DNS Dynamique/ DHCP

Ce tutoriel développe la mise en place d'un serveur DNS (BIND) Master, qui sera mit à jour dynamiquement par un serveur DHCP. Puis le serveur DNS Master mettra à jour un serveur DNS Slave. Les routeurs transféreront les demandes dhcp des stations par dhcp-relay.

Installation des packages

Mandrake	debian
Sur les 2 serveurs : bind-9.2.3-6.rpm bind-utils-9.2.3-6.rpm **Sur le serveur Master :** dhcp-common-3.0-1.rc14.rpm dhcp-server-3.0-1.rc14.rpm (ne pas installer dhcp-client-xx) **Sur les clients :** dhcp-common-3.0-1.rc14.rpm dhcp-client-3.0-1.rc14.rpm	**Sur les 2 serveurs :** bind-9_9.2.3+9.2.4-rc2-1_i386.deb bind9-host_9.2.3+9.2.4-rc2-1_i386.deb dnsutils_9.2.3+9.2.4-rc2-1_i386.deb libdns11_9.2.3+9.2.4-rc2-1_i386.deb **Sur le serveur Master :** dhcp3-common_3.0.1-1_i386.deb dhcp3-server_3.0.1-1_i386.deb (ne pas installer dhcp3-client_xx) **Sur les clients :** dhcp3-common_3.0.1-1_i386.deb dhcp3-client_3.0.1-1_i386.deb

Génération de la clef TSIG (Transaction SIGnatures)

BIND utilise une signature par clef cryptée pour authentifier les transactions le concernant. Pour que DHCP soit autorisé à mettre à jour la base DNS Master et que le DNS Slave puisse être mis a jour par le Master, ils devront connaître cette clef.

La commande suivante génère une paire de clefs HMAC-MD5 à 128 bits intitulé mykey

```
[root@pc user]# dnssec-keygen -a HMAC-MD5 -b 128 -n USER mykey
[root@pc user]# ls
Kmykey.+157+12345.key    Kmykey.+157+12345.private
[root@pc user]#
```

Ouvrez le fichier Kmykey.+157+12345.private pour extraire la clef

```
Private-key-format: v1.2
Algorithm: 157 (HMAC_MD5)
Key: vwMIK07Iqm5+LjnKaiOvsg==
```

Copiez cette clef dans le fichier

Mandrake	debian
/etc/rndc.key(chmod 600) sous cette forme :	**/etc/bind/rndc.key**(chmod 600) sous cette forme :

```
key mykey {
        algorithm        hmac-md5;
        secret "vwMIK07Iqm5+LjnKaiOvsg==";
};
```

Configuration de DHCP

Mandrake	debian
Modifiez le fichier **/etc/dhcpd.conf**	Modifiez le fichier **/etc/dhcp3/dhcpd.conf**

```
# Indique une mise à jour DNS.
ddns-update-style interim;

# Indique que notre serveur fait autorité sur le réseau (master)
authoritative;

# Refuse les adresses MAC en double.
deny duplicates;

# Ignore les messages DHCPDECLINE des clients, permet d'éviter
# l'abandon successif d'adresses.
ignore declines;

# Nom ou adresses des DNS pour tout nos réseaux.
option domain-name-servers 192.168.0.1, 192.168.0.5;

# Divers renseignements sont disponible pour paramétrer les clients.
# voir man dhcp-options pour la liste. Dans notre cas ces options
# sont les mêmes pour tout nos réseaux.
option lpr-servers 192.168.0.7;
option netbios-name-servers 192.168.0.2, 192.168.0.6;
option smtp-server 192.168.1.3;
option pop-server 192.168.1.3;

# Indiquez l'adresse de votre réseau ou sous réseau avec son masque.
# Paramètres pour le réseau 192.168.0.0/24
subnet 192.168.0.0 netmask 255.255.255.0 {

# Nom de votre domaine pour cette zone.
option domain-name "alex.fr";

# Information sur votre réseau.
option routers 192.168.0.8;
option subnet-mask 255.255.255.0;
```

```
option broadcast-address 192.168.0.255;

# Plages d'adresses couvertes par DHCP.
range 192.168.0.20 192.168.0.250;
default-lease-time 21600;
max-lease-time 43200;

# Updates dynamique.
ddns-updates on;
ddns-domainname "alex.fr";
# Il faut mettre la valeur "in-addr.arpa" pour chaque réseaux/sous-réseaux.
ddns-rev-domainname "in-addr.arpa";

# La clef autorisant DHCP à écrire dans la base DNS.
```

Mandrake	debian
`include "/etc/rndc.key";`	`include "/etc/bind/rndc.key";`

```
# Indique dans quelle zone DNS, DHCP peut écrire.
# Ce sont les zones pour ce réseau, données dans named.conf
zone alex.fr {
primary 192.168.0.1;
key mykey;
}

# La zone reverve pour alex.fr
zone 0.168.192.in-addr.arpa {
primary 192.168.0.1;
key mykey;
}

# Déclaration des adresses fixes.
host srv2 {
hardware ethernet 00:50:04:87:41:3B;
fixed-address 192.168.0.2;
option host-name "srv2";
}
host srv5 {
hardware ethernet 00:50:0F:87:E1:3B;
fixed-address 192.168.0.5;
option host-name "srv5";
}
host srv6 {
hardware ethernet 00:0C:6E:7A:B8:21;
fixed-address 192.168.0.6;
option host-name "srv6";
}
host srv7 {
hardware ethernet 00:d0:19:24:96:7R;
fixed-address 192.168.0.7;
option host-name "srv7";
```

```
}
host fw2 {
hardware ethernet 00:30:V6:S4:78:43;
fixed-address 192.168.0.8;
option host-name "fw2";
}
host rt1 {
hardware ethernet 00:e4:24:j3:85:03;
fixed-address 192.168.0.254;
option host-name "rt1";
}
}
# Fin des paramètres pour le réseau 192.168.0.0/24

# Pas de paramètres pour le réseau 192.168.1.0/24 car il n'y a que des
serveurs.

# Paramètres pour le réseau 192.168.2.0/24
subnet 192.168.2.0 netmask 255.255.255.0 {

# Nom de votre domaine pour cette zone.
option domain-name "compta.alex.fr";

# Information sur votre réseau.
option routers 192.168.2.1;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.2.255;

# Plages d'adresses couvertes par DHCP.
range 192.168.2.20 192.168.2.250;
default-lease-time 21600;
max-lease-time 43200;

# Updates dynamique.
ddns-updates on;
ddns-domainname "compta.alex.fr";
ddns-rev-domainname "in-addr.arpa";

# La clef autorisant DHCP à écrire dans la base DNS.
include "/etc/rndc.key";

# Ce sont les zones pour ce réseau, données dans named.conf
zone compta.alex.fr {
primary 192.168.0.1;
key mykey;
}

zone 2.168.192.in-addr.arpa {
primary 192.168.0.1;
key mykey;
}
}
# Fin des paramètres pour le réseau 192.168.2.0/24
```

```
# Paramètres pour le réseau 192.168.3.0/24
subnet 192.168.3.0 netmask 255.255.255.0 {

# Nom de votre domaine pour cette zone.
option domain-name "etude.alex.fr";

# Information sur votre réseau.
option routers 192.168.3.1;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.3.255;

# Plages d'adresses couvertes par DHCP.
range 192.168.3.20 192.168.3.250;
default-lease-time 21600;
max-lease-time 43200;

# Updates dynamique.
ddns-updates on;
ddns-domainname "etude.alex.fr";
ddns-rev-domainname "in-addr.arpa";

# La clef autorisant DHCP à écrire dans la base DNS.
include "/etc/rndc.key";

# Ce sont les zones pour ce réseau, données dans named.conf
zone etude.alex.fr {
primary 192.168.0.1;
key mykey;
}

zone 3.168.192.in-addr.arpa {
primary 192.168.0.1;
key mykey;
}
}
# Fin des paramètres pour le réseau 192.168.3.0/24

# Paramètres pour le réseau 192.168.4.0/24
subnet 192.168.4.0 netmask 255.255.255.0 {

# Nom de votre domaine pour cette zone.
option domain-name "methode.alex.fr";

# Information sur votre réseau.
option routers 192.168.4.1;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.4.255;

# Plages d'adresses couvertes par DHCP.
range 192.168.4.245 192.168.4.250;
default-lease-time 21600;
max-lease-time 43200;

# Updates dynamique.
```

```
ddns-updates on;
ddns-domainname "methode.alex.fr";
ddns-rev-domainname "in-addr.arpa";

# La clef autorisant DHCP à écrire dans la base DNS.
include "/etc/rndc.key";

# Ce sont les zones pour ce réseau, données dans named.conf
zone methode.alex.fr {
primary 192.168.0.1;
key mykey;
}

zone 4.168.192.in-addr.arpa {
primary 192.168.0.1;
key mykey;
}
}
# Fin des paramètres pour le réseau 192.168.4.0/24
```

Configuration de BIND

Mandrake	debian

Modifiez le fichier **/etc/named.conf** sur le Master	Appliquez les droits suivants sur **/etc/bind/**
	`pc:/home/user# chmod 2775 /etc/bind/`
	`pc:/home/user# chown root:bind / etc/bind/`
	
	Modifiez le fichier **/etc/bind/named.conf** sur le Master

`// Déclaration de la clef en incluant directement le fichier clef.` `include "/etc/rndc.key";`	`// Déclaration de la clef en incluant directement le fichier clef.` `include "/etc/bind/rndc.key";`

```
// Instructions de mise a jour du DNS Slave.
server 192.168.0.1 {
provide-ixfr yes;
keys { mykey; };
};

// Autorise une mise a jour avec clef sur le port 953.
controls {
inet 127.0.0.1 port 953 allow { 127.0.0.1; } keys { mykey; };
};


// Définit les options du serveur dans son ensemble.
```

Mandrake

```
options {
directory "/var/named";
pid-file "/var/run/named/named.pid";

// Permet de masquer la version de
BIND.
version "SECRET";

// Indique les serveurs vers
lesquelles les requêtes seront
// retransmissent si votre serveur
DNS ne peut répondre.
# forward first;
# forwarders { 212.27.32.17; };

// Indique que le port 53 est le port
d'échange entre les serveurs DNS
// Recommandé lorsque l'on traverse
un Firewall.
query-source address * port 53;

// Contient une liste des adresses
dont le serveur acceptera ou
// refusera les requêtes :
// 127.0.0.0/8 Autorise localhost.
// !192.168.0.19 Interdit cette
adresse.
// Autorise les réseaux
192.168.0.0/24 192.168.2.0/24 ...
Allow-query { 127.0.0.0/8; !
192.168.0.19; 192.168.0.0/24;
192.168.2.0/24; 192.168.3.0/24;
192.168.4.0/24;};

// Indique un transfert de zones pour
le DNS Slave.
allow-transfer { 192.168.0.5; };

// Indique le port en écoute pour les
clients et les interfaces.
// Indiquer {*;}; pour écouter toutes
les interfaces.
listen-on port 53 { 127.0.0.1;
192.168.0.1; };
};
```

debian

```
include
"/etc/bind/named.conf.options";
```

Contenu du fichier /etc/bind/named.conf.options

```
options {
directory "/var/cache/bind";
pid-file
"/var/run/bind/run/bind.pid";

// Permet de masquer la version de
BIND.
version "SECRET";

// Indique les serveurs vers
lesquelles les requêtes seront
// retransmissent si votre serveur
DNS ne peut répondre.
# forward first;
# forwarders { 212.27.32.17; };

// Indique que le port 53 est le port
d'échange entre les serveurs DNS.
query-source address * port 53;

// Contient une liste des adresses
dont le serveur acceptera ou
// refusera les requêtes :
// 127.0.0.0/8 Autorise localhost.
// !192.168.0.19 Interdit cette
adresse.
// Autorise les réseaux
192.168.0.0/24 192.168.2.0/24 ...
Allow-query { 127.0.0.0/8; !
192.168.0.19; 192.168.0.0/24;
192.168.2.0/24; 192.168.3.0/24;
192.168.4.0/24;};

// Indique un transfert de zones pour
le DNS Slave.
allow-transfer { 192.168.0.5; };

// Indique le port en écoute pour les
clients et les interfaces.
// Indiquer {*;}; pour écouter toutes
les interfaces.
listen-on port 53 { 127.0.0.1;
192.168.0.1; };
};
```

Fin de/etc/bind/named.conf.options

```
// Zones locales, pour les
résolutions propre à la machine.
zone "localhost" {
type master;
file "zone/db.localhost";
};

zone "0.0.127.in-addr.arpa" {
type master;
file "zone/db.127.0.0.1";
allow-transfer { 127.0.0.1; };
notify no;
};

// Zone racine contenant les adresses
des serveurs DNS racine d'internet.
// Je ne l'utilise pas car mes DNS ne
sortent pas vers Internet.
// zone "." {
// type hint;
// file "zone/root.hints";
// };

// Zone de recherche pour le domaine
alex.fr
zone "alex.fr" {
type master;
file "zone/db.alex.fr";
// Autorise la mise à jour du fichier
"db.alex.fr" avec la clef.
allow-update { key mykey; };
// Indique le transfert de zone pour
le DNS Slave.
allow-transfer { 192.168.0.5; };
notify yes;
};

// Zone de recherche inversée pour le
domaine alex.fr
zone "0.168.192.in-addr.arpa" {
type master;
file "zone/db.alex.fr.rev";
// Autorise la mise à jour du fichier
"db.alex.fr.rev" avec la clef.
allow-update { key mykey; };
// Indique le transfert de zone pour
le DNS Slave.
allow-transfer { 192.168.0.5; };
notify yes;
};
```

```
// Zones locales, pour les
résolutions propre à la machine.
zone "localhost" {
type master;
file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
type master;
file "/etc/bind/db.127";
allow-transfer { 127.0.0.1; };
notify no;
};

zone "0.in-addr.arpa" {
type master;
file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
type master;
file "/etc/bind/db.255";
};

// Zone racine contenant les adresses
des serveurs DNS racine d'internet.
// Je ne l'utilise pas car mes DNS ne
sortent pas vers Internet.
// zone "." {
// type hint;
// file "/etc/bind/db.root";
// };

include "/etc/bind/named.conf.local";
```

Contenu du fichier /etc/bind/named.conf.local

```
// Zone de recherche pour le domaine
alex.fr
zone "alex.fr" {
type master;
file "/etc/bind/db.alex.fr";
// Autorise la mise à jour du fichier
"alex.fr.db" avec la clef.
allow-update { key mykey; };
// Indique le transfert de zone pour
le DNS Slave.
allow-transfer { 192.168.0.5; };
notify yes;
};
```

```
// Zone de recherche pour le domaine dmz.alex.fr
// Il n'y aura pas de mise à jour dynamique DHCP pour cette zone.
zone "dmz.alex.fr" {
type master;
file "zone/db.dmz.alex.fr";
allow-transfer { 192.168.0.5; };
notify yes;
};

// Zone de recherche inversée pour le domaine dmz.alex.fr
// Il n'y aura pas de mise à jour dynamique DHCP pour cette zone.
zone "1.168.192.in-addr.arpa" {
type master;
file "zone/db.dmz.alex.fr.rev";
allow-transfer { 192.168.0.5; };
notify yes;
};

// Zone de recherche pour le domaine compta.alex.fr
zone "compta.alex.fr" {
type master;
file "zone/db.compta.alex.fr";
allow-update { key mykey; };
allow-transfer { 192.168.0.5; };
notify yes;
};

// Zone de recherche inversée pour le domaine compta.alex.fr
zone "2.168.192.in-addr.arpa" {
type master;
file "zone/db.compta.alex.fr.rev";
allow-update { key mykey; };
allow-transfer { 192.168.0.5; };
notify yes;
};

// Zone de recherche pour le domaine etude.alex.fr
zone "etude.alex.fr" {
type master;
file "zone/db.etude.alex.fr";
allow-update { key mykey; };
allow-transfer { 192.168.0.5; };
notify yes;
};
```

```
// Zone de recherche inversée pour le domaine alex.fr
zone "0.168.192.in-addr.arpa" {
type master;
file "/etc/bind/db.alex.fr.rev";
// Autorise la mise à jour du fichier "db.alex.fr.rev" avec la clef.
allow-update { key mykey; };
// Indique le transfert de zone pour le DNS Slave.
allow-transfer { 192.168.0.5; };
notify yes;
};

// Zone de recherche pour le domaine dmz.alex.fr
// Il n'y aura pas de mise à jour dynamique DHCP pour cette zone.
zone "dmz.alex.fr" {
type master;
file "/etc/bind/db.dmz.alex.fr";
allow-transfer { 192.168.0.5; };
notify yes;
};

// Zone de recherche inversée pour le domaine dmz.alex.fr
// Il n'y aura pas de mise à jour dynamique DHCP pour cette zone.
zone "1.168.192.in-addr.arpa" {
type master;
file "/etc/bind/db.dmz.alex.fr.rev";
allow-transfer { 192.168.0.5; };
notify yes;
};


// Zone de recherche inversée pour le domaine compta.alex.fr
zone "2.168.192.in-addr.arpa" {
type master;
file
"/etc/bind/db.compta.alex.fr.rev";
allow-update { key mykey; };
allow-transfer { 192.168.0.5; };
notify yes;
};

// Zone de recherche pour le domaine compta.alex.fr
```

```
// Zone de recherche inversée pour le domaine etude.alex.fr
zone "3.168.192.in-addr.arpa" {
type master;
file "zone/db.etude.alex.fr.rev";
allow-update { key mykey; };
allow-transfer { 192.168.0.5; };
notify yes;
};

// Zone de recherche pour le domaine methode.alex.fr
zone "methode.alex.fr" {
type master;
file "zone/db.methode.alex.fr";
allow-update { key mykey; };
allow-transfer { 192.168.0.5; };
notify yes;
};

// Zone de recherche inversée pour le domaine methode.alex.fr
zone "4.168.192.in-addr.arpa" {
type master;
file "zone/db.methode.alex.fr.rev";
allow-update { key mykey; };
allow-transfer { 192.168.0.5; };
notify yes;
};
```

```
zone "compta.alex.fr" {
type master;
file "/etc/bind/db.compta.alex.fr";
allow-update { key mykey; };
allow-transfer { 192.168.0.5; };
notify yes;
};

// Zone de recherche pour le domaine etude.alex.fr
zone "etude.alex.fr" {
type master;
file "/etc/bind/db.etude.alex.fr";
allow-update { key mykey; };
allow-transfer { 192.168.0.5; };
notify yes;
};

// Zone de recherche inversée pour le domaine etude.alex.fr
zone "3.168.192.in-addr.arpa" {
type master;
file
"/etc/bind/db.etude.alex.fr.rev";
allow-update { key mykey; };
allow-transfer { 192.168.0.5; };
notify yes;
};

// Zone de recherche pour le domaine methode.alex.fr
zone "methode.alex.fr" {
type master;
file "/etc/bind/db.methode.alex.fr";
allow-update { key mykey; };
allow-transfer { 192.168.0.5; };
notify yes;
};

// Zone de recherche inversée pour le domaine methode.alex.fr
zone "4.168.192.in-addr.arpa" {
type master;
file
"/etc/bind/db.methode.alex.fr.rev";
allow-update { key mykey; };
allow-transfer { 192.168.0.5; };
notify yes;
};
Fin de /etc/bind/named.conf.local
```

Mandrake	debian
Modifiez le fichier **/etc/named.conf**sur le Slave.	Modifiez le fichier **/etc/bind/named.conf**sur le Slave.
`// Déclaration de la clef en incluant directement le fichier clef.` `include "/etc/rndc.key";`	`// Déclaration de la clef en incluant directement le fichier clef.` `include "/etc/bind/rndc.key";`

```
// Instructions de mise à jour depuis le DNS Master.
server 192.168.0.5 {
request-ixfr yes;
keys { mykey; };
};

// Autorise une mise à jour avec clef depuis le DNS Master.
controls {
inet 127.0.0.1 allow { 192.168.0.1; } keys { mykey; };
};

// Définit les options du serveur dans son ensemble.
```

Mandrake	debian

`Options {`
`directory "/var/named";`
`pid-file "/var/run/named/named.pid";`
 	
`// Permet de masquer la version de BIND.`
`version "SECRET";`
`// Indique les serveurs vers lesquelles les requêtes seront`
`// retransmissent si votre serveur DNS ne peut répondre.`
`# forward first;`
`# forwarders { 192.168.0.1;`
`212.27.32.17; };`
 	
`// Indique que le port 53 est le port d'échange entre les serveurs DNS`
`// Recommandé lorsque l'on traverse un Firewall.`
`query-source address * port 53;`
	`include "/etc/bind/named.conf.options";`
	Contenu du fichier /etc/bind/named.conf.options
	
	`options {`
	`directory "/var/cache/bind";`
	`pid-file "/var/run/bind/run/bind.pid";`
	
	`// Permet de masquer la version de BIND.`
	`version "SECRET";`
	
	`// Indique les serveurs vers lesquelles les requêtes seront`
	`// retransmissent si votre serveur DNS ne peut répondre.`
	`# forward first;`
	`# forwarders { 192.168.0.1;`
	`212.27.32.17; };`
	
	`// Indique que le port 53 est le port d'échange entre les serveurs DNS.`
	`// Recommandé lorsque l'on traverse un Firewall.`
	`query-source address * port 53;`

```
// Contient une liste des adresses
dont le serveur acceptera ou
// refusera les requêtes :
// 127.0.0.0/8 Autorise localhost.
// !192.168.0.19 Interdit cette
adresse.
// Autorise les réseaux
192.168.0.0/24 192.168.2.0/24 ...
Allow-query { 127.0.0.0/8; !
192.168.0.19; 192.168.0.0/24;
192.168.2.0/24; 192.168.3.0/24;
192.168.4.0/24;};

// Indique le port en écoute pour les
clients et les interfaces.

// Indiquer {*;}; pour écouter toutes
les interfaces.
listen-on port 53 { 127.0.0.1;
192.168.0.5; };

};
```

```
// Contient une liste des adresses
dont le serveur acceptera ou
// refusera les requêtes :
// 127.0.0.0/8 Autorise localhost.
// !192.168.0.19 Interdit cette
adresse.
// Autorise les réseaux
192.168.0.0/24 192.168.2.0/24 ...
Allow-query { 127.0.0.0/8; !
192.168.0.19; 192.168.0.0/24;
192.168.2.0/24; 192.168.3.0/24;
192.168.4.0/24;};

// Indique le port en écoute pour les
clients et les interfaces.

// Indiquer {*;}; pour écouter toutes
les interfaces.
listen-on port 53 { 127.0.0.1;
192.168.0.5; };

};
Fin de/etc/bind/named.conf.options
```

Mandrake

```
// Zones locales, pour les
résolutions propre à la machine.
zone "localhost" {
type master;
file "zone/db.localhost";
};

zone "0.0.127.in-addr.arpa" {
type master;
file "zone/db.127.0.0.1";
allow-transfer { 127.0.0.1; };
notify no;
};

// Zone racine contenant les adresses
des serveurs DNS racine d'internet.
// Je ne l'utilise pas car mes DNS ne
sortent pas vers Internet.
// zone "." {
// type hint;
// file "zone/root.hints";
// };

// Demande la mise à jour de la zone
alex.fr depuis le DNS Master.
zone "alex.fr" {
type slave;
file "zone/db.alex.fr";
masters {192.168.0.1;};
};

// Demande la mise à jour de la zone
reverve alex.fr depuis le DNS Master.
zone "0.168.192.in-addr.arpa" {
type slave;
file "zone/db.alex.fr.rev";
masters {192.168.0.1;};
};

// Demande la mise à jour de la zone
dmz.alex.fr depuis le DNS Master.
zone "dmz.alex.fr" {
type slave;
file "zone/db.dmz.alex.fr";
masters {192.168.0.1;};
};
```

debian

```
// Zones locales, pour les
résolutions propre à la machine.
zone "localhost" {
type master;
file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
type master;
file "/etc/bind/db.127";
allow-transfer { 127.0.0.1; };
notify no;
};

zone "0.in-addr.arpa" {
type master;
file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
type master;
file "/etc/bind/db.255";
};

// Zone racine contenant les adresses
des serveurs DNS racine d'internet.
// Je ne l'utilise pas car mes DNS ne
sortent pas vers Internet.
// zone "." {
// type hint;
// file "/etc/bind/db.root";
// };

include "/etc/bind/named.conf.local";
```

Contenu du fichier /etc/bind/named.conf.local

```
// Demande la mise à jour de la zone
alex.fr depuis le DNS Master.
zone "alex.fr" {
type slave;
file "/etc/bind/db.alex.fr";
masters {192.168.0.1;};
};

// Demande la mise à jour de la zone
reverve alex.fr depuis le DNS Master.
```

```
// Demande la mise à jour de la zone reverve dmz.alex.fr depuis le DNS Master.
zone "1.168.192.in-addr.arpa" {
type slave;
file "zone/db.dmz.alex.fr.rev";
masters {192.168.0.1;};
};

// Demande la mise a jour de la zone compta.alex.fr depuis le DNS Master.
zone "compta.alex.fr" {
type slave;
file "zone/db.compta.alex.fr";
masters {192.168.0.1; };
};

// Demande la mise à jour de la zone reverve compta.alex.fr depuis le DNS Master.
zone "2.168.192.in-addr.arpa" {
type slave;
file "zone/db.compta.alex.fr.rev";
masters {192.168.0.1; };
};

// Demande la mise a jour de la zone etude.alex.fr depuis le DNS Master.
zone "etude.alex.fr" {
type slave;
file "zone/db.etude.alex.fr";
masters {192.168.0.1; };
};

// Demande la mise à jour de la zone reverve etude.alex.fr depuis le DNS Master.
zone "3.168.192.in-addr.arpa" {
type slave;
file "zone/db.etude.alex.fr.rev";
masters {192.168.0.1; };
};

// Demande la mise a jour de la zone methode.alex.fr depuis le DNS Master.
zone "methode.alex.fr" {
type slave;
file "zone/db.methode.alex.fr";
masters {192.168.0.1; };
};
```

```
zone "0.168.192.in-addr.arpa" {
type slave;
file "/etc/bind/db.alex.fr.rev";
masters {192.168.0.1;};
};

// Demande la mise à jour de la zone dmz.alex.fr depuis le DNS Master.
zone "dmz.alex.fr" {
type slave;
file "/etc/bind/db.dmz.alex.fr";
masters {192.168.0.1;};
};

// Demande la mise à jour de la zone reverve dmz.alex.fr depuis le DNS Master.
zone "1.168.192.in-addr.arpa" {
type slave;
file "/etc/bind/db.dmz.alex.fr.rev";
masters {192.168.0.1;};
};

// Demande la mise à jour de la zone compta.alex.fr depuis le DNS Master.
zone "compta.alex.fr" {
type slave;
file "/etc/bind/db.compta.alex.fr";
masters {192.168.0.1;};
};

// Demande la mise à jour de la zone reverve compta.alex.fr depuis le DNS Master.
zone "2.168.192.in-addr.arpa" {
type slave;
file
"/etc/bind/db.compta.alex.fr.rev";
masters {192.168.0.1;};
};

// Demande la mise à jour de la zone etude.alex.fr depuis le DNS Master.
zone "etude.alex.fr" {
type slave;
file "/etc/bind/db.etude.alex.fr";
masters {192.168.0.1;};
};
```

```
// Demande la mise à jour de la zone reverve methode.alex.fr depuis le DNS Master.
zone "4.168.192.in-addr.arpa" {
type slave;
file "zone/db.methode.alex.fr.rev";
masters {192.168.0.1; };
};
```

```
// Demande la mise à jour de la zone reverve etude.alex.fr depuis le DNS Master.
zone "3.168.192.in-addr.arpa" {
type slave;
file
"/etc/bind/db.etude.alex.fr.rev";
masters {192.168.0.1;};
};

// Zone de recherche pour le domaine methode.alex.fr
zone "methode.alex.fr" {
type slave;
file "/etc/bind/db.methode.alex.fr";
masters {192.168.0.1;};
};

// Zone de recherche inversée pour le domaine methode.alex.fr
zone "4.168.192.in-addr.arpa" {
type slave;
file
"/etc/bind/db.methode.alex.fr.rev";
masters {192.168.0.1;};
};
Fin de /etc/bind/named.conf.local
```

Mandrake	debian

Modifiez le fichier **/etc/rndc.conf sur le Master.**
`options {`
`default-server 127.0.0.1;`
`default-key "mykey";`
`default-port 953;`
`};`
 	
`server localhost {`
`key "mykey";`
`};`
`include "/etc/rndc.key";`
 	
Modifiez le fichier /etc/rndc.conf sur le Slave.
`options {`
`default-server localhost;`
`default-key "mykey";`
`};`
`server localhost { key "mykey"; };`
`include "/etc/rndc.key";`
 	
Modifiez le fichier /var/named/zone/db.127.0.0.1 (initialement appelé named.local) il sera pratiquement le même pour le Master et le Slave.
 	
Ajoutez simplement la ligne en rouge :
`$TTL 3D`
`@ IN SOA alex.fr. root.alex.fr. (`
`31082004 ; Serial`
`28800 ; Refresh`
`7200 ; Retry`
`604800 ; Expire`
`86400 ) ; Minimum TTL`
`NS srv1.alex.fr.`
`localhost IN A 127.0.0.1`
	Créez le fichier **/etc/bind/rndc.conf sur le Master.**
	`options {`
	`default-server 127.0.0.1;`
	`default-key "mykey";`
	`default-port 953;`
	`};`
	
	`server localhost {`
	`key "mykey";`
	`};`
	`include "/etc/bind/rndc.key";`
	
	Modifiez le fichier /etc/bind/rndc.conf sur le Slave.
	`options {`
	`default-server localhost;`
	`default-key "mykey";`
	`};`
	`server localhost { key "mykey"; };`
	`include "/etc/bind/rndc.key";`
	
	Modifiez le fichier /etc/bind/db.127 il sera pratiquement le même pour le Master et le Slave.
	
	Ajoutez simplement la ligne en rouge :
	`$TTL 604800`
	`@ IN SOA localhost. root.localhost.(`
	`1 ; Serial`
	`604800 ; Refresh`
	`86400 ; Retry`
	`2419200 ; Expire`
	`604800 ) ; Negative Cache TTL`
	`NS srv1.alex.fr.`
	`@ IN NS localhost.`
	`1.0.0 IN PTR localhost.`

Conservez le fichier **/var/named/zone/root.hints** (initialement appelé named.ca)

Créez le fichier **/var/named/zone/db.alex.fr** sur le Master uniquement.

```
$ORIGIN .
$TTL 259200 ; 3 days
alex.fr IN SOA srv1.alex.fr.
root.srv1.alex.fr. (
    31082015 ; serial
    28800    ; refresh (8 hours)
    7200     ; retry (2 hours)
    2419200  ; expire (4 weeks)
    86400    ; minimum (1 day)
)
NS srv1.alex.fr.
NS srv5.alex.fr.

$ORIGIN alex.fr.
localhost A 127.0.0.1
srv1 A 192.168.0.1
srv2 A 192.168.0.2
srv5 A 192.168.0.5
srv6 A 192.168.0.6
srv7 A 192.168.0.7
srv11 A 192.168.0.11
srv12 A 192.168.0.12
srv13 A 192.168.0.13
fw2 A 192.168.0.8
rt1 A 192.168.0.254
; aliases
intranet CNAME srv5.alex.fr.
```

Conservez le fichier **/etc/bind/db.root**

Créez le fichier **/etc/bind/db.alex.fr** sur le Master uniquement.

```
$ORIGIN .
$TTL 259200 ; 3 days
alex.fr IN SOA srv1.alex.fr.
root.srv1.alex.fr. (
    31082015 ; serial
    28800    ; refresh (8 hours)
    7200     ; retry (2 hours)
    2419200  ; expire (4 weeks)
    86400    ; minimum (1 day)
)
NS srv1.alex.fr.
NS srv5.alex.fr.

$ORIGIN alex.fr.
localhost A 127.0.0.1
srv1 A 192.168.0.1
srv2 A 192.168.0.2
srv5 A 192.168.0.5
srv6 A 192.168.0.6
srv7 A 192.168.0.7
srv11 A 192.168.0.11
srv12 A 192.168.0.12
srv13 A 192.168.0.13
fw2 A 192.168.0.8
rt1 A 192.168.0.254
; aliases
intranet CNAME srv5.alex.fr.
```

Créez le fichier **/var/named/zone/db.alex.fr.rev** sur le Master uniquement.

```
$ORIGIN .
$TTL 259200 ; 3 days
0.168.192.in-addr.arpa IN SOA
srv1.alex.fr. srv1.alex.fr. (
    31082012 ; serial
    10800    ; refresh (3 hours)
    3600     ; retry (1 hour)
    604800   ; expire (1 week)
    86400    ; minimum (1 day)
)
IN NS srv1.alex.fr.
IN NS srv5.alex.fr.

$ORIGIN 0.168.192.in-addr.arpa.
; adresses IP inverses
1 IN PTR srv1.alex.fr.
2 IN PTR srv2.alex.fr.
5 IN PTR srv5.alex.fr.
6 IN PTR srv6.alex.fr.
7 IN PTR srv7.alex.fr.
8 IN PTR fw2.alex.fr.
11 IN PTR srv11.alex.fr.
12 IN PTR srv12.alex.fr.
13 IN PTR srv13.alex.fr.
254 IN PTR rt1.alex.fr.
```

Créez le fichier **/var/named/zone/db.dmz.alex.fr** sur le Master uniquement. Et copiez le, en le renommant db.votre_zone et ainsi de suite.

```
$ORIGIN .
$TTL 259200 ; 3 days
dmz.alex.fr IN SOA srv1.alex.fr.
root.srv1.alex.fr. (
    31082015 ; serial
    28800    ; refresh (8 hours)
    7200     ; retry (2 hours)
    2419200  ; expire (4 weeks)
    86400    ; minimum (1 day)
)
NS srv1.alex.fr.
NS srv5.alex.fr.
; MX = serveur de Mail
MX 10 srv3.dmz.alex.fr.

$ORIGIN dmz.alex.fr.
localhost A 127.0.0.1
srv8 A 192.168.1.1
srv9 A 192.168.1.2
srv3 A 192.168.1.3
srv4 A 192.168.1.4
```

Créez le fichier **/etc/bind/db.alex.fr.rev** sur le Master uniquement.

```
$ORIGIN .
$TTL 259200 ; 3 days
0.168.192.in-addr.arpa IN SOA
srv1.alex.fr. srv1.alex.fr. (
    31082012 ; serial
    10800    ; refresh (3 hours)
    3600     ; retry (1 hour)
    604800   ; expire (1 week)
    86400    ; minimum (1 day)
)
IN NS srv1.alex.fr.
IN NS srv5.alex.fr.

$ORIGIN 0.168.192.in-addr.arpa.
; adresses IP inverses
1 IN PTR srv1.alex.fr.
2 IN PTR srv2.alex.fr.
5 IN PTR srv5.alex.fr.
6 IN PTR srv6.alex.fr.
7 IN PTR srv7.alex.fr.
8 IN PTR fw2.alex.fr.
11 IN PTR srv11.alex.fr.
12 IN PTR srv12.alex.fr.
13 IN PTR srv13.alex.fr.
254 IN PTR rt1.alex.fr.
```

Créez le fichier **/etc/bind/db.dmz.alex.fr** sur le Master uniquement. Et copiez le, en le renommant db.votre_zone et ainsi de suite.

```
$ORIGIN .
$TTL 259200 ; 3 days
dmz.alex.fr IN SOA srv1.alex.fr.
root.srv1.alex.fr. (
    31082015 ; serial
    28800    ; refresh (8 hours)
    7200     ; retry (2 hours)
    2419200  ; expire (4 weeks)
    86400    ; minimum (1 day)
)
NS srv1.alex.fr.
NS srv5.alex.fr.
; MX = serveur de Mail
MX 10 srv3.dmz.alex.fr.

$ORIGIN dmz.alex.fr.
localhost A 127.0.0.1
srv8 A 192.168.1.1
srv9 A 192.168.1.2
srv3 A 192.168.1.3
srv4 A 192.168.1.4
```

```
vpn A 192.168.1.5
fw1 A 192.168.1.10
; aliases
mail CNAME srv3.dmz.alex.fr.
smtp CNAME srv3.dmz.alex.fr.
www CNAME srv8.dmz.alex.fr.
```

Créez le fichier **/var/named/zone/db.dmz.alex.fr.rev** sur le Master uniquement. Et copiez le, en le renommant db.votre_zone.rev et ainsi de suite.

```
$ORIGIN .
$TTL 259200 ; 3 days
1.168.192.in-addr.arpa IN SOA
srv1.alex.fr. srv1.alex.fr. (
    31082012 ; serial
    10800    ; refresh (3 hours)
    3600     ; retry (1 hour)
    604800   ; expire (1 week)
    86400    ; minimum (1 day)
)
IN NS srv1.alex.fr.
IN NS srv5.alex.fr.

$ORIGIN 1.168.192.in-addr.arpa.
; adresses IP inverses
1 IN PTR srv8.dmz.alex.fr.
2 IN PTR srv9.dmz.alex.fr.
3 IN PTR srv3.dmz.alex.fr.
4 IN PTR srv4.dmz.alex.fr.
5 IN PTR vpn.dmz.alex.fr.
10 IN PTR fw1.dmz.alex.fr.
```

```
vpn A 192.168.1.5
fw1 A 192.168.1.10
; aliases
mail CNAME srv3.dmz.alex.fr.
smtp CNAME srv3.dmz.alex.fr.
www CNAME srv8.dmz.alex.fr.
```

Créez le fichier **/etc/bind/db.dmz.alex.fr.rev** sur le Master uniquement. Et copiez le, en le renommant db.votre_zone.rev puis db.votre_zone.rev et ainsi de suite.

```
$ORIGIN .
$TTL 259200 ; 3 days
1.168.192.in-addr.arpa IN SOA
srv1.alex.fr. srv1.alex.fr. (
    31082012 ; serial
    10800    ; refresh (3 hours)
    3600     ; retry (1 hour)
    604800   ; expire (1 week)
    86400    ; minimum (1 day)
)
IN NS srv1.alex.fr.
IN NS srv5.alex.fr.

$ORIGIN 1.168.192.in-addr.arpa.
; adresses IP inverses
1 IN PTR srv8.dmz.alex.fr.
2 IN PTR srv9.dmz.alex.fr.
3 IN PTR srv3.dmz.alex.fr.
4 IN PTR srv4.dmz.alex.fr.
5 IN PTR vpn.dmz.alex.fr.
10 IN PTR fw1.dmz.alex.fr.
```

Modifiez le fichier **/etc/resolv.conf** des serveurs DNS et des autres serveurs qui s'adresseront aux DNS dans la zone alex.fr.

```
search alex.fr local
nameserver 127.0.0.1
nameserver 192.168.0.1
nameserver 192.168.0.5
```

Pour les machines des autres zones qui n'utilisent pas DHCP modifiez le fichier **/etc/resolv.conf** de cette facon :

```
# Pour la zone compta.alex.fr par exemple.
search compta.alex.fr local
nameserver 192.168.0.1
nameserver 192.168.0.5
```

Vérifiez que le fichier **/etc/nsswitch.conf** contient la ligne :

```
hosts: files dns
```

et que **/etc/host.conf**:

```
order hosts,bind
multi on
```

Vous pouvez aussi ajouter la liste de vos serveurs dans **/etc/hosts**

Configuration de dhcp-relay sur les routeurs

Installation des packages

Sur les routeurs :

dhcp-relay-3.0-1.rc14.rpm

Editez le script **/etc/init.d/dhcrelay** pour ajouter l'adresse du serveur DHCP et l'interface du coté du serveur DHCP :

```
...
# Define SERVERS with a list of one or more DHCP servers where
# DHCP packets are to be relayed to and from. This is mandatory.
#SERVERS="10.11.12.13 10.9.8.7"
SERVERS="192.168.0.1"

# Define OPTIONS with any other options to pass to the dhcrelay server. See
dhcrelay(8) for available options and syntax.
#OPTIONS="-q -i eth0 -i eth1"
# l'option -q pour silencieux.
OPTIONS="-q"
...
```

Lancez le script : `[root@rt1 user]# /etc/init.d/dhcrelay start`

Sur les routeurs :

dhcp3-relay_3.0+3.0.1rc14_i386.deb

Répondez à l'assistant :

Ce qui modifira le fichier **/etc/default/dhcp3-relay :**

```
# Defaults for dhcp3-relay initscript
# sourced by /etc/init.d/dhcp3-relay
# installed at /etc/default/dhcp3-relay by the maintainer scripts
#
# This is a POSIX shell fragment
#
# What servers should the DHCP relay forward requests to?
SERVERS="192.168.0.1"

# On what interfaces should the DHCP relay (dhrelay) serve DHCP requests?
INTERFACES="eth0"

# Additional options that are passed to the DHCP relay daemon?
OPTIONS="-q"
```

Configuration des Clients DHCP

Sous Linux:

Mandrake	debian
vous devez installer uniquement dhcp-commun-3.0-1.rc13.4.rpm et dhcp-client-3.0-1.rc13.4.rpm Copiez ensuite le fichier d'exemple **/usr/share/doc/dhcpclient-3.0/dhclient.conf** fournit à l'installation vers **/etc/dhclient-eth0.conf** (Adaptez selon le nom de votre interface réseau) Editez le pour modifier :	vous devez installer uniquement dhcp3-common_3.0+3.0.1rc13-1_i386.deb et dhcp3-client_3.0+3.0.1rc13-1_i386.deb Editez le fichier **/etc/dhcp3/dhclient.conf** pour modifier :

```
# Détermine le temps maximum entre le moment ou le client
# demande une adresse et le moment de réponse. Si personne
# ne lui répond au bout de x secondes, le client prendra
# une adresse existante dans sa base
# /var/lib/dhcp/dhclient-eth0.leases
timeout 60;

# Détermine l'intervalle de temps ou le client doit
# rechercher un serveur DHCP.
retry 60;

# Détermine la durée avant que le client redemande son
# ancienne adresse au lieu de prendre une nouvelle
# après un reboot de la machine.
reboot 10;

# Détermine le temps d'une réponse de la part d'un serveur
# après une demande d'adresse.
initial-interval 5;

# Dans le cas ou vous utilisez plusieurs serveurs DHCP,
# lorsque votre client lance une demande, il attend x secondes
# avant de recommencer si personne lui a répondu.
select-timeout 5;
```

Mandrake	debian
`# Indique le chemin du fichier de configuration dhclient-script.` `script "/sbin/dhclient-script";`	`# Indique le chemin du fichier de configuration dhclient-script.` `script "/etc/dhcp3/dhclient-script";`

```
# Informations sur le client qui seront envoyées au serveur DHCP.
# son hostname et sa MAC
```

```
send host-name "momclient.alex.fr";
send dhcp-client-identifier 00:0C:29:E2:4B:28;
send dhcp-lease-time 3600;

# Informations demandées au serveur DHCP.
request subnet-mask, broadcast-address, time-offset, routers, domain-name,
domain-name-servers, host-name, netbios-name-servers, netbios-scope;
require subnet-mask, domain-name-servers;
# Si vous utilisez plusieurs serveurs DHCP, vous ne voulez
# pas qu'ils donnent 2 fois la même adresse. Cette option
# demande de rejeter les offres du serveur indiqué.
# reject 192.168.0.1x;

# Permet en cas de non réponse du serveur DHCP d'utiliser
# les paramètres suivant.
lease {
  interface "eth0";
  option host-name "momclient.alex.fr";
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.0.255;
  option routers 192.168.0.8;
  option domain-name-servers 192.168.0.1, 192.168.0.5;
}
```

Mandrake	debian

Vérifiez le contenu du fichier **/etc/sysconfig/network** sur vos clients.
`HOSTNAME=momclient.alex.fr`
`NETWORKING=yes`
 	
Modifiez le fichier **/etc/sysconfig/network-scripts/ifcfg-eth0**
 	
`DEVICE=eth0`
`BOOTPROTO=dhcp`
`ONBOOT=yes`
`MII_NOT_SUPPORTED=yes`
 	
Relancez l'interface réseau :
`[root@momclient user]`
`# /etc/init.d/network restart`
	Vérifiez le contenu du fichier **/etc/network/interfaces** sur vos clients.
	
	`auto lo`
	`iface lo inet loopback`
	
	`auto eth0`
	`iface eth0 inet dhcp`
	
	Relancez l'interface réseau :
	`momclient:/home/user#`
	`/etc/init.d/networking restart`

Vérifiez dans le fichier **/var/lib/dhcp/dhcpd.leases** du serveur DHCP si la transaction a bien été effectuée.

```
lease 192.168.0.247 {
  starts 2 2004/03/16 17:45:32;
  ends 2 2004/03/16 18:45:32;
  tstp 2 2004/03/16 18:45:32;
  binding state free;
  hardware ethernet 00:0C:29:E2:4B:28;
  uid "\000\014)\342K(";
  client-hostname "momclient.alex.fr";
}
```

Sinon lancez manuellement la commande suivante sur le client et comparez le résultat sur le serveur.

```
[root@momclient user]# dhclient
```

Sous Windows :
Démarrer > Paramètres > Connexion réseau > Propriété sur votre interface > Propriétés sur "Protocole Internet (TCP/IP)" > cochez "Obtenir une adresse IP automatiquement" et "Obtenir les adresses des serveurs DNS automatiquement".

Source : http://www.faqs.org/docs/securing/soft-netwrkng.html

Document mis à jour : 09/06/05