
ÍNDICE – U04 – A 01

1. *Configuración de DNS.*
2. *Configuración de DNS Master.*
3. *Configuración de zona inversa.*

1.- Configuración de DNS.

- Instalamos el servidor bind.

```
miadmin@igcdaw:/$ sudo apt-get install bind9
```

```
miadmin@igcdaw:/$ ls /etc/bind/  
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
```

- Para controlar los errores usamos sudo nano /var/log/syslog o sudo cat /var/log/syslog.

```
miadmin@igcdaw:/$ sudo nano /var/log/syslog
```

- Cambiamos la configuración de DNS y el search para que la máquina actúe con su propio DNS, vamos al archivo de conexión con el comando sudo nano /etc/netplan/50-cloud-init.yaml.

```
network:  
  ethernets:  
    enp0s3:  
      addresses:  
        - 192.168.1.140/24  
      dhcp4: false  
      gateway4: 192.168.1.1  
      nameservers:  
        addresses:  
          - 192.168.20.20  
          - 1.1.1.1_  
      search:  
        - sauces.local  
  
version: 2
```

```
network:  
  ethernets:  
    enp0s3:  
      addresses:  
        - 192.168.1.140/24  
      dhcp4: false  
      gateway4: 192.168.1.1  
      nameservers:  
        addresses:  
          - 192.168.1.140_  
      search:  
        - sauces.local  
  
version: 2
```

- Usamos el comando netplan apply para aplicar la nueva configuración.

```
miadmin@igcdaw:/$ sudo netplan apply
```

- Con `systemd-resolve --status` listamos los DNS del servidor.

```
miadmin@igcdaw:/$ systemd-resolve --status
```

```
Global
    DNSSEC NTA: 10.in-addr.arpa
                16.172.in-addr.arpa
                168.192.in-addr.arpa
                17.172.in-addr.arpa
                18.172.in-addr.arpa
                19.172.in-addr.arpa
                20.172.in-addr.arpa
                21.172.in-addr.arpa
                22.172.in-addr.arpa
                23.172.in-addr.arpa
                24.172.in-addr.arpa
                25.172.in-addr.arpa
                26.172.in-addr.arpa
                27.172.in-addr.arpa
                28.172.in-addr.arpa
                29.172.in-addr.arpa
                30.172.in-addr.arpa
                31.172.in-addr.arpa
                corp
                d.f.ip6.arpa
                home
                internal
                intranet
                lan
                local
                private
                test

Link 2 (enp0s3)
    Current Scopes: DNS
    LLMNR setting: yes
    MulticastDNS setting: no
    DNSSEC setting: no
    DNSSEC supported: no
    DNS Servers: 192.168.1.140
lines 1-36_
```

- Editamos el archivo `/etc/default/bind9` de la siguiente forma.

```
miadmin@igcdaw:/$ sudo nano /etc/default/bind9
```

```
GNU nano 2.9.3

#
# run resolvconf?
RESOLVCONF=no

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

```
GNU nano 2.9.3
#
# run resolvconf?
RESOLVCONF=yes_
#
# startup options for the server
OPTIONS="-u bind"
```

- Editamos el archivo `/etc/bind/named.conf.options` de la siguiente forma.

```
miadmin@igcdaw:/$ sudo nano /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
    //=====
    dnssec-validation auto;

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

```
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 {
        1.1.1.1;
    };

    //=====
    // 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; };
};
```

- Reiniciamos el servicio de bind9.

```
miadmin@igcdaw:/$ sudo service bind9 restart
miadmin@igcdaw:/$ host cristianoronaldo.com
cristianoronaldo.com has address 34.255.174.49
miadmin@igcdaw:/$ dig cristianoronaldo.com

; <>> DiG 9.11.3-1ubuntu1.3-Ubuntu <>> cristianoronaldo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39960
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;cristianoronaldo.com.      IN      A

;; ANSWER SECTION:
cristianoronaldo.com.      277     IN      A      34.255.174.49

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Feb 18 12:22:33 UTC 2019
;; MSG SIZE rcvd: 65
```

2.- Configuración de DNS Master.

- Configuramos la zona para nuestro DNS entrando en el fichero name.conf.local con el comando `sudo nano /etc/named.conf.local` de la siguiente forma.

```
miadmin@igcdaw:/$ sudo nano /etc/named.conf.local
```

```
zone "israel.com" {
    type master;
    file "/etc/bind/db.israel.com";
};_
```

- Checkeamos el fichero con `named-checkconf /etc/bind/named.conf.local`.

```
miadmin@igcdaw:/$ named-checkconf /etc/bind/named.conf.local
```

- Copiamos el fichero db.local con el nombre db.israel.com.

```
miadmin@igcdaw:/etc/bind$ sudo cp db.local db.israel.com
```

- Editamos el nuevo fichero db.israel.com.

```
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      IGCUSED.israel.com.      israel.garcab@educa.jcyl.es. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )    ; Negative Cache TTL
;
@         IN      NS       IGCUSED.israel.com.
IGCUSED   IN      A        192.168.1.140
```

- Checkeamos el fichero db.israel.com, reiniciamos el servicio y probamos la resolución de nombres.

```
miadmin@igcdaw:/etc/bind$ named-checkzone israel.com db.israel.com
db.israel.com:5: warning: israel.garcab\@educa.jcyl.es: bad name (check-names)
zone israel.com/IN: loaded serial 2
OK
miadmin@igcdaw:/etc/bind$ service bind9 restart
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'bind9.service'.
Authenticating as: miadmin
Password:
==== AUTHENTICATION COMPLETE ====
```

- Editamos el fichero de nuevo añadiendo dos nuevas líneas.

```
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      IGCUSED.israel.com.      israel.garcab.educa.jcyl.es. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )    ; Negative Cache TTL
;
@         IN      NS       IGCUSED.israel.com.
@         IN      A        192.168.1.140
IGCUSED   IN      A        192.168.1.140
www       IN      CNAME     IGCUSED.israel.com.
```

- Hacemos reboot a la máquina y comprobamos que resuelve las direcciones correctamente.

```
miadmin@igcdaw:~$ host www.israel.com
www.israel.com has address 104.27.191.49
www.israel.com has address 104.27.190.49
www.israel.com has IPv6 address 2606:4700:30::681b:bf31
www.israel.com has IPv6 address 2606:4700:30::681b:be31
```

3.- Configuración de zona inversa.

- Vamos al directorio bind y copiamos el fichero de la zona directa con el siguiente nombre y lo editamos a de la siguiente forma.

```
miadmin@igcdaw:~$ cd /etc/bind/
miadmin@igcdaw:/etc/bind$ sudo cp db.israel.com db.1.168.192.in-addr.arpa
[sudo] password for miadmin:
```

```
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      IGCUSED.israel.com.    israel.garcab.educa.jcyl.es. (
                                2                  ; Serial
                                604800               ; Refresh
                                86400                ; Retry
                                2419200              ; Expire
                                604800 )            ; Negative Cache TTL
;
@         IN      NS       IGCUSED.israel.com.
103       IN      PTR      israel.com.
103       IN      PTR      IGCUSED.israel.com.
```

- Checkeamos el fichero.

```
miadmin@igcdaw:/etc/bind$ named-checkzone 1.168.192.in-addr.arpa /etc/bind/db.1.168.192.in-addr.arpa
zone 1.168.192.in-addr.arpa/IN: loaded serial 2
OK
```

- Editamos el fichero named.conf.local.

```
miadmin@igcdaw:/etc/bind$ ls
bind.keys          db.127            db.israel.com     named.conf         named.conf.options
db.0               db.255           db.local          named.conf.default-zones  rndc.key
db.1.168.192.in-addr.arpa  db.empty         db.root          named.conf.local    zones.rfc1918
```

```
//
// 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 "israel.com" {
    type master;
    file "/etc/bind/db.israel.com";
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.1.168.192.in-addr.arpa";
};
```

- Checkeamos el fichero con el comando `named-checkconf /etc/bind/named.conf.local` y probamos preguntando por la IP con el `nslookup`.

```
miadmin@igcdaw:/etc/bind$ named-checkconf /etc/bind/named.conf.local
```

```
miadmin@igcdaw:/etc/bind$ nslookup
> server 192.168.1.140
Default server: 192.168.1.140
Address: 192.168.1.140#53
```