DNS Session 3: Configuration du serveur autoritaire

Alain Patrick AINA

Grégoire EHOUMI

AFNOG 2014, Djibouti, Djibouti

RECAPITULATION

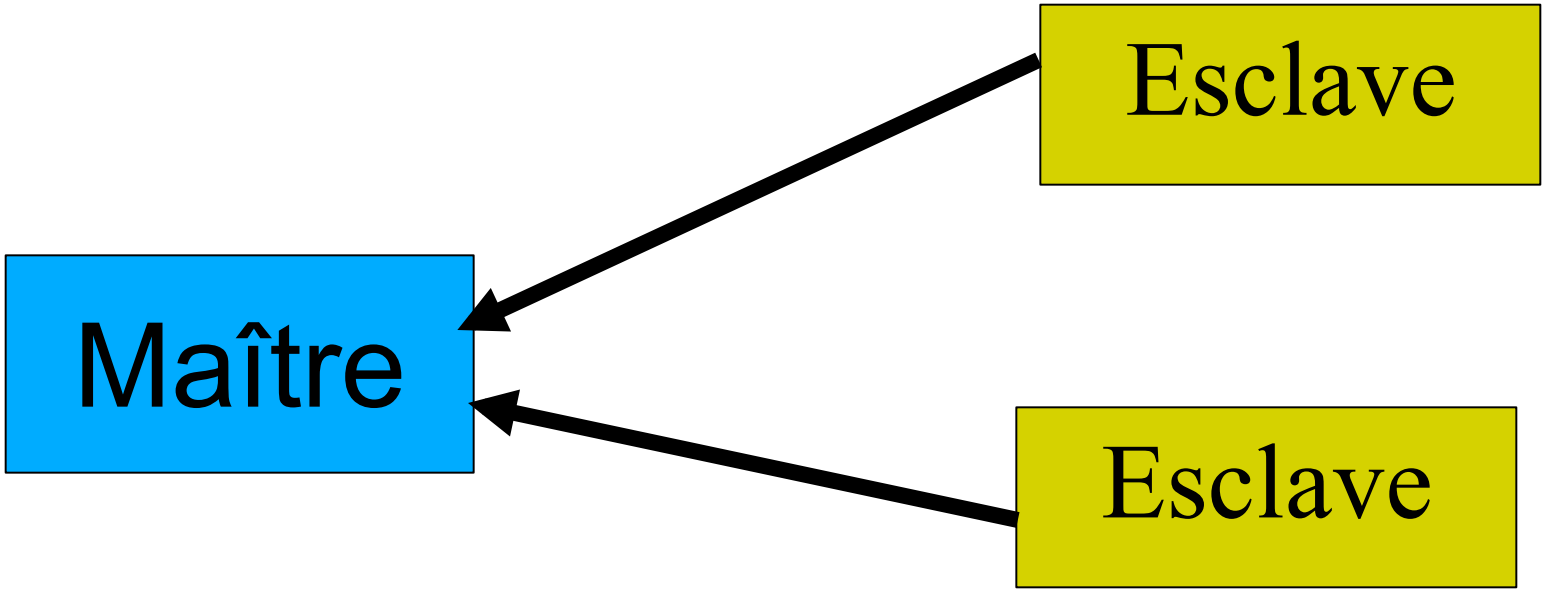
- Le DNS est une base de données distribuée
- Le resolver s'adresse au serveur Cache pour l'information
- Le cache traverse l'arborescence du DNS pour trouver le serveur autoritaire qui a l'information demandée.
- Une mauvaise configuration des serveurs autoritaires peut aboutir à la panne du domaine

REPLICATION DNS

- Pour chaque domaine, nous avons besoin de plus d'un serveur autoritaire avec la même information (RFC 2182)
- Les données sont enregistrées sur un seul serveur (le maître) et répliquées sur les autres (les esclaves)
- Le monde extérieur ne peut faire la différence entre le maître et le slave
  - Les enregistrements NS sont retournés de façon aléatoire pour le partage de charge égal

Sont appelés le " primaire " et " le secondaire " le secondaire?

Les esclaves se connectent au maître pour rechercher la copie des données de la zone



- Le maître ne dépose de données sur les esclaves

Quand est ce que la réplique a lieu ?

- L'esclave scrute le maître périodiquement– appelé ``Temps de rafraîchissement``
  - A l'origine c'était le seul mécanisme
- Avec les nouveaux logiciels, le maître peut aussi notifier les esclaves quand les données changent
  - Aboutit à des mises à jours plus rapides
- La notification est incertaine (ex. le réseau peut perdre le paquet) ainsi nous avons toujours besoin de contrôler l'intervalle de rafraîchissement

Le numéro de série

- Chaque fichier de zone a un numéro de série (Serial Number)
- L'esclave seul copiera les données quand le numéro AUGMENTE
  - Les requêtes UDP périodiques pour vérifier le numéro de série
  - S'il a augmenté, le transfert TCP des données de zone
- C'est votre responsabilité d'augmenter le numéro de série après chaque changement, autrement les esclaves et le maître seront contradictoires

Format de numéro de série recommandé: AAAAMMJJNN

- AAAA = Année
- MM = mois (01-12)
- JJ = jour (01-31)
- NN = numéro de changement du jour (00-99)
  - Ex. Si vous changez le fichier le 27 mai 2014, le numéro de série sera 2014052701. Si vous le changez encore une fois le même jour, ce sera 2014052701

Numéro de série: Danger 1

- Si jamais vous diminuez le numéro de série, les esclaves ne se mettront plus jamais à jour jusqu'à ce que le numéro de série aille au dessus de sa précédente valeur
- Au pire, vous devez entrer en contact avec tous vos esclaves et obtenir d'eux de supprimer leur copie des données de zone

Numéro de série: Danger 1

- Le numéro de série est un nombre de 32 bits non signé
- Choix : 0 à 4294967295
- Toute valeur plus grande que celle-ci est silencieusement tronquée
- Ex. 20040303000 (noté un chiffre extra)
  - = 4AA7EC198 (hex)
  - = AA7EC198 (32 bits)
  - = 2860433816
- Si vous faites cette erreur, alors corriger la, le numéro de sérié aura diminué

Configuration du Maître

- /etc/bind/named.conf.local pointe sur le fichier de zone (créé manuellement)
- Choisissez un emplacement logique pour le garder
- Ex. /etc/bind/m/example.com
- Ou /etc/bind/m/com.example

```
Zone "example.com" {
        type master;
        file"/m/example.com";
Allow-transfer { 192.188.58.126; 192.188.58.2; };
};
```

Configuration de l'esclave

- /etc/bind/named.conf pointe sur l'adresse IP du maître et l'emplacement du fichier de zone

- Les fichiers de zone sont transférés automatiquement

```
Zone "example.com" {
        type slave;
        masters { 192.188.58.126; }
        file "s/example.com";
        allow-transfer  { none;};
};
```

Maître et esclave

- Il est parfaitement bien pour qu'un serveur soit principal pour les zones et esclave pour d'autres

- C'est pourquoi nous recommandons de maintenir les fichiers dans répertoires différents
  - /etc/bind/m
  - /etc/bind/s

allow-transfer { ....; }

- Les machine à distance peuvent demander un transfert du contenu entier de zone
- Par défaut, ceci est autorisé à n'importe qui
- Vaut mieux de limiter ceci
- Vous pouvez en fixer un par défaut, et passer autre ceci pour chaque zone s'il y a lieu.

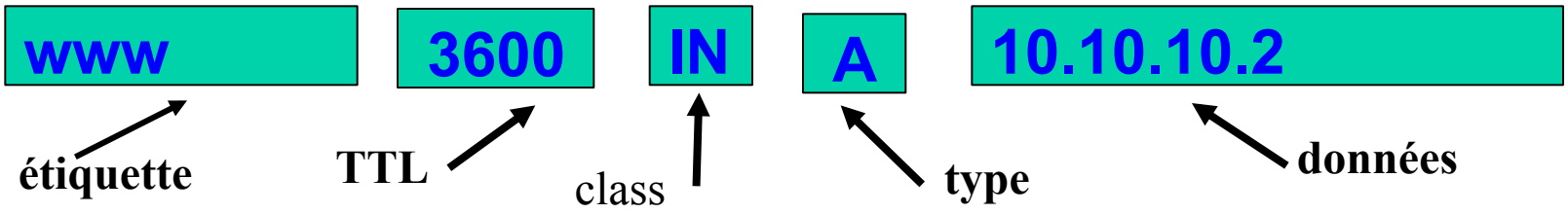
```
Options {
        allow-transfer  { 127.0.0.1; };
};
```

La structure d'un fichier de zone

- Options globales
  - $TTL 1d
  - Fixe le TTL par défaut pour tous les enregistrements
- ER SOA
  - "Start Of Authority"
  - Gère les informations pour la zone
- Les ERs NS
  - Listent les serveurs de noms de la zone, le maître et les esclaves
- Les autres ERs
  - Les données réelles que souhaitez publier

Format des Enregistrements de Ressources (ERs)

- Un par ligne (excepté SOA qui peut se prolonger au-delà de plusieurs lignes)
- Si vous omettez le nom de domaine, c'est pareil que la ligne précédente
- Les raccourcis TTL : Ex. 60s, 30m, 4h, 1w2d
- Si vous omettez le TTL, il prend la valeur $TTL par défaut
- Si vous omettez la Classe (Class), il se transfère en IN
- Le type et les données ne peuvent pas être omis
- Les commentaires commencent avec le Point-virgule (;)



Les raccourcis

- Si le nom de domaine ne se termine pas un point, le propre domaine de la zone ("origin") est ajouté
- Un nom de domaine de "@" signifie l'origine elle-même
- Ex. dans le fichier de zone de example.com
  - @ signifie example.com.
  - www signifie www.example.com.

Si vous écrivez ceci

```
$TTL 1d
@                       SOA ( . . . . )
                        NS      ns0
                        NS      ns0.as9105.net.
;Serveur de messagerie et web
www                     A       212.74.12.80
                        MX      10 mail
```

Il devient ceci

example.com	**86400**	**IN**	**SOA (. . .)**	
example.com	86400	IN	NS	ns0.**example.com.**
example.com	86400	IN	NS	ns0.as91504.net.
www.example.com.	86400	IN	A	212.74.112.80
www.example.com.	86400	IN	MX	10 mail**.example.com.**

Format de l'enregistrement SOA

```
$TTL 1d
@    1h      IN  SOA    ns1.example.net.   brian.nsrc.orig. (
                        2004030300     ;Serial
                        8h       ;Refresh
                        1h       ;Retry
                        4w       ;Expire
                        1h)      ;Negative
                IN  NS  ns1.example.net.
                IN  NS  ns2.example.net.
                IN  NS  ns1.othernetwork.com.
```

Format de l'enregistrement SOA

- ns1.example.net
  - Nom d'hôte du serveur maître
- greg.afnog.org.
  - L'adresse électronique de la personne responsable, avec @ changé en point
- Numéro de série (serial Number)
- Intervalle de rafraîchissement (Refresh interval)
  - Combien de fois l'esclave vérifie le numéro de série sur le maître
- Intervalle de nouvelle tentative (Retry Interval)
  - Combien de fois l'esclave vérifie le numéro de série si le maître ne répond pas

Format de l'enregistrement SOA

- Temps d'expiration (Expiry time)
- Si l'esclave ne peut entrer en contact avec le maître pour cette période, il supprimera sa copie de données de zone
- Negative / Minimum
  - L'ancien logiciel utilisait ceci comme valeur minimum de TTL
  - Maintenant, ceci est utilisé pour la cache négatif: indique combien de temps le cache peu stocker la non-existence d'un ER
- RIPE-2003 a recommandé les valeurs
  - http://www.ripe.net/ripe/docs/dns-soa.html

Format de l'enregistrement NS

```
$TTL 1d
@       1h   IN   SOA      ns1.example.net.   Brian.nsrc.org. (
                            2004030300   ; Serial
                            8h           ; Refresh
                            1h           ; Retry
                            4w           ; Expiry
                            1h)          ; negative
              IN   NS   ns1.example.net.
              IN   NS   ns2.exaple.net.
              IN   NS   ns1.othernotwork.com.
```

- **Liste tous les serveurs de noms autoritaires de la zone maître et les esclaves**
- **Doit pointer sur le nom d'hôte non sur l'adresse IP**

Format des autres ERs

- IN A 1.2.3.4
- IN MX 10 mailhost.example.com
  - Le nombre est une "valeur de préférence". Le courrier est délivré au plus petit nombre MX en premier
  - Doit pointer sur le NOM d'HÔTE , non sur l'adresse IP
- IN CNAME host.example.com.
- IN PTR host.example.com
- IN TXT "tout texte que vous aimez"

Quand vous avez ajouté ou changé le fichier de zone

- Vérifiez le numéro de série
- Named-checkzone example.com /etc/bind/m/example.com
  - Dispositif de Bind 9
  - Il rapporte les erreurs de synrax; corrige les
- rndc reload
  - ou : rndc reload exemple.com
- Tail /var/log/syslog

Ces vérifications sont essentielles

- Si vous avez une erreur dans le fichier named.conf ou le fichier de zone, named continuera de fonctionner mais ne sera pas autoritaire pour la mauvaise zone(s)
- Vous serez "lame" une boiteuse pour la zone sans le réaliser
- Les esclaves ne pourront pas contacter les maîtres
- par la suite (ex. pendant 4 semaines plus tard) les esclaves s'expireront la zone
- Votre domaine arrêtera de travailler

D'autres vérifications que vous pouvez faire

- Dig +norec @x.x.x.x example.com. Soa
- Vérifie le drapeau AA
- Vérifie le maître et tous les esclaves
- Vérifie que les numéro de séries correspondent
- Dig @x.x.x.x example.com. Axfr
- "Transfert autoritaire"
- Demande la copie complète du contenu de la zone à travers le TCP, comme les esclaves le font pour le maître
- Ceci fonctionnera uniquement à partir des adresses IP énumérés dans la section de : allow-transfert { .....}

Donc maintenant, vous avez des serveurs autoritaires fonctionnels

- Mais rappeler vous qu'aucun d'eux ne fonctionnera jusqu'à ce que vous ayez la délégation du domaine au-dessus de vous.
- C'est : Il mettront les enregistrements pour votre domaine en pointant vers votre serveurs de noms
- Vous mettrez aussi les enregistrements NS dans votre fichier de zone
- Les deux éléments doivent correspondances

Les 10 erreurs principales dans les serveurs autoritaires

- Tous les opérateurs des serveurs autoritaires doivent lire le RFC 1912
  - L'opération commun du DNS et les erreurs de configuration
- Voir aussi le RFC 2182
  - Sélection et l'opération des serveurs DNS secondaires

Les erreurs de numéro de série

- Oublier d'incrémenter le numéro de série
- Incrémenter le numéro de série puis le décrémenter
- Utiliser le numéro de série plus grand que 2^{32}
- Impact :
  - Les esclaves ne sont pas à jour
  - Le maître et les esclaves ont des données contradictoires
  - Les caches obtiennent parfois les nouvelles données et parfois les anciennes – Problème intermittent

Les commentaire dans les fichiers de zone commencent avec " # " au lieu de " ; "

- Erreur de syntaxe dans le fichier de zone
- Le maître n'est plus autoritaires pour la zone
- Les esclaves ne peuvent pas vérifier le SOA
- Les esclaves par la suite expirent la zone, et votre domaine cesse de fonctionner entièrement
- utilisez 'named-checkzone"
- utilisez "tail /var/log/messages"

Manque du point de fin

```
;    zone example.com.
@  IN  MX     10 mailhost.example.com
```

devient

```
@  IN  MX     10      mailhost.example.com.example.com.
```

```
; zone  2.0.192.in-addr.arpa.
1    IN  PTR    host.example.com
```

devient

```
1    IN  PTR    host.example.com.2.0.192.in-addr.arpa.
```

Les enregistrements NS et MX pointent vers les adresses IP

- Ils doivent pointer vers les nom d'hôtes, pas vers les adresses
- Malheureusement, quelques serveurs de messagerie acceptent des adresses IP dans les enregistrements MX, Ainsi vous ne pouvez pas voir un problème avec tous les sites à distance

Les esclaves ne peuvent pas transférer la zone du maître

- Accès limité par allow-transfer { ....} et les esclaves ne sont pas listés.
- Ou les filtres IP ne sont pas correctement bien configurés
- L'esclave sera boiteuse (lame server) car non autoritaire

Délégation boiteuse –Lame delegation

- Vous ne pouvez pas lister simplement n'importe quel serveur de noms dans des enregistrements NS pour votre domaine
- Vous devez obtenir l'accord de l'opérateur du serveur de noms et ils doivent le configurer comme slave pour votre zone
- Au mieux: une résolution de DNS et un manque de résilience beaucoup plus lents
- Au pire; échecs intermittents pour résoudre votre domaine

Aucune délégation du tout

- Vous pouvez configurer " example.com" sur vos serveurs de noms mais l'extérieur du monde n'enverrons pas des requêtes vers eux jusqu'à ce que vous ayez la délégation.
- Le problème est caché si votre serveur de noms agit comme votre cache et un serveur autoritaire
- Vos propres clients peuvent résoudre
- www.example.com, mais le reste du monde ne peut pas

Les enregistrements « glue records »

- A voir plus tard

La NON Gestion correcte du TTL pendant le changement

- Ex. Si vous avez un TTL de 24 heures, et vous basculer www.example.com pour le pointer vers le nouveau serveur; alors ils auront une période prolongée quand quelques utilisateurs saisissent une machine et certains saisissent l'autre
- Suivre cette procédure
  - Diminuer le TTL à 10 minutes
  - Attendre au moins 24 heures
  - Faire le changement
  - Remettre le TTL à 24 heures

Questions ?

Matières finales

- DNS inverse
- Comment délégué un sous-domaine

Comment gérer le DNS inverse

- si vous avez au moins un /24 de l'espace d'adresses alors votre provider se chargera de la délégation à votre serveur de noms.
- Ex. Votre bloc réseau est 192.0.2.0/24
- Créer la zone 2.0.192.in-addr.arpa.
- Si vous avez plus qu'un /24 alors chaque /24 sera une zone séparée
- Si vous avez assez de chance d'avoir /16 alors il seront une seule zone.
  - 172.16.0.0/16 est 16.172.in-addr.arpa

Exemple : 192.0.2.0/24

```
Zone "2.0.292.in-addr.arpa" {
        type master:
        file "m/192.0.2";
        allow-transfer { . . . };
};

/etc/bind/m/192.0.2
@IN             SOA             .......
        IN      NS      ns0.example.com
        IN      NS      ns0.otherwork.com.

1       IN      PTR             router-e0.example.com.
2       IN      PTR             ns0.example.com.
3       IN      PTR             mailhost.example.com.
4       IN      PTR             www.example.com.
; etc...
```

Comment est-ce qu'il fonctionne ?

- Ex. pour 192.0.2.4, l'hôte distant consultera 4.2.0.192.in-addr.arpa. (PTR)
- La requête suit l'arborescence de la délégation comme la normale. Si tout est correct, alors Il atteint vos serveurs et vous aurez la réponse.
- Maintenant vous pouvez voir pourquoi les octets sont inversés.
- Le propriétaire du grand bloc réseau (192/8) peut déléguer le DNS inverse dans de gros morceaux de /16. le propriétaire d'un /16 peut délégué un gros morceau de /24

Il n'y a rien de spécial au sujet du DNS inverse

- Vous avez toujours besoin du maître et des esclaves
- Il ne fonctionnera en moins que vous obteniez la délégation du dessus de vous
- S'assurer que si vous avez un enregistrement PTR pour l'adresse IP, ce nom d'hôte fait la résolution à la même adresse IP
- Autrement beaucoup de sites sur l'Internet croirons que vous êtes un DNS inverse "spoofing" et refuserons de vous laisser connecter

Qu'est ce qu'il y a si vous avez moins que / 24 ?

- Le DNS inverse pour /24 est délégué à votre fournisseur ascendant
- **Option 1:** demandez à votre fournisseur d'insérer les enregistrements PTR dans ses serveurs DNS.
  - **Problème**: vous devez leur demander tout le temps que vous voulez de faire le changement
- **Option 2** : Suivez la procédure dans le RFC2317
  - Utilisez l'astuce avec le CNAME pour rediriger les requêtes PTR pour vos adresses IP vers vos serveurs de noms.

Ex. Vous possédez 192.0.2.64/29

```
; Dans le fichier de zone du fournisseur 2.0.192.in-addr.arpa
64      IN      CNAME   64.64/29.2.0.192.in-addr.arpa.
65      IN      CNAME   65.64/292.0.192..in-addr.arpa.
66      IN      CNAME   66.64/29.2.0.192.in-addr.arpa.
67      IN      CNAME   67.64/29.2.0.192.in-addr.arpa.
68      IN      CNAME   68.64/29.2.0.192.in-addr.arpa.
69      IN      CNAME   69.64/29.2.0.192.in-addr.arpa.
70      IN      CNAME   70.64/29.2.0.192.in-addr.arpa.
71      IN      CNAME   71.64/29.2.0.192.in-addr.arpa.
64/29   IN      NS      ns0.customer.com.
64/29   IN      NS      ns1.customer.com.
Configuration de la zone "64/29.2.0.192.in-addr.arpa" sur vos serveurs
65      IN      PTR     www.customer.com..
66      IN      PTR     mailhost.customer.com.
; etc
```

Comment est ce que vous déléguer un sous-domaine ?

- En principe simple : juste insérer les enregistrements NS pour le sous-domaine, en pointant vers les quelques d'autres serveurs
- Si vous avez fait attention, vous devriez en premier *vérifier* que les serveurs sont autoritaires pour les sous-domaines.
  - En utilisant "dig" sur tous les serveurs
- Si le sous-domaine est mal géré, il réfléchit mal sur vous

Le fichier de zone pour "example.com"

```
$TTL 1d
@       1h      IN   SOA     ns1.example.net. Brian.nsrc.org. (
                                2014030300 ; Serial
                                8h         ;Refresh
                                1h         ; Retry
                                4w         ; expire
                                1h )       ; Negative
                IN   NS   ns1.example.net.
                IN   NS   ns2.example.net.
                IN   NS   ns1.othernetwork.com.
; Les données de ma propre zone
                IN   MX 10  mailhost.example.net.
www             IN   A    212.74.112.80

; Sous domaine délégué
Subdom          IN   ns1.othernet.net.
                IN   ns2.othernet.net.
```

Il n' y a aucun problème la-bàs

- Les enregistrements NS pointent vers le noms, pas vers les adresses IP
- Qu'est ce que c'est si "example.com" est délégué pour ns.example.com
- Quelqu'un qui est en cours de résolution de (dir) www.example.com doit d'abord résoudre ns.example.com
- Mais ils ne peuvent pas résoudre ns.example.com sans en premier résoudre ns.example.com!!!

Dans ce cas vous avez besoin de "glue record"

- L'enregistrement "glue record" est un enregistrement de type A pour les noms de serveur
- Exemple : considérer les serveurs de noms .com

```
; C'est la zone .com
example          NS      ns.example.com.
                 NS      ns.othernet.net.
ns.example.com.  A       192.0.2.1        ; GLUE RECORD
```

Ne pas mettre les « glue record » exceptés en cas de besoin

- Dans l'exemple précédent, "ns.othernet.net" est le sous-domaine de "example.com" . Par conséquent pas de glue record nécessaire.
- Les « glue record » dépassés sont de grandes sources des problèmes
- Ex. Après une renumérotation de votre serveur de noms dans un autre réseau
- Difficile de corriger, demandes " dig +norec"

Exemple où un « glue record » est necessaire

```
; Les  données de ma propre zone
                IN   MX       10 mailhost.example.net.
www             IN   A        212.74.112.80

; Le sous-domaine délégué
Subdom          IN   NS  ns1.subdom       ; nécessaire
                IN   NS  ns2.othernet.net.      ; non nécessaire
Ns1.subdom IN   A    192.0.2.4
```

Vérification des « Glue record »

- Dig +norec @a.gtld-servers.net. www.as9105.net. A
- Rechercher les enregistrements A dans la section "Additionnelle" dont le TTL ne dimunue pas.

Exemple dig +norec @a.gtld-servers.net www.psg.com a

DNS : Résumé global

- Base de données distribuée d'enregistrements de ressources (ER)
- Trois rôles : resolver, le cache et l'autoritaire
- Le resolver est configuré statiquement avec le(s)cache les plus proches(s)
  - Ex. /etc/resolv.conf
- Les caches sont statiquement configurés avec la liste des serveurs de noms racines
  - Le type de zone "hint", /var/named/named.ca

DNS : Résumé global (suite)

- Les serveurs de noms racine contiennent les délégations (enregistrements NS) au gtld ou les serveurs de noms géographiques "country-level servers" (com. fr. tg, bj)
- D'autres délégations aux sous-domaines
- Le cache se localise finalement sur un serveur d'autorité contenant le RRs que nous exigeons
- Les erreurs dans les délégation ou dans la configuration aboutit à aucune réponse ou des réponses contradictoires.