ERCOM

UPEC
UNIVERSITÉ PARIS-EST CRÉTEIL

IUT
SENART
FONTAINEBLEAU

Le DNS

Damien SIMONET
damien@mysimonet.fr

16-Sept
2015

Le DNS

- Source Wikipedia : Le **Domain Name System** (ou **DNS**, système de noms de domaine) est un service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom.

- Dans ce cours, je ne parle que de ce qu'il est nécessaire de comprendre pour Exchange.
  - Je ne traite pas des enregistrements SRV, SOA…
  - Je ne parle pas des registrar

ERCOM

FQDN (Fully Qualified Domaine Name)

- Un FQDN (ou nom de domaine complètement qualifié) est un nom de domaine qui révèle la position absolue d'un nœud dans l'arborescence DNS en indiquant tous les domaines de niveau supérieur jusqu'à la racine.

- *commons.wikimedia.org.* est un FQDN car aucun sous-domaine supérieur n'est omis et il se termine par un point final.
- *commons* et *commons.wikimedia* ne sont pas des FQDN car les domaines de niveau supérieur sont omis.

CRYPTOSMART

BY ERCOM

Les types d'enregistrement

A. A
B. CNAME
C. TXT
D. MX

ERCOM

L’enregistrement A

- **L’enregistrement A permet de relier un nom d’hôte à l’adresse IP d’un serveur**
  - **nomdedomaine.com** vers un serveur portant l’IP **.31.192.222.xxx**
  - **Ex:**
    - **nomdedomaine.com** A **46.31.192.222 .xxx**
    - **www.nomdemonaine.com** A **46.31.192.222.yyy**
    - **intranet.mondomaine.com** A **46.31.192.222.zzz**

L’enregistrement CNAME

- **L’enregistrement CNAME permet de relier un nom d’hôte vers l’enregistrement DNS d’un autre nom d’hôte.**
  - **C’est le principe d’alias**
  - **blog.nomdemonaine.com** doit pointer vers la même IP que **www.nomdedomaine.com**

  - **Ex :**
    - **blog.nomdemonaine.com** CNAME **www.nomdedomaine.com**
    - **blog2.nomdemonaine.com** CNAME **www.nomdedomaine.com**
    - **blog3.nomdemonaine.com** CNAME **www.nomdedomaine.com**

Pourquoi créer un CNAME plutôt qu'un enregistrement A ?

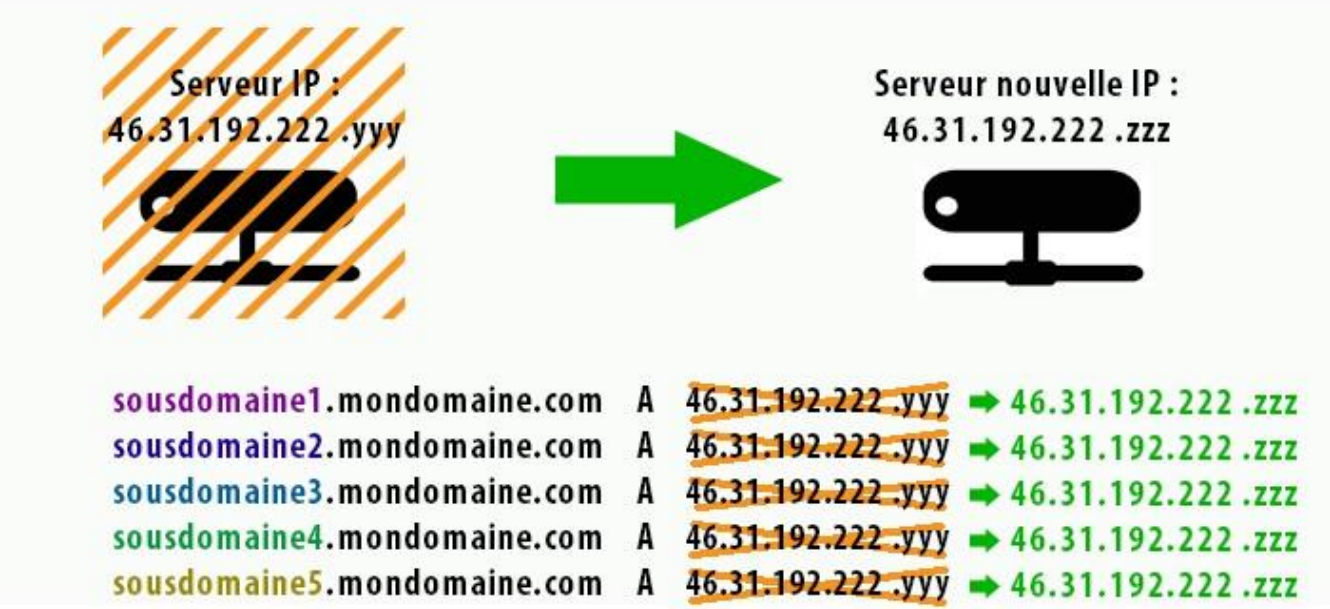
- Imaginons que vous ayez de nombreux sous-domaines qui doivent pointer vers une même adresse IP :

- Vous pouvez créer, pour chacun de ces sous-domaines, des enregistrements de type A :

```
sousdomaine1.mondomaine.com   A   46.31.192.222 .yyy
sousdomaine2.mondomaine.com   A   46.31.192.222 .yyy
sousdomaine3.mondomaine.com   A   46.31.192.222 .yyy
sousdomaine4.mondomaine.com   A   46.31.192.222 .yyy
sousdomaine5.mondomaine.com   A   46.31.192.222 .yyy
```

Pourquoi créer un CNAME plutôt qu'un enregistrement A ?

- Mais si un jour, l'IP de votre serveur change, il vous faut modifier chacun des enregistrements de type A individuellement :



- **Le CNAME permet d'éviter des modifications multiples.**

Pourquoi créer un CNAME plutôt qu'un enregistrement A ?

- En effet, si vous créez vos enregistrements DNS ainsi :

```
sousdomaine1.mondomaine.com   A   46.31.192.222 .yyy
sousdomaine2.mondomaine.com   CNAME   sousdomaine1.mondomaine.com.
sousdomaine3.mondomaine.com   CNAME   sousdomaine1.mondomaine.com.
sousdomaine4.mondomaine.com   CNAME   sousdomaine1.mondomaine.com.
sousdomaine5.mondomaine.com   CNAME   sousdomaine1.mondomaine.com.
```

- **En cas de changement d'IP de votre serveur, vous n'aurez qu'UN SEUL enregistrement à modifier :**

```
sousdomaine1.mondomaine.com   A   46.31.192.222 .yyy ➡ 49.31.192.222.zzz
sousdomaine2.mondomaine.com   CNAME   sousdomaine1.mondomaine.com.
sousdomaine3.mondomaine.com   CNAME   sousdomaine1.mondomaine.com.
sousdomaine4.mondomaine.com   CNAME   sousdomaine1.mondomaine.com.
sousdomaine5.mondomaine.com   CNAME   sousdomaine1.mondomaine.com.
```

L’enregistrement TXT

- **L’enregistrement TXT permet d’intégrer une zone DNS en texte libre**
- Il est notamment utilisé par prouver que vous avez accès aux paramètres DNS (et donc que vous êtes propriétaire du domaine).
  - Par exemple, si vous souhaitez acheter un certificat ssl pour votre domaine « www.lpassr.com », il y a de fortes chances pour que votre tiers de confiance (GlobalSign, Symantec, OVH, Gandi…) ne vous demande d’ajouter un enregistrement TXT vous vérifier que vous êtes le propriétaire de la zone.
  - C’est aussi utilisé par Google quand vous voulez souscrire à Google Apps
    - https://support.google.com/a/answer/2716800?hl=fr
- Il est aussi utilisé pour lister les serveurs autorisés à expédier des courriers électroniques depuis votre nom de domaine.
  - (Pour information, on appelle cela un SPF : https://fr.wikipedia.org/wiki/Sender_Policy_Framework)
  - Son utilisation est facultative, mais recommandé (Sur mon domaine mysimonet.fr, je ne l’ai pas ajouté).

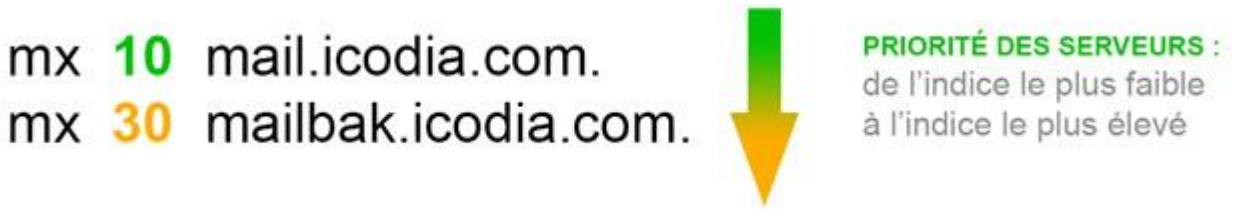
- **www.lpassr.com** doit envoyer le message « JeSuisProprietaireDuDomaine »

  - **Ex :**
    - **www.lpassr.com** TXT ``**JeSuisProprietaireDuDomaine**``

ERCOM

L’enregistrement MX

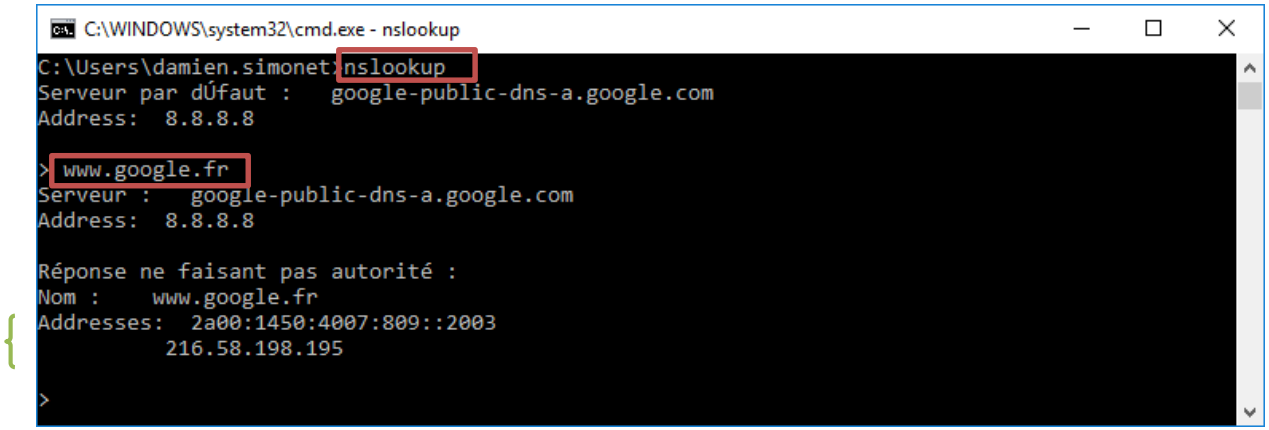
- **L’enregistrement MX** définit **quel est ou quels sont les serveurs qui gèrent les services emails** reliés à un nom de domaine.
- Afin que vos boîtes email soient toujours accessibles, il est fortement recommandé de paramétrer plusieurs enregistrements MX :
- Si le serveur principal qui gère votre courrier n’est pas disponible, les emails envoyés sur les adresses liées à votre nom de domaine seront redirigés vers un ou plusieurs serveurs secondaires, afin de garantir que l’email puisse bien être distribué.
- L’ordre de priorité pour chacun des enregistrements MX, est défini par une numérotation :
- Le serveur principal vers lequel les emails seront aiguillés en priorité portera un nombre plus petit, le ou les serveurs secondaires un nombre plus grand.



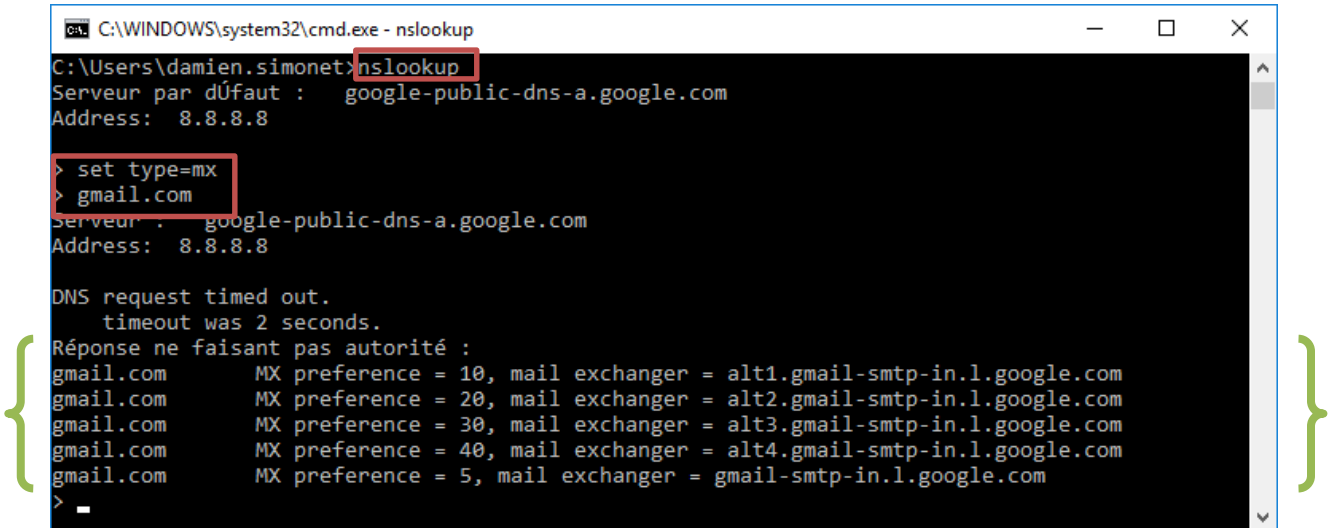
- Il est recommandé de numéroter les priorités de 10 en 10, afin de pouvoir, le cas échéant, intercaler un serveur supplémentaire entre deux enregistrements.

Consulter des enregistrements DNS

- On utilise la commande nslookup :



- Pour consulter les enregistrements MX et TXT, on précise le type :



Pour information : Le TTL (Durée de vie)

- Dans le protocole utilisé par les serveurs DNS, une donnée *Time to Live* est présente et indique le temps, **en secondes**, pendant lequel l'information donnée par le serveur DNS peut être conservée en cache. Passé ce délai, l'information doit être considérée comme obsolète et être mise à jour.
- Le TTL est en général de l'ordre d'un jour (TTL = 86400), il peut être réduit jusqu'à 0 pour des informations variant fréquemment.

- Cela veut dire que lorsque vous faites une modification sur un enregistrement DNS, le délai de propagation dépendra du TTL fixé.

- Lp66.mysimonet.fr 600 IN A 151.80.90.66 → Le TTL est de 600 secondes
- Lp65.mysimonet.fr 10800 IN MX 40 lp65.mysimonet.fr. → Le TTL est de 10800 secondes

Pour information : Le PTR

- Un enregistrement PTR associe une adresse IP à un nom d'hôte. (reverse DNS).
- La plupart des serveurs de messagerie entrant contrôlent l'authenticité du serveur de messagerie pour courrier sortant.
  - Le serveur de courrier entrant contrôle si l'adresse IP utilisée par le serveur de courrier sortant correspond au nom de ce serveur.

- https://onlinehelp.cloud.telenet.be/article.php?id=1292

Pour aller plus loin…

- Dans ce cours, j'ai repris l'excellent support de Icodia :
  - https://docs.icodia.com/general/zones-dns
  - J'y apporte quelques nuances et j'ai structuré le cours en fonction de vos besoins pour le TP Exchange.
  - Vous avez beaucoup de documentation à ce sujet sur internet