# Outils

## Windows

### nslookup (cmd)

La commande nslookup est un invite de commande interactif permettant d'interroger des serveurs DNS. Il est disponible par défaut sous Windows mais est aussi disponible sous Linux et MacOS.

L'invocation de la commande "nslookup" ouvrira la console nslookup et affichera ">". À cet endroit vous pourrez paramétrer votre requête. Vous pouvez mentionner le serveur à interroger avec "server [adresse du serveur]", le type d'enregistrement à demander avec "set type=[type d'enregistrement]" (par défaut, le type A sera sélectionné) et le domaine à chercher en mentionnant tout simplement l'adresse recherchée.

Exemple d'une requête en nslookup pour récupérer l'enregistrement "NS" du domaine "cegepat.qc.ca" :

```
❯ nslookup
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> set type=NS
> cegepat.qc.ca
Server:  8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
cegepat.qc.ca nameserver = ns2.zonerisq.ca.
cegepat.qc.ca nameserver = ns1.zonerisq.ca.
```

### Resolve-DNSName (powershell)

Resolve-HostName est la commande en Windows la plus près de la fameuse commande "dig". Il s'agit d'un applet de commande powershell qui permet d'interroger un serveur DNS en une seule ligne de commande ce qui permet d'utiliser la réponse dans un script.

Une requête de base pour une entrée A aurait comme strucure "Resolve-DNSName -Name [nom de domaine]". Pour spécifier un autre type d'entrée DNS, il est possible d'utiliser l'option -Type dans une commande telle que "Resolve-DNSNae -Name [nom de domaine] -Type [type]". Il est aussi

possible de mentionner le serveur à questionner en ajoutant l'option "-Server [adresse du server]".

Exemple d'une requête avec Resolve-DNSName demandant l'adresse du serveur de courriel pour le domaine "cegepat.qc.ca" au serveur DNS de Google :

```
PS C:\Windows\system32> Resolve-DnsName -Name cegepat.qc.ca -Server 8.8.8.8 -Type MX


Name                                   Type   TTL   Section
NameExchange                            Preference
----                                   ----   ---   -------    ------------
                               ----------
cegepat.qc.ca                          MX     3600  Answer     cegepat-qc-
ca.mail.protection.outlook.com 0
```

# Unix (Linux/MacOS)

## dig

La commande "dig" est probablement la commande la plus populaire et la plus bavarde pour interroger un serveur DNS. Cette commande fait partie du package nommé "bind-utils" ou "dnsutils" dans la majorité des distributions de Linux. Cette commande permet d'interroger des serveurs DNS avec une panoplie d'options ainsi que des serveurs DoH (DNS-over-HTTPS). La structure de cette requête est "dig @[adresse du serveur] [type d'enregistrement] [options supplémentaires] [domaine].

Exemple d'une requête demandant l'ensemble des types d'entrées DNS pour le domaine "bad.horse" :

```
❯ dig +noall +answer +multiline bad.horse any
bad.horse.□□7200 IN□A 162.252.205.157
bad.horse.□□7200 IN□CAA 0 issue "letsencrypt.org"
bad.horse.□□7200 IN□CAA 0 issuewild ";"
bad.horse.□□7200 IN□CAA 128 issuemail ";"
bad.horse.□□7200 IN□CAA 0 iodef "mailto:abuse@sandwich.net"
bad.horse.□□7200 IN□MX 10 mx.sandwich.net.
bad.horse.□□7200 IN□NS a.sn1.zone.
bad.horse.□□7200 IN□NS b.sn1.zone.
bad.horse.□□7200 IN□SOA a.sn1.zone. n.sn1.zone. (
□□□□2023040401 ; serial
□□□□1200       ; refresh (20 minutes)
□□□□180        ; retry (3 minutes)
```

```
□□□□1209600    ; expire (2 weeks)
□□□□60         ; minimum (1 minute)
□□□□)
```

Exemple d'une requête encryptée demandant les entrées TXT du domaine "dns.google" auprès du serveur DNS de Cloudflare en DoH (DNS par HTTPS) :

```
❯ dig @one.one.one.one +https TXT dns.google

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2427
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;dns.google.□□□IN□TXT

;; ANSWER SECTION:
dns.google.□□300□IN□TXT□"v=spf1 -all"
dns.google.□□300□IN□TXT□"https://xkcd.com/1361/"

;; Query time: 63 msec
;; SERVER: 1.0.0.1#443(one.one.one.one) (HTTPS)
```

## whois

La commande est un outil permettant d'interroger le registraire d'un domaine plutôt que le serveur de nom de domaine pour trouver les informations au sujet du locateur et du locataire du domaine. Certains outils en ligne permettent aussi de récupérer ces informations mais il s'agit d'un outil à la ligne de commande Linux. Cette commande interroge les registraires de domaines plutôt que les serveurs de noms de domaine.

Exemple des informations pertinentes d'une requête whois du domaine "cegepat.qc.ca"

```
whois cegepat.qc.ca

Domain Name: cegepat.qc.ca
Registry Domain ID: D270086-CIRA
Registrar WHOIS Server: whois.ca.fury.ca
Registrar URL: www.rebel.ca
Updated Date: 2024-04-29T12:40:57Z
Creation Date: 2000-11-02T18:22:55Z
Registry Expiry Date: 2025-06-14T04:00:00Z
```

Registrar: Rebel.ca Corp.
Registrar IANA ID: not applicable
Registrar Abuse Contact Email: abuse@rebel.com
Registrar Abuse Contact Phone: +1.6132252000
Registry Registrant ID: 91219630-CIRA
Registrant Name: Cegep AT
Registrant Organization:
Registrant Street: 425 Boulevard du Collège
Registrant City: Rouyn-Noranda
Registrant State/Province: QC
Registrant Postal Code: J9X5E5
Registrant Country: CA
Registrant Phone: +1.8197620931
Registrant Email: hostmaster@cegepat.qc.ca
Registry Admin ID: 91219635-CIRA
Admin Name: Dave St-Germain
Admin Organization: Cegep AT
Admin Street: 425 Boulevard du Collège
Admin City: Rouyn-Noranda
Admin State/Province: QC
Admin Postal Code: J9X5E5
Admin Country: CA
Admin Phone: +1.8197620931
Admin Email: hostmaster@cegepat.qc.ca
Registry Tech ID: 91219635-CIRA
Tech Name: Dave St-Germain
Tech Organization: Cegep AT
Tech Street: 425 Boulevard du Collège
Tech City: Rouyn-Noranda
Tech State/Province: QC
Tech Postal Code: J9X5E5
Tech Country: CA
Tech Phone: +1.8197620931
Tech Email: hostmaster@cegepat.qc.ca
Name Server: ns1.zonerisq.ca
Name Server: ns2.zonerisq.ca
DNSSEC: unsigned

Revision #14
Created 2024-11-16 20:17:41 UTC by Alexandre Arsenault-Jetté
Updated 2024-12-08 04:42:15 UTC by Alexandre Arsenault-Jetté