dig Cheat Sheet

by TME520 (TME520) via cheatography.com/20978/cs/7279/

Syntaxe générale

dig [@serveur] [-b adresse] [-c classe] [-f fichier] [-k fichier] [-m] [-p port#] [-q nom] [-t type] [-x adresse] [-y [hmac:]nom:clef] [-4] [-6] [nom] [type] [classe] [options...]

Configuration

Lasse de taper toujours les mêmes options ? Créez un fichier Run Control pour dig.	`vi $HOME/.digrc`

```
$ cat $HOME/.digrc
+noall +answer
```

Lister certains types de Resource Records (RRs)

Les adresses (A / AAAA)	`dig -t A tme520.net`
Les alias (CNAME)	`dig -t CNAME tme520.net`
Trouver qui gère un domaine (SOA)	`dig -t SOA tme520.net`
Serveurs de courriel (MX)	`dig tme520.net MX`
Serveurs de noms (NS)	`dig tme520.net NS`
Tous les types (ANY)	`dig tme520.net ANY`

Il existe 40 types de RRs ; voici les 5 plus importants :

- **A** : Adresse IPv4 (AAAA pour IPv6),
- **CNAME** : Canonical Name. Alias vers un A ou AAAA,
- **SOA** : Start Of Authority. En charge du domaine,
- **MX** : Mail eXchange. Serveur de courriels,
- **NS** : Serveur de noms (un DNS quoi).

L'affichage décortiqué

HEADER	L'entête ; affiche la version de dig, les options utilisées, le type d'opération (opcode), le statut de ladite opération (NOERROR) et l'identifiant du message, indispensable pour faire correspondre questions et réponses.
QUESTION	La question que vous avez posée au DNS.
ANSWER	Le 2ème champs indique le temps en secondes (TTL) durant lequel le contenu peut être conservé en cache (0=pas de cache), le 3ème champs est la classe de l'entrée DNS (Internet (IN), Chaos (CH), Hesiod (HS)...), le 4ème est le type (A, NS, CNAME...) et le 5ème est l'IP.
AUTHORITY	Indique quel serveur de noms fait figure d'autorité pour un domaine.
ADDITIONAL	Contient les entrées DNS voisines du nom recherché.
STATISTICS	Affiche le temps qu'il a fallu pour obtenir une réponse, l'IP du DNS utilisé, la date et la taille du message.

Pour savoir à coup sûr si *dig* a trouvé une réponse à votre requête, vérifiez la valeur du champ ANSWER dans l'entête (HEADER). S'il est à 0, aucun résultat n'a été retourné.

Mode batch : plusieurs requêtes d'un coup

Utiliser une liste	`dig -f domaines.liste`
Passer plusieurs arguments	`dig centos.org MX +noall +answer suckless.org ANY +short`

Le mode batch prend un nom de fichier texte en entrée ; il doit contenir un domaine par ligne.

```
$ cat domaines.liste

redhat.com
ubuntu.com
perdu.com
```

Faites causer ce DNS !

N'afficher que la section ANSWER	`dig opensuse.org +noall +answer`
Passer l'affichage en mode concis	`dig perdu.com +short`
Résolution inversée (trouver le nom à partir de l'IP)	`dig -x 208.97.177.124`
Spécifier le DNS à utiliser	`dig @8.8.4.4 redhat.com`
Afficher le cheminement de la résolution	`dig google.com +trace`
Demander un transfert de zone	`dig microsoft.com AXFR`

Le transfert de zone est un mécanisme permettant à un admin de répliquer une base DNS. Deux modes existent : AXFR (complet) et IXFR (incrémental). Des pirates ayant abusé de ce système, la plupart des DNS refusent les transferts.

By **TME520** (TME520)
cheatography.com/tme520/
tme520.com

Published 24th February, 2016.
Last updated 12th May, 2016.