DNS – Zones et enregistrements

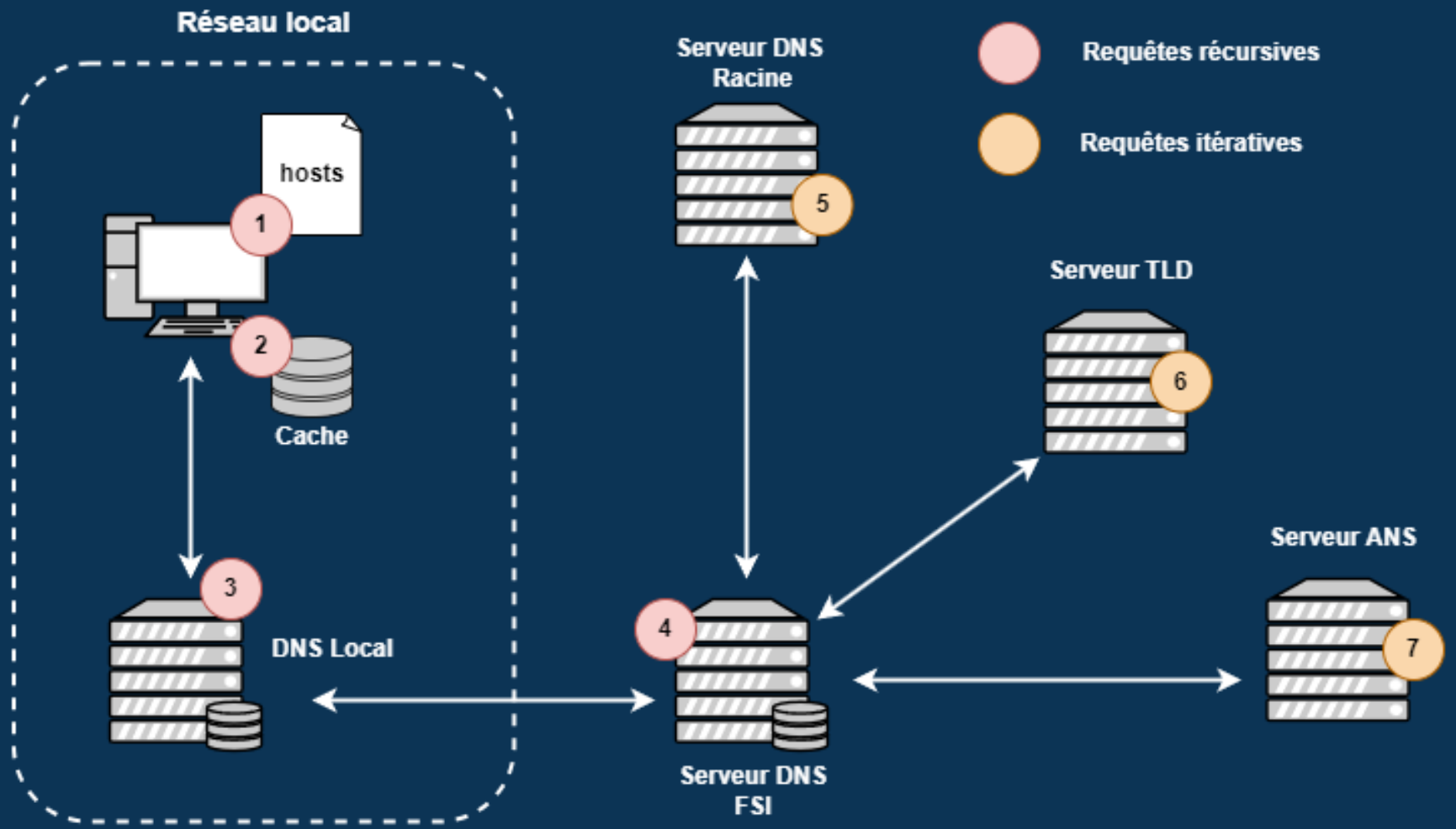
420-2S5-EM

Serveur 1 – Services intranet

Retour sur l'introduction

- Le service DNS permet une résolution de nom hiérarchique.
- Chaque serveur de cette hiérarchie s'occupe d'une portion précise du nom à résoudre.
- Les serveurs DNS peuvent gérer des requêtes récursives ou itératives.
- La mémoire cache des clients et des serveurs DNS permet d'accélérer le processus de résolution en évitant de résoudre une requête qui a été déjà été résolu.

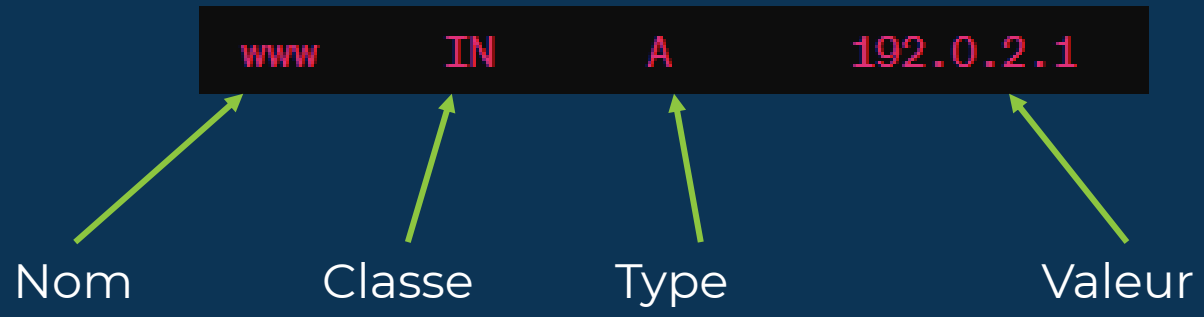
Retour sur le processus de résolution



ÉDOUARD MONTPETIT
CÉGEP D'AVENIR

Les enregistrements DNS

Pour qu'un serveur DNS puisse traduire un nom en IP, celui-ci doit posséder les données qu'on lui demande de traduire, soit le nom concerné par la requête et l'adresse IP correspondante. Cette correspondance, c'est ce que l'on nomme un enregistrement. Exemple:



ÉDOUARD MONTPETIT
CÉGEP D'AVENIR

Les zones de recherche

Les enregistrements sont stockés dans des zones.

Une zone de recherche contient tous les enregistrements d'un nom de domaine.

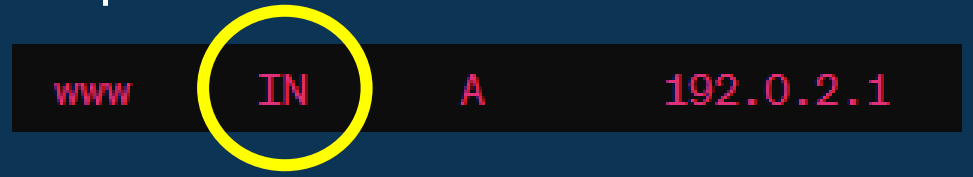
Il existe deux types de zone de recherche:

Principal: Ces zones sont ouvertes en écriture. Les enregistrements y sont donc modifiables.

Secondaire: C'est une copie de la zone principale et elle n'est disponible qu'en lecture seule. Les zones secondaires permettent de distribué la charge de travail entre les serveurs DNS.

Les classes d’enregistrement

Les classes d’enregistrement sont un héritage de la structure originelle du système de noms de domaine (DNS). Elles ont été conçues à une époque pour supporter différents types de réseaux et d’infrastructures sur Internet et au sein de systèmes informatiques.



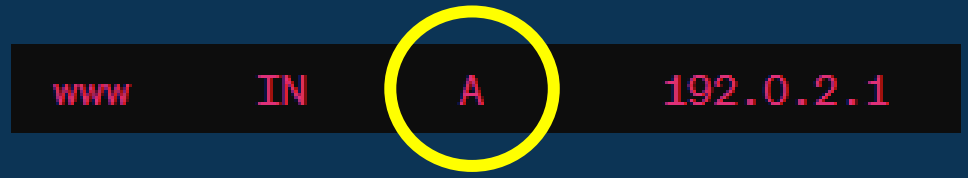
Aujourd’hui, toutes les autres classes autres que « IN » (internet) sont devenues obsolètes.

Vous devez donc toujours utiliser la classe « IN ».

ÉDOUARD MONTPETIT
CÉGEP D'AVENIR

Les types d’enregistrement

Les types d’enregistrement détermine le type d’information que l’on retrouvera dans la valeur d’un enregistrement donné.



Dans cet exemple, le type d’enregistrement « A » nous indique que la valeur sera une adresse IP, laquelle sera associé au nom d’hôte « www ».

ÉDOUARD MONTPETIT
CÉGEP D'AVENIR

Les types d'enregistrement

Type	Explication
A	Ce type d'enregistrement permet d'associer un nom de domaine à une IP.
AAAA	C'est la même chose que l'enregistrement « A » mais pour l'IPv6
CNAME	Permet de définir un alias pour un nom de domaine existant.
MX	Spécifie les serveurs de messagerie utilisés pour les courriels d'un domaine particulier.
NS	Indique les serveurs DNS autoritaires pour le domaine.
SOA	Contient plusieurs informations essentielles sur le domaine.
SRV	Permet de spécifier l'emplacement des serveurs pour des services spécifiques.
TXT	Contient du texte, ni plus ni moins. Ces enregistrements sont souvent utilisés dans les politiques d'envoi de courriels par exemple.

Exemple de zone

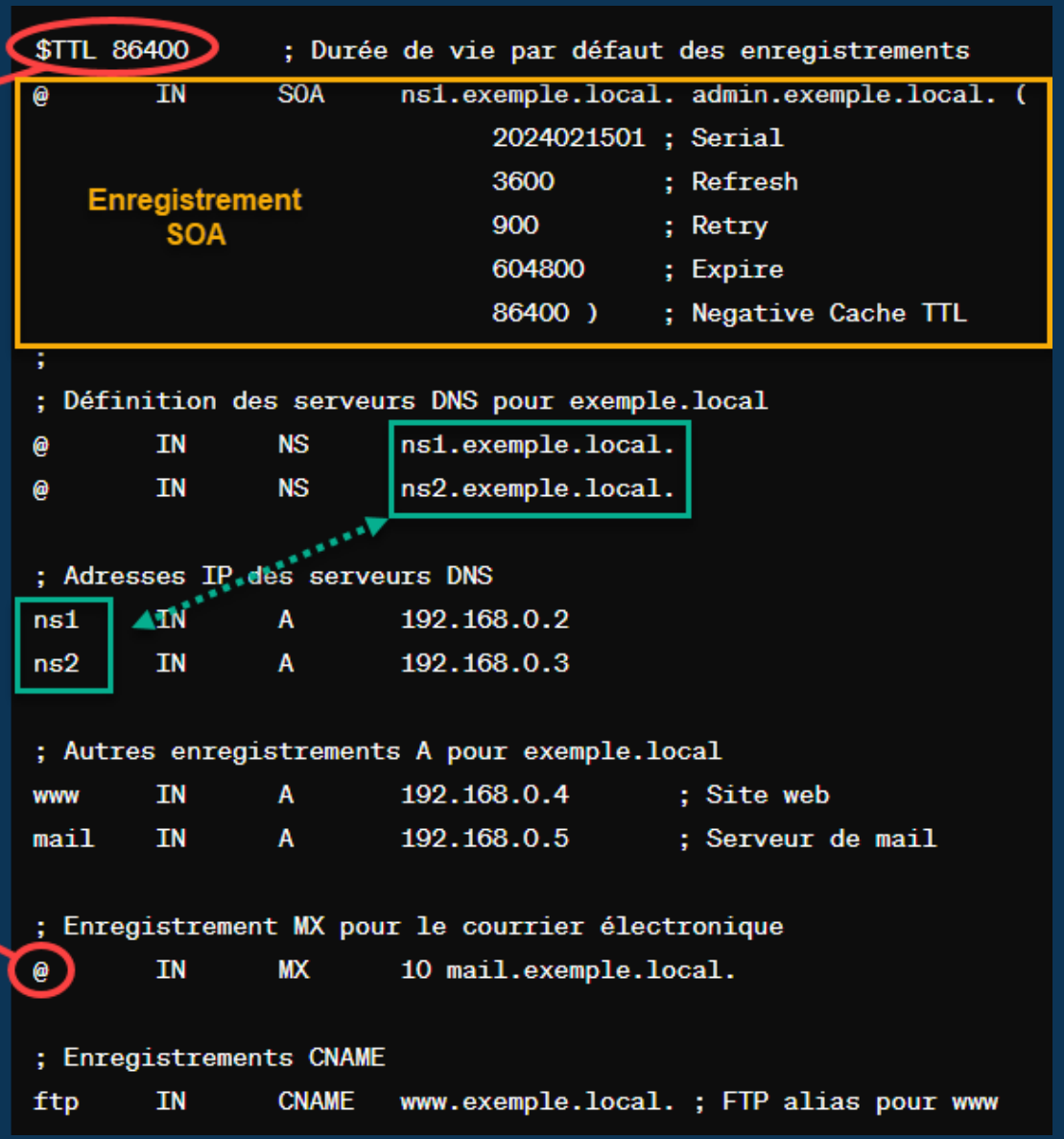
TTL : Time To Live

Le TTL est une valeur exprimée en secondes. Ici 86400 est l'équivalent de 24h. C'est la durée de vie qu'auront les enregistrements dans les différentes mémoires caches des clients.

@ : alias du domaine

Le caractère « @ » est particulier dans les fichiers de zone. En effet, celui-ci est un alias du nom de domaine. Donc que vous écriviez exemple.local ou « @ », c'est exactement la même chose.

Le caractère « ; » permet d'insérer des commentaires!



ÉDOUARD MONTPETIT
CÉGEP D'AVENIR

L'entrée SOA

Courriel de l'administrateur de la zone. Le « @ » est remplacé par un « . »

```
@       IN      SOA     ns1.exemple.local.  admin.exemple.local. (
                        2024021501 ;        Serial
                        3600       ;        Refresh
                        900        ;        Retry
                        604800     ;        Expire
                        86400 )    ;        Negative Cache TTL
```

Il s'agit du serveur qui a autorité sur la zone et qui peut y apporter des modifications.

Numéro de série de la zone. Ce numéro est incrémenté à chaque modification. Cela permet aux serveurs secondaires de savoir s'il possède une copie à jour de la zone.

Le temps, en secondes que les serveurs secondaires doivent attendre avant de vérifier si des modifications ont été apportées à la zone. (1h)

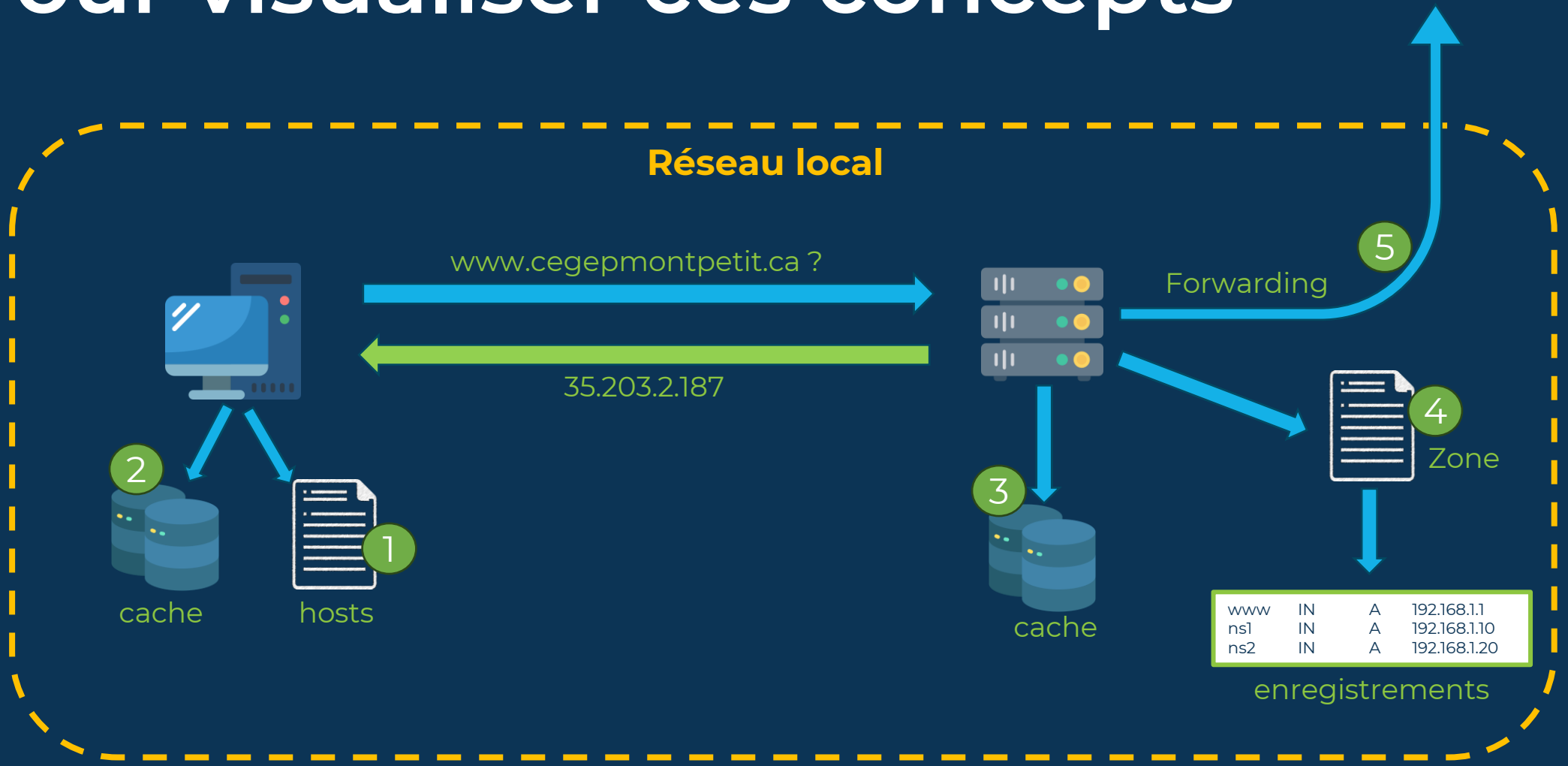
Le temps, en secondes que les serveurs secondaires doivent attendre avant de réessayer de se mettre à jour suite à un échec de la requête initial. (15min)

Le temps, en secondes après lequel une copie de la zone est considérée obsolète si aucune communication avec le serveur qui a autorité n'a pu être établie. (7 jours)

Le temps en seconde pour la mise en cache des domaines non-trouvées dans les ordinateurs clients. Cela permet d'éviter le trop grand trafic que pourrait généré des requêtes répétées pour des domaines inexistants. (1 jour)

ÉDOUARD MONTPETIT
CÉGEP D'AVENIR

Pour visualiser ces concepts



ÉDOUARD MONTPETIT
CÉGEP D'AVENIR

La commande nslookup

Cette commande permet d'interroger les serveurs de noms de domaine (DNS) afin d'obtenir des informations sur les enregistrements DNS d'un domaine spécifique.

C'est un outil essentiel pour diagnostiquer et résoudre certains problèmes en lien avec le DNS.

nslookup est disponible sur plusieurs systèmes d'exploitation.

Utilisation de nslookup

Syntaxe:

`nslookup <options> <nom de domaine/ip> <serveur>`

Exemple:

```
>nslookup -type=soa google.com
Address:  192.168.2.3

Réponse ne faisant pas autorité :
google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 607273169
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
```

Résultat d'ipconfig /all

```
Carte Ethernet Ethernet 7 :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Dell GigabitEthernet
   Adresse physique . . . . . . . . . . . : 0C-37-96-A4-0A-E4
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::ab3d:5cf:86c2:fd1d%15(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.2.136(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Bail obtenu. . . . . . . . . . . . . . : 16 février 2024 09:08:51
   Bail expirant. . . . . . . . . . . . . : 16 février 2024 12:08:50
   Passerelle par défaut. . . . . . . . . : 192.168.2.1
   Serveur DHCP . . . . . . . . . . . . . : 192.168.2.3
   IAID DHCPv6 . . . . . . . . . . . : 772552598
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2C-CD-2F-56-74-5D-22-F5-FF-56
   Serveurs DNS. . . . . . . . . . . . . : 192.168.2.3
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

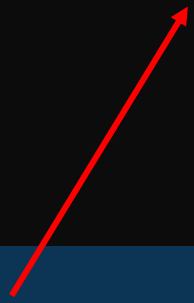
ÉDOUARD MONTPETIT
CÉGEP D'AVENIR

Utilisation de nslookup

Exemple supplémentaire:

```
C:\Users\Gabriel>nslookup -type=a www.cegepmontpetit.ca ns1-32.azure-dns.com
Serveur :   UnKnown
Address:  150.171.10.32

Nom :    www.cegepmontpetit.ca
Address:  35.203.2.187
```



Dans cet exemple, je précise le serveur que je désir interroger en fin de commande. Cela peut être pratique dans les environnements locaux possédant plus d'un serveur DNS.

Avez-vous remarqué que je n'ai pas reçu le message « réponse ne faisant pas autorité » ? Pourquoi ?

La commande Resolve-DnsName

La commande resolve-dnsname s'utilise avec PowerShell.
Son utilisation est très similaire à nslookup.

Syntaxe:

```
resolve-dnsname <nom> <-type> <-server>
```

Exemple:

```
PS C:\Users\Gabriel> resolve-dnsname www.cegepmontpetit.ca -type A

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
www.cegepmontpetit.ca                          A      19135 Answer     35.203.2.187
```

ÉDOUARD MONTPETIT
CÉGEP D'AVENIR

Utilisation de Resolve-DnsName

Autres exemple:

```
PS C:\Users\Gabriel> resolve-dnsname perdu.com -type A -server 8.8.8.8

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
perdu.com                                      A      300   Answer     104.21.5.178
perdu.com                                      A      300   Answer     172.67.133.176
```

Étrange... 🤔
Dans cet exemple, on retrouve deux enregistrements « A » pour le même nom de domaine mais contenant des valeurs (adresses IP) différentes.

Qu'est-ce qui pourrait expliquer cela ? Une idée ?

La commande dig

Finalement, la commande dig permet, elle aussi, d'interroger les serveurs DNS. Cette commande est cependant réservée pour les systèmes Linux.

Syntaxe:

```
dig <serveur> <nom> <type>
```

Exemple:

```
manager@ubuntuserver:~$ dig 8.8.8.8 www.cegepmontpetit.ca A_
```

ÉDOUARD MONTPETIT
CÉGEP D'AVENIR

Particularités des réponses de dig

La commande dig fournit des réponses très détaillée.

Ces réponses peuvent vite devenir intimidantes au début. Cependant, elles peuvent s'avérer utiles aussi.

Qui plus est, vous pouvez spécifier à dig le niveau de détails désiré.

```
; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> 8.8.8.8 www.cegepmontpetit.ca A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 3693
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;8.8.8.8.                       IN      A

;; AUTHORITY SECTION:
.                       79286   IN      SOA     a.root-servers.net. nstld.verisign-grs.com.
00 1800 900 604800 86400

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Feb 16 16:11:35 UTC 2024
;; MSG SIZE  rcvd: 111

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60997
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.cegepmontpetit.ca.         IN      A

;; ANSWER SECTION:
www.cegepmontpetit.ca.  6451    IN      A       35.203.2.187

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Feb 16 16:11:35 UTC 2024
:_
```

ÉDOUARD MONTPETIT
CÉGEP D'AVENIR

Gérer les réponses de dig

Il est possible de gérer le niveau de détails que l'on souhaite que dig nous renvoie. Par exemple, en ajoutant le terme « +short » à la fin de la commande, vous aurez une réponse très minimaliste:

```
manager@ubuntuserver:~$ dig 8.8.8.8 www.cegepmontpetit.ca A +short
35.203.2.187
```

Cela dit, on passe un peu d'un extrême à un autre de cette façon.

Gérer les réponses de dig

Vous pouvez donc faire afficher seulement la partie « réponse » en détail en ajoutant les termes « +noall » et « +answer » à la fin de votre commande. Vous aurez ainsi une quantité limitée de détails:

```
manager@ubuntuserver:~$ dig 8.8.8.8 www.cegepmontpetit.ca A +noall +answer
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 61952
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;8.8.8.8.                       IN      A

;; AUTHORITY SECTION:
.                       76912   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 20240216
00 1800 900 604800 86400

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Feb 16 16:51:09 UTC 2024
;; MSG SIZE  rcvd: 111

www.cegepmontpetit.ca.  4077    IN      A       35.203.2.187
```

ÉDOUARD MONTPETIT
CÉGEP D'AVENIR

Bonnes pratiques

1. Le nom d'hôte d'un ordinateur doit toujours correspondre au nom d'hôte dans le serveur DNS.

2. Incrémentez la valeur du champ « serial » lorsque vous apportez des modifications à une zone manuellement.

3. Maitrisez rapidement l'outil nslookup afin de pouvoir vous debugger rapidement.

Ressources complémentaires:

- La commande nslookup et resolve-dnsname:

Comment utiliser nslookup et Resolve-DnsName sous Windows ? (it-connect.fr)

- Documentation d'Ubuntu en lien avec Bind9

bind9 [Wiki ubuntu-fr]

- Fonctionnement des requêtes DNS

DNS Explained (youtube.com)

- Série de fiches d'apprentissage réalisé par Cloudflare sur le fonctionnement du service DNS

Qu'est-ce qu'un DNS ? | Fonctionnement du DNS | Cloudflare