3.3 Añadir un grupo al directorio LDAP.....	30
Actividad 3.4. Añadir un usuario al directorio LDAP. ....	32

## Ejercicio 1.- DNS y Dominios. (RA5.a, RA5.g)

Actividad 1.1.- Jerarquía de dominios. Explica qué son los dominios TLD, cómo se clasifican y pon ejemplos de de varios tipos.

El espacio de nombres de dominio (el universo de todos los nombres de dominio) está organizado de forma jerárquica. El nivel más alto en la jerarquía es el dominio raíz, que se representa como un punto (".") y el siguiente nivel en la jerarquía se llama Dominio de Nivel Superior (TLD). Sólo hay un dominio raíz, pero hay muchos TLD y cada TLD se llama dominio secundario del dominio raíz. En este contexto, el dominio raíz es el dominio principal, ya que está un nivel por encima de un TLD y cada TLD, a su vez, pueden tener muchos dominios hijos.

Sólo hay una raíz de dominio, pero hay más de 250 dominios de nivel superior, clasificados en los siguientes tres tipos:

- TLD de código de país (ccTLD): dominios asociados con países y territorios. Hay más de 240 ccTLD. Están formados por 2 letras, por ejemplo: es, uk, en, y jp.
- Dominios de nivel superior genéricos (gTLD): están formados por 3 o más letras. A su vez se subdividen en:
  - Dominios de internet patrocinados (sTLD): representan una comunidad de intereses, es decir, detrás existe una organización u organismo público que propone el dominio y establece las reglas para optar a dicho dominio. Por ejemplo: edu, gov, int, mil, aero, museum.
  - Dominios de internet no patrocinados (uTLD). Sin una organización detrás que establezca las reglas para optar a dicho dominio. La lista de gTLD incluye: com, net, org, biz, info.

Actividad 1.2.- Ventajas del uso de DNS. Explica las ventajas que aporta el uso de un servicio como el DNS.

Podemos resumir las ventajas de la configuración y empleo de un servidor DNS en las siguientes:

- Desaparece la carga excesiva en la red y en los hosts: ahora la información está distribuida por toda la red, al tratarse de una base de datos distribuida.
- No hay duplicidad de nombres: el problema se elimina debido a la existencia de dominios controlados por un único administrador. Puede haber nombres iguales, pero en dominios diferentes.
- Consistencia de la información: ahora la información que está distribuida es actualizada automáticamente sin intervención de ningún administrador.

Actividad 1.3.- Tipos de registros DNS. Enumera y explica los tipos de registros DNS más habituales y su finalidad.

Registro	Descripción, sintaxis y ejemplo
A	<b>Descripción:</b> Address (Dirección). Este registro se usa para traducir nombres de hosts a direcciones IP versión 4. <b>Sintaxis:</b> <i>propietario clase ttl A IP_version4</i> . <b>Ejemplo:</b> host1.ejemplo.com IN A 127.0.0.1.
AAAA	<b>Descripción:</b> Address (Dirección). Este registro se usa para traducir nombres de hosts a direcciones IP versión 6. <b>Sintaxis:</b> <i>propietario clase ttl AAAA IP_version6</i> . <b>Ejemplo:</b> host1ipv6.ejemplo.com. IN AAAA 1234:0:1:2:3:4:567:89ab.
CNAME	<b>Descripción:</b> Canonical Name (Nombre Canónico). Se usa para crear nombres de

Registro	Descripción, sintaxis y ejemplo
	<p>hosts adicionales, o alias. Hay que tener en cuenta que el nombre de host al que el alias referencia debe haber sido definido previamente como registro tipo "A". Comúnmente usado cuando un servidor con una sola dirección IP ejecuta varios servicios, como: ftp, web... y cada servicio tiene su propia entrada DNS. También es utilizado cuando el servidor web aloja distintos dominios en una misma IP (virtualhosts).</p> <p><b>Sintaxis:</b> <i>propietario ttl clase CNAME nombreCanónico.</i></p> <p><b>Ejemplo:</b> <code>nombrealias.ejemplo.com CNAME nombreverdadero.ejemplo.com.</code></p> <p>Como se ha comentado anteriormente <code>nombreverdadero.ejemplo.com</code> previamente debe estar definido como registro tipo A.</p>
NS	<p><b>Descripción:</b> Name Server (Servidor de Nombres). Indica qué servidores de nombres tienen total autoridad sobre un dominio concreto. Cada dominio se puede asociar a una cantidad cualquiera de servidores de nombres.</p> <p><b>Sintaxis:</b> <i>propietario ttl IN NS nombreServidorNombreDominio.</i></p> <p><b>Ejemplo:</b> <code>ejemplo.com. IN NS nombreservidor1.ejemplo.com.</code></p>
MX	<p><b>Descripción:</b> Mail eXchange (Registro de Intercambio de Correo). Asocia un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio.</p> <p><b>Sintaxis:</b> <i>propietario ttl clase MX preferencia hostIntercambiadorDeCorreo.</i></p> <p><b>Ejemplo:</b> <code>ejemplo.com. MX 10 servidorcorreo1.ejemplo.com.</code></p> <p>El número, en este caso 10, indica la preferencia, y tiene sentido en caso de existir varios servidores de correo. A menor número mayor preferencia.</p>
PTR	<p><b>Descripción:</b> Pointer (Indicador). Traduce direcciones IP en nombres de dominio. También conocido como 'registro inverso', ya que funciona a la inversa del registro "A".</p> <p><b>Sintaxis:</b> <i>propietario ttl clase PTR nombreDominioDestino.</i></p> <p><b>Ejemplo:</b> <code>1.0.0.10.in-addr.arpa. PTR host.ejemplo.com.</code></p>
SOA	<p><b>Descripción:</b> Start Of Authority (Autoridad de la zona). Proporciona información sobre el servidor DNS primario de la zona.</p> <p><b>Sintaxis:</b> <i>propietario clase SOA servidorNombres personaResponsable (numeroSerie intervaloActualización intervaloReintento caducidad tiempoDeVidaMínimo).</i></p> <p><b>Ejemplo:</b></p> <pre> @ IN SOA nombreServidor.ejemplo.com. postmaster.ejemplo.com. (     1 ; número de serie     3600 ; actualizar [1h]     600 ; reintentar [10m]     86400 ; caducar [1d]     3600 ) ; TTL mínimo [1h] </pre> <p>El propietario (servidor DNS principal) se especifica como "@" porque el nombre de dominio es el mismo que el origen de todos los datos de la zona (<code>ejemplo.com</code>). Se trata de una convención de nomenclatura estándar para registros de recursos y se utiliza más a menudo en los registros SOA. El número de serie es el número de versión de esta base de datos. Debes incrementar este número cada vez que modificas la base de datos.</p>

Registro	Descripción, sintaxis y ejemplo
TXT	<p><b>Descripción:</b> TeXT (Información textual). Permite a los dominios identificarse de modos arbitrarios.</p> <p><b>Sintaxis:</b> <i>propietario ttl clase TXT cadenaDeTexto</i>.</p> <p><b>Ejemplo:</b> ejemplo.com. TXT "Ejemplo de información de nombre de dominio adicional."</p>
SPF	<p><b>Descripción:</b> Sender Policy Framework. Es un registro de tipo TXT que va creado en una zona directa del DNS, en la cual se ponen las informaciones del propio servidor de correo con la sintaxis SPF. Se utiliza para evitar el envío de correos suplantando identidades. Por lo tanto, ayuda a combatir el SPAM, ya que, en este registro se especifica qué hosts están autorizados a enviar correo desde el dominio dado. El servidor que recibe, consulta el DNS para comparar la IP desde la cual le llega, con los datos de este registro.</p> <p><b>Sintaxis:</b> <i>propietario ttl clase IN SPF cadenaDeTexto</i>.</p> <p><b>Ejemplo:</b> ejemplo.com IN SPF "v=spf1 a:mail.ejemplo.com -all".</p>

Actividad 1.4.- Uso del servicio DNS. Utilizando los comandos vistos en la unidad, averigua la IP a la que responden los siguientes dominios:

[www.educacionyfp.gob.es](http://www.educacionyfp.gob.es)

```
profesor@profesoradodaw:/etc/default$ nslookup www.educacionyfp.gob.es
Server:      192.168.0.27
Address:     192.168.0.27#53

Non-authoritative answer:
Name:   www.educacionyfp.gob.es
Address: 212.128.114.28

profesor@profesoradodaw:/etc/default$ dig www.educacionyfp.gob.es

; <>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <>> www.educacionyfp.gob.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 24319
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 5ce63809007b49b50100000065dc6871ed6f8d41cb8a582d (good)
;; QUESTION SECTION:
;www.educacionyfp.gob.es.      IN      A

;; ANSWER SECTION:
www.educacionyfp.gob.es. 3592  IN      A      212.128.114.28

;; Query time: 0 msec
;; SERVER: 192.168.0.27#53(192.168.0.27) (UDP)
;; WHEN: Mon Feb 26 11:31:13 CET 2024
;; MSG SIZE  rcvd: 96
```

[www.juntaandalucia.es](http://www.juntaandalucia.es)

```
profesor@profesoradodaw:/etc/default$ nslookup www.juntaandalucia.es
Server:      192.168.0.27
Address:     192.168.0.27#53

Non-authoritative answer:
Name:   www.juntaandalucia.es
Address: 64.190.63.222

profesor@profesoradodaw:/etc/default$ dig www.juntaandalucia.es

; <>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <>> www.juntaandalucia.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44231
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 721c3ed0b79c33c1010000006dc680e9e748ea57a55eda2 (good)
;; QUESTION SECTION:
;www.juntaandalucia.es.      IN      A

;; ANSWER SECTION:
www.juntaandalucia.es.  291      IN      A      64.190.63.222

;; Query time: 0 msec
;; SERVER: 192.168.0.27#53(192.168.0.27) (UDP)
;; WHEN: Mon Feb 26 11:29:34 CET 2024
;; MSG SIZE  rcvd: 94
```

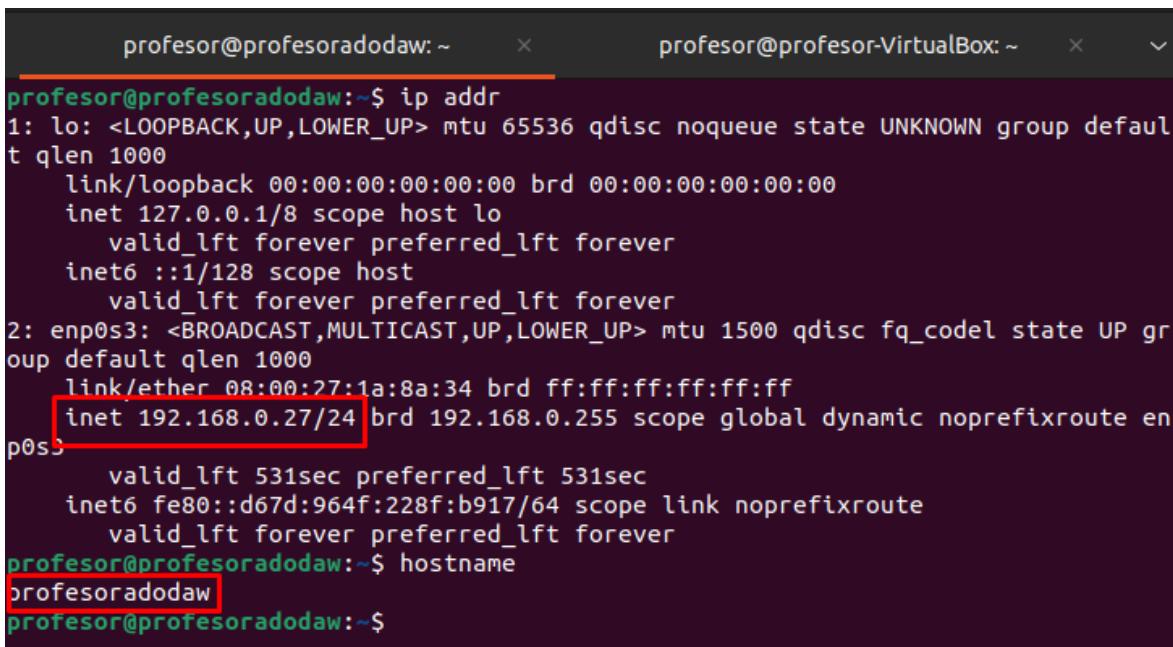
## EJERCICIO 2. SERVIDOR DNS.

### Actividad 2.1. Instalación de bind9.

Realiza la instalación del servicio DNS en Linux (bind9) y configura la interfaz de red para indicarle que el servidor DNS preferido será nuestra propia máquina. Es conveniente (aunque no imprescindible) que configures la interfaz de red como estática. Comprueba que el servicio está funcionando y que el puerto está accesible.

Para una instalación del servidor DNS BIND en Linux Ubuntu 22s realiza el siguiente procedimiento como usuario **root**, teniendo en cuenta que el servidor está identificado como sigue:

- Hostname: **profesoradodaw**
- IP: **192.168.0.27**

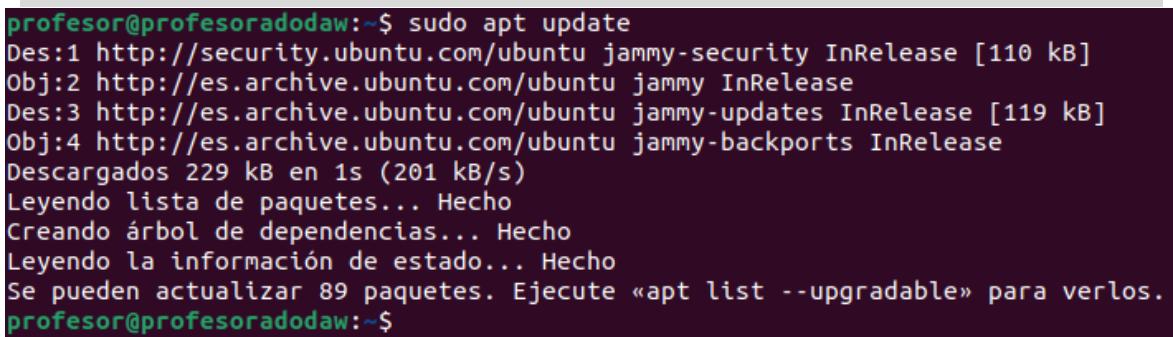


The screenshot shows two terminal windows side-by-side. The left window is titled 'profesor@profesoradodaw: ~' and the right window is titled 'profesor@profesor-VirtualBox: ~'. Both windows have a close button 'x' and a dropdown arrow. In the left window, the command 'ip addr' is run, showing network interfaces. The 'enp0s3' interface is highlighted with a red box, showing its MAC address (08:00:27:1a:8a:34), broadcast address (ff:ff:ff:ff:ff:ff), and assigned IP address (inet 192.168.0.27/24). The right window shows the command 'hostname' output, which is 'profesoradodaw'.

```
profesor@profesoradodaw:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1a:8a:34 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.27/24 brd 192.168.0.255 scope global dynamic noprefixroute enp0s3
        valid_lft 531sec preferred_lft 531sec
        inet6 fe80::d67d:964f:228f:b917/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
profesor@profesoradodaw:~$ hostname
profesoradodaw
profesor@profesoradodaw:~$
```

#### Paso 1. Actualizar los repositorios:

```
$ apt update ó $ apt-get update
```



The screenshot shows a single terminal window with the command 'sudo apt update' run. The output shows the download of several packages from the 'jammy' repository, including 'jammy-security', 'jammy', 'jammy-updates', and 'jammy-backports'. It also shows the creation of dependency trees and a message indicating 89 upgradeable packages.

```
profesor@profesoradodaw:~$ sudo apt update
Des:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Obj:2 http://es.archive.ubuntu.com/ubuntu jammy InRelease
Des:3 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Obj:4 http://es.archive.ubuntu.com/ubuntu jammy-backports InRelease
Descargados 229 kB en 1s (201 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 89 paquetes. Ejecute «apt list --upgradable» para verlos.
profesor@profesoradodaw:~$
```

## Paso 2. Instalar los paquetes necesarios para el correcto funcionamiento de BIND:

```
$ apt-get install bind9 bind9utils
```

```
profesor@profesoradodaw:~$ sudo apt install bind9 bind9utils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
  linux-headers-6.2.0-37-generic linux-hwe-6.2-headers-6.2.0-37
  linux-image-6.2.0-37-generic linux-modules-6.2.0-37-generic
  linux-modules-extra-6.2.0-37-generic
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  bind9-utils
Paquetes sugeridos:
  bind-doc resolvconf
Se instalarán los siguientes paquetes NUEVOS:
  bind9 bind9-utils bind9utils
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 89 no actualizados.
Se necesita descargar 426 kB de archivos.
Se utilizarán 1.722 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

NOTA: La instalación crea el usuario **bind** que ejecuta el servicio dns denominado **named**.

## Paso 3. Verificamos que el servidor DNS está activo:

```
$ service bind9 status $ /etc/init.d/named status $ systemctl status bind9
```

```
profesor@profesoradodaw:~$ sudo systemctl status bind9
● named.service - BIND Domain Name Server
  Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2024-02-22 11:35:59 CET; 1min 37s ago
    Docs: man:named(8)
    Process: 5648 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 5649 (named)
     Tasks: 5 (limit: 2260)
    Memory: 7.1M
      CPU: 52ms
     CGroup: /system.slice/named.service
             └─5649 /usr/sbin/named -u bind
```

```
profesor@profesoradodaw:~$ sudo systemctl status named
● named.service - BIND Domain Name Server
  Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2024-02-22 11:35:59 CET; 2min 4s ago
    Docs: man:named(8)
    Process: 5648 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 5649 (named)
     Tasks: 5 (limit: 2260)
    Memory: 7.1M
      CPU: 53ms
     CGroup: /system.slice/named.service
             └─5649 /usr/sbin/named -u bind
```

## Paso 4. Verifica en qué puertos TCP y UDP está activo el servidor bind9, para ello comprueba el servicio named:

```
$ netstat -natp | grep named
```

```
$ netstat -naup | grep named
```

```

profesor@profesoradodaw:~$ sudo netstat -natp | grep named
tcp      0      0 127.0.0.1:53          0.0.0.0:*                  ESCUCHAR   5649/named
tcp      0      0 127.0.0.1:953        0.0.0.0:*                  ESCUCHAR   5649/named
tcp      0      0 192.168.0.27:53      0.0.0.0:*                  ESCUCHAR   5649/named
tcp6     0      0 ::1:953            ::*:*                   ESCUCHAR   5649/named
tcp6     0      0 fe80::d67d:964f:228f:53  ::*:*                 ESCUCHAR   5649/named
tcp6     0      0 ::1:53             ::*:*                   ESCUCHAR   5649/named
profesor@profesoradodaw:~$ sudo netstat -naup | grep named
udp     0      0 192.168.0.27:53      0.0.0.0:*                  5649/named
udp     0      0 127.0.0.1:53        0.0.0.0:*                  5649/named
udp6    0      0 ::1:53             ::*:*                   5649/named
udp6    0      0 fe80::d67d:964f:228f:53  ::*:*                 5649/named
profesor@profesoradodaw:~$ 

```

## Paso 5. Arrancar, parar y comprobar el estado de nuestro servidor DNS BIND9

```

$ systemctl stop named.service
$ systemctl status named.service
$ systemctl start named.service
$ systemctl status named.service

```

```

profesor@profesoradodaw:~$ sudo systemctl stop named
profesor@profesoradodaw:~$ sudo systemctl status named
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Thu 2024-02-22 11:40:45 CET; 5s ago
     Docs: man:named(8)
  Process: 5648 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
  Process: 6255 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 5649 (code=exited, status=0/SUCCESS)
    CPU: 78ms

feb 22 11:40:45 profesor-VirtualBox named[5649]: no longer listening on 127.0.0.1#53
feb 22 11:40:45 profesor-VirtualBox named[5649]: no longer listening on 192.168.0.27#53
feb 22 11:40:45 profesor-VirtualBox named[5649]: no longer listening on ::1#53
feb 22 11:40:45 profesor-VirtualBox named[5649]: no longer listening on fe80::d67d:964f:228f:b917%2#53
feb 22 11:40:45 profesor-VirtualBox named[5649]: shutting down: flushing changes
feb 22 11:40:45 profesor-VirtualBox named[5649]: stopping command channel on 127.0.0.1#953
feb 22 11:40:45 profesor-VirtualBox named[5649]: stopping command channel on ::1#953
feb 22 11:40:45 profesor-VirtualBox named[5649]: exiting
feb 22 11:40:45 profesor-VirtualBox systemd[1]: named.service: Deactivated successfully.
feb 22 11:40:45 profesor-VirtualBox systemd[1]: Stopped BIND Domain Name Server.

```

```

profesor@profesoradodaw:~$ sudo systemctl start named
profesor@profesoradodaw:~$ sudo systemctl status named
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-02-22 11:41:01 CET; 1s ago
     Docs: man:named(8)
  Process: 6266 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 6267 (named)
   Tasks: 4 (limit: 2260)
   Memory: 5.4M
      CPU: 45ms
     CGroup: /system.slice/named.service
             └─6267 /usr/sbin/named -u bind

feb 22 11:41:01 profesor-VirtualBox named[6267]: network unreachable resolving './DNSKEY/IN': 2001:503:c27::2
feb 22 11:41:01 profesor-VirtualBox named[6267]: network unreachable resolving './NS/IN': 2001:503:c27::2
feb 22 11:41:01 profesor-VirtualBox named[6267]: network unreachable resolving './DNSKEY/IN': 2001:500:2d::1
feb 22 11:41:01 profesor-VirtualBox named[6267]: network unreachable resolving './NS/IN': 2001:500:2d::1
feb 22 11:41:02 profesor-VirtualBox named[6267]: managed-keys-zone: Key 20326 for zone . is now trusted (...)
feb 22 11:41:02 profesor-VirtualBox named[6267]: resolver priming query complete: success
feb 22 11:41:02 profesor-VirtualBox named[6267]: checkhints: b.root-servers.net/A (170.247.170.2) missing
feb 22 11:41:02 profesor-VirtualBox named[6267]: checkhints: b.root-servers.net/A (199.9.14.201) extra re...
feb 22 11:41:02 profesor-VirtualBox named[6267]: checkhints: b.root-servers.net/AAAA (2801:1b8:10::b) miss...
feb 22 11:41:02 profesor-VirtualBox named[6267]: checkhints: b.root-servers.net/AAAA (2001:500:200::b) ex...

```

- Modificamos el archivo resolv.conf:

```
profesor@profesoradodaw: /etc/default      x      profesor@profesor-VirtualBox: ~
GNU nano 6.2          /etc/resolv.conf
# This is /run/systemd/resolve/stub-resolv.conf managed by man:sys
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're look
# /etc/resolv.conf and seeing this text, you have followed the sy
#
# This is a dynamic resolv.conf file for connecting local clients
# internal DNS stub resolver of systemd-resolved. This file lists
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS serv
# currently in use.
#
# Third party programs should typically not access this file direc
# through the symlink at /etc/resolv.conf. To manage man:resolv.co
# different way, replace this symlink by a static file or a differ
#
# See man:systemd-resolved.service(8) for details about the support
# operation for /etc/resolv.conf.
#nameserver 127.0.0.53
nameserver 192.168.0.27
options edns0 trust-ad
search fpad.com
```

Si reiniciamos, posiblemente habría que modificar de nuevo este archivo.

## Actividad 2.2. Creación de una zona directa e inversa.

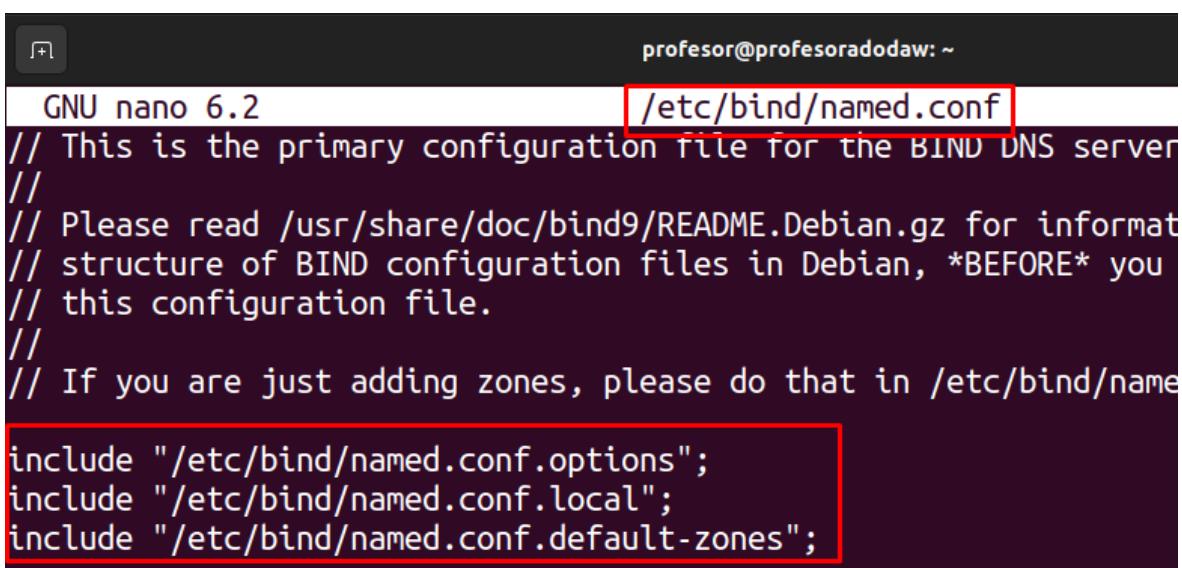
Configura el servidor como un servidor DNS principal y realiza la configuración necesaria para que gestione una zona directa (**fpad.db**) y una inversa (**fpad.rev**) para el dominio **fpad.com**.

Tras la instalación del servidor DNS BIND (**bind9**) existe la ruta **/etc/bind**, la cual contiene sus ficheros de configuración. Una estructura tipo **/etc/bind** que puedes encontrar al instalar bind sería similar a la que se muestra en la siguiente imagen:

```
profesor@profesoradodaw:~$ ls /etc/bind -l
total 48
-rw-r--r-- 1 root root 2403 feb 12 20:29 bind.keys
-rw-r--r-- 1 root root 237 sep 21 00:15 db.0
-rw-r--r-- 1 root root 271 abr 12 2023 db.127
-rw-r--r-- 1 root root 237 abr 12 2023 db.255
-rw-r--r-- 1 root root 353 abr 12 2023 db.empty
-rw-r--r-- 1 root root 270 abr 12 2023 db.local
-rw-r--r-- 1 root bind 463 sep 21 00:15 named.conf
-rw-r--r-- 1 root bind 498 abr 12 2023 named.conf.default-zones
-rw-r--r-- 1 root bind 165 abr 12 2023 named.conf.local
-rw-r--r-- 1 root bind 846 abr 12 2023 named.conf.options
-rw-r----- 1 bind bind 100 feb 22 11:35 rndc.key
-rw-r--r-- 1 root root 1317 abr 12 2023 zones.rfc1918
profesor@profesoradodaw:~$
```

Si editamos el fichero **/etc/bind/named.conf**, podemos ver que hace referencia a 3 ficheros de configuración:

```
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```



```
GNU nano 6.2 /etc/bind/named.conf
// This is the primary configuration file for the BIND DNS server
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information
// structure of BIND configuration files in Debian, *BEFORE* you
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

- **/etc/bind/named.conf.options**: hace referencia al archivo de configuración que posee opciones genéricas.
- **/etc/bind/named.conf.local**: hace referencia al archivo de configuración para opciones

particulares.

- **/etc/bind/named.conf.default-zones**: hace referencia al archivo de configuración de zonas.

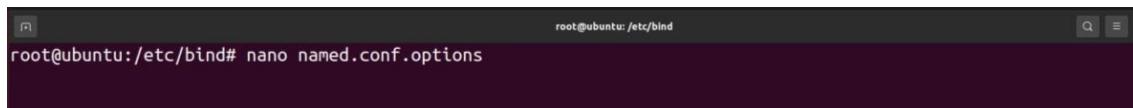
Dentro de cada uno de estos archivos encontrarás partes de código agrupadas entre llaves que finalizan con el carácter punto y coma (;), conocidos como **declaraciones**, las cuales indicarán **secciones de ejecución**. Cualquier código en un archivo de configuración que comience con los caracteres doble barra (//), almohadilla (#) o aparezca encerrado entre barra asterisco /\*) y asterisco barra (\*/) son considerados comentarios y por lo tanto no se ejecuta.

Puedes modificar los ficheros de configuración a tu antojo. Así, puedes crear incluso nuevos ficheros de configuración que sean llamados desde otros mediante la directiva **include**.

Antes de crear las zonas, vamos a configurar nuestro servidor DNS como servidor primario y le vamos a añadir la dirección de los ‘forwarders’, que se encargarán de resolver las peticiones que no estén configuradas en nuestro servidor principal. Para ello tenemos que modificar la configuración de un par de ficheros.

- En primer lugar, editaremos el fichero **/etc/bind/named.conf.options**:

```
$ sudo nano /etc/bind/named.conf.options
```



A screenshot of a terminal window on a dark background. The window title is 'root@ubuntu:/etc/bind#'. The command 'sudo nano /etc/bind/named.conf.options' is being typed into the terminal. The cursor is at the end of the command line.

- A continuación, buscaremos dentro del bloque ‘options’, un bloque ‘forwarders’ e incluiremos las direcciones de los DNS de Google:

```
forwarders {
```

```
    8.8.8.8;
```

```
    8.8.4.4;
```

```
};
```

```

GNU nano 6.2                               /etc/bind/named.conf.options *
options {
    directory "/var/cache/bind";

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

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

    // forwarders {
    //     0.0.0.0;
    // };
forwarders {
    8.8.8.8;
    8.8.4.4;
};

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

listen-on-v6 { any; };

};
```

- Guardamos y salimos.

Ahora vamos a configurar el fichero **/etc/bind/named.conf.local** para indicar qué zonas son servidas por el servidor, qué zonas son servidas como máster y el fichero donde se guarda el contenido de la zona. Crearemos una zona que se llamará **fpad.com**, que será de tipo máster y luego la configuraremos:

- Editamos el fichero **/etc/bind/named.conf.local**

**\$ sudo nano /etc/bind/named.conf.local**

- Vamos a incluir la configuración:

```

zone "fpad.com" {
    type master;
    file "/etc/bind/fpad.db";
};

zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/fpad.rev";
};
```

```

GNU nano 6.2                               /etc/bind/named.conf.local
//                                         //
// Do any local configuration here          //
//                                         //
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "fpad.com" {
    type master;
    file "/etc/bind/fpad.db";
};

zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/fpad.rev";
};

```

[Recuerda que el nombre de la zona inversa se forma con la ip de tu servidor leída de derecha a izquierda y cambiando el último octeto por ‘in-addr.arpa’ ]

- Guardamos y salimos.

*Se puede o debe realizar una comprobación con named-checkconf*

### Actividad 2.3. Añadiendo registros DNS a las zonas.

Edita los ficheros de zona directa e inversa y crea los registros necesarios para que el servidor resuelva lo siguiente:

- Un servidor web llamado [www.fpad.com](http://www.fpad.com)
- Un servidor ftp llamado ftp.fpad.com
- Un servidor de correo llamado mail.fpad.com
- El servidor web también se puede llamar por alumno.fpad.com.
  
- Creamos el fichero de **zona fpad.db**:

**\$ sudo nano /etc/bind/fpad.db**

- El contenido que tendrá nuestro fichero es el siguiente:

```

GNU nano 6.2                               /etc/bind/fpad.db
$TTL    604800
@       IN      SOA    ns1.fpad.com. root.fpad.com. (
                           1           ;Serial
                           604800     ;Refresh
                           86400      ;Retry
                           24192000   ;Expire
                           604800 )    ;Negative Cache TTL
;
@       IN      NS     ns1.fpad.com.
@       IN      MX     10    mail.fpad.com
ns1.fpad.com.  IN      A      192.168.0.27
mail.fpad.com. IN      A      192.168.0.28
ftp      IN      A      192.168.0.29
www     IN      A      192.168.0.30
alumno  IN      CNAME  www

```

```

$TTL 604800
@   IN  SOA  ns1.fpad.com. root.fpad.com.(
                           1           ;Serial
                           604800     ;Refresh
                           86400      ;Retry
                           24192000   ;Expire
                           604800 )    ;Negative Cache TTL
;
@   IN  NS   ns1.fpad.com.
@   IN  MX   10  mail.fpad.com
ns1.fpad.com. IN  A  192.168.0.27
mail.fpad.com. IN  A  192.168.0.28
ftp   IN  A  192.168.0.29
www   IN  A  192.168.0.30
alumno IN  CNAME  www

```

- Creamos el fichero de ***zona inversa fpad.rev***:

***\$ sudo nano /etc/bind/fpad.rev***

- El contenido que tendrá nuestro fichero es el siguiente:

```

GNU nano 6.2                               /etc/bind/fpad.rev
$TTL 604800
@ IN SOA ns1.fpad.com. root.fpad.com. (
    1 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ); Negative Cache TTL
;
@ IN NS ns1.fpad.com.
27.0.168.192.in-addr.arpa. IN PTR ns1.fpad.com.
28.0.168.192.in-addr.arpa. IN PTR mail.fpad.com.
29 IN PTR ftp.fpad.com.
30 IN PTR www.fpad.com.

```

```

$TTL 604800
@ IN SOA ns1.fpad.com. root.fpad.com. (
    1 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ); Negative Cache TTL
;
@ IN NS ns1.fpad.com.
27.0.168.192.in-addr.arpa. IN PTR ns1.fpad.com.
28.0.168.192.in-addr.arpa. IN PTR mail.fpad.com.
29 IN PTR ftp.fpad.com.
30 IN PTR www.fpad.com.

```

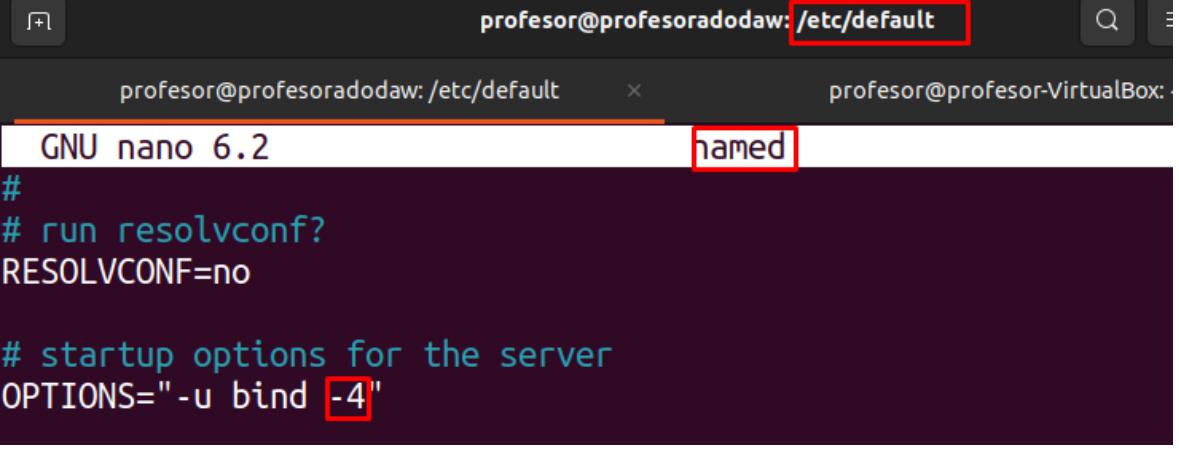
- Reiniciamos el servicio y comprobamos el estado:

```

profesor@profesoradodaw:/etc/default$ service bind9 restart
profesor@profesoradodaw:/etc/default$ service bind9 status
● named.service - BIND Domain Name Server
    Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor>
    Active: active (running) since Mon 2024-02-26 10:48:22 CET; 3s ago
      Docs: man:named(8)
    Process: 20030 ExecStart=/usr/sbin/named $OPTIONS (code=exited, sta>
   Main PID: 20032 (named)
     Tasks: 4 (limit: 2260)
    Memory: 5.2M
       CPU: 38ms
      CGroup: /system.slice/named.service
              └─20032 /usr/sbin/named -u bind -4

```

Opcional: para evitar advertencias relacionadas con direcciones IPv6 en el status de bind9, modificar el archivo /etc/default/named



```
profesor@profesoradodaw: /etc/default
profesor@profesoradodaw: /etc/default          x      profesor@profesor-VirtualBox:
GNU nano 6.2                                     named
#
# run resolvconf?
RESOLVCONF=no

# startup options for the server
OPTIONS="-u bind -4"
```

#### Actividad 2.4. Comprobando que los registros funcionan.

Realiza la comprobación de los ficheros de zona con named checkzone y realiza la consulta de registros tanto directa como inversa (nslookup, dig,...).

```
profesor@profesoradodaw: /etc/default$ named-checkconf /etc/bind/named.conf
profesor@profesoradodaw: /etc/default$ named-checkconf /etc/bind/named.conf.local
profesor@profesoradodaw: /etc/default$ named-checkconf /etc/bind/named.conf.options
profesor@profesoradodaw: /etc/default$ named-checkzone fpad.com /etc/bind/fpad.db
zone fpad.com/IN: loaded serial 1
OK
profesor@profesoradodaw: /etc/default$ named-checkzone 0.168.192.in-addr.arpa /etc/bind/fpad.rev
zone 0.168.192.in-addr.arpa/IN: loaded serial 1
OK
profesor@profesoradodaw: /etc/default$
```

#### Nslookup

- Comprobamos si nos resuelve el dominio y si la ip del servidor que responde es la ip de nuestro servidor (192.168.0.27) o es la ip interna (127.0.0.53):

```
$ nslookup ns1.fpad.com
$ nslookup mail.fpad.com
$ nslookup ftp.fpad.com
$ nslookup www.fpad.com
$ nslookup alumno.fpad.com
```

```
profesor@profesoradodaw:/etc/default$ nslookup ns1.fpad.com
Server:      192.168.0.27
Address:     192.168.0.27#53

Name: ns1.fpad.com
Address: 192.168.0.27

profesor@profesoradodaw:/etc/default$ nslookup mail.fpad.com
Server:      192.168.0.27
Address:     192.168.0.27#53

Name: mail.fpad.com
Address: 192.168.0.28

profesor@profesoradodaw:/etc/default$ nslookup ftp.fpad.com
Server:      192.168.0.27
Address:     192.168.0.27#53

Name: ftp.fpad.com
Address: 192.168.0.29

profesor@profesoradodaw:/etc/default$ nslookup www.fpad.com
Server:      192.168.0.27
Address:     192.168.0.27#53

Name: www.fpad.com
Address: 192.168.0.30

profesor@profesoradodaw:/etc/default$ nslookup alumno.fpad.com
Server:      192.168.0.27
Address:     192.168.0.27#53

alumno.fpad.com canonical name = www.fpad.com.
Name: www.fpad.com
Address: 192.168.0.30

profesor@profesoradodaw:/etc/default$
```

```
$ nslookup 192.168.0.27  
$ nslookup 192.168.0.28  
$ nslookup 192.168.0.29  
$ nslookup 192.168.0.30
```

```
profesor@profesoradodaw:/etc/default      profesor@profesor-VirtualBox: ~  
profesor@profesoradodaw:/etc/default$ nslookup 192.168.0.27  
27.0.168.192.in-addr.arpa      name = ns1.fpad.com.  
  
profesor@profesoradodaw:/etc/default$ nslookup 192.168.0.28  
28.0.168.192.in-addr.arpa      name = mail.fpad.com.  
  
profesor@profesoradodaw:/etc/default$ nslookup 192.168.0.29  
29.0.168.192.in-addr.arpa      name = ftp.fpad.com.  
  
profesor@profesoradodaw:/etc/default$ nslookup 192.168.0.30  
30.0.168.192.in-addr.arpa      name = www.fpad.com.  
  
profesor@profesoradodaw:/etc/default$
```

Como vemos, la ip del servidor que nos responde es la correcta, la 192.168.0.27, y además nos resuelve tanto de forma directa como inversa.

*Lanzamos consultas con el comando DIG:*

```
$ dig ns1.fpad.com  
$ dig mail.fpad.com  
$ dig ftp.fpad.com  
$ dig alumno.fpad.com  
$ dig www.fpad.com
```

```
profesor@profesoradodaw:/etc/default$ dig ns1.fpad.com  
  
; <>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <>> ns1.fpad.com  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51066  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 1232  
; COOKIE: 7fb96bac10b537870100000065dc615fd70b9d7ab1f2a3bc (good)  
;; QUESTION SECTION:  
;ns1.fpad.com.           IN      A  
  
;; ANSWER SECTION:  
ns1.fpad.com.       604800  IN      A      192.168.0.27  
  
;; Query time: 0 msec  
;; SERVER: 192.168.0.27#53(192.168.0.27) (UDP)  
;; WHEN: Mon Feb 26 11:01:03 CET 2024  
;; MSG SIZE  rcvd: 85
```

```
profesor@profesoradodaw:/etc/default$ dig mail.fpad.com

; <>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <>> mail.fpad.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58178
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 509341cd24c08b780100000065dc62513a3150f561cc6543 (good)
;; QUESTION SECTION:
;mail.fpad.com.           IN      A

;; ANSWER SECTION:
mail.fpad.com.       604800  IN      A      192.168.0.28

;; Query time: 0 msec
;; SERVER: 192.168.0.27#53(192.168.0.27) (UDP)
;; WHEN: Mon Feb 26 11:05:05 CET 2024
;; MSG SIZE  rcvd: 86

profesor@profesoradodaw:/etc/default$ dig ftp.fpad.com

; <>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <>> ftp.fpad.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47768
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 2fb9896c1ca9cecf0100000065dc625628a50945e118d208 (good)
;; QUESTION SECTION:
;ftp.fpad.com.           IN      A

;; ANSWER SECTION:
ftp.fpad.com.       604800  IN      A      192.168.0.29

;; Query time: 0 msec
;; SERVER: 192.168.0.27#53(192.168.0.27) (UDP)
;; WHEN: Mon Feb 26 11:05:10 CET 2024
;; MSG SIZE  rcvd: 85
```

```
profesor@profesoradodaw:/etc/default$ dig alumno.fpad.com

; <>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <>> alumno.fpad.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25142
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 4e40cfcc53dd1c720100000065dc625a180b1c78925ce520 (good)
;; QUESTION SECTION:
;alumno.fpad.com.           IN      A

;; ANSWER SECTION:
alumno.fpad.com.      604800  IN      CNAME   www.fpad.com.
www.fpad.com.          604800  IN      A       192.168.0.30

;; Query time: 0 msec
;; SERVER: 192.168.0.27#53(192.168.0.27) (UDP)
;; WHEN: Mon Feb 26 11:05:14 CET 2024
;; MSG SIZE rcvd: 106
```

```
profesor@profesoradodaw:/etc/default$ dig www.fpad.com

; <>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <>> www.fpad.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 132
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 3a328b9d4d4bd62c0100000065dc61a451340ae0d6bd6354 (good)
;; QUESTION SECTION:
;www.fpad.com.           IN      A

;; ANSWER SECTION:
www.fpad.com.      604800  IN      A       192.168.0.30

;; Query time: 0 msec
;; SERVER: 192.168.0.27#53(192.168.0.27) (UDP)
;; WHEN: Mon Feb 26 11:02:12 CET 2024
;; MSG SIZE rcvd: 85

profesor@profesoradodaw:/etc/default$
```

```
$ dig 192.168.0.27
$ dig 192.168.0.28
$ dig 192.168.0.29
$ dig 192.168.0.30
```

```
profesor@profesoradodaw:/etc/default$ dig 192.168.0.27

; <>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <>> 192.168.0.27
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 25367
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 89c92c32798492a70100000065dc61d2b60cf1bf41a8c020 (good)
;; QUESTION SECTION:
;192.168.0.27.           IN      A

;; AUTHORITY SECTION:
.          10800  IN      SOA      a.root-servers.net. nstl
d.verisign-grs.com. 2024022600 1800 900 604800 86400

;; Query time: 44 msec
;; SERVER: 192.168.0.27#53(192.168.0.27) (UDP)
;; WHEN: Mon Feb 26 11:02:58 CET 2024
;; MSG SIZE  rcvd: 144

profesor@profesoradodaw:/etc/default$ dig 192.168.0.28

; <>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <>> 192.168.0.28
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 28654
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 6310ce813a8bc9050100000065dc6213527a675a004083d8 (good)
;; QUESTION SECTION:
;192.168.0.28.           IN      A

;; AUTHORITY SECTION:
.          86095  IN      SOA      a.root-servers.net. nstl
d.verisign-grs.com. 2024022600 1800 900 604800 86400

;; Query time: 0 msec
;; SERVER: 192.168.0.27#53(192.168.0.27) (UDP)
;; WHEN: Mon Feb 26 11:04:03 CET 2024
;; MSG SIZE  rcvd: 144
```

```
profesor@profesoradodaw:/etc/default$ dig 192.168.0.29

; <>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <>> 192.168.0.29
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 14114
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: fcf70d06cc252f900100000065dc62169c2d40ca452da607 (good)
;; QUESTION SECTION:
;192.168.0.29.           IN      A

;; AUTHORITY SECTION:
.          86092    IN      SOA      a.root-servers.net. nstl
d.verisign-grs.com. 2024022600 1800 900 604800 86400

;; Query time: 0 msec
;; SERVER: 192.168.0.27#53(192.168.0.27) (UDP)
;; WHEN: Mon Feb 26 11:04:06 CET 2024
;; MSG SIZE  rcvd: 144

profesor@profesoradodaw:/etc/default$ dig 192.168.0.30

; <>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <>> 192.168.0.30
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 18090
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 95f59d2118617fb50100000065dc61f236689f152837e12e (good)
;; QUESTION SECTION:
;192.168.0.30.           IN      A

;; AUTHORITY SECTION:
.          86128    IN      SOA      a.root-servers.net. nstl
d.verisign-grs.com. 2024022600 1800 900 604800 86400

;; Query time: 0 msec
;; SERVER: 192.168.0.27#53(192.168.0.27) (UDP)
;; WHEN: Mon Feb 26 11:03:30 CET 2024
;; MSG SIZE  rcvd: 144
```

## EJERCICIO 3. SERVIDOR LDAP.

### Actividad 3.1. Instalación de LDAP.

Realiza la instalación del servicio de LDAP con OpenLDAP (slapd). Una vez instalado realiza la configuración inicial utilizando como dominio raíz **distancia24.com** y el password **distancia**. Realiza una comprobación de la instalación (con slapcat).

Para realizar la instalación de OpenLDAP en Linux Ubuntu 22 realizaremos el siguiente procedimiento como usuario **root**, o usando **sudo** en cada comando:

#### Paso 1. Actualizar los repositorios:

```
$ apt update ó $ apt-get update
```

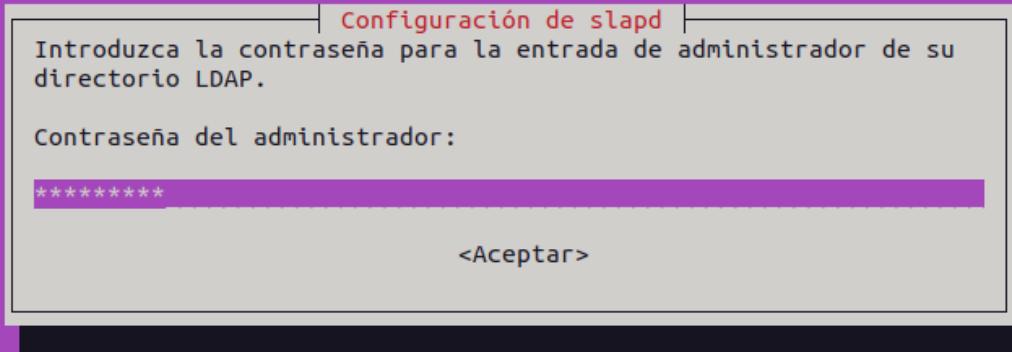
```
profesor@profesor-VirtualBox:~$ sudo apt update
Obj:1 http://es.archive.ubuntu.com/ubuntu jammy InRelease
Des:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Obj:4 http://es.archive.ubuntu.com/ubuntu jammy-backports InRelease
Des:5 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1.3
77 kB]
Des:6 http://es.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [570
kB]
Des:7 http://es.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Package
```

#### Paso 2. Instalar los paquetes necesarios para OpenLDAP:

```
$ sudo apt install slapd ldap-utils
profesor@profesor-VirtualBox:~$ sudo apt install slapd ldap-utils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
  linux-headers-6.2.0-37-generic linux-hwe-6.2-headers-6.2.0-37
  linux-image-6.2.0-37-generic linux-modules-6.2.0-37-generic
  linux-modules-extra-6.2.0-37-generic
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  libodbc2
Paquetes sugeridos:
  odbc-postgresql tdsodbc
Se instalarán los siguientes paquetes NUEVOS:
  ldap-utils libodbc2 slapd
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 89 no actualizados.
Se necesita descargar 1.843 kB de archivos.
Se utilizarán 6.041 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] ■
```

Durante la instalación nos solicitará una contraseña de administrador.

Configuración de paquetes

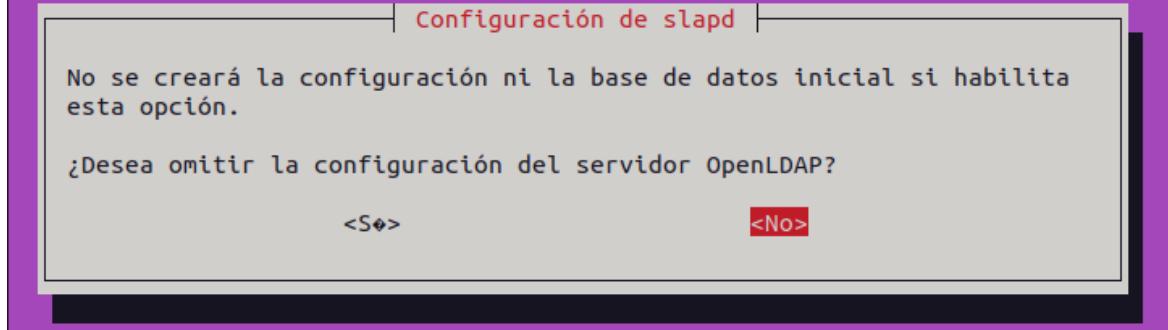


Una vez finalizada la instalación, debemos reconfigurar nuestro servicio.

### Paso 3. Configuración básica inicial

```
$ sudo dpkg-reconfigure slapd
```

Configuración de paquetes



¿Omitir configuración? Contestamos que No

## Configuración de paquetes

### Configuración de slapd

El nombre de dominio DNS se utiliza para construir el DN base del directorio LDAP. Por ejemplo, si introduce «foo.example.org» el directorio se creará con un DN base de «dc=foo, dc=example, dc=org».

Introduzca el nombre de dominio DNS:

distancia24.com

<Aceptar>

En el DNS domain name podemos poner el dominio para el que queremos crear la estructura.

## Configuración de paquetes

### Configuración de slapd

Introduzca el nombre de la organización a utilizar en el DN base del directorio LDAP.

Nombre de la organización:

distancia24

<Aceptar>

Aquí podemos poner el nombre de nuestra organización, que es para la que crearemos el árbol de LDAP.

## Configuración de paquetes

### Configuración de slapd

Introduzca la contraseña para la entrada de administrador de su directorio LDAP.

Contraseña del administrador:

\*\*\*\*\*

<Aceptar>

Debemos dar una contraseña de administrador, que es la que nos pedirá para añadir objetos al dominio principal. (En mi caso es %D1st4nCIA24%)

Configuración de paquetes

Configuración de slapd

¿Desea que se borre la base de datos cuando se purge el paquete slapd?

<Sí>

<No>

¿Eliminar la base de datos antigua? Le decimos que sí (Yes)

Configuración de paquetes

Configuración de slapd

Existen ficheros en «/var/lib/ldap» que probablemente interrumpan el proceso de configuración. Si activa esta opción, se moverán los ficheros de las bases de datos antiguas antes de crear una nueva base de datos.

¿Desea mover la base de datos antigua?

<Sí>

<No>

¿Autorizamos a eliminar el resto de archivos antiguos? Le respondemos que Sí (Yes)

```
profesor@profesor-VirtualBox:~$ sudo dpkg-reconfigure slapd
  Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.5.16+dfsg-0ubuntu0.22.04.
2... done.
  Moving old database directory to /var/backups:
    - directory unknown... done.
  Creating initial configuration... done.
  Creating LDAP directory... done.
profesor@profesor-VirtualBox:~$
```

Y con esto habrá finalizado la configuración inicial de nuestro OpenLDAP.

#### Paso 4. Comprobamos la instalación.

```
$ sudo slapcat
profesor@profesor-VirtualBox:~$ sudo slapcat
dn: dc=distancia24,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: distancia24
dc: distancia24
structuralObjectClass: organization
entryUUID: 81166e9a-65ac-103e-9ce3-21aae3d28fcc
creatorsName: cn=admin,dc=distancia24,dc=com
createTimestamp: 20240222090000Z
entryCSN: 20240222090000.557155Z#000000#000#000000
modifiersName: cn=admin,dc=distancia24,dc=com
modifyTimestamp: 20240222090000Z

profesor@profesor-VirtualBox:~$
```

## Actividad 3.2. Añadir una unidad organizativa el directorio LDAP.

Tras la instalación del servidor OpenLDAP vamos a agregar una unidad organizativa. Para ello crearemos un fichero que se puede llamar como queramos. Yo lo voy a nombrar uniorg.ldif

```
$ sudo nano uniorg.ldif
```

```
GNU nano 6.2                               uniorg.ldif *
dn: ou=profesorado,dc=distancia24,dc=com
objectClass: top
objectClass: organizationalUnit
ou: profesorado
```

Ahora añadimos el fichero a nuestro árbol LDAP

```
$ sudo ldapadd -x -D cn=admin,dc=distancia24,dc=com -W -f
uniorg.ldif
```

(Nos solicita la contraseña de administrador que hemos puesto antes)

```
profesor@profesor-VirtualBox:~$ sudo ldapadd -x -D cn=admin,dc=distancia24,dc=com -W -f uniorg.ldif
Enter LDAP Password:
adding new entry "ou=profesorado,dc=distancia24,dc=com"

profesor@profesor-VirtualBox:~$
```

Para comprobar que se ha añadido:

```
$ sudo slapcat
profesor@profesor-VirtualBox:~$ sudo slapcat
dn: dc=distancia24,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: distancia24
dc: distancia24
structuralObjectClass: organization
entryUUID: 81166e9a-65ac-103e-9ce3-21aae3d28fcc
creatorsName: cn=admin,dc=distancia24,dc=com
createTimestamp: 20240222090000Z
entryCSN: 20240222090000.557155Z#000000#000#000000
modifiersName: cn=admin,dc=distancia24,dc=com
modifyTimestamp: 20240222090000Z

dn: ou=profesorado,dc=distancia24,dc=com
objectClass: top
objectClass: organizationalUnit
ou: profesorado
structuralObjectClass: organizationalUnit
entryUUID: cdfe9f88-65b2-103e-8a8d-95fcc2e5764c
creatorsName: cn=admin,dc=distancia24,dc=com
createTimestamp: 20240222094506Z
entryCSN: 20240222094506.566059Z#000000#000#000000
modifiersName: cn=admin,dc=distancia24,dc=com
modifyTimestamp: 20240222094506Z

profesor@profesor-VirtualBox:~$
```

### Actividad 3.3 Añadir un grupo al directorio LDAP

Al igual que hemos hecho en el apartado anterior, vamos a crear un grupo haciendo un fichero ldif y agregándolo al árbol de nuestra organización:

```
$ sudo nano group.ldif
```

```
GNU nano 6.2                                     group.ldif *
dn: cn=grupo1,ou=profesorado,dc=distancia24,dc=com
objectClass: top
objectClass: posixGroup
gidNumber: 10001
cn: grupo1
```

Ahora añadimos el fichero a nuestro árbol LDAP

```
$ sudo ldapadd -x -D cn=admin,dc=distancia24,dc=com -W -f group.ldif
```

(Nos solicita la contraseña de administrador que hemos puesto antes)

```
profesor@profesor-VirtualBox:~$ sudo ldapadd -x -D cn=admin,dc=distancia24,dc=com -W -f group.ldif
Enter LDAP Password:
adding new entry "cn=grupo1,ou=profesorado,dc=distancia24,dc=com"

profesor@profesor-VirtualBox:~$
```

Para comprobar que se ha añadido:

```
$ sudo slapcat
```

```
profesor@profesor-VirtualBox:~$ sudo slapcat
dn: dc=distancia24,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: distancia24
dc: distancia24
structuralObjectClass: organization
entryUUID: 81166e9a-65ac-103e-9ce3-21aae3d28fcc
creatorsName: cn=admin,dc=distancia24,dc=com
createTimestamp: 20240222090000Z
entryCSN: 20240222090000.557155Z#000000#000#000000
modifiersName: cn=admin,dc=distancia24,dc=com
modifyTimestamp: 20240222090000Z

dn: ou=profesorado,dc=distancia24,dc=com
objectClass: top
objectClass: organizationalUnit
ou: profesorado
structuralObjectClass: organizationalUnit
entryUUID: cdfe9f88-65b2-103e-8a8d-95fcc2e5764c
creatorsName: cn=admin,dc=distancia24,dc=com
createTimestamp: 20240222094506Z
entryCSN: 20240222094506.566059Z#000000#000#000000
modifiersName: cn=admin,dc=distancia24,dc=com
modifyTimestamp: 20240222094506Z

dn: cn=grupo1,ou=profesorado,dc=distancia24,dc=com
objectClass: top
objectClass: posixGroup
gidNumber: 10001
cn: grupo1
structuralObjectClass: posixGroup
entryUUID: 9c74f15a-65b3-103e-8a8e-95fcc2e5764c
creatorsName: cn=admin,dc=distancia24,dc=com
createTimestamp: 20240222095052Z
entryCSN: 20240222095052.952150Z#000000#000#000000
modifiersName: cn=admin,dc=distancia24,dc=com
modifyTimestamp: 20240222095052Z

profesor@profesor-VirtualBox:~$
```

#### Actividad 3.4. Añadir un usuario al directorio LDAP.

Para añadir un usuario primero debemos crear una contraseña con la herramienta slappasswd. La contraseña que nos genere debemos copiarla e incluirá en el fichero de usuario.

Para crear la contraseña:

```
$ sudo slappasswd  
profesor@profesor-VirtualBox:~$ sudo slappasswd  
New password:  
Re-enter new password:  
{SSHA}Kv4v/kqArRUM3FobT0IpQHDbKjorYAfN  
profesor@profesor-VirtualBox:~$
```

{SSHA}JnkYNp5agveD8YoI7BagY1xD3qtYzNj

Creamos el fichero

```
$ sudo nano user.ldif  
GNU nano 6.2 user.ldif *  
dn: uid=profesor, ou=profesorado, dc=distancia24, dc=com  
objectClass: top  
objectClass: posixAccount  
objectClass: inetOrgPerson  
objectClass: person  
cn: profesor  
ou: grupo1  
uidNumber: 2001  
gidNumber: 10001  
homeDirectory: /home/profesor  
loginShell: /bin/shell  
userPassword: {SSHA}JnkYNp5agveD8YoI7BagY1xD3qtYzNj  
sn: daw  
mail: profesorado.daw@gmail.com  
givenName: profesor  
  
^G Ayuda      ^O Guardar      ^W Buscar      ^K Cortar      ^T Ejecutar      ^C Ubica  
^X Salir      ^R Leer fich.  ^V Reemplazar  ^U Pegar       ^J Justificar  ^/ Ir a
```

Añadimos el fichero a nuestro árbol LDAP

```
$ sudo ldapadd -x -D cn=admin,dc=distancia24,dc=com -W -f user.ldif
```

(Nos solicita la contraseña de administrador que hemos puesto antes)

```
profesor@profesor-VirtualBox:~$ sudo ldapadd -x -D cn=admin,dc=distancia24,dc=com -W -f user.ldif  
Enter LDAP Password:  
adding new entry "uid=profesor, ou=profesorado, dc=distancia24, dc=com"  
profesor@profesor-VirtualBox:~$
```

Comprobamos con Slapcat

```
$ sudo slapcat
# modifyTimestamp: 20240222095052Z

dn: uid=profesor,ou=profesorado,dc=distancia24,dc=com
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: profesor
ou: grupo1
uidNumber: 2001
gidNumber: 10001
homeDirectory: /home/profesor
loginShell: /bin/shell
userPassword:: e1NTSEF9Sm5rWU5wNWFndmVE0FlvSTdCYWdZMXhYZDNxdFl6Tmo=
sn: daw
mail: profesorado.daw@gmail.com
givenName: profesor
structuralObjectClass: inetOrgPerson
uid: profesor
entryUUID: f0d52930-65b4-103e-8a8f-95fcc2e5764c
creatorsName: cn=admin,dc=distancia24,dc=com
createTimestamp: 20240222100024Z
entryCSN: 20240222100024.008079Z#000000#000#000000
modifiersName: cn=admin,dc=distancia24,dc=com
modifyTimestamp: 20240222100024Z

profesor@profesor-VirtualBox:~$
```

Por último, vamos a recuperar la información de nuestro usuario:

```
$ sudo ldapsearch -xLLL -b "dc=distancia24, dc=com" uid=profesor sn
cn
profesor@profesor-VirtualBox:~$ sudo ldapsearch -xLLL -b "dc=distancia24,dc=com"
uid=profesor sn cn givenName mail
dn: uid=profesor,ou=profesorado,dc=distancia24,dc=com
cn: profesor
sn: daw
mail: profesorado.daw@gmail.com
givenName: profesor

profesor@profesor-VirtualBox:~$
```