fase 1, configuración de la red de linux server

poner una ip estatica

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.1.5/24
      routes:
        - to: default
          via: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

comprobacion desde otro equipo

```
:\Users\oscar>ping 192.168.1.5

laciendo ping a 192.168.1.5 con 32 bytes de datos:
espuesta desde 192.168.1.5: bytes=32 tiempo=17ms TTL=64
espuesta desde 192.168.1.5: bytes=32 tiempo=119ms TTL=64
espuesta desde 192.168.1.5: bytes=32 tiempo=20ms TTL=64
espuesta desde 192.168.1.5: bytes=32 tiempo=26ms TTL=64

stadísticas de ping para 192.168.1.5:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
iempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 17ms, Máximo = 119ms, Media = 45ms

C:\Users\oscar>
```

fase 2, implementación de un servidor dhcp y dns

configurar un servidor DHCP, primero se instal y luego se configura

```
Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
oscar@srv-base-oscarhernandez:~$
```

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.10 192.168.1.50;
  option routers 192.168.1.1;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.1.255;
  option domain-name-servers 8.8.8.8, 8.8.4.4;
}
```

comprobamos el estado

```
oscar@srv-base-oscarhernandez:~$ sudo systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPv4 server
     Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; enabled;
     Active: active (running) since Tue 2025-06-24 19:37:10 CEST; 39s ago
       Docs: man:dhcpd(8)
   Main PID: 2801 (dhcpd)
      Tasks: 1 (limit: 2267)
     Memory: 3.7M (peak: 3.9M)
        CPU: 52ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─2801 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/

jun 24 19:37:10 srv-base-oscarhernandez dhcpd[2801]: PID file: /run/dhcp-serve
jun 24 19:37:10 srv-base-oscarhernandez sh[2801]: Wrote 0 leases to leases fil
jun 24 19:37:10 srv-base-oscarhernandez dhcpd[2801]: Wrote 0 leases to leases
jun 24 19:37:10 srv-base-oscarhernandez dhcpd[2801]: Listening on LPF/enp0s3/0
jun 24 19:37:10 srv-base-oscarhernandez sh[2801]: Listening on LPF/enp0s3/08:0
jun 24 19:37:10 srv-base-oscarhernandez sh[2801]: Sending on   LPF/enp0s3/08:0
jun 24 19:37:10 srv-base-oscarhernandez sh[2801]: Sending on   Socket/fallback
jun 24 19:37:10 srv-base-oscarhernandez dhcpd[2801]: Sending on   LPF/enp0s3/0
jun 24 19:37:10 srv-base-oscarhernandez dhcpd[2801]: Sending on   Socket/fallb
jun 24 19:37:10 srv-base-oscarhernandez dhcpd[2801]: Server starting service.
```

instalar un servicio de DNS, después de instar configuramos el archivo para que pueda resolver las consultas de los clientes

```
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-ke
        //========================================================================
        #dnssec-validation auto;
        dnssec-validation no;
        listen-on-v6 { any; };
};
```

configuramos el archivo para zonas de búsqueda directa e inversas

```
//
// Do any local configuration here
//

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

//zona de resolucion directa
zone "serv-vase-oscarhernandez" {
        type master;
        file "/etc/bind/zones/db.srv-vase-oscarhernandez";
};

//zona de resolucion inversa
zone "1.168.192.in.arpa" {
        type master;
        file "/etc/bind/zones/db.1.168.192";
};
```

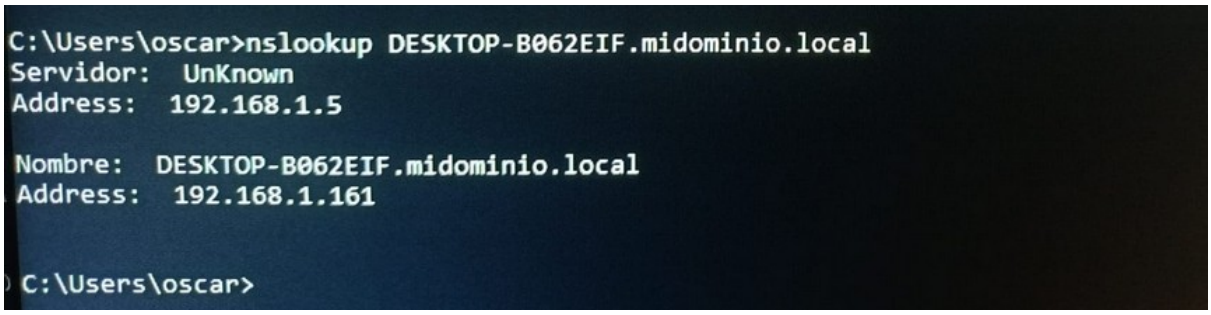
y creamos las zonas

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     srv-base-oscarhernandez. admin.midominio.local. (
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      srv-base-oscarhernandez.
srv-base-oscarhernandez.        IN      A       192.168.1.5
DESKTOP-B062EIF IN      A       192.168.1.161
```

```
;
; BIND data file para la resolucion directa
;
$TTL    604800
@       IN      SOA     oscar.srv-vase-oscarhernandez. root.srv-vase-oscarhern
                         20220202               ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@               IN      NS      oscar.srv-vase-oscarhernandez.
oscar.          IN      A       192.168.1.5
cliente-dns     IN      A       192.168.1.161
server          IN      CNAME   oscar.srv-vase-oscarhernandez.
```

he tenido varios problemas por culpa del nombre del host del equipo donde he realizado la prueba, así que en las zonas he tenido que hacer desde el principio y he

cambiado el nombre del dominio a midominio.local. después la prueba ha salido bien con el comando nslookup DESKTOP-B062EIF.midominio.local



fase 4, configuracion de firewall y seguridad

instalar ufw

```
oscar@srv-base-oscarhernandez:~$ sudo ufw enable
Firewall is active and enabled on system startup
oscar@srv-base-oscarhernandez:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

permitir trafico saliente

```
oscar@srv-base-oscarhernandez:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
oscar@srv-base-oscarhernandez:~$
```

denegar el trafico entrate por defecto

```
oscar@srv-base-oscarhernandez:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
oscar@srv-base-oscarhernandez:~$
```

permitir dn desde laip autorizada

```
oscar@srv-base-oscarhernandez:~$ sudo ufw allow from 192.168.1.161 to any port 53 proto tcp
Rule added
oscar@srv-base-oscarhernandez:~$ sudo ufw allow from 192.168.1.161 to any port 53 proto udp
Rule added
```

permitir ssh desde la mis ip

```
Rule added
oscar@srv-base-oscarhernandez:~$ sudo ufw allow from 192.168.1.161 to any port 22  proto tcp
Rule added
oscar@srv-base-oscarhernandez:~$ _
```

implementar reglas de seguridad para evitar ataques de red

bloquea todo el trafico entrante y permite solo que explicitamente autorice

```
oscar@srv-base-oscarhernandez:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
oscar@srv-base-oscarhernandez:~$
```

bloquear intentos de conexión no deseados

```
oscar@srv-base-oscarhernandez:~$ sudo ufw deny 23
Rule added
Rule added (v6)
oscar@srv-base-oscarhernandez:~$ sudo ufw deny 445
Rule added
Rule added (v6)
oscar@srv-base-oscarhernandez:~$ sudo ufw deny 139
Rule added
Rule added (v6)
oscar@srv-base-oscarhernandez:~$ sudo ufw deny 3389
çRule added
Rule added (v6)
oscar@srv-base-oscarhernandez:~$
```

limitar intentos para evitar ataque de tipo fuerza bruta

```
oscar@srv-base-oscarhernandez:~$ sudo ufw limit ssh
Rule updated
Rule updated (v6)
oscar@srv-base-oscarhernandez:~$ _
```

bloquear una ip maliciosa

```
Rule updated (v6)
oscar@srv-base-oscarhernandez:~$ sudo ufw deny from 192.168.1.200
Rule added
oscar@srv-base-oscarhernandez:~$ _
```

permitir solo una subred especifica

```
Rule added
oscar@srv-base-oscarhernandez:~$ sudo ufw allow from 192.168.1.0/24
Rule added
oscar@srv-base-oscarhernandez:~$ _
```

ver reglas activas

```
oscar@srv-base-oscarhernandez:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     LIMIT IN    Anywhere
53/tcp                     ALLOW IN    192.168.1.161
53/udp                     ALLOW IN    192.168.1.161
22/tcp                     ALLOW IN    192.168.1.161
23                         DENY IN     Anywhere
445                        DENY IN     Anywhere
139                        DENY IN     Anywhere
3389                       DENY IN     Anywhere
Anywhere                   DENY IN     192.168.1.200
Anywhere                   ALLOW IN    192.168.1.0/24
22/tcp (v6)                LIMIT IN    Anywhere (v6)
23 (v6)                    DENY IN     Anywhere (v6)
445 (v6)                   DENY IN     Anywhere (v6)
139 (v6)                   DENY IN     Anywhere (v6)
3389 (v6)                  DENY IN     Anywhere (v6)

oscar@srv-base-oscarhernandez:~$
```