Enzo Lefrançois

version 1.0

Installation Configuration

Serveur DHCP + DNS

Objectif : mettre en place un serveur DHCP + DNS afin de tester les résolution de noms et les fonctions diverses du DHCP sur Debian.

Installation et configuration des services DHCP / DNS sous debian :

En premier lieu, nous allons installer le paquet DHCP grâce à la commande **apt-get install isc-dhcp-server**. Ensuite, nous allons modifier le fichier de configuration du service DHCP avec la commande **nano /etc/dhcp/dhcpd.conf**. Paramètres à modifier :

option domain-name "xxxxx.xxxx";
option domain-name-servers 192.168.x.x;

default-lease-time 86400; (en secondes)

max-lease-time 604800; (en secondes)

authoritative; (décommenter)
log-facility local7; (décommenter)
Subnet 192.168.x.x netmask 255.255.255.0 {

range 192.168.x.x 192.168.x.x;
option subnet-mask 255.255.255.0;
option routers 192.168.x.x;
}

Par la suite nous allons aller déclarer l'interface eth0 avec la commande **nano /etc/default/isc-dhcp-server** et modifier la dernière ligne : **INTERFACES="eth0"**. Pour finir on redémarre le service.

Notes: Pour voir quels PC ont une adresse distribuée de notre serveur DHCP, la liste est présente dans **/etc/var/lib/dhcp/dhcpd.leases**.

Ensuite nous allons installer le paquet pour le serveur DNS avec la commande **apt-get install bind9**. Les fichiers qui sont en **named** sont des fichiers de configurations qui définissent le type de zone. Les fichiers **db** sont des fichiers de zones directes pour un domaine.

Dans le fichier **/etc/bind/named.conf.local** est le fichier dans lequel on définie nos zones directes ou inversées de notre domaine.

Exemple de configuration :

```
zone « lycée.fr » IN{
        type master ; #slave (secondaire)
        file « /var/cache/bind/db.lycée.fr » ;  #db pour la zone directes
} ;

zone « 1.168.192.in-addr.arpa » IN{
        type master ;
        file « var/cache/bind/rev.lycée.fr » ;  #rev pour la zone inversée
} ;
```

Pour tester notre fichier de configuration on utilise la commande **named-checkconf / chemincomplet (/etc/bind/named.conf.local).**
Une fois ceci fait on créer notre zone directe dans **/var/cache/bind/xxxxxxxxx (db.lycee.fr).**

Structure du fichier :

$TTL ttl // durée de vie en seconde de la conservation en cache
@ IN SOA serveur.domain.local. Mailadmin. (#nom zone : @ #mail : admin.lycee.fr

20140925	;	SERIAL
172800	;	REFRESH
600	;	RETRY
1209600	;	EXPIRE
600)	;	Negative Cache TTL

@ IN NS serveur.domain.local. (debian.lycee.fr)
debian IN A 192.168.1.93 (serveur IN A adresse ip serveur)
ENZO-PCINA192.168.1.94 (machine)

Ensuite on créer la zone inversée dans **/var/cache/bind/xxxxxxxxx (rev.lycee.fr)**.

Structure du fichier :

$TTL 3600
@ IN SOA serveur.domain.local. Mailadmin. (

20140925	;	SERIAL
172800	;	REFRESH
600	;	RETRY
1209600	;	EXPIRE
600)	;	Negative Cache TTL

@ IN NS serveur.
93 IN PTR serveur.domaine.local. (93 = 4^{e} octet de l'ip)
94 IN PTR machine.domaine.local. (machine)

Ensuite redémarrez le service avec ma commande **service bind9 restart** ou recharger les fichiers de configuration sans redémarrer le service avec la commande : **rndc reload.**

Tolérance de panne de serveur DNS (DNS secondaire) :

Il suffira d'installer **bind9** sur une machine secondaire et de rajouter dans le fichier **named.conf.local** de la machine maître les lignes suivantes dans chaque zone :

notify yes ;
allow-transfer {192.168.1.x;} ; #@ip du serveur secondaire

Ensuite n'oubliez pas de changer le nom de votre machine si votre machine secondaire a le même nom que votre machine principale avec la commande **nano /etc/hostname** et **nano /etc/hosts**.

Une fois ceci fait, il faut configurer le fichier named.conf.local de votre machine secondaire :

```
zone « lycée.fr » IN{
        type slave ;
        masters {192.168.1.x;} ; #@ip serveur principal
        file «  /var/cache/bind/db.lycée.fr » ; #db pour la zone directes };
} ;
zone « 1.168.192.in-addr.arpa » IN{
        type slave ;
        masters {192.168.1.x;} ; #@ip serveur principal
        file « var/cache/bind/rev.lycée.fr » ; #rev pour la zone inversée };
} ;
```

Vous devrez ensuite ajoutez plusieurs lignes dans votre zone directe de votre machine principale :

@ IN NS hostname (de la machine secondaire).lycee.fr.
hostname(de la machine secondaire).lycee.fr. IN A 192.168.1.x # @ip serveur secondaire

Ensuite ajoutez plusieurs lignes dans votre zone inversée de votre machine principale :

@ IN NS hostname (de la machine secondaire).lycee.fr.
95 IN PTR hostname(de la machine secondaire).lycee.fr.

Pour vérifier le bon fonctionnement, modifiez les zones sur le DNS principal en changeant les valeurs de la ligne SERIAL en incrémentant et tapez la commande **rndc reload.** Si vous avez les nouveaux fichiers de zones dans votre serveur secondaire alors votre serveur DNS marche !

Mise à jour automatique du serveur DNS :

Nous allons d'abord modifier le fichier **named.conf.local** et lui ajouter la ligne dans chaque zone :

allow-update {@IP serveur DHCP ;} ;

```
zone    "sio2a.fr"      IN      {
type master     ;
file    "/var/cache/bind/db.sio2a.fr"   ;
notify  yes     ;
allow-transfer  {       192.168.1.90    ;       }
allow-update {127.0.0.1;};
};
```

```
zone    "1.168.192.in-addr.arpa"        IN      {
type master     ;
file    "/var/cache/bind/rev.sio2a.fr"  ;
notify  yes     ;
allow-transfer  {       192.168.1.90    ;       }
allow-update {127.0.0.1;};
};
```

Ensuite nous allons rajouter des lignes dans le fichier de configuration du serveur DHCP dans **/etc/dhcp** et **nano dhcpd.conf** et ajouter les lignes au début :

ddns-update-style interim ;

ddns-updates on :
ignore client-updates ; / /facultatif

update-static-leases on ; / /facultatif

allow-update-clients ; / /facultatif

```
ddns-update-style interim;
ddns-updates on;
ignore client-updates;
update-static-leases on;
allow-update-clients;
# option definitions common to all supported networks...
option domain-name "sio2a.fr";
option domain-name-servers 192.168.1.89;
```

Ensuite il faut rajouter à la fin du fichiers les deux lignes suivantes :

zone lycee.fr. {primary @IP DNS;}
zone 1.168.192.in-addr.arpa. {primary @IP DNS;}

```
#}
zone sio2a.fr. {primary 127.0.0.1;}
zone 1.168.192.in-addr.arpa. {primary 127.0.0.1;}
```

Pour finir on redémarre les service DNS et DHCP avec les commandes : **service bind9 restart** et **service isc-dhcp- server restart**.

Test du serveur DNS sur des machines clientes :

Pour consulter les clients qui se sont connecté au DHCP on utilise la commande **nano /var/lib/dhcp/dhcpd.leases**.

```
lease 192.168.1.90 {
  starts 4 2014/10/09 08:11:50;
  ends 4 2014/10/09 08:21:50;
  cltt 4 2014/10/09 08:11:50;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 74:d4:35:8f:f6:b5;
  uid "\001t\3245\217\366\265";
  set ddns-rev-name = "90.1.168.192.in-addr.arpa.";
  set ddns-txt = "31c24697a853aa1cb921b30761a1c5d36a";
  set ddns-fwd-name = "POSTE03.sio2a.fr";
  client-hostname "POSTE03";
}
```

Consulter ensuite les logs dans **/var/log/syslog** pour voir les requête et que les zones ont bien été mises à jour.

```
Oct  9 09:45:06 Debian named[3480]: client 127.0.0.1#18504: updating zone 'sio2
Oct  9 09:45:06 Debian dhcpd: DHCPREQUEST for 192.168.1.92 from 08:00:27:e9:aa:
Oct  9 09:45:06 Debian dhcpd: DHCPACK on 192.168.1.92 to 08:00:27:e9:aa:be (mac
Oct  9 09:45:06 Debian named[3480]: zone sio2a.fr/IN: sending notifies (serial
Oct  9 09:45:06 Debian dhcpd: Added new forward map from machine-PC.sio2a.fr to
Oct  9 09:45:06 Debian named[3480]: client 127.0.0.1#18504: updating zone '1.16
Oct  9 09:45:06 Debian named[3480]: client 127.0.0.1#18504: updating zone '1.16
Oct  9 09:45:06 Debian dhcpd: Added reverse map from 92.1.168.192.in-addr.arpa.
Oct  9 09:45:06 Debian named[3480]: zone 1.168.192.in-addr.arpa/IN: sending not
```

Lorsque qu'un client Windows s'est connecté au DHCP et au DNS, des fichiers .jnl se créent dans **/var/cache/bind**.

```
root@Debian:/var/cache/bind# ls
db.sio2a.fr      managed-keys.bind      rev.sio2a.fr
db.sio2a.fr.jnl  managed-keys.bind.jnl  rev.sio2a.fr.jnl
root@Debian:/var/cache/bind# _
```

Si on réalise un **nslookup** sur Windows, on peut voir que la résolution direct et inversée se réalisent.

```
> 192.168.1.90
Serveur :   Debian.sio2a.fr
Address:  192.168.1.89

Nom :    POSTE03.sio2a.fr
Address:  192.168.1.90
```

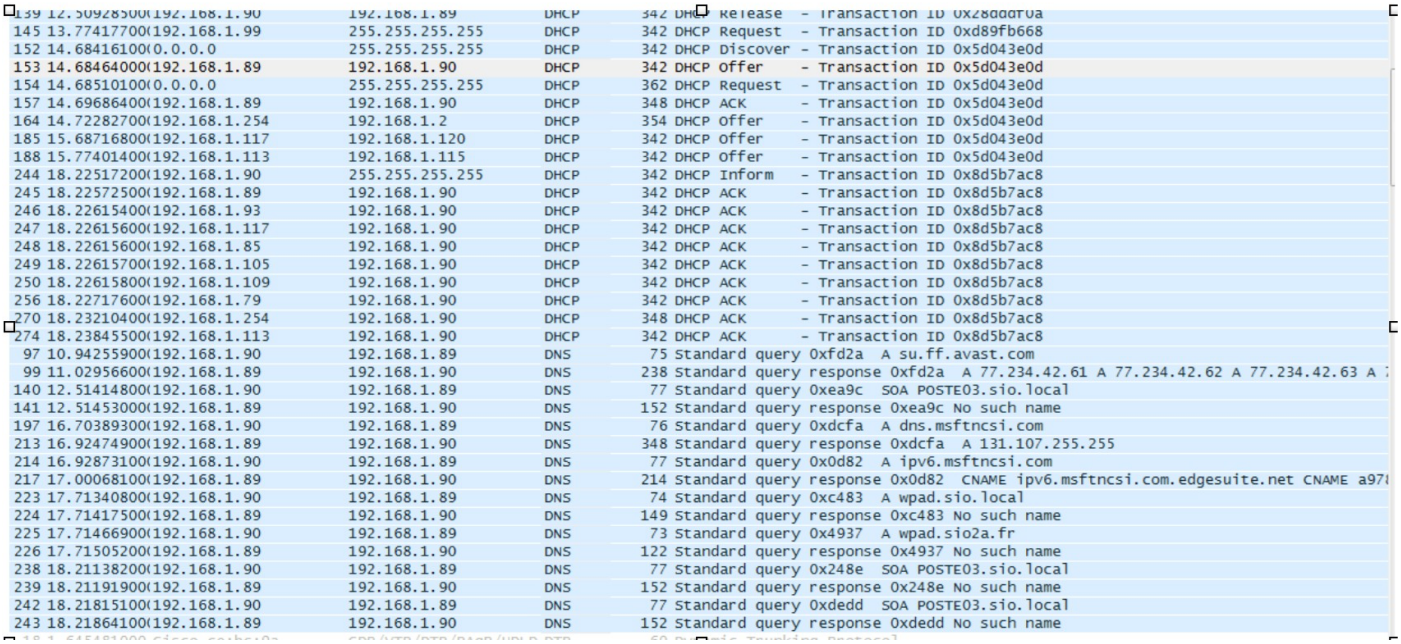
```
> POSTE03.sio2a.fr
Serveur :   Debian.sio2a.fr
Address:  192.168.1.89

Nom :    POSTE03.sio2a.fr
Address:  192.168.1.90
```

Pour un client Linux le nom de la machine s'écrit directement dans les fichiers de zones directe et inversé.

```
$ORIGIN .
$TTL 86400      ; 1 day
1.168.192.in-addr.arpa  IN SOA  Debian.sio2a.fr. admin.sio2a.fr. (
                                2509201406 ; serial
                                30         ; refresh (30 seconds)
                                3600       ; retry (1 hour)
                                604800     ; expire (1 week)
                                600        ; minimum (10 minutes)
                                )
                        NS      Debian.
                        NS      VincentDB.sio2a.fr.
$ORIGIN 1.168.192.in-addr.arpa.
10                      PTR     POSTE01.sio2a.fr.
11                      PTR     POSTE02.sio2a.fr.
12                      PTR     POSTE03.sio2a.fr.
89                      PTR     Debian.sio2a.fr.
$TTL 300        ; 5 minutes
90                      PTR     POSTE03.sio2a.fr.
92                      PTR     machine-PC.sio2a.fr.
$TTL 86400      ; 1 day
```

On peut ensuite capturer les trames grâce à WIRESHARK. On peut y voir les trames DHCP et DNS entre le serveur debian et notre machine cliente.



```
145 13.77417700(192.168.1.99    255.255.255.255  DHCP  342 DHCP Request  - Transaction ID 0xd89fb668
152 14.68416100(0.0.0.0         255.255.255.255  DHCP  342 DHCP Discover - Transaction ID 0x5d043e0d
153 14.68464000(192.168.1.89    192.168.1.90     DHCP  342 DHCP Offer    - Transaction ID 0x5d043e0d
154 14.68510100(0.0.0.0         255.255.255.255  DHCP  362 DHCP Request  - Transaction ID 0x5d043e0d
157 14.69686400(192.168.1.89    192.168.1.90     DHCP  348 DHCP ACK      - Transaction ID 0x5d043e0d
164 14.72282700(192.168.1.254   192.168.1.2      DHCP  354 DHCP Offer    - Transaction ID 0x5d043e0d
185 15.68716800(192.168.1.117   192.168.1.120    DHCP  342 DHCP Offer    - Transaction ID 0x5d043e0d
188 15.77401400(192.168.1.113   192.168.1.115    DHCP  342 DHCP Offer    - Transaction ID 0x5d043e0d
244 18.22517200(192.168.1.90    255.255.255.255  DHCP  342 DHCP Inform   - Transaction ID 0x8d5b7ac8
245 18.22572500(192.168.1.89    192.168.1.90     DHCP  342 DHCP ACK      - Transaction ID 0x8d5b7ac8
246 18.22615400(192.168.1.93    192.168.1.90     DHCP  342 DHCP ACK      - Transaction ID 0x8d5b7ac8
247 18.22615600(192.168.1.117   192.168.1.90     DHCP  342 DHCP ACK      - Transaction ID 0x8d5b7ac8
248 18.22615600(192.168.1.85    192.168.1.90     DHCP  342 DHCP ACK      - Transaction ID 0x8d5b7ac8
249 18.22615700(192.168.1.105   192.168.1.90     DHCP  342 DHCP ACK      - Transaction ID 0x8d5b7ac8
250 18.22615800(192.168.1.109   192.168.1.90     DHCP  342 DHCP ACK      - Transaction ID 0x8d5b7ac8
256 18.22717600(192.168.1.79    192.168.1.90     DHCP  342 DHCP ACK      - Transaction ID 0x8d5b7ac8
270 18.23210400(192.168.1.254   192.168.1.90     DHCP  348 DHCP ACK      - Transaction ID 0x8d5b7ac8
274 18.23845500(192.168.1.113   192.168.1.90     DHCP  342 DHCP ACK      - Transaction ID 0x8d5b7ac8
 97 10.94255900(192.168.1.90    192.168.1.89     DNS    75 Standard query 0xfd2a  A su.ff.avast.com
 99 11.02956600(192.168.1.89    192.168.1.90     DNS   238 Standard query response 0xfd2a  A 77.234.42.61 A 77.234.42.62 A 77.234.42.63 A
140 12.51414800(192.168.1.90    192.168.1.89     DNS    77 Standard query 0xea9c  SOA POSTE03.sio.local
141 12.51453000(192.168.1.89    192.168.1.90     DNS   152 Standard query response 0xea9c No such name
197 16.70389300(192.168.1.90    192.168.1.89     DNS    76 Standard query 0xdcfa  A dns.msftncsi.com
213 16.92474900(192.168.1.89    192.168.1.90     DNS   348 Standard query response 0xdcfa  A 131.107.255.255
214 16.92873100(192.168.1.90    192.168.1.89     DNS    77 Standard query 0x0d82  A ipv6.msftncsi.com
217 17.00068100(192.168.1.89    192.168.1.90     DNS   214 Standard query response 0x0d82  CNAME ipv6.msftncsi.com.edgesuite.net CNAME a97
223 17.71340800(192.168.1.90    192.168.1.89     DNS    74 Standard query 0xc483  A wpad.sio.local
224 17.71417500(192.168.1.89    192.168.1.90     DNS   149 Standard query response 0xc483 No such name
225 17.71466900(192.168.1.90    192.168.1.89     DNS    73 Standard query 0x4937  A wpad.sio2a.fr
226 17.71505200(192.168.1.89    192.168.1.90     DNS   122 Standard query response 0x4937 No such name
238 18.21138200(192.168.1.90    192.168.1.89     DNS    77 Standard query 0x248e  SOA POSTE03.sio.local
239 18.21191900(192.168.1.89    192.168.1.90     DNS   152 Standard query response 0x248e No such name
242 18.21815100(192.168.1.90    192.168.1.89     DNS    77 Standard query 0xdedd  SOA POSTE03.sio.local
243 18.21864100(192.168.1.89    192.168.1.90     DNS   152 Standard query response 0xdedd No such name
```

On peut capturer également les demandes de résolution directe (type A/AAAA) et inversé (type PTR) avec des questions/réponses comme ci-dessous :

```
 30 2.490102000 192.168.1.90  192.168.1.89  DNS   85 Standard query 0x0007  PTR 90.1.168.192.in-addr.arpa
 31 2.490815000 192.168.1.89  192.168.1.90  DNS  175 Standard query response 0x0007  PTR POSTE03.sio2a.fr
 49 5.401371000 192.168.1.90  192.168.1.89  DNS   86 Standard query 0x0008  A POSTE03.sio2a.fr.sio.local
 50 5.402079000 192.168.1.89  192.168.1.90  DNS  161 Standard query response 0x0008 No such name
 51 5.402355000 192.168.1.90  192.168.1.89  DNS   86 Standard query 0x0009  AAAA POSTE03.sio2a.fr.sio.local
 52 5.402913000 192.168.1.89  192.168.1.90  DNS  161 Standard query response 0x0009 No such name
 53 5.403220000 192.168.1.90  192.168.1.89  DNS   76 Standard query 0x000a  A POSTE03.sio2a.fr
 54 5.403741000 192.168.1.89  192.168.1.90  DNS  169 Standard query response 0x000a  A 192.168.1.90
 55 5.404096000 192.168.1.90  192.168.1.89  DNS   76 Standard query 0x000b  AAAA POSTE03.sio2a.fr
 56 5.404671000 192.168.1.89  192.168.1.90  DNS  125 Standard query response 0x000b
```