06/06/2017

Sommaire :

Sommaire :	1
Introduction	1
Configurer le DNS Esclave - Debian :	2
Configurer le DNS Maître - Windows :	4
Activer le DNSSEC :	8
ANNEXES	. 11

Introduction

<u>Objectif :</u> 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.

<u>Pré-requis :</u> 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 \rightarrow Permet de vérifier les fichiers de configuration. **named-checkzone domaine fichier** \rightarrow Permet de vérifier les fichiers de zones.

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

06/06/2017

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 r	network interface
allow∙	-hotplug e	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@dnsse	c:/etc/bin	d# ls		
bind.keys	db.255	db.root	named.conf.default-zones	rndc.key
db.O	db.empty	meszones	named.conf.local	zones.rfc1918
db.127	db.local	named.conf	named.conf.options	

06/06/2017

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 :

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.

06/06/2017

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 :

Nouvel hôte X
Nom (utilise le domaine parent si ce champ est vide) :
dnssec
Nom de domaine pleinement qualifié (FQDN) :
dnssec.GSB.local.
Adresse IP :
192.168.1.117
Créer un pointeur d'enregistrement PTR associé
Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire
Ajouter un hôte Annuler

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

	– E4		
DETROZS	Sébastien	Version 1	06/06/2017

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 :

	roprice	és de : L	ABANNU1.GS	SB.loc	al	? X
Enregistrement de dél	bogage	Enregistre	ement des événem	ents	Analyse	Sécurité
Interfaces Redirecteurs Avancé Indications de racine						
Numéro de version d	u serveur :					
6 2 9200 (0x23f0)	a servear .					
0.2 0200 (at2010)						
Options de serveur :						
Activer les zones	secondaire	s BIND				~
Échec de charger	ment si les	données d	e zone sont erroné	es		
Activer le toumiqu	et (round r	obin)				
Activer le tri de ma	asques rése	eau				≡
Sécuriser le cache	e contre la	pollution				
Activer la validation	n DNSSE	C pour les r	éponses distantes			
						×
Vérification de nom :		Surp	lusieurs octets (U1	(F8)		¥
Charger les données	de zone	٨	tir da Activa Diract	on ot a	lu Docistro	
au démarrage :		Apa	ui de Active Direct	lory et d	u negisire	¥
Activer le nettoya	ge automat	ique des e	nregistrements obs	olètes		
Dábi do pottouro		0				
Delai de riettoyag	je.	U	Jours			~
			Restaurer I	es para	mètres par o	défaut

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* » :

å.		Gestionnaire	DNS		_ □	x
Fichier Action Afficha	ige ?					
(= =) 🖄 🖬 🗙 🗉	2 🗟 🖸					
DNS LABANNU1 LABANNU1.GSB.loc LABANNU1.GSB.loc I Journaux globau Zones de recher GSB.locc Cons de re Points d'app Points d'app Redirecteurs	al IX Che directes Iocal Mettre à jour u Charger à nou Nouvel hôte (/ Nouvel alias (C Nouveau serve Nouveau dom Nouvela diég Nouveaux enre DNSSEC Toutes les tâch Affichage Supprimer A studiore	Nom 	Тур •	ce de nom (SOA) sur de noms (NS) sur de noms (NS) sur de noms (NS) (A) (A) (A) (A) (A) (A) (A) (A) (A) (A	Données [369], labannu1.gsb.local., dnssec. labannu1.gsb.local. labannu2.gsb.local. 192.168.1.130 192.168.1.110 192.168.1.114 fd23:6507:b29b:0001:797a: 192.168.1.131 172.16.0.163 fd23:6507:b29b:0001:0a00: 192.168.1.117 192.168.1.112 172.16.0.104 192.168.1.111	Hot ^ stat stat 22/ 02/ 02/ 02/ 02/ 02/ 02/ 02/ 30/ 24/ stat stat 30/ 02/ 24/
	Exporter la list	e		I		>
Affiche l'aide pour l'élér	Propriétés					

	Situation Professionnelle – DNS Secondaire Sécurisé – E4			
DETROZ Sébastien	Version 1	06/06/2017		

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* » :

	Propriétés	s de : GSB.loc	al	?	x		
Général	Sauraa da na	ma (SOA)	Conversion				
WINS	Transfe	Transferts de zone					
Un transfert de zone envoie une copie de la zone aux serveurs qui en font la demande.							
Autoriser les trans	ferts de zone :						
O Vers n'importe	quel serveur						
Uniquement ve	ers les serveurs listés	dans l'onglet Serv	eurs de noms				
O Uniquement ve	ers les serveurs suiva	nts					
Adresse IP		Nom de domaine	complet du				
Pour spécifier de des mises à jour	s serveurs secondaire de zone, cliquez sur N	es à notifier lors Notifier.	Modifier Notifier				
	ОК	Annuler	Appliquer	Ai	de		

Nous ajoutons donc ensuite notre serveur esclave :

chior_	Action Affichage					
		Propriétés de : GSB.loo	cal	?	x	
D	WINS	Transferts de zone	Sécu	urité		
	Général	Source de noms (SOA)	Serveurs de	e noms		
	Pour ajouter des serve	urs de noms à la liste, cliquez sur Aj	outer.			
1	Serveurs de noms :					
	Nom de domaine pleir	nement qualifié du serveur (FQDN)	Adresse IP			Isc
4	labannu1.gsb.local.		[192.168.1.130]			
¢	labannu2.gsb.local.		[192.168.1.110]			5 (1
	Nour	ver enregistrement de serv	reur de noms			
Entre	z un nom de serveur et u ifier le serveur de noms.	une ou plusieurs adresses IP. Ces in	nformations sont néc	essaire	s pour	
Entre identi Nom (ez un nom de serveur et u ifier le serveur de noms, de domaine complet (FQI	une ou plusieurs adresses IP. Ces in DN) du serveur :	nformations sont néc	essaire	s pour	
Entre identi Nom o dnss	z un nom de serveur et u ifier le serveur de noms. de domaine complet (FQI sec	une ou plusieurs adresses IP. Ces in DN) du serveur :	nformations sont néc	essaire	s pour Résou	dre
Entre identi Nom o dnss Adres	zz un nom de serveur et u ifier le serveur de noms. de domaine complet (FQI sec sses IP de cet enregistre	une ou plusieurs adresses IP. Ces in DN) du serveur : ment NS :	nformations sont néc	essaire	s pour Résou	dre
Entre identi Nom o dnss Adres	ez un nom de serveur et u ifier le serveur de noms, de domaine complet (FQI sec sses IP de cet enregistre esse IP	une ou plusieurs adresses IP. Ces in DN) du serveur : ment NS : Validé	nformations sont néc		s pour Résou Suppri	dre mer
Entre identi Nom o dnss Adres	z un nom de serveur et u ifier le serveur de noms, de domaine complet (FQI sec sses IP de cet enregistrei esse IP <cliquez ajouter<="" ici="" pour="" td=""><td>une ou plusieurs adresses IP. Ces in DN) du serveur : ment NS : Validé une adres</td><td>nformations sont néc</td><td></td><td>s pour Résou Suppri</td><td>dre mer</td></cliquez>	une ou plusieurs adresses IP. Ces in DN) du serveur : ment NS : Validé une adres	nformations sont néc		s pour Résou Suppri	dre mer
Entre identi Nom o dnss Adres	z un nom de serveur et u ifier le serveur de noms, de domaine complet (FQI sec sses IP de cet enregistre esse IP <cliquez ajouter<br="" ici="" pour="">192.168.1.117</cliquez>	une ou plusieurs adresses IP. Ces in DN) du serveur : ment NS : Validé une adres OK	nformations sont néc		s pour Résou Suppri	dre mer er
Entre identi Nom o drss Adres	z un nom de serveur et u ifier le serveur de noms, de domaine complet (FQI sec sses IP de cet enregistre esse IP <cliquez ajouter<br="" ici="" pour="">192.168.1.117</cliquez>	une ou plusieurs adresses IP. Ces in DN) du serveur : ment NS : Validé une adres OK	nformations sont néc		s pour Résou Suppri Mont	dre mer er
Entre identi Nom dnss Adres Adres	z un nom de serveur et u ifier le serveur de noms, de domaine complet (FQI sec sses IP de cet enregistrei esse IP <cliquez ajouter<br="" ici="" pour="">192.168.1.117</cliquez>	une ou plusieurs adresses IP. Ces in DN) du serveur : ment NS : Validé une adres OK	nformations sont néc		s pour Résou Suppri Mont Descer	dre mer er
Entre identi Nom dnss Adres	z un nom de serveur et u ifier le serveur de noms, de domaine complet (FQI sec sses IP de cet enregistre esse IP <cliquez ajouter<br="" ici="" pour="">192.168.1.117</cliquez>	une ou plusieurs adresses IP. Ces in DN) du serveur : ment NS : Validé une adres OK	formations sont néc		s pour Résou Suppri Mont Descer	dre mer er
Entre identi Nom dnss Adres	z un nom de serveur et u ifier le serveur de noms, de domaine complet (FQI sec sses IP de cet enregistrei resse IP «Cliquez ici pour ajouter 192.168.1.117	une ou plusieurs adresses IP. Ces in DN) du serveur : ment NS : Validé une adres OK	formations sont néc		s pour Résou Suppri Mont Descer	dre mer er ndre
Entre identi Nom dnss Adres	zz un nom de serveur et u tifer le serveur de noms, de domaine complet (FQI sec sses IP de cet enregistre resse IP <cliquez ajouter<br="" ici="" pour="">192.168.1.117</cliquez>	une ou plusieurs adresses IP. Ces in DN) du serveur : ment NS : Validé une adres OK	formations sont néc		s pour Résou Suppri Mont Descer	dre mer er ndre
Entre identi Nom dns: Adres	zz un nom de serveur et u ifier le serveur de noms, de domaine complet (FQI sec sses IP de cet enregistre resse IP <cliquez ajouter<br="" ici="" pour="">192. 168. 1. 117</cliquez>	une ou plusieurs adresses IP. Ces in DN) du serveur : ment NS : Validé une adres OK	formations sont néc		s pour Résou Suppri Mont Descer	dre mer er ndre
Entre identi Nom dns: Adres	zz un nom de serveur et u ifier le serveur de noms, de domaine complet (FQI sec sses IP de cet enregistre resse IP <cliquez ajouter<br="" ici="" pour="">192. 168. 1. 117</cliquez>	une ou plusieurs adresses IP. Ces in DN) du serveur : ment NS : Validé une adres OK	formations sont néc		s pour Résou Supprii Mont	dre mer er ndre
Entre identi Nom i dns: Adres	zz un nom de serveur et u ifier le serveur de noms, de domaine complet (FQI sec sses IP de cet enregistre esse IP <cliquez ajouter<br="" ici="" pour="">192. 168. 1. 117</cliquez>	une ou plusieurs adresses IP. Ces in DN) du serveur : ment NS : Validé une adres OK	formations sont néc		s pour Résou Suppri Mont	dre mer er ndre
Entre identi Nom drss Adres Adres	zz un nom de serveur et u ifier le serveur de noms. de domaine complet (FQI sec sses IP de cet enregistre esse IP <cliquez ajouter<br="" ici="" pour="">192. 168. 1. 117</cliquez>	une ou plusieurs adresses IP. Ces in DN) du serveur : ment NS : Validé une adres OK	formations sont néc		s pour Résou Suppri Mont	dre mer er ndre

06/06/2017

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\$
Iun	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/k	oind∕⊓	neszor	ies# .	ls	-1		
total 8									
-rw-rr	1	bind	bind	972	juin		6	09:00	slave.1.168.192.in-addr.arpa
-rw-rr	1	bind	bind	3091	juin		6	09:00	slave.zone.GSB.local

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

ro Se Ac	oot@dnssec:~# ns erver: 19 ddress: 19	lookup A 92.168.1 92.168.1	nthony-PC .130 .130#53	
Na Ac	ame: Anthony–Pi ldress: 192.168.3	C.GSB.lo 1.131	cal	
root@dnssec:~# Server: Address:	nslookup 192.168 192.168.1.130 192.168.1.130#5	3.1.131 53		
131.1.168.192.	in–addr.arpa	name =	anthony-pc.g	sb.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.

DETROZ Sébastien

Version 1

06/06/2017

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 :

Assistant Signature de zone	X
Options de signature Le serveur DNS prend en charge trois options de signature.	
Choisissez l'une des options disponibles pour signer la zone :	
O Personnalisez les paramètres de signature de zone.	
Signe la zone avec un jeu de paramètres de signature de zone.	
\bigcirc Signer la zone à l'aide des paramètres d'une zone existante.	
Signe la zone à l'aide des paramètres d'une zone signée existante,	
Nom de la zone ;	
 Utiliser les paramètres pour signer la zone. 	
Signe la zone à l'aide des paramètres par défaut.	
< Précédent Suivant >	Annuler

DETROZ Sébastien	Version 1	06/06/2017

Situation Professionnelle – DNS Secondaire Sécurisé – E4

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 :

Assistant Signature de zone	×
Signature de la zone Les paramètres de la zone ont été appliqués et le processus de signature a débuté.	The second
La zone a été correctement signée. Cliquez sur Terminer pour fermer l'Assistant.	
< Précédent Terminer	Annuler
 LABANNU1.GSB.local Journaux globaux Zones de recherche directes _msdcs.GSB.local GSB.local Zones de recherche inversée 1.168.192.in-addr.arpa 	

DETROZ Sébastien Version 1 06/06/2017	

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 :



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 (
                                AwEAAbtExK8b1pNe++gHuvk4U29NH6cEag9Pw9LmHoSA
                                MaHh1BAsbaEviNeaaqEtkMp4v7R53xSjtyYJRvy3H3Li
                                swJ4ic37h0I+vIj7oBIGdqS1E08RtoCIt+5QbV4ACrX
                                 +AGIatW5E3vSuzHykLKMAV/FhMyPkOtisvCmkwaxtV06
                                EaWlp1XWuFC5YstY1ZpSB+e3fJoR120UijX3brSbkbXT
                                 PghduPbOKuO5p1kotG2NO/k6sF8MiyQE3oShdQEg/GUn
                                mKCt3z+MBdNYmtqCfcygh8K84ckYzxlo4SsEBJe+brlf
                                 qxF1jbwZIInG2fDK0igivlZItor/gr9G/C7K8/8=
                                 ) ; KSK; alg = RSASHA256; key id = 55547
                        3600 IN DNSKEY 256 3 8
GSB.local.
                                 AwEAAfsyL900XkUC9vyi0Azh8hP/kk1djAHFKOvoJYP1
                                 eKLWV/pOMkk6RJzcIdE0wJ05Z2nfiYZ+6C/n0BBb6vIS
                                 JO8Fz0r8aVsTnUGs8cRNWo0exJH4hVPk1cCNMmrJXVVH
                                 ykwvJ5JRjGNgrP+/VDJf6xR/g73zMUqpDzgwAUWkTwL*
```

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