INSTALLATION SERVEUR DNS PRIMAIRE/SECONDAIRE OU MASTER/SLAVE (BIND9)

http://www.commentcamarche.net/contents/internet/dns.php3#q=qu%27est+ce+qu%27un+dns&cur=2&url=%2F
http://fr.wikipedia.org/wiki/Domain_Name_System
http://wiki.goldzoneweb.info/

I) Installation du package « Bind9 »

apt-get install bind9

II) Autoriser l'écriture de bind dans le logiciel apparmor

II-A) Modification du fichier "usr.sbin.named", "named" pour le DNS

Editez /etc/apparmor.d/usr.sbin.named sur les Serveurs et rajouter "w" sur la ligne "/etc/bind/** r,"
  /etc/bind/** r,
=>
  /etc/bind/** rw,

II-B) Redémarrage du service apparmor

/etc/init.d/apparmor restart

III) Serveur Primaire (Prepav5 = 192.168.11.254)

III-A) Fichier /etc/bind/named.conf (Rien à modifier) du Serveur Primaire

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

III-B) Fichier /etc/bind/named.conf.options du Serveur Primaire

```
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.

    //L'option « forwarders » permet de rediriger les requêtes qui ne sont pas résolues
    // par notre serveur vers un serveur DNS distant (serveurs DNS de votre FAI par exemple).
    // Cela permet d'utiliser le cache d'un serveur déjà existant et donc d'obtenir des temps d'accès plus rapides.
    //Si la requête DNS n'est pas résolue par le serveur DNS « distant » alors la requête sera envoyée au serveur
```

```
    // DNS racine
    // Utile pour les clients VPN
    // DNS Public Google : 8.8.8.8 & 8.8.4.4
    // DNS Public Proxad.net : 212.27.40.240 & 212.27.40.241

    forwarders {8.8.8.8; 8.8.4.4;};

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

III-C) Fichier /etc/bind/named.conf.local du Serveur Primaire

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

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

// Création de la zone de recherche normale

zone "sannois.local" {
    type master;
    file "/etc/bind/zones/db.sannois.local";
    allow-transfer {192.168.11.252; 192.168.11.253;};
    allow-update {192.168.11.252; 192.168.11.253;};
};

// Création de la zone de recherche normale inversée

zone "11.168.192.in-addr.arpa" {
    type master;
    notify no;
    file "/etc/bind/zones/db.192_11";
    allow-transfer {192.168.11.252; 192.168.11.253;};
    allow-update {192.168.11.252; 192.168.11.253;};
};
```

III-D) Fichier /etc/bind/zones/db.sannois.local du Serveur Primaire

```
;
; BIND data file for local loopback interface
;

;TTL (Time To Live) : Temps en secondes / Temps avant que le cache du serveur soit réinitialisé
$TTL    604800

; @ = Nom du suffixe DNS spécifié par le nom de la zone dans le fichier "named.conf.local"
; e-mail : le @ est remplacé par un "."
; rr = Type d'enregistrement (A, MX, CNAME, PTR)
; Serial = Numéro à incrémenter afin que la réplication se fasse
; Refresh = Durée avant un rafraichissement Secondaire → Primaire
; Retry = En cas d'échec du rafraichissement, temps avant un nouvel essai
; Expire = Temps avant que le Secondaire considère que le Primaire est mort
; Negative Cache TTL = Durée de vie minimum du cache
```

```
;name    [ttl]   [class]   rr      name-server           e-mail                ( [...] )
@       IN      SOA                 prepav5.sannois.local.  mail.sannois.local.   (
                                                                                    2013020802      ; Serial
                                                                                    2h              ; Refresh
                                                                                    1h              ; Retry
                                                                                    5w              ; Expire
                                                                                    10m )           ; Negative TTL Cache
                NS                  prepav5.sannois.local.
                NS                  prepav1.sannois.local.
                NS                  prepav7.sannois.local.

prepav5                 A           192.168.11.254
prepav7                 A           192.168.11.253
prepav1                 A           192.168.11.252
prepav100               A           192.168.11.9

dns-prim                CNAME       prepav5.sannois.local.
dns-sec01               CNAME       prepav7.sannois.local.
dns-sec02               CNAME       prepav1.sannois.local.
```

III-E) Fichier /etc/bind/zones/db.192_11 du Serveur Primaire

```
;
; BIND data file for local loopback interface
;
;TTL (Time To Live) : Temps en secondes / Temps avant que le cache du serveur soit réinitialisé
$TTL    604800

; @ = Nom du suffixe DNS spécifié par le nom de la zone dans le fichier "named.conf.local"
; e-mail : le @ est remplacé par un "."
; rr = Type d'enregistrement (A, MX, CNAME, PTR)
; Serial = Numéro à incrémenter afin que la réplication se fasse
; Refresh = Durée avant un rafraichissement Secondaire → Primaire
; Retry = En cas d'échec du rafraichissement, temps avant un nouvel essai
; Expire = Temps avant que le Secondaire considère que le Primaire est mort
; Negative Cache TTL = Durée de vie minimum du cache

;name    [ttl]   [class]   rr      name-server           e-mail                ( [...] )
@       IN      SOA                 prepav5.sannois.local.  mail.sannois.local.   (
                                                                                    2013020802      ; Serial
                                                                                    2h              ; Refresh
                                                                                    1h              ; Retry
                                                                                    5w              ; Expire
                                                                                    10m )           ; Negative TTL Cache

                NS                  prepav5.sannois.local.
                NS                  prepav1.sannois.local.
                NS                  prepav7.sannois.local.

254     IN              PTR         prepav5.sannois.local.
253     IN              PTR         prepav7.sannois.local.
252     IN              PTR         prepav1.sannois.local.
9       IN              PTR         prepav100.sannois.local.
```

IV) Serveurs Secondaires (Prepav1 = 192.168.11.252 & Prepav7 = 192.168.11.253)

IV-A) Fichier /etc/bind/named.conf (Pas de modification) du(des) Serveur(s) Secondaire(s)

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
```

```
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

IV-B) Fichier /etc/bind/named.conf.options du(des) Serveur(s) Secondaire(s)

```
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.

    //L'option “forwarders” permet de rediriger les requêtes qui ne sont pas résolues
    // par notre serveur vers un serveur DNS distant (serveurs DNS de votre FAI par exemple).
    // Cela permet d'utiliser le cache d'un serveur déjà existant et donc d'obtenir des temps d'accès plus rapides.
    //Si la requête DNS n'est pas résolue par le serveur DNS ”distant” alors la requête sera envoyée aux serveurs DNS racine
    // Utile pour les clients VPN
    // DNS Public Google : 8.8.8.8 & 8.8.4.4
    // DNS Public Proxad.net : 212.27.40.240 & 212.27.40.241

    forwarders {8.8.8.8; 8.8.4.4;};

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

IV-C) Fichier /etc/bind/named.conf.local du(des) Serveur(s) Secondaire(s)

IV-C-1) Sur le Secondaire 192.168.11.252 (/etc/bind/name.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 "sannois.local" {
     type slave;
// « /var/cache/bind/zones » est le dossier dans lequel, le serveur principal va envoyer les fichiers de DNS.
// Et dans lequel le Serveur Secondaire va utiliser les fichiers « db.sannois.local » et « db.192_11 »,
// qui sont les noms des fichiers du Serveur Primaire.
     file "/var/cache/bind/zones/db.sannois.local";
     masters {192.168.11.254;};
    allow-transfer {192.168.11.254; 192.168.11.253;}; // @ IP du Principal et du 2e Secondaire
};
```

```
zone "11.168.192.in-addr.arpa" {
      type slave;
      file "/var/cache/bind/zones/db.192_11";
      masters {192.168.11.254;};
     allow-transfer {192.168.11.254; 192.168.11.253;}; // @ IP du Principal et du 2e Secondaire
};
```

IV-C-2) Sur le Secondaire 192.168.11.253 (/etc/bind/name.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 "sannois.local" {
      type slave;
      file "/var/cache/bind/zones/db.sannois.local";
      masters {192.168.11.254;};
     allow-transfer {192.168.11.254; 192.168.11.252;}; // @ IP du Principal et du 1er Secondaire
};

zone "11.168.192.in-addr.arpa" {
      type slave;
      file "/var/cache/bind/zones/db.192_11";
      masters {192.168.11.254;};
     allow-transfer {192.168.11.254; 192.168.11.252;}; // @ IP du Principal et du 1er Secondaire
};
```

IV-D) Vérification que des droits des dossiers /var/cache/bind & /var/cache/bind/zones du(des) Serveur(s) Secondaire(s)

root@Prepav7:~/# **cd /var/cache/bind**

root@Prepav7:/var/cache/bind# **ls -alF**
drwxrwxr-x 3 root bind 4096 févr. 8 10:49 bind/

root@Prepav7:/var/cache/bind# **mkdir zones**

root@Prepav7:/var/cache/bind# **ls -alF**
total 20
drwxrwxr-x 3 root bind 4096 févr. 8 10:49 ./
drwxr-xr-x 17 root root 4096 janv. 31 15:22 ../
-rw-r--r-- 1 bind bind 221 févr. 7 09:47 managed-keys.bind
-rw-r--r-- 1 bind bind 512 févr. 7 09:47 managed-keys.bind.jnl
drwxr-xr-x 2 bind bind 4096 févr. 8 11:29 zones/

Si le répertoire « zones » n'a pas comme utilisateur et groupe « bind », faîtes

chown -R bind:bind zones

V) Synchronisation des serveurs DNS

Vous pouvez dans une 2e fenêtre "terminal", lancer la log en temps réel ou ne pas le faire et aller au paragraphe suivant pour analyser la log.

tail -f /var/log/syslog

Quel que soit votre choix, continuer la procédure avec les points ci-dessous (V-A, V-B & V-C)

VI-A) Sur le(s) Serveur(s) Secondaire(s)

/etc/init.d/bind9 stop

VI-B) Sur le Serveur Primaire

/etc/init.d/bind9 restart

VI-C) Sur le Serveur(s) Secondaire(s)

/etc/init.d/bind9 start

VI) Vérification dans la log

La valeur de tail, ici "100", est variable selon les rôles que vous avez installé sur votre serveur (DHCP, ssh, etc...)

Ici la log est celle du 1er Serveur Secondaire (Prepav7 = 192.168.11.253)

more /var/log/syslog | tail -n100

```
Feb  8 11:44:05 Prepav7 named[3292]: starting BIND 9.8.1-P1 -u bind
Feb  8 11:44:05 Prepav7 named[3292]: built with '--prefix=/usr' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--
sysconfdir=/etc/bind' '--localstatedir=/var' '--enable-threads' '--enable-largefile' '--with-libtool' '--enable-shared' '--enable-static'
'--with-openssl=/usr' '--with-gssapi=/usr' '--with-gnu-ld' '--with-geoip=/usr' '--enable-ipv6' 'CFLAGS=-fno-strict-aliasing
-DDIG_SIGCHASE -O2' 'LDFLAGS=-Wl,-Bsymbolic-functions -Wl,-z,relro' 'CPPFLAGS=-D_FORTIFY_SOURCE=2'
Feb  8 11:44:05 Prepav7 named[3292]: adjusted limit on open files from 4096 to 1048576
Feb  8 11:44:05 Prepav7 named[3292]: found 4 CPUs, using 4 worker threads
Feb  8 11:44:05 Prepav7 named[3292]: using up to 4096 sockets
Feb  8 11:44:05 Prepav7 named[3292]: loading configuration from '/etc/bind/named.conf'
Feb  8 11:44:05 Prepav7 named[3292]: using default UDP/IPv4 port range: [1024, 65535]
Feb  8 11:44:05 Prepav7 named[3292]: using default UDP/IPv6 port range: [1024, 65535]
Feb  8 11:44:05 Prepav7 named[3292]: listening on IPv6 interfaces, port 53
Feb  8 11:44:05 Prepav7 named[3292]: listening on IPv4 interface lo, 127.0.0.1#53
Feb  8 11:44:05 Prepav7 named[3292]: listening on IPv4 interface eth0, 192.168.0.198#53
Feb  8 11:44:05 Prepav7 named[3292]: listening on IPv4 interface eth1:avahi, 169.254.5.64#53
Feb  8 11:44:05 Prepav7 named[3292]: listening on IPv4 interface eth2, 192.168.11.253#53
Feb  8 11:44:05 Prepav7 named[3292]: generating session key for dynamic DNS
Feb  8 11:44:05 Prepav7 named[3292]: sizing zone task pool based on 7 zones
Feb  8 11:44:05 Prepav7 named[3292]: set up managed keys zone for view _default, file 'managed-keys.bind'
Feb  8 11:44:05 Prepav7 named[3292]: Warning: 'empty-zones-enable/disable-empty-zone' not set: disabling RFC 1918 empty
zones
Feb  8 11:44:05 Prepav7 named[3292]: automatic empty zone: 254.169.IN-ADDR.ARPA
Feb  8 11:44:05 Prepav7 named[3292]: automatic empty zone: 2.0.192.IN-ADDR.ARPA
Feb  8 11:44:05 Prepav7 named[3292]: automatic empty zone: 100.51.198.IN-ADDR.ARPA
Feb  8 11:44:05 Prepav7 named[3292]: automatic empty zone: 113.0.203.IN-ADDR.ARPA
Feb  8 11:44:05 Prepav7 named[3292]: automatic empty zone: 255.255.255.255.IN-ADDR.ARPA
Feb  8 11:44:05 Prepav7 named[3292]: automatic empty zone:
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA
Feb  8 11:44:05 Prepav7 named[3292]: automatic empty zone:
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA
Feb  8 11:44:05 Prepav7 named[3292]: automatic empty zone: D.F.IP6.ARPA
Feb  8 11:44:05 Prepav7 named[3292]: automatic empty zone: 8.E.F.IP6.ARPA
Feb  8 11:44:05 Prepav7 named[3292]: automatic empty zone: 9.E.F.IP6.ARPA
Feb  8 11:44:05 Prepav7 named[3292]: automatic empty zone: A.E.F.IP6.ARPA
Feb  8 11:44:05 Prepav7 named[3292]: automatic empty zone: B.E.F.IP6.ARPA
Feb  8 11:44:05 Prepav7 named[3292]: automatic empty zone: 8.B.D.0.1.0.0.2.IP6.ARPA
Feb  8 11:44:05 Prepav7 named[3292]: command channel listening on 127.0.0.1#953
Feb  8 11:44:05 Prepav7 named[3292]: command channel listening on ::1#953
Feb  8 11:44:05 Prepav7 named[3292]: zone 0.in-addr.arpa/IN: loaded serial 1
Feb  8 11:44:05 Prepav7 named[3292]: zone 127.in-addr.arpa/IN: loaded serial 1
```

Feb 8 11:44:05 Prepav7 named[3292]: zone 255.in-addr.arpa/IN: loaded serial 1
Feb 8 11:44:05 Prepav7 named[3292]: zone localhost/IN: loaded serial 2
Feb 8 11:44:05 Prepav7 named[3292]: managed-keys-zone ./IN: loaded serial 7
Feb 8 11:44:05 Prepav7 named[3292]: running
Feb 8 11:44:05 Prepav7 named[3292]: zone sannois.local/IN: Transfer started.
Feb 8 11:44:05 Prepav7 named[3292]: transfer of 'sannois.local/IN' from 192.168.11.254#53: connected using 192.168.11.253#42035
Feb 8 11:44:05 Prepav7 named[3292]: zone sannois.local/IN: transferred serial 2013020727
Feb 8 11:44:05 Prepav7 named[3292]: transfer of 'sannois.local/IN' from 192.168.11.254#53: Transfer completed: 1 messages, 7 records, 210 bytes, 0.001 secs (210000 bytes/sec)
Feb 8 11:44:06 Prepav7 named[3292]: zone 11.168.192.in-addr.arpa/IN: Transfer started.
Feb 8 11:44:06 Prepav7 named[3292]: transfer of '11.168.192.in-addr.arpa/IN' from 192.168.11.254#53: connected using 192.168.11.253#50267
Feb 8 11:44:06 Prepav7 named[3292]: zone 11.168.192.in-addr.arpa/IN: transferred serial 2013020712
Feb 8 11:44:06 Prepav7 named[3292]: transfer of '11.168.192.in-addr.arpa/IN' from 192.168.11.254#53: Transfer completed: 1 messages, 6 records, 223 bytes, 0.001 secs (223000 bytes/sec)

Partie en violet, confirme la copie des fichiers « db.sannois.local » et « db.192_11 ».

VII) Vérification que les fichiers de zones ont bien été copié du Primaire au(x) Secondaire(s)

root@Prepav7:/var/cache/bind/zones# ls -alF
total 16
drwxr-xr-x 2 bind bind 4096 févr. 8 11:44 ./
drwxrwxr-x 3 root bind 4096 févr. 8 11:44 ../
-rw-r--r-- 1 bind bind 431 févr. 8 11:44 db.192_11
-rw-r--r-- 1 bind bind 414 févr. 8 11:44 db.sannois.local

Les fichiers ont bien été copié et on bien l'utilisateur « bind » et le groupe « bind ».

VIII) Tests DNS

VIII-A) Test sur le Serveur Primaire

name-checkzones sannois.local /etc/bind/zones/db.sannois.local
« sannois.local » étant le nom d'une des zones qui est dans le fichier « /etc/bind/name.conf.local » et que l'on associe le test avec le fichier « /etc/bind/zones/db/sannois.local » où est configurer la zone de recherche normale.
On peux aussi tester la zone de recherche inversée.
name-checkzones 11.168.192.in-addr.arpa /etc/bind/zones/db.192_11

VIII-B) Test sur le Serveur Primaire

name-checkzones sannois.local /var/cache/bind/zones/db.sannois.local
 # name-checkzones 11.168.192.in-addr.arpa /var/cache/bind/zones/db.192_11

VIII-C) Test sur tous les Serveurs

Test dns : # dig prepav5
dig -x 192.168.11.254
nslookup

IX) Outils DNS

dnstop eth0
Pour plus d'information sur dnstop, faîtes
man dnstop

Vider le cache DNS : **# rndc flush**
Vider le cache DNS et le recharger de la configuration : # **/etc/init.d/bind9 reload**

Prise en compte des modifications : # rndc reload