Sommaire :

Introduction

Objectif : L'objectif de cette situation professionnelle est de mettre en place un service DNS secondaire, qui récupère automatiquement les zones DNS d'un serveur principal. Le transfert des zones entre les deux DNS doit se faire de manière sécurisée grâce au protocole DNSSEC.

Pré-requis : Il faut vérifier que bind a les droits sur les répertoires ***/etc/bind*** et ***/var/cache/bind***, ou tout répertoire de destination ! On utilise la commande chown –R bind.bind bind par exemple.
Il faut également mettre l'adresse de son serveur DNS dans ***/etc/resolv.conf*** !
Il faut redémarrer le ***service bind9 restart*** et incrémenter le fichier de zone à chaque modification !

named-checkconf fichierdeconf → Permet de vérifier les fichiers de configuration.
named-checkzone domaine fichier → Permet de vérifier les fichiers de zones.

Norme : Toutes les commandes issues d'une machine avec un système d'exploitation Debian ou Windows sont écrites ***en gras et en italique***.

Configurer le DNS Esclave - Debian :

Nous commençons par configurer le serveur DNS qui sera considéré comme Esclave. Pour commencer, il faut modifier le nom d'hôte de notre machine, à travers les fichiers ***/etc/hosts*** et ***/etc/hostname*** :

```
  GNU nano 2.2.6                Fichier : /etc/hosts

127.0.0.1       localhost
192.168.1.117   dnssec
```

```
  GNU nano 2.2.6              Fichier : /etc/hostname

dnssec
```

Nous attribuons ensuite une adresse IP à notre machine, dans le fichier ***/etc/network/interfaces*** :

```
# The primary network interface
allow-hotplug eth0
iface eth0 inet static
        address 192.168.1.117
        netmask 255.255.255.0
        gateway 192.168.1.254
```

Enfin, nous modifier le fichier /etc/resolv.conf afin de pouvoir contacter le DNS Windows mis en place dans le contexte GSB :

```
  GNU nano 2.2.6              Fichier : /etc/resolv.conf

#domain sio.local
#search sio.local
#nameserver 192.168.1.49
#nameserver 192.168.1.50
#nameserver 8.8.8.8

domain GSB.local
search GSB.local
nameserver 192.168.1.130
```

Enfin, nous redémarrons la machine. Après cela, c'est le moment d'installer le service DNS Bind9 en utilisant la commande ***apt-get install bind9***. Des documents ont été ajouté à l'emplacement ***/etc/bind*** :

```
root@dnssec:/etc/bind# ls
bind.keys   db.255    db.root     named.conf.default-zones  rndc.key
db.0        db.empty  meszones    named.conf.local          zones.rfc1918
db.127      db.local  named.conf  named.conf.options
```

Le fichier de configuration qui nous intéresse est ici le ***/etc/bind/named.conf.options***, que nous modifions ainsi :

```
options {

check-names master warn; // Must be WARN only for AD

allow-notify {
localhost; AD_SERVER.IP.ADDRESS;
};

allow-transfer {
localhost; AD_SERVER.IP.ADDRESS;
};

dnssec-enable yes; //optional
dnssec-validation yes; // optional, can be yes or no
dnssec-lookaside auto; // MUST be auto for AD

};
```

Pour obtenir en résultat suivant, et ainsi autoriser le transfert des fichiers de zones DNS de l'AD sur notre machine, et activer les quelques prérequis à la sécurisation DNS :

```
        check-names master warn;
        allow-notify {
                localhost; 192.168.1.130;
        };
        allow-transfer {
                localhost; 192.168.1.130;
        };
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;
        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
};
```

Puis nous passons à la configuration du fichier ***/etc/bind/named.conf.local*** pour pouvoir récupérer nos fichiers de zones depuis l'AD :

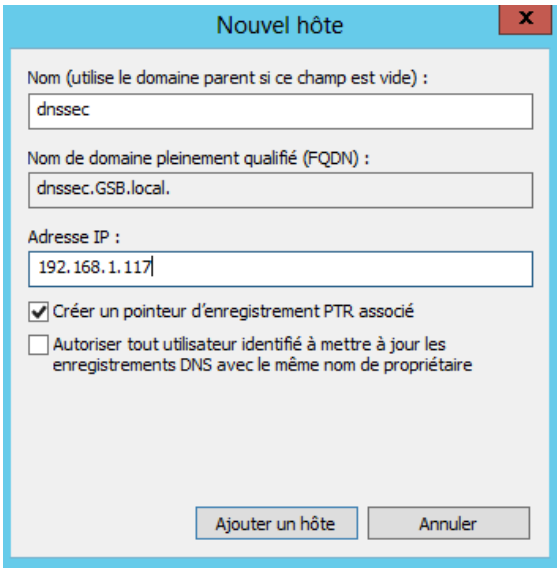
```
zone "GSB.local" IN {
        type slave;
        masters { 192.168.1.130; } ;
        file "/etc/bind/meszones/slave.zone.GSB.local";
};

zone "1.168.192.in-addr.arpa" IN {
        type slave;
        masters { 192.168.1.130; } ;
        file "/etc/bind/meszones/slave.1.168.192.in-addr.arpa";
};
```

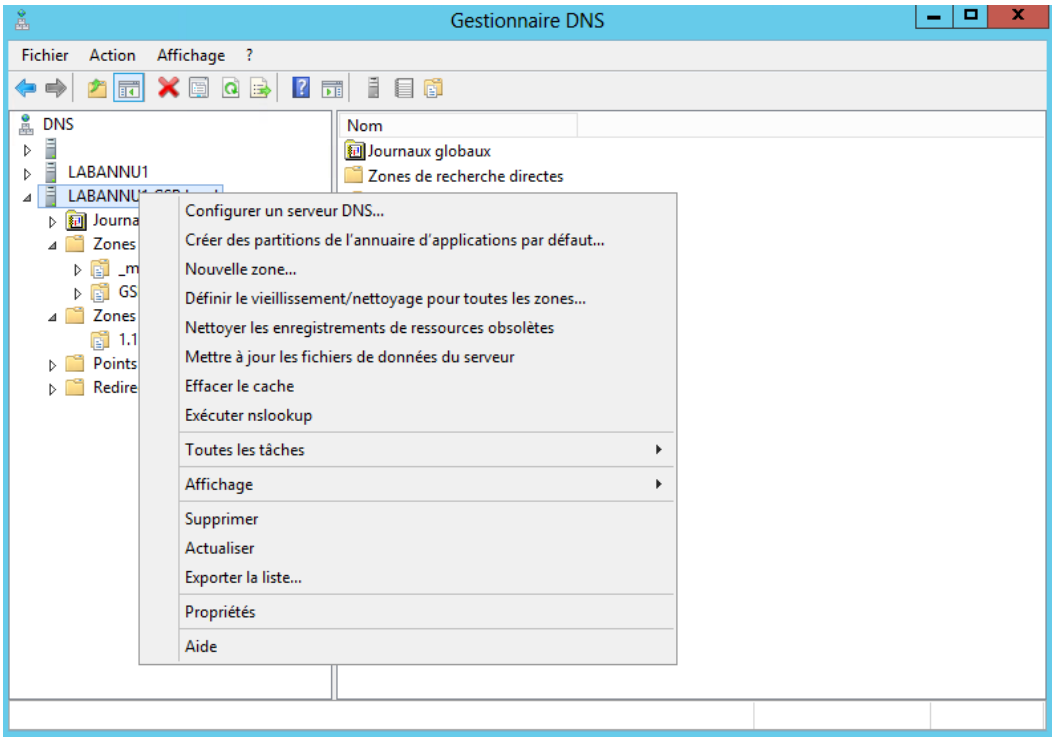
Il ne reste plus qu'à créer le répertoire /etc/bind/meszones, afin de récupérer les fichiers de zones, redémarrer le service bind9, et vérifier l'accès en écriture de bind9 sur les répertoires suivants : ***/etc/bind*** et ***/var/cache/bind.***

Configurer le DNS Maître - Windows :

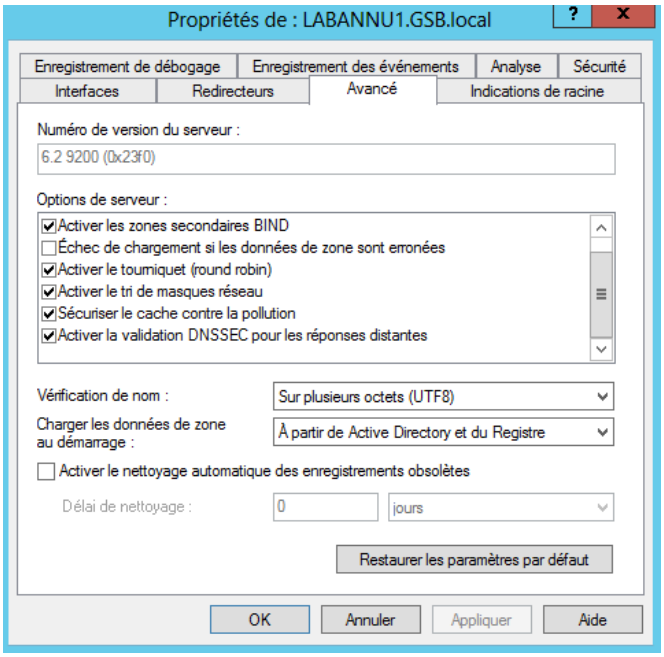
Il y a quelques modifications à réaliser sur le DNS Windows afin transmettre les fichiers de zones à notre serveur esclave déjà configuré. Tout d'abord, il est important d'ajouter un nouvel enregistrement de type A afin de résoudre le nom de notre nouveau serveur bind9 :



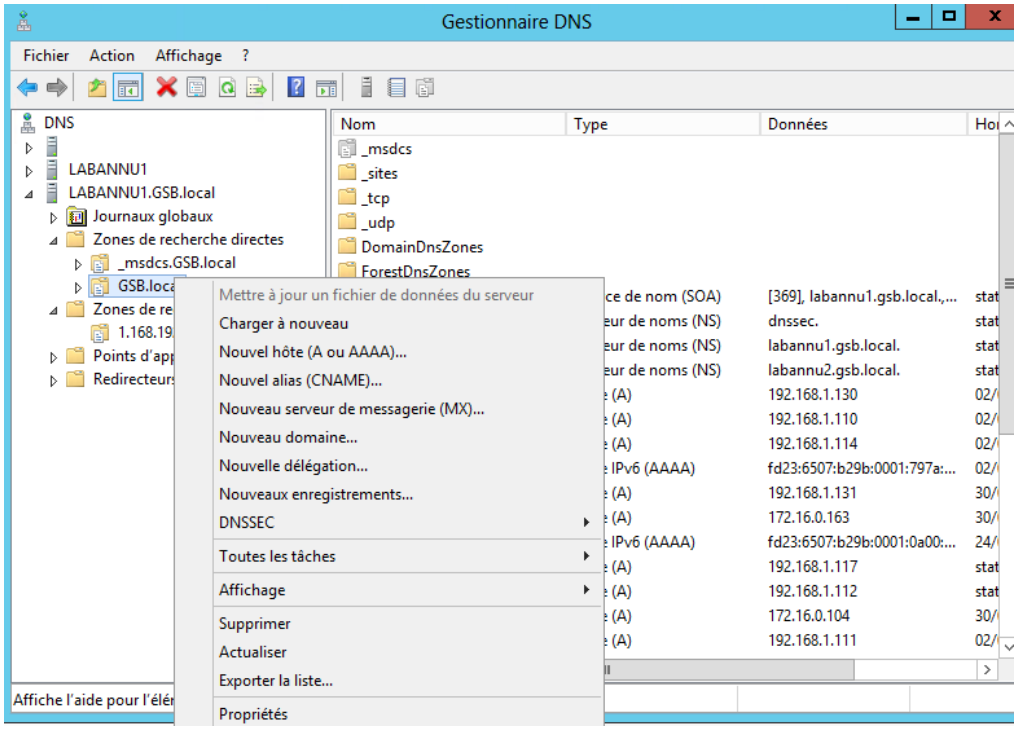
Une fois ceci fait, il faut faire un clic droit sur le serveur DNS principal, et cliquer sur « ***Propriétés*** » :



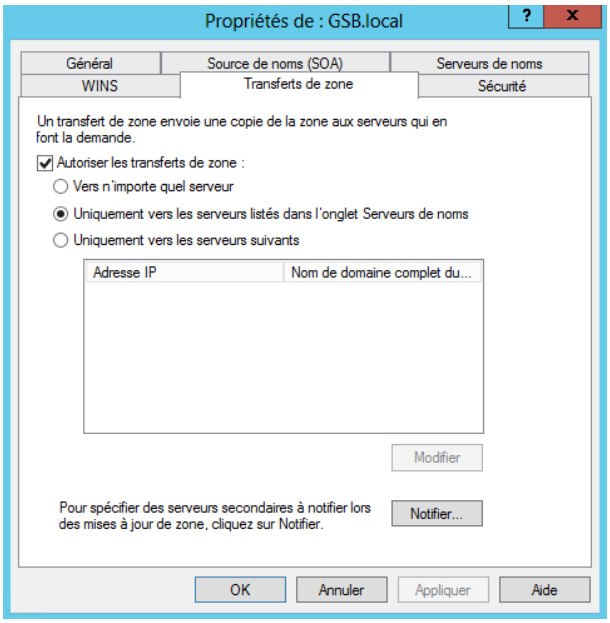
Puis, dans l'onglet « ***Avancé*** », il faut activer toutes les options ci-dessous, afin d'autoriser le transfert de zone vers les services Bind et le DNSSEC :



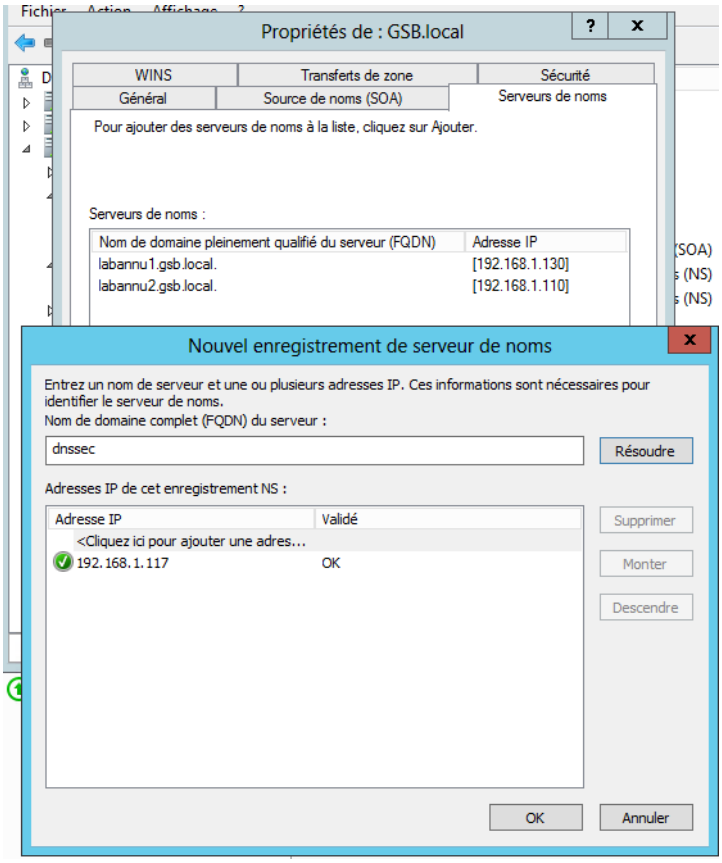
Une fois ceci appliqué, il faut maintenant configurer tous les fichiers de zones que nous voulons répliquer. Pour cela, il faut faire un clic droit dessus et cliquer sur « ***Propriétés*** » :



Dans l'onglet « ***Transferts de zone*** », il faut autoriser les transferts de zone vers les serveurs que nous ajouterons juste après dans l'onglet « ***Serveurs de noms*** » :



Nous ajoutons donc ensuite notre serveur esclave :



Pour obtenir le résultat suivant :

Serveurs de noms :

Nom de domaine pleinement qualifié du serveur (FQDN)	Adresse IP
dnssec.	[192.168.1.117]
labannu1.gsb.local.	[192.168.1.130]
labannu2.gsb.local.	[192.168.1.110]

Il faut ensuite répéter cette opération pour le fichier de zone inverse, et pour tout autre fichier que nous voulons répliquer, et le transfert de zone est finalement effectif sur notre serveur esclave :

```
Jun  6 08:57:06 dnssec named[776]: zone GSB.local/IN: Transfer started.
Jun  6 08:57:06 dnssec named[776]: transfer of 'GSB.local/IN' from 192.168.1.13$
Jun  6 08:57:06 dnssec named[776]: zone GSB.local/IN: TEST_SITUATIONP.GSB.local$
Jun  6 08:57:06 dnssec named[776]: zone GSB.local/IN: transferred serial 374
Jun  6 08:57:06 dnssec named[776]: transfer of 'GSB.local/IN' from 192.168.1.13$
Jun  6 08:57:06 dnssec named[776]: zone GSB.local/IN: sending notifies (serial $
Jun  6 08:57:07 dnssec named[776]: zone 1.168.192.in-addr.arpa/IN: Transfer sta$
Jun  6 08:57:07 dnssec named[776]: transfer of '1.168.192.in-addr.arpa/IN' from$
Jun  6 08:57:07 dnssec named[776]: zone 1.168.192.in-addr.arpa/IN: transferred $
Jun  6 08:57:07 dnssec named[776]: transfer of '1.168.192.in-addr.arpa/IN' from$
Jun  6 08:57:07 dnssec named[776]: zone 1.168.192.in-addr.arpa/IN: sending noti$
```

Et nous retrouvons nos fichiers de zones dans ***/etc/bind/meszones*** :

```
root@dnssec:/etc/bind/meszones# ls -l
total 8
-rw-r--r-- 1 bind bind  972 juin   6 09:00 slave.1.168.192.in-addr.arpa
-rw-r--r-- 1 bind bind 3091 juin   6 09:00 slave.zone.GSB.local
```

Nous testons la résolution dans les deux sens avec un ***nslookup*** :

```
root@dnssec:~# nslookup Anthony-PC
Server:         192.168.1.130
Address:        192.168.1.130#53

Name:   Anthony-PC.GSB.local
Address: 192.168.1.131
```

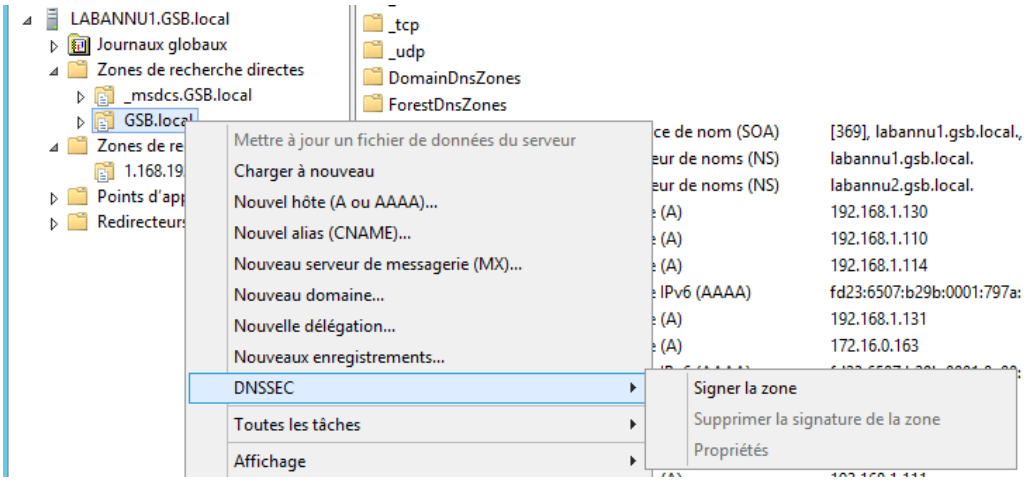
```
root@dnssec:~# nslookup 192.168.1.131
Server:         192.168.1.130
Address:        192.168.1.130#53

131.1.168.192.in-addr.arpa      name = anthony-pc.gsb.local.
```

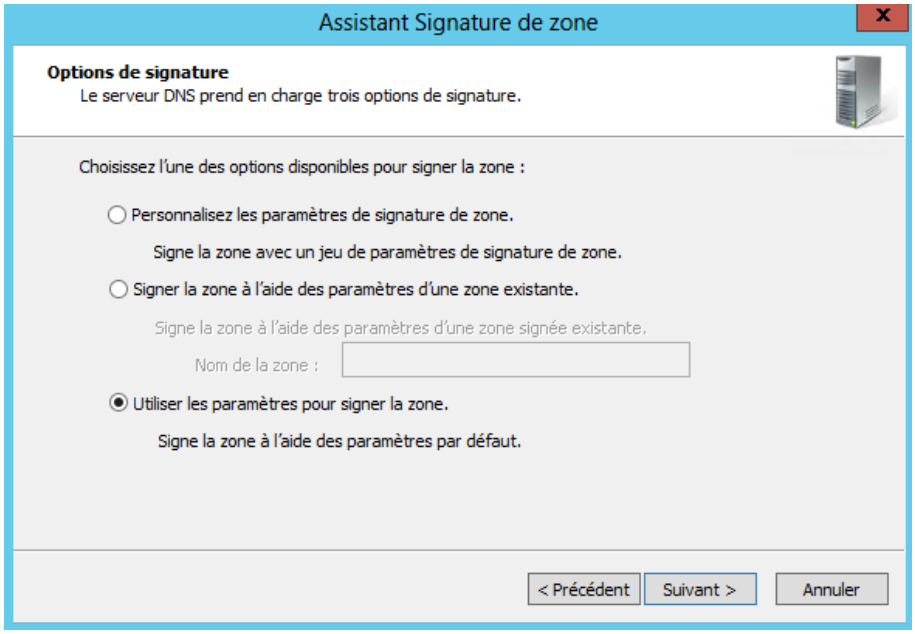
Tout fonctionne convenablement. Il ne nous reste plus qu'à sécuriser le transfert en activant DNSSEC sur les fichiers de zones de notre serveur Windows.

Activer le DNSSEC :

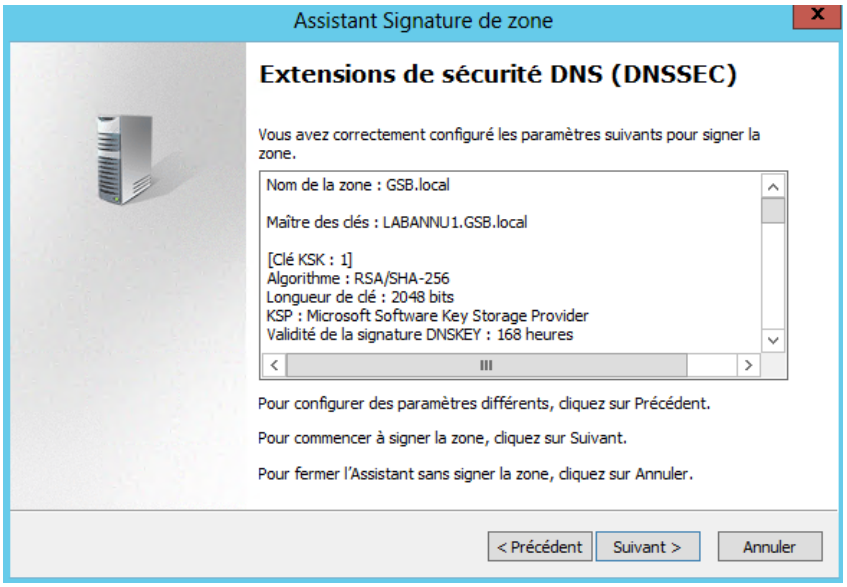
Pour activer la communication sécurisée entre les deux serveurs, il suffit de signer les zones que nous voulons transmettre de manière sécurisée, en faisant un clic droit sur ces zones, et en choisissant « ***DNSSEC*** » puis « ***Signer la zone*** » :



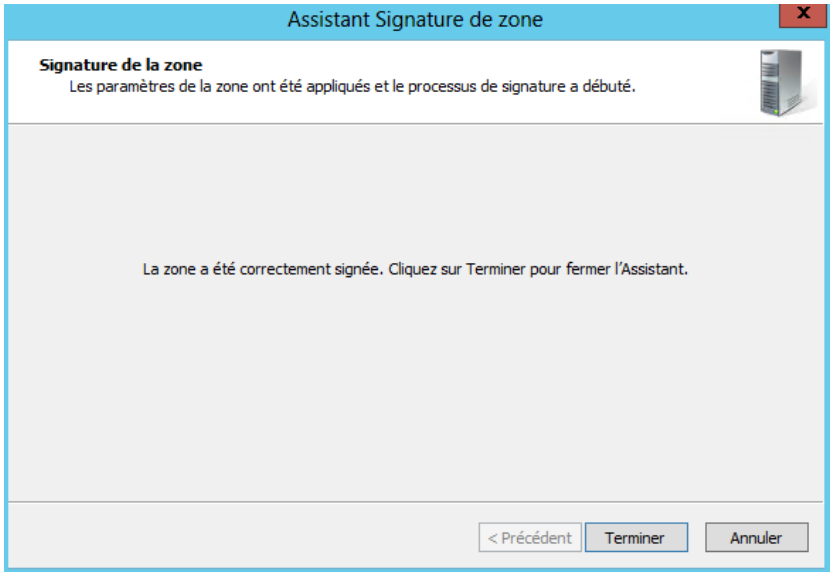
Ensuite, nous avons le choix de paramétrer la zone manuellement, ou automatiquement si vous souhaitez utiliser les paramètres par défaut :

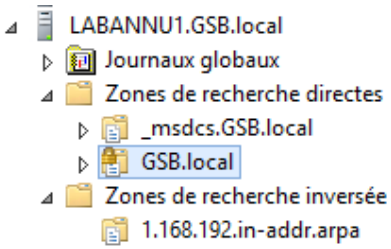


Un résumé de notre configuration est ensuite disponible à la fin de la configuration, il ne reste plus qu'à l'appliquer en cliquant sur « ***Suivant*** » :



Ainsi, notre zone DNS est signée, et cela est visible grâce au petit verrou qui vient d'apparaître sur la zone :





Il faut donc répéter cette action sur toutes les zones que nous souhaitons signer, puis quand cela est fait, il faut ajouter une petite modification au serveur esclave. En effet, il faut maintenant accéder au fichier ***/etc/bind/named.conf.local*** et ajouter un « ***.signed*** » à la fin de nos fichiers de zones afin de les différencier des fichiers non sécurisés :

```
zone "GSB.local" IN {
        type slave;
        masters { 192.168.1.130; } ;
        file "/etc/bind/meszones/slave.zone.GSB.local.signed";
};

zone "1.168.192.in-addr.arpa" IN {
        type slave;
        masters { 192.168.1.130; } ;
        file "/etc/bind/meszones/slave.1.168.192.in-addr.arpa.signed";
};
```

Et voici nos nouveaux fichiers de zone :

```
root@dnssec:/etc/bind/meszones# ls -l
total 44
-rw-r--r-- 1 bind bind  9318 juin   6 09:20 slave.1.168.192.in-addr.arpa.signed
-rw-r--r-- 1 bind bind 29150 juin   6 09:20 slave.zone.GSB.local.signed
```

Pour vérifier que la communication s'effectue avec le DNSSEC, nous utilisons la commande : ***dig DNSKEY GSB.local. @localhost +multiline***

```
root@dnssec:~# dig DNSKEY GSB.local. @localhost +multiline

; <<>> DiG 9.9.5-9+deb8u11-Debian <<>> DNSKEY GSB.local. @localhost +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31075
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;GSB.local.                     IN DNSKEY

;; ANSWER SECTION:
GSB.local.              3600 IN DNSKEY 257 3 8 (
                                AwEAAbtExK8blpNe++gHuvk4U29NH6cEag9Pw9LmHoSA
                                MaHhlBAsbaEviNeaaqEtkMp4v7R53xSjtyYJRvy3H3Li
                                swJ4ic37h0I+vIj7oBIGdqSlE08RtoCIt+5QbV4ACrXx
                                +AGIatW5E3vSuzHykLKMAV/FhMyPkOtisvCmkwaxtVO6
                                EaWlplXWuFC5YstYlZpSB+e3fJoRl2OUijX3brSbkbXT
                                PghduPbOKuO5plkotG2NO/k6sF8MiyQE3oShdQEg/GUn
                                mKCt3z+MBdNYmtqCfcygh8K84ckYzxlo4SsEBJe+brlf
                                qxF1jbwZIInG2fDKOigivlZItor/gr9G/C7K8/8=
                                ) ; KSK; alg = RSASHA256; key id = 55547
GSB.local.              3600 IN DNSKEY 256 3 8 (
                                AwEAAfsyL90OXkUC9vyiOAzh8hP/kk1djAHFKOvoJYP1
                                eKLWV/pOMkk6RJzcIdEOwJO5Z2nfiY2+6C/nOBBb6vIS
                                JO8Fz0r8aVsTnUGs8cRNWo0exJH4hVPk1cCNMmrJXVVH
                                ykwvJ5JRjGNgrP+/VDJf6xR/g73zMUqpDzgwAUWkTwL7
```

ANNEXES

DNS -> AD DNS Server

Right Click, Properties

Advanced Tab

Select the following options (ALL are required):

- Enable BIND secondaries
- Enable round robin (domain clients will fail to hit BIND otherwise)
- Enable netmask ordering
- Enable DNSSEC validation for remote responses (UNCHECK if feeding from non-DNSSEC BIND)
- Name checking: Multibyte (UTF8) or All Names
- Load zone data on startup: From Active Directory and registry
- Enable automatic scavenging should be checked
- Scavenging period should be set appropriately

Root Hints **MUST BE UPDATED MANUALLY**. You can use the "Resolve" button to do this.

Forward Lookup Zone -> EXAMPLE.COM

- Do NOT add BIND to Name Servers (yet)
- Zone Transfers -> Allow zone transfers
- Zone Transfers -> Only to servers listed on the Name Servers tab
- Apply Changes
- Name Servers -> Add BIND servers one at a time
- If accepting dynamic updates from BIND (nsupdate), TSIG or GSS must be configured for Secure only updating

Forward Lookup Zone -> _msdcs.EXAMPLE.COM

- Repeat the same steps as in EXAMPLE.COM
- Dynamic updates must be **Secure Only**

Reverse Lookup Zone -> 0.0.10.in-addr.arpa (repeat for all reverse zones)

- Repeat as in EXAMPLE.COM
- Security -> "Everyone" must have Read allowed

Pour sécuriser, activer le DNSSEC sur la zone directe et inverse sur l'AD DS.
Et ajouter .signed à la fin des fichiers de zones sur Debian.

Et tester avec :

```
dig DNSKEY GSB.local. @localhost +multiline
```

https://www.digitalocean.com/community/tutorials/how-to-setup-dnssec-on-an-authoritative-bind-dns-server--2