



Linkia FP

Formación Profesional Oficial a Distancia

Actividad

Desarrollo de aplicaciones web

M08 – Despliegue de aplicaciones web

Instalación y configuración servidores DNS y LDAP

Carlos Manuel González Negral

Actividad

Instalación y configuración servidores DNS y LDAP

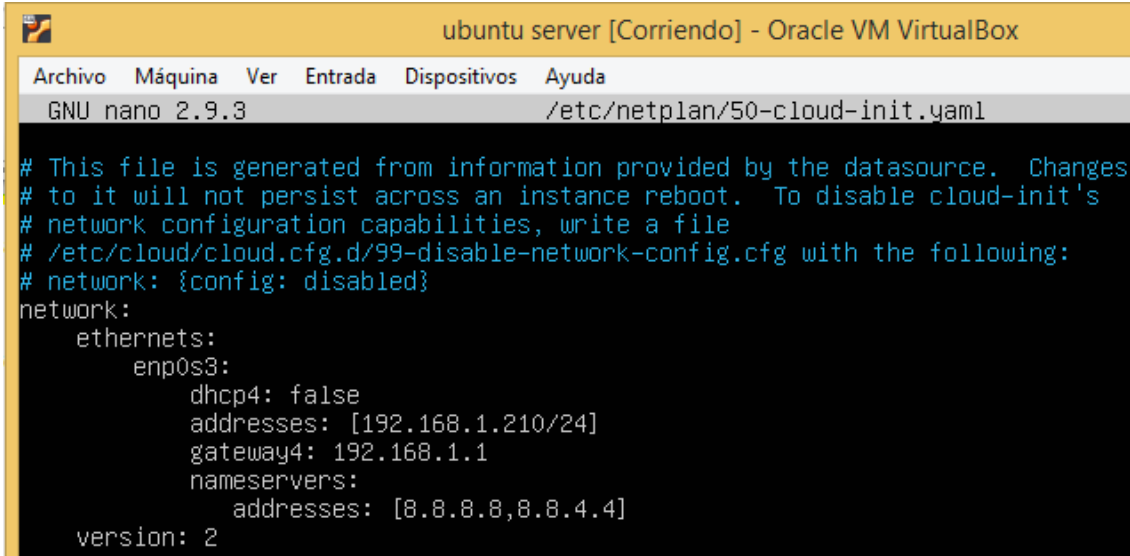
Contenido

0. Equipos utilizados en esta práctica:	3
Actividad 1. Instalación y configuración servidores DNS	5
1. Instala y configura un servidor web, basado en Apache, sobre una máquina Virtual Linux sin interfaz gráfica (por ej. Ubuntu Server 18.04).	5
2. Instala y configura un servidor DNS sobre la misma máquina Virtual Linux sin interfaz gráfica del ejercicio anterior.	7
3. Crea 2 registros en el servidor DNS UBUNTU Windows para un dominio llamado www.hulktunombre.com, que apuntará a la IP de la VM del apartado 1, y otro dns.hulktunombre.com, que apuntará a la misma IP de la VM.	13
4. Configura Round Robin en el servidor DNS para el registro de recurso de la página web, www.hulktunombre.com.	17
Instalación y configuración de LDAP	19
1. Instala y configura un servidor controlador de dominio con Active Directory y DNS sobre una máquina virtual Windows Server 2016.	19
2. Configura el servidor web para que autentique al usuario mediante Active Directory. .	21
Webgrafía.....	24

0. Equipos utilizados en esta práctica:

- Máquina virtual con un servidor Linux Ubuntu 18.04.

Utilizaré la máquina usada en la UF 1 que ya tiene instalado apache y tiene ip fija:

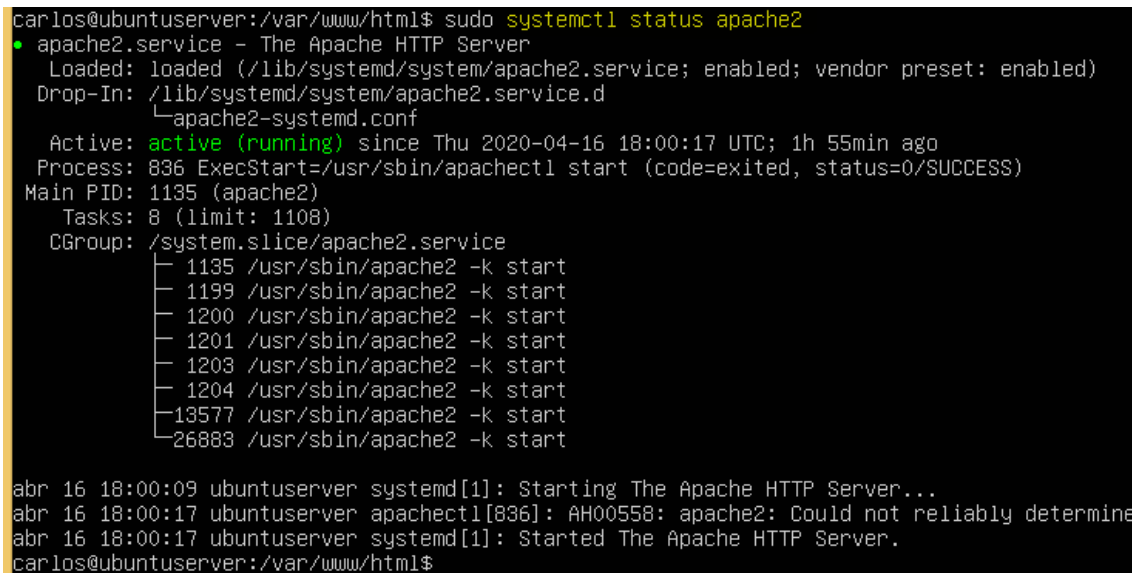


```

ubuntu server [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 2.9.3  /etc/netplan/50-cloud-init.yaml

# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  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:
      dhcp4: false
      addresses: [192.168.1.210/24]
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8,8.8.4.4]
  version: 2
  
```

Ilustración 1. Máquina virtual Ubuntu server con ip fija



```

carlos@ubuntuserver:/var/www/html$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Drop-In: /lib/systemd/system/apache2.service.d
            └─ apache2-systemd.conf
   Active: active (running) since Thu 2020-04-16 18:00:17 UTC; 1h 55min ago
   Process: 836 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 1135 (apache2)
    Tasks: 8 (limit: 1108)
   CGroup: /system.slice/apache2.service
           └─ 1135 /usr/sbin/apache2 -k start
             1199 /usr/sbin/apache2 -k start
             1200 /usr/sbin/apache2 -k start
             1201 /usr/sbin/apache2 -k start
             1203 /usr/sbin/apache2 -k start
             1204 /usr/sbin/apache2 -k start
            13577 /usr/sbin/apache2 -k start
            26883 /usr/sbin/apache2 -k start

abr 16 18:00:09 ubuntuserver systemd[1]: Starting The Apache HTTP Server...
abr 16 18:00:17 ubuntuserver apachectl[836]: AH00558: apache2: Could not reliably determine
abr 16 18:00:17 ubuntuserver systemd[1]: Started The Apache HTTP Server.
carlos@ubuntuserver:/var/www/html$
  
```

Ilustración 2. La máquina virtual con apache instalado

```
carlos@ubuntu:~$ sudo netstat -ptan
[sudo] password for carlos:
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      747/systemd-resolve
tcp        0      0 192.168.1.210:33226     0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.1.210:58704     0.0.0.0:*               LISTEN      -
tcp6       0      0 :::21                   :::*                    LISTEN      1114/vsftpd
tcp6       0      0 :::80                   :::*                    LISTEN      1263/apache2
```

Ilustración 3. Puertos de escucha.

- Máquina virtual con un servidor Windows 2016 Server.

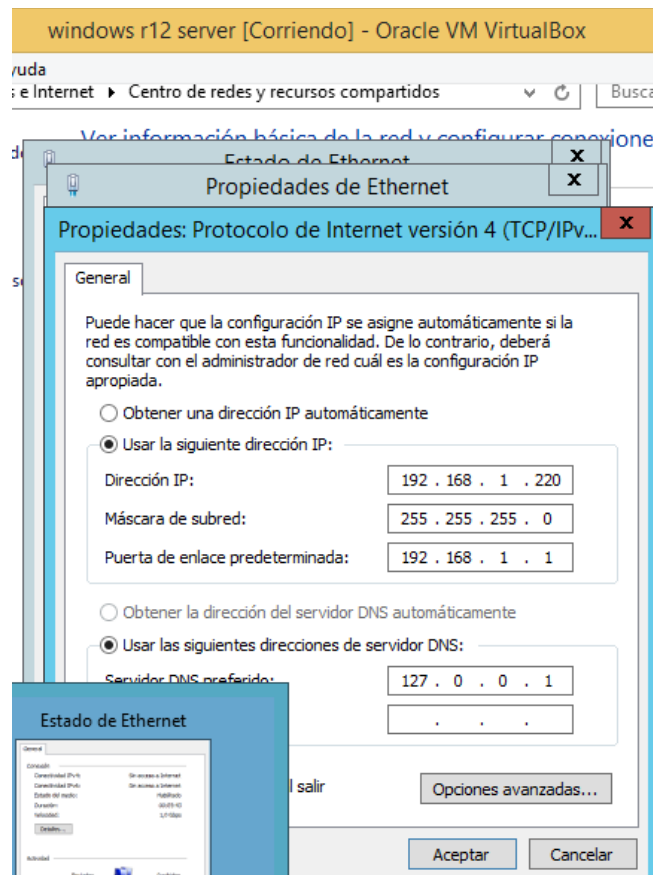


Ilustración 4. MV Windows server r12 con ip fija

- Máquina virtual con el sistema operativo que quieras. El único requisito que debe cumplir es que tenga instalado un navegador web.

Para ello uso una máquina virtual con Ubuntu desktop sin ip fija.

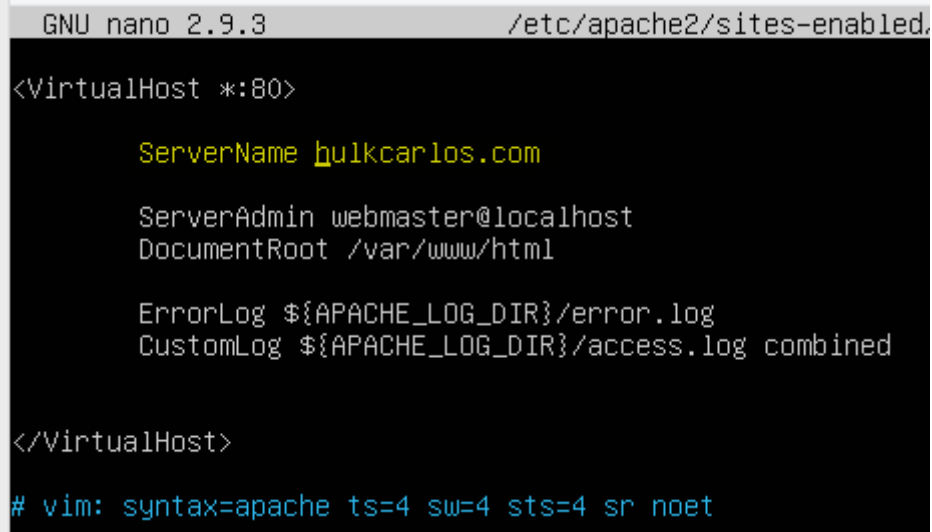
Actividad 1. Instalación y configuración servidores DNS

1. Instala y configura un servidor web, basado en Apache, sobre una máquina Virtual Linux sin interfaz gráfica (por ej. Ubuntu Server 18.04). El servidor deberá tener IP fija. Las características de este dominio han de ser las siguientes:

- Nombre del dominio: hultunombre.com (ej. dominiojuan.com)
- Nombre del sitio web: www.hultunombre.com (www.hulkjuan.com)
- IP red: 192.168.1.X
- Contenido de la web: “Yo, Nombre Apellidos, soy Hulk!”.

(1 punto)

Editamos el archivo de configuración de apache para cambiar el nombre de dominio:



```
GNU nano 2.9.3 /etc/apache2/sites-enabled/000-default.conf
<VirtualHost *:80>

    ServerName hulkcarlos.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

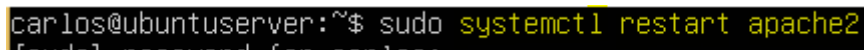
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Ilustración 5. Nombre de dominio cambiado a www.hulkcarlos.com

Este nombre de dominio es el nombre del servidor. Sin embargo todavía falta poner el nombre del sitio web. Como hemos hecho un cambio en el servidor de apache, hay que reiniciar el servicio:



```
carlos@ubuntuuserver:~$ sudo systemctl restart apache2
[sudo] password for carlos:
```

Ilustración 6. Restablecemos apache después de hacer cambios.

Ahora cambiamos el contenido de la web. En el archivo de configuración anterior se ve que la ruta por defecto de las webs que se muestran es `/var/www/html`, así que ahí modificamos el `index.html`

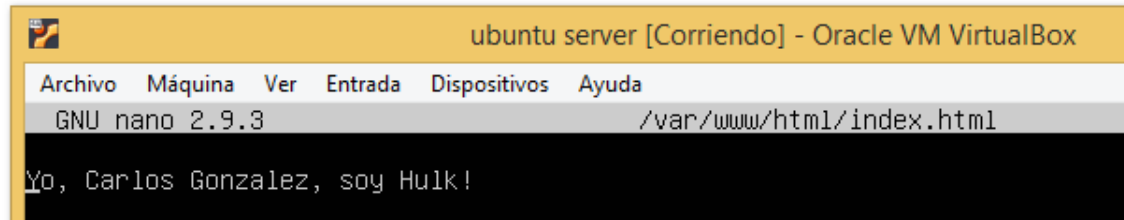


Ilustración 7. Editando index.html

Y comprobamos desde otra máquina el resultado:



Ilustración 8. Accedemos al servidor desde MV cliente.

2. Instala y configura un servidor DNS sobre la misma máquina Virtual Linux sin interfaz gráfica del ejercicio anterior. Configura un servidor tipo master con la siguiente configuración:

- Nombre de zona principal directa: hultunombre.com
- Archivo de zona principal directa: hultunombre.com.zona
- Crear una zona de búsqueda inversa (**zona directa es cuando preguntas por el nombre y te responde la ip, y la zona inversa es cuando preguntas por una ip y te responde el nombre**)
- Type master (**quiere decir principal, podría ser tipo slave, quiere decir que es como una réplica del principal y si éste falla, quedaría el master**)
- Zona de búsqueda inversa para IPv4
- Id red: 192.168.1.X

(1,5 puntos)

Empezamos instalando el servidor DNS en Ubuntu server, instalamos el paquete *bind9*:

```
carlos@ubuntuserver:~$ sudo apt install bind9
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  linux-image-4.15.0-76-generic linux-modules-4.15.0-76-generic
  linux-modules-extra-4.15.0-76-generic
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  bind9utils python3-ply
Paquetes sugeridos:
  bind9-doc resolvconf python-ply-doc
Los siguientes paquetes se ELIMINARÁN:
  linux-headers-4.15.0-76-generic
Se instalarán los siguientes paquetes NUEVOS:
  bind9 bind9utils python3-ply
0 actualizados, 3 nuevos se instalarán, 1 para eliminar y 0 no actualizados.
1 no instalados del todo o eliminados.
Se necesita descargar 660 kB de archivos.
Se liberarán 9.515 kB después de esta operación.
¿Desea continuar? [S/n] _
```

Ilustración 9. Instalación de bind9 (DNS)

Una vez instalado el DNS, éste dispone de varios archivos para configurar parámetros.

```
carlos@ubuntuserver:/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
carlos@ubuntuserver:/etc/bind$ _
```

Ilustración 10. Varios archivos de configuración del DNS

El fichero `db.root` tiene un listado de los servidores raíz.

El fichero `named.conf` tiene un listado de los ficheros en los que hay configuración de este servicio.

```
carlos@ubuntuserver:/etc/bind$ cat 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";
carlos@ubuntuserver:/etc/bind$ _
```

Ilustración 11. Contenido del fichero `named.conf`

En el fichero `named.conf.default-zones` podemos ver como es la estructura de definición de zona, para crear nosotros una nueva zona:

```
zone "localhost" {
    type master;
    file "/etc/bind/db.localhost";
};

zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};
```

Ilustración 12. Ejemplos de definiciones de zona (fichero `named.conf.default-zones`)

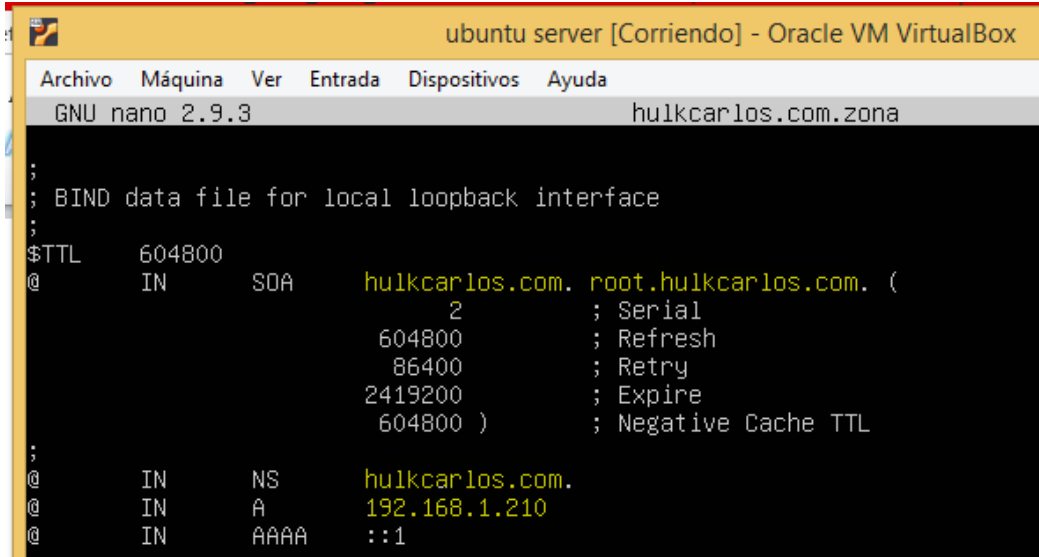
Para configurar las zonas, tendremos que modificar el contenido del fichero `named.conf.local`. En el fichero `db.localhost` viene una plantilla de zona directa, y en `db.127` viene la plantilla de una zona inversa.

Por tanto, para crear una zona local, creamos una copia del fichero de plantilla de zona directa y lo llamamos como nos pide el enunciado:

```
carlos@ubuntuserver:/etc/bind$ sudo cp db.localhost hulkcarlos.com.zona
[sudo] password for carlos:
Sorry, try again.
[sudo] password for carlos:
carlos@ubuntuserver:/etc/bind$ ls
bind.keys  db.255    db.root   named.conf.default-zones  rndc.key
db.0       db.empty  hulkcarlos.com.zona      named.conf.local          zones.rfc1918
db.127     db.localhost  named.conf               named.conf.options
carlos@ubuntuserver:/etc/bind$ _
```

Ilustración 13. Creo nueva zona directa y compruebo que se ha creado

A continuación editamos el nuevo fichero y lo adaptamos:



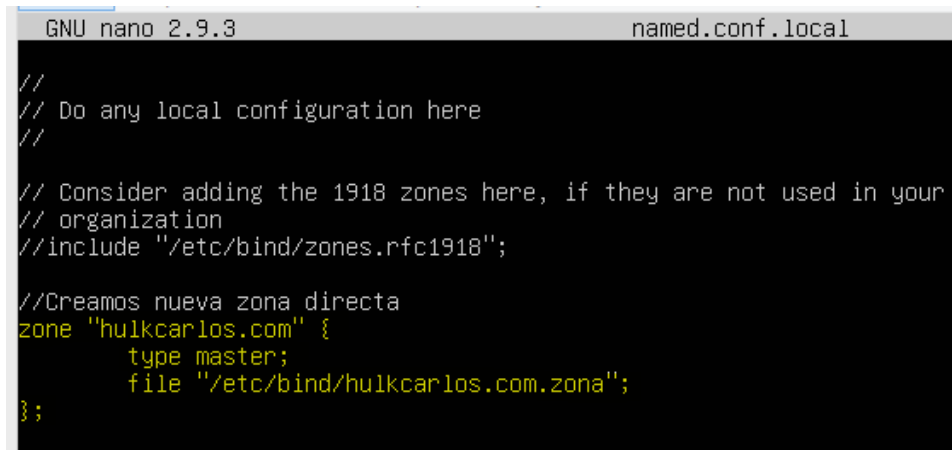
```

ubuntu server [Corriendo] - Oracle VM VirtualBox
GNU nano 2.9.3 hulkcarlos.com.zona

;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      hulkcarlos.com. root.hulkcarlos.com. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       hulkcarlos.com.
@         IN      A        192.168.1.210
@         IN      AAAA     ::1
  
```

Ilustración 14. Fichero modificado de zona

Ahora hay que crear el registro correspondiente al fichero recién modificado. Lo añadimos en el fichero named.conf, no en el default-zones, sino en el local, porque trabajaremos en local, pero nos apoyamos en el named.conf-default-zones para ver la sintaxis:



```

GNU nano 2.9.3 named.conf.local

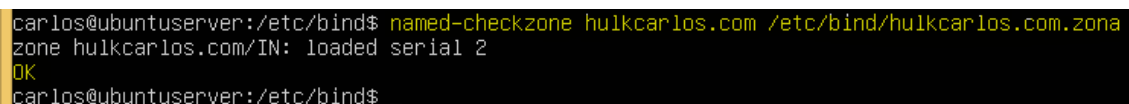
//
// Do any local configuration here
//

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

//Creamos nueva zona directa
zone "hulkcarlos.com" {
    type master;
    file "/etc/bind/hulkcarlos.com.zona";
};
  
```

Ilustración 15. Editamos named.conf.local para añadir nuestra nueva zona

Para asegurarnos que hemos escrito bien la nueva zona podemos comprobarlo con la herramienta named-checkzone:



```

carlos@ubuntu-server:/etc/bind$ named-checkzone hulkcarlos.com /etc/bind/hulkcarlos.com.zona
zone hulkcarlos.com/IN: loaded serial 2
OK
carlos@ubuntu-server:/etc/bind$ _
  
```

Ilustración 16. Nos indica que está bien creada la zona.

```
carlos@ubuntuserver:/etc/bind$ sudo systemctl restart bind9
carlos@ubuntuserver:/etc/bind$ sudo systemctl status bind9
• bind9.service - BIND Domain Name Server
  Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor
  Active: active (running) since Sun 2020-04-19 09:35:28 UTC; 25s ago
  Docs: man:named(8)
```

Ilustración 17. Como siempre, restableciendo servicio después de hacer modificaciones

Para la zona inversa es lo mismo. Creamos una copia de la “plantilla” db.127, y modificamos su contenido:

```
carlos@ubuntuserver:/etc/bind$ sudo cp db.127 hulkcarlos.inversa.com.zona
```

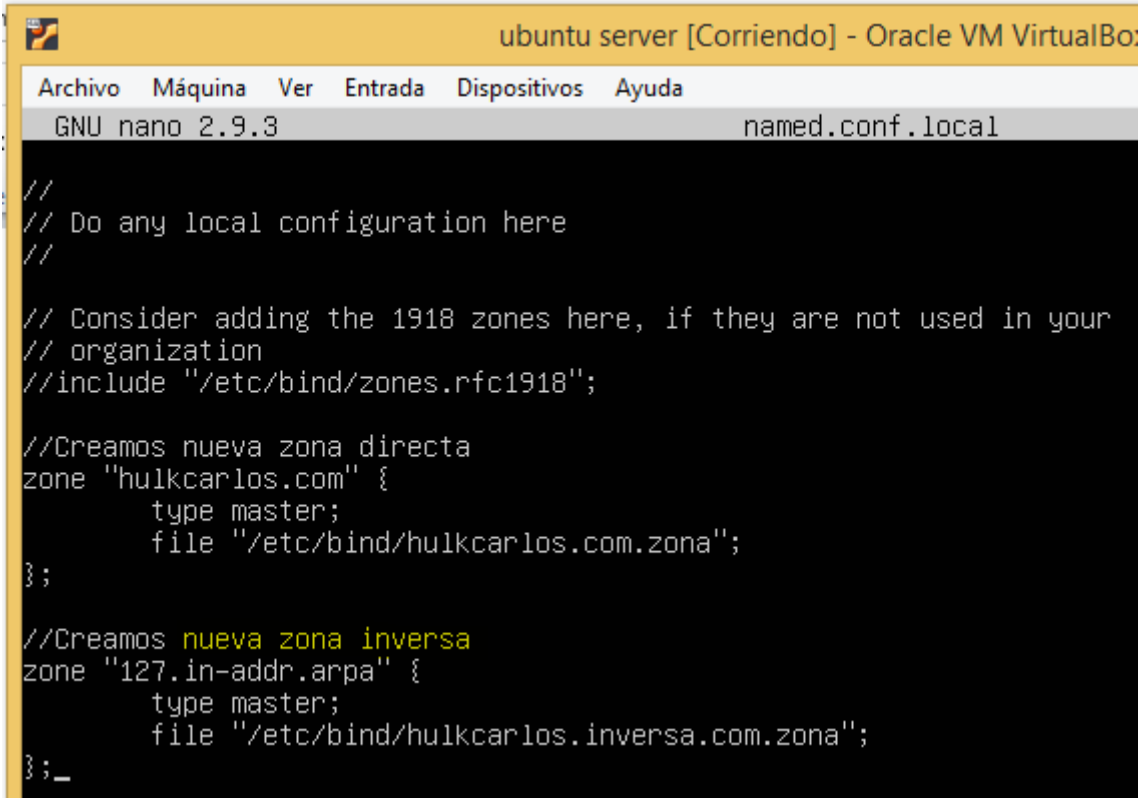
Ilustración 18. Creando zona inversa

Ahora modificamos el nuevo fichero:

```
GNU nano 2.9.3 hulkcarlos.inversa.com.zona
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
@ IN SOA hulkcarlos.com. root.hulkcarlos.com. (
        1          ; Serial
        604800     ; Refresh
        86400      ; Retry
        2419200    ; Expire
        604800 )   ; Negative Cache TTL
;
@ IN NS hulkcarlos.com.
1.0.0 IN PTR hulkcarlos.com.
```

Ilustración 19. Fichero de zona inversa

Ahora añadimos el registro en el fichero named.conf.local:



```
ubuntu server [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 2.9.3 named.conf.local

//
// Do any local configuration here
//

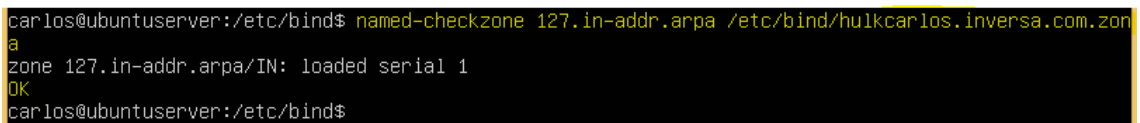
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

//Creamos nueva zona directa
zone "hulkcarlos.com" {
    type master;
    file "/etc/bind/hulkcarlos.com.zona";
};

//Creamos nueva zona inversa
zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/hulkcarlos.inversa.com.zona";
};_
```

Ilustración 20. Registramos la nueva zona inversa que acabamos de crear

Por último reseteamos el servicio y comprobamos de la misma manera que lo hicimos con la zona directa, que funciona correctamente:



```
carlos@ubuntu-server:/etc/bind$ named-checkzone 127.in-addr.arpa /etc/bind/hulkcarlos.inversa.com.zona
zone 127.in-addr.arpa/IN: loaded serial 1
OK
carlos@ubuntu-server:/etc/bind$
```

Ilustración 21. Zona inversa funcionando bien.

```

carlos@ubuntuuserver:/etc/bind$ sudo systemctl restart bind9
carlos@ubuntuuserver:/etc/bind$ sudo systemctl status bind9
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2020-04-19 14:04:33 UTC; 12s ago
     Docs: man:named(8)
  Process: 8519 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 31479 (named)
    Tasks: 4 (limit: 1108)
   CGroup: /system.slice/bind9.service
           └─31479 /usr/sbin/named -f -u bind

abr 19 14:04:38 ubuntuuserver named[31479]: network unreachable resolving './DNSKEY/IN': 2001:500:12:
abr 19 14:04:38 ubuntuuserver named[31479]: network unreachable resolving './DNSKEY/IN': 2001:500:2::
abr 19 14:04:38 ubuntuuserver named[31479]: resolver priming query complete
abr 19 14:04:38 ubuntuuserver named[31479]: checkhints: b.root-servers.net/A (199.9.14.201) missing f
abr 19 14:04:38 ubuntuuserver named[31479]: checkhints: b.root-servers.net/A (192.228.79.201) extra r
abr 19 14:04:38 ubuntuuserver named[31479]: checkhints: b.root-servers.net/AAAA (2001:500:200::b) mis
abr 19 14:04:38 ubuntuuserver named[31479]: checkhints: b.root-servers.net/AAAA (2001:500:84::b) extr
abr 19 14:04:38 ubuntuuserver named[31479]: checkhints: l.root-servers.net/AAAA (2001:500:9f::42) mis
abr 19 14:04:38 ubuntuuserver named[31479]: checkhints: l.root-servers.net/AAAA (2001:500:3::42) extr
abr 19 14:04:43 ubuntuuserver named[31479]: managed-keys-zone: Unable to fetch DNSKEY set '': timed
carlos@ubuntuuserver:/etc/bind$ netstat -ptan
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 192.168.1.210:53        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      0 127.0.0.1:953          0.0.0.0:*                LISTEN      -
tcp6       0      0 :::53                  :::*                    LISTEN      -
tcp6       0      0 :::21                  :::*                    LISTEN      -
tcp6       0      0 :::1:953                :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
carlos@ubuntuuserver:/etc/bind$ _

```

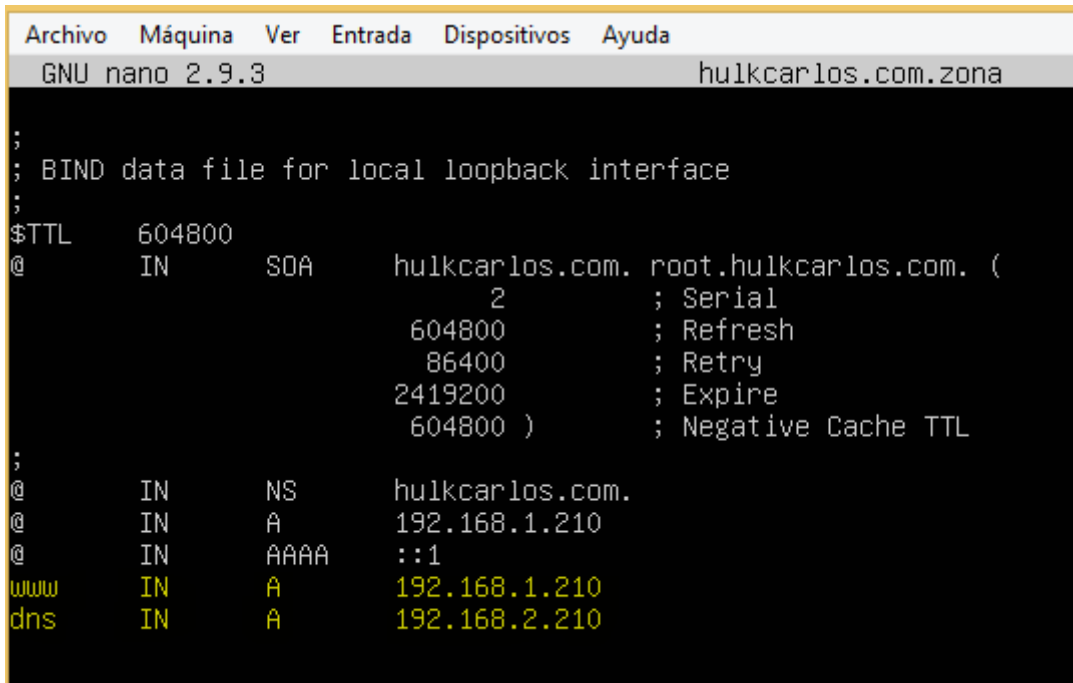
Ilustración 22. Reinicio del servicio y comprobamos el status.

3. Crea 2 registros en el servidor DNS **UBUNTU** Windows para un dominio llamado `www.hulktunombre.com`, que apuntará a la IP de la VM del apartado 1, y otro `dns.hulktunombre.com`, que apuntará a la misma IP de la VM. Comprueba desde una máquina cliente la resolución de este dominio.

(2 puntos)

Utilizaremos el dns de UBUNTU sobre el que venimos trabajando hasta ahora.

Para añadir los dos registros hay que editar el fichero de zona creado, en nuestro caso `hulkcarlos.com.zona`:



```

Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 2.9.3 hulkcarlos.com.zona

;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      hulkcarlos.com. root.hulkcarlos.com. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       hulkcarlos.com.
@         IN      A        192.168.1.210
@         IN      AAAA     ::1
www       IN      A        192.168.1.210
dns       IN      A        192.168.2.210

```

Ilustración 23. Añadimos dos registros, uno `www` y otro `dns`

Importante!! Para comprobar los resultados, podemos comprobarlo desde el propio servidor, pero es importante acordarse de que el dns que utiliza no es el que hemos instalado, sino el que tiene configurado por nosotros, que no es el que hemos instalado. Por tanto es importante, antes de probar, configurar el dns, es decir, la máquina de Ubuntu server con la que estoy trabajando, decirle que utilice el dns que hemos instalado en esta práctica y no otro, como puede ser el del router al cual está conectada o la máquina física en cual se hospeda.

Lo mismo pasa desde cliente, hay que configurar el DNS para que en primer lugar utilice el dns de ésta máquina virtual Ubuntu.

```

Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 2.9.3 /etc/netplan/50-cloud-init.yaml

# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. 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:
      dhcp4: false
      addresses: [192.168.1.210/24]
      gateway4: 192.168.1.1
      nameservers:
        addresses: [192.168.1.210,8.8.4.4]
  version: 2

```

Ilustración 24. Cambio de DNS. En primer lugar consulta a esta máquina

```

carlos@ubuntuuser: /etc/bind$ sudo netplan apply
carlos@ubuntuuser: /etc/bind$

```

Ilustración 25. Aplicamos cambios de DNS

Para comprobar desde el propio servidor podemos utilizar nslookup

```

carlos@ubuntuuser: ~$ nslookup www.hulkcarlos.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.hulkcarlos.com
Address: 192.168.1.210

carlos@ubuntuuser: ~$ nslookup dns.hulkcarlos.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   dns.hulkcarlos.com
Address: 192.168.2.210

carlos@ubuntuuser: ~$

```

Ilustración 26. Comprobación desde el propio servidor

Ahora comprobamos desde la MV Ubuntu cliente. Para ello configuramos previamente el DNS, para que utilice el que acabamos de crear:

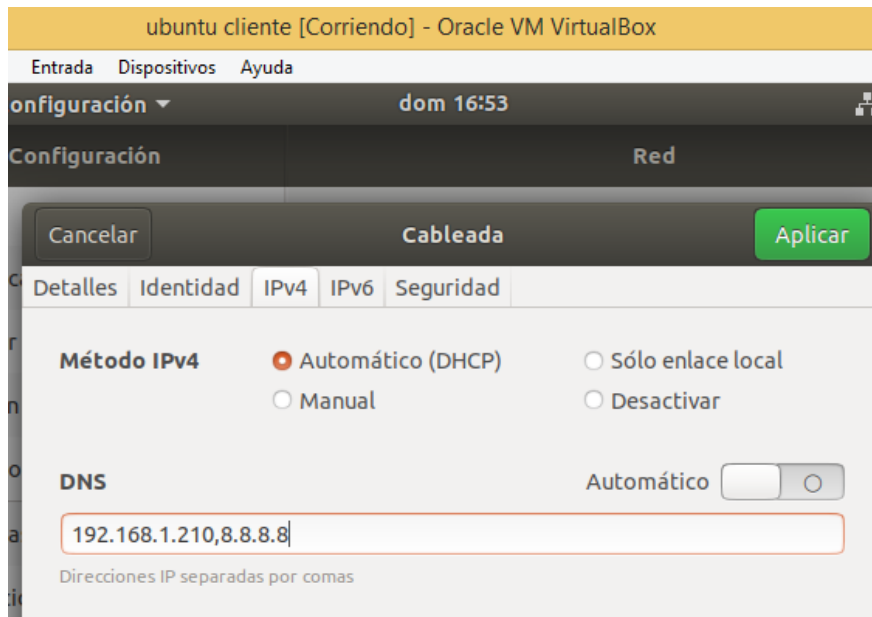


Ilustración 27. Configuramos dns en cliente

```
carlos@carlos-VirtualBox:~$ nmcli dev show | grep DNS
IP4.DNS[1]: 192.168.1.210
IP4.DNS[2]: 8.8.8.8
carlos@carlos-VirtualBox:~$
```

Ilustración 28. Vemos que tenemos configurado como DNS nuestro servidor

Teniendo configurado el DNS en cliente, comprobamos que funciona bien:

```
carlos@carlos-VirtualBox:~$ nslookup www.hulkcarlos.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: www.hulkcarlos.com
Address: 192.168.1.210

carlos@carlos-VirtualBox:~$ nslookup dns.hulkcarlos.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: dns.hulkcarlos.com
Address: 192.168.2.210

carlos@carlos-VirtualBox:~$
```

Ilustración 29. comprobamos con nslookup que accedemos a ambos nombres

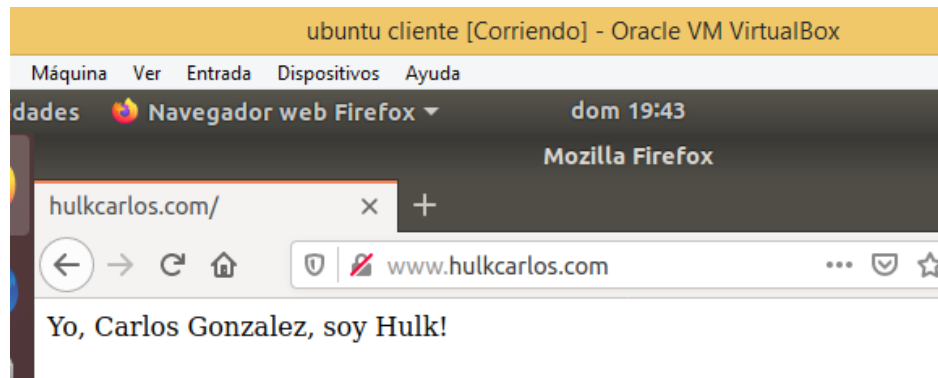


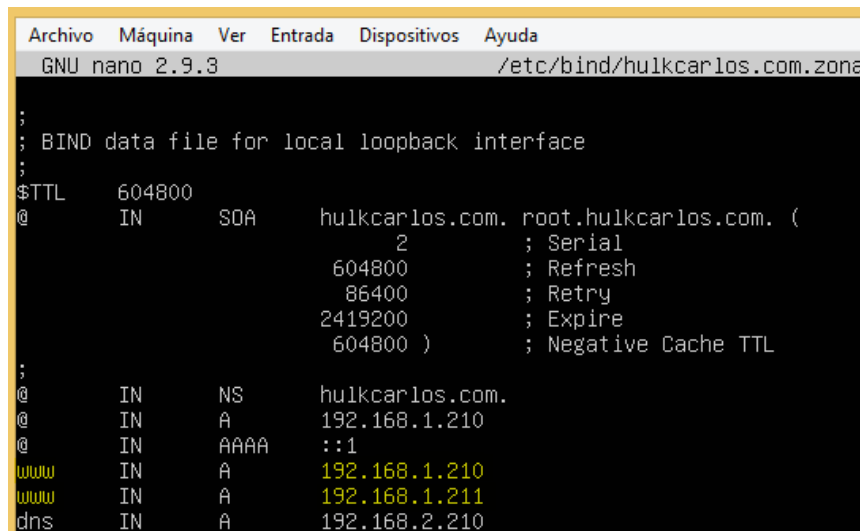
Ilustración 30. Comprobamos con el navegador que accedemos a www.hulkcarlos.com

4. Configura Round Robin en el servidor DNS para el registro de recurso de la página web, www.hulktunombre.com.

(2 puntos)

Round Robin lo que hace es que cuando se solicita un sitio web, indiscriminadamente responde un servidor u otro, de tal forma que esos servidores tienen la misma información que muestran al usuario. De esta manera se evita sobrecargar un servidor, repartiendo la carga entre dos o más.

Para ello editamos el fichero de la zona que hemos creado antes y para un mismo nombre de dominio, le añadimos varias direcciones ip.



```

Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 2.9.3 /etc/bind/hulkcarlos.com.zona

;
; BIND data file for local loopback interface
;
$TTL 604800
@      IN      SOA      hulkcarlos.com. root.hulkcarlos.com. (
                        2      ; Serial
                        604800  ; Refresh
                        86400   ; Retry
                        2419200 ; Expire
                        604800  ) ; Negative Cache TTL
;
@      IN      NS       hulkcarlos.com.
@      IN      A        192.168.1.210
@      IN      AAAA     ::1
www    IN      A        192.168.1.210
www    IN      A        192.168.1.211
dns    IN      A        192.168.2.210

```

Ilustración 31. Un mismo nombre de dominio con varias ip.

Además de esa configuración se necesitaría otro servidor con esa nueva ip y que ambos tuvieran el mismo contenido. Se guardan los cambios y se reinicia el servicio:

```
carlos@ubuntuuserver:~$ sudo systemctl restart bind9
carlos@ubuntuuserver:~$ sudo systemctl status bind9
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2020-04-19 19:35:50 UTC; 4s ago
     Docs: man:named(8)
  Process: 1076 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 1080 (named)
    Tasks: 4 (limit: 1108)
   CGroup: /system.slice/bind9.service
           └─1080 /usr/sbin/named -f -u bind

abr 19 19:35:50 ubuntuuserver named[1080]: network unreachable resolving './DNSKEY/IN': 2001:500:3::4
abr 19 19:35:50 ubuntuuserver named[1080]: network unreachable resolving './NS/IN': 2001:500:3::42#53
abr 19 19:35:50 ubuntuuserver named[1080]: managed-keys-zone: Key 20326 for zone . acceptance timer c
abr 19 19:35:50 ubuntuuserver named[1080]: resolver priming query complete
abr 19 19:35:50 ubuntuuserver named[1080]: checkhints: b.root-servers.net/A (199.9.14.201) missing fr
abr 19 19:35:50 ubuntuuserver named[1080]: checkhints: b.root-servers.net/A (192.228.79.201) extra re
abr 19 19:35:50 ubuntuuserver named[1080]: checkhints: b.root-servers.net/AAAA (2001:500:200::b) miss
abr 19 19:35:50 ubuntuuserver named[1080]: checkhints: b.root-servers.net/AAAA (2001:500:84::b) extra
abr 19 19:35:50 ubuntuuserver named[1080]: checkhints: l.root-servers.net/AAAA (2001:500:9f::42) miss
abr 19 19:35:50 ubuntuuserver named[1080]: checkhints: l.root-servers.net/AAAA (2001:500:3::42) extra
carlos@ubuntuuserver:~$
```

Ilustración 32. Restablecemos servicio DNS después de añadir dos ips a una misma web

Y probamos con nslookup desde cliente para comprobar que nos muestre una ip diferente con el mismo nombre de dominio.

```
carlos@carlos-VirtualBox:~$ nslookup www.hulkcarlos.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.hulkcarlos.com
Address: 192.168.1.210
Name:   www.hulkcarlos.com
Address: 192.168.1.211

carlos@carlos-VirtualBox:~$ nslookup www.hulkcarlos.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.hulkcarlos.com
Address: 192.168.1.211
Name:   www.hulkcarlos.com
Address: 192.168.1.210

carlos@carlos-VirtualBox:~$
```

Ilustración 33. Cada vez me devuelve las ips en un orden distinto.

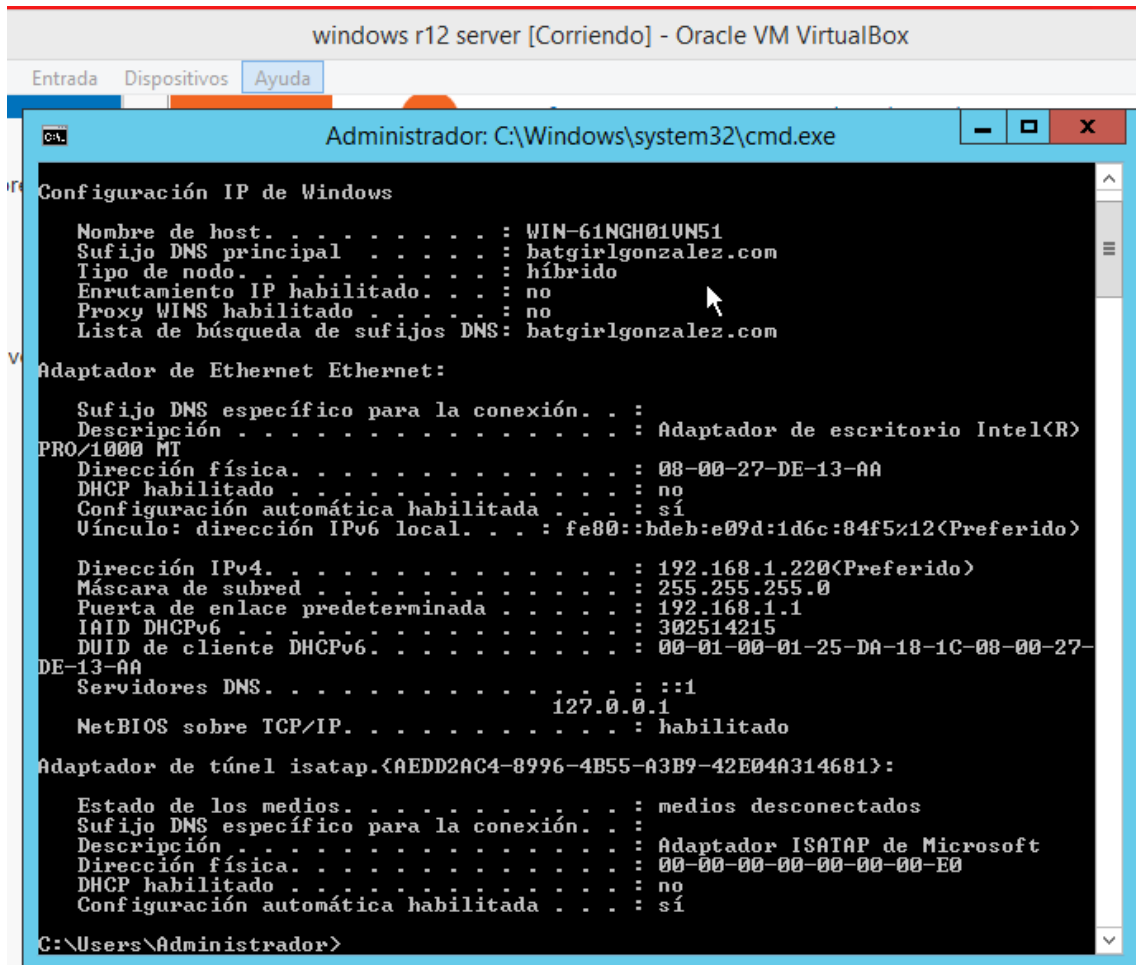
Instalación y configuración de LDAP

1. Instala y configura un servidor controlador de dominio con Active Directory y DNS sobre una máquina virtual Windows Server 2016.

- El servidor deberá tener una IP fija.
- El dominio deberá ser batgirltuapellido.com (ejemplo batgirllopez.com)
- Deberás crear un usuario inicialnombreapellido (ejemplo: jlopez), y un grupo de prueba llamado linkia al que pertenezca el usuario creado.

(1,5 puntos)

Para la realización de este apartado, partimos de una máquina virtual Windows server 2012 utilizada en la unidad formativa 1, que ya dispone de DNS instalado. Instalamos el servicio de dominio de directorio activo y nos queda la siguiente configuración:



```

windows r12 server [Corriendo] - Oracle VM VirtualBox
Entrada Dispositivos Ayuda

Administrador: C:\Windows\system32\cmd.exe

Configuración IP de Windows
Nombre de host. . . . . : WIN-61NGH01VN51
Sufijo DNS principal . . . . . : batgirlgonzalez.com
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . . . : no
Proxy WINS habilitado . . . . . : no
Lista de búsqueda de sufijos DNS: batgirlgonzalez.com

Adaptador de Ethernet Ethernet:
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Adaptador de escritorio Intel(R)
PRO/1000 MT
Dirección física. . . . . : 08-00-27-DE-13-AA
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::bdeb:e09d:1d6c:84f5%12(Preferido)

Dirección IPv4. . . . . : 192.168.1.220(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 302514215
DUID de cliente DHCPv6. . . . . : 00-01-00-01-25-DA-18-1C-08-00-27-
DE-13-AA
Servidores DNS. . . . . : ::1
127.0.0.1
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de túnel isatap.<AEDD2AC4-8996-4B55-A3B9-42E04A314681>:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Adaptador ISATAP de Microsoft
Dirección física. . . . . : 00-00-00-00-00-00-E0
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí

C:\Users\Administrador>
  
```

Ilustración 34. Configuración de la MV W server r12

Creamos usuario desde herramientas > Usuarios y equipos de Active Directory. Accedemos a la ventana para crear usuarios y grupos. Creamos un grupo llamado 'linkia' y un usuario 'cgonzalez':

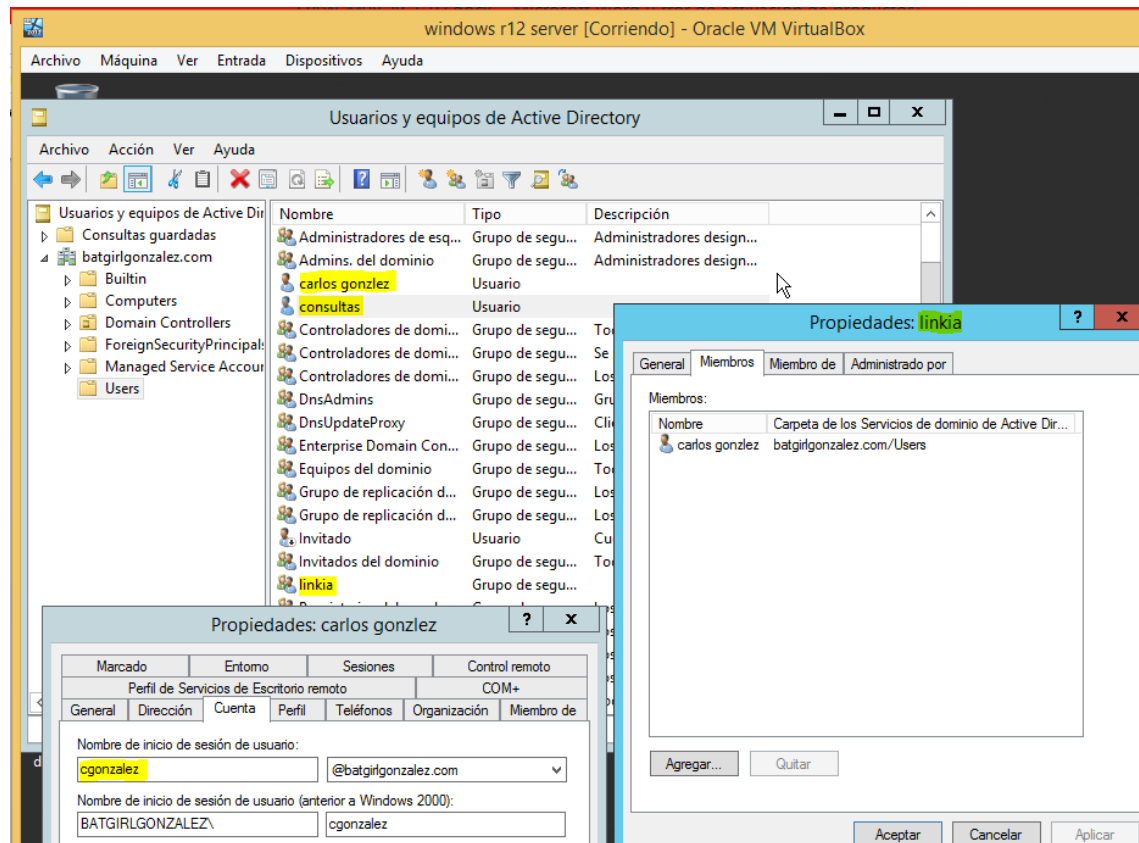


Ilustración 35. Se ha creado un grupo llamado 'linkia' y un usuario 'cgonzalez' que pertenece al grupo creado 'linkia'

También he creado un usuario "consultas" para que sirva de nexo con Apache del servidor Ubuntu. Esto servirá para el siguiente apartado, para que al acceder a apache desde cliente, vaya a autenticarse al LDAP.

2. Configura el servidor web para que autentique al usuario mediante Active Directory.

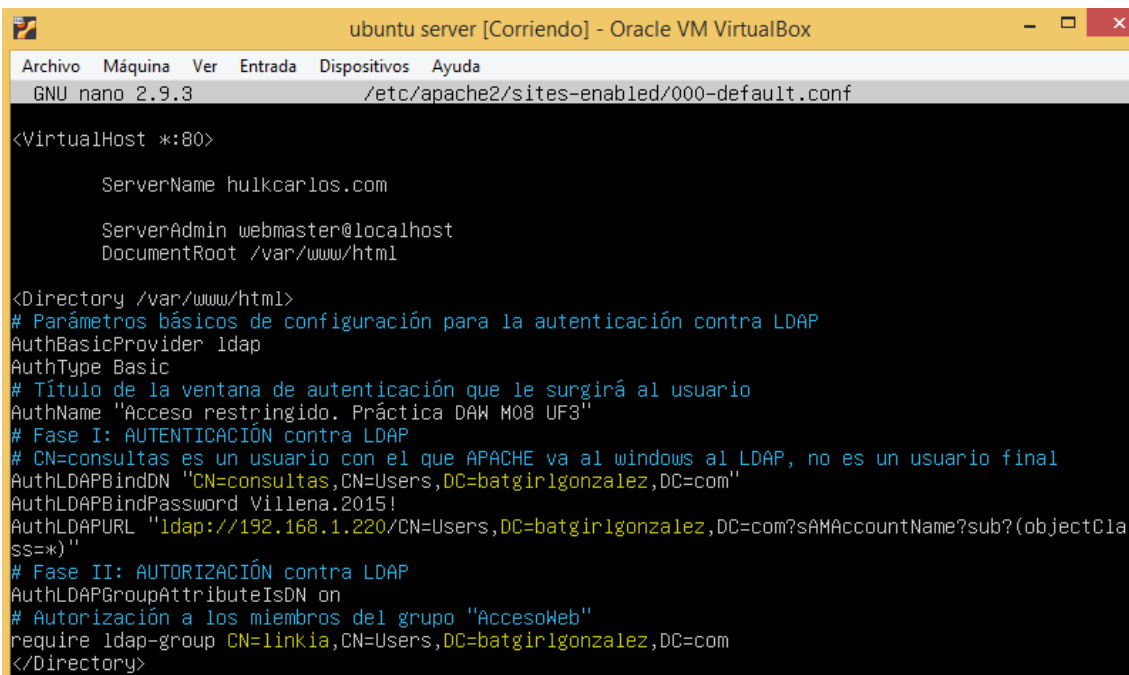
(1 punto)

Para configurar el apache de tal forma que autentique con el LDAP de Windows hay que habilita un módulo de apache:

```
carlos@ubuntuserver:~$ sudo a2enmod authnz_ldap
[sudo] password for carlos:
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
```

Ilustración 36. Módulo de autenticación LDAP en windows para Apache

Una vez finalizada la configuración en Windows server, ahora en Apache de la máquina de Ubuntu server tenemos que decir, mediante directivas, que cuando se acceda, que pida credenciales de LDAP:



```

<VirtualHost *:80>

    ServerName hulkcarlos.com

    ServerAdmin webmaster@localhost
    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. Práctica DAW M08 UF3"
        # Fase I: AUTENTICACIÓN contra LDAP
        # CN=consultas es un usuario con el que APACHE va al windows al LDAP, no es un usuario final
        AuthLDAPBindDN "CN=consultas,CN=Users,DC=batgirlgonzalez,DC=com"
        AuthLDAPBindPassword Villena.20151
        AuthLDAPURL "ldap://192.168.1.220/CN=Users,DC=batgirlgonzalez,DC=com?sAMAccountName?sub?(objectClass=*)"
        # Fase II: AUTORIZACIÓN contra LDAP
        AuthLDAPGroupAttributeIsDN on
        # Autorización a los miembros del grupo "AccesoWeb"
        require ldap-group CN=linkia,CN=Users,DC=batgirlgonzalez,DC=com
    </Directory>

```

Ilustración 37. Agregamos la configuración en Apache para que se identifique con las credenciales LDAP

Una vez configurado y realizado cambios en apache, como siempre, reiniciamos apache.

```
carlos@ubuntuuserver:~$ sudo systemctl restart apache2
carlos@ubuntuuserver:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Drop-In: /lib/systemd/system/apache2.service.d
            └─apache2-systemd.conf
   Active: active (running) since Mon 2020-04-20 15:44:09 UTC; 1min 22s ago
```

Ilustración 38. Reiniciamos Apache2 después de hacer cambios

Después reiniciamos el servicio y miramos el estado, para evitar posibles errores.

```
carlos@ubuntuuserver:~$ sudo systemctl restart apache2
carlos@ubuntuuserver:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Drop-In: /lib/systemd/system/apache2.service.d
            └─apache2-systemd.conf
   Active: active (running) since Sun 2020-04-19 19:58:36 UTC; 2min 22s ago
     Process: 31796 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS)
     Process: 31801 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 31817 (apache2)
     Tasks: 6 (limit: 1108)
   CGroup: /system.slice/apache2.service
           └─31817 /usr/sbin/apache2 -k start
             └─31829 /usr/sbin/apache2 -k start
               └─31830 /usr/sbin/apache2 -k start
                 └─31831 /usr/sbin/apache2 -k start
                   └─31832 /usr/sbin/apache2 -k start
                     └─31833 /usr/sbin/apache2 -k start

abr 19 19:58:36 ubuntuuserver systemd[1]: Starting The Apache HTTP Server...
abr 19 19:58:36 ubuntuuserver apachectl[31801]: AH00558: apache2: Could not reliably determine the se
abr 19 19:58:36 ubuntuuserver systemd[1]: Started The Apache HTTP Server.
carlos@ubuntuuserver:~$
```

Ilustración 39. Se reinicia y se comprueba estado de apache.

Y por último comprobamos desde la MV cliente, accedemos al dominio y vemos que ahora pide autenticación.

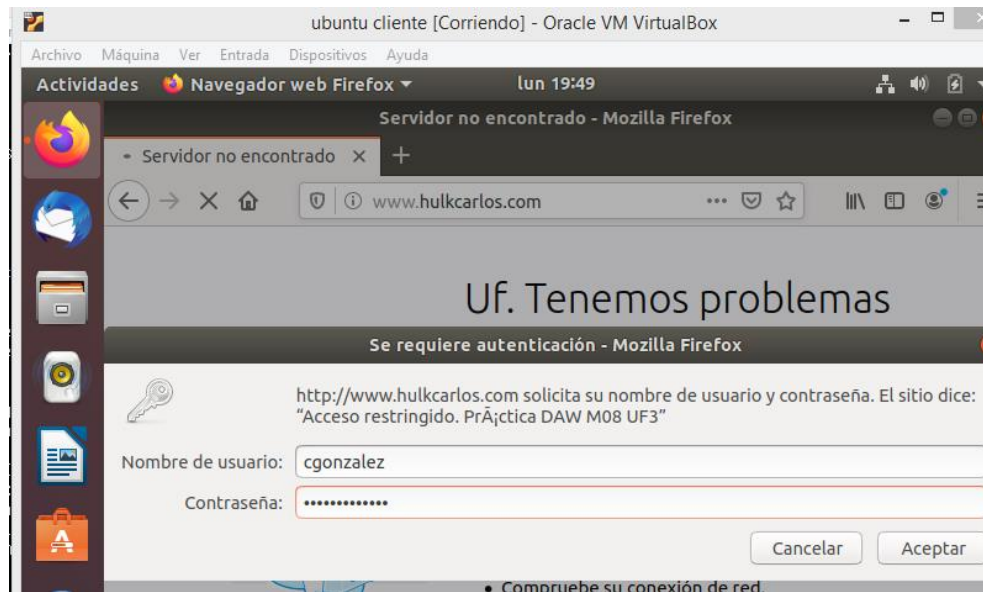


Ilustración 40. Acceso desde cliente a www.hulkcarlos.com y vemos que pide credenciales.

Utilizamos las credenciales del usuario creado en LDAP para acceder:

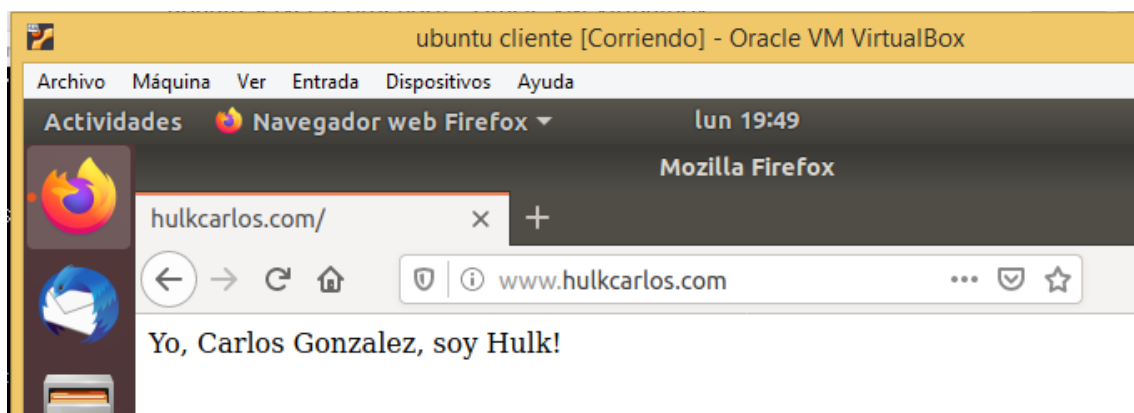


Ilustración 41. Hemos accedido con las credenciales de LDAP a un sitio hospedado en Apache

Webgrafía

<https://unix.stackexchange.com/questions/204477/named-checkzone-fails-reverse-zone-file-with-ns-has-no-address-records-a-or-aaa>

<https://serverfault.com/questions/693352/not-able-to-load-reverse-zone-with-bind>

<https://www.enmimaquinafunciona.com/pregunta/47122/como-saber-que-dns-estoy-utilizando-de-ubuntu-1404-en-adelante>