

DNS

Parte 2: Instalación y Configuración de un Servicio DNS en Entorno Local

Despliegue de Aplicaciones Web

Francisco Javier Arruabarrena Sabroso
Erlin Francisco Sapeg Soriano

Índice

Supuestos previos	2
Práctica	3
Parte 1: Configuración del Servidor Raíz.....	3
Instalación de BIND en el servidor raíz	3
Configurar BIND como servidor raíz	3
Definir la zona raíz y reenviar consultas	5
Reiniciar BIND	5
Parte 2: Configuración del Servidor Autoritativo para el Dominio .	6
Instalación de BIND en el servidor autoritativo	6
Configurar la zona autoritativa para lapaloma.com	6
Crear el archivo de zona db.lapaloma.com	7
Reiniciar BIND	9
Parte 3: Comprobación de configuración correcta.....	10
Parte 4: Configuración del cliente	12
Configuración de DNS preferido	12
Comprobación con nslookup	13
Bibliografía	14

Supuestos previos

Se va a partir de una arquitectura con tres máquinas:

- **Máquina Anfitriona Windows** (192.186.56.1): Actuará como el cliente DNS, que realizará consultas de nombres de dominio.
- **Servidor DNS raíz (Ubuntu)** (192.168.56.101): Este servidor recibirá las consultas iniciales y redirigirá al servidor autoritativo para resolver nombres específicos del dominio lapaloma.com.
- **Servidor DNS autoritativo (Ubuntu)** (192.168.56.102): Este servidor será responsable de responder a las consultas para el dominio lapaloma.com.

Estas tres máquinas estarán ya activas y funcionando por lo que se obviará el cómo se ha llegado hasta este punto.

Se va a ir haciendo y documentando con explicaciones capturas de todos los pasos. Además, se va a explicar la razón del por qué se hace cada cosa.

Práctica

Parte 1: Configuración del Servidor Raíz

Instalación de BIND en el servidor raíz

Se ha de abrir un terminal en el servidor raíz, donde primero se van a actualizar los repositorios. Este paso asegura que se tiene la lista más reciente de paquetes disponibles. Es crucial para garantizar que se instale la versión más actualizada de BIND y sus dependencias.

```
jarasa03@Jarasa03-Ubuntu-24:~$ sudo apt update
```

Ahora ya se puede proceder a la instalación. BIND es el servidor DNS más utilizado en sistemas Unix/Linux. Se va a instalar para proporcionar servicios DNS, permitiendo la resolución de nombres de dominio a direcciones IP y viceversa. Los utils y la documentación se van a instalar para facilitar la configuración y solución de problemas a futuro.

```
jarasa03@Jarasa03-Ubuntu-24:~$ sudo apt install bind9 bind9utils bind9-doc
```

Configurar BIND como servidor raíz

Se va a comenzar por editar el archivo de configuración. Este archivo contiene las opciones globales para BIND. Editarlo permite personalizar el comportamiento general del servidor DNS.

```
jarasa03@Jarasa03-Ubuntu-24:~$ sudo nano /etc/bind/named.conf.options
```

Se verá este archivo, el cual se tendrá que editar. Es recomendado editar las cosas poniendo comentarios cuando se editan, por si en un futuro se necesita ver lo que se cambió.

```
GNU nano 7.2 /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

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

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

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // 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
    //=====
```

[^]G Ayuda [^]O Guardar [^]W Buscar [^]K Cortar [^]T Ejecutar [^]C Ubicación
[^]X Salir [^]R Leer fich. [^]\ Reemplazar [^]U Pegar [^]J Justificar [^]/ Ir a línea

No se debe borrar nada de lo que ya está en este archivo de configuración y el archivo deberá quedar de manera que se muestra a continuación. “directory”, especifica dónde BIND almacenará sus archivos de caché, mejorando el rendimiento, por lo que no se tocará. “recursion yes”, permite que el servidor realice consultas recursivas, buscando respuestas completas para las consultas DNS. Esto es esencial para un servidor raíz que debe resolver consultas para cualquier dominio. “allow-query { any; }”, permite que cualquier cliente realice consultas a este servidor, necesario para un servidor DNS público o de prueba.

```
GNU nano 7.2 /etc/bind/named.conf.options *
options {
    directory "/var/cache/bind";

    // Edición realizada por jarasa03 a 15/11/2024
    recursion yes;
    allow-query { any; };

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

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

    // forwarders {
    //     0.0.0.0;
    // };

    // forwarders {
    //     0.0.0.0;
    // };
}
```

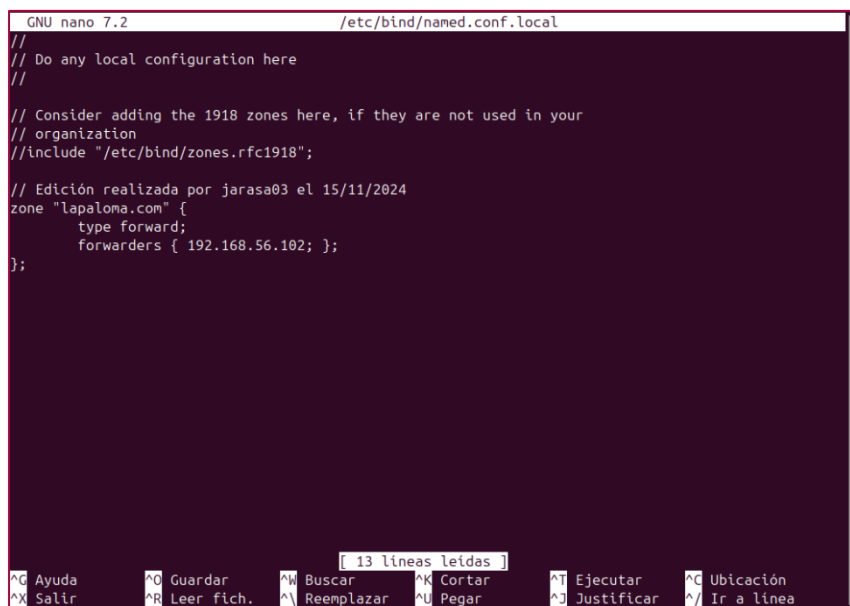
[^]G Ayuda [^]O Guardar [^]W Buscar [^]K Cortar [^]T Ejecutar [^]C Ubicación
[^]X Salir [^]R Leer fich. [^]\ Reemplazar [^]U Pegar [^]J Justificar [^]/ Ir a línea

Definir la zona raíz y reenviar consultas

Se va a editar un archivo de configuración que sirve para configurar zonas específicas. En este caso, se usará para definir cómo manejar las consultas para el dominio lapaloma.com.

```
jarasa03@Jarasa03-Ubuntu-24:~$ sudo nano /etc/bind/named.conf.local
```

Se pondrá la configuración mostrada a continuación, como siempre comentando el cambio. Esta configuración establece una zona de reenvío para lapaloma.com. Todas las consultas para este dominio serán reenviadas al servidor autoritativo (192.168.56.102). Esto es crucial para la estructura jerárquica de DNS, donde el servidor raíz sabe a quién preguntar por dominios específicos.



```
GNU nano 7.2 /etc/bind/named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
// Edición realizada por jarasa03 el 15/11/2024
zone "lapaloma.com" {
    type forward;
    forwarders { 192.168.56.102; };
};
```

[13 líneas leídas]

^G Ayuda	^O Guardar	^W Buscar	^K Cortar	^T Ejecutar	^C Ubicación
^X Salir	^R Leer fich.	^M Reemplazar	^U Pegar	^J Justificar	^L Ir a línea

Reiniciar BIND

Reiniciar el servicio es necesario para que BIND cargue y aplique los cambios de configuración realizados. Sin este paso, BIND continuaría operando con la configuración anterior.

```
jarasa03@Jarasa03-Ubuntu-24:~$ sudo systemctl restart bind9
```

Parte 2: Configuración del Servidor Autoritativo para el Dominio

Instalación de BIND en el servidor autoritativo

Se va a seguir el mismo proceso que en la parte uno para la instalación, así que no se explicará el por qué, solo se indicarán de nuevos los comandos utilizados.

```
jarasa03@Jarasa03-Ubuntu-24:~$ sudo apt update
```

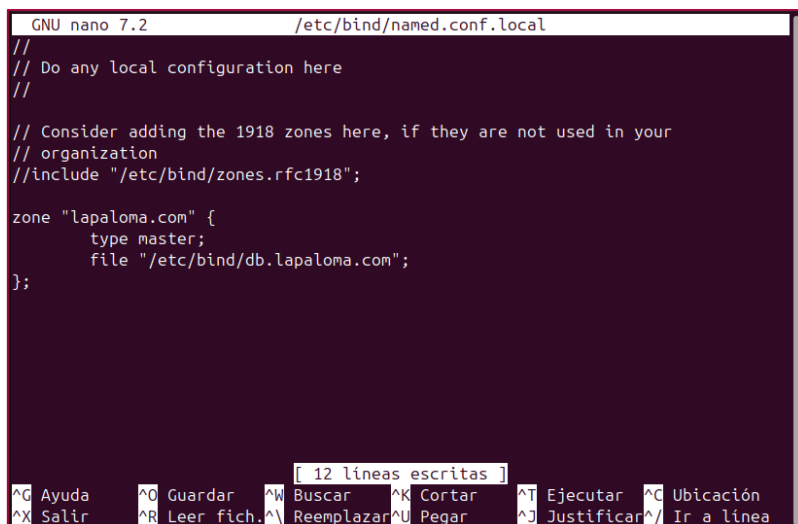
```
jarasa03@Jarasa03-Ubuntu-24:~$ sudo apt install bind9 bind9utils bind9-doc
```

Configurar la zona autoritativa para lapaloma.com

Se va a editar el archivo de configuración local en el servidor autoritativo. Este archivo se usa para definir las zonas para las cuales este servidor es la fuente autoritativa de información.

```
jarasa03@Jarasa03-Ubuntu-24:~$ sudo nano /etc/bind/named.conf.local
```

Se va a añadir la configuración mostrada en la siguiente captura. Esta configuración declara que este servidor es el maestro (autoritativo) para la zona lapaloma.com. El tipo "master" indica que este servidor tiene la información original y autoritativa para este dominio. El archivo especificado contendrá los registros DNS reales para el dominio.



```
GNU nano 7.2 /etc/bind/named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

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

[ 12 líneas escritas ]
^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación
^X Salir ^R Leer fich. ^V Reemplazar ^U Pegar ^J Justificar ^_ Ir a línea
```

Crear el archivo de zona db.lapaloma.com

Primero se va a copiar un archivo de ejemplo. Usar un archivo existente como plantilla ahorra tiempo y reduce errores, ya que proporciona una estructura básica correcta para un archivo de zona DNS.

```
jarasa03@Jarasa03-Ubuntu-24:~$ sudo cp /etc/bind/db.local /etc/bind/db.lapaloma.com
```

Ahora se editará este nuevo archivo con la configuración mostrada a continuación. Este archivo contiene los registros DNS reales para el dominio.

- SOA (Start of Authority): Define la información autoritativa de la zona.
- NS (Name Server): Especifica el servidor de nombres para el dominio.
- Registros A: Mapean nombres de host a direcciones IP. Estos registros son esenciales para que el DNS funcione, permitiendo la resolución de nombres como www.lapaloma.com a sus respectivas direcciones IP.

1. \$TTL 1

Define el Time To Live (TTL) predeterminado para todos los registros en este archivo. Un valor de 1 segundo es muy bajo y se usa generalmente para pruebas, permitiendo que los cambios se propaguen rápidamente.

2. @ IN SOA ns.lapaloma.com. admin.lapaloma.com. (

Esta línea inicia el registro SOA (Start of Authority).

- @ representa el dominio actual (lapaloma.com).
- IN significa "Internet".
- SOA indica que es un registro Start of Authority.
- ns.lapaloma.com. es el nombre del servidor DNS primario.
- admin.lapaloma.com. es el correo del administrador (reemplaza @ por .).

3. 2 ; Serial

Es un número de serie que debe incrementarse cada vez que se modifica el archivo. Ayuda a los servidores DNS secundarios a saber cuándo deben actualizar sus copias.

4. 604800 ; Refresh

Indica cada cuántos segundos un servidor secundario debe comprobar si hay actualizaciones.

5. 86400 ; Retry

Si un servidor secundario no puede contactar al primario, esperará este tiempo antes de volver a intentarlo.

6. 2419200 ; Expire

Si un servidor secundario no puede contactar al primario durante este tiempo, considerará que sus datos han expirado.

7. 1) ; Negative Cache TTL

Por qué y para qué: TTL para respuestas negativas (cuando un nombre no existe). El paréntesis cierra el registro SOA.

8. @ IN NS ns.lapaloma.com.

Define el servidor de nombres (NS) para el dominio. Indica que ns.lapaloma.com es el servidor de nombres autoritativo para lapaloma.com.

9. ns IN A 192.168.56.102

Por qué y para qué: Define la dirección IP del servidor de nombres ns.lapaloma.com.

10. www IN A 192.168.56.103

Define la dirección IP para www.lapaloma.com.

11. mail IN A 192.168.56.104

Define la dirección IP para mail.lapaloma.com.

```
jarsa03@Jarsa03-Ubuntu-24:~$ sudo nano /etc/bind/db.lapaloma.com
```

```

GNU nano 7.2 /etc/bind/db.lapaloma.com
$TTL 1
@ IN SOA ns.lapaloma.com. admin.lapaloma.com. (
    2 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    1 ) ; Negative Cache TTL
;
@ IN NS ns.lapaloma.com
ns IN A 192.168.56.102
www IN A 192.168.56.103
mail IN A 192.168.56.104

```

[12 líneas escritas]

^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación
 ^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^_ Ir a línea

Reiniciar BIND

Misma razón que en la parte 1.

```
jarasa03@Jarasa03-Ubuntu-24:~$ sudo systemctl restart bind9
```

Al haber cambiado los archivos de configuración BIND9, se sugiere ejecutar un comando así que se hará. Este comando hará que systemd vuelva a leer todas las configuraciones de unidades, incluyendo la de BIND9

```
jarasa03@Jarasa03-Ubuntu-24:~$ sudo systemctl daemon-reload
```

Ahora se volverá a hacer un restart de BIND9.

```
jarasa03@Jarasa03-Ubuntu-24:~$ sudo systemctl restart bind9
```

Parte 3: Comprobación de configuración correcta

Se va a usar dig para realizar la verificación. Dig es una herramienta de verificación DNS. Estas consultas verifican que:

1. El servidor raíz conoce el servidor NS correcto para lapaloma.com.
2. Las consultas para www y mail se resuelven correctamente a través de la cadena de servidores DNS configurada. Esta comprobación es crucial para asegurar que toda la configuración DNS funciona como se espera.

Muy importante, esto ha de hacerse desde el servidor raíz.

```
jarasa03@Jarasa03-Ubuntu-24:~$ dig @192.168.56.101 lapaloma.com

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> @192.168.56.101 lapaloma.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33827
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 5226557156a74cf9010000006740a067d1a4a4ed1cbd4336 (good)
;; QUESTION SECTION:
;lapaloma.com.                IN      A

;; AUTHORITY SECTION:
lapaloma.com.                1       IN      SOA     ns.lapaloma.com. admin.lapaloma.com. 2 604800 86400 2419200 1

;; Query time: 2 msec
;; SERVER: 192.168.56.101#53(192.168.56.101) (UDP)
;; WHEN: Fri Nov 22 15:16:55 UTC 2024
;; MSG SIZE rcvd: 114
```

Se le está preguntando a la paloma.com y dig está respondiendo con todo lo del SOA puesto con anterioridad.

```

jarasa03@Jarasa03-Ubuntu-24:~$ dig @localhost www.lapaloma.com

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> @localhost www.lapaloma.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55720
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c160ef67dbb870770100000067409e45d912b0960ef9f80f (good)
;; QUESTION SECTION:
;www.lapaloma.com.                IN      A

;; ANSWER SECTION:
www.lapaloma.com.                1       IN      A      192.168.56.103

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Fri Nov 22 15:07:49 UTC 2024
;; MSG SIZE rcvd: 89

```

En la captura anterior se quiere saber con qué IP resuelve el www y el comando dig devuelve la .103, como se puso en el archivo de configuración.

```

jarasa03@Jarasa03-Ubuntu-24:~$ dig @localhost mail.lapaloma.com

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> @localhost mail.lapaloma.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33821
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 2f52961d4bd098a20100000067409e4dc3277876bfea0b24 (good)
;; QUESTION SECTION:
;mail.lapaloma.com.                IN      A

;; ANSWER SECTION:
mail.lapaloma.com.                1       IN      A      192.168.56.104

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Fri Nov 22 15:07:57 UTC 2024
;; MSG SIZE rcvd: 90

```

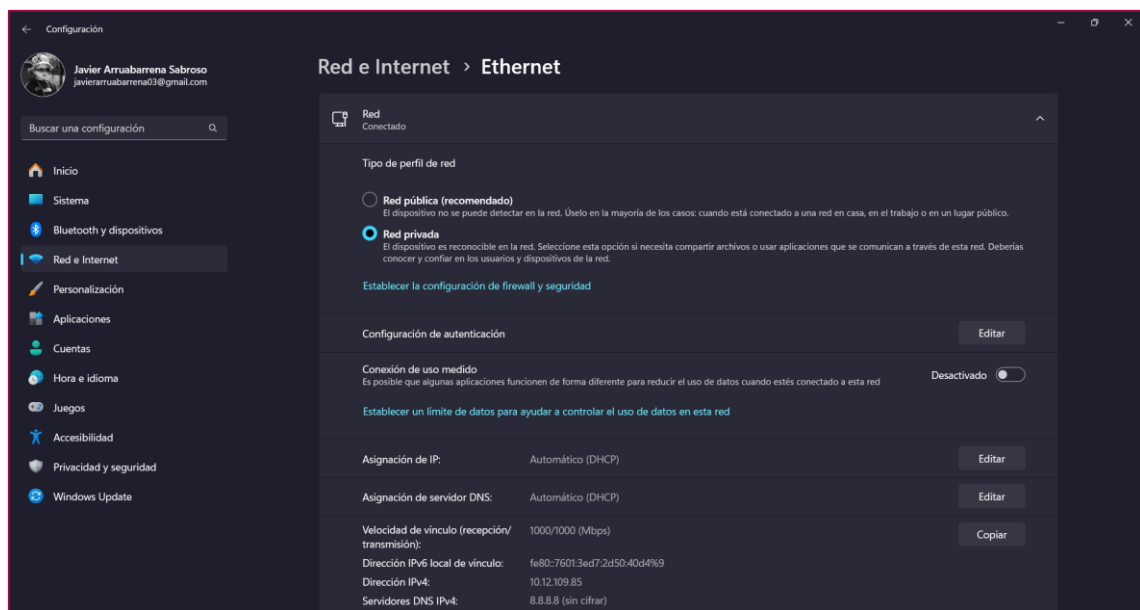
En la captura de arriba se muestra como resuelve el mail y lo hace con la .104., como se indicó en el fichero de configuración.

Parte 4: Configuración del cliente

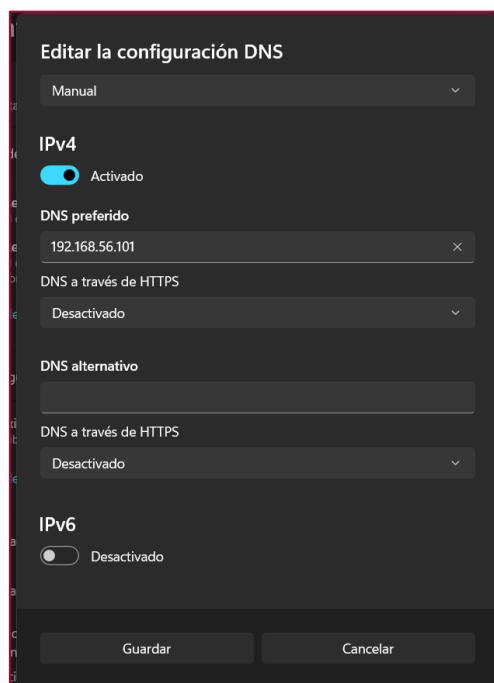
Configuración de DNS preferido

Ahora, se cambiará la configuración DNS del equipo anfitrión para usar el servidor DNS raíz (192.168.56.101). Esto va a permitir probar que el servidor DNS raíz esté funcionando correctamente desde la perspectiva de un cliente real. Se simula como un usuario final interactuaría con esta infraestructura DNS.

Primero se accede a la configuración de red del equipo anfitrión.



Se ha de localizar la opción de editar la asignación de servidor DNS y poner la ip 192.168.56.101. Se dará a guardar.



Comprobación con nslookup

Se va a utilizar la herramienta nslookup para resolver los nombres de dominio configurados. Esta herramienta permite verificar que las consultas DNS se resuelven correctamente a través del servidor raíz.

Se ha de abrir una terminal y ejecutar el siguiente comando. Se puede apreciar como devuelve la ip .103.

```
C:\Windows\System32>nslookup www.lapaloma.com
Servidor:  UnKnown
Address:  192.168.56.101

Respuesta no autoritativa:
Nombre:   www.lapaloma.com
Address:  192.168.56.103
```

Ahora se comprobará si funcional el mail.lapaloma.com. Se podrá apreciar que devuelve la .104.

```
C:\Windows\System32>nslookup mail.lapaloma.com
Servidor:  UnKnown
Address:  192.168.56.101

Respuesta no autoritativa:
Nombre:   mail.lapaloma.com
Address:  192.168.56.104
```

En ambas consultas, se puede apreciar como el servidor es el 192.168.56.101. Con todo esto, se habrá realizado todo correctamente.

Bibliografía

- [fpgenre](#)
- [gestal](#)
- [ucam](#)
- [digitalocean](#)
- [fpgenre](#)
- [martinber](#)
- [servidordebian](#)
- [sergio-gonzalez](#)