# DESARROLLO DE APLICACIONES WEB

## Módulo 08. Despliegue de Aplicaciones Web

**Silvia Macho**
**Lidia Porcel**

VERSIÓN IMPRIMIBLE A LINKIAFP

**Unidad Formativa 3.**
Despliegue de aplicaciones Web

Linkia FP
Formación Profesional Oficial a Distancia

VERSIÓN IMPRIMIBLE ALUMNO LINKIAFP

# DESARROLLO DE APLICACIONES WEB

VERSIÓN IMPRIMIBLE ALUMNO LINKIAFP

## Módulo 08. Despliegue de Aplicaciones Web

Silvia Macho
Lidia Porcel

**Unidad Formativa 3.**
Despliegue de aplicaciones Web

Linkia FP
Formación Profesional Oficial a Distancia

VERSIÓN IMPRIMIBLE ALUMNO LINKIAFP

© Macho y Porcel, 2018
© Ediciones Linkia FP, 2018
Calle Pelayo 7, principal 1ª. 08001 Barcelona.
1ª edición: septiembre 2017
Reservados todos los derechos. El material es de uso exclusivo para alumnos de LinkiaFP. No se permite la reproducción total o parcial de esta obra, ni su incorporación a un sistema informático, ni su transmisión en cualquier forma o por cualquier medio (electrónico, mecánico, fotocopia, grabación u otros) sin autorización previa y por escrito de los titulares del copyright. La infracción de dichos derechos puede constituir un delito contra la propiedad intelectual.

# Índice


Tema 1: Servicios de red implicados en una aplicación Web 4

1. Introducción 5

1.1. Domain Name System (DNS) 5

1.1.1. Jerarquía DNS 7

1.1.2. Zonas y registros DNS 8

1.1.3. Servidores DNS 11

1.1.4. Consultas DNS 14

1.1.5. Caché DNS 17

1.1.6. Round Robin DNS 18

1.1.7. Paquetes DNS 20

2. Servidor de nombres (DNS) 21

2.1. Implementación de DNS en Windows Server 2016 21

2.1.1. Configuración software de Virtualización 21

2.1.2. Configuración del servidor DNS en Windows 2016 Server 22

2.1.3. Instalación y puesta en marcha 23

2.1.4. Creación de zonas y registros 26

2.1.5. Zonas secundarias 34

2.1.6. Reenviadores y servidores raíz 40

2.1.7. Round Robin DNS 42

2.1.8. Caché en el servidor DNS 44

2.2. Implementación de DNS en Ubuntu Server 45

2.2.1. Configuración del servidor DNS en Ubuntu Server 18.04 45

2.2.2. Instalación y puesta en marcha 46

2.2.3. Zonas y registros 48

2.2.4. Zonas secundarias 51

3. Lightweight Directory Access Protocol (LDAP) 52

3.1. Introducción 52

3.1.1. Jerarquía y nomenclatura LDAP 53

3.2. Implementación de Active Directory en Windows Server 2016 56

3.2.1. Instalación y puesta en marcha 59

3.2.2. Creación de usuarios y grupos 65

3.2.3. Instalar un controlador de dominio adicional 68

3.2.4. Integración de Apache con Active Directory 72

Recursos/Enlaces 76

Test de autoevaluación 77

# T1 Tema 1: Servicios de red implicados en una aplicación Web

## ¿Qué aprenderás?

- Instalar y configurar un servidor DNS en Windows.
- Instalar y configurar un servidor DNS en Linux
- Configurar un servidor DNS esclavo en ambos servidores.
- Configurar Round Robin en ambos servidores.

## ¿Sabías que…?

- Cuando tecleamos una dirección en la barra de direcciones de nuestro navegador, la página a la que queremos acceder se carga a los pocos segundos, como por arte de magia. En realidad, no hay ninguna chistera detrás de este acto, sino una serie de tecnologías bastante complejas que hacen que Internet, la red de redes, funcione correctamente en cualquier dispositivo.
- Existen 13 servidores DNS raíz en toda Internet.
- Active Directory (AD) o Directorio Activo son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de equipos. Utiliza distintos protocolos, principalmente LDAP, DNS, DHCP.

VERSIÓN IMPRIMIBLE ALUMNO LINKIAFP

# 1. Introducción

Para desplegar una aplicación web no sólo es necesario disponer de un servidor web. Habitualmente hay servicios de red adicionales que prestan ayuda a la aplicación web en diferentes funcionalidades de la misma.

Por ejemplo, el servicio DNS es el encargado de dirigir a los clientes hasta el servidor. Sin el DNS, los clientes tendrían que conocer directamente todas las IPs de los servidores a los que necesitaran acceder, algo que resultaría muy poco práctico. Gracias al DNS, los clientes acceden a nombres (FQDN, fully qualified domain name) que el servicio DNS traducirá a IPs para que puedan alcanzar el destino deseado.

Otro ejemplo de servicio adicional es el servicio de autenticación de usuarios. Aunque es posible autenticar a los usuarios de forma local en el propio servidor web, este sistema tiene muy poca flexibilidad y es muy difícil de escalar para grandes instalaciones donde hay involucrados muchos servidores web. Un servicio de autenticación de usuarios centralizado lo puede proporcionar un servidor LDAP, que almacena de forma segura una base de datos de usuarios a la que consultarán todos los servidores web existentes cuando algún cliente solicite el acceso.

En este apartado se estudiarán los dos servicios comentados: DNS y LDAP.

## 1.1. Domain Name System (DNS)

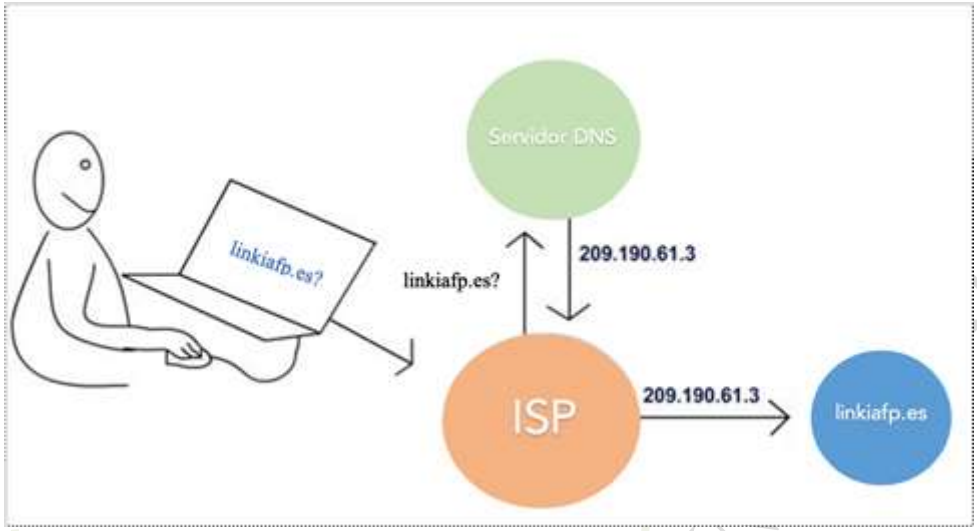
DNS (Domain Name System) es el sistema de nomenclatura utilizado en Internet. DNS es un sistema distribuido de nomenclatura jerárquica para computadoras, servicios u otros recursos conectados a una red.

Los equipos conectados a una red se comunican gracias a la IP que cada uno tiene asignada, sin embargo, trabajar con IPs de 32 bits (o más en IPv6) es muy poco práctico para el manejo y configuración de los sistemas. El servicio de DNS se encarga de traducir los nombres de máquina en sus IPs correspondientes, de esa forma no es necesario recordar todas las IPs de los servicios o máquinas a las que se desea acceder.

Cualquier cliente, cuando desea acceder a un servidor mediante su nombre DNS, tiene primero que realizar una consulta DNS a un servidor DNS. Éste le devolverá la IP correspondiente al nombre por el que pregunta, y entonces el cliente, una vez sabe la IP de destino, puede acceder a ella.

VERSIÓN IMPRIMIBLE ALUMNO LINUXFP

El servicio DNS es un directorio de nombres e IPs al que todas las máquinas preguntan para encontrar direcciones IP.




En la imagen de ejemplo mostrada, el cliente pregunta al servidor DNS cual es la IP de un sitio web al que desea acceder (www.linkiafp.es). El servidor DNS responde con la IP que tiene almacenada en su base de datos (209.190.61.3). El cliente entonces ya es capaz de acceder al servidor web que deseaba.

Este proceso sucede de forma invisible para el usuario cuando navega mediante un navegador web. El sistema en segundo plano realiza esta consulta DNS sin que el usuario intervenga.

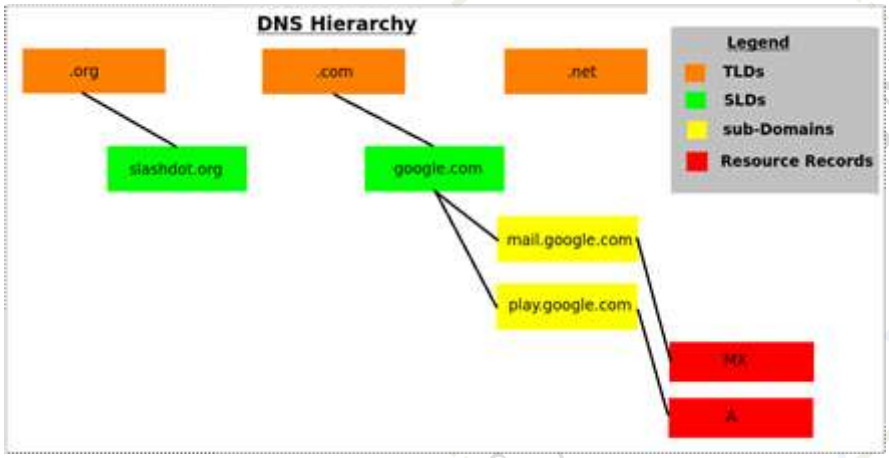
El acrónimo DNS puede entenderse desde diferentes puntos de vista:

1. Es la normativa que establece una nomenclatura para equipos y servicios en internet. Rige los caracteres válidos y la forma en la que se construyen los nombres
2. Es un protocolo de comunicación para el envío de consultas y respuestas. Se definen los tipos de paquetes con su contenido y formato para enviar consultas a través de una red TCP/IP. El caso más habitual es que el servicio DNS trabaje sobre UDP en el puerto 53
3. Es una base de datos distribuida. Los servidores DNS a través de la red se replican el contenido de todos los directorios de IPs y nombres, formando una gran base de datos distribuida por toda la red.

### 1.1.1. **Jerarquía DNS**

El sistema de nomenclatura DNS es un sistema jerárquico. Todos los nombres parten de una raíz, que se simboliza con punto "." . El punto es el denominado dominio raíz, y a partir de él surge un árbol de posibles nombres de dominio a diferentes niveles.

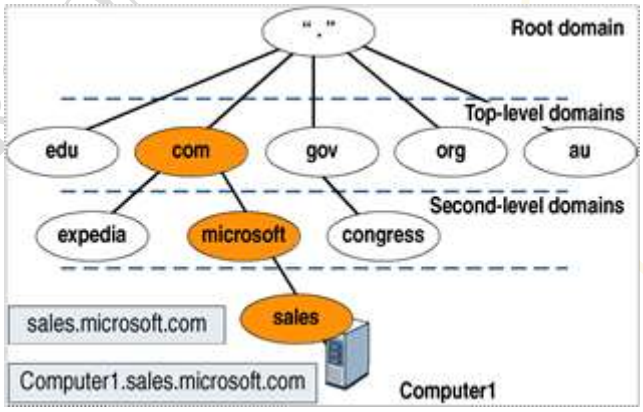
Los dominios del primer nivel son los denominados TLD (Top Level Domains), mientras que los del siguiente nivel son los SLD (second Level Domains)




http://thejimmahknows.com

A partir de los SLDs pueden surgir tantos niveles como sea necesario, a los cuales se les suele denominar de forma genérica subdominios. Finalmente, dentro de cada subdominio constan los diferentes registros DNS, los cuales almacenan la información final de nombre e IP de la máquina o servicio.

El nombre DNS completo de un equipo, se construye leyendo al revés el recorrido del árbol DNS al que pertenece:




http://microsoft.com

En el ejemplo anterior, el equipo de nombre "Computer1" que pertenece al dominio "sales.microsoft.com" tiene un FQDN (Fully Qualified Domain Name) que se construye con la concatenación:

"Computer1.sales.microsoft.com"

En ocasiones también se incluye al final del fqdn un "." para representar al dominio raíz al que todos los nombres pertenecen.

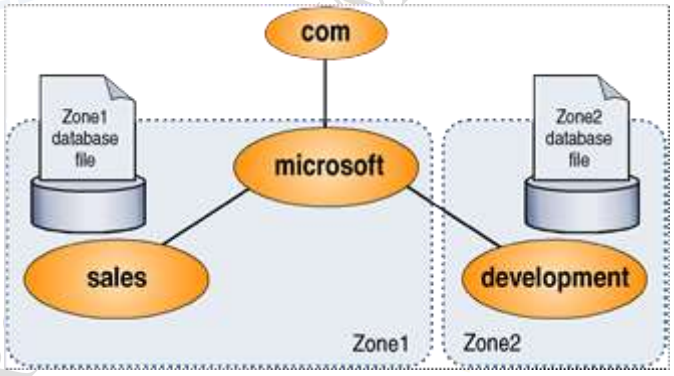
Los TLDs (Top Level Domains) han sido hasta el momento un número limitado de dominios bajo la regulación del ICANN (Internet Corporation for Assigned Names and Numbers). Entre ellos se encuentran los primeros .com .net o .gov y los llamados ccTLDs, es decir, TLDs asociados a códigos de países.

Esta estructura ha sido muy rígida hasta hace pocos años cuando ha empezado una revolución en cuanto a la nomenclatura de dominios en internet. Hoy en día se empiezan a registrar los nuevos Generic TLDs (gTLDS) que son mucho más abiertos y se admiten palabras completas como por ejemplo .education o .download

Para más información sobre los nuevos gTLDs: http://newgtlds.icann.org/en/

### 1.1.2. **Zonas y registros DNS**

La información de todos los nombres DNS existentes en el árbol DNS está seccionada en zonas. Las zonas DNS son archivos que contienen registros de uno o más dominios de una misma rama del árbol.

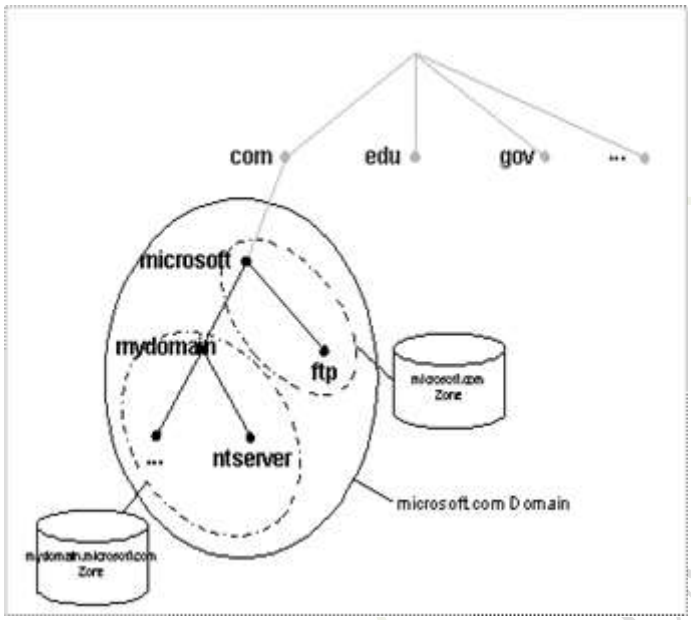



http://microsoft.com

En el ejemplo mostrado, toda la información (registros) del dominio microsoft.com se ha partido en dos trozos:

4. En la zona1 se almacenan todos los registros del dominio microsoft.com y del subdominio sales.microsoft.com.
5. En la zona2 se almacenan todos los registros del subdominio development.microsoft.com

En definitiva, las zonas son una forma de seccionar por ramas todo el conjunto de registros del árbol DNS. Otro ejemplo, a continuación




http://microsoft.com

Dentro de cada zona están los registros DNS, que son los que contienen la información de nombre e IP del recurso, máquina o servicio.

Existen diversos tipos de registros:

| Type of record | Associated entity | Description |
|---|---|---|
| SOA | Zone | Holds information on the represented zone |
| A | Host | Contains an IP address of the host this node represents |
| MX | Domain | Refers to a mail server to handle mail addressed to this node |
| SRV | Domain | Refers to a server handling a specific service |
| NS | Zone | Refers to a name server that implements the represented zone |
| CNAME | Node | Symbolic link with the primary name of the represented node |
| PTR | Host | Contains the canonical name of a host |
| HINFO | Host | Holds information on the host this node represents |
| TXT | Any kind | Contains any entity-specific information considered useful |

VERSIÓN IMPRIMIBLE ALUMNO LINKIAFP

Cabe destacar los siguientes tipos:

SOA (Start os Authority): es el registro que identifica al servidor primario de una zona además de información adicional como el email del administrador de la zona.

A: identifica un nombre de host con su IPv4 (existe el tipo AAAA para IPv6).

NS: identifica al servidor DNS que alberga la zona.

MX: identifica al servidor de correo que gestiona un nombre de dominio.

CNAME: es un alias añadido al nombre principal del host.

Una zona DNS puede quedar almacenada en un servidor DNS en forma de fichero, en donde constan, uno por línea, todos los registros de la zona.

Por ejemplo, a continuación se muestra un posible contenido de un fichero de zona:

```
;
; Host addresses
;
localhost.movie.edu.  IN A     127.0.0.1
robocop.movie.edu.    IN A     192.249.249.2
terminator.movie.edu. IN A     192.249.249.3
diehard.movie.edu.    IN A     192.249.249.4
misery.movie.edu.     IN A     192.253.253.2
shining.movie.edu.    IN A     192.253.253.3
carrie.movie.edu.     IN A     192.253.253.4
;
; Multi-homed hosts
;
wormhole.movie.edu.   IN A     192.249.249.1
wormhole.movie.edu.   IN A     192.253.253.1
;
; Aliases
;
bigt.movie.edu.       IN CNAME terminator.movie.edu.
dh.movie.edu.         IN CNAME diehard.movie.edu.
```

Se puede observar como en la zona hay diversos registros de tipo A, que vinculan diversos nombres (fqdn) con sus respectivas IPs. También se pueden observar registros CNAME, que añaden nombres adicionales al nombre existente como registro A.

Por ejemplo, en el fichero mostrado, existe el CNAME "dh.movie.edu" que está vinculado al otro nombre "diehard.movie.edu" para el cual ya existe un registro A que lo vincula con la IP 192.249.249.4. Si a éste servidor se le pregunta por cualquiera de los dos nombres, la respuesta será en ambos casos la misma IP (192.249.249.4).

A continuación se muestra un ejemplo más completo de un archivo de zona DNS:

```
$ORIGIN example.com.     ; designates the start of this zone file in the namespace
$TTL 1h                  ; default expiration time of all resource records without their own TTL value
example.com.  IN  SOA  ns.example.com. username.example.com. (
              2007120710 ; serial number of this zone file
              1d         ; slave refresh (1 day)
              2h         ; slave retry time in case of a problem (2 hours)
              4w         ; slave expiration time (4 weeks)
              1h         ; maximum caching time in case of failed lookups (1 hour)
              )
example.com.  NS    ns                    ; ns.example.com is a nameserver for example.com
example.com.  NS    ns.somewhere.example. ; ns.somewhere.example is a backup nameserver for example.com
example.com.  MX    10 mail.example.com.  ; mail.example.com is the mailserver for example.com
@             MX    20 mail2.example.com. ; equivalent to above line, "@" represents zone origin
@             MX    50 mail3              ; equivalent to above line, but using a relative host name
example.com.  A     192.0.2.1             ; IPv4 address for example.com
              AAAA  2001:db8:10::1        ; IPv6 address for example.com
ns            A     192.0.2.2             ; IPv4 address for ns.example.com
              AAAA  2001:db8:10::2        ; IPv6 address for ns.example.com
www           CNAME example.com.          ; www.example.com is an alias for example.com
wwwtest       CNAME www                   ; wwwtest.example.com is another alias for www.example.com
mail          A     192.0.2.3             ; IPv4 address for mail.example.com,
                                          ;  any MX record host must be an address record
                                          ; as explained in RFC 2181 (section 10.3)
mail2         A     192.0.2.4             ; IPv4 address for mail2.example.com
mail3         A     192.0.2.5             ; IPv4 address for mail3.example.com
```

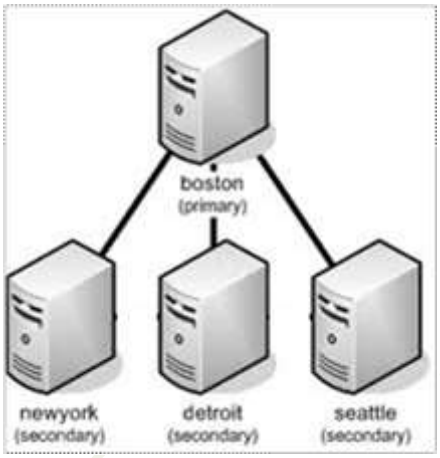
En el ejemplo se pueden ver otros tipos de registro, como el registro SOA, que identifica al servidor principal de la zona entre otros parámetros de la zona. También se pueden ver registros NS que identifican a los servidores DNS de la zona, registros MX, que identifican a los servidores de correo del dominio (@example.com), registros CNAMEs que aportan alias adicionales, y finalmente registros tipo A y AAAA que identifican nombres de host IPv4 e IPv6 con sus IPs correspondientes.

### 1.1.3. **Servidores DNS**

Los servidores DNS son máquinas que gestionan las peticiones DNS de los clientes a través de la red y almacenan las zonas DNS de forma local. Un servidor DNS puede albergar una o varias zonas DNS.

Por cuestiones de redundancia, y también de balanceo de carga, las zonas DNS se suelen almacenar en varios servidores. Es decir, una misma zona se replica entre diferentes servidores DNS a través de la red. De esa forma, si uno de los servidores cae, los demás están preparados para seguir respondiendo a consultas DNS que les puedan hacer los clientes. Para ello, los clientes pueden tener configurado no sólo un servidor DNS al que realizarle las preguntas, sino varios.

De cada zona existe un servidor primario, y pueden existir varios secundarios asociados.




http://docs.oracle.com

En el primario (master) es donde se pueden realizar todos los cambios y ediciones de la zona, mientras que en los secundarios (slave) la información sólo se puede leer, sólo pueden responder a consultas, pero no pueden ser modificadas las zonas.

Los secundarios, cuando cae el primario, pueden seguir respondiendo a las consultas, pero tarde o temprano se deberá recuperar el primario ya que depende de él que se puedan hacer futuras modificaciones a la zona. Si el primario cae de forma definitiva (por ej, por culpa de un virus) normalmente se puede "promocionar " uno de los servidores secundarios a servidor primario.

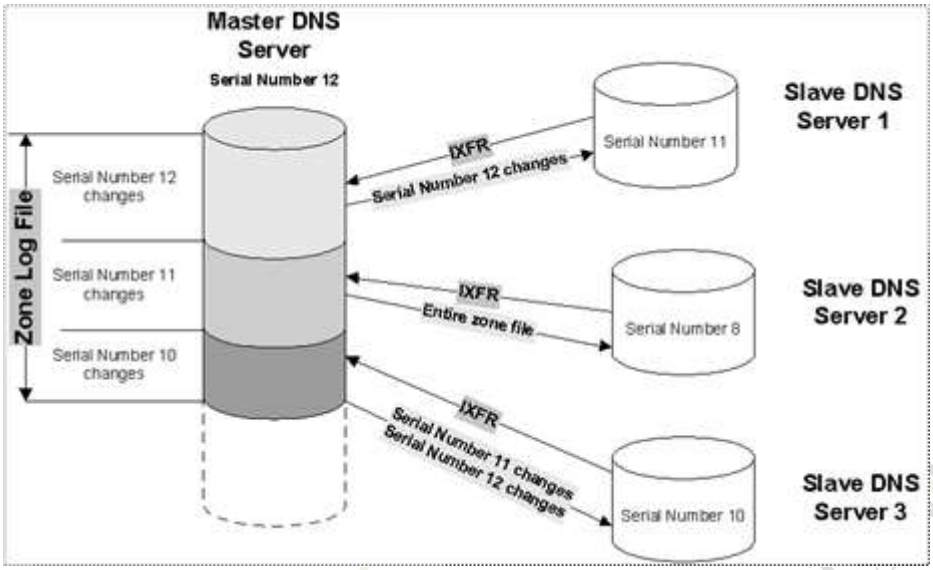
Así que cada zona puede estar albergada en diferentes servidores, pero uno de ellos será el servidor primario de la zona, mientras que los demás contendrán copias (réplicas) enviadas a través de la red entre el primario y los posibles secundarios.

Las transferencias de zona suceden entre el servidor primario y los servidores secundarios. Existen dos tipos de transferencia de zona:

6. Full AXFR.
7. Incremental IXFR.

Con el tipo AXFR se envía una copia completa de la zona, mientras que con una transferencia del tipo IXFR se envían tan sólo los cambios acontecidos en la zona (sólo los registros que han cambiado).

El primario mantiene un número de versión (serial number) en el registro SOA de la zona. Este número se va incrementando si la zona va cambiando. Los servidores secundarios pueden preguntar al servidor primario cuál es el número de versión actual, para compararlo con el que ellos mismos tienen en su copia local, si hay diferencias significa que ha habido cambios y por lo tanto se inicia un proceso de transferencia de zona. Dependiendo de la diferencia entre números de versión se decide qué tipo de transferencia de zona.

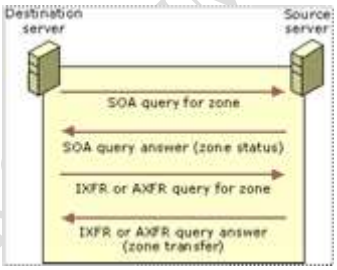



http://docs.microsoft.com

En la imagen anterior se aprecia como en el servidor primario (master) suceden tres cambios, que se identifican con un número de serie cada uno. Los servidores secundarios (slave) tienen por su parte una copia más antigua de la zona con números de versión más bajos.

En el ejemplo los números de versión de las zonas de los secundarios no son demasiado bajos respecto al primario y se solicita entonces transferencia incremental (solo de los cambios). Sin embargo, en el server2, se considera que los cambios son demasiados y se envía toda la zona.

En resumen, en primer lugar, el servidor secundario solicita el valor del registro SOA que tiene el primario en la zona, el primario responde y entonces se decide el tipo de transferencia.




http://docs.microsoft.com

Es importante destacar que una vez la zona DNS está replicada en diferentes servidores, es necesario que los clientes hagan uso de esa redundancia. Para ello, en la configuración de red de los clientes DNS, es recomendable configurar varios servidores DNS.

A continuación, se muestra un ejemplo de configuración de red de un cliente tipo windows:

Como se puede observar, se debe especificar además de un servidor DNS preferido, también un servidor DNS alternativo. Si falla el preferido, las consultas se realizarán al alternativo.

### 1.1.4. **Consultas DNS**

Cuando en un cliente se abre un navegador web para acceder a una página web de nombre "www.example.com", el sistema operativo genera en segundo plano una consulta DNS hacia el servidor DNS que se haya configurado en el adaptador de red, para averiguar en qué IP se encuentra el servidor web de la página "www.example.com".

Una vez se consigue la respuesta, el cliente ya puede acceder a la IP obtenida mediante diferentes métodos y protocolos como http.

Aunque este proceso es invisible para el usuario, se puede testear mediante el comando "nslookup". Mediante este comando se pueden realizar consultas de prueba a los servidores DNS que se desee. También existen otros comandos de test DNS como "dig" o "host".

A continuación se muestra un ejemplo de ejecución del comando "nslookup":

VERSIÓN NO VISIBLE ALUMNO LINKIAFP

```
C:\Users\user>nslookup
Servidor predeterminado:  33.Red-80-58-0.staticIP.rima-tde.net
Address:  80.58.0.33

> google.com
Servidor:  33.Red-80-58-0.staticIP.rima-tde.net
Address:  80.58.0.33

Respuesta no autoritativa:
Nombre:  google.com
Addresses:  74.125.230.84
          74.125.230.80
          74.125.230.81
          74.125.230.82
          74.125.230.83

> set type=mx
> google.com
Servidor:  33.Red-80-58-0.staticIP.rima-tde.net
Address:  80.58.0.33

Respuesta no autoritativa:
google.com      MX preference = 400, mail exchanger = google.com.s9b2.psmtp.com
google.com      MX preference = 100, mail exchanger = google.com.s9a1.psmtp.com
google.com      MX preference = 200, mail exchanger = google.com.s9a2.psmtp.com
google.com      MX preference = 300, mail exchanger = google.com.s9b1.psmtp.com

google.com.s9b2.psmtp.com       internet address = 74.125.148.14
google.com.s9a1.psmtp.com       internet address = 74.125.148.10
google.com.s9a2.psmtp.com       internet address = 74.125.148.11
google.com.s9b1.psmtp.com       internet address = 74.125.148.13
```

En el ejemplo mostrado se observa como al ejecutar el comando nslookup sin parámetros, se accede a una shell propia del comando, y preguntando al servidor DNS configurado en la máquina, que en el ejemplo es un servidor DNS público en internet (80.58.0.33, que en concreto está administrado por Movistar). Justo después de ejecutar el comando, el servidor en cuestión se identifica y se queda a la espera de que se le pregunte.

La primera pregunta que se le hace es por "google.com". La respuesta es "no autoritativa", lo cual quiere decir que el servidor de Movistar no tenía la respuesta a esa pregunta en una de sus zonas locales, pero ha ido a buscarla para el cliente a otros servidores DNS. El servidor de Movistar no es autoritativo en la zona, pero ha conseguido la respuesta.

La respuesta no es sólo una IP, sino varias, cosa muy común en los servicios de Internet de tamaño medio y grande.

Siguiendo con el ejemplo de la imagen, el comando siguiente es "set type=mx". Con ese comando se indica que las siguientes preguntas buscaran registros MX (y no registros A como hasta ahora), con los cuales se identifica a los servidores de correo asociados a un dominio en concreto.

Ahora que el tipo de pregunta establecida es MX, cuando se pregunta por "google.com" la respuesta es diferente, la respuesta muestra los cuatro servidores de correo asociados a ese dominio.  Cada servidor tiene asociada una prioridad.

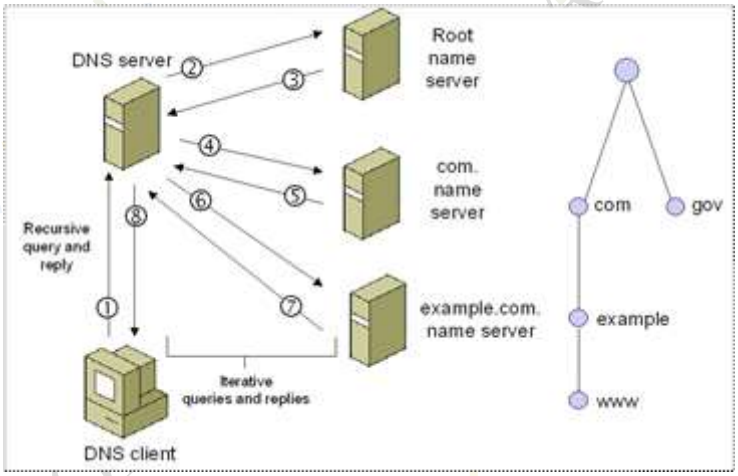
Por último, ya que los servidores de correo están resueltos con un nombre, el comando resuelve también esos nombres de servidores con sus IPs gracias a los registros A existentes también en la zona. Es decir, el nombre de dominio apunta a varios nombres de servidor mediante registros MX, y esos nombres de servidor apuntan a unas IPs mediante registros tipo A. La respuesta en este caso también es no autoritativa.

Cuando un cliente pregunta una duda DNS, es decir, realiza una consulta DNS, existen diferentes formas de hacerlo, lo que implica un comportamiento diferente por parte de los servidores.

Principalmente existen dos tipos de consultas DNS:

8. Recursivas: si la consulta es recursiva, el servidor DNS tiene que devolver al cliente la respuesta final a la consulta, o en su defecto, contestar que no conoce la respuesta.
9. Iterativas: si la consulta es iterativa, el servidor, si no conoce la respuesta directamente de sus zonas locales o de su caché, podrá responder dirigiendo al cliente a otros servidores DNS de nivel superior. El cliente entonces tendrá que repreguntar a esos servidores DNS.

El tipo más habitual de consultas DNS en Internet funciona mediante una mezcla de los dos tipos de consulta. El cliente suele enviar a su servidor DNS local consultas recursivas para que éste le proporcione respuestas finales, sin embargo, estos servidores DNS se preguntan entre sí de forma iterativa, de forma que se van reenviando del uno al otro hasta llegar al servidor autoritativo de la zona por la que se pregunta, quién ofrece una respuesta al servidor DNS, que se la pasa al cliente que le preguntó de forma recursiva.




http://docs.microsoft.com

Como se puede observar, el cliente lanza una consulta recursiva (1) a su servidor DNS local. La pregunta del ejemplo pretende averiguar cuál es la IP del nombre "www.example.com". El servidor DNS local, al ser la consulta recursiva debe proporcionar al cliente una respuesta definitiva (8), no le podrá redirigir a otros servidores.

El servidor DNS local, para obtener la información que le solicita el cliente, se encarga él mismo de realizar la consulta a otros servidores de más arriba en la jerarquía DNS. En el ejemplo le pasa la consulta (2) a un root server (servidor DNS de la zona root). Esta consulta la realiza de forma iterativa, así que el root server, que no sabe la respuesta a la pregunta, le responde (3) con la IP de otro servidor DNS que alberga la zona ".com".

El servidor DNS local acude de nuevo con la pregunta iterativa al servidor DNS de la zona ".com" (4), el cual tampoco conoce la respuesta definitiva, pero responde (5) con la IP, ahora sí, del servidor autoritativo en la zona "example.com". Éste sí que conoce la ip correspondiente al nombre preguntado, y responde (7) al servidor DNS local del cliente.

Finalmente, el servidor DNS local envía al cliente (8) la respuesta definitiva a la pregunta.

En todo el proceso, la consulta (1) es recursiva y las consultas (2), (4) y (6) son iterativas.

La respuesta (6) es autoritativa mientras que la (8) es no autoritativa.

### 1.1.5. **Caché DNS**

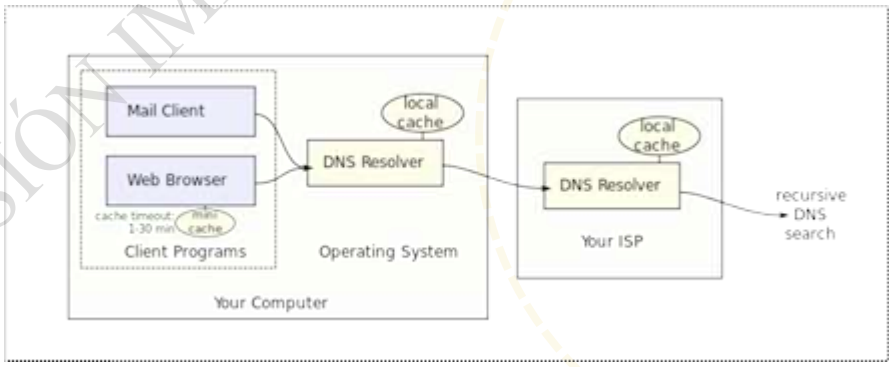
En todos los procesos de consultas DNS hay implicadas diversas memorias caché que se deben tener en cuenta.

Una memoria caché es un almacenamiento temporal de los datos más recientes o más utilizados por un servidor, para que estén fácilmente disponibles para otros usos que sucederán probablemente con mucha frecuencia.

En el ámbito de DNS, por ejemplo, cuando a un servidor DNS se le consulta por un nombre, después de responder al cliente la IP correspondiente, el servidor DNS se guarda en memoria caché esa IP, de forma que si vienen otros clientes preguntando por el mismo nombre, el servidor tendrá accesible la respuesta en su memoria caché de forma muy rápida para responderles.

Los registros quedan almacenados en memoria caché normalmente con una caducidad configurable en los servidores, ya que, si hay cambios en los registros DNS, la memoria caché podría responder de forma errónea (poco actualizada) a los clientes.

En el proceso que pasa por todos los diferentes pasos de una consulta DNS puede haber diferentes puntos en los que se almacenen de forma temporal una memoria caché.




http://wikipedia.org

Desde el navegador web del cliente, pasando por el sistema operativo cliente, hasta todos los servidores DNS involucrados en una consulta DNS, todos ellos pueden mantener memorias cachés para mejorar la rapidez y eficiencia de las resoluciones,

aunque en momentos concretos pueden llevar a errores de resolución por falta de actualización.

### 1.1.6. **Round Robin DNS**

DNS dispone de un mecanismo muy sencillo para distribuir la carga entre diferentes servidores. Se trata del Round Robin DNS.

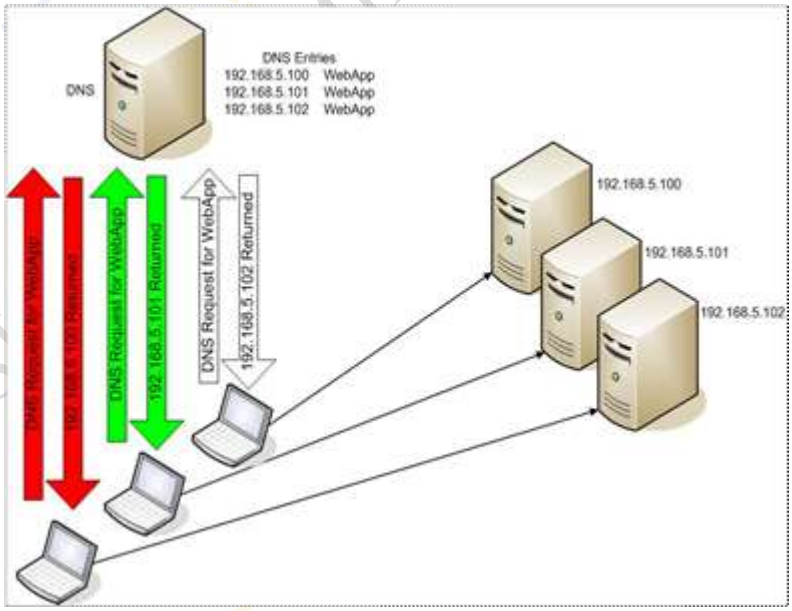
Round Robin es un término genérico que suele hacer referencia a procesos de reparto de una carga de trabajo a partes iguales entre diferentes nodos.

En el caso de DNS, su aplicación es muy sencilla. Dentro de una zona DNS, se crean, por ejemplo, dos registros A con el mismo nombre, pero con diferentes IPs. De esa forma, cuando un cliente pregunte por el nombre en cuestión, el servidor responderá con las dos IPs asociadas al nombre.

El cliente recibe la lista de IPs y prueba acceder a la primera, si no responde, probará con la segunda, y así sucesivamente. Además, el servidor DNS, cuando le pregunten de nuevo por el nombre en cuestión, volverá a responder con toda la lista, pero en esta ocasión, en diferente orden, de forma que el cliente probará primero otra de las IPs.

El servidor DNS, de esta manera está repartiendo a todos los clientes entre todos los servidores que constan asociados a un mismo nombre DNS.

A continuación, un ejemplo gráfico:




http://docs.oracle.com

En el ejemplo anterior se observa como existen tres entradas (tres IPs) para el mismo nombre "WebApp".

Cuando tres clientes diferentes preguntan al DNS por el nombre, a cada uno se le responde con una IP diferente. De esa forma, el servidor DNS consigue repartir a los clientes entre los tres servidores web disponibles.

En realidad, cuando el servidor DNS responde, envía las tres IPs a cada cliente, pero ordenadas de forma diferente para cada uno.

A continuación, se presenta un ejemplo de round robin DNS testeado con la herramienta nslookup:

```
> dominio.local
Servidor:  server2.dominio.local
Address:  192.168.150.3

Nombre:  dominio.local
Addresses:  192.168.150.15
          192.168.150.3                    1

> dominio.local
Servidor:  server2.dominio.local
Address:  192.168.150.3

Nombre:  dominio.local
Addresses:  192.168.150.3
          192.168.150.15                   2

> dominio.local
Servidor:  server2.dominio.local
Address:  192.168.150.3

Nombre:  dominio.local
Addresses:  192.168.150.15
          192.168.150.3                    3

> dominio.local
Servidor:  server2.dominio.local
Address:  192.168.150.3

Nombre:  dominio.local
Addresses:  192.168.150.3
          192.168.150.15                   4

> dominio.local
Servidor:  server2.dominio.local
Address:  192.168.150.3

Nombre:  dominio.local
Addresses:  192.168.150.15
          192.168.150.3                    5

>
```

Se pueden observar cinco consultas realizadas una después de la otra, y las cinco respuestas (numeradas del 1 al 5 y remarcadas en rojo). En las cinco ocasiones se pregunta por "dominio.local", y el servidor siempre responde con dos IPs asociadas a ese nombre, pero cada vez ordenadas de forma diferente.

La caché DNS se puede reiniciar y borrar su contenido de la siguiente forma:

10. Windows:
    - ipconfig /displaydns → para consultar la caché DNS.
    - ipconfig /flushdns → para reiniciarla y borrar las entradas.

11. Linux:
    - Por defecto no viene instalado el Servicio nscd (Name Service Cache Daemon).

      → sudo apt install bind9
    - Reiniciando este Servicio se borra la caché.

      → sudo /etc/init.d/bind9 restart
    - Estado del Servicio dns

      → sudo /etc/init.d/bind9 status
    - También se puede reiniciar el Servicio de red

      → sudo /etc/init.d/networking restart

VERSIÓN ALUMNO LINKIAFP

### 1.1.7. **Paquetes DNS**

DNS es un protocolo de nivel de aplicación, que no se utiliza a nivel de usuario final, sino que son otros protocolos (o aplicaciones) los que lo utilizan para averiguar una dirección IP. Ejemplo: HTTP, Ping, FTP... utilizan DNS si no saben la dirección IP del destino

DNS funciona sobre UDP, es decir, no establece circuito virtual con el destino, y por tanto no garantiza que el paquete llegue al destino.

Existen 2 tipos de paquete DNS:

12. **Query**: Paquete de solicitud que hace el cliente preguntando la dirección IP de un nombre de dominio al servidor DNS.
13. **Answer** Respuesta que el servidor DNS informando al cliente de la dirección IP de un nombre de dominio.

VERSIÓN IMPRIMIBLE ALUMNO LINKZ FP

# 2. Servidor de nombres (DNS)

## 2.1. Implementación de DNS en Windows Server 2016

En este apartado se muestra como instalar y configurar un servicio DNS en Windows Server 2016.

### 2.1.1. Configuración software de Virtualización

Es importante hacer una correcta configuración del software de virtualización para que la configuración tanto del cliente como el servidor sean las adecuadas. La configuración que se muestra a continuación está realizada con Virtual Box.

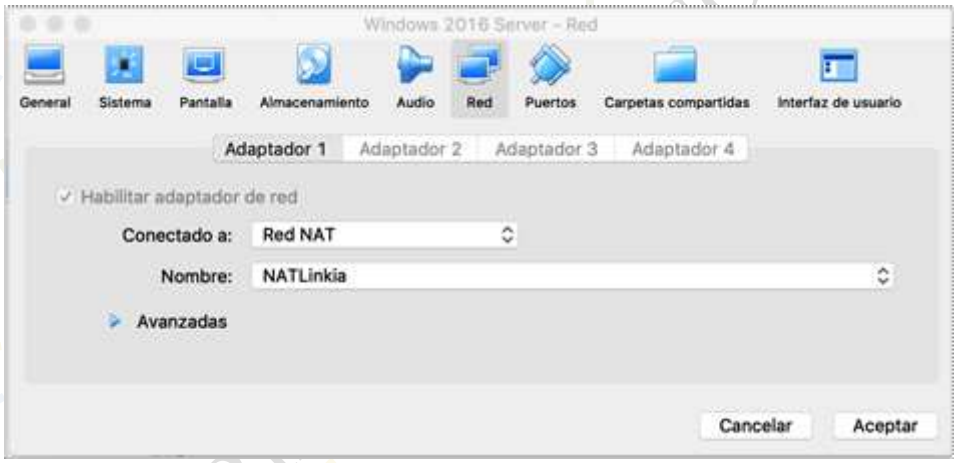
Antes de nada, debemos crear una red NAT entre las máquinas cliente y servidor.

1. Vamos al menú VirtualBox – Preferencias para poder crear una red NAT que después configuraremos en todos los clientes que utilicemos.

2. Creamos una red introduciendo el nombre que queramos y que identifique de forma fácil nuestra red NAT, en este caso hemos puesto NATLinkiaDHCP. Después introduciremos la dirección IP de la red, recordad que ésta acaba en .0 y muy importante desactivar el checkbox que soporta DHCP como se muestra en la imagen.

VERSIÓN IMPRESA LINKIAFP

3. Una vez creada deberemos hacer click en la configuración de las máquinas virtuales y dirigirnos en Red y Adaptador y seleccionamos la Red Nat creada.



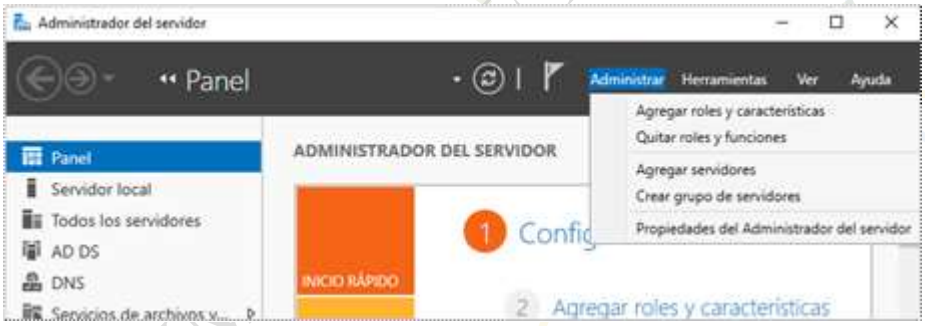

## 2.1.2. **Configuración del servidor DNS en Windows 2016 Server**

Lo primero de todo es configurar la tarjeta de red del servidor para que ésta tenga una configuración de red estática. La IP deberá ser del rango configurado en la red NAT. En el caso que se utilice Virtual Box la puerta de enlace deberá ser la IP interna que virtualiza el software que es la .1 y como dns primario deberemos poner su misma IP ya que él mismo es el servidor dns y como alternativa para tener acceso a Internet, de momento, la 8.8.8.8, como se muestra en la imagen.

### 2.1.3. **Instalación y puesta en marcha**

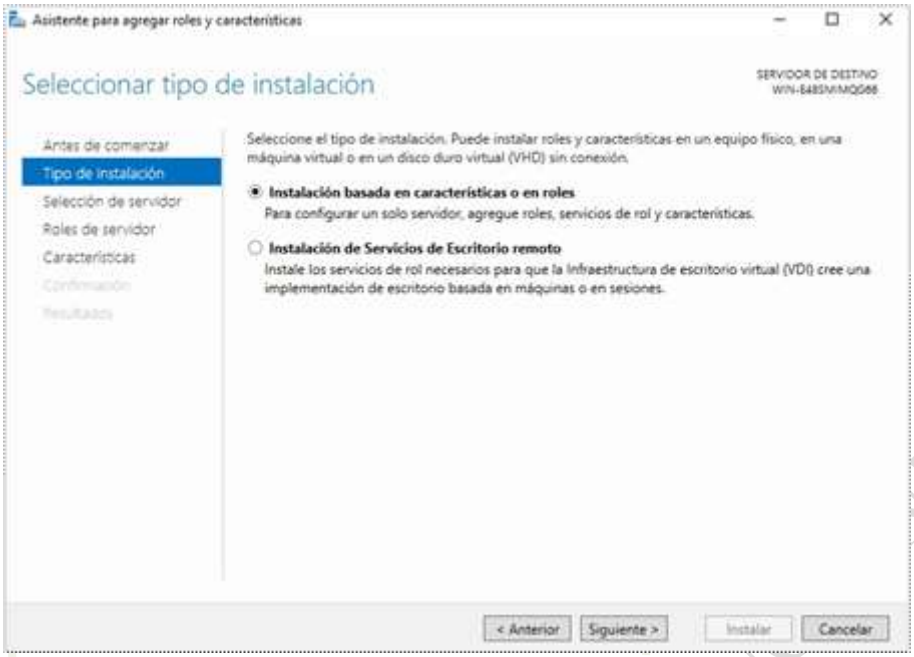
El servicio de DNS forma parte del sistema operativo, pero se debe añadir el rol correspondiente. Es imprescindible que el servidor esté configurado con una IP estática.

Desde el administrador del servidor, se debe agregar el rol:

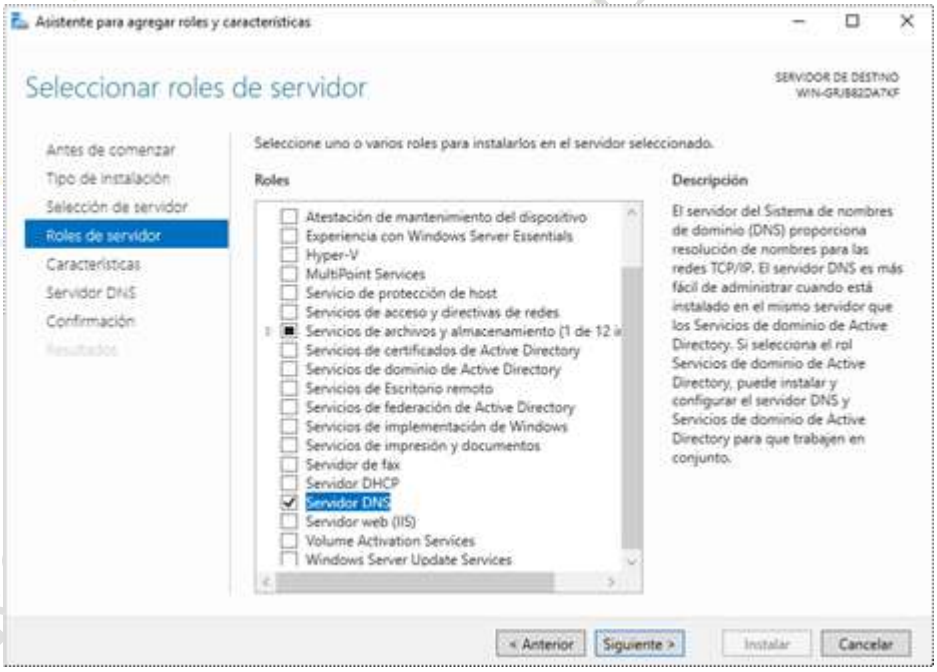



En el tipo de instalación se seleccionará la Instalación basada en características o en roles:

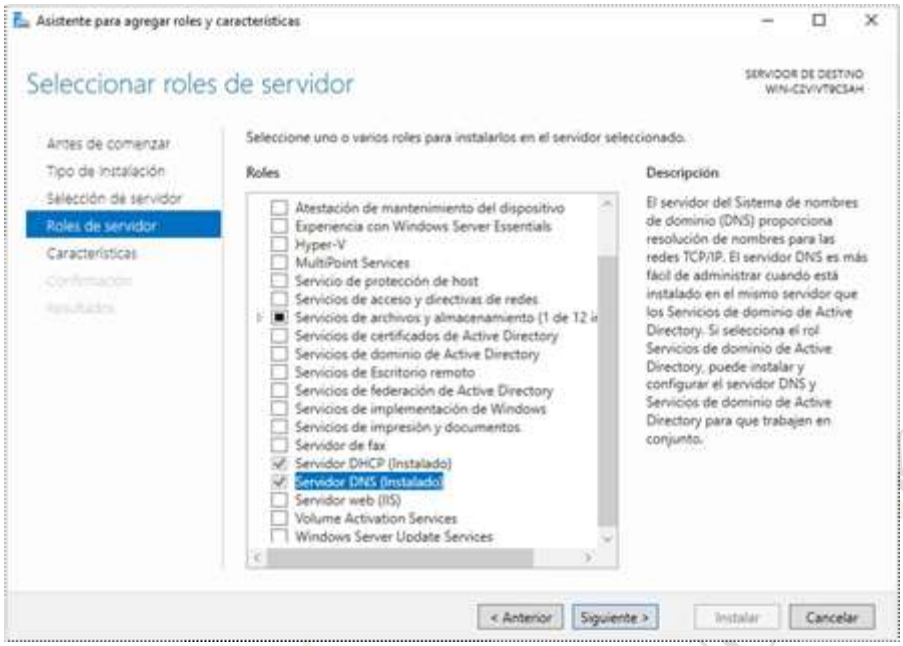
VERSIÓN INTERMEDIA LINKIAFP



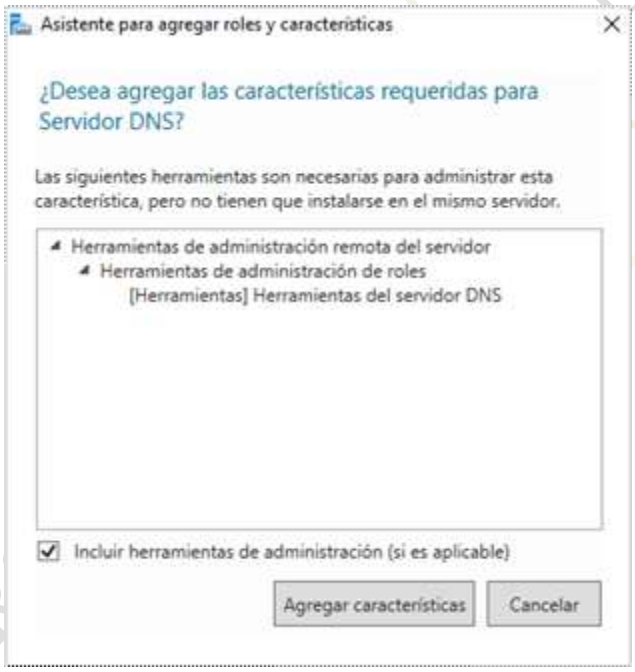

Después de seleccionar al propio servidor como destino de la instalación, se procederá a seleccionar el rol de servidor DNS.



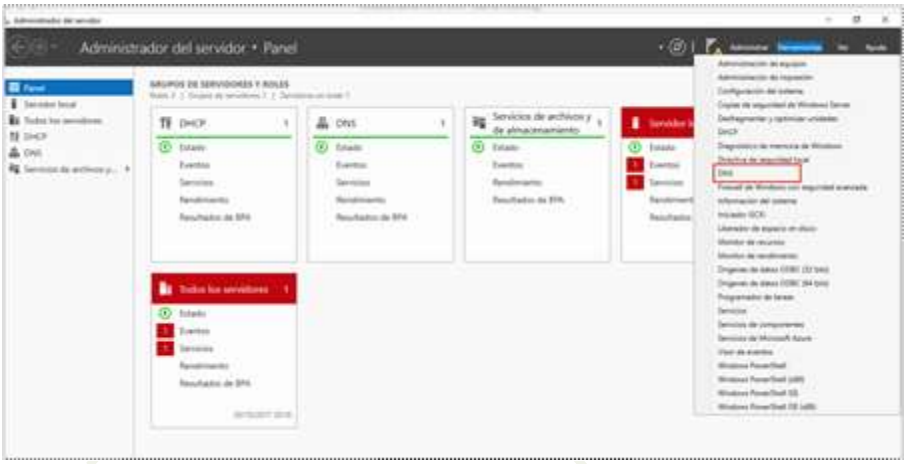

Al seleccionar el rol de servidor DNS es posible que surja un proceso de validación que pida configurar IPs estáticas en el equipo, tanto para IPv4 como para IPv6. SI todo está correcto se podrá seleccionar el rol de DNS.




Al seleccionar el rol, se propone también instalar las características asociadas. Las características son las herramientas, mientras que el rol es el servicio propiamente dicho.




Si todo acaba correctamente, la instalación finaliza y se añade una consola de gestión del servicio, en el administrador del servidor, bajo la opción de Herramientas:




El administrador del DNS muestra los apartados de zonas para su creación.

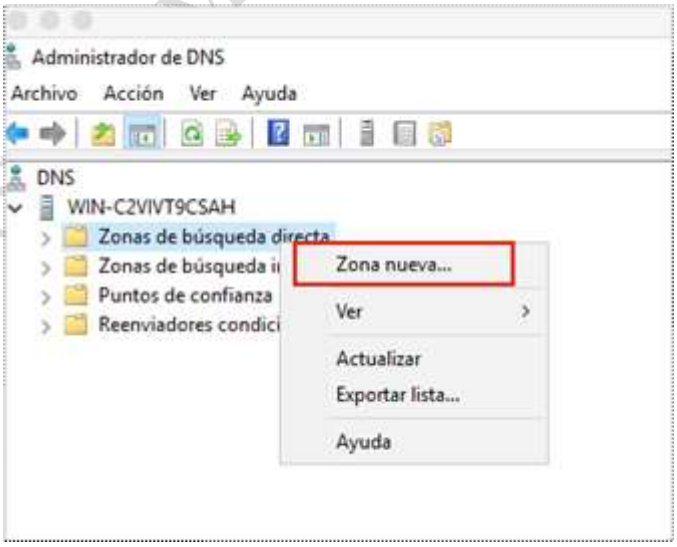
Se dispone de zonas de búsqueda directa y zonas de búsqueda inversa.

Las zonas de búsqueda directa responden a preguntas para obtener una IP a partir de un nombre conocido (registros A), mientras que las zonas de búsqueda inversa responden a preguntas para obtener un nombre a partir de una IP conocida (registros PTR).

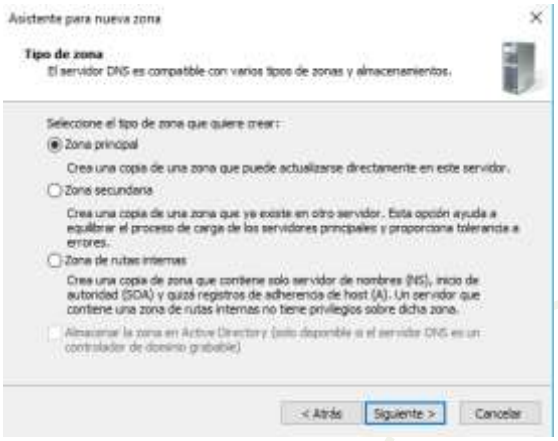
Las zonas de uso más común son las de búsqueda directa, las zonas de búsqueda inversa tienen hoy en día un uso muy reducido.

### 2.1.4. **Creación de zonas y registros**

El elemento esencial donde se almacenan los registros en un servidor DNS es la zona DNS. Para crearla se debe elegir la opción con el botón derecho del ratón en "Zonas de búsqueda directa" y entonces seleccionar "Zona Nueva"

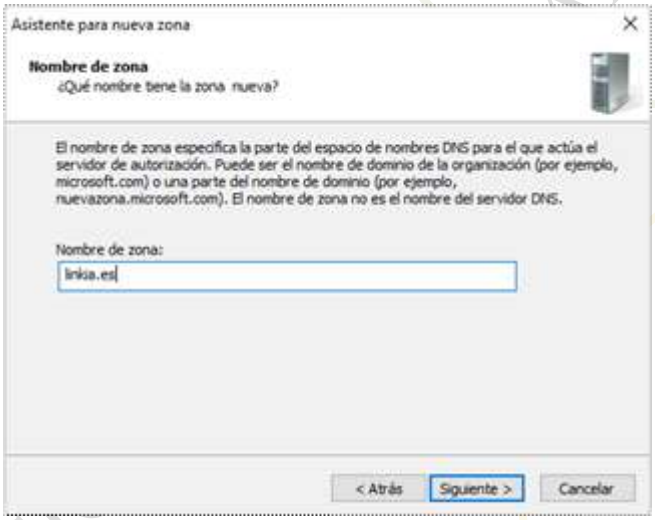


Primero se deberá escoger el tipo de zona, en este caso zona principal:



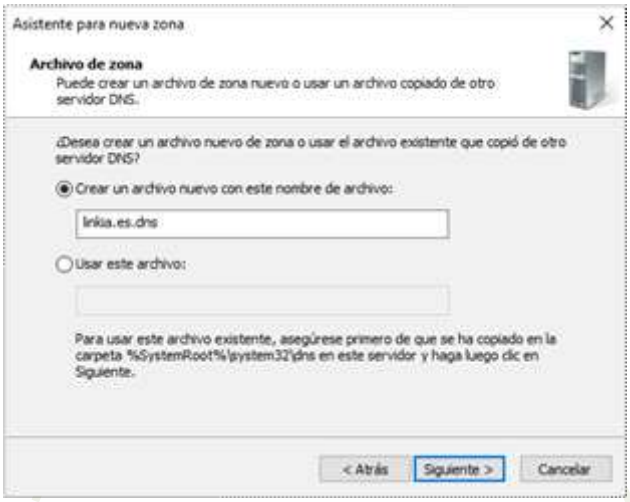

Se podrá elegir entre zona primaria, que se creará desde cero en ese momento, zona secundaria, para la que pedirá identificar al primario correspondiente para sincronizar su contenido con él, además de otras opciones como la zona de rutas internas y el almacenamiento de la zona DNS dentro de Active Directory.

Después se deberá elegir un nombre para la zona



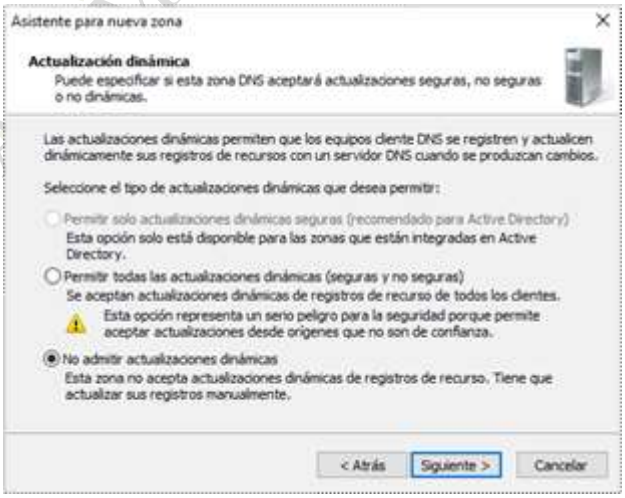

VERSIÓN ALUMNO INKIAFP

A continuación se puede especificar el nombre del fichero de zona:

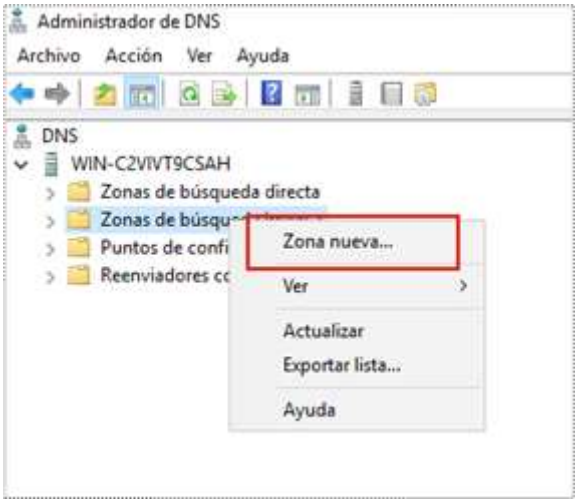



Por defecto el fichero está en la carpeta C:\Windows\system32\dns.

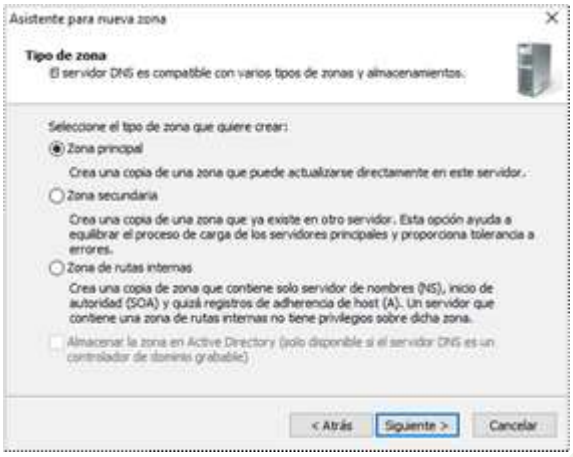
La siguiente decisión es si activar o no las actualizaciones dinámicas en la zona. Si las actualizaciones dinámicas están habilitadas, las máquinas cliente podrán ellas mismas acceder la zona DNS y modificar el registro que les hace referencia. Esto es muy práctico en casos en que todos los PCs de una empresa reciben la IP por DHCP, y por lo tanto no se puede asegurar normalmente que le vayan a proporcionar a un cliente cada día las misma IP. En ese caso, cuando la máquina cliente recibe una IP del DHCP, el cliente acude al servidor DNS a realizar el cambio si es oportuno, y actualizar la IP si es que ha cambiado.

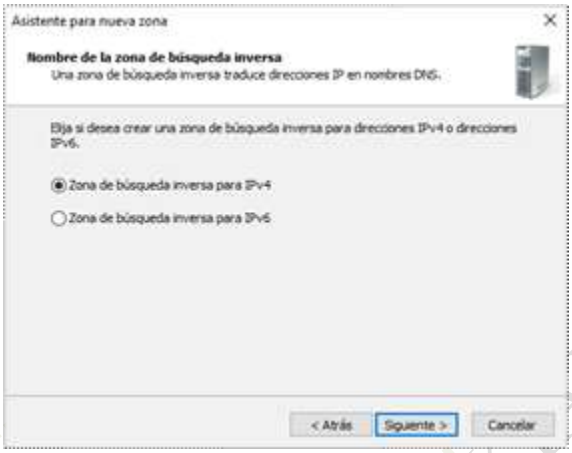


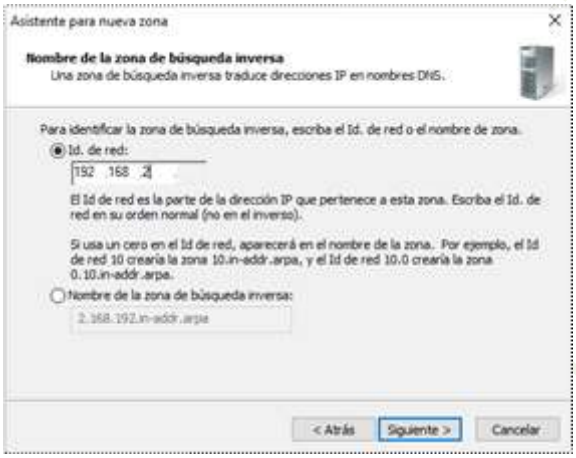

Por defecto, al instalar un servidor DNS quedan las actualizaciones deshabilitadas por motivos de seguridad. Con las actualizaciones dinámicas deshabilitadas, la única forma de crear nuevos registros es hacerlo manualmente.

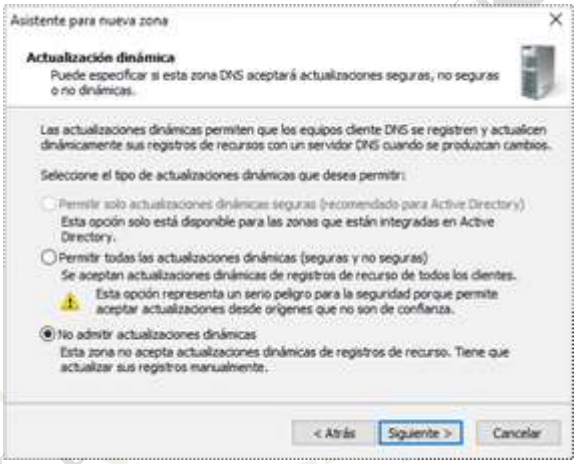



Una vez creada la zona directa se procede a crear la zona inversa.


Asistente para nueva zona
Tipo de zona
El servidor DNS es compatible con varios tipos de zonas y almacenamientos.
Seleccione el tipo de zona que quiere crear:
Zona principal
Crea una copia de una zona que puede actualizarse directamente en este servidor.
Zona secundaria
Crea una copia de una zona que ya existe en otro servidor. Esta opción ayuda a equilibrar el proceso de carga de los servidores principales y proporciona tolerancia a errores.
Zona de rutas internas
Crea una copia de zona que contiene solo servidor de nombres (NS), inicio de autoridad (SOA) y quizá registros de adherencia de host (A). Un servidor que contiene una zona de rutas internas no tiene privilegios sobre dicha zona.
Almacenar la zona en Active Directory (solo disponible si el servidor DNS es un controlador de dominio grabable)
< Atrás
Siguiente >
Cancelar

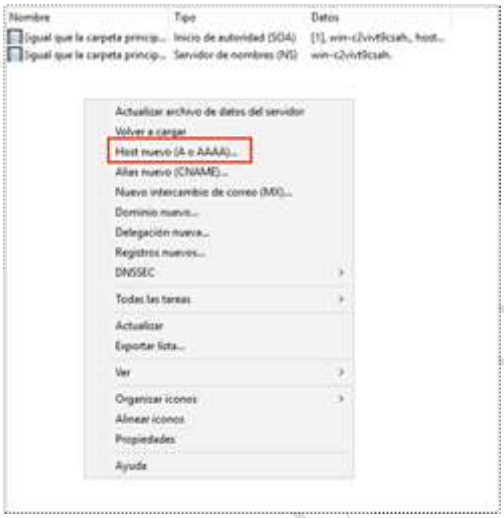

Asistente para nueva zona
Nombre de la zona de búsqueda inversa
Una zona de búsqueda inversa traduce direcciones IP en nombres DNS.
Elija si desea crear una zona de búsqueda inversa para direcciones IPv4 o direcciones IPv6.
Zona de búsqueda inversa para IPv4
Zona de búsqueda inversa para IPv6
< Atrás
Siguiente >
Cancelar


Asistente para nueva zona
Nombre de la zona de búsqueda inversa
Una zona de búsqueda inversa traduce direcciones IP en nombres DNS.
Para identificar la zona de búsqueda inversa, escriba el Id. de red o el nombre de zona.
Id. de red:
192 168 2
El Id de red es la parte de la dirección IP que pertenece a esta zona. Escriba el Id. de red en su orden normal (no en el inverso).
Si usa un cero en el Id de red, aparecerá en el nombre de la zona. Por ejemplo, el Id de red 10 crearía la zona 10.in-addr.arpa, y el Id de red 10.0 crearía la zona 0.10.in-addr.arpa.
Nombre de la zona de búsqueda inversa:
2.168.192.in-addr.arpa
< Atrás
Siguiente >
Cancelar


Asistente para nueva zona
Actualización dinámica
Puede especificar si esta zona DNS aceptará actualizaciones seguras, no seguras o no dinámicas.
Las actualizaciones dinámicas permiten que los equipos cliente DNS se registren y actualicen dinámicamente sus registros de recursos con un servidor DNS cuando se produzcan cambios.
Seleccione el tipo de actualizaciones dinámicas que desea permitir:
Permitir solo actualizaciones dinámicas seguras (recomendado para Active Directory)
Esta opción solo está disponible para las zonas que están integradas en Active Directory.
Permitir todas las actualizaciones dinámicas (seguras y no seguras)
Se aceptan actualizaciones dinámicas de registros de recurso de todos los clientes.
Esta opción representa un serio peligro para la seguridad porque permite aceptar actualizaciones desde orígenes que no son de confianza.
No admitir actualizaciones dinámicas
Esta zona no acepta actualizaciones dinámicas de registros de recurso. Tiene que actualizar sus registros manualmente.
< Atrás
Siguiente >
Cancelar

Asistente para nueva zona
Finalización del Asistente para nueva zona
Se ha completado correctamente el Asistente para nueva zona. Ha especificado la siguiente configuración:
Nombre: 2.168.192.in-addr.arpa
Tipo: Primaria estándar
Tipo de búsqueda: Invertir
Nombre de archivo: 2.168.192.in-addr.arpa.dns
Nota: ahora debe agregar registros a la zona o asegurarse de que los registros se actualizan dinámicamente. A continuación, compruebe la resolución de nombres con nslookup.
Para cerrar este asistente y crear la zona nueva, haga clic en Finalizar.
< Atrás
Finalizar
Cancelar

Una vez creada la zona se puede proceder a crear manualmente los registros. Es importante que el checkbox de crear registro del PTR (pointer) esté activado para que se cree que registro de la zona inversa asociado. Por ejemplo, para crear un registro tipo A, se realiza un click con el botón derecho en la zona recién creada y se selecciona "Host Nuevo (A o AAAA)..."




Debido a que se trata de una zona primaria, en ella se pueden crear diferentes tipos de registros y configuraciones, es decir, es modificable.

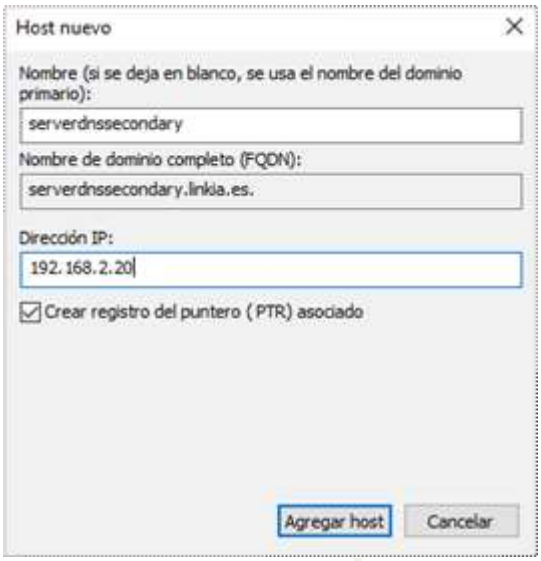
Al elegir crear un host nuevo tipo A, aparece la siguiente ventana

Se observa que se deberá introducir un nombre de host, sólo en su parte inicial ya que el sistema completará el nombre con el nombre de dominio, para construir el nombre completo DNS, o FQDN. En el ejemplo se observa cómo tras introducir "serverdns" en el

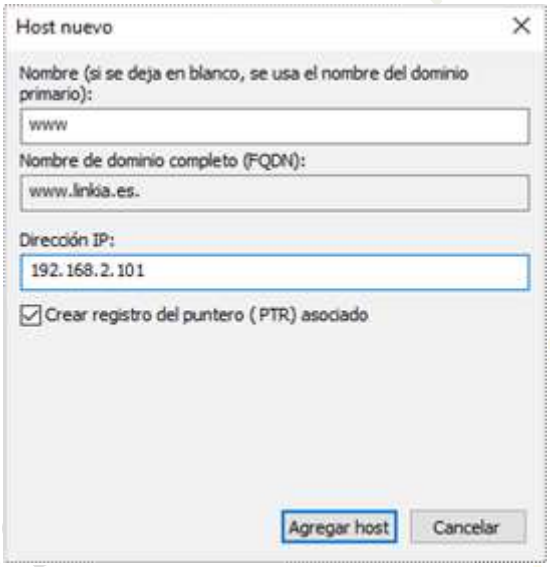
VERSIÓN IMPRIMIBLE AL © LINKIAFP

Nombre, se genera automáticamente el FQDN "servidor.linkia.es." Por último, se deberá asignar una IP a ese nombre (en el ejemplo 192.168.2.10).

Creamos un nuevo host A:




En este ejemplo se observa cómo tras introducir "serverdnssecondary" en el Nombre, se genera automáticamente el FQDN "serverdnssecondary.linkia.es." Asignamos una IP a ese nombre (en el ejemplo 192.168.2.20).

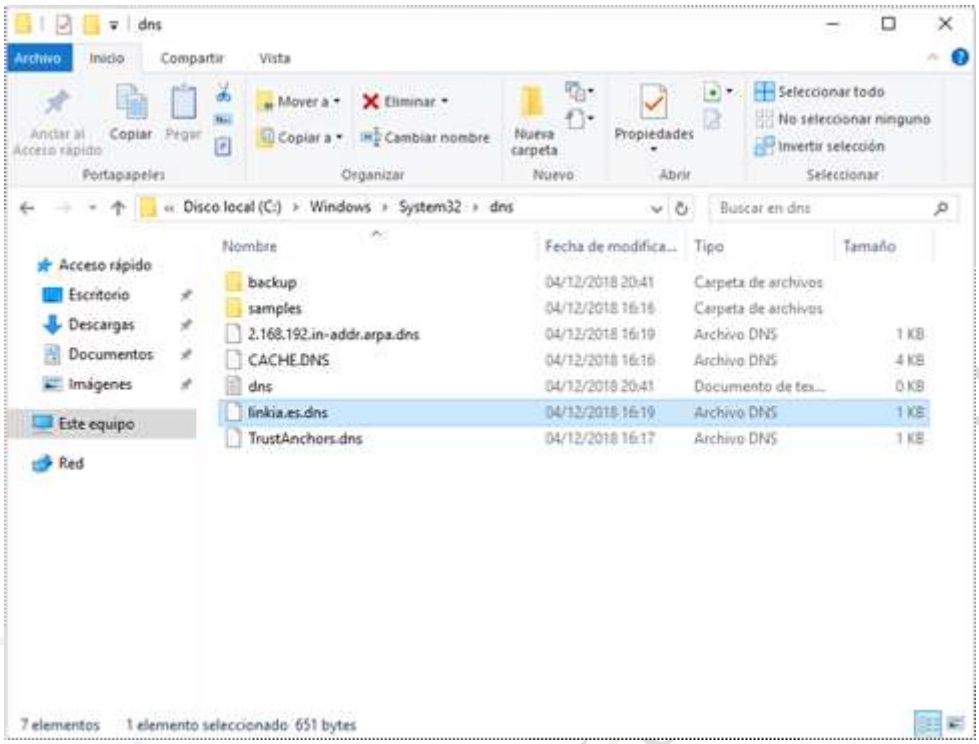



En este ejemplo se observa cómo tras introducir "www" en el Nombre, se genera automáticamente el FQDN "www.linkia.es." Asignamos una IP a ese nombre (en el ejemplo 192.168.2.101).

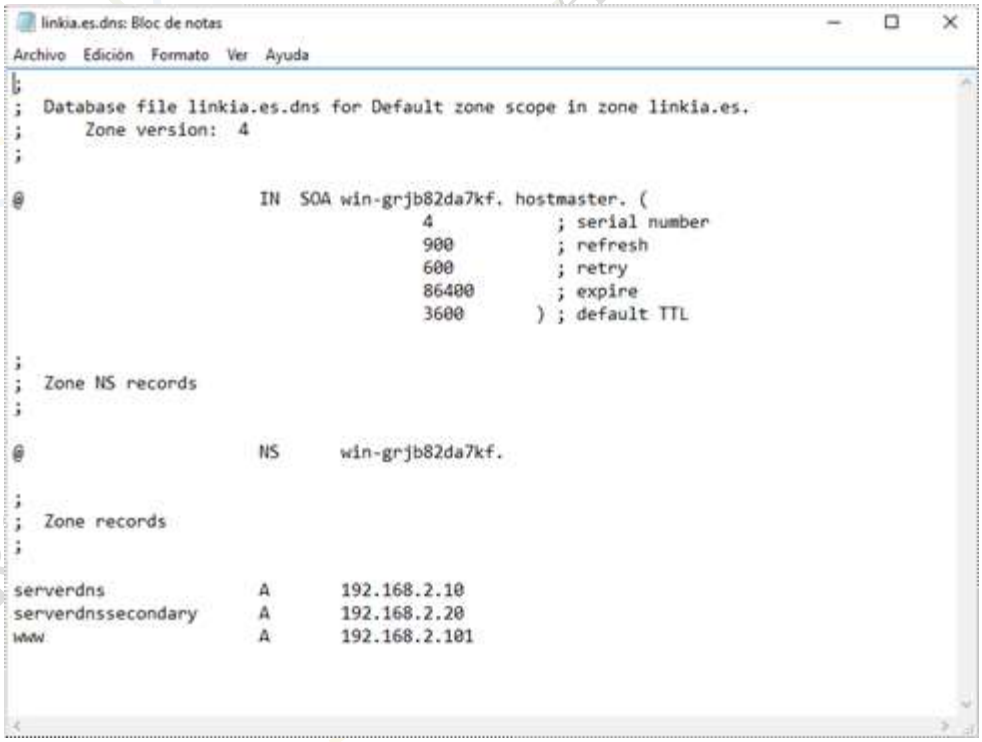
Toda la información queda almacenada en un simple fichero de texto. Se puede comprobar la ubicación del fichero en cuestión, aunque en Windows no será necesario editarlo manualmente, ya que se deben realizar todas las operaciones en la consola DNS.

VERSIÓN ALUMNO LINKIAFP

A continuación, se observa la ubicación del fichero de zona:




Si se abre el fichero se puede observar la sintaxis de los ficheros de zona DNS.




Una zona primaria recién creada sólo contiene, como se puede observar, el registro SOA, que identifica al servidor como el autoritativo en la zona, además de un registro NS, que identifica también al servidor como un servidor DNS.

En este caso también se observa la presencia de los registros A creado anteriormente.

Para hacer una comprobación final del servicio se puede ejecutar el comando "nslookup" preguntando por el registro creado, desde un cliente externo con conectividad con el servidor DNS instalado.

```
C:\Users\Administrador>nslookup
Servidor predeterminado:  serverdns.linkia.es
Address:  192.168.2.10

> serverdns.linkia.es
Servidor:  serverdns.linkia.es
Address:  192.168.2.10

Nombre:  serverdns.linkia.es
Address:  192.168.2.10

> serverdnssecondary.linkia.es
Servidor:  serverdns.linkia.es
Address:  192.168.2.10

Nombre:  serverdnssecondary.linkia.es
Address:  192.168.2.20

> www.linkia.es
Servidor:  serverdns.linkia.es
Address:  192.168.2.10

Nombre:  www.linkia.es
Address:  192.168.2.101
```

Al hacer la pregunta desde un cliente externo por el host "serverdns.linkia.es", el servidor DNS responde identificándose con su IP (192.168.2.10) y a continuación aparece la respuesta a la pregunta, que en el ejemplo es la IP 192.168.2.10.

Cabe destacar que el servido DNS no se preocupa de que la IP que envía como respuesta esté operativa. En el ejemplo mostrado, el servidor informa al cliente de que la IP que busca es la IP 192.168.2.10 o la 192.168.2.20 o la 192.168.2.101, porque así consta en su zona DNS, entonces es el cliente quien debe llegar a esa IP, el servidor DNS no lleva el tráfico del cliente hasta esa IP. Una vez el cliente es informado de la IP de destino, él mismo tiene que llegar a ella. SI la IP no está operativa, la comunicación fallará, pero el DNS habrá respondido por completo a la pregunta, a partir de ahí no es su problema si el cliente llega a la IP o no.

También se puede comprobar que el DNS funciona con el comando ping. Recordar que se deberá desactivar el firewall para que de respuesta.

```
C:\Users\Administrador>ping serverdns.linkia.es

Haciendo ping a serverdns.linkia.es [192.168.2.10] con 32 bytes de datos:
Respuesta desde 192.168.2.10: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.2.10: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.2.10: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.2.10: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.2.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

### 2.1.5. **Zonas secundarias**

Para proporcionar al servicio DNS de alta disponibilidad y poder repartir la carga entre varios servidores se pueden instalar diversas zonas secundarias replicadas de la zona primaria.

Una vez creada la zona primaria se muestra a continuación el procedimiento para instalar una zona secundaria asociada.

En primer lugar, será necesario acudir a la zona primaria para permitir la transferencia de la zona hacia otros servidores secundarios.

Por defecto las transferencias no están permitidas por motivos de seguridad.

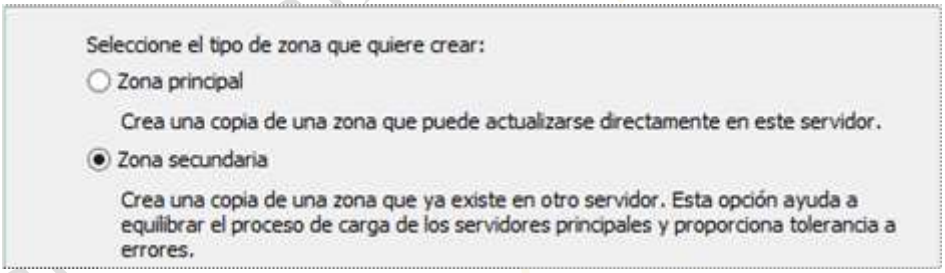
Haciendo click con el botón derecho en la zona primaria se debe seleccionar las propiedades de la zona:

VERSIÓN IMPRIMIBLE PARA USO ALUMNO LINKIAFP

Se puede habilitar la transferencia de la zona a cualquier servidor, o se pueden especificar los servidores a los que se permite enviar una copia de la zona.

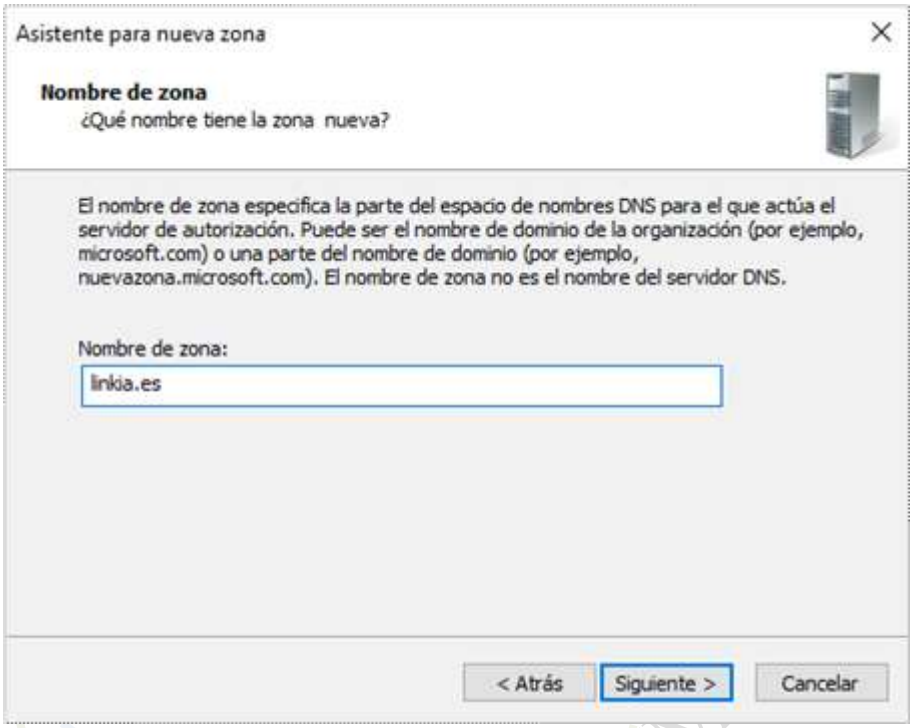
Después de permitir el envío desde la zona primaria se debe crear la zona secundaria con el mismo nombre en otro servidor.

Después de instalar el servicio DNS en un nuevo servidor se crea una nueva zona, pero esta vez de tipo secundaria:

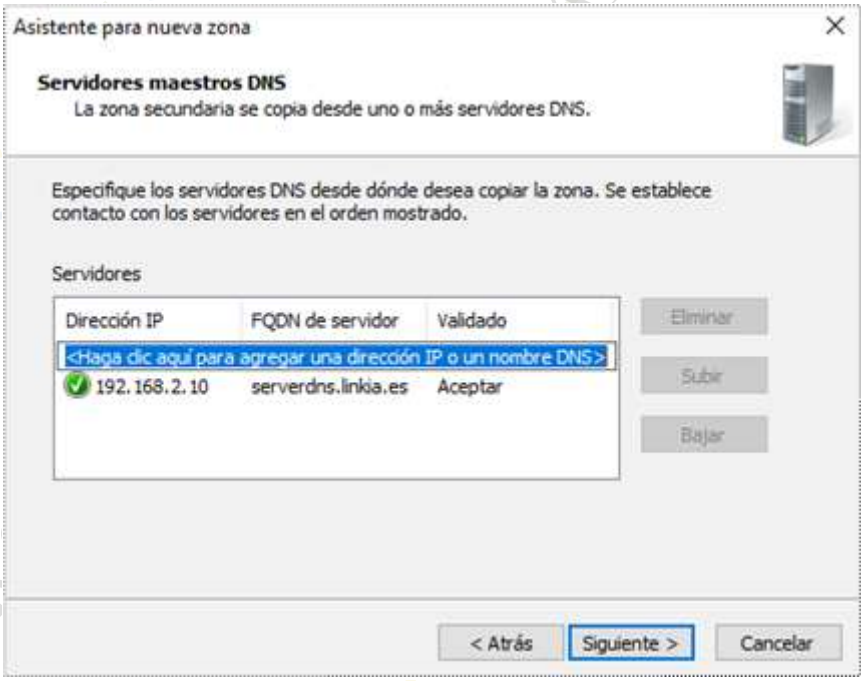



A continuación pedirá el nombre de la zona, que <u>obligatoriamente tendrá que ser igual que el de la zona primaria.</u>

VERSIÓN DE USO EXCLUSIVO LINKIAFP

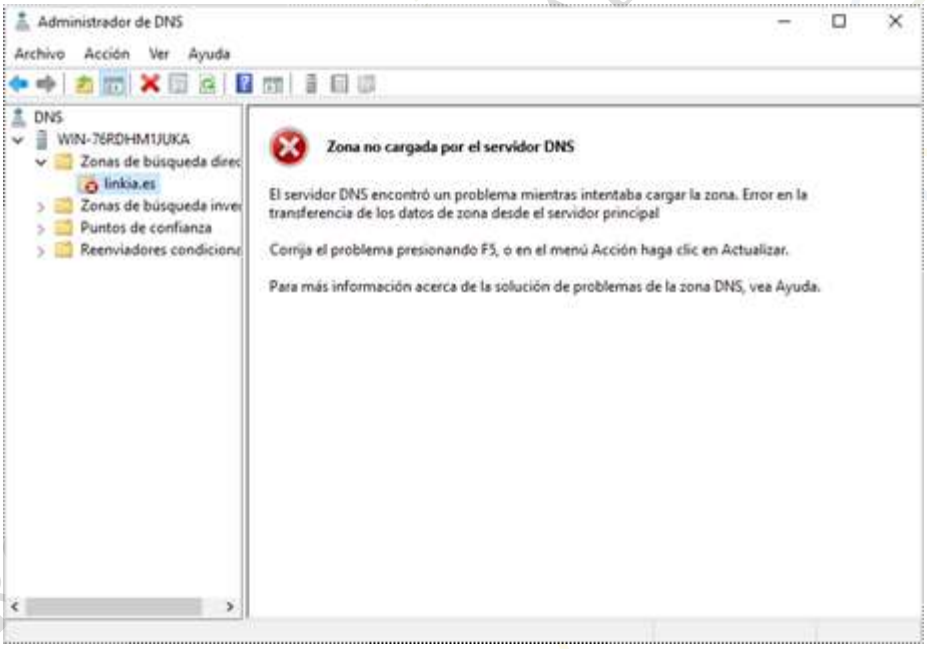



A continuación, se pedirá que se introduzca la IP del servidor que alberga la zona primaria, con el que debe haber conectividad:

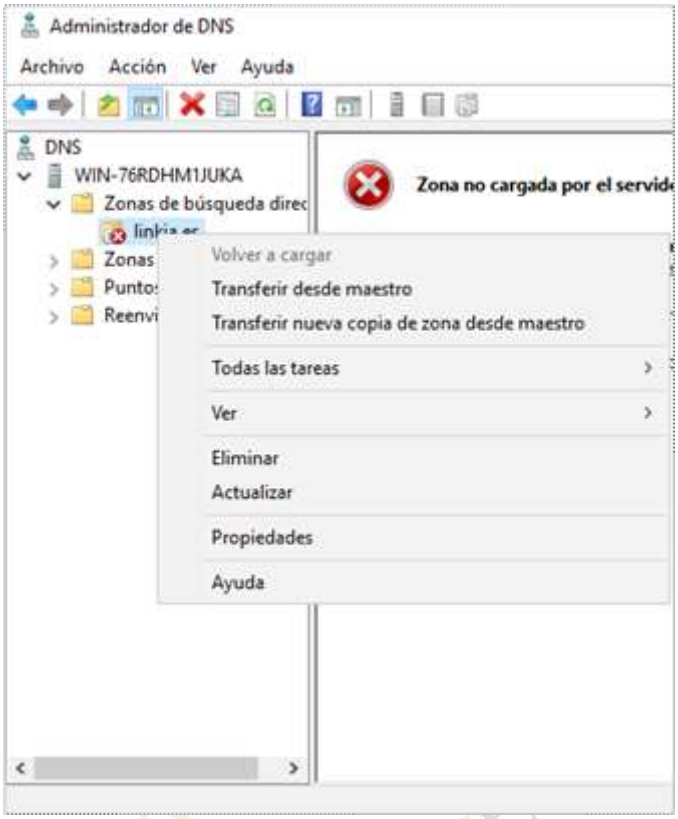



En la imagen mostrada, 192.168.2.10 es la IP del servidor primario o maestro (master).

Es posible que si está recién creada la zona informe con error de que la zona no se ha cargado desde el primario aún:

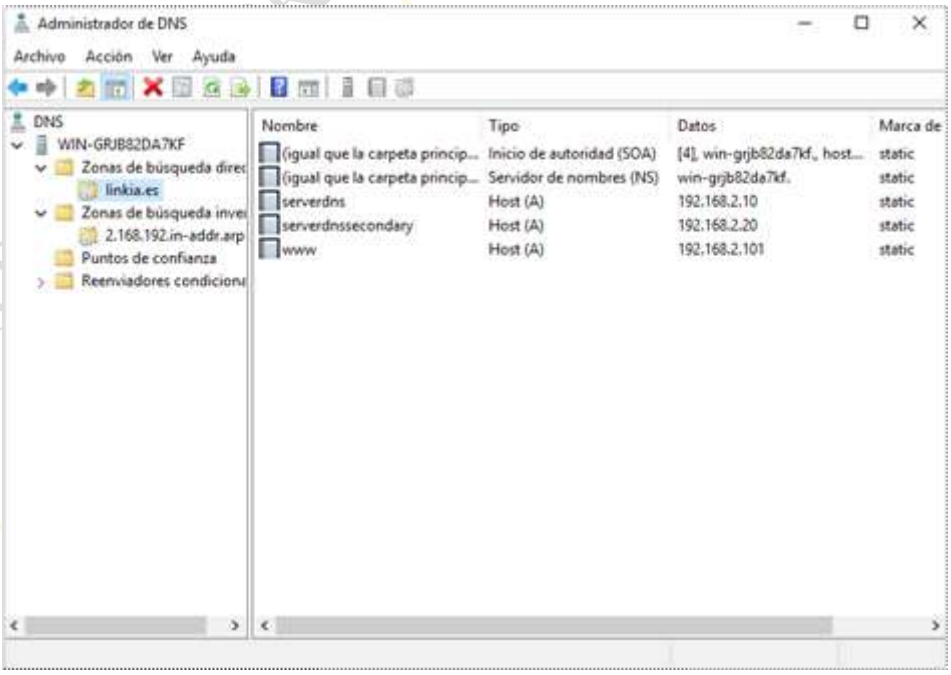


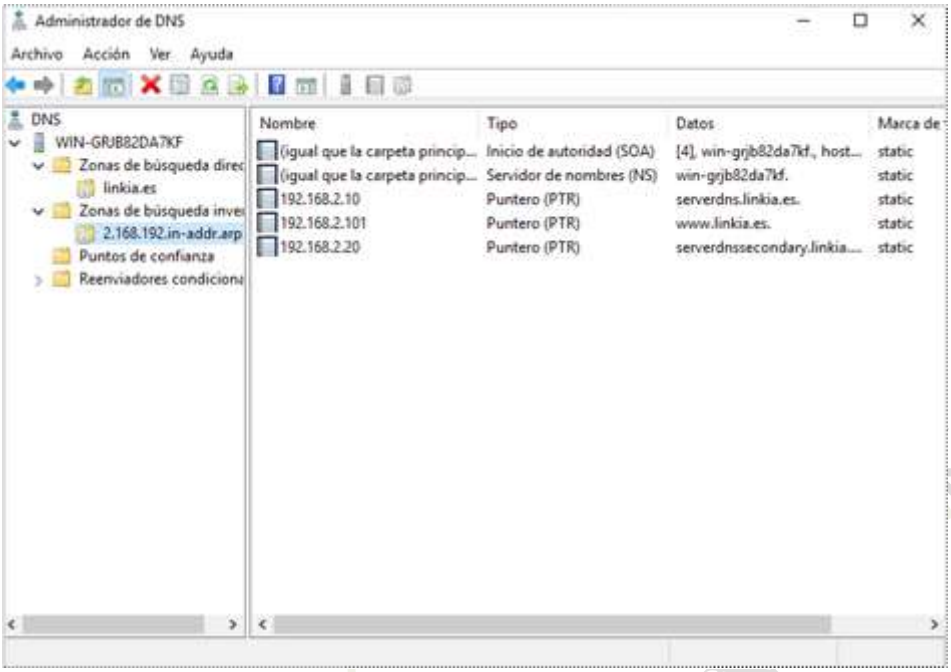
Se puede al principio forzar manualmente la transferencia desde el maestro. La opción aparece con el botón derecho en la zona:



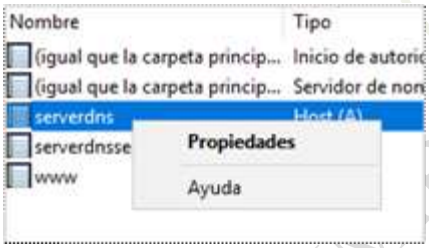

Después de crear la zona secundaria directa, se deberá hacer el mismo proceso con la zona inversa, especificando el identificador de la red, que en este caso, es 192.168.2.

En cualquier caso, después de reiniciar y quizá deshabilitar firewall, las zonas secundarias se verán accesibles en pocos minutos.






Para darse cuenta de que esta zona no es modificable se puede comprobar que los registros no se pueden borrar y que no se pueden crear registros nuevos. Sin embargo, el servicio es capaz de responder a todas las consultas DNS que le hagan sobre la zona.

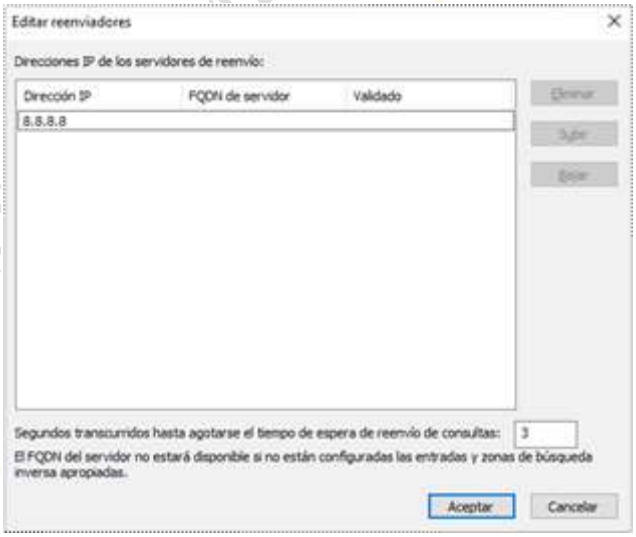


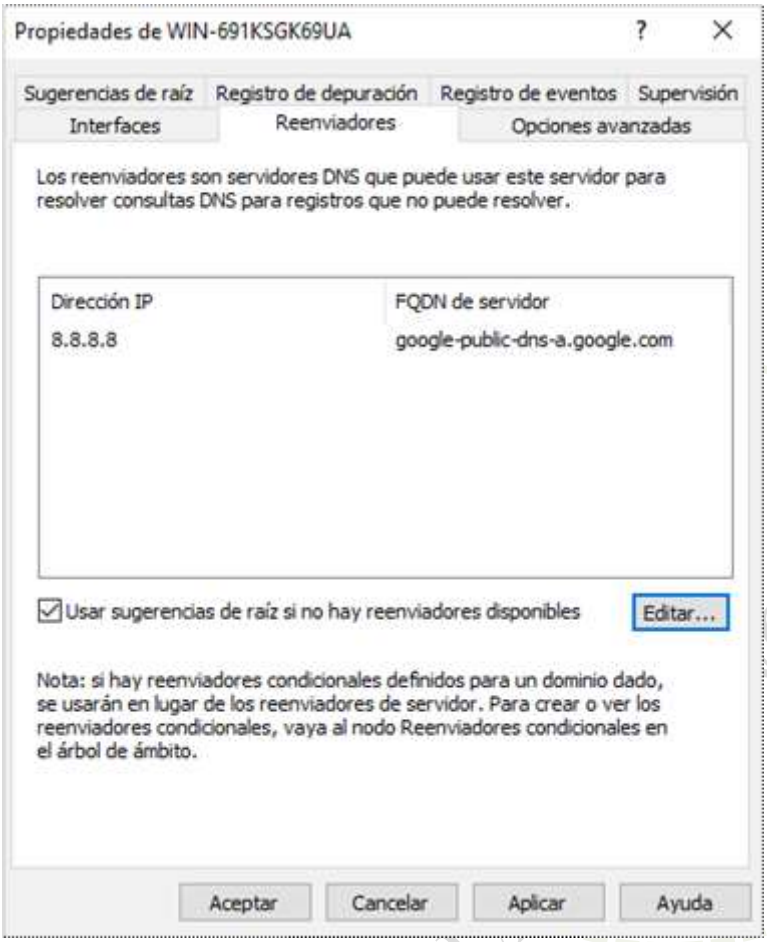

El último paso necesario sería que los clientes no sólo apuntaran a un servidor DNS, sino que hicieran uso de los dos, uno como preferido, y el otro en caso de que el primero no responda. Esto se consigue configurando las dos IPs de los dos servidores DNS en la configuración de red de los clientes.

### 2.1.6. **Reenviadores y servidores raíz**

Cuando al servidor le preguntan por un nombre que no pertenece a sus zonas locales, ni tiene la respuesta en la caché, entonces tiene que acudir a otros servidores para obtener la respuesta.

Es posible decidir a qué servidores preguntará el servidor DNS cuando no sabe alguna respuesta a las preguntas que le hacen. Esto se decide configurando los reenviadores. Dicha pestaña de configuración se encuentra accediendo a las propiedades del servidor DNS desde la consola DNS:



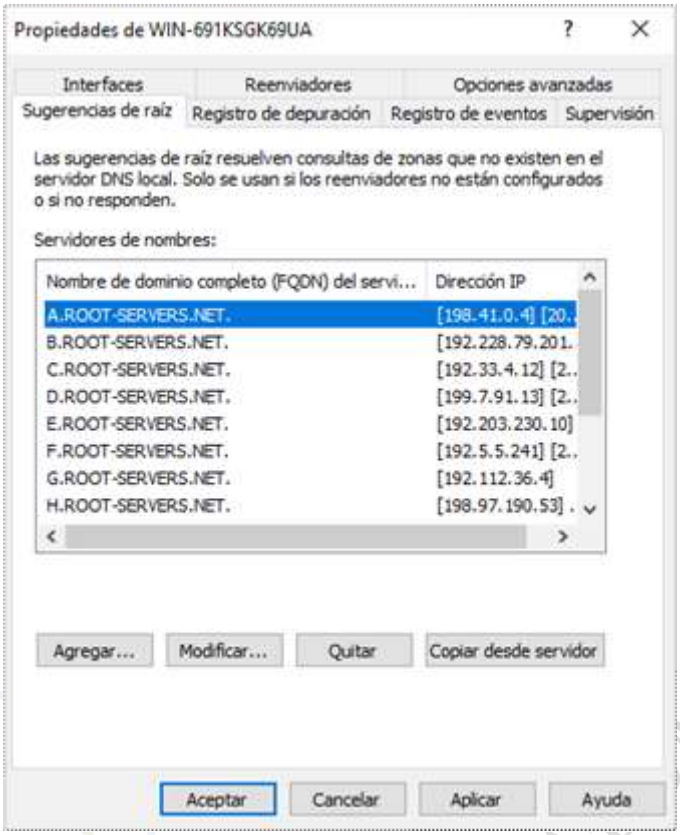



En la imagen mostrada, se le preguntará al servidor 8.8.8.8 (que es un DNS público) todo aquello que el servidor no sepa de forma local.

Se puede configurar una lista de reenviadores, en caso de que alguno de ellos no responda, se reformulará la pregunta al siguiente.

Cuando no hay reenviadores configurados, por defecto el servidor DNS pasa las preguntas a los servidores raíz (root servers) que tiene configurados en la pestaña "Sugerencias de Raíz"

VERSIÓN NO VENDIBLE © LINKIAFP




En esta pestaña ya constan precargadas las IPs de los servidores DNS públicos que albergan la zona raíz. A partir de ellos se podrá obtener la respuesta necesitada.

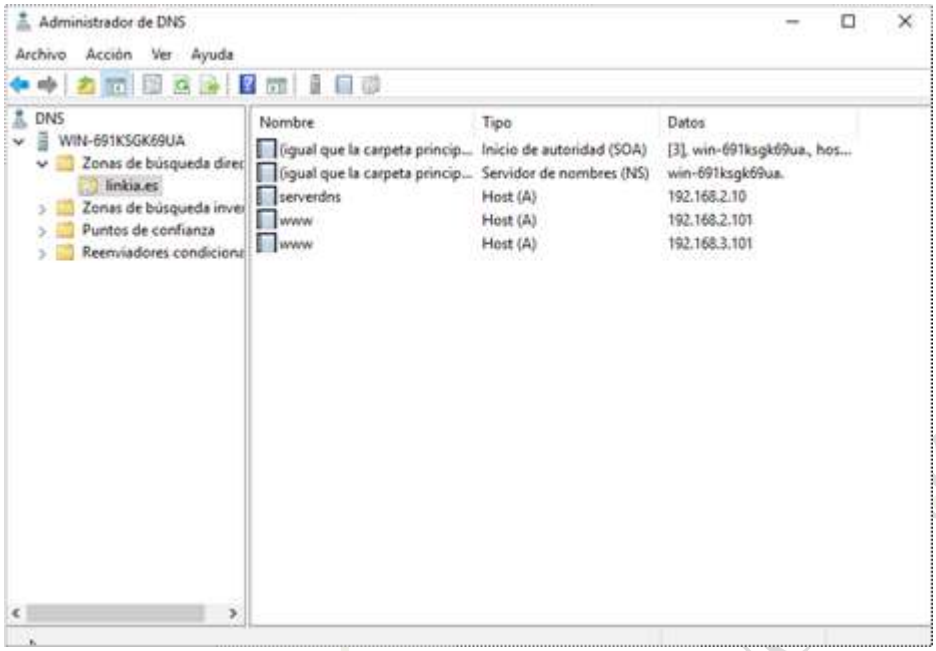
Es posible que reenviar las preguntas a los servidores raíz no sea lo más óptimo, ya que pueden estar lejos geográficamente, y el camino final hasta obtener una respuesta puede ser largo ya que pasaría por todos los niveles. Configurar un reenviador conocido y próximo puede agilizar el proceso de resolución ya que quizás además tenga la IP preguntada en su caché y entonces la respuesta será inmediata.

### 2.1.7. **Round Robin DNS**

El Round Robin de DNS es un mecanismo muy simple y fácil de configurar que aporta tanto alta disponibilidad como balanceo de carga.

Para implementarlo tan sólo es necesario crear dos registros con el mismo nombre y diferentes IPs. De esta forma ya funcionará el Round Robin DNS:

VERSIÓN IMPRESA ALUMNO LINKIAFP



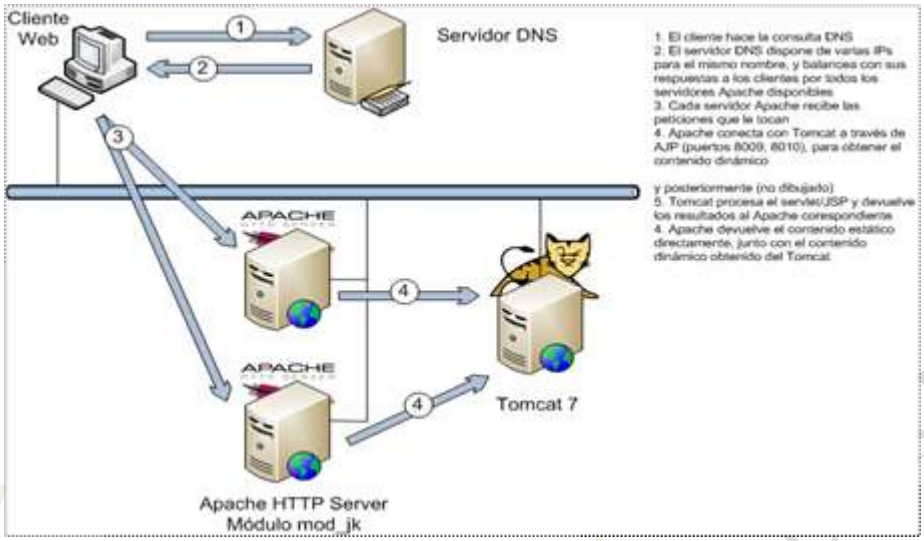

Como se puede ver, asociado al mismo nombre "www.linkia.es" hay dos IPs diferentes. Si ahora se pregunta al servidor por ese nombre, cada vez devolverá toda la lista de IPs (192.168.2.101 y la 192.168.3.101) pero cada vez en un orden distinto.

Observe las siguientes consultas realizadas con nslookup:

```
C:\Users\Administrador>nslookup
Servidor predeterminado:  serverdns.linkia.es
Address:  192.168.2.10

> www.linkia.es
Servidor:  serverdns.linkia.es
Address:  192.168.2.10

Nombre:  www.linkia.es
Addresses:  192.168.2.101
          192.168.3.101
```

Se pueden lanzar preguntas desde el propio servidor a sí mismo para comprobar el funcionamiento del mecanismo Round Robin. En la imagen se observa cómo cada vez que se pregunta por el nombre www.linkia.es, el servidor responde con las dos IPs asociadas, pero cada vez en un orden diferente.

Un ejemplo de aplicación en el entorno de servidores de aplicaciones web sería el siguiente:



http://docs.oracle.com

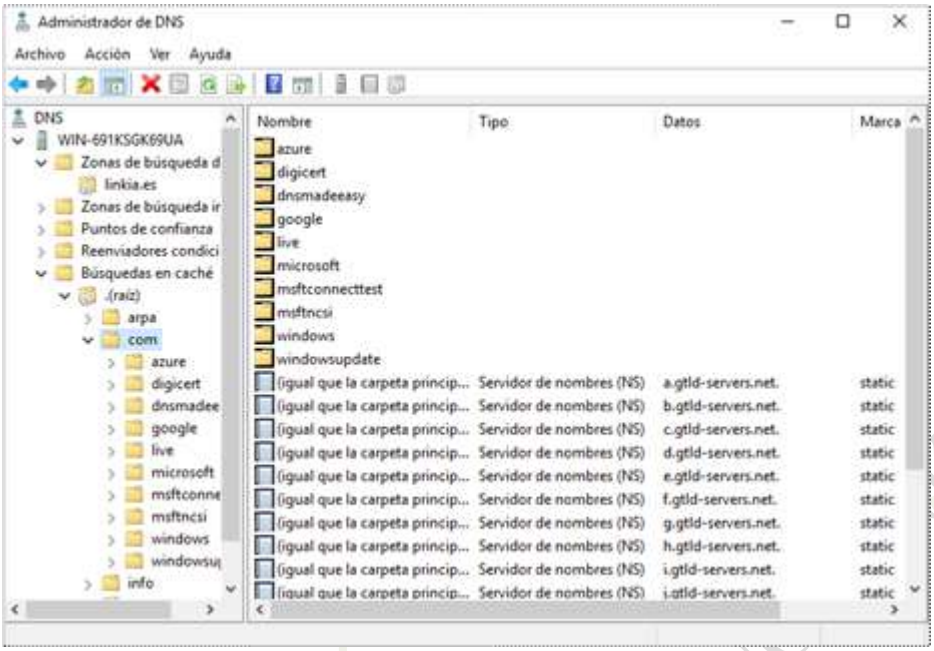
### 2.1.8. **Caché en el servidor DNS**

El servidor DNS, cuando consigue la respuesta para un cliente, además de pasársela al cliente, también se la guarda en memoria caché. De esa forma, si alguien le vuelve a preguntar por lo mismo, ya tiene la respuesta en local y puede responder mucho más rápido.

En la consola DNS, la memoria caché no es visible directamente, se deben habilitar las características avanzadas.

En el menú "Ver" de la consola DNS se puede habilitar la vista Avanzada:

Una vez habilitada, se puede observar el contenido de la caché en la consola




Todos los registros presentes son consultas previas que ya han sido resultas y almacenadas en caché. En la imagen se ven agrupadas todas las consultas resueltas con el dominio ".com" y el dominio ".net".

## 2.2. Implementación de DNS en Ubuntu Server

En este apartado se instalará BIND (Berkeley Internet Name Domain) en Ubuntu Server 18.04. BIND es el software DNS más utilizado en Internet y se ha convertido en un estándar de facto. Actualmente es vigente su versión 9, que fue escrita desde cero.

### 2.2.1. Configuración del servidor DNS en Ubuntu Server 18.04

Lo primero de todo es configurar la tarjeta de red del servidor para que ésta tenga una configuración de red estática. La IP deberá ser del rango configurado en la red NAT. En el caso que se utilice Virtual Box la puerta de enlace deberá ser la IP interna que virtualiza el software que es la .1 y como dns primario deberemos poner su misma IP ya que él mismo es el servidor dns y como alternativa para tener acceso a Internet configuraremos la 8.8.8.8, como se muestra en la imagen.

```
# This file is generated from information provided by
# the datasource.  Changes to it will not persist across an instance.
# To disable cloud-init's network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    ethernets:
        enp0s3:
            addresses:
            - 192.168.2.30/24
            gateway4: 192.168.2.1
            nameservers:
                addresses:
                - 192.168.2.30
                - 8.8.8.8
                search: []
            optional: true
    version: 2
"/etc/netplan/50-cloud-init.yaml" 18L, 609C                    15,21         Todo
```

## 2.2.2. **Instalación y puesta en marcha**

La instalación en Ubuntu Server puede realizarse mediante apt install bind9.

```
linkia@linkia:~$ sudo apt install bind9
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
bind9 ya está en su versión más reciente (1:9.11.3+dfsg-1ubuntu1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
```

Una vez instalado el servicio está en marcha. Se crea el usuario y grupo de nombre "bind" y el servicio se pone a la escucha en el puerto 53. Mediante el comando "netstat -nat" se pueden comprobar los puertos que tiene a la escucha el servidor, entre los que se debe encontrar el puerto 53 del DNS:

```
linkia@linkia:~$ netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.2.30:53         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 192.168.2.30:34213      192.203.230.10:53       TIME_WAIT
tcp        0      0 192.168.2.30:51783      192.203.230.10:53       TIME_WAIT
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
```

De forma opcional, se pueden instalar herramientas de diagnóstico mediante:

```
linkia@linkia:~$ sudo apt install dnsutils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
dnsutils ya está en su versión más reciente (1:9.11.3+dfsg-1ubuntu1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
```

Los archivos de configuración del servicio están almacenados en el directorio /etc/bind:

```
linkia@linkia:~$ cd /etc/bind/
linkia@linkia:/etc/bind$ ls
bind.keys  db.255    db.root                  named.conf.local    zones.rfc1918
db.0       db.empty  named.conf                named.conf.options
db.127     db.local  named.conf.default-zones rndc.key
```

El archivo principal de configuración es /etc/bind/named.conf:

```
  GNU nano 2.9.3                          named.conf

// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

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

Como se puede observar, en dicho archivo están simplemente mencionados los demás archivos de configuración del servicio.

En el archivo /etc/bind/db.root: Están las IPs de los root servers precargados:

```
  GNU nano 2.9.3                          db.root

;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:    February 17, 2016
;       related version of root zone:   2016021701
;
; formerly NS.INTERNIC.NET
;
                         3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
                         3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     192.228.79.201
B.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:84::b
;
; FORMERLY C.PSI.NET
;
                         3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
C.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:2::c
```

Si nada más instalar el servicio se configuran unos reenviadores (lo cual es más eficiente que redireccionar todo a los root servers), estará en marcha ya un servidor caché DNS, sin ninguna zona albergada localmente, pero almacenando en caché todas las consultas que recibe. De alguna forma también se puede entender esta configuración como la de un "proxy" DNS.

Para configurar reenviadores, se edita el fichero /etc/bind/named.conf.options, un ejemplo sería:

```
forwarders {
                1.2.3.4;
                5.6.7.8;
            };
```

Al añadir este bloque de "forwarders", se configura el servicio para que todas las consultas que reciba, y que no sepa contestar con las zonas locales, las reenvíe a los servidores especificados (en el ejemplo 1.2.3.4 y 5.6.7.8).

Para cada cambio realizado en los ficheros de configuración, se debe reiniciar el servicio:

```
linkia@linkia:/etc/bind$ sudo service bind9 restart
```

### 2.2.3. **Zonas y registros**

1. Para configurar una zona primaria y de búsqueda directa se debe primero editar el fichero /etc/bind/named.conf.default-zones. Este fichero por defecto no contiene ninguna zona. Si se desea crear una, se debe seguir la siguiente sintaxis:

```
  GNU nano 2.9.3                    named.conf.default-zones

        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};


//zona directa
zone "linkia.es" {
        type master;
        file "/etc/bind/linkiadirecta.com.zona";
};
```

En la zona consta el nombre "linkia.es", se declara del tipo primaria (master) y se indica la ubicación del archivo de zona, donde estarán todos los registros.

Para el archivo de zona también hay que seguir una sintaxis concreta. Lo más fácil es basarse en una plantilla de ejemplo que se instala con el servicio.

Se puede generar una copia de la plantilla existente y después modificar el fichero de zona según convenga:

```
linkia@linkia:~$ sudo cp /etc/bind/db.local /etc/bind/linkiadirecta.com.zona
```

El fichero "db.local" es la plantilla, y en el ejemplo se ha generado una copia con el nombre al que se ha hecho referencia cuando se declaró la zona en /etc/bind/named.conf.local.

El fichero db.local está pensado para el loopback interface.

Pero a partir de él se puede construir el fichero de zona deseado añadiendo los registros necesarios. Un ejemplo de fichero de zona se muestra a continuación:

```
  GNU nano 2.9.3                          linkiadirecta.com.zona

;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     serverdns.linkia.es. root.linkia.es. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      serverdns.linkia.es.
@       IN      A       195.168.1.10
www     IN      A       195.168.1.101
```

Como siempre, el registro SOA es imprescindible en cualquier fichero de zona, y a partir de ahí se pueden añadir nuevos registros al final del fichero.

En el ejemplo se observa un registro A para el nombre serverdns.linkia.es con la IP 195.168.1.10, para el que después se asocia un registro NS.

1. Editar los forwards (si es necesario) en el fitxer named.conf.options para poder salir a Internet: sudo nano /etc/bind/named.conf.options

```
  GNU nano 2.9.3                     /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 {
                8.8.8.8;
        };

        //========================================================================
        // 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;

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
};
```

2. Para ejecutar el servicio DNS, podemos hacer:

sudo /etc/init.d/bind/bind9 stop/start/restart

Para saber si el Servicio arranca correctamente: sudo service bind9 status o sudo /etc/init.d/bind/bind9 status

VERSIÓN LIMITADA

```
linkia@linkia:/etc/bind$ sudo /etc/init.d/bind9 start
[ ok ] Starting bind9 (via systemctl): bind9.service.
linkia@linkia:/etc/bind$ sudo /etc/init.d/bind9 status
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2018-12-02 12:33:49 UTC; 16min ago
     Docs: man:named(8)
  Process: 1944 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 1947 (named)
    Tasks: 4 (limit: 1113)
   CGroup: /system.slice/bind9.service
           └─1947 /usr/sbin/named -f -u bind

dic 02 12:33:49 linkia named[1947]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
dic 02 12:33:49 linkia named[1947]: managed-keys-zone: Key 19036 for zone . acceptance timer …
dic 02 12:33:49 linkia named[1947]: managed-keys-zone: Key 20326 for zone . acceptance timer …
dic 02 12:33:49 linkia named[1947]: resolver priming query complete
dic 02 12:33:49 linkia named[1947]: checkhints: b.root-servers.net/A (199.9.14.201) missing f…
dic 02 12:33:49 linkia named[1947]: checkhints: b.root-servers.net/A (192.228.79.201) extra r…
dic 02 12:33:49 linkia named[1947]: checkhints: b.root-servers.net/AAAA (2001:500:200::b) mis…
dic 02 12:33:49 linkia named[1947]: checkhints: b.root-servers.net/AAAA (2001:500:84::b) extr…
dic 02 12:33:49 linkia named[1947]: checkhints: l.root-servers.net/AAAA (2001:500:9f::42) mis…
dic 02 12:33:49 linkia named[1947]: checkhints: l.root-servers.net/AAAA (2001:500:3::42) extr…
Hint: Some lines were ellipsized, use -l to show in full.
```

3. Para testear podemos utilizar la herramienta nslookup, que genera consultas DNS.

```
Nombre:  serverdns.linkia.es
Address:  195.168.1.10

> www.linkia.es
Servidor:  UnKnown
Address:  195.168.1.10

Nombre:  www.linkia.es
Address:  195.168.1.101
```

4. La herramienta genérica ping puede servir también para comprobar si la resolución de nombres funciona correctamente.

```
C:\Users\Linkia>ping serverdns.linkia.es

Haciendo ping a serverdns.linkia.es [195.168.1.10] con 32 bytes de datos:
Respuesta desde 195.168.1.10: bytes=32 tiempo<1m TTL=64
Respuesta desde 195.168.1.10: bytes=32 tiempo<1m TTL=64
Respuesta desde 195.168.1.10: bytes=32 tiempo<1m TTL=64
Respuesta desde 195.168.1.10: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 195.168.1.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Linkia>
```

5. La herramienta named-checkzone sirve para revisar el archivo de zona, incluyendo la sintaxis o cualquier otro problema que detecte → named-checkzone linkia.com /etc/bind/linkiad.com

```
linkia@linkia:~$ named-checkzone linkia.es /etc/bind/linkiadirecta.com.zona
zone linkia.es/IN: loaded serial 2
OK
linkia@linkia:~$ _
```

VERSIÓN ALUMNO LINKIA FP

### 2.2.4. **Zonas secundarias**

Para dar alta disponibilidad al servicio se puede replicar la zona creada en un servidor secundario. A continuación se muestra un ejemplo de configuración donde las IPs utilizadas son:

- Primario: 195.168.1.10
- Secundario: 195.168.1.11

En primer lugar se debe permitir la transferencia desde la zona primaria. Para ello se debe añadir lo siguiente al fichero donde se declara la zona primaria:

```
//zona directa
zone "linkia.es"{
        type master;
        file "/etc/bind/linkiadirecta.com.zona";
        allow-transfer { 195.168.1.11; };
};
```

Con el comando "allow-transfer", se permite la transferencia al servidor declarado, en el ejemplo el servidor con IP 195.168.1.11.

A continuación se debe instalar el servicio en un nuevo servidor, y se debe editar el fichero de declaración de zonas (/etc/bind/named.conf.local) de la siguiente manera:

```
//zona directa
zone "linkia.es"{
        type slave;
        file "linkiadirecta.com.zona";
        allow-transfer { 195.168.1.10; };
};
```

Como se puede ver, se declara la zona con el mismo nombre, esta vez del tipo "slave", se indica el fichero de la zona (linkiadirecta.com.zona en el ejemplo), y por último se indica dónde está el servidor primario (master) para ir a buscar la zona y traer una réplica de sólo lectura, en el ejemplo en la IP 195.168.1.10.

# 3. Lightweight Directory Access Protocol (LDAP)

## 3.1. Introducción

LDAP es una versión simple y reducida del estándar X.500 (de ahí el término lightweight = ligero) el cual especifica diferentes servicios de directorio.

LDAP es un protocolo de acceso a información de un directorio (consultas, actualizaciones…), aunque también es considerado una base de datos, pero en realidad es sólo el protocolo de acceso a una base de datos, que podría ser de otro tipo.

Habitualmente LDAP almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse, aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc). A manera de síntesis, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

LDAP puede ayudar a unificar e integrar diferentes sistemas como bases de datos, correo electrónico y otros, ya que actualmente está soportado por muchas aplicaciones y sistemas operativos. Se trata de un estándar abierto.

LDAP permite la delegación y establecimiento de permisos de administración del directorio y soporta la replicación para proporcionar alta disponibilidad al servicio.

LDAP funciona de forma óptima en escenarios con operaciones de lectura intensivas, sin embargo, no es tan eficiente en entornos donde se requieran muchas actualizaciones frecuentemente.

Es muy común utilizar LDAP como base para implantar sistemas de autenticación centralizada y single sign on, donde diferentes servicios, proporcionados por diferentes aplicaciones y servidores, comparten una contraseña centralizada para comodidad de los usuarios. Los usuarios sólo se validan una vez, y a partir de ahí tienen acceso a diferentes servicios.

Si un sitio web se debe desplegar en muchos servidores web a la vez para repartir la carga, y se necesita un sistema de control de acceso autenticado, resulta muy poco práctico configurar la autenticación de forma local en cada servidor. Para evitarlo, es posible poner en marcha un servidor LDAP, con un directorio de usuarios permitidos (con sus contraseñas), al que todos los servidores web se conectarán cuando un usuario intente acceder al sitio web.

En este apartado se explican unos conceptos básicos sobre LDAP y se mostrará cómo poner en marcha un servicio LDAP, y cómo integrar el servidor web Apache con ese servicio LDAP.

### 3.1.1. **Jerarquía y nomenclatura LDAP**

LDAP tiene una estructura jerárquica. Un árbol de directorio LDAP a veces refleja varios límites políticos, geográficos u organizacionales, dependiendo del modelo elegido. Los despliegues actuales de LDAP tienden a usar nombres de DNS para estructurar los niveles más altos de la jerarquía.

Conforme se desciende en el directorio pueden aparecer entradas que representan personas, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier cosa que representa una entrada dada en el árbol (o múltiples entradas).

LDAP consta principalmente de objetos y contenedores de objetos. Los contenedores de objetos son las llamadas Unidades Organizativas (UO, en inglés OU), que le dan la estructura al árbol LDAP. Los objetos pueden ser por ejemplo cuentas de usuario con todas sus propiedades.

La raíz del árbol LDAP es el llamado Base Distinguished Name (Base DN). A partir de él, puede haber objetos o Unidades Organizativas que contengan más objetos, formando un árbol.

Base DN está formado por los llamados Domain Components (dc). A continuación, un ejemplo de jerarquía LDAP:

```
dc=foobar, dc=com
    ou=customers
        ou=asia
        ou=europe
        ou=usa
    ou=employees
    ou=rooms
    ou=groups
    ou=assets-mgmt
    ou=nisgroups
    ou=recipes
```

https://www.oreilly.com

El base DN del ejemplo es "dc=foobar, dc=com". A partir de ahí están las diferentes OU, que a su vez pueden tener más OUs en su interior.

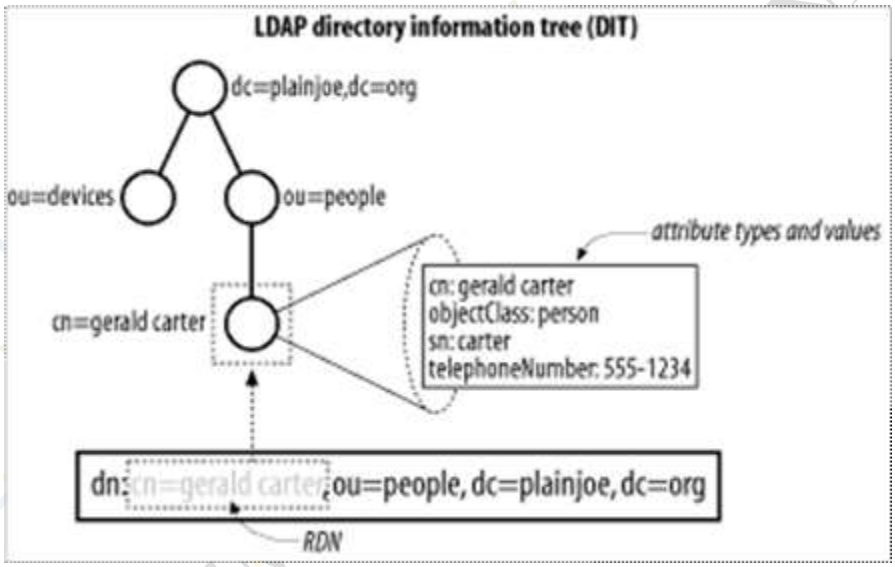
Todas las entradas (objetos) de un directorio LDAP tienen un Distinguished Name, que es único. El DN está compuesto de dos partes: el Relative Distinguished Name (RDN) y la ubicación dentro del directorio.

Un ejemplo de un distinguished name de un objeto que podría representar a una cuenta de usuario:

**cn=Fran Smith,ou=employees,dc=foobar,dc=com**

Toda la cadena es el DN del usuario, la parte inicial "cn=Fran Smith" es el DN relativo (RDN).

A continuación, un ejemplo gráfico de un directorio LDAP:




https://www.oreilly.com

Un objeto tiene unos atributos y pertenece a una clase de objetos. Cada clase de objetos está definida con unos atributos específicos. La definición de clases y atributos por clase se denomina el esquema LDAP.

A continuación, se muestra como queda definida una clase de objetos:

```
objectclass ( 2.5.6.6 NAME 'person' SUP top STRUCTURAL
        MUST ( sn $ cn )
        MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )
```

La clase "person" tiene como atributos obligatorios "sn" y "cn" y como atributos opcionales los mencionados dentro del paréntesis del "MAY".

Un objeto puede tener un listado extenso de atributos como el que se observa en el ejemplo siguiente:

```
dn: cn=Tom Syroid, ou=employee, dc=syroidmanor, dc=com
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: Tom Syroid
cn: Thomas Syroid
sn: Syroid
givenName: Tom
initials: TMS
title: Project Manager
uid: tsyroid
mail: tom@syroidmanor.com
telephoneNumber: 306 555 1212
mobile: 306 555 1999
roomNumber: 115
employeeNumber: 33
employeeType: full time
```

Se puede observar cómo el objeto tiene un dn, que debe ser único. El objeto puede pertenecer a varias clases (objectClass), y a continuación constan todos los atributos con sus valores.

La sintaxis mostrada está basada en el estándar LDIF para el intercambio de información entre directorios LDAP.

A continuación, se muestra otro ejemplo de objeto LDAP:

```
dn: uid=fsmith, ou=employees, dc=foobar, dc=com
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: foobarPerson
uid: fsmith
givenname: Fran
sn: Smith
cn: Fran Smith
cn: Frances Smith
telephonenumber: 510-555-1234
roomnumber: 122G
o: Foobar, Inc.
mailRoutingAddress: fsmith@foobar.com
mailhost: mail.foobar.com
userpassword: {crypt}3x1231v76T89N
uidnumber: 1234
gidnumber: 1200
homedirectory: /home/fsmith
loginshell: /usr/local/bin/bash
```

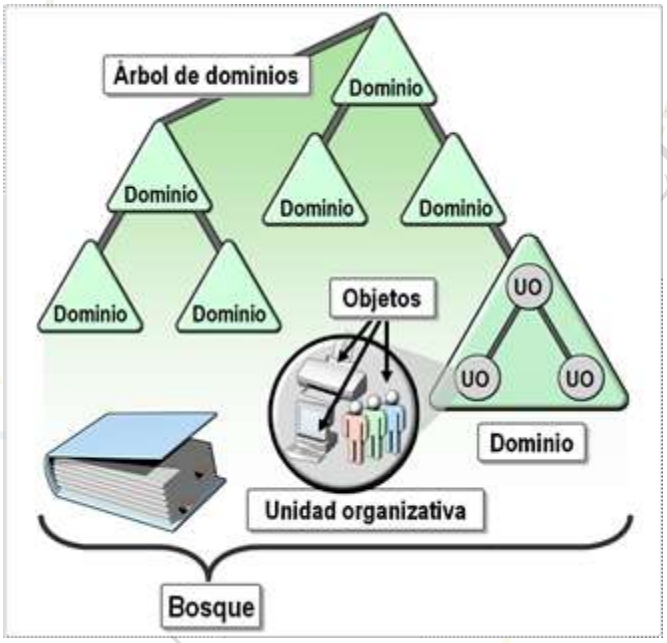
En este caso, se aprecian atributos que asocian a este objeto con cuentas de usuarios de sistemas UNIX (userpassword, uidnumber, gidnumber, homedirectory, etc).

## 3.2. Implementación de Active Directory en Windows Server 2016

AD, Active Directory es la implementación de un directorio LDAP por parte de Microsoft. Active Directory está disponible desde la versión Windows 2000 Server hasta la actualidad, donde sigue vigente como el centro de gestión de los sistemas operativos Windows.

Active Directory es una base de datos centralizada desde la que se puede administrar toda una organización de sistemas operativos Windows de forma eficiente y flexible.

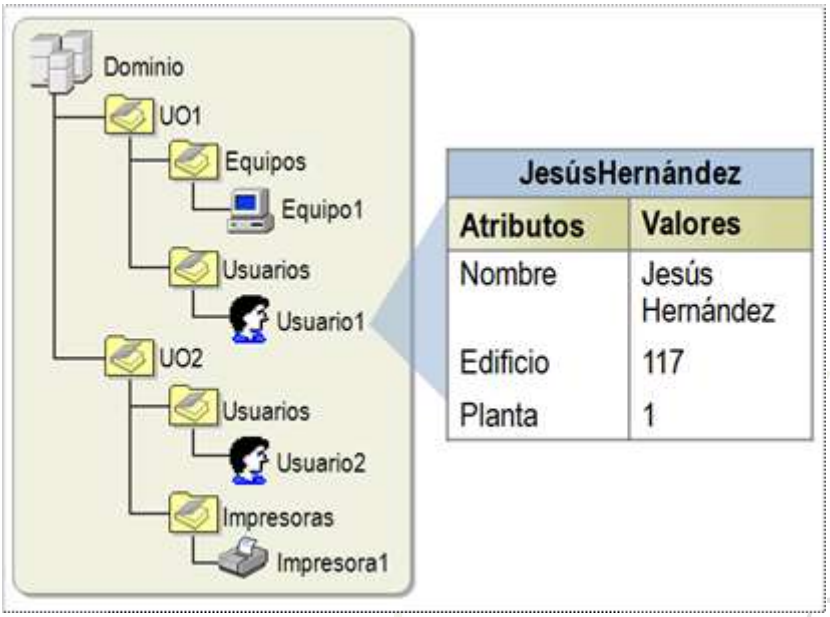
Active Directory organiza objetos mediante una estructura jerárquica de diferentes niveles. El nivel de agrupación básico es el denominado "dominio", para el que existe un administrador que gestiona todos sus recursos. Por encima del dominio existen estructuras como los llamados "árboles" y "bosques". Por debajo están las unidades organizativas que contienen los objetos, que son finalmente cuentas de usuario, grupos de usuarios y cuentas de máquina, entre otros.




http://microsoft.com

Aunque la función principal de Active Directory es la autenticación centralizada, este servicio es mucho más potente y permite gestionar de forma completa una red corporativa de extensión internacional. Funcionalidades como el despliegue de software, gestión de certificados, control del entorno de trabajo del usuario, etc. se llevan a cabo a través del servicio de Active Directory.

Active Directory es una implementación de LDAP, y por lo tanto, en esencia es un repositorio de información estructurado sobre personas y recursos de una organización:




http://microsoft.com

Cada cuenta de usuario o de máquina es un objeto ubicado en el árbol LDAP del dominio, formado por "ramas" llamadas Unidades Organizativas (UO). Cada objeto, que pertenece a una clase, tiene unos atributos, que tienen unos valores.

Cuando se instala Active Directory en un servidor, se convierte éste en un controlador de dominio. Los equipos de la red se añaden al dominio para quedar bajo su gestión.

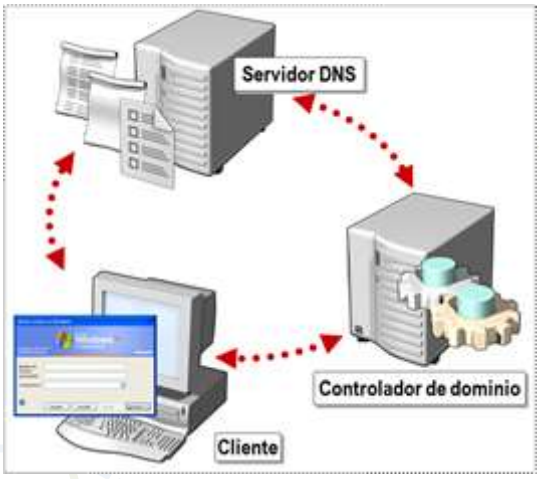
Si una máquina pertenece al dominio, un usuario se puede validar con credenciales de dominio al arrancar la máquina. La información se pasa a un controlador de dominio para que se verifique. Si está todo bien, se le entrega al usuario y máquina, un token, que después presenta para autentificarse en cualquier acceso futuro a cualquier máquina o recurso del dominio.

Todo este proceso es transparente para el usuario.

http://microsoft.com

De esta forma, el usuario sólo se valida una vez (single sign on).

Active Directory reposa en el servicio DNS para establecer su sistema de nomenclatura del directorio, y como sistema de resolución de nombres en la red. Un servicio DNS modificable es un requisito para instalar Active Directory.

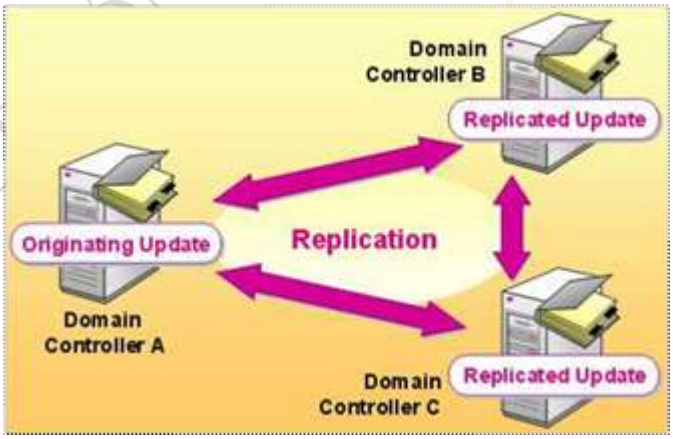



http://microsoft.com

DNS es el servicio que utilizan las máquinas cliente para encontrar los controladores de dominio. Cuando en una máquina se valida un usuario de dominio, la máquina pregunta al servidor DNS quién es el controlador de dominio. El servidor DNS, le dará al cliente la IP del controlador de dominio. DNS es por lo tanto, un servicio esencial para el correcto funcionamiento de Active Directory.

Para la existencia de un dominio, se necesita como mínimo un Controlador de Dominio. Puede haber más de un controlador de dominio del mismo dominio. De hecho, es recomendable, ya que proporciona alta disponibilidad para el dominio.

Entre los diferentes controladores de dominio del mismo dominio se produce de forma automática una replicación multi-master, donde cualquier modificación que suceda en cualquiera de las réplicas será enviada a las demás.




http://microsoft.com

### 3.2.1. **Instalación y puesta en marcha**

Para instalar Active Directory es necesario disponer de un servicio DNS modificable. El proceso de instalación modificará el servidor DNS que se le indique, y si no encuentra ninguno, propondrá instalar uno en la misma máquina.

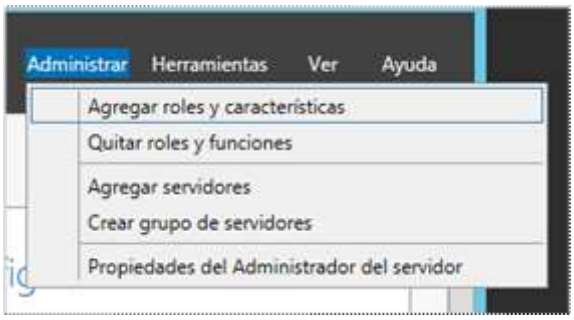
Antes de empezar con la instalación se debe configurar un IP fija en el servidor y se debe hacer al servidor cliente DNS de sí mismo.

Cuando empiece la instalación, el proceso buscará un servicio DNS en el propio servidor, y al no encontrarlo (suponiendo que no está), propondrá la instalación y configuración del servicio DNS además del de Active Directory. En definitiva, se instalarán los dos servicios en el mismo proceso, y quedarán los dos servicios ejecutándose en el mismo servidor.

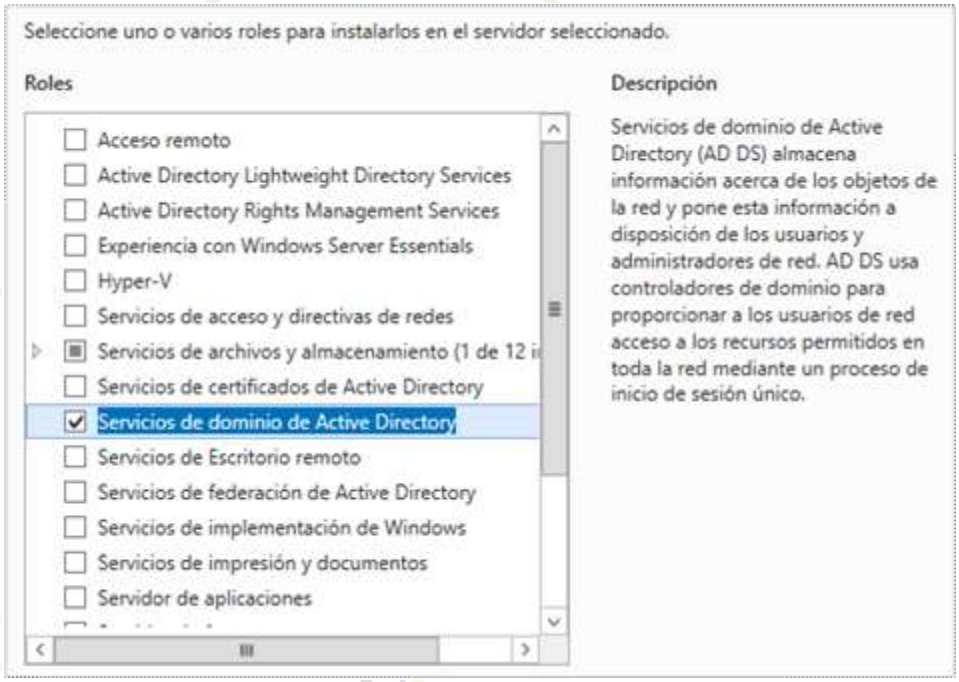
Aunque el servidor DNS puede estar en otro servidor diferente, es muy común la configuración en que los dos servicios conviven en la misma máquina.

A continuación, se muestra una configuración de red de ejemplo del servidor justo antes de empezar la instalación de Active Directory.

Para llevar a cabo la instalación se debe empezar agregando el rol correspondiente desde el administrador del servidor:



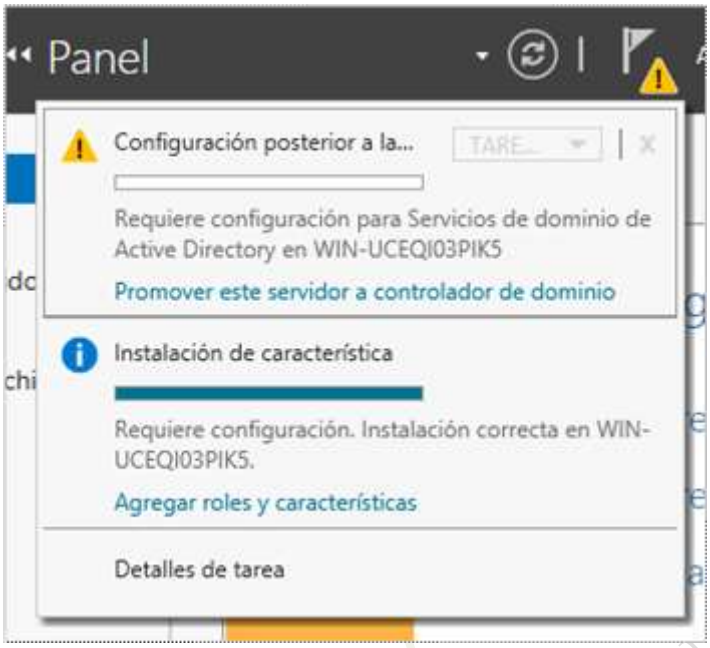

Se debe seleccionar el rol "Servicios de dominio de Active Directory"




Al seleccionar el servicio, el sistema propone también añadir las características relacionadas

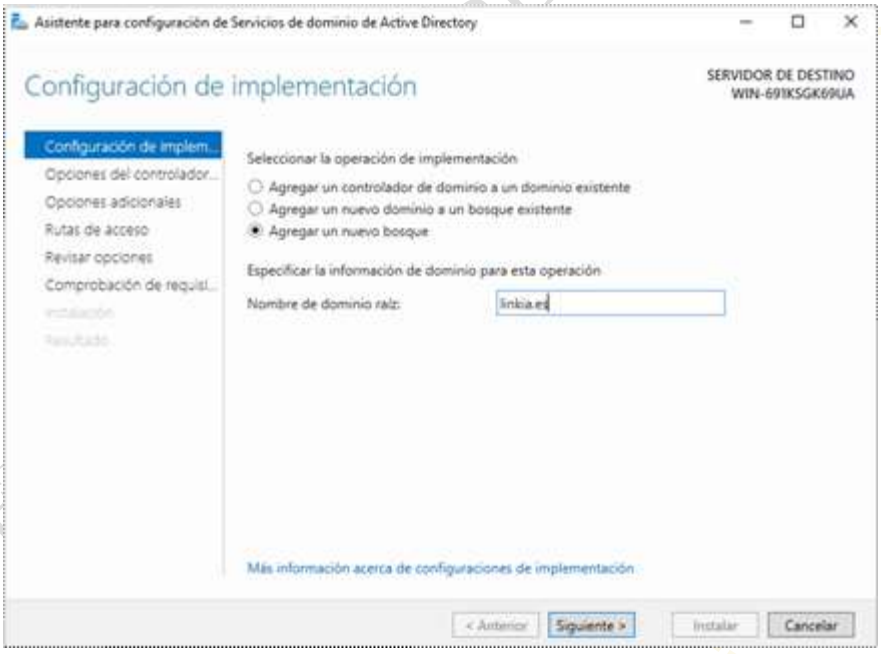
Se debe aceptar agregar las características propuestas.

Una vez acabado este primer proceso de instalación, el administrador del servidor avisa que aún quedan los pasos de configuración inicial del servicio:




Al seleccionar la opción "Promover este servidor a controlador de dominio" se inicia la configuración inicial.

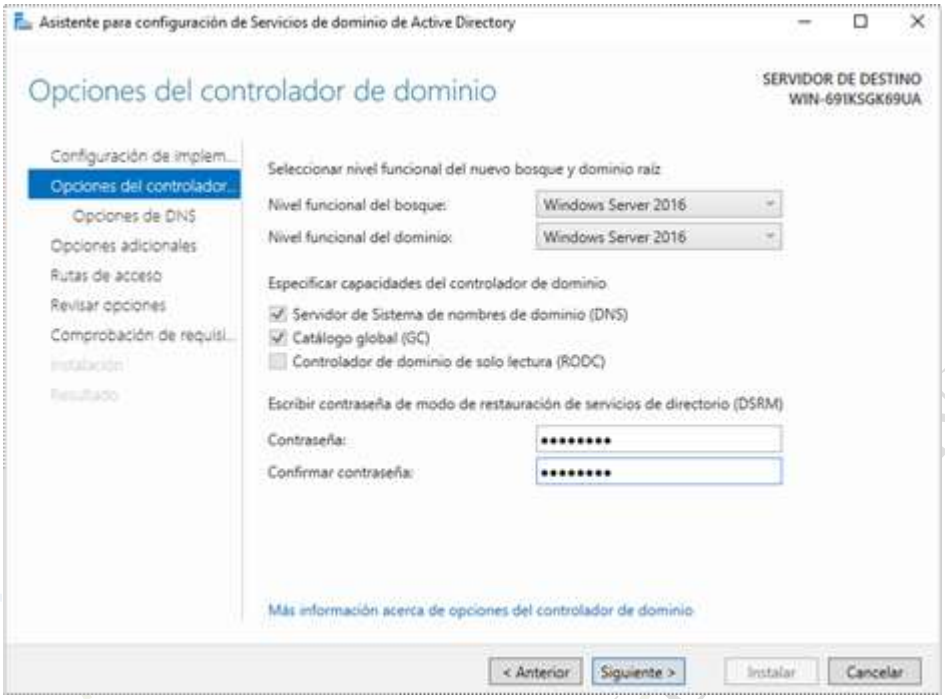
En el primer paso se selecciona la opción para crear un nuevo dominio desde cero:




Se creará un nuevo bosque con un nuevo dominio. El nombre deberá ser compatible con la nomenclatura DNS.

VE... ALUMNO LINKIAFP

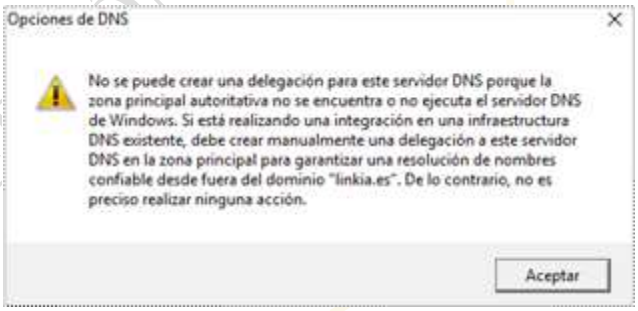
A continuación se decide el nivel funcional del bosque, que dependerá de las versiones de sistema operativo utilizadas en los controladores de dominio.




También se puede marcar la opción para que se instale el servicio DNS junto con Active Directory, y finalmente se establece la contraseña de restauración del servicio.

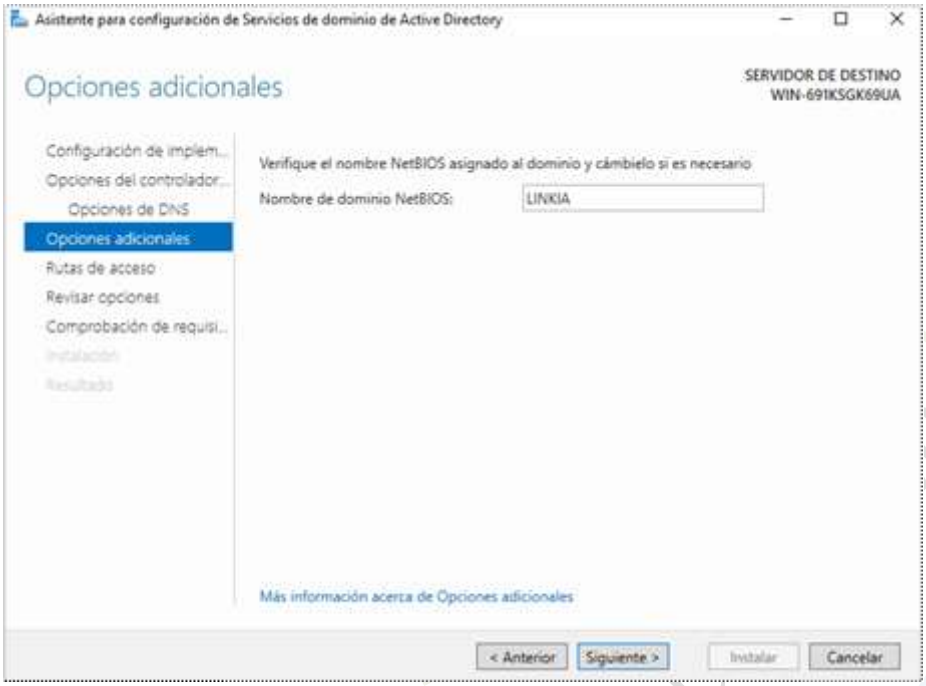
Esta contraseña NO es la contraseña del futuro administrador del dominio. La contraseña del administrador del dominio será la misma que la del actual administrador local, el cual desaparecerá. La contraseña de restauración sólo se utilizará cuando Active Directory tenga problemas para arrancar y se precise de una autenticación básica para poder restaurar el servicio.

En el paso siguiente surge una advertencia avisando que no existe una zona DNS para modificarla y utilizarla con Active DIrectory.

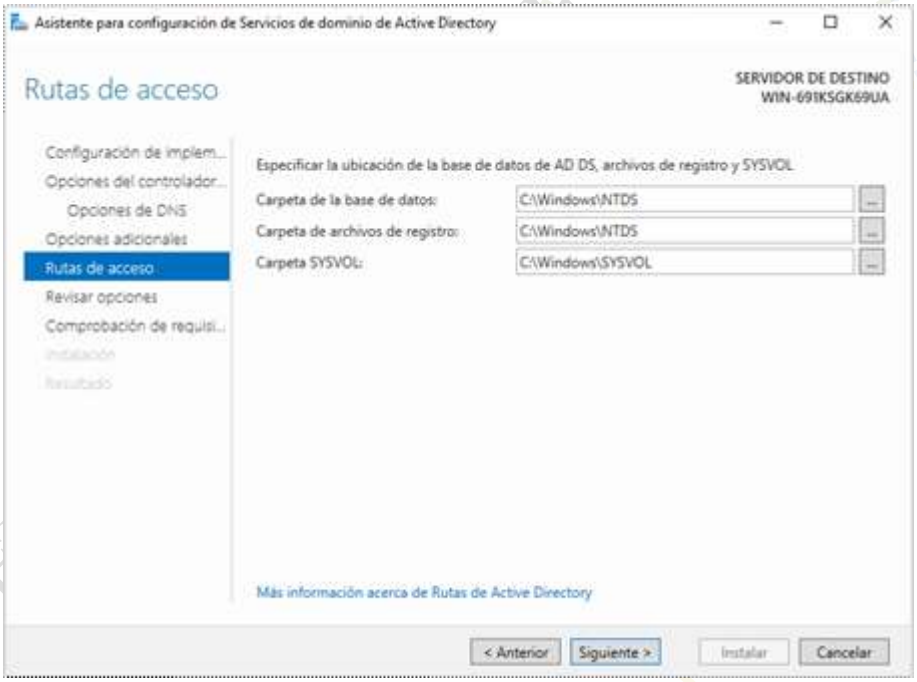



En este caso no supone un problema, ya que el proceso también creará la zona DNS.

El proceso propone un nombre NETBIOS para el dominio por compatibilidad con sistemas anteriores:

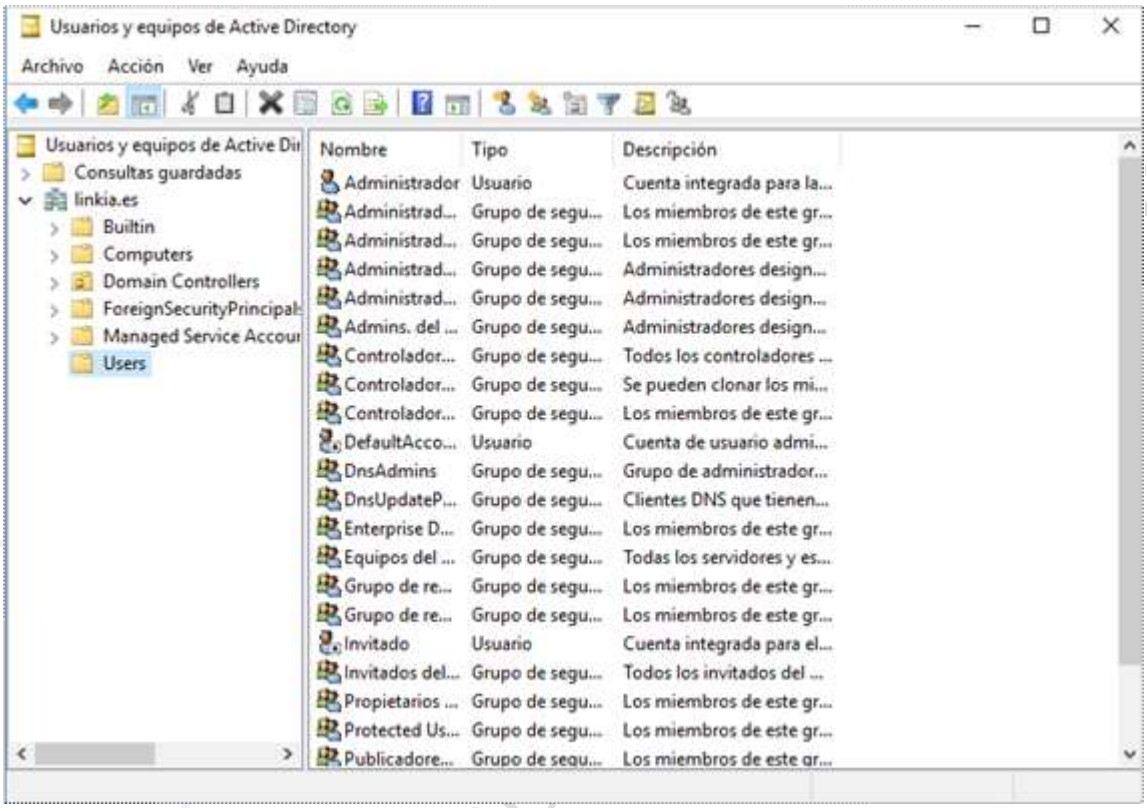



El proceso propone una ubicación en el disco para los ficheros de Active Directory:



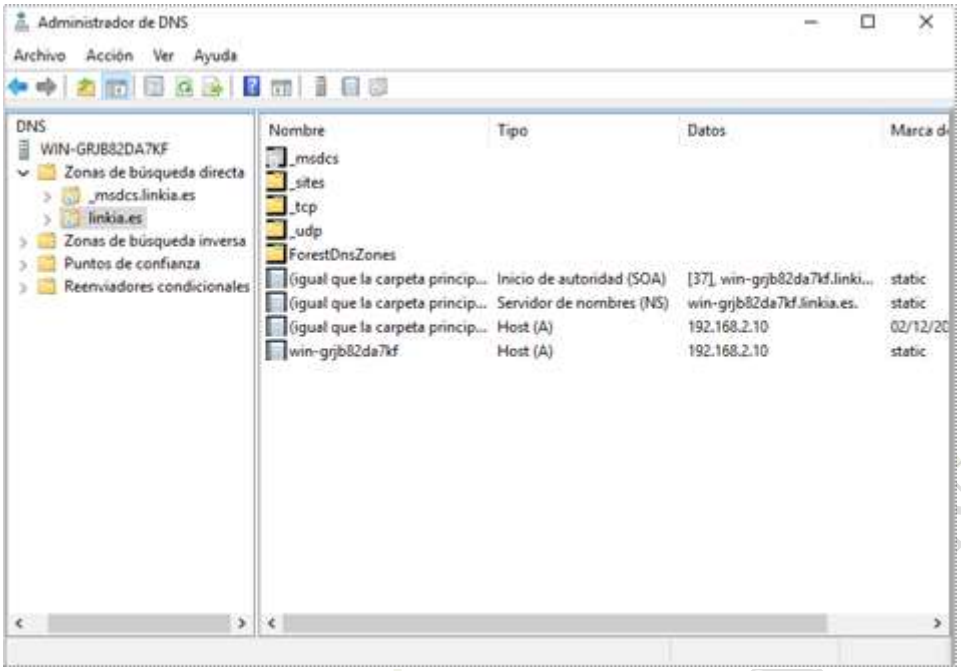

El proceso hará unas comprobaciones finales y reiniciará el servidor. El servicio estará en marcha una vez reiniciado el servidor.

Para comprobarlo se puede abrir la herramienta "Usuarios y equipos de Active Directory" desde el administrador del servidor:




Se pueden observar diversas unidades organizativas con usuarios y grupos dentro. El directorio se ha creado desde cero pero contiene algunos objetos predeterminados. Como administrador es posible añadir nuevos objetos.

También se ha añadido el servicio de DNS instalado anteriormente con el nombre del dominio. Para verlo se abre la consola DNS desde el administrador del servidor:




Se puede observar que existe la zona con los registros dentro.

### 3.2.2. Creación de usuarios y grupos

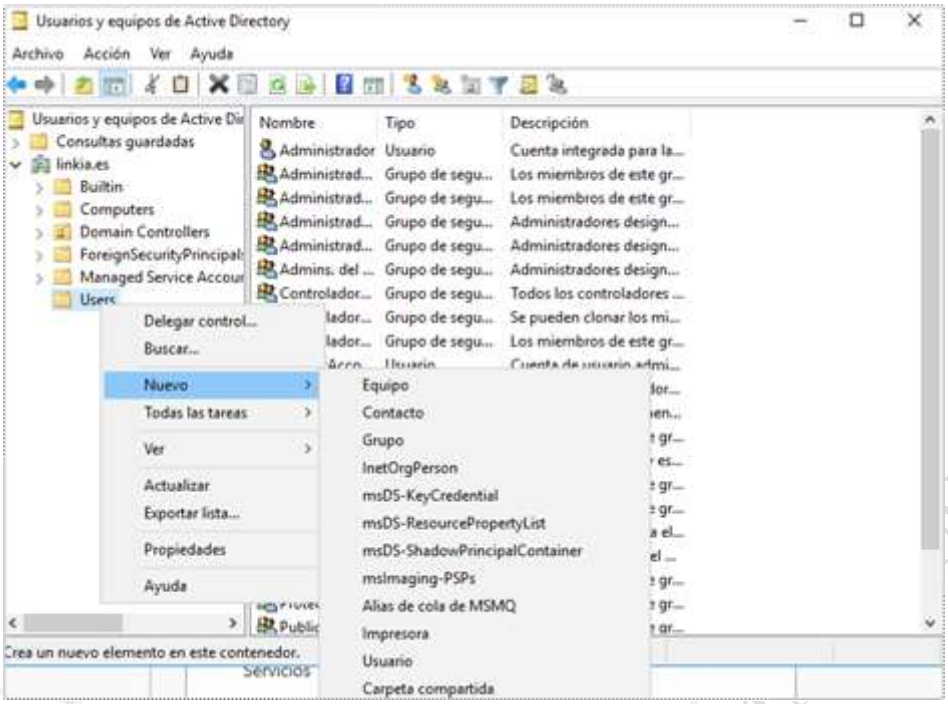
Una vez instalado el servicio se pueden crear usuarios y grupos dentro de las unidades organizativas existentes, o dentro de nuevas UOs.

Para crear un usuario se debe hacer click con el botón derecho en la UO que se desee que vaya a parar el usuario.

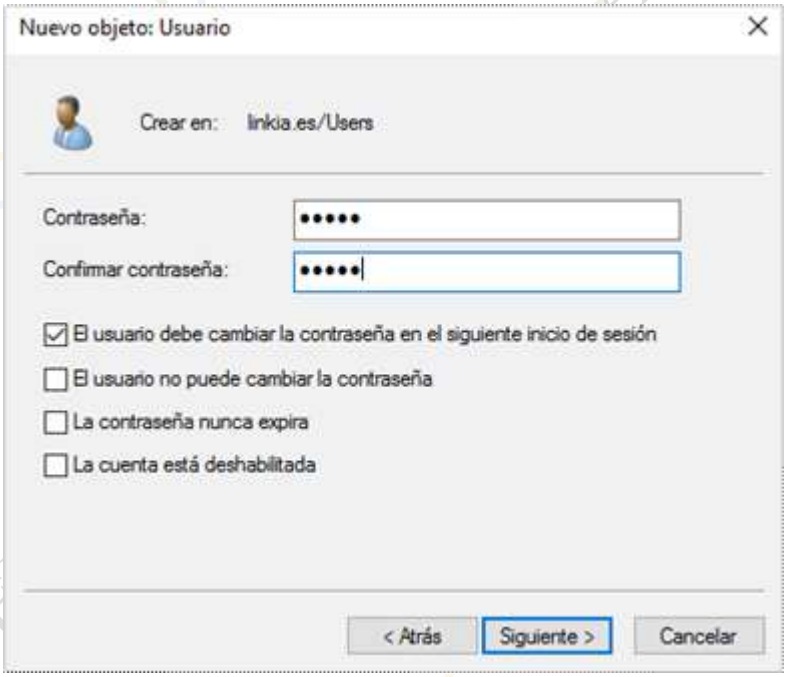
En el ejemplo de la imagen se creará el usuario dentro de la UO "Users".

Se deben introducir nombres descriptivos y un nombre de inicio de sesión que debe ser único en el dominio.

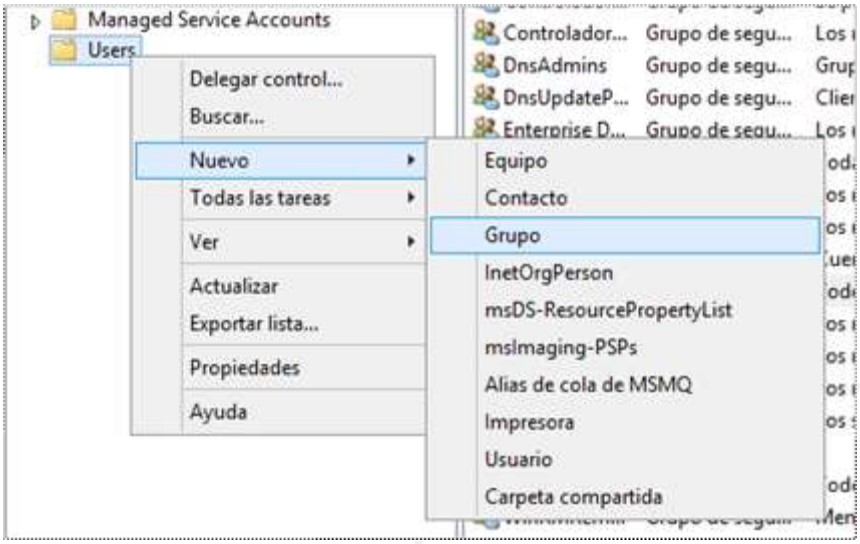
VERSIÓN IMPRIMIBLE ALUMNO LINKIAFP



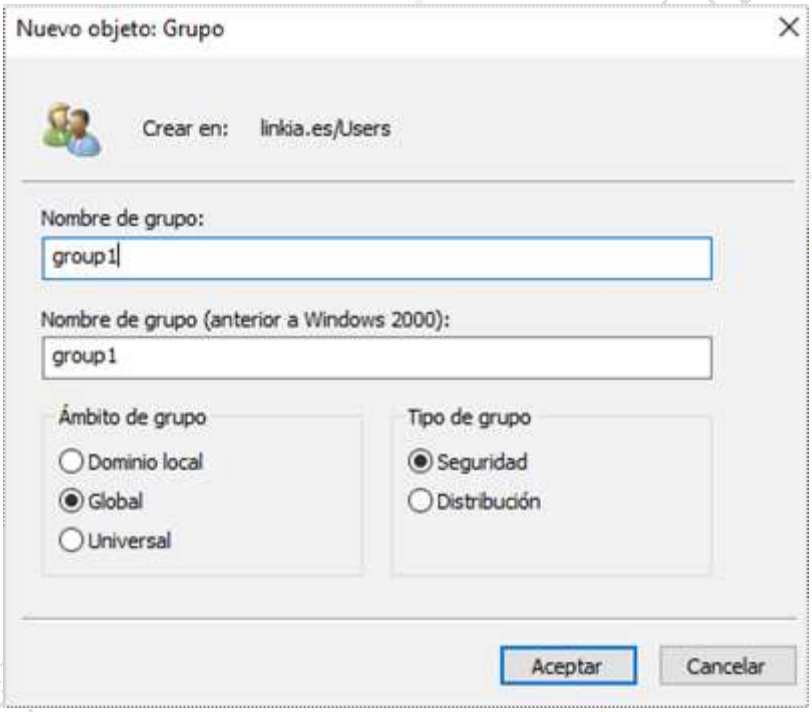

Y por supuesto, se debe asociar una contraseña al usuario, que por defecto debe cumplir unos requisitos de complejidad.



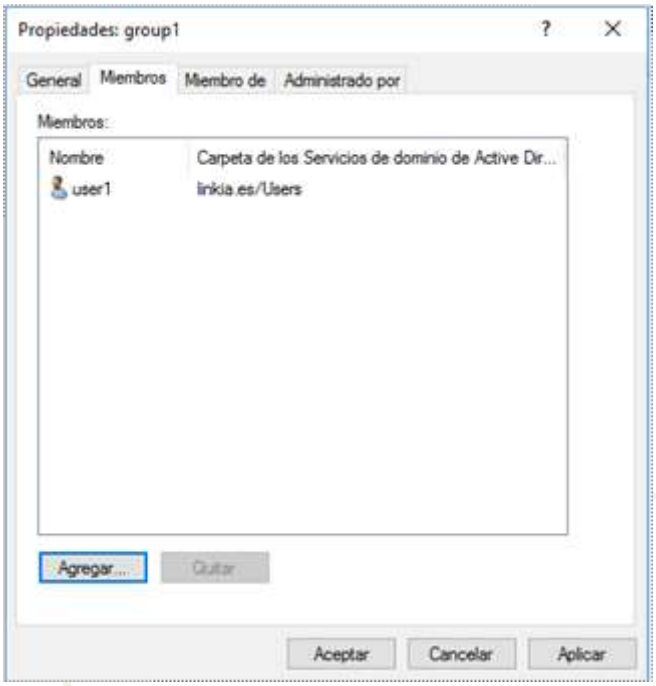

De la misma manera se pueden crear también grupos de usuarios, que no son más que conjuntos de usuarios agrupados dentro de un objeto al que luego se le pueden atribuir permisos especiales. El uso de grupos en Active Directory facilita la administración de permisos, ya que evita tener que establecerlos usuario por usuario.




El grupo tiene un nombre y un ámbito y tipo, que afecta a qué tipo de usuarios pueden pertenecer a él.




Una vez creado el grupo, se pueden editar sus propiedades para agregar miembros al grupo.




También desde las propiedades de cada usuario es posible agregarlo a grupos.

### 3.2.3. **Instalar un controlador de dominio adicional**

Para dar alta disponibilidad al servicio de Active Directory se puede instalar un controlador de dominio adicional en el mismo dominio. De esa forma, se realizará una réplica de la base de datos de Active Directory en otra máquina a través de la red.

El nuevo controlador de dominio podrá atender a peticiones de clientes y además podrá también realizar cambios en la base de datos. Se trata de una replicación multi-master, donde se pueden realizar cambios desde cualquiera de las réplicas. Una vez realizado el cambio se enviará la actualización a todos los controladores de dominio del dominio.

Como en la primera instalación, también ahora se instalará junto con Active Directory el servicio DNS, lo cual también dará alta disponibilidad a este servicio. Además, cuando el controlador de dominio y el servicio DNS se encuentran en la misma máquina, Windows configura las zonas DNS del dominio como "Integradas en Active Directory". De esta forma, las zonas DNS ya no se almacenan en ficheros de texto, sino que pasan a formar parte de la base de datos de Active Directory, con lo que se benefician de la estructura de replicación multi-master, pudiéndose realizar cambios en cualquier servidor DNS con este tipo de zonas.

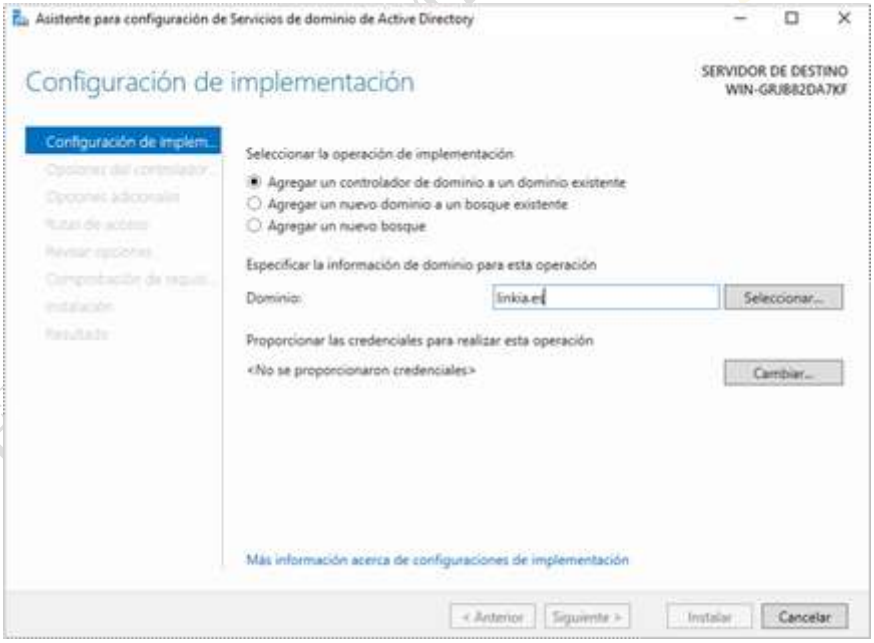
Antes de empezar con la instalación, se debe configurar el nuevo servidor con una IP estática, y como cliente DNS del primer servidor DNS ya instalado.

A continuación se muestra un ejemplo de configuración válido y coherente con el controlador de dominio instalado anteriormente en este apartado de Active Directory:

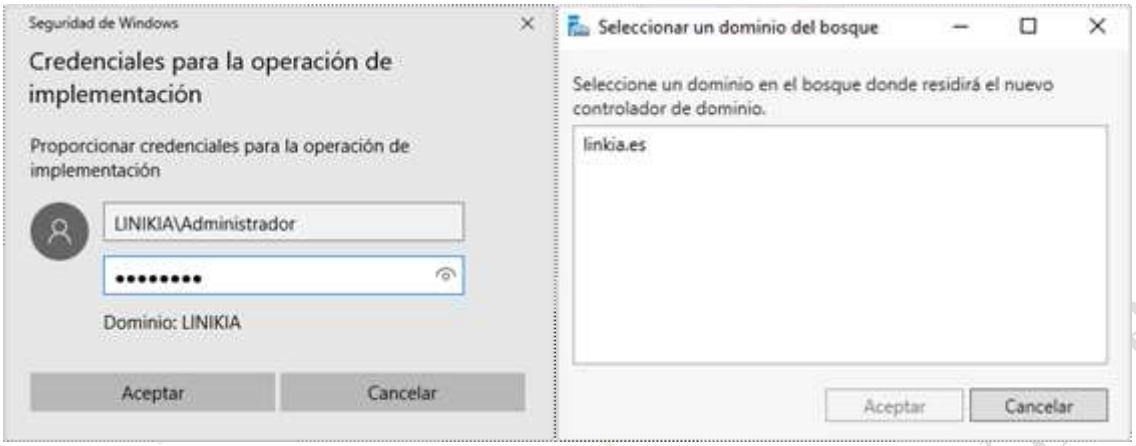
VERSIÓN NO VENDIBLE ALUMNO LINKIAFP

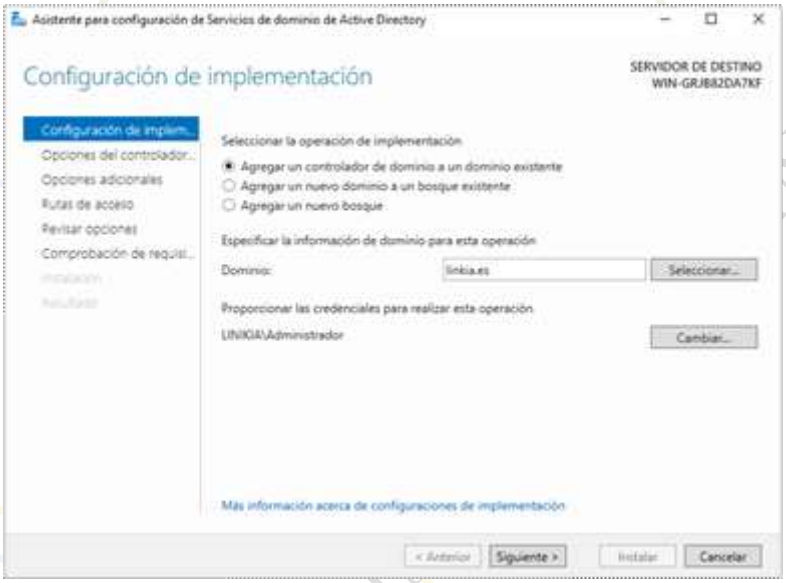
Se observa como el servidor DNS preferido debe ser el servidor DNS ya existente en el dominio, y anteriormente instalado (192.168.2.10 en el ejemplo)

Para instalar este controlador de dominio adicional se procede igual que el primero agregando el rol correspondiente. Sin embargo, en este caso no se creará un nuevo bosque, sino que se agregará un controlador de dominio al dominio existente:

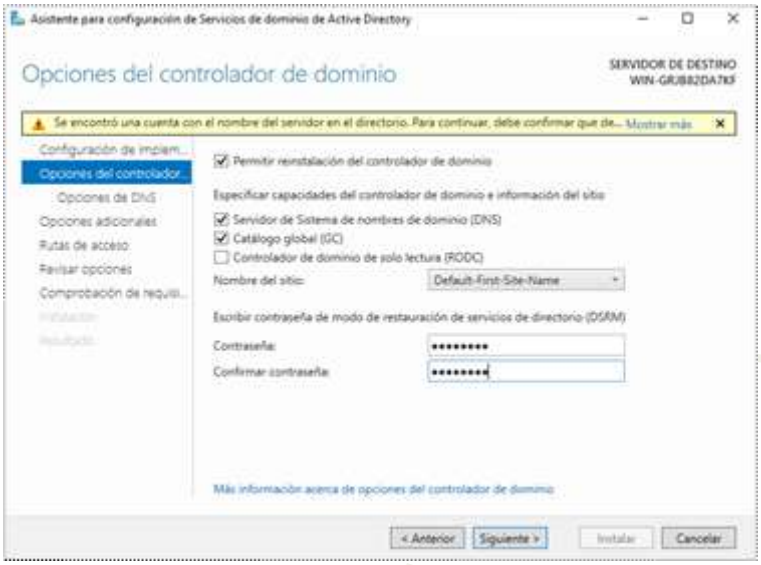


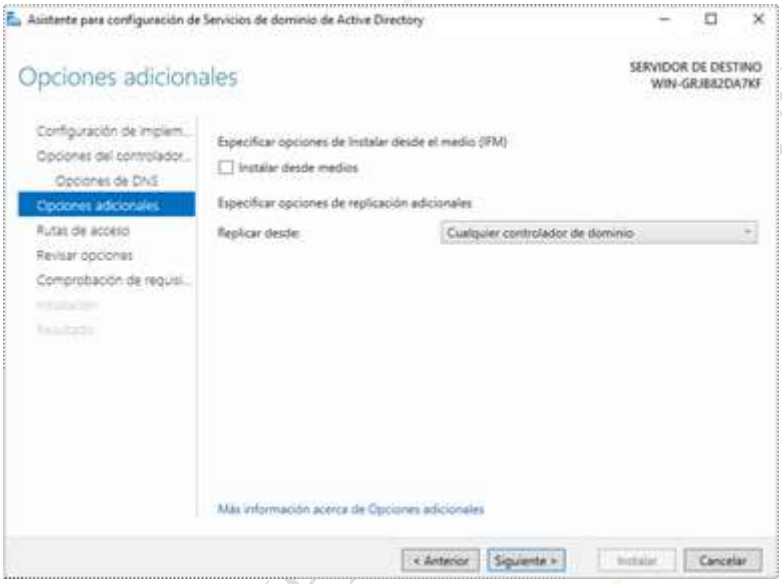

Se debe especificar el nombre del dominio existente, y credenciales válidas en el dominio existente para realizar la operación.




El resto del proceso es muy similar al del primer controlador de dominio. En un punto de la instalación se solicita que se selecciona el controlador de dominio (en caso de que hubiera varios) desde el que se desea traer la copia de la base de datos. Se puede seleccionar "desde cualquier controlador de dominio".



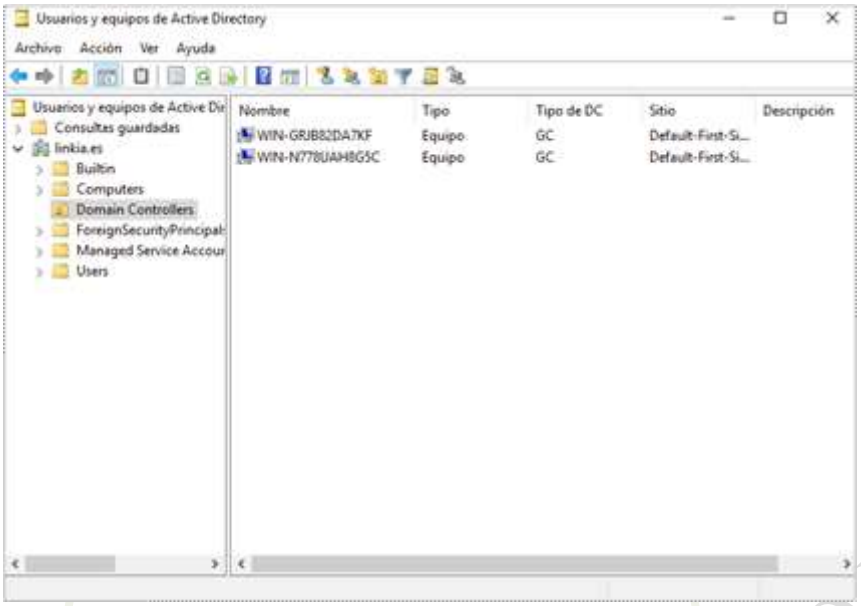




También en esta ocasión dará la opción de instalar el servicio DNS en este nuevo controlador.

Una vez finalizada la instalación, se puede comprobar que aparece la herramienta de "Usuarios y equipos de Active Directory" en el nuevo servidor, desde la cual se puede observar la nueva copia generada de la base de datos. En ella deben estar todos los usuarios que ya se habían creado desde el otro controlador.

Por ejemplo, el usuario "user1" fue creado previamente en el primer controlador y ahora está presente también en éste, ya que es una réplica de toda la base de datos.

En la Unidad Organizativa "Domain Controllers" se crea una cuenta de máquina para cada controlador, con lo que se deberían encontrar ya las dos cuentas de los dos controladores instalados en el dominio.




También debe haberse instalado el servicio DNS. En la consola DNS se debe observar ya replicada la zona del dominio existente. Dentro de ella se pueden observar los registros (de tipo SRV) que identifican a los dos controladores de dominio como dos servidores LDAP.

Por último, será necesario reconfigurar la configuración de red de los dos controladores de dominio. Los controladores tendrán que ser clientes DNS del controlador compañero en primer lugar, y de sí mismo en segundo lugar.

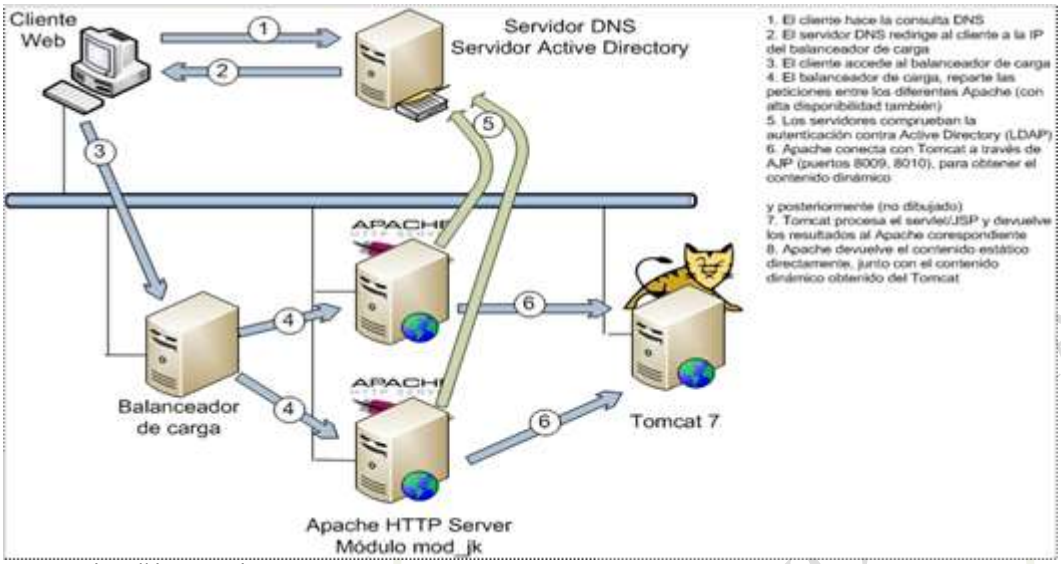
### 3.2.4. **Integración de Apache con Active Directory**

Es muy habitual que un sitio web no lo pueda servir un solo servidor web y se necesiten varios servidores para repartirse la carga y dar alta disponibilidad al servicio. Si además es necesario autenticar a los usuarios que acceden, entonces es muy engorroso manejar usuarios locales en cada uno de los servidores web, ya que las tareas de mantenimiento de los usuarios se tendrían que repetir en cada servidor.

Para evitarlo, se puede hacer uso de un servicio LDAP externo al servidor web (por ejemplo Active Directory), al que todos los servidores web accedan para comprobar las credenciales introducidas por el usuario en el sitio web. De esa forma el servicio queda centralizado y permite el escalado del sitio web con más servidores de forma sencilla.

A continuación, se presenta un escenario de ejemplo:

Los dos servidores  Apache se configuran para integrarlos con el servidor de Active Directory para la autenticación.



http://docs.oracle.com

Para que Apache pueda entenderse con un directorio LDAP se debe habilitar el módulo de autenticación LDAP.

Para habilitar un módulo en apache se utiliza el comando "a2enmod" seguido del nombre del módulo, que este caso es "authnz_ldap".

```
linkia@linkia:/etc/apache2$ sudo a2enmod authnz_ldap
Considering dependency ldap for authnz_ldap:
Enabling module ldap.
Enabling module authnz_ldap.
To activate the new configuration, you need to run:
  systemctl restart apache2
linkia@linkia:/etc/apache2$
```

Después de habilitarlo es necesario reiniciar el servicio de apache.

Una vez habilitado el módulo ya se puede hacer uso de las directivas específicas para configuración de LDAP en Apache. A continuación, se muestra un ejemplo de configuración ya completa:

# Parámetros básicos de configuración para la autenticación contra LDAP

***AuthBasicProvider ldap***

***AuthType Basic***

# Título de la ventana de autenticación que le surgirá al usuario

***AuthName "Acceso restringido"***

# Fase I: AUTENTICACIÓN contra LDAP

***AuthLDAPBindDN "CN=consultas,CN=Users,DC=ejemplo,DC=com"***

***AuthLDAPBindPassword P@ssw0rd***

***AuthLDAPURL***

***"ldap://192.168.227.3/CN=Users,DC=ejemplo,DC=com?sAMAccountName?sub?(objectClass=*)"***

# Fase II: AUTORIZACIÓN contra LDAP

***AuthLDAPGroupAttributeIsDN on***

**# Autorización a los miembros del grupo "AccesoWeb"**

**require ldap-group CN=AccesoWeb,CN=Users,DC=ejemplo,DC=com**

Para que esta configuración de ejemplo funcione se deben haber realizado las siguientes configuraciones:

- disponer de un directorio LDAP con un base DN "dc=ejemplo, dc=com" (ejemplo.com en formato DNS de Active Directory)
- disponer de un usuario de nombre "consultas" en la Unidad Organizativa "Users" del dominio, y con el password que se indica en la configuración (en el ejemplo P@ssw0rd). Este usuario sólo sirve para vincular Apache con Active Directory, es el utilizado para que Apache pueda acceder al directorio a comprobar las credenciales de los usuarios que quieran acceder a la web.
- un controlador de dominio con la IP 192.168.227.3
- un grupo de nombre "AccesoWeb" en la unidad organizativa "Users". Los usuarios miembros de ese grupo serán los que tengan acceso al sitio web

Se pueden adaptar estos valores de ejemplo a los de cada configuración y aplicarlos en el fichero de configuración de apache. Todas las directivas de la configuración se deben incluir en una etiqueta <Directory>

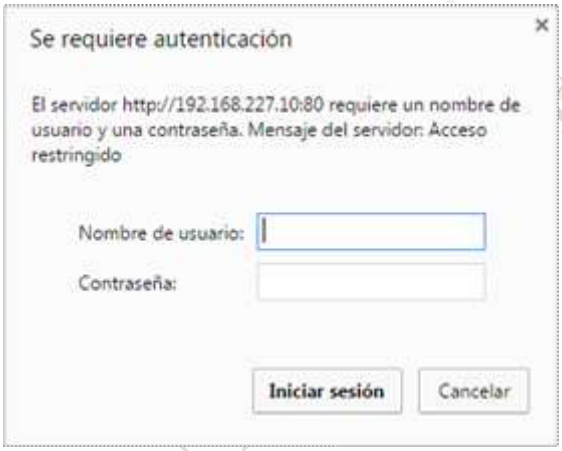
Aquí se muestra el fichero con los valores de ejemplo utilizados:

VERSIÓN SIMPLE ALUMNO LANKIAFP

```
<VirtualHost *:80>

        DocumentRoot /var/www/html

        <Directory /var/www/html>
        # Parámetros básicos de configuración para la autenticación contra LDAP
                AuthBasicProvider ldap
                AuthType Basic
        # Título de la ventana de autenticación que le surgirá al usuario
                AuthName "Acceso restringido"
        # Fase I: AUTENTICACIÓN contra LDAP
                AuthLDAPBindDN "CN=consultas,CN=Users,DC=ejemplo,DC=com"
                AuthLDAPBindPassword P@ssw0rd
                AuthLDAPURL "ldap://192.168.227.3/CN=Users,DC=ejemplo,DC=com?sAMAccountName?sub?(objectClass=*)"
        # Fase II: AUTORIZACIÓN contra LDAP
                AuthLDAPGroupAttributeIsDN on
        # Autorización a los miembros del grupo "AccesoWeb"
                require ldap-group CN=AccesoWeb,CN=Users,DC=ejemplo,DC=com
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
```

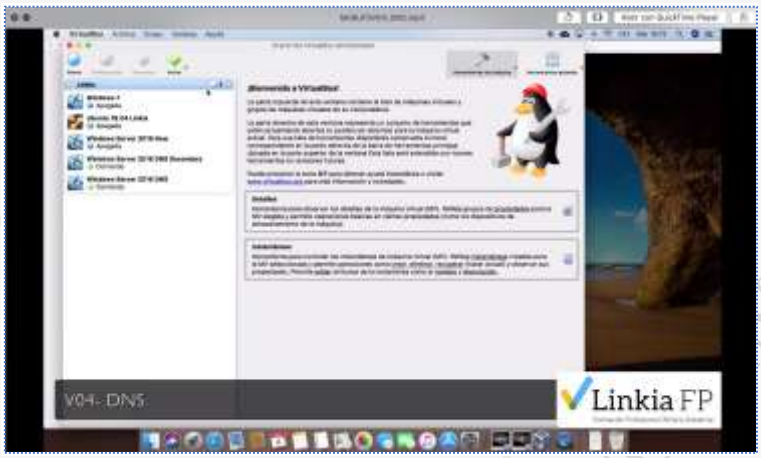
También se han configurado las directivas de log para revisar posibles errores en la conexión entre Apache y Active directory.

Si todo es correcto, al acceder al sitio web, al usuario se le exigirá autenticarse.




Si se introduce un usuario válido (en el ejemplo, que pertenezca al grupo AccesoWeb) entonces el acceso debe ser permitido.

## Recursos/Enlaces




→ Video instalación DNS

→ Ubuntu server **[Enlace]**

→ Windows 2016 Server **[Enlace]**

## Conceptos clave

- Nombre de dominio: Los nombres de dominio son la forma que usamos para organizar, navegar y entender la web. Sin nombres de dominio, las URL serían una serie de números, o direcciones IP, casi imposibles de recordar.
- ISP: Sus siglas son Internet Service Provider El proveedor de servicios de Internet, es la empresa que brinda conexión a Internet a sus clientes.
- Árbol de dominios. Un árbol de dominios (tree) es una colección de uno o más dominios que comparten un espacio de nombre contiguo. En un bosque de Active Directory pueden existir múltiples árboles de dominio.

VERSIÓN IMPRIMIBLE ALUMNO LINKIAFP

## Test de autoevaluación

¿Qué registro de recursos hace referencia a un intercambiador de correo?

a. A
b. CNAME
c. MX
d. Text

¿En qué ruta se encuentra el fichero named.conf.default-zones?

e. /etc/bind9
f. /etc/bind
g. c/etc/bind
h. /bind

VERSIÓN IMPRIMIBLE AL

# Ponlo en práctica

## Actividad 1

1. Instalación de Servidor DNS:
   a. Crea una máquina virtual con Windows 2016 Server
   b. Instala el servicio de DNS y configura 2 registros de recurso de tipo A, y un CNAME que apunte a uno de los anteriores.

SOLUCIÓN

## Actividad 2

2. Completa el siguiente código para crear una zona con el nombre de dominio prueba.com, y que la IP del servidor sea 200.200.200.2.

```
$TTL    604800
@       IN      SOA     [1.                ] [2.                ] (
                                2          ; Serial
                           604800          ; Refresh
                            86400          ; Retry
                          2419200          ; Expire
                           604800 )        ; Negative Cache TTL
;
@               IN      [3.]    [4.                ]
[5.            ]IN      A       [6.                ]
```

SOLUCIÓN

VERSIÓN ... MNO LINKIA FP

VERSIÓN IMPRIMIBLE ALUMNO LINKIAFP

VERSIÓN IMPRIMIBLE ALUMNO LINKIAFP

Linkia FP

Formación Profesional Oficial a Distancia

VERSIÓN IMPRIMIBLE ALUMNO LINKIAFP