Bonnes pratiques et fiabilisation du DNS

Olivier Prins - DSI du CNRS

JoSY DNS – 04/11/2021

Les services DNS de la DSI du CNRS

- Reprise des activités DNS de l'Urec en 2011.
- 4 serveurs ayant autorité: ns0.cnrs.fr, ns2.cnrs.fr, ns3.cnrs.fr et ns4.cnrs.fr
- Périmètre:
  - 166 zones maîtres dont 27 inverses.
- Délégation de zones en cnrs.fr
- Support général aux unités CNRS.
- Hébergement de zones esclaves sur ns4.cnrs.fr, dédié aux unités.
  - 420 zones dont 112 inverses.
- Ressource: 0,25 ETP ☺
- Contact: dnsmaster@dsi.cnrs.fr

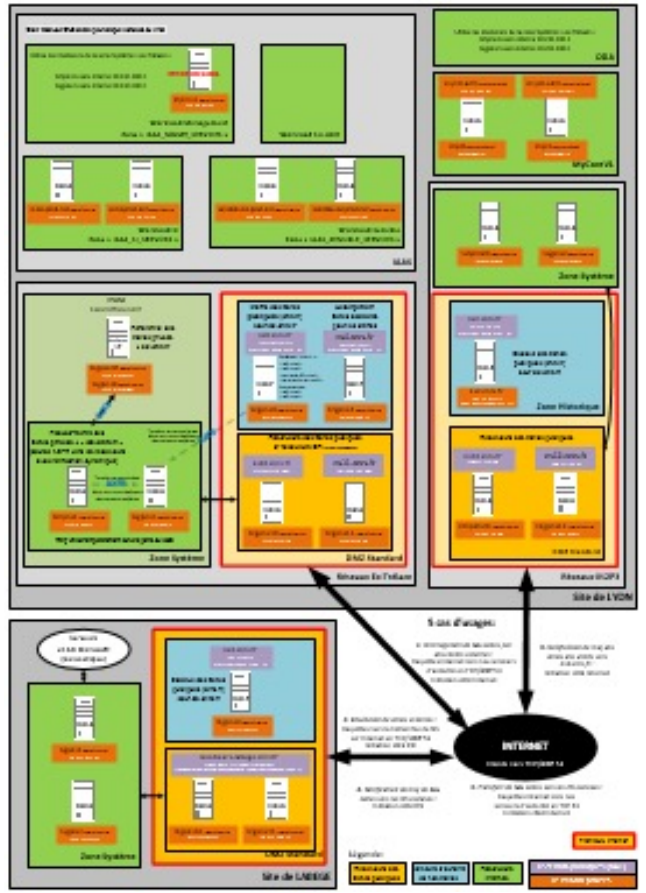
Architecture à la DSI

4 Serveurs d'autorité et 20 résolveurs:

- Serveurs virtuels Vmware (clusters et standalone suivant les sites)
  - RedHat 7 et Bind 9.11.4
- IPv4 et IPv6
- Répartis sur 3 sites géographiques et des réseaux distincts.
- IPAM Efficient IP pour la gestion des zones internes (masqué).
- Bind pour la gestion des zones publiques.

Un des NS d'autorité esclave est volontairement hétérogène:

- Machine physique
  - FreeBSD 13
  - NSD 4.3



Plan de cette présentation

- Rappels de fondamentaux
- Conseils : Gestion administrative des domaines
- Conseils : Sécurisation et optimisations techniques
- Illustration d’incidents classiques
- DNS et messagerie
- Infos diverses
- DNSsec

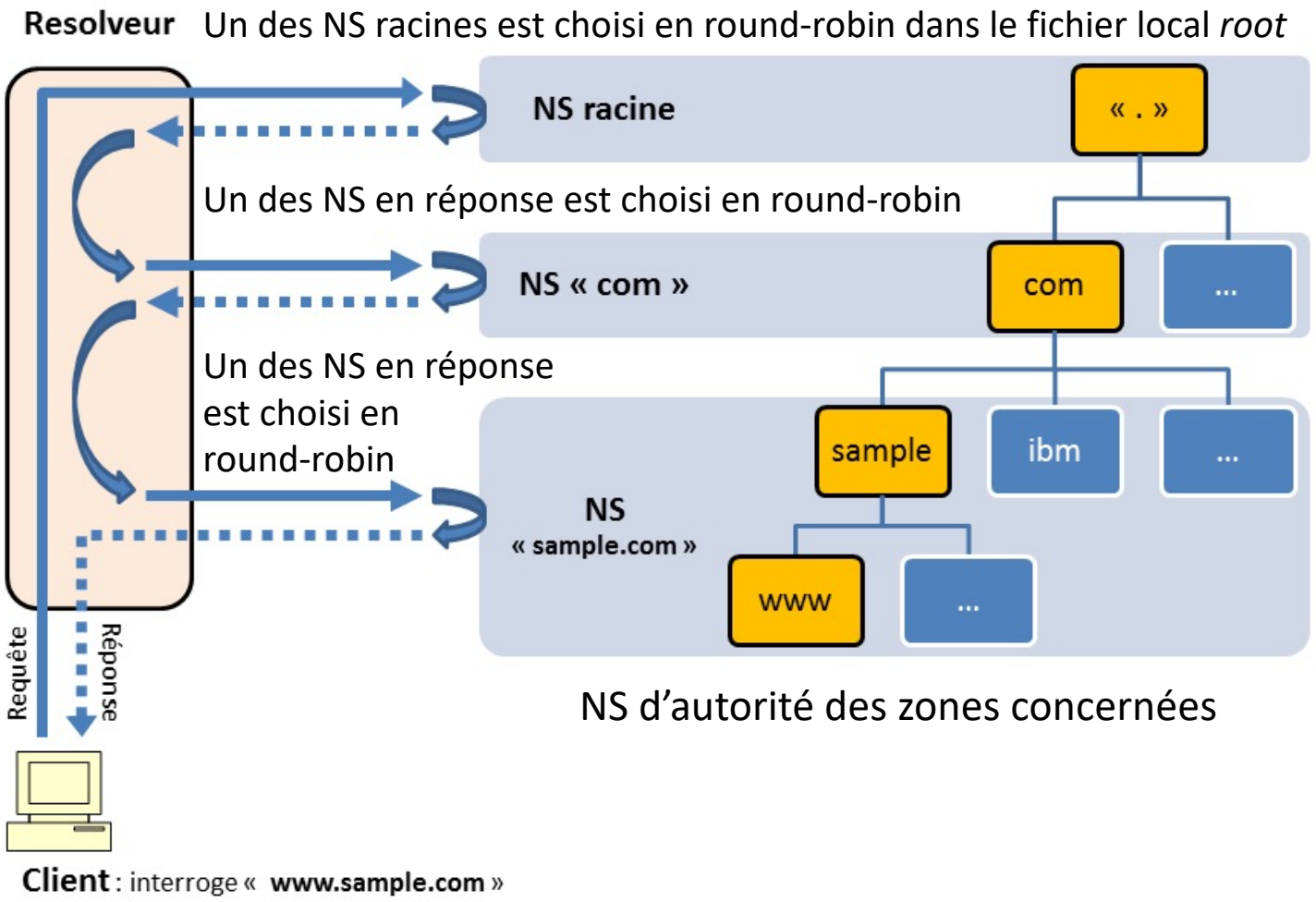
Rappels de fondamentaux

Vocabulaire / glossaire

- **NS** (**N**ame **S**erver) Serveur DNS.
- **NS maître** Serveur de nom ayant autorité primaire.
- **NS esclave** Serveur de nom ayant autorité secondaire.
- **Bureau d'enregistrement** (registrar) Sociétés gestionnaires des noms de domaines.
- **AXFR** Transfert de zone complet.
- **IXFR** Transfert de zone incrémental.
- **DKIM** (**D**omain**K**eys **I**dentified **M**ail) Authentification du domaine expéditeur par signature du mail.
- **SPF** (**S**ender **P**olicy **F**ramework) Vérif. serveurs SMTP du domaine via des entrées DNS dédiées.
- **TLD** (**T**op-**L**evel **D**omain) Domaine de 1er niveau, par exemple « .com » ou « .arpa »
- **TSIG** (**T**ransaction **SIG**nature) Mise à jour entre NS authentifiée par clef symétrique.
- **TTL** (**T**ime **T**o **L**ive) Durée de vie avant péremption.

Le DNS est strictement hiérarchique

Exemple de résolution récursive



NS d'autorité des zones concernées

Les requêtes sont traitées:

- **En UDP/53 par défaut**
- **En TCP/53 à la demande**

Remarques sur la résolution récursive

- Plusieurs tentatives d'une même requête cliente sera résolue par des « chemins » à chaque fois différents.

  Rmq: en faisant abstraction du cache de son résolveur qui n'est pas utilisé lors d'un « *dig +trace* »
- A chaque strate le NS interrogé est en effet choisi par round-robin.
- Et certains NS peuvent héberger plusieurs strates, ce qui fait varier le nombre d'étapes.

En 4 étapes : les NS de la zone parente (ici cnrs.fr) publient la délégation et héberge la zone interrogée

```
dig +trace NS dsi.cnrs.fr

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.7 <<>> +trace NS dsi.cnrs.fr
;; global options: +cmd
.                       277304  IN      NS      j.root-servers.net.
.                       277304  IN      NS      l.root-servers.net.
.                       277304  IN      NS      h.root-servers.net.
.                       277304  IN      NS      c.root-servers.net.
.                       277304  IN      NS      e.root-servers.net.
.                       277304  IN      NS      f.root-servers.net.
.                       277304  IN      NS      m.root-servers.net.
.                       277304  IN      NS      b.root-servers.net.
.                       277304  IN      NS      g.root-servers.net.
.                       277304  IN      NS      k.root-servers.net.
.                       277304  IN      NS      i.root-servers.net.
.                       277304  IN      NS      a.root-servers.net.
.                       277304  IN      NS      d.root-servers.net.
;; Received 1097 bytes from 10.232.200.1#53(10.232.200.1) in 0 ms

fr.                     172800  IN      NS      d.nic.fr.
fr.                     172800  IN      NS      e.ext.nic.fr.
fr.                     172800  IN      NS      f.ext.nic.fr.
fr.                     172800  IN      NS      g.ext.nic.fr.
;; Received 623 bytes from 2001:7fd::1#53(k.root-servers.net) in 2 ms

cnrs.fr.                172800  IN      NS      ns2.cnrs.fr.
cnrs.fr.                172800  IN      NS      panoramix.rap.prd.fr.
cnrs.fr.                172800  IN      NS      ns0.cnrs.fr.
cnrs.fr.                172800  IN      NS      ns3.cnrs.fr.
cnrs.fr.                172800  IN      NS      camus.dr15.cnrs.fr.
;; Received 735 bytes from 2001:678:4c::1#53(g.ext.nic.fr) in 2 ms

dsi.cnrs.fr.            3600    IN      NS      ns3.cnrs.fr.
dsi.cnrs.fr.            3600    IN      NS      ns0.cnrs.fr.
dsi.cnrs.fr.            3600    IN      NS      ns2.cnrs.fr.
;; Received 226 bytes from 193.52.36.172#53(ns2.cnrs.fr) in 0 ms
```

En 5 étapes : les NS de la zone parente publient uniquement la délégation

```
dig +trace NS dsi.cnrs.fr

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.7 <<>> +trace NS dsi.cnrs.fr
;; global options: +cmd
.                       277301  IN      NS      j.root-servers.net.
.                       277301  IN      NS      d.root-servers.net.
.                       277301  IN      NS      c.root-servers.net.
.                       277301  IN      NS      a.root-servers.net.
.                       277301  IN      NS      h.root-servers.net.
.                       277301  IN      NS      g.root-servers.net.
.                       277301  IN      NS      e.root-servers.net.
.                       277301  IN      NS      i.root-servers.net.
.                       277301  IN      NS      f.root-servers.net.
.                       277301  IN      NS      k.root-servers.net.
.                       277301  IN      NS      b.root-servers.net.
.                       277301  IN      NS      l.root-servers.net.
.                       277301  IN      NS      m.root-servers.net.
;; Received 1097 bytes from 10.232.200.1#53(10.232.200.1) in 0 ms

fr.                     172800  IN      NS      d.nic.fr.
fr.                     172800  IN      NS      e.ext.nic.fr.
fr.                     172800  IN      NS      f.ext.nic.fr.
fr.                     172800  IN      NS      g.ext.nic.fr.
;; Received 623 bytes from 2001:500:2d::d#53(d.root-servers.net) in 2 ms

cnrs.fr.                172800  IN      NS      ns3.cnrs.fr.
cnrs.fr.                172800  IN      NS      ns0.cnrs.fr.
cnrs.fr.                172800  IN      NS      ns2.cnrs.fr.
cnrs.fr.                172800  IN      NS      panoramix.rap.prd.fr.
cnrs.fr.                172800  IN      NS      camus.dr15.cnrs.fr.
;; Received 735 bytes from 2001:678:c::1#53(d.nic.fr) in 6 ms

dsi.cnrs.fr.            3600    IN      NS      ns2.cnrs.fr.
dsi.cnrs.fr.            3600    IN      NS      ns3.cnrs.fr.
dsi.cnrs.fr.            3600    IN      NS      ns0.cnrs.fr.
;; Received 226 bytes from 193.50.20.1#53(panoramix.rap.prd.fr) in 6 ms

dsi.cnrs.fr.            3600    IN      NS      ns0.cnrs.fr.
dsi.cnrs.fr.            3600    IN      NS      ns2.cnrs.fr.
dsi.cnrs.fr.            3600    IN      NS      ns3.cnrs.fr.
;; Received 226 bytes from 2001:660:500a:2103::10#53(ns2.cnrs.fr) in 0 ms
```

Rmq : 10.232.200.1 est ici le résolveur local qui fournit les NS racines via son fichier local /var/named/named.ca

Attention, cela peut masquer certaines erreurs, avec un comportement changeant suivant le chemin emprunté pour la résolution récursive.

Par exemple si la délégation devient erronée sur le maître ns0.cnrs.fr :

```
sample.cnrs.fr IN   NS   ns0.cnrs.fr
               IN   NS   ns2.cnrs.fr
               IN   NS   ns666.cnrs.fr
```

En 4 étapes : aucune référence à ns666 car c'est directement le NS du fichier de zone qui est retourné mais pas la délégation.

```
dig +trace NS sample.cnrs.fr

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.7 <<>> +trace NS sample.cnrs.fr
;; global options: +cmd
.                       263704  IN      NS      c.root-servers.net.
.                       263704  IN      NS      k.root-servers.net.
.                       263704  IN      NS      j.root-servers.net.
.                       263704  IN      NS      l.root-servers.net.
.                       263704  IN      NS      i.root-servers.net.
.                       263704  IN      NS      d.root-servers.net.
.                       263704  IN      NS      g.root-servers.net.
.                       263704  IN      NS      b.root-servers.net.
.                       263704  IN      NS      e.root-servers.net.
.                       263704  IN      NS      f.root-servers.net.
.                       263704  IN      NS      h.root-servers.net.
.                       263704  IN      NS      a.root-servers.net.
.                       263704  IN      NS      m.root-servers.net.
;; Received 1097 bytes from 10.232.200.1#53(10.232.200.1) in 0 ms

fr.                     172800  IN      NS      d.nic.fr.
fr.                     172800  IN      NS      e.ext.nic.fr.
fr.                     172800  IN      NS      f.ext.nic.fr.
fr.                     172800  IN      NS      g.ext.nic.fr.
;; Received 624 bytes from 2001:500:a8::e#53(e.root-servers.net) in 3 ms

cnrs.fr.                172800  IN      NS      panoramix.rap.prd.fr.
cnrs.fr.                172800  IN      NS      camus.dr15.cnrs.fr.
cnrs.fr.                172800  IN      NS      ns2.cnrs.fr.
cnrs.fr.                172800  IN      NS      ns3.cnrs.fr.
cnrs.fr.                172800  IN      NS      ns0.cnrs.fr.
;; Received 736 bytes from 194.146.106.46#53(f.ext.nic.fr) in 214 ms

sample.cnrs.fr.         3600    IN      NS      ns2.cnrs.fr.
sample.cnrs.fr.         3600    IN      NS      ns3.cnrs.fr.
sample.cnrs.fr.         3600    IN      NS      ns0.cnrs.fr.
;; Received 227 bytes from 193.52.36.172#53(ns2.cnrs.fr) in 0 ms
```

En 5 étapes : la délégation via ns666 est publiée par les NS de la zone parente

```
dig +trace NS sample.cnrs.fr

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.7 <<>> +trace NS sample.cnrs.fr
;; global options: +cmd
.                       263670  IN      NS      f.root-servers.net.
.                       263670  IN      NS      m.root-servers.net.
.                       263670  IN      NS      a.root-servers.net.
.                       263670  IN      NS      d.root-servers.net.
.                       263670  IN      NS      g.root-servers.net.
.                       263670  IN      NS      k.root-servers.net.
.                       263670  IN      NS      c.root-servers.net.
.                       263670  IN      NS      i.root-servers.net.
.                       263670  IN      NS      h.root-servers.net.
.                       263670  IN      NS      j.root-servers.net.
.                       263670  IN      NS      e.root-servers.net.
.                       263670  IN      NS      l.root-servers.net.
.                       263670  IN      NS      b.root-servers.net.
;; Received 1097 bytes from 10.232.200.1#53(10.232.200.1) in 0 ms

fr.                     172800  IN      NS      d.nic.fr.
fr.                     172800  IN      NS      e.ext.nic.fr.
fr.                     172800  IN      NS      f.ext.nic.fr.
fr.                     172800  IN      NS      g.ext.nic.fr.
;; Received 624 bytes from 202.12.27.33#53(m.root-servers.net) in 11 ms

cnrs.fr.                172800  IN      NS      ns0.cnrs.fr.
cnrs.fr.                172800  IN      NS      ns2.cnrs.fr.
cnrs.fr.                172800  IN      NS      ns3.cnrs.fr.
cnrs.fr.                172800  IN      NS      camus.dr15.cnrs.fr.
cnrs.fr.                172800  IN      NS      panoramix.rap.prd.fr.
;; Received 725 bytes from 193.176.144.22#53(e.ext.nic.fr) in 20 ms

sample.cnrs.fr.         3600    IN      NS      ns2.cnrs.fr.
sample.cnrs.fr.         3600    IN      NS      ns0.cnrs.fr.
sample.cnrs.fr.         3600    IN      NS      ns666.cnrs.fr.
couldn't get address for 'ns666.cnrs.fr': not found
;; Received 184 bytes from 147.210.72.192#53(camus.dr15.cnrs.fr) in 13 ms

sample.cnrs.fr.         3600    IN      NS      ns3.cnrs.fr.
sample.cnrs.fr.         3600    IN      NS      ns0.cnrs.fr.
sample.cnrs.fr.         3600    IN      NS      ns2.cnrs.fr.
;; Received 227 bytes from 2001:660:500a:2103::10#53(ns2.cnrs.fr) in 0 ms
```

Les « Time To Live » ou TTL sur les serveurs ayant autorité

TTL par défaut de la zone

Pour chaque zone il spécifie la durée de validité des enregistrements dans le cache des résolveurs. Une fois ce délai échu les résolveurs réinterrogent les NS afin de rafraichir leur cache pour une nouvelle période.

```
$TTL 10800          ; TTL par defaut (3h)
```

Ce TTL peut être redéfini spécifiquement et indépendamment au niveau de **chaque enregistrement**.

```
test        300     IN      A       198.51.100.0
```

Cela permet par exemple de limiter le délai de prise en compte lors d'une maj par exemple.

Attention : la valeur tu TTL utilisée par le résolveur est celle de son cache tant que celui-ci reste valide. Il faut donc anticiper la maj du TTL d'une durée au moins égale à la valeur initiale pour être certain que tous les résolveurs seront ensuite bien à jour dans un délai de 300 secondes.

Par exemple si le TTL initial était de 10800 secondes (3h): au moment de la publication du nouveau TTL le résolveur qui aurait rafraichi son cache juste avant attendra 3h pour le mettre de nouveau à jour, et non pas 5 minutes.

Remarque : les TTL < à 300 secondes sont susceptibles d'être réévaluées arbitrairement par les résolveurs, afin de limiter leur charge (notamment ceux des providers). 300 est donc la valeur minimale conseillée.

Le TTL de l'enregistrement SOA

Ils définissent le comportement que doivent suivre les NS esclaves pour le transfert de la zone.

```
example.com.    IN    SOA    example.com.    dnsmaster.example.com. (
                             2013101104      ; Version
                             21600           ; Refresh (6h)
                             3600            ; Retry   (1h)
                             3600000         ; Expire  (1000h)
                             3600            ; Negative caching TTL (1h)
                       )
```

- **Refresh** Délai avant maj de la zone auprès du NS maître. *
- **Retry** Délai de nouvelle tentative en cas d'échec.
- **Expire** Délai avant péremption de la zone sur l'esclave si non maj depuis le NS maître.
- **Negative caching TTL** Délai avant réitération pour les requêtes « sans-réponse » (RFC 2308).

* : le mécanisme de notification dynamique du NS maître vers les NS esclaves a rendu cette notion désuète.

Critères pour définir une valeur de TTL adaptée

- Le niveau de redondance de l'architecture DNS: le TTL doit être supérieur à la durée estimée d'une interruption du service DNS
- La charge: plus le TTL est faible, plus le DNS sera interrogé fréquemment.
- La réactivité lors d'une modification de la zone: le TTL doit être inférieur à la durée souhaitée d'expiration des enregistrements dans les caches des résolveurs.
  - Exemple : le serveur web change d'adresse IP, si le TTL est à 24h, l'ancienne adresse IP doit continuer à répondre pendant une journée avant qu'on puisse la supprimer.
- Les risques d'empoisonnement de cache: plus le TTL est élevé, plus les risques d'empoisonnement du cache sont faibles. Les valeurs les plus communes du TTL sont entre 1h et 24h.

Attention au TTL du cache négatif: les résolveurs gardent en cache non-seulement les enregistrements trouvés, mais également les réponses indiquant qu'un enregistrement n'existe pas, et cela pour une durée de plusieurs minutes à plusieurs heures.

Par exemple, si lors de la modification d'un enregistrement, il y a un intervalle de temps pendant lequel l'enregistrement n'existe pas (entre le moment de la suppression et le moment de la recréation) le risque existe qu'un résolveur mette en cache la réponse négative.

Conseils

Gestion administrative des domaines

Choix du TLD

Du fait du fonctionnement hiérarchique du DNS, le choix de l'extension d'un domaine n'est pas neutre.

En effet le niveau de fiabilité des TLDs n'est pas homogène.

Depuis 10 ans le nombre de TLDs disponibles a explosé (des centaines).

Mieux vaut éviter les extensions « exotiques ».

Choix du bureau d’enregistrement

La qualité de service des différents bureaux d'enregistrement est également hétérogène.

Il faut veiller à la qualité, à la souplesse et à la réactivité des procédures de mise à jour (l'idéal étant une interface de management en ligne avec la disponibilité d’une API).

En effet, pour une zone de premier niveau, tout changement de NS nécessitera une demande de maj de la délégation auprès du bureau d'enregistrement, afin qu'il la relaie

Rmq: je ne traite pas du cas où les zones ne sont pas déléguées mais hébergées directement par le registrar (comportement par défaut chez OVH ou Gandi par exemple).

Whois: informations diffusées par les TLDs

Les TLDs diffusent via le service Whois des informations administratives et techniques sur les zones DNS, notamment le propriétaire et les contacts techniques ainsi que la liste des NS.

Ces informations sont purement indicatives.

Les NS indiqués peuvent par exemple ne pas correspondre aux NS ayant effectivement délégation: cela n’a pas d'incidence pratique.

Néanmoins il est souhaitable que les données Whois soient maintenues à jour via le bureau d’enregistrement.

Création et suivi du domaine

- Pour limiter les risques de cybersquating, il est conseillé d’enregistrer les déclinaisons du nom pouvant être confondues par les utilisateurs.
- Lors de la création, il faut vérifier que la zone sont corrects avec un outil comme **Zonemaster** (successeur de ZoneCheck).
- Il faut consulter régulièrement les informations concernant le domaine grâce à Whois, et veiller à renouveler le contrat pour éviter l'expiration du domaine. Autant que possible, il est recommandé d’automatiser la surveillance et/ou le renouvellement.

Anti-spoofing / cybersquating
Réservation des noms proches

Réserver les déclinaisons proches sous différents TLDs :

- mondomaine.fr, mon-domaine.fr, mondomaine.fr, etc.
- mondomaine.net, mondomaine.org, etc.

Y compris les déclinaisons accentuées.

Exemple pour cnrs.fr :

Nom de zone	Correspondance
cnrs.fr	cnrs.fr
xn--nrs-1la.fr	çnrs.fr
xn--crs-7ma.fr	cñrs.fr
xn--rs-3ia4b.fr	çñrs.fr

Eviter de choisir un nom dont un TLD majeur (.com, .fr) n'est pas disponible.

Communauté enseignement/recherche

Pour le TLD « **.fr** » il est recommandé d'utiliser le service **Renater** qui propose les avantages suivants:

- Acteur naturel pour la communauté.
- Ouvert à tout établissement agréé.
- Reconduction annuelle tacite.
- Gestion semi-automatique des demandes de zones inverses IPv4 et IPv6.
- Pas de frais.

Rmq: Renater démantèle son service payant pour les autres TLDs fin 2021.

Transfert administratif du domaine

Lors de l'enregistrement d'un domaine, il faut s'assurer d'être bien déclaré comme propriétaire administratif du domaine, notamment lorsque l'on passe par un prestataire de service.

Car le cas échéant, seul le propriétaire pourra initier la session ou la migration du domaine.

Il faut également prendre soin de définir une personne morale comme propriétaire et non une personne physique qui risque de partir un jour vers de nouveaux horizons.

Délégation de sous-domaines

La délégation de zone est à réaliser avec prudence car une fois un sous-domaine délégué celui-ci échappe au domaine parent.

Il est ainsi fréquent qu'un sous-domaine soit abandonné sans que l'administrateur du domaine parent en soit averti.

Pour garder un œil sur les zones déléguées, il est intéressant de mettre en place un outillage qui réalisera périodiquement un ensemble de contrôle : connectivité DNS aux NS, transfert de zone si l'on est esclave, etc.

La seule intervention technique possible est de révoquer la délégation.

Conseils

Sécurisation et optimisations techniques

Panacher OS et services DNS

Afin d'améliorer la résilience on peut utiliser différents systèmes d'exploitation ou distribution:

Debian Linux, RedHat Linux, OpenBSD ou FreeBSD par exemple.

Et différents serveurs DNS:

ISC Bind ou NSD par exemple.

Cela permet de limiter les risques d'attaques en s'appuyant sur des ressources hétérogènes qui n'auront pas des faiblesses exploitables simultanément.

La synchro du temps est importante : NTP

La bonne gestion des clefs, des signatures, des transferts de zones ou l'obtention de métriques précis dans les logs nécessitent que les différents NS soient correctement synchronisés au niveau temporel.

Il faut donc activer et surveiller le bon fonctionnement du service **NTP**.

NS maître « caché »

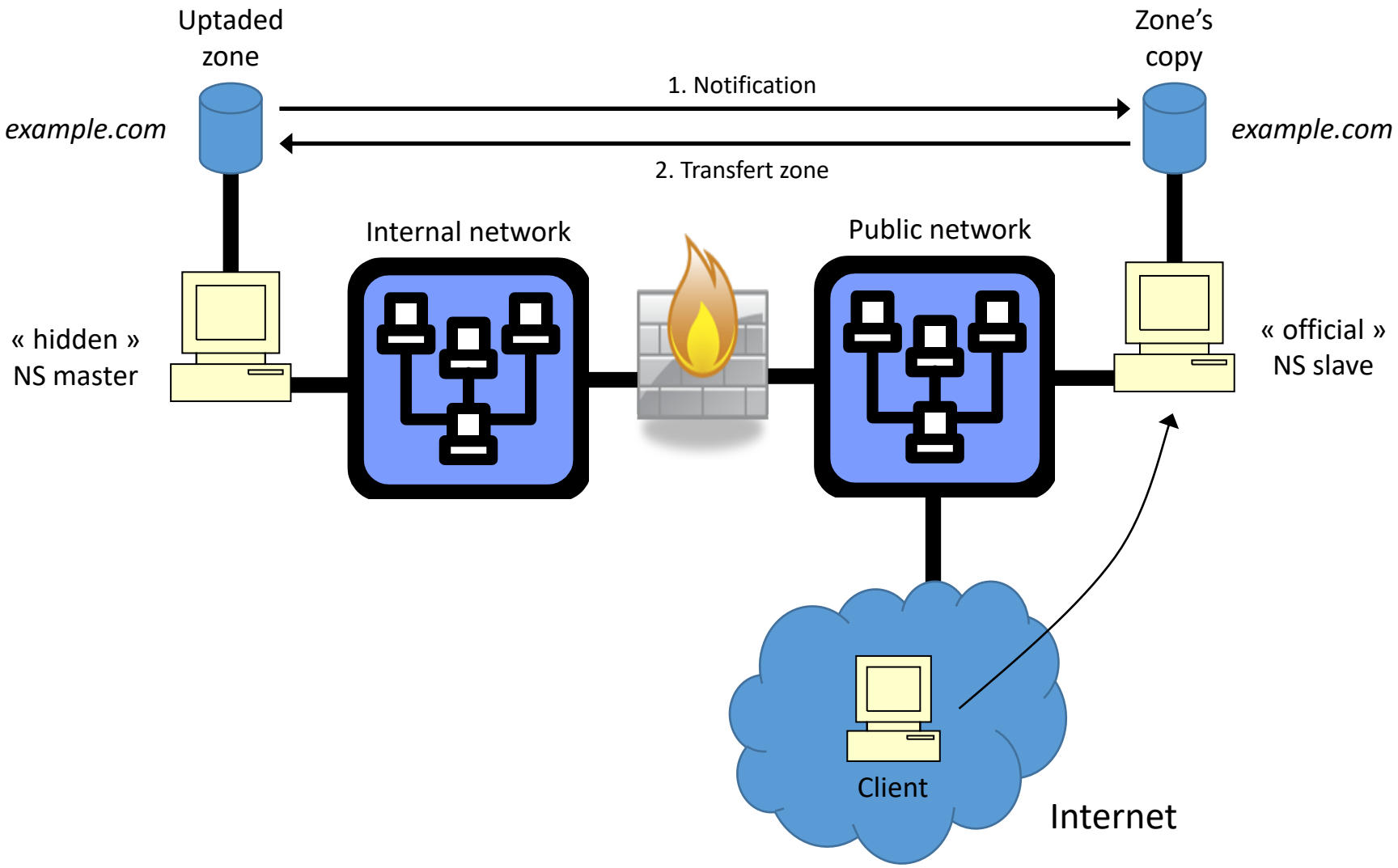
Il est possible d'isoler le NS maître dans une architecture dite « *stealth master DNS* » ou « *hidden master DNS* »: le vrai NS maître sur lequel les zones sont modifiées n'est ni accessible ni visible de l'extérieur.

Il peut s'agir d'un IPAM par exemple.

Le NS maître public, dont le nom est référencé dans le SOA et par délégation de plus haut niveau, est en réalité un NS esclave qui synchronise ses zones depuis le NS maître caché.

Chaque fois qu'une zone est modifiée sur le maître caché, les esclaves sont notifiés par celui-ci, suivi du transfert de zone, en cascade.

Stealth DNS Master



Séparer l’IP du service et l’IP de gestion

Le NS doit disposer d’une adresse IP dédiée pour la gestion (accès SSH, supervision, contrôle à distance du serveur de nom etc.) et d’une autre adresse IP consacrée au service DNS, sur une autre interface.

Cela permet de séparer l’administration du serveur et l’accès au service, et cela autorise différentes technique de redondance (VRRP, Anycast, etc.).

Gérer l'IPv6

Afin de pouvoir répondre à des clients IPv6 il est souhaitable d'avoir au moins un NS adressable en IPv6.

L'IPv6 est notamment très utilisé en Asie, où il y a pénurie de plage IPv4.

La DSI du CNRS propose aux unités CNRS ce type d'hébergement.

Filtrage des serveurs

Seul le port **53** en **TCP** et en **UDP** doit être accessible de l'Internet pour un serveur public.

Aucun autre service ne devrait tourner sur les serveurs en dehors du DNS.

Il faut maintenir à jour le logiciel de serveur de nom, appliquer les correctifs de sécurité de l'OS et restreindre l'accès à ce serveur.

Chroot et limitation de privilèges

Il est recommandé de chrooter le service DNS dans une arborescence dédiée afin de limiter la portée d'une exploitation de faille de sécurité.

De plus, le service ne doit pas être lancé via un compte ayant les droits d'administration (« root » ou « Administrateur ») mais via un compte dédié ayant un minimum de privilèges (« named » par exemple).

Politique de nommage

Les données servies par les DNS sont publiques par nature.

Il faut veiller à ne pas y mettre des données sensibles ou qui pourraient faciliter des attaques :

- Noms de logiciels, de zones réseaux explicites, etc.

De plus, il est recommandé de définir et d'appliquer une politique de nommage.

Par exemple choisir un domaine dédié aux infrastructures internes qui ne sera pas diffusée publiquement.

Par exemple local.sample.com (à préférer à .local)

Isoler zones publiques et zones privées

En complément du filtrage réseau, compartimenter les serveurs faisant autorité pour les zones publiques et les serveurs faisant autorité pour les zones privées.

En effet, ces périmètres ont des finalités bien distinctes et des besoins de sécurité opposés :

- les zones publiques sont destinées à être visibles sur tout l'Internet pour que les services qui en dépendent (serveur web, messagerie etc.) soient accessibles.
- les zones privées contiennent des adresses internes qui intéressent uniquement les clients internes.

Faire une séparation entre les données des zones publiques et celle des zones privées, et isoler au niveau réseau l'accès à ces zones privées garantit la non-divulgation d'informations vers l'extérieur : architecture du réseau interne, plans d'adressage, noms des serveurs, etc.

Isoler sur des plateformes distinctes les résolveurs récursifs et les serveurs faisant autorité

Il s'agit en effet de 2 services DNS distincts.

- Le **résolveur récursif** répond aux requêtes concernant n'importe quel domaine public, en résolvant récursivement depuis la racine les différentes délégations, jusqu'au NS portant le domaine demandé. Ce dernier fournira la réponse. Ce résultat est ensuite mis en cache sur le résolveur durant une durée égale au TTL publié par la zone.
- Le **serveur d'autorité** répond lui uniquement aux requêtes des résolveurs concernant **vos zones**. C'est lui qui en publie les entrées. Il apparait comme ayant délégation dans la zone parente.

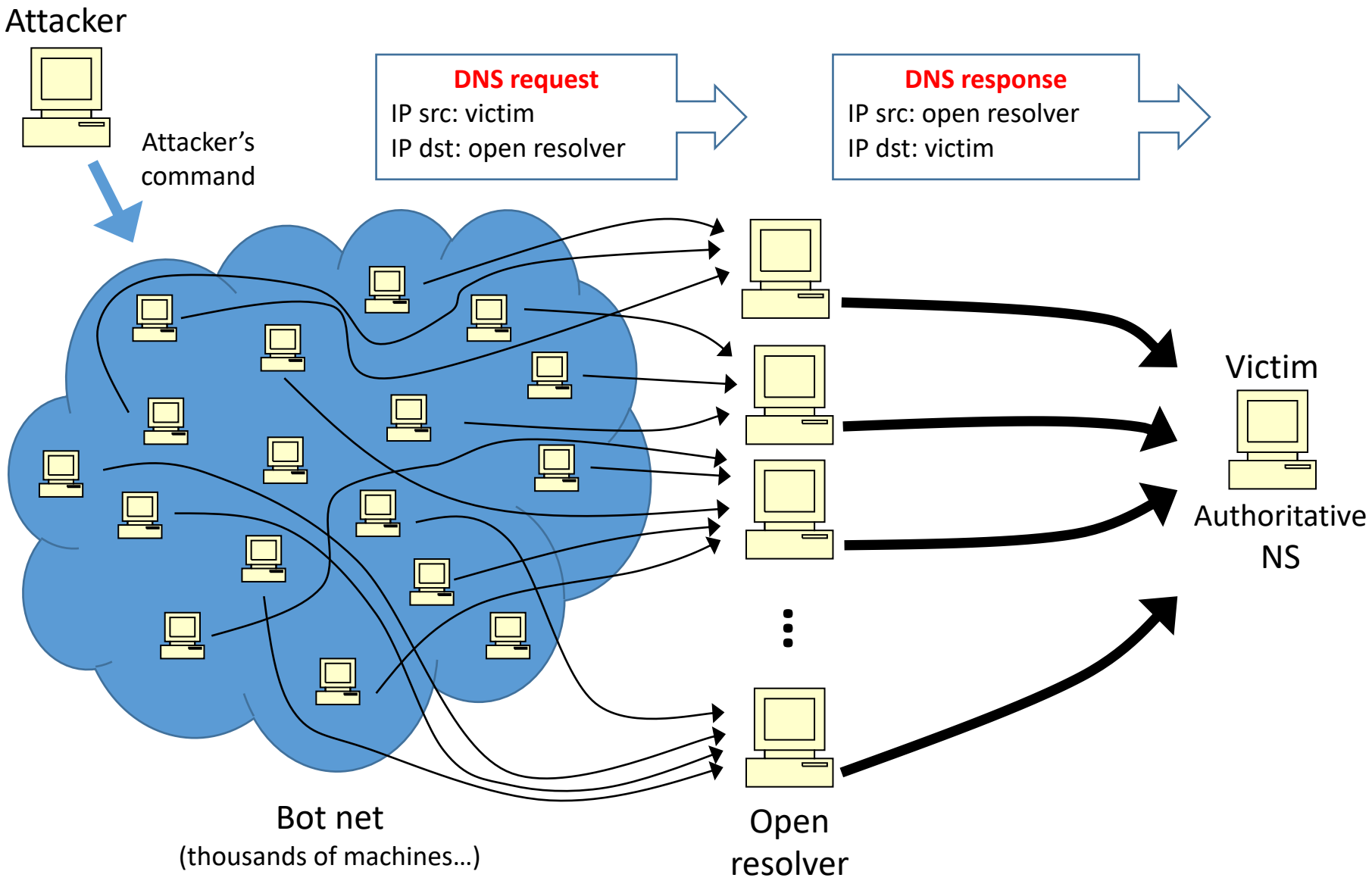
Restreindre l’accès aux résolveurs récursifs

Un résolveur ouvert à tout l’Internet présente des risques importants:

- d’empoisonnement du cache.
- d’être victime d’une attaque de déni de service (DOS) ciblée sur le résolveur (impactant l’ensemble des utilisateurs internes).
- de servir de vecteur indirect dans une attaque de déni de service distribuée (DDOS) : attaque DNS par amplification en usurpant l’adresse IP source.

Bind: `allow-recursion` Unbound: `access-control`

DNS DDoS Amplification Attack



Synchronisation des zones entre NS

Lors de la maj d'une zone sur le NS maître, celui-ci émet par défaut une notification dynamique à destination des NS esclaves, afin de les en avertir.

En réaction chaque NS esclave contrôle le n° SOA et s'il a progressé lance une demande transfert de la zone auprès du NS maître (en TCP/53).

Cela permet une synchronisation immédiate, sans attendre l'échéance du TTL SOA Refresh sur les esclaves.

Le comportement par défaut de Bind est de notifier tous les serveurs renseignés en type NS dans le fichier de zone.

Sous Bind il s'agit de la clause par défaut « `notify yes;` ».

Restriction des transferts de zones

Un NS maître ne doit autoriser les transferts de zones (AXFR ou IXFR) qu'à ses seuls NS esclaves (directive « **`allow-transfer`** » sous Bind).

Habituellement un NS esclave ne doit lui autoriser aucun transfert, sauf dans une archi d'un NS maître « caché » pour le « faux » NS maître public.

En l'absence de restriction le risque d'attaque DDOS est fort. Et la publication des fichiers de zones complets pourrait fournir des informations sensibles (fournir un liste exhaustive des hosts à attaquer par exemple).

Signature TSIG des échanges entre NS

Afin de contrôler l'identité des NS lors des transferts de zones, il est important de mettre en place une signature symétrique TSIG (**T**ransaction **SIG**nature) [RFC2845].

Cela implique de d’activer une clef sur les NS pour signer les transferts.

Attention de veiller à la bonne synchro temps (NTP) des NS.

Exemple de config TSIG sous Bind

```
key "tsig_001." {
        algorithm "hmac-md5";
        secret "IaPUtN3x+xxxxxxxxxxxx...xxxxxS4g==";
};

server 198.51.100.1 {
        keys { tsig_001.; };
};
server 2001:DB8::ABCD:ABCD:1 {
        keys { tsig_001.; };
};
```

Maj dynamiques

Par défaut Bind interdit les maj automatiques.

Autoriser une IP à faire des mises à jour dynamiques est dangereux.

Si cette fonctionnalité est vraiment nécessaire, il faut utiliser TSIG pour authentifier ces mises à jour dynamiques.

Et elles ne devraient s'opérer que sur des réseaux privés sécurisés.

Vues et split DNS

La séparation des zones publiques et privée peut se faire en utilisant des vues ou via une architecture scindée en deux dite « Split DNS ».

Il est ainsi possible de créer plusieurs vues à destination des clients différents. En fonction de son adresse IP, chaque client verra d'autres enregistrements.

Par exemple, pour la zone « example.com », les clients internes verront l'ensemble des postes, des imprimantes et des serveurs internes déclarés dans la vue interne, et les clients externes ne verront que le serveur web et les relais de messagerie publics.

L'utilisation des vues présente des risques opérationnels. Dans la mesure où, en fonction de son adresse IP source, on ne reçoit pas la même réponse, cela peut introduire des problèmes qui n'existent pas dans le fonctionnement normal du DNS et peut compliquer le débogage. Il est recommandé de bien mettre en perspective le risque et le gain de sécurité avant de choisir d'implémenter les vues DNS.

Exemple de vues sous Bind

```
view "internal" {
  match-clients { 192.0.2.0/24; }; # uniquement les adresses internes
  zone "example.com" {
    type master;
    file "internal/example.com";   # contient l'ensemble des enregistrements
  }
}
view "external" {
  match-clients { any; };
  zone "example.com" {
    type master;
    file "external/example.com";   # ne contient que "www" et "mail"
  }
}
```

Plusieurs NS esclaves

Afin d’assurer la continuité de service en cas de défaillance du NS maître il est indispensable de prévoir des NS esclaves afin de répartir le service sur plusieurs NS.

La bonne pratique recommande d’avoir au moins 3 NS (un maître et deux esclaves), répartis sur des **réseaux et des sites distincts** afin d'augmenter la résilience.

Prévoir un canal de communication fiable entre les gestionnaires des NS maître et esclaves afin d’échanger sur les évolutions et incidents.

Maj des NS esclaves: communiquez !

Attention aux serveurs esclaves qui ne font plus autorité.

Il peut arriver que le gestionnaire du NS maître supprime l'esclave dans sa liste des NS à notifier ou autorisés à transférer une zone.

Dans ce cas, le NS esclave risque de continuer à servir des données périmées localement, ou même publiquement si la délégation de plus haut niveau n'a pas été mise à jour correctement.

Les serials des différents NS sont alors déphasés. Pour les confronter :

```
dig +nssearch sample.com
```

Le gestionnaire du NS maître doivent donc absolument avertir de tout changement les gestionnaires des NS esclaves.

NS maître et esclave

La notion de NS **maître** (primaire) ou **esclave** (secondaire) n'impacte que la mécanique de transfert des zones entres NS en définissant un NS maître référentiel et des NS esclaves qui se synchronisent en recevant des notifications dynamiques de la part du maître.

Un résolveur client ne fait pas de différence entre un NS maître ou esclave. Il s'agit pour lui d'un ensemble de NS d'autorité indifférenciés.

D'un point de vue public seul le SOA permet de connaitre le NS maître, et cette info n'a aucun rôle technique, comme le mail de contact.

Au niveau de la délégation des zones parentes il n'apparait également aucune distinction.

Conseils

Organisation pratique

Gestion manuelle des zones

La gestion manuelle des fichiers de zones est conseillée pour les zones ayant peu d'entrées et/ou peu de maj.

C'est également envisageable pour les zones plus complexes si l'on adopte une grande rigueur dans le formatage des fichiers.

En l'occurrence:

- Utilisation d'une arborescence « inverse » pour les fichiers de zones.
- Maj systématique du cartouche.
- Classement par ordre alphabétique stricte :
  - Dans le cas d'entrées multi-niveaux classer sur le niveau parent (alpha de droite à gauche)
- Vérifier que la valeur du champ Serial est bien incrémentée (ou l'incrémenter automatiquement pas script)

Une arborescence « inverse » pour le stockage des fichiers de zones permet un parcours prédictible

```
eu
├── cnrs
│   ├── cnrs.eu
│   └── magnetometry
│       └── magnetometry.cnrs.eu
├── core-xpert
│   └── core-xpert.eu
├── genolevures
│   └── genolevures.eu
├── hut-occitanie
│   └── hut-occitanie.eu
└── ips2
    └── ips2.eu
```

Cela permet de dresser facilement la liste des zones gérées afin de réaliser des outils de contrôle de cohérence et de métrologie:

- N° de SOA en phase entre NS
- NS joignables
- Etc.

```
;------------------------------ DEBUT DE FICHIER ------------------------------
; Zone example.fr
;------------------------------------------------------------------------------
; 20130701 pdupond : update "web" from 203.0.113.1 to 203.0.113.2
; 20130627 pdupond : create zone
;------------------------------------------------------------------------------

; TTL par defaut
$TTL 3600

;---------------------------------- RACINE ------------------------------------
$ORIGIN example.com.
;                                   Serveur maitre      Mail contact technique
;                                   ------------------- ----------------------
@                   IN       SOA    ns1.example.com.    dnsmaster.example.com.                (
                                    2013070101          ; Version
                                    21600               ; Refresh (6h)
                                    3600                ; Retry   (1h)
                                    3600000             ; Expire  (1000h)
                                    3600                ; Negative caching TTL (1h)
                                    )

; Serveurs maitre et esclave(s)
                    IN              NS                  ns1.example.com.
                    IN              NS                  ns2.example.com.
                    IN              NS                  ns3.example.com.

; Messagerie
                    IN              MX 0                smtp1.example.com.
                    IN              MX 0                smtp2.example.com.
                    IN              TXT                 "v=spf1 mx mx:smtprelay.example.com ~all"

; Microsoft Office 365
                    IN              TXT                 "MS=ms12345678"

;---------------------------------- COLLE -------------------------------------
; Les adresses des NS sous example.com
;------------------------------------------------------------------------------
ns1                 IN              A                   192.0.2.1
                    IN              AAAA                2001:DB8:1234:1234:1234:1
ns2                 IN              A                   198.51.100.1
                    IN              AAAA                2001:DB8:ABCD:ABCD:ABCD:1
ns3                 IN              A                   203.0.113.1
                    IN              AAAA                2001:DB8:CDEF:CDEF:CDEF:1
ns1.succursale      IN              A                   192.0.2.200
ns2.succursale      IN              A                   198.51.100.200
ns3.succursale      IN              A                   203.0.113.200

;------------------------------------------------------------------------------
; DECLARATION DES ENTREES
;------------------------------------------------------------------------------
; Ordre alphabetique sur le 1er niveau de droite a gauche (ex: xxx.yyy est trie sur yyy).
; Les zones deleguees sont mixees avec les non deleguees.
; Separateur: tabulation (sauf entre MX et son poids: utiliser un espace).
;------------------------------------------------------------------------------

abc                 IN              CNAME               web

;                                                       <pierre.dupond@succursale.example.com>
succursale          IN              NS                  ns1.succursale
                    IN              NS                  ns2.succursale
                    IN              NS                  ns3.succursale

test                IN              CNAME               web
www.test            IN              CNAME               web
intranet.test       IN              CNAME               web
www.intranet.test   IN              CNAME               web
web                 IN              A                   203.0.113.2

;------------------------------ FIN DE FICHIER --------------------------------
```

300 ZONES ESCLAVES						
# / 300	PARAMETRAGE LOCAL		INTERROGATION VIA DIG (le 20190107_153942)			
	Zone esclave	IP maître	Nom serveur maître	Mail contact technique	SOA	Transfert de zone
1	0.9.5.nrenum.net	193.49.159.2	ns1.renater.fr.	hostmaster@renater.fr	2013021504	OK
2	2.6.2.nrenum.net	193.49.159.2	ns1.renater.fr.	hostmaster@renater.fr	2013021504	OK
3	3.3.nrenum.net	193.49.159.2	ns1.renater.fr.	hostmaster@renater.fr	2015042735	OK
4	4.9.5.nrenum.net	193.49.159.2	ns1.renater.fr.	hostmaster@renater.fr	2013021504	OK
5	6.9.5.nrenum.net	193.49.159.2	ns1.renater.fr.	hostmaster@renater.fr	2013021504	OK
6	7.8.6.nrenum.net	193.49.159.2	ns1.renater.fr.	hostmaster@renater.fr	2013021504	OK
7	9.8.6.nrenum.net	193.49.159.2	ns1.renater.fr.	hostmaster@renater.fr	2013021504	OK
8	ades.cnrs.fr	147.210.72.192	camus.dr15.cnrs.fr.	hostmaster@dr15.cnrs.fr	2018032701	OK
9	adess.cnrs.fr	147.210.72.192	camus.dr15.cnrs.fr.	hostmaster@dr15.cnrs.fr	2018032801	OK
10	adm.cnrs-gif.fr	157.136.10.1	hermes.cnrs-gif.fr.	informatique@dr4.cnrs.fr	2018121108	OK
11	afsr.cnrs.fr	193.49.15.1	iresco-1.pouchet.cnrs.fr.	Le serveur maître ne répond pas		KO
12	agriped.fr	195.221.212.199	ns1.osupytheas.fr.	dns@osupytheas.fr	2018092001	OK
13	alpes.cnrs.fr	147.173.176.87	ns1.dr11.cnrs.fr.	admin@dr11.cnrs.fr	2018120601	OK
14	ampere-lab.cnrs.fr	156.18.22.3	cri03.cri.ec-lyon.fr.	dnsmaster@ec-lyon.fr	2018071601	OK
15	ampere-lab.fr	156.18.22.3	cri03.cri.ec-lyon.fr.	dnsmaster@ec-lyon.fr	2018071601	OK
16	ampere-lyon.cnrs.fr	156.18.22.3	cri03.cri.ec-lyon.fr.	dnsmaster@ec-lyon.fr	2018071601	OK
17	ampere-lyon.fr	156.18.22.3	cri03.cri.ec-lyon.fr.	dnsmaster@ec-lyon.fr	2018071601	OK
18	aquitaine.cnrs.fr	147.210.72.192	camus.dr15.cnrs.fr.	hostmaster@dr15.cnrs.fr	2018112301	OK
19	aquitaine-limousin.cnrs.fr	147.210.72.192	camus.dr15.cnrs.fr.	hostmaster@dr15.cnrs.fr	2018062501	OK
20	archam.cnrs.fr	193.49.19.1	mx1.mae.u-paris10.fr.	adminserver@mae.u-paris10.fr	2018092101	OK
21	archeotransfert.cnrs.fr	147.210.72.192	camus.dr15.cnrs.fr.	hostmaster@dr15.cnrs.fr	2018032702	OK
22	archeovision.cnrs.fr	147.210.72.192	camus.dr15.cnrs.fr.	hostmaster@dr15.cnrs.fr	2018112701	OK
23	archi.fr	193.50.232.12	corbu.gamsau.archi.fr.	dnsmaster@archi.fr	2018122101	OK
24	argos.cnrs.fr	157.136.10.1	hermes.cnrs-gif.fr.	informatique@dr4.cnrs.fr	2018041200	OK
25	arp.cnrs.fr	193.52.92.2	euclide.ens-rennes.fr.	hostmaster@bretagne.ens-cachan.fr	2018092701	OK
26	asie-pacifique.cnrs.fr	195.220.198.130	Nom DNS inconnu	dnsmaster@dr1.cnrs.fr	2018082701	OK
27	auteuil.cnrs-dir.fr	193.55.76.241	gauguin.dmz.cnrs-dir.fr.	dnsmaster@cnrs-dir.fr	2018122102	OK

Contrôler la syntaxe des zones après maj

Attention, en présence d'une erreur de syntaxe dans un fichier de zone Bind ne le signale pas lors d'un simple « `rndc reload` », mais uniquement en redémarrant le service.

Pour éviter cela on peut utiliser les outils dédiés de Bind :

- **named-checkconf** pour les fichiers de configuration
- **named-checkzone** pour les fichiers de zones

On peut également contrôler la bonne progression du n° de serial.

Exemple d’exploitation via script Bash

```
root@t2gpns0:~ [2021/11/03-14:40:38]
#reload cnrs.fr
~~~~~ Generation de la liste des zones DNS maitres - 2021/11/03 14:40:49 ~~~~~~
Generation du fichier:
 - /data/parser/liste_zones_20211103_144049.txt .............................OK
~~~~~~~~~~~~~~~~ Liste generee avec succes - 2021/11/03 14:40:49 ~~~~~~~~~~~~~~~~

~~~~~~~~~~ Validation de la configuration DNS - 2021/11/03 14:40:49 ~~~~~~~~~~
Controles des fichiers de configuration:
 - named.conf et ses includes.....................................................OK
 - Controle des fichiers de zones.................................................OK
~~~~~~~~~ Configuration et 170 zones maitres OK - 2021/11/03 14:40:55 ~~~~~~~~~
zone reload up-to-date
Rechargement de la zone cnrs.fr OK
```

Ventiler les fichiers de configuration Bind

Par défaut l'ensemble de la configuration Bind est dans l'unique fichier /etc/**named.conf**

En y utilisant la clause « `include` » on peut ventiler les différentes sections pour une meilleures visibilité. On peut alors utiliser des fichiers dédiées pour la définition des zones standards, inverses, les logs, etc.

```
root@t2gpns0:/etc/named [2021/11/03-18:01:12]
#ls
controls.conf  masters.conf         masters_reverse.conf  rndc-cnrs-dir.key  tsig.key
logging.conf   masters_dnssec.conf  options.conf          slaves_cnrs.conf
```

Extrait de named.conf :

```
// ################################
// # Definition des ZONES MAITRES #
// ################################

// Definition des ZONES LOCALES (rfc1912)
include "/etc/named.rfc1912.zones";

// Definition des ZONES MAITRES
include "/etc/named/masters.conf";

// Definition des ZONES MAITRES DNSSEC
include "/etc/named/masters_dnssec.conf";

// Definition des ZONES MAITRES REVERSE
include "/etc/named/masters_reverse.conf";

// Definition des ZONES ESCLAVES -> Pour DSI.CNRS.FR
include "/etc/named/slaves_cnrs.conf";

// FIN DU FICHIER "named.conf"
```

Ventiler les logs pour un meilleur suivi

Par défaut l'ensemble des logs sont stockés dans un fichier unique. Il est conseillé de les ventiler par type via la section « logging » sous Bind par exemple.

`/var/log/queries/queries.log`	*Requêtes clientes*
`/var/log/lamers.log`	*Erreurs serveurs DNS distants*
`/var/log/xfer-out.log`	*Transferts de zones sortant*
`/var/log/xfer-in.log`	*Transferts de zones entrant*
`/var/log/client.log`	*Erreurs lors émission réponse*
`/var/log/default.log`	*Autres messages*

Il peut être judicieux d'exploiter ces logs pour réaliser des statistiques afin de détecter d'éventuelles dérives.

Par exemple la commande suivante fournit le palmarès des IP des 10 plus gros requêteurs :

```
cat /var/named/chroot/var/log/queries/queries.log* | cut -d" " -f6 | cut -d"#" -f1 | sort | uniq -c | sort -nr | head -10
```

Des utilitaires tiers comme **dnstop** ou **dnsperf** offrent des tableaux de bord complets.

Il est recommandé de centraliser les logs sur un serveur de log distant.

Gestion « industrielle » : IPAM

À l'inverse de la gestion « manuelle », il est possible de gérer l'ensemble des informations du DNS dans une base externe au serveur de nom.

Il existe des outils libres ou commerciaux, les **IPAM** (IP Address Management), permettant de maintenir un référentiel des données du DNS : noms de domaines, noms des machines, sous-réseaux, adresses IP etc.

Avantages des IPAM

- Cohérence des données (ex: création auto du PTR associé à un type A).
- Gestion intégrée d'autres services d'infrastructure (DHCP, routage de messagerie, etc.
- Délégation d'admin sur des périmètres restreints via une IHM web.
- Gestion de workflow de validation.
- Automatisation de certaines tâches (renommage en masse, etc.)
- Application systématique de politiques (respect d'une politique nommage spécifique aux postes de travail ou aux interfaces de routeurs, etc.)
- Fourniture de ressources IP/DNS via des API (pour un IaaS par exemple).

Risques induits par les IPAM

- Plus grand complexité, et donc des difficultés de débogage, en raison des dépendances entre les différents éléments : outils de génération, interface web, authentification des utilisateurs, base de données, etc.
- Un filtrage et des restrictions d'accès sévères sont indispensables (pas d'ouverture de l'IHM sur l'Internet).
- En cas de faille de sécurité dans l'outil il y risque de compromission.
- La rapidité de correction des failles sur les briques embarquées (Bind notamment) dépend de la réactivité de l'éditeur de l'IPAM. C'est habituellement bien moins réactif que pour des distributions classiques.

Synchroniser les zones sur les résolveurs internes

Afin d'éviter les latences de mise à jour des zones liées au TTL, il est possible de déclarer ses zones sur les résolveurs internes.

Elles y servent uniquement de cache, bénéficiant d'une notification active de la part du NS maître (clause « `notify-also` » sous Bind).

Techniquement ces résolveurs seront des NS esclaves non officiels « stealth » qui n'apparaissent pas dans la délégation des zones concernées.

Sauvegardes

- Sauvegarde distante classique

- Sauvegarde périodique du delta de la config Bind (locale ou distante):

```
# 20120402 OPR Sauvegarde config Bind locale via rsync toutes les 5 minutes
*/5 * * * * rsync --force --ignore-errors --delete --backup --backup-
dir=/bak_rsync/MASTERS_$(date +%Y%m%d_%H%M%S) -av /var/named/MASTERS /bak_rsync
```

  Offre une sauvegarde de la config courante ainsi que l'historique de tous les deltas avec une granularité de 5 minutes.

Rmq: on ne peut considérer les NS esclaves comme des sauvegardes car ils peuvent eux-mêmes être impactés par un incident ou une attaque.

Illustration d’incidents classiques

La délégation de la zone parente ne publie pas les mêmes NS que la zone .

```
dig +trace NS dr42.cnrs.fr

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.7 <<>> +trace NS dr4.cnrs.fr
;; global options: +cmd
.                       276815  IN      NS      l.root-servers.net.
.                       276815  IN      NS      g.root-servers.net.
.                       276815  IN      NS      e.root-servers.net.
.                       276815  IN      NS      i.root-servers.net.
.                       276815  IN      NS      j.root-servers.net.
.                       276815  IN      NS      d.root-servers.net.
.                       276815  IN      NS      k.root-servers.net.
.                       276815  IN      NS      f.root-servers.net.
.                       276815  IN      NS      c.root-servers.net.
.                       276815  IN      NS      b.root-servers.net.
.                       276815  IN      NS      m.root-servers.net.
.                       276815  IN      NS      a.root-servers.net.
.                       276815  IN      NS      h.root-servers.net.
;; Received 1097 bytes from 10.232.200.1#53(10.232.200.1) in 5 ms

fr.                     172800  IN      NS      d.nic.fr.
fr.                     172800  IN      NS      e.ext.nic.fr.
fr.                     172800  IN      NS      f.ext.nic.fr.
fr.                     172800  IN      NS      g.ext.nic.fr.
;; Received 623 bytes from 2001:500:a8::e#53(e.root-servers.net) in 1 ms

cnrs.fr.                172800  IN      NS      ns0.cnrs.fr.
cnrs.fr.                172800  IN      NS      ns2.cnrs.fr.
cnrs.fr.                172800  IN      NS      ns3.cnrs.fr.
cnrs.fr.                172800  IN      NS      camus.dr15.cnrs.fr.
cnrs.fr.                172800  IN      NS      panoramix.rap.prd.fr.
;; Received 724 bytes from 193.176.144.22#53(e.ext.nic.fr) in 20 ms

dr42.cnrs.fr.           3600    IN      NS      graal.dr42.cnrs.fr.
dr42.cnrs.fr.           3600    IN      NS      ns4.cnrs.fr.
;; Received 168 bytes from 193.50.20.1#53(panoramix.rap.prd.fr) in 6 ms

dr42.cnrs.fr.           180     IN      NS      themis.dr42.cnrs.fr.
dr42.cnrs.fr.           180     IN      NS      ns4.cnrs.fr.
;; Received 185 bytes from 2001:660:500a:2210::11#53(ns4.cnrs.fr) in 0 ms
```

Dans cet exemple le NS themis.dr42.cnrs.fr (un « nouveau » NS maître) de la zone ne pourra **jamais** être sollicité par des résolveurs publics car son nom n'est pas diffusé par la délégation parente : il leur reste inconnu.

Il vont par contre 50% du temps solliciter graal.dr42.cnrs.fr qui n'existe plus, ce qui entrainera la réitération vers l'autre NS valide.

Ce genre d'incident est assez courant et peut rester non détectée tant qu'un seul NS valide reste délégué.

Le niveau de résilience de la zone devient alors très faible malgré la présence de 2 NS parfaitement opérationnels mais qui sont ne sont pas tous « publiés ».

Si l'unique NS publié venait à ne plus être joignable l**a zone ne sera plus résolvable depuis l'Internet.**

Vérifiez que la délégation de vos zones est à jour !

Qui contacter pour maj la délégation ?

Une demande de maj de la délégation dans la zone parente doit être systématiquement demandée lors de l'évolution de la liste des NS.

Exemple de cas :

zone **xxx.cnrs.fr :** il faut demander la maj à la DSI du CNRS -> dnsmaster@dsi.cnrs.fr

Zone **xxx.fr** :

- Si réservé via Renater suivre la procédure Renater.
- Si réservé via un registrar privé (OVH, Gandi, NameShield, etc.) utiliser leur IHM d'administration.

Autres TLDs que .fr : utiliser l'IHM d'administration du registrar concerné.

DNS et messagerie

DNS et messagerie
Les **MX**

Les serveurs SMTP d'une zone sont publiés au travers des enregistrements de type « MX ».

On y associe un indice de priorité permettant une répartition de charge de type round robin.

Lorsqu'un serveur est déclaré avec un « poids » faible il est prioritaire.

Mais attention, même dans ce cas certaines requêtes seront affectées au serveur(s) non prioritaire(s).

DNS et messagerie
Se prémunir du « phishing » : SPF

Une zone DNS peut publier les serveurs SMTP ayant autorité pour l'envoi de mails avec ce domaine en clause « FROM ». Cela se fait au travers d'un enregistrement de type « Sender Policy Framework » (RFC4408). Il s'agit d'une entrée de type « TXT » ou « SPF » déclarant les serveurs SMTP valides.

Exemple de syntaxe :

```
@ IN TXT "v=spf1 mx mx:smtprelay.cnrs.fr a:sgaia1.dsi.cnrs.fr -all"
```

DNS et messagerie
Signer un domaine de messagerie : DKIM

Le « DomainKeys Identified Mail » (RFC4871) ajoute une signature dans l'entête du message qui authentifie le domaine expéditeur.

Exemple de syntaxe dans le fichier de zone :

```
dkim._domainkey.secours IN TXT "v=DKIM1;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDI8W7ZkozIjg1R9kavGJj
Peief5Tdf++wIA4mVbOGAn3xsh8WPHoL2OGqEl7xKZcfCyBFhlI3bkb31hsWv
7SDyoVP4IBO/K7hYufrzLt3zIWmijAWerEhgPx91u3cxHN3KRxT4e30DE4gVq
jZQom4xKUaMtULO5pDh13xxTwgn3wIDAQAB"
```

Rmq: syntaxe d'une entrées DKIM > 1024 bits

Bind n'accepte pas d'entrée TXT de plus de 256 caractères d'une traite.

La clef doit être découpée en 2 chaînes plus courtes déclarées sur la même ligne, encadrées par des doubles guillemets.

Exemple:

```
dkim._domainkey    TXT    "v=DKIM1;k=rsa;p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC
gKCAQEArxq3wCEVvfOVNbAnGypE8aFTF0Htm32DeQ2ouQppEsF77O9uhK6H/N/5hotosZBdSwxHPLfnf
WuDUD2L7n+cwPoMsr0zZZUwot8VkxFlnmmqdulv7lDOHftVRFZwUKs51dx3aWRkF2s+FOU""0I5S7oWg
DVq+mpVR87AieSmaxAHPFl6C1gfGSF+Q/M+hUVkYEYhXj45e6rlUdgE6hjw3T7U4gRRvxCSDCfol+MSn
I+D2OzfzVGU7bPtB9t6Efw4WoW6VLHlgyhWNUYVxwRVO3UbbwkBYAewssYxxndWHeXmztY5NxjR8z0mK
iiSlj5FjaIZlBHjtULwDkQvOPbjJzQQIDAPAK"
```

DNS et messagerie
Résolveur locaux sur les serveurs SMTP

Les serveurs de messagerie sont très consommateurs de requêtes DNS.

Il peut être intéressant d'installer localement sur ces machines un résolveur DNS (par exemple Unbound) qui permettra de profiter de son cache localement et déchargera le résolveur mutualisé habituel.

Infos diverses

Caches DNS sur les clients

Il faut avoir conscience qu'il existe une chaîne de cache DNS entre les serveurs ayant autorité et le poste client.

Cela explique souvent la persistance d'une ancienne valeur.

Un exemple de 5 strates :

1. Serveur ayant autorité	-
2. Résolveur Bind en DMZ	NS esclave non officiel chez nous -> immédiat
3. AD Microsoft	Cache piloté par le TTL de la zone
4. OS Microsoft	Voir « **`ipconfig /flushdns`** »
5. Firefox	Voir « **`network.dnsCacheExpiration`** »

Comportement par défaut des applis clientes

Il faut également garder en tête que les applications peuvent interpréter les requêtes DNS avec des politiques qui leur sont propres.

Par exemple un navigateur web utilisera le TLD « .com » par défaut.

Et en l'absence de l'entrée DNS racine demandée, Firefox testera automatiquement la déclinaison en « www. » de manière transparente.

On pourrait alors penser que la racine est déclarée au niveau DNS alors que cela n'est pas le cas.

Rmq: ce comportement par défaut Firefox peut être désactivé: **`browser.fixup.alternate.enabled`**

Résolveurs (trop ou pas assez) publics

Il n’est pas conseillé d’utiliser des résolveurs ouverts « publics » comme Google (8.8.8.8) car on n’est pas certain de l’intégrité de la réponse (dans une optique commerciale par exemple), ni du respect du protocole (durées de TTL, etc.)

Si besoin la DSI propose 2 résolveurs récursifs aux unités CNRS :

- ns10.cnrs.fr
- ns11.cnrs.fr

Restriction d’accès à l’IP cliente.

DNSsec …

Les apports de DNSsec

DNSSEC garantit l'intégrité des informations servies par le DNS.

Chaque enregistrement est augmenté d'une signature cryptographique.

Au moment de la résolution, la signature est validée.

Comme le DNS est hiérarchique, il est nécessaire d'établir une chaîne de confiance de la racine jusqu'à la zone feuille.

La zone parente doit être signée et une délégation vers la zone fille doit exister (enregistrement de type DS, **D**elegation **S**igner).

DNSsec induit des risques opérationnels nouveaux

- Risques d'expiration : les clefs et signatures possèdent une date d'expiration. Au-delà les enregistrements servis par le DNS seront invalides pour les résolveurs qui vérifient la signature, même si l'infra DNS est OK.
- Risque de compromission des clefs : il faut sécuriser les clefs privées servant à signer les clefs ou les zones. Pb classique de gestion des clefs.
- Risque d'inaccessibilité de la zone : diverses raisons peuvent empêcher la résolution sur une zone sécurisée par DNSsec: filtrage de paquets DNS particuliers (EDNS0 notamment), désynchro NTP, filtrage des fragments IP ou des messages ICMP, etc. Il s'agit souvent de firewalls ou de relais applicatifs mal configurés. Un pourcentage d'utilisateurs risque ainsi de ne pas pouvoir résoudre des enregistrements DNS à cause de DNSsec.

Mise en œuvre de DNSsec

Il faut générer deux types de clef :

- la KSK (Key Signing Key) qui servira à signer les clefs
- la ZSK (Zone Signing Key) qui servira à signer la zone

Il faut ensuite ajouter les clefs à la zone. Puis il faut signer la zone et la redéployer.

Rotation des clefs

Les signatures ayant une date d'expiration il convient d'anticiper celle-ci en publiant deux clefs à un instant donné :

- une clef A active, qui expire à un instant T,
- une clef B inactive, qui expire à un instant T+3 mois par exemple

La transition de la clef A vers la clef B doit se faire avant l'expiration de la clef A. La clef B est créée par anticipation pour qu'elle soit présente dans les caches des résolveurs au moment où on effectue la transition. La rotation des clefs doit être automatisée.

DNSsec et la zone cnrs.fr

Actuellement les ressource dédiée au DNS à la DSI du CNRS ne sont pas suffisantes pour assurer correctement la signature DNSsec des zones.

Mais la non signature de cnrs.fr bloque les sous-domaines qui souhaitent adopter DNSsec.

Une évolution est entrevue début 2022:

- Recrutement d'une personne pour renforcer l'équipe (diffusion en cours).
- Bascule de la gestion des zones publique vers notre IPAM *Efficient IP* en tant que NS maître « caché ». C'est lui qui gérera la rotation des clefs.

Synthèse des recommandations

	Continuité et intégrité du service			Sécurité des infos	Confort
	Critique	Important	Conseillé		
Renouvellement de la délégation	X				
Au moins un NS esclave	X				
Restreindre la résolution récursive	X				
Isolement Résolveur/Autorité		X			
Isolement zones privées/publiques		X			
Isolement NS management/publics			X		
Plusieurs NS esclaves		X			
NS sur réseaux distincts		X			
Panachage OS & serveur DNS			X		
Interface d'administration *					X
Virtualisation *					X
DNSsec **				X	
Messagerie : DKIM et SPF				X	
Chrootage du service			X		
Ventilation des fichiers de config					X
Ventilation des logs					X

* : peut potentiellement engendrer une faiblesse de sécurité
** : peut potentiellement bloquer la résolution si mal géré

Maj: on peut ajouter la signature TSIG en « critique »

Référence

FIABILISATION ET SECURISATION DU DNS

Best Practice Document

Groupe de travail « DNS » du GIP RENATER

Auteurs:

Jean Benoit - jean@unistra.fr (Université de Strasbourg/GIP RENATER)

Olivier Prins - olivier.prins@dsi.cnrs.fr (CNRS/GIP RENATER)

3/12/2013