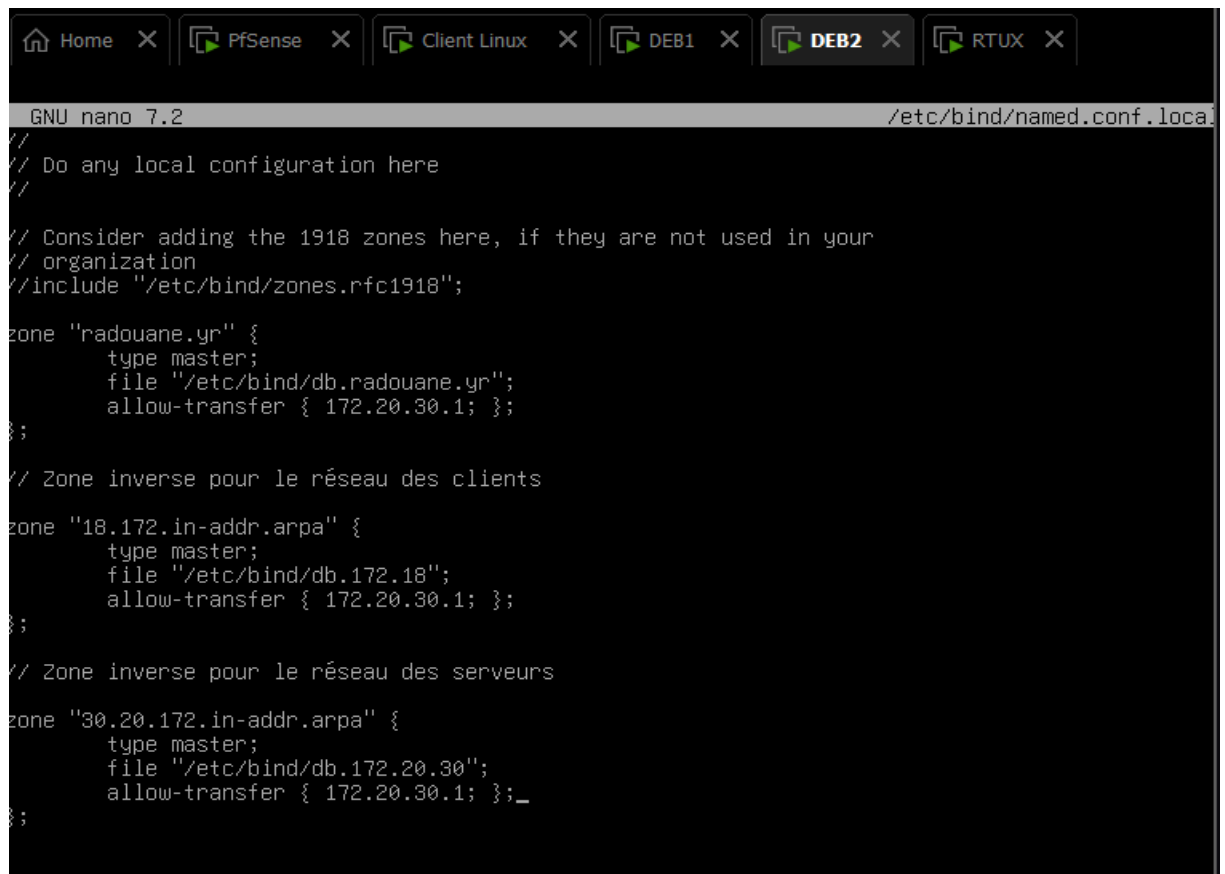


TP DNS DHCP

1.1 Configuration du DNS Primaire (SRV-DEB2)

1. Modification de /etc/bind/named.conf.local :

On ajoute la directive allow-transfer à chaque déclaration de zone en spécifiant l'IP de DEB1.



```
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";

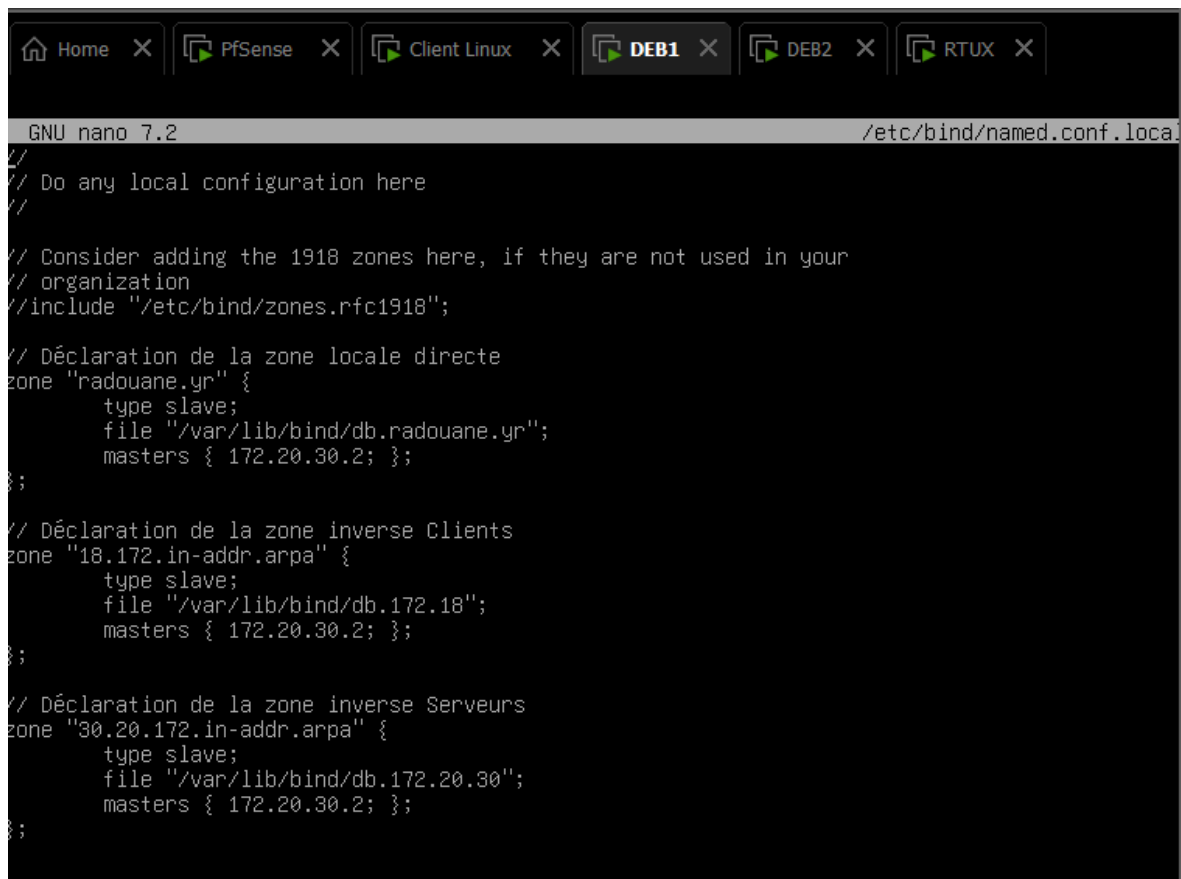
zone "radouane.yr" {
    type master;
    file "/etc/bind/db.radouane.yr";
    allow-transfer { 172.20.30.1; };
};

// Zone inverse pour le réseau des clients
zone "18.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.172.18";
    allow-transfer { 172.20.30.1; };
};

// Zone inverse pour le réseau des serveurs
zone "30.20.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.172.20.30";
    allow-transfer { 172.20.30.1; };
};
```

1.2 Configuration du DNS Secondaire (DEB1)

1. On installe bind9 sur la machine
2. On configure le named.conf.local en déclarant les mêmes zones mais en type slave et en indiquant l'IP de DEB2 qui est le serveur maître.



```
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";

// Déclaration de la zone locale directe
zone "radouane.gr" {
    type slave;
    file "/var/lib/bind/db.radouane.gr";
    masters { 172.20.30.2; };
};

// Déclaration de la zone inverse Clients
zone "18.172.in-addr.arpa" {
    type slave;
    file "/var/lib/bind/db.172.18";
    masters { 172.20.30.2; };
};

// Déclaration de la zone inverse Serveurs
zone "30.20.172.in-addr.arpa" {
    type slave;
    file "/var/lib/bind/db.172.20.30";
    masters { 172.20.30.2; };
};
```

1.3. Mise à jour du DHCP (DEB1)

1. Modification du dhcp.conf (ajout des deux IP DNS)

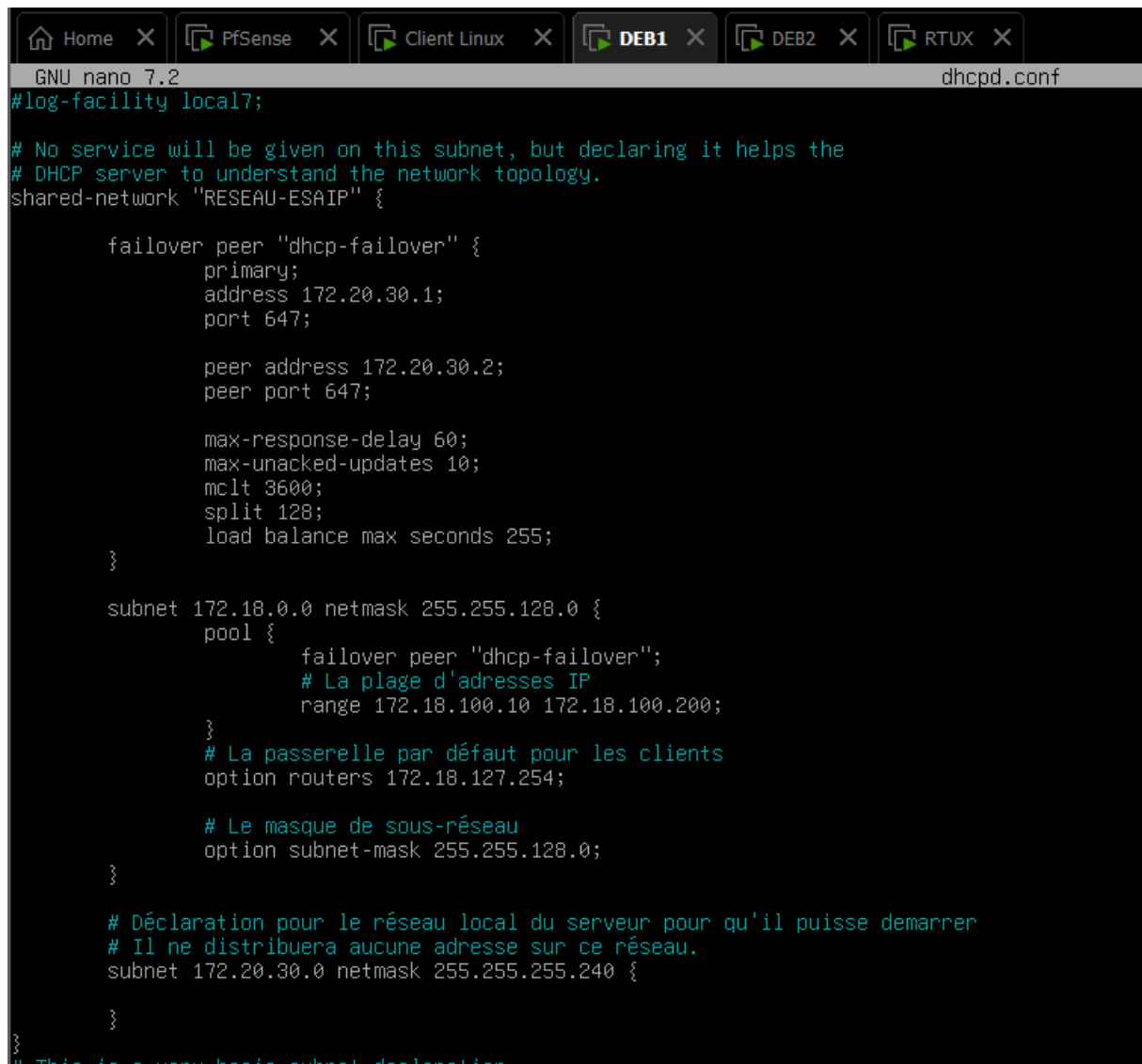
```
option domain-name "radouane.gr";
option domain-name-servers 172.20.30.2, 172.20.30.1, 1.1.1.1;
```

Partie 2 : DHCP Failover

2.1. Config du DHCP Primaire (DEB1)

1. Modification du dhcpd.conf :

On encapsule la config dans un shared-network (obligatoire pour le failover) puis on ajoute la déclaration failover peer en mode primary.



The screenshot shows a terminal window with a tabbed interface at the top. The tabs are labeled: Home, PfSense, Client Linux, DEB1, DEB2, and RTUX. The active tab is DEB1. The terminal is running GNU nano 7.2 and editing the file dhcpd.conf. The configuration includes a shared-network block for 'RESEAU-ESAIP' with a failover peer 'dhcp-failover' configured as primary on 172.20.30.1. It also defines a subnet 172.18.0.0/24 with a pool of addresses 172.18.100.10 to 172.18.100.200, a default router of 172.18.127.254, and a subnet mask of 255.255.128.0. A final subnet 172.20.30.0/24 is declared for the local server network.

```
GNU nano 7.2 dhcpd.conf
#log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.
shared-network "RESEAU-ESAIP" {

    failover peer "dhcp-failover" {
        primary;
        address 172.20.30.1;
        port 647;

        peer address 172.20.30.2;
        peer port 647;

        max-response-delay 60;
        max-unacked-updates 10;
        mclt 3600;
        split 128;
        load balance max seconds 255;
    }

    subnet 172.18.0.0 netmask 255.255.128.0 {
        pool {
            failover peer "dhcp-failover";
            # La plage d'adresses IP
            range 172.18.100.10 172.18.100.200;
        }
        # La passerelle par défaut pour les clients
        option routers 172.18.127.254;

        # Le masque de sous-réseau
        option subnet-mask 255.255.128.0;
    }

    # Déclaration pour le réseau local du serveur pour qu'il puisse démarrer
    # Il ne distribuera aucune adresse sur ce réseau.
    subnet 172.20.30.0 netmask 255.255.255.240 {

    }
}

# This is a very basic subnet declaration
```

2.2 Configuration du DHCP Secondaire (DEB2)

1. Installation de isc-dhcp-server

2. config du dhcpd.conf : on copie la config de deb1 en changeant primary par secondary et on retire « split » et « load balance » qui sont elles définis par le primary seulement.

```
GNU nano 7.2 dhcpd.conf
# network, the authoritative directive should be uncommented.
authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
#log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

shared-network "RESEAU-ESAIP" {
    failover peer "dhcp-failover" {
        secondary;
        address 172.20.30.2;
        port 647;

        peer address 172.20.30.1;
        peer port 647;

        max-response-delay 60;
        max-unacked-updates 10;
        mclt 3600;
    }

    subnet 172.18.0.0 netmask 255.255.128.0 {
        pool {
            failover peer "dhcp-failover";
            range 172.18.100.10 172.18.100.200;
        }
        option routers 172.18.127.254;
        option broadcast-address 172.18.127.255;
    }

    subnet 172.20.30.0 netmask 255.255.255.240 {
    }
}

host deb-clt {
    hardware ethernet 00:0c:29:4b:6c:b0;
    fixed-address 172.18.4.20;
    ddns-hostname "deb-clt";
}
```

Partie 3 : Mise a jour du relais et test de basculement

3.1 Config du RTUX :

1. Modification du /etc/default/dhcp-helper (le relais) : on ajoute les 2 IP

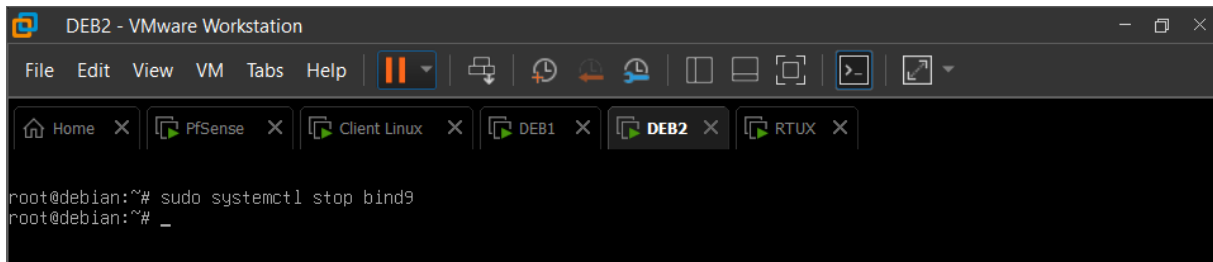
```
RTUX - VMware Workstation
GNU nano 7.2 dhcp-helper
# Option flags used to start dhcp-helper.
#
# You will need at least "-s <DHCP server>" or
# "-b <interface>" so that dhcp-helper knows where
# to relay DHCP requests.
#
# See "man 8 dhcp-helper" for more details.

DHCPHELPER_OPTS="-s 172.20.30.1 -s 172.20.30.2 -i ens37"
```

3.2. Test de basculement (Client)

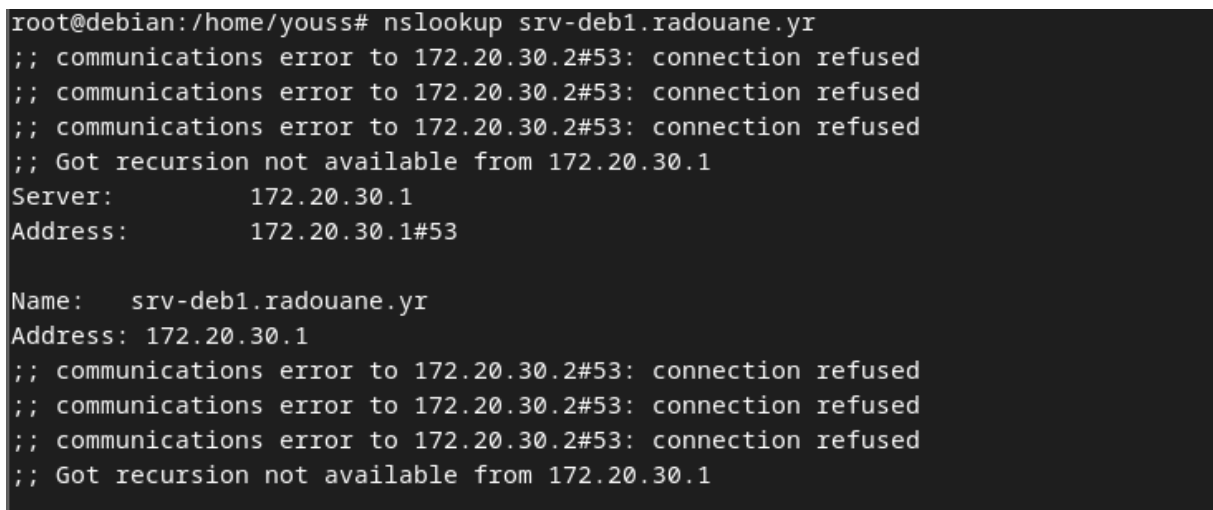
1. Test de Basculement DNS :

- Service Bind9 arrêté sur DEB2



```
DEB2 - VMware Workstation
File Edit View VM Tabs Help
root@debian:~# sudo systemctl stop bind9
root@debian:~# _
```

- Le client utilise nslookup et obtient toujours une réponse de DEB1

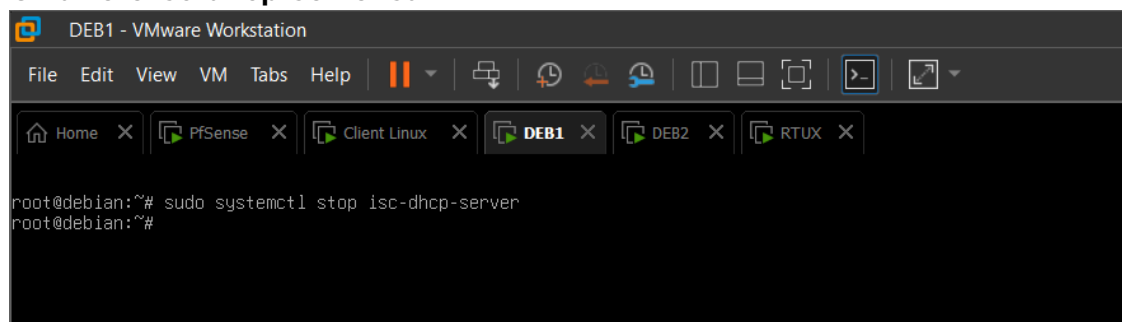


```
root@debian:/home/youss# nslookup srv-deb1.radouane.yr
;; communications error to 172.20.30.2#53: connection refused
;; communications error to 172.20.30.2#53: connection refused
;; communications error to 172.20.30.2#53: connection refused
;; Got recursion not available from 172.20.30.1
Server:          172.20.30.1
Address:         172.20.30.1#53

Name:   srv-deb1.radouane.yr
Address: 172.20.30.1
;; communications error to 172.20.30.2#53: connection refused
;; communications error to 172.20.30.2#53: connection refused
;; communications error to 172.20.30.2#53: connection refused
;; Got recursion not available from 172.20.30.1
```

2. Test de Basculement DHCP (Panne du DHCP Primaire)

- On rétablit d'abord Bind9 sur le DEB2
- On arrête isc-dhcp-server sur DEB1



```
DEB1 - VMware Workstation
File Edit View VM Tabs Help
root@debian:~# sudo systemctl stop isc-dhcp-server
root@debian:~#
```

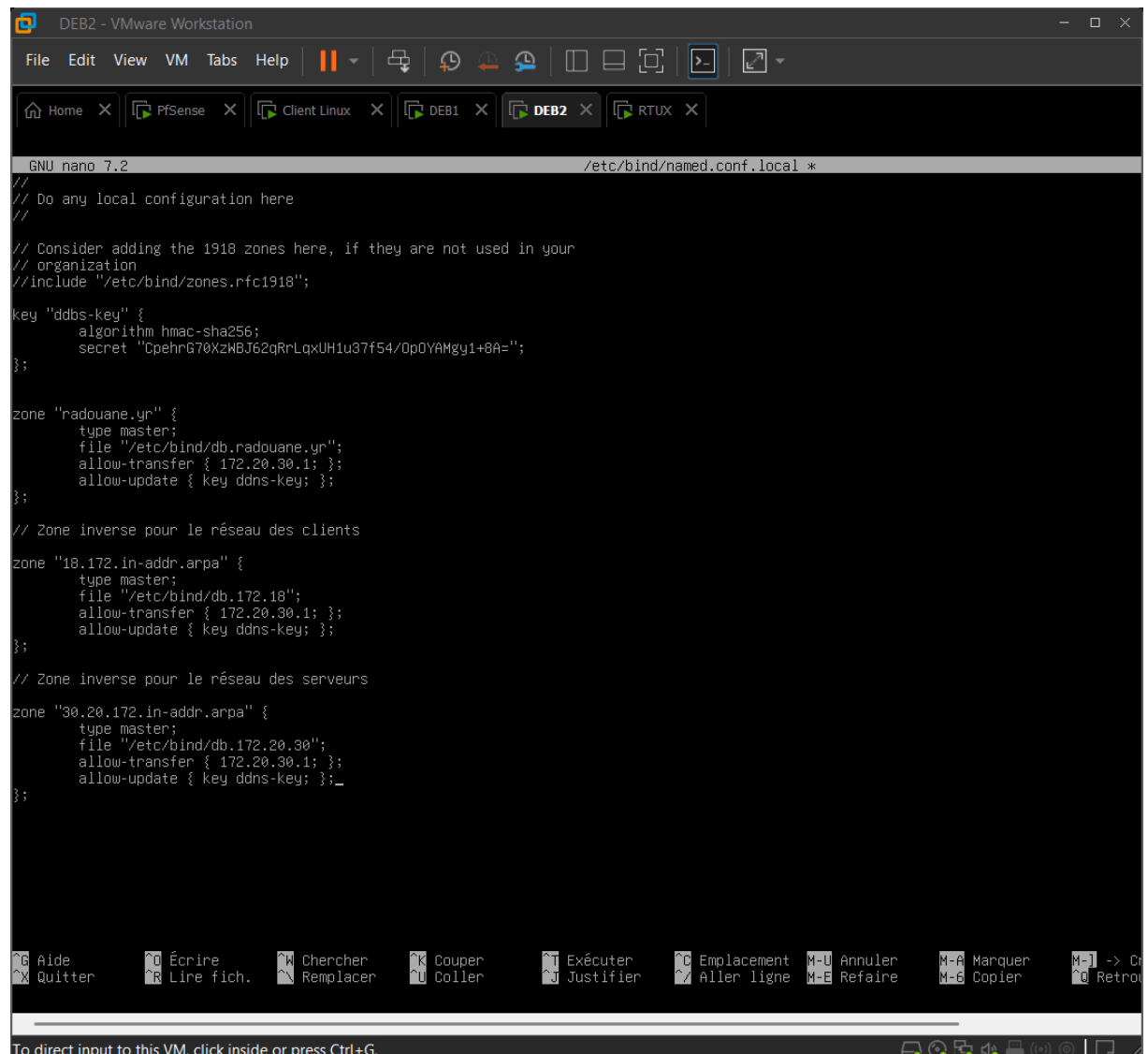
- On teste le basculement :
 - o On force une nouvelle demande avec `sudo dhclient -r` et `// -v`
 - o On vérifie qu'on a bien obtenu une adresse IP

```
root@debian:/home/youss# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:4b:6c:b0 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 172.18.4.20/17 brd 172.18.127.255 scope global dynamic ens33
        valid_lft 592sec preferred_lft 592sec
    inet6 fe80::20c:29ff:fe4b:6cb0/64 scope link
        valid_lft forever preferred_lft forever
root@debian:/home/youss#
```

L'adresse 172.18.4.20 apparaît bien.

Partie 4 : Bonus – Mises a jour dynamiques DDNS

- 1 Génération de la clé (dans DEB2) : On génère une clé TSIG pour sécuriser la communication. (sudo ddns-confgen -k ddns key > /etc/bind/ddns-key.conf)**
- 2 Configuration du DNS : On modifie /etc/bind/named.conf.local pour y inclure la clé et autoriser les mises à jour avec allow-update**



```
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";

key "ddns-key" {
    algorithm hmac-sha256;
    secret "CpehrG70XzWBj62qRnLqxUH1u37f54/Op0YAMgy1+8A=";
};

zone "radouane.yn" {
    type master;
    file "/etc/bind/db.radouane.yn";
    allow-transfer { 172.20.30.1; };
    allow-update { key ddns-key; };
};

// Zone inverse pour le réseau des clients
zone "18.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.172.18";
    allow-transfer { 172.20.30.1; };
    allow-update { key ddns-key; };
};

// Zone inverse pour le réseau des serveurs
zone "30.20.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.172.20.30";
    allow-transfer { 172.20.30.1; };
    allow-update { key ddns-key; };
};
```

3 Configuration des serveurs DHCP sur DEB1 et DEB2 :

- Les fichiers dhcpd.conf sont modifiés pour inclure la clé, les zones à mettre à jour, et la gestion des conflits DHCPID
- J'ai changé le ddns-update-style en « interim »
- Sur DEB1, le ddns-updates est en on, et en off sur DEB2 pour éviter les conflits
- Dans la section « host deb-clt » j'ai ajouté « ddns-hostname « deb-clt » pour utiliser le nom de la réservation

4 Validation Finale (DDNS)

Le client obtient son adresse

Le log du serveur DHCP montre le succès de la mise à jour

Le client peut maintenant résoudre son propre nom

```
nov. 06 17:52:53 debian dhcpd[1644]: Added new forward map from deb-clt.radouane.yn to 172.18.4.20
nov. 06 17:52:53 debian dhcpd[1644]: Added reverse map from 20.4.18.172.in-addr.arpa. to deb-clt.radouane.yn
```

```
Home X PfSense X Client Linux X DEB1 X DEB2 X RTUX X
root@debian:/home/youss# dig deb-clt.radouane.yr

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> deb-clt.radouane.yr
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 52322
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 6e4a71c4adf5b5930100000690cd393811ca771582cfac (good)
;; QUESTION SECTION:
;deb-clt.radouane.yr.          IN      A
;; ANSWER SECTION:
deb-clt.radouane.yr.  300     IN      A      172.18.4.20
;; Query time: 3 msec
;; SERVER: 172.20.30.2#53(172.20.30.2) (UDP)
;; WHEN: Thu Nov 06 17:57:55 CET 2025
;; MSG SIZE rcvd: 92

root@debian:/home/youss#
```