1. Instalación de servidor DNS

Bind es el estándar de facto para servidores DNS. Es una herramienta de software libre y se distribuye con la mayoría de plataformas Unix y Linux, donde también se le conoce con el sobrenombre de named (*name daemon*). Bind9 es la versión recomendada para usarse.

Puedes ejecutar BIND en un único servidor, pero se recomienda utilizar varios servidores para configurar el Servidor DNS de Alta Disponibilidad

Empezaremos actualizando los repositorios y los paquetes.

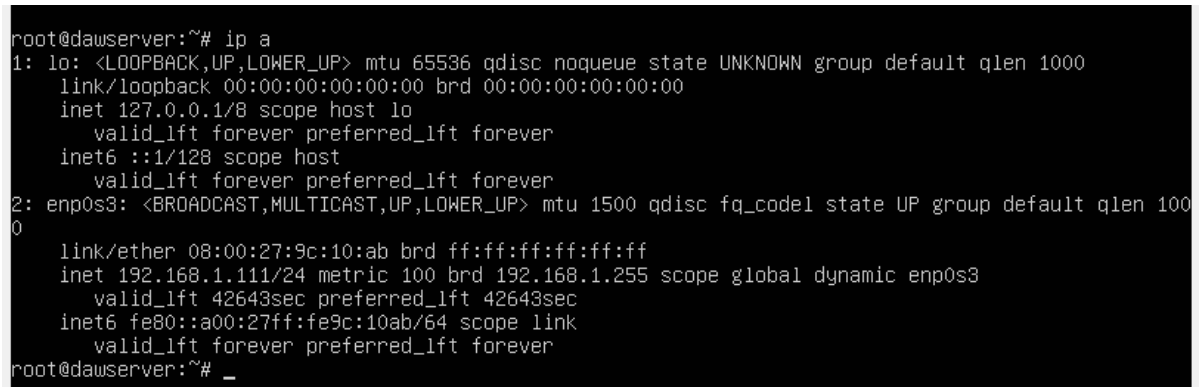
```
sudo apt-get update
```

Luego instalamos los paquetes actualizados.

```
sudo apt-get upgrade
```

Antes de empezar a instalar los paquetes BIND, vamos a comprobar qué dirección IP tenemos asignada a través del comando:

```
ip a
```



(*la dirección IP variará según la red en la que estemos conectado*)

Tenemos que darle una configuración de IP estática. La configuración de red se realiza a través de Netplan, que se encuentra dentro del directorio /etc. Para ello, vamos a acceder al archivo 00-installer-config.yaml para configurar la red del equipo.

El comando que vamos a utilizar es:

```
sudo nano /etc/netplan/00-installer-config.yaml
```

Su contenido inicial puede ser similar al siguiente:

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: true
  version: 2
```

Cuando entremos en el archivo lo modificaremos de la misma forma que veis en la imagen siguiente:

```
 GNU nano 6.2                          00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: false
      addresses:
      - 192.168.1.100/24
      routes:
        - to: default
          via: 192.168.1.1
      nameservers:
        addresses:
          - 192.168.1.100
  version: 2
```

Ahora aplicamos el cambio en la red con el comando:

```
sudo netplan apply
```

También debes asegurarte de que el nombre de host y el FQDN de tu servidor es correcto. En caso de utilizar dos servidores Ubuntu (*la dirección IP variará según la red en la que estemos conectado*):

```
Hostname     IP Address       FQDN                    Used        As
-------------------------------------------------------------
ns1          192.168.1.100    ns1.daw.es              BIND Master

ns2          192.168.1.110    ns2.daw.es              BIND Slave
```

Ejecuta el siguiente comando para configurar el FQDN (Nombre de Dominio Completamente Cualificado).

Configura el FQDN en el servidor “**ns1**”

```
sudo hostnamectl set-hostname ns1.daw.es
```

A continuación, edita el archivo */etc/hosts* utilizando el siguiente comando.

```
sudo nano /etc/hosts
```

Añade la siguiente configuración a cada servidor.

```
192.168.1.100  ns1.deaw.es    ns1
192.168.1.110  ns2.deaw.es    ns2
```

Puedes comprobar y verificar el FQDN en cada servidor utilizando el siguiente comando. En el servidor "**ns1**" obtendrás el FQDN como **ns1.deaw.es**.

```
sudo hostname -f
```

Para instalar el servidor DNS en Ubuntu Server, usaremos los repositorios oficiales. Por ello, podremos instalarlo como cualquier paquete en Ubuntu:

```
sudo apt install bind9 bind9utils bind9-doc dnsutils
```

```
root@ns1:~#
root@ns1:~# sudo apt install bind9 bind9utils bind9-doc dnsutils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bind9-utils dns-root-data
Suggested packages:
  bind-doc resolvconf
The following NEW packages will be installed:
  bind9 bind9-doc bind9-utils bind9utils dns-root-data dnsutils
0 upgraded, 6 newly installed, 0 to remove and 0 not upgraded.
Need to get 3,540 kB of archives.
After this operation, 7,739 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 https://mirrors.edge.kernel.org/ubuntu jammy-updates/main amd64 bind9-utils am
Get:2 https://mirrors.edge.kernel.org/ubuntu jammy/main amd64 dns-root-data all 2021
```

Una vez terminado podemos comprobar si el servicio está funcionando correctamente:

```
root@dawserver:~# service bind9 status
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-09-27 19:52:41 UTC; 39s ago
       Docs: man:named(8)
    Process: 15034 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 15035 (named)
      Tasks: 10 (limit: 4558)
     Memory: 8.3M
        CPU: 147ms
     CGroup: /system.slice/named.service
             └─15035 /usr/sbin/named -u bind
```

Añadimos una regla en el firewall ufw para permitir el servicio Bind9

```
root@dawserver:/# ufw app list
Available applications:
  Bind9
  OpenSSH
root@dawserver:/# ufw allow OpenSSH
Rules updated
Rules updated (v6)
root@dawserver:/# ufw allow Bind9
Rules updated
Rules updated (v6)
root@dawserver:/# ufw enable
Firewall is active and enabled on system startup
root@dawserver:/# _
```

2. Configuración del servidor

Puesto que sólo vamos a utilizar IPv4, debemos decírselo a Bind, en su archivo general de configuración. El archivo named.conf es el archivo de configuración predeterminado para el **daemon named.** Este archivo named se encuentra en el directorio `/etc/default`

Edita la configuración /etc/default/named

```
sudo nano /etc/default/named
```

La línea «OPTIONS=» te permite configurar opciones específicas cuando se ejecuta el servicio BIND. Y para indicarle que sólo use IPv4, debemos modificar la línea siguiente con el texto resaltado:

```
OPTIONS="-u bind -4"
```

```
. . .
OPTIONS="-u bind -4"
```

Guarda y cierra el archivo cuando hayas terminado.

Ahora ejecuta el siguiente comando para reiniciar el servicio Bind *named*. A continuación, comprueba y verifica el estado del servicio BIND. Deberías ver que el servicio Bind «*named*» se está ejecutando en ambos servidores.

```
sudo systemctl restart named
sudo systemctl status named
```

```
root@ns1:~#
root@ns1:~# sudo nano /etc/default/named
root@ns1:~#
root@ns1:~# sudo systemctl restart named
root@ns1:~# sudo systemctl status named
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2022-07-08 02:08:06 UTC; 4s ago
       Docs: man:named(8)
    Process: 2500 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 2501 (named)
      Tasks: 4 (limit: 2241)
     Memory: 5.4M
        CPU: 46ms
     CGroup: /system.slice/named.service
             └─2501 /usr/sbin/named -u bind -4
```

Una vez instalado Bind9 se habrán creado unos archivos dentro de la carpeta /etc/bind

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

named.conf	Este archivo sirve para agrupar a los archivos de configuración que usaremos. Estos 3 includes hacen referencia a los 3 diferentes archivos donde deberemos realizar la verdadera configuración, ubicados en el mismo directorio.
named.conf.local	Archivo principal donde tendremos que crear las nuevas zonas del DNS y opciones del servidor.
named.conf.options	Almacena sentencias para permitir la transferencia de zona (*allow-transfer*). La zona de reenviadores donde agregaremos otros servidores DNS
named.conf.default-zones	Almacena las zonas
db.localhost	Es el archivo principal donde se realizan las peticiones y resolución de direcciones IP por nombres de dominio.
db.127	Es el archivo donde se resuelven las direcciones de zona inversa de mi red local.
db.local	Es el archivo donde se resuelven las direcciones de zona directa de mi red local.

Si consultamos el archivo de configuración `named.conf` veremos lo siguiente:

```
// 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";
```

Configuración named.conf.options

Es una buena práctica que hagáis siempre una copia de seguridad de un archivo de configuración cada vez que vayáis a realizar algún cambio:

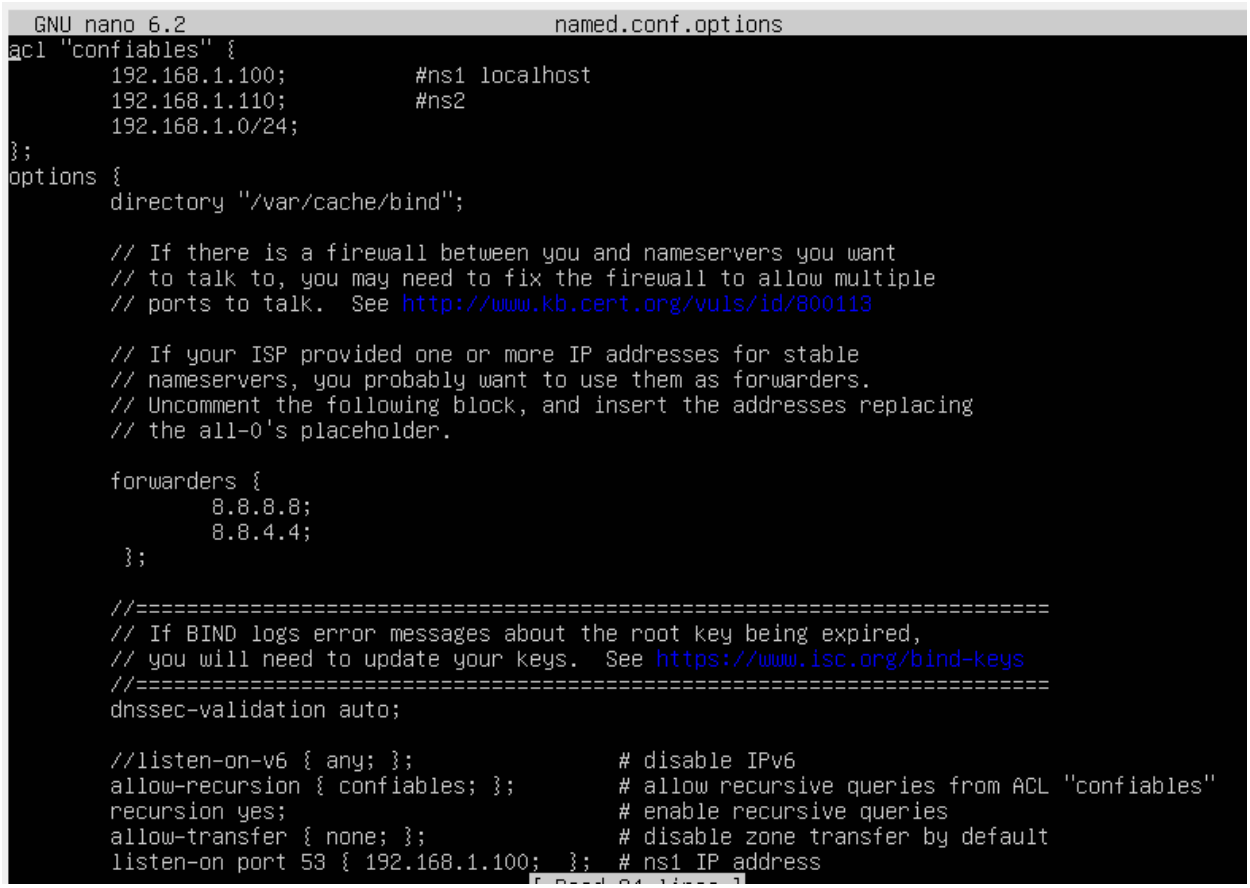
```
sudo cp /etc/bind/named.conf.options /etc/bind/named.conf.options.backup
```

Por motivos de seguridad, vamos a incluir una lista de acceso para que sólo puedan hacer consultas recursivas al servidor aquellos hosts que nosotros decidamos. Por tanto, estarás creando una ACL (Lista de Control de Acceso) con el nombre "**confiables**", que incluye todas las direcciones IP y redes de confianza de tu entorno. Asegúrate también de añadir la dirección IP del servidor local ns1

Ejecuta el siguiente comando para editar el archivo de configuración */etc/bind/named.conf.options*

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

- Los hosts confiables serán los de la red 192.168.X.0/24 (donde la X depende de vuestra red). Así pues, justo antes del bloque `options {…}`, al principio del archivo, añadiremos la lista de control de acceso ACL "confiables"
- Si nos fijamos el servidor por defecto ya viene configurado para ser un DNS caché. El directorio donde se cachearán o guardarán las zonas es `/var/cache/bind`.
- Vamos a deshabilitar el soporte para IPv6 comentando la opción "*listen-on-v6"*. Para comentarla basta añadir al principio de la línea dos barras `//`
- Habilitar y permitir la recursión desde la ACL "**confiables"**, es decir, que sólo se permitan las consultas recursivas a los hosts que hemos decidido en la lista de acceso anterior.
- Permitir las consultas recursivas, ya que en el punto anterior ya le hemos dicho que sólo puedan hacerlas los hosts de la ACL
- Desactivar la transferencia de zona por defecto. No permitir transferencia de zonas a nadie
- Ejecutar el servicio BIND en la dirección IP específica *ns1*. Configurar el servidor para que escuche consultas DNS en el puerto 53 (por defecto DNS utiliza puerto 53 UDP) y en la IP de su interfaz de la red privada. **Deberéis colocar la IP de la interfaz de vuestra Ubuntu**, puesto que resolverá las consultas DNS del cliente/s de esa red.
- Los reenviadores contienen las direcciones IP de DNS servidores a los que se redirige la solicitud si nuestro servidor no contiene los datos requeridos. Define los reenviadores específicos para el servidor DNS BIND a Google Public DNS *8.8.8.8* y *8.8.4.4*



Guarda y cierra el archivo cuando hayas terminado.

Por último, ejecuta el siguiente comando para comprobar y verificar el archivo de configuración «*/etc/bind/named.conf.options*«. Si no aparece ningún mensaje de salida, entonces tu configuración es correcta.

```
sudo named-checkconf /etc/bind/named.conf.options
```

Si hay algún error, nos lo hará saber. En caso contrario, nos devuelve a la línea de comandos.

Reiniciamos el servidor y comprobamos su estado

```
sudo systemctl restart named
sudo systemctl status named
```

3. Configurar zonas

Después de establecer la configuración básica del maestro BIND, ahora vamos a configurar las zonas para tu nombre de dominio.

Para ello, editaremos el archivo named.conf.local. Pero primero sería conveniente hacer una copia

```
sudo cp /etc/bind/named.conf.local /etc/bind/named.conf.local.backup
```

En este archivo configuraremos aspectos relativos a nuestras zonas. Vamos a declarar la zona “deaw.es”. Por ahora simplemente indicaremos que el servidor DNS es maestro para esta zona y donde estará ubicado el archivo de zona que crearemos más adelante:

Edita el archivo de configuración utilizando el siguiente comando:

```
sudo nano /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 "deaw.es" {
        type master;
        file "/etc/bind/db.deaw.es"; //Ruta donde ubicamos nuestro archivo de zona
};
```

Vamos a crear el archivo de zona de resolución directa con el mismo nombre que hemos indicado antes (/etc/bind/db.deaw.es). En esta configuración, definirás dos archivos de zona, la zona directa y la zona inversa para tu nombre de dominio. La zona directa contendrá la configuración de dónde se resolverán tus nombres de dominio a la dirección IP, mientras que la zona inversa traducirá la dirección IP a qué nombre de dominio.

Podemos copiar la base de datos que tenemos en «db.local» darle el nombre de «**db.deaw.es**» que hemos definido en el fichero anterior.

```
sudo cp /etc/bind/db.local /etc/bind/db.deaw.es
sudo nano /etc/bind/db.deaw.es
```

Recordad de teoría que los registros SOA son para detallar aspectos de la zona autoritativa, los NS para indicar los servidores DNS de la zona y los A las IPs respectivas.

Inicialmente, tendrá un aspecto similar al siguiente:

```
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.      ; delete this line
@       IN      A       127.0.0.1       ; delete this line
@       IN      AAAA    ::1             ; delete this line
```

En la línea que comienza por @, el registro SOA o «*Start of Authority*«, indicamos cuál es el servidor de nombres del dominio y la dirección de correo electrónico del administrador, especificada sin el carácter @, es decir, *admin@deaw.es* se indica como *admin.deaw.es*.

Serial: Es un número que se incrementa cada vez que se modifica un fichero de una zona, de forma que Bind se dé cuenta de que tiene que recargar esta zona.

Debéis poner vuestras IPs privadas correspondientes de vuestro servidor.

El contenido será algo así (procurad respetar el formato):

```
  GNU nano 6.2                                    db.deaw.es
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns1.deaw.es. admin.deaw.es. (
                              3         ; Serial
                         604800         ; Refresh (7 dias)
                          86400         ; Retry (1 dia)
                        2419200         ; Expire (28 dias)
                         604800 )       ; Negative Cache TTL (7 dias)
;
        IN      NS      ns1.deaw.es.    ; definimos el servidor de nombres
        IN      NS      ns2.deaw.es.    ;

ns1.deaw.es.    IN      A       192.168.1.100   ; definimos la IP para el DNS
ns2.deaw.es.    IN      A       192.168.1.110
deaw.es.        IN      A       192.168.1.100
```

Creación del archivo de zona para la resolución inversa

Recordad que deben existir ambos archivos de zona, uno para la resolución directa y otro para la inversa. Vamos pues a crear el archivo de zona inversa.

En primer lugar, debemos añadir las líneas correspondientes a esta zona inversa en el archivo **`named.conf.local`**, igual que hemos hecho antes con la zona de resolución directa:

```
// organization
//include "/etc/bind/zones.rfc1918";

zone "deaw.es" {
        type master;
        file "/etc/bind/db.deaw.es"; //Ruta donde ubicamos nuestro archivo de zona
};

zone "X.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.X.168.192"; //Ruta donde ubicamos nuestro archivo de zona
};
```

Donde la X es el tercer byte de vuestra red.

A continuación, copia el archivo de configuración de la zona inversa por defecto en «*/etc/bind/db.1.168.192*» y edita el nuevo archivo utilizando el siguiente comando.

```
sudo cp /etc/bind/db.127 /etc/bind/db.1.168.192
sudo nano /etc/bind/db.1.168.192
```

Inicialmente, tendrá un aspecto similar al siguiente:

```
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.      ; delete this line
1.0.0   IN      PTR     localhost.      ; delete this line
```

Cambia el registro SOA por defecto utilizando tu nombre de dominio. Además, no olvides cambiar el número de «**Serie**» dentro del registro SOA.

Define registros NS para tus servidores DNS. Son los mismos servidores de nombres que utilizaste en la zona de reenvío.

Y la configuración de la zona de resolución inversa:

```
  GNU nano 6.2                                  db.1.168.192
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns1.deaw.es. admin.deaw.es. (
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns1.deaw.es.
IN      NS      ns2.deaw.es.

100     IN      PTR     ns1.deaw.es.    ; 192.168.1.100
110     IN      PTR     ns2.deaw.es.    ; 192.168.1.110
```

Comprobación de las configuraciones

Para comprobar la sintaxis de los archivos name.conf

```
sudo named-checkconf named.conf.local
```

Para comprobar la configuración de la zona de resolución directa:

```
sudo named-checkzone db.deaw.es db.1.168.192
```

Y para comprobar la configuración de la zona de resolución inversa:

```
sudo named-checkzone db.1.168.192 db.deaw.es
```

```
root@dawserver:/etc/bind# named-checkconf named.conf.local
root@dawserver:/etc/bind# named-checkzone db.deaw.es db.1.168.192
zone db.deaw.es/IN: loaded serial 3
OK
root@dawserver:/etc/bind# named-checkzone db.1.168.192 db.deaw.es
db.deaw.es:15: ignoring out-of-zone data (ns1.deaw.es)
db.deaw.es:16: ignoring out-of-zone data (ns2.deaw.es)
zone db.1.168.192/IN: loaded serial 3
OK
root@dawserver:/etc/bind#
```

Si todo está bien, devolverá OK. En caso de haber algún error, nos informará de ello.

Reiniciamos el servicio y comprobamos el estado

4. Comprobación de las resoluciones y de las consultas

Podemos comprobar desde los clientes, con **dig** o **nslookup** las resoluciones directas e inversas:

```
root@dawserver:/etc# dig deaw.es

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> deaw.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13828
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: f5784b0bb67e3ce0010000006519b18e5ac37f3acbcb1821 (good)
;; QUESTION SECTION:
;deaw.es.                       IN      A

;; AUTHORITY SECTION:
deaw.es.                604800  IN      SOA     ns1.deaw.es. admin.deaw.es. 3 604800 86400 2419200 6
04800

;; Query time: 0 msec
;; SERVER: 192.168.1.100#53(192.168.1.100) (UDP)
;; WHEN: Sun Oct 01 17:51:10 UTC 2023
;; MSG SIZE  rcvd: 110

root@dawserver:/etc#
```

```
root@dawserver:/etc# dig -x 192.168.1.100

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> -x 192.168.1.100
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 64528
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 920ab607ad0a128b010000006519b1f3d392a57494e5df2c (good)
;; QUESTION SECTION:
;100.1.168.192.in-addr.arpa.    IN      PTR

;; AUTHORITY SECTION:
168.192.IN-ADDR.ARPA.   86400   IN      SOA     168.192.IN-ADDR.ARPA. . 0 28800 7200 604800 86400

;; Query time: 0 msec
;; SERVER: 192.168.1.100#53(192.168.1.100) (UDP)
;; WHEN: Sun Oct 01 17:52:51 UTC 2023
;; MSG SIZE  rcvd: 138

root@dawserver:/etc# _
```

```
root@dawserver:/etc# nslookup ns1.deaw.es
Server:         192.168.1.100
Address:        192.168.1.100#53

Name:   ns1.deaw.es
Address: 192.168.1.100

root@dawserver:/etc#
```

```
root@dawserver:/etc/bind# nslookup 192.168.1.100
100.1.168.192.in-addr.arpa      name = ns1.deaw.es.

root@dawserver:/etc/bind# _
```