

Solaris 9

ADMINISTRATION DU SYSTEME UNIX
OLIVIER D.

Table des matières

1	Organisation des disques.....	3
2	Gestion des disques.....	3
3	Gestion du système de fichiers Solaris	5
4	Montage et démontage des FS	6
5	Procédures de démarrage et d'arrêt	7
6	Administration des comptes utilisateurs.....	8
7	La sécurité.....	9
8	Planification des tâches.....	9
9	Les droits.....	10
10	Installation de logiciels	10
11	Configuration TCP/IP sous Unix	11

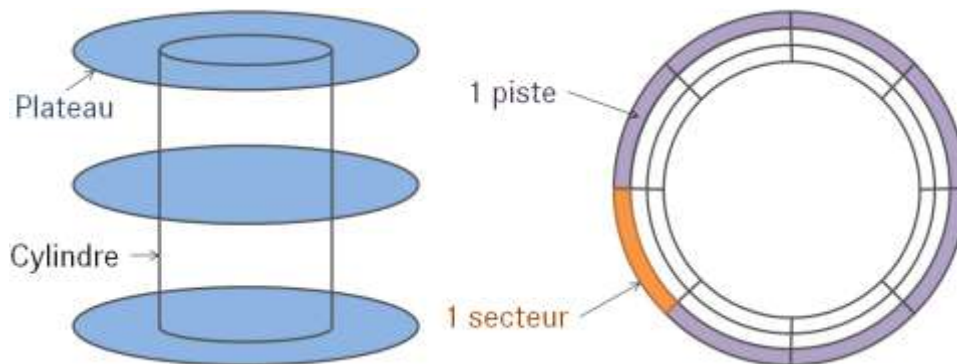
1 Organisation des disques

Arborescence Unix

/bin	lien vers /usr/bin
/dev	contient les liens vers /devices
/devices	fichiers de périphériques
/etc	fichiers de configuration
/export	contient le répertoire de base des utilisateurs
/home	réservé à l'automontage ; inaccessible en écriture
/kernel	modules + partie du noyau ne dépendant pas de la plateforme
/plateforme	modules + partie du noyau spécifiques à la plateforme (exemple : i386)
/mnt	répertoire vide servant de point de montage ponctuel
/opt	répertoire des applications supplémentaires
/sbin	exécutables nécessaires au démarrage du système
/tmp	répertoire temporaire ; en RAM
/var	fichiers de taille variable (log ; spool ; www ; mysql ...)

2 Gestion des disques

La gestion physique



La gestion physique des disques Solaris

Les tranches (slices)

Toutes les tranches d'un OS Solaris doivent être situées sur une seule partition Intel par disque dur.

Numéro de tranches :

0	/
1	swap
2	disque entier
3	-
4	-
5	-
6	-
7	/export/home
8	système (cyl. 0)
9	système (cyl. 1 et 2)

Nom des tranches

`/dev/dsk/c0t0d0s2` est égal à `/dev/dsk/c0d0s2`

<code>c0</code>	numéro de contrôleur
<code>t0</code>	target (pour les disques SCSI) ; laisser vide si ce n'est pas un disque SCSI
<code>d0</code>	ID de disque (pour les disques IDE)
<code>s2</code>	numéro de tranche (slice)

Lister les périphériques du système

```
less /etc/path_to_inst
prtconf
format
```

Reconfiguration des périphériques

Après l'ajout d'un disque dur, de RAM, d'une carte son, etc. il faut reconfigurer les périphériques.

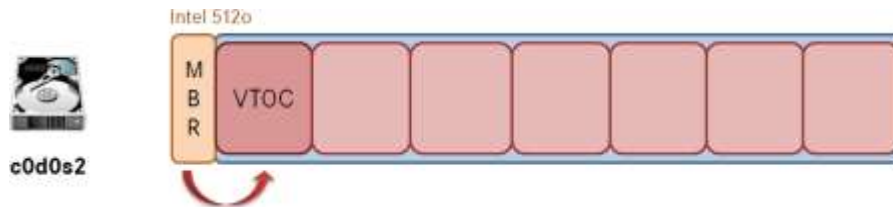
```
touch /reconfigure
reboot
```

ou

```
devfsadm
```

-v pour connaître les modifications apportées

Découpage d'un disque dur



Découpage des disques durs Solaris

```
# fdisk
fdisk> partition                créer les partition, ne pas modifier la tranche 2
fdisk> verify
fdisk> label                    appliquer les modifications
```

dans `format`, la commande `verify` affiche les infos du disque :

part	tag	flag	cylinders	size	blocks
0	root	wm	3-12984	5.85gb	-
1	swap	wu	-	-	-
2	backup	wm	-	-	-
3	-	-	-	-	-
4	-	-	-	-	-
5	-	-	-	-	-
6	-	-	-	-	-
7	-	-	-	-	-
8	-	-	-	-	-
9	-	-	-	-	-

verify affiche les informations de la VTOC telles qu'elles seront si on fait `Label`

```
prvtoc /dev/dsk/c0d0s2          affiche aussi les infos du disque en ligne de commande
prvtoc /dev/dsk/c0d0s2 > /disk0 sauvegarde de la VTOC (idéal sur un autre hdd)
fmthard -s /disk /dev/rdisk/c0d0s2 restauration de la VTOC
```

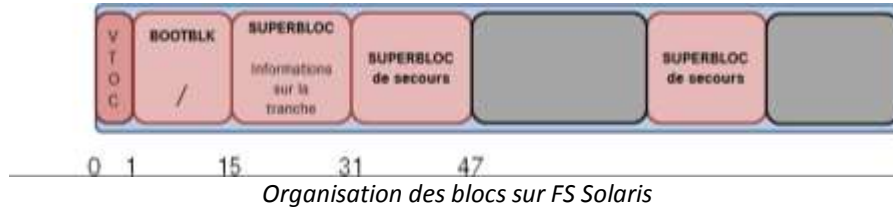
3 Gestion du système de fichiers Solaris

FS sur disque (ufs, ...)

FS distribués (exemple : cifs)

Pseudos FS (exemple : swap, /tmp)

- UFS : Solaris9
- XFS : Solaris10
- ZFS : Solaris11
- HSFS : CD/DVD (read only)



VTOC toujours réservé mais seulement présent sur le 1er secteur

BOOTBLK toujours réservé mais seule la tranche / a un BOOTBLK

SUPERBLOC chaque FS a un SUPERBLOC

SUPERBLOC de secours chaque FS a des superbloc de secours

Structure de l'inode UFS

Une inode contient : type, permissions, UID, GID, dates, taille, nombre de liens physiques

+ des pointeurs :

12 pointeurs directs	12 x 8ko	
1 pointeur de simple indirection	2048 pointeurs directs	16mo
1 pointeur de double indirection	2048 point. de simple indirection	32go
1 pointeur de triple indirection	2048 point. de double indirection	64To

Créer un FS : newfs

`newfs /dev/rdisk/c0d1s0` créer un FS ufs sur la tranche 0 du disque 1 (\approx mkfs)
`-m 1` réserver 1% de l'espace disque pour la maintenance

`fstyp /dev/dsk/c0d0s0` afficher les infos du FS

`tunefs -m 1 /dev/dsk/c0d0s0` modifier les paramètres d'un disque

`fsck -y (auto yes) /dev...` vérification (à ne pas faire sur un système monté !)

Réparer un superbloc

`fsck -o b=32 /dev/rdisk/c0d1s0` copie le bloc de secours qui commence à b=32 à la place du superbloc

`newfs -N /dev/rdisk/...` récupère les adresse des blocs de secours (à faire **AVANT** plantage)

Surveiller un système de fichiers

`df -h` afficher l'espace disponible
`-e` renvoie le nombre d'inodes disponibles

`du -hs /etc` renvoie l'espace de /etc et de son arborescence

`du -hs /*` renvoie la taille de chacun des fichiers et répertoires de /

`mount` informations sur les options de montage

4 Montage et démontage des FS



Prise en compte des périphériques

`defsadm`



Création de la table de découpage

`format / fdisk`



Création du système de fichiers

`newfs (mkfs)`



Utilisation des systèmes de fichiers

`mount (/etc/vfstab)`

Etapes de l'ajout d'un disque dur sous Solaris

`/etc/vfstab` fichiers montés au démarrage

Faire un `vi` pour en modifier le contenu

Montages :

Il existe deux types d'options de montage :

- Options liées à la commande `mount`
- Options liées au FS monté

```
mount /dev/fd0 /disquette
```

périphérique à monter pt de montage

```
mount -F ufs -o option1,option2 <périphérique à monter> <point de montage>
```

`mountall` permet de monter le contenu de `/etc/vfstab` (pour tester avant reboot)

`umountall -r` démonter tous les FS distants

Démontage

`umount /data` démonter cette occurrence du disque

`umount /dav/dsk/c0d1s0` démonte toutes les occurrences de ce disque

Démontage d'un FS occupé

`fuser` liste des processus qui utilisent un fichier (répertoire)

`umount -f` force de démontage d'un FS

```
fuser -cu /data
```

liste des utilisateurs de /data

```
fuser -ck /data
```

tue les processus sur /data

```
umount /data
```

démonte /data

Procédure à suivre pour démonter un FS occupé

Réparer les fichiers stratégiques si le démarrage ne s'effectue pas correctement

1. insérer le CD-ROM d'installation
2. démarrer sur le CD-ROM
3. arrivé au 2ème écran gris : `b -s`
4. au besoin, `fsck /dev/rdisk/c0d0s0`
5. monter le FS / du disque dur : `mount /dev/dsk/c0d0s0 /a`
6. pour utiliser `vi`, il faut modifier les variables :
 - a. `TERM=sun`
 - b. `export TERM`

Montage des périphériques amovibles

`volmgt` service d'automontage des périphériques amovibles

daemon `vold` permet aux utilisateurs de bénéficier des cd-rom sans avoir les droits root

- Nota : `vold` ne monte pas automatiquement les disquettes : il faut utiliser `volcheck`
- Nota : Pour éjecter un cd-rom, il faut le démonter puis l'éjecter : `eject cdrom`

`/etc/init.d/volmgt stop` désactive le service d'automontage

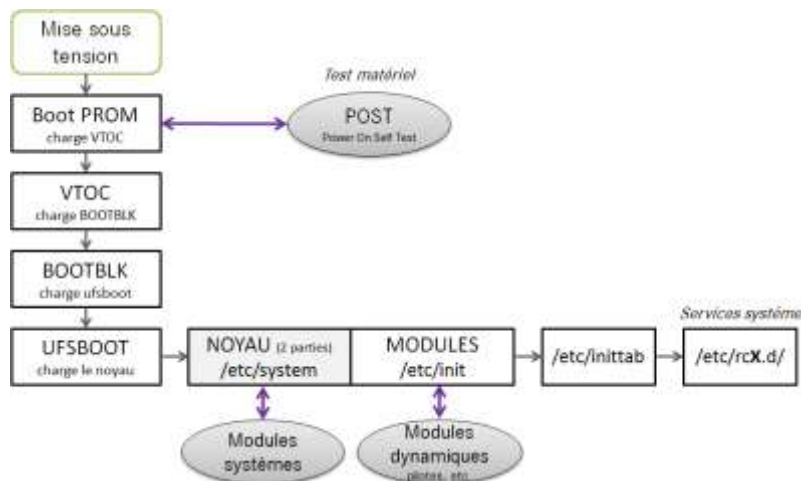
5 Procédures de démarrage et d'arrêt

who -r niveau d'exécution actuel

Niveau d'exécution	détail
0	Aller dans le BIOS de Sparks
3 S	Mode maintenance (mono-utilisateur)
1	Mono-user, les FS locaux sont montés
2	Multi-user sans NFS
3	Multi-user console
4	/
5	Arrêt avec mise hors tension
6	Redémarrage

Les niveaux d'exécution de Solaris

Phases de démarrage :



Les phases du démarrage d'un OS Solaris

/etc/system : emplacement des modules système

moddir chemin des modules
 root dev ... type de fs de la racine
 exclude exclure certains modules (chemin relatif par rapport à moddir)
 forceload force le chargement de modules (chemins relatif par rapport à moddir)
 set options du noyau

en cas de problème :

- soit CD-ROM
- soit `boot -a` (sans le cd) : indique qu'on veut charger /dev/null à la place de /etc/system

La phase initialisation :

Une fois les modules du noyau chargés, le processus init est lancé

/dev/inittab

```

is:3:initdefault:                                définit le démarrage par défaut
id:rstate:action:process                        que pour le choix de démarrage par défaut
  initdefault                                  lance ce processus en premier
  sysinit
  wait
  respawn                                       impossible à tuer
  powerfail
rstate                                          niveaux de fonctionnement concernés
  
```

/bin/rc2 : /etc/rc2.d/K...script stop
/etc/rc2.d/S...script start

Nota : on retrouve aussi les scripts dans /etc/init.d (/etc/init.d/nfs.server stop|start)

Arrêter un système :

shutdown [options] arrêt programmé

6 Administration des comptes utilisateurs

`/etc/passwd` définition des utilisateurs
`/etc/shadow` définition des mots de passe
`/etc/group` définition des groupes

Fichier `/etc/passwd` :

```
login:X:UID:GID:commentaires:répertoire_home:shell_de_l'utilisateur
odehecq:X:100:10:eleve:/export/home/odehecq:/bin/bash
```

Fichier `/etc/group` :

```
nom_du_groupe:mot_de_passe:GID:liste_en_secondaire
root::0:root
```

Options par défauts des mots de passe : `/etc/default/passwd`

Création d'un compte utilisateur :

```
useradd [-u UID] [-g GID] [-G GID[,GID...]] [-d dir] -m loginname
```

- m copie le contenu de `/etc/skel` dans `dir` et prévient si ça foire !
- D affiche les valeurs par défaut (sur Solaris : `useradd -D -b /export/home`)
- s spécifier le shell (chemin absolu)
- c commentaires

Modifier un compte utilisateur :

```
usermod [-u UID] [-g GID] [-G GID[,GID...]] [-d dir] loginname
```

Nota : pour ajouter un groupe, il faut mettre TOUS les groupes auxquels l'utilisateur appartient

Supprimer un compte utilisateur :

```
userdel [-r] loginname
```

- r supprime en même temps le répertoire `$HOME`

Créer / modifier un groupe :

```
groupadd [-g GID] groupname
groupmod [-g GID] [-n name] groupname
```

Verrouillage de compte :

`passwd -l user2` verrouille le compte `user2` et supprime le mot de passé

`passwd -d -f user 2` déverrouille le compte `user2` et force le changement de mot de passe

Problèmes de connexion sous CDE (Common Desktop Environment) :

`~/dt` ne pas hésiter à le supprimer en cas de problème de connexion

Gestion des fichiers d'initialisation :

	Paramètres par défauts tout le monde	Paramètres de l'utilisateur et propre au shell utilisé
SH (bourne Shell)	<code>/etc/profile</code>	<code>~/profile</code>
BASH (bourne Again Shell)	<code>/etc/profile</code>	<code>~/bashrc</code>
KSH (korn Shell)	<code>/etc/profile</code>	<code>~/profile</code> <code>~/kshrc</code>
CSH (C Shell)	<code>/etc/login</code>	<code>~/login</code> <code>~/cshrc</code>

OBJECTIFS

- Définir les alias
- Définir les variables
- Définir le umask
- Exécuter des scripts

Personnalisation de l'environnement :

`/etc/skel/` contient :

```
.profile
local.cshrc : ~/cshrc
local.login : ~/login
local.profile : ~/profile
```

Documents par défaut (documents « publics ») créés par smuser (interface graphique)

La sécurité

Règle n°1 : **NE JAMAIS SE CONNECTER EN ROOT ! FAIRE UN su – A LA PLACE !**

Règle n°2 : Tous les matins, regarder les fichiers de log afin de détecter des problèmes éventuels

who	lister les utilisateurs connectés
finger [utilisateur@adresse_ip]	informations sur les utilisateurs
last	lister les redémarrages + connexions réelles
logname	UID
id	EUID (utilisateur du shell en cours)

Journaliser les accès à la commande su :

`/etc/default/su` journalisation des su dans `/var/adm/sulog`

Accès au système :

`/etc/default/login` paramétrer les accès

`CONSOLE=/dev/console` root ne peut se connecter qu'en console locale

`CONSOLE=` root ne peut pas se connecter ! (faire des su -)

Accès ftp

`/etc/ftpd/ftplib` les utilisateurs définis dedans **NE PEUVENT PAS** se connecter en FTP

Supprimer les fichiers « remote hosts » :

Le fichier `~/rhosts` permet de se connecter sans mot de passe ; avec une connexion non chiffrée

Script : `find /home [ou /export/home] -name .rhosts -exec rm -f {} \;`

```
vi /etc/inetd.conf configuration du service « autoservices »
mettre # devant les lignes contenant :
rusersd répondre au scan des utilisateurs et postes du réseau (rusers)
in.fingerd donner les informations de ses utilisateurs (finger)
in.telnetd permet les connexions en telnet (non chiffré)
puis pkill -1 inetd relance le service inetd
```

pkill et pgrep

`pkill <- signal> <nom du processus>` \neq `kill <signal> <PID>`

`pgrep [-l infos_longues] <chaine>` recherche une chaine parmi les processus

Planification des tâches

La commande at (Taches ponctuelles. Pas de répétition des tâches)

```
at 21:30 at -l indique les tâches planifiées par EUID (≈ atq) ou TLM si UID=root
at> /script/srveillance.sh
at> ^D
```

`/etc/cron.d/at.deny :`

`toto` toto ne peut plus faire de `at` (fonctionne aussi pour root)

`/etc/cron.d/at.allow :`

`titi` plus personne ne peut faire de `at` (sauf root et titi) prend le pas sur `at.deny`

La crontab (Attention : ne jamais faire crontab sans argument)

`crontab -e` éditer
`crontab -l` lister le contenu

```
10 3 * * 0 /usr/lib/fs/nfsfind pas de */n
minute heure jour mois j/sem commande (chemin absolu !)
```

`crontab -r user4` supprimer une crontab utilisateur (root)

`/var/spool/cron/crontab` emplacement des fichiers de crontab

`/etc/cron.d/cron.deny` les utilisateurs présents ne peuvent pas éditer la crontab

Les droits

Les droits spéciaux n'ont de sens que si le droit x est positionné aussi (SetUID, SetGID, StickyBit).

Sticky Bit (1)

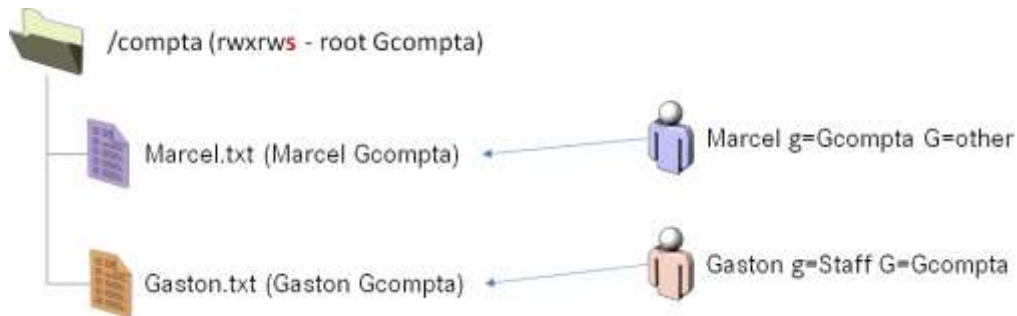
- REPERTOIRE : les fichiers ne pourront être supprimés que par leur propriétaire
`chmod +t /rep` : ajouter le Sticky Bit
- FICHIER : le fichier sera conservé en mémoire vive après sa première exécution

Set GID (2)

- REPERTOIRE : les fichiers créés dans le répertoire auront le même GID que le répertoire parent

Set UID (4)

- FICHIERS : le fichier sera exécuté avec les droits du propriétaire du fichier
`chmod -R a+rx rep1` : tous les dossiers ont +x ; des droits des fichiers ne changent pas



Fonctionnement du sticky bit

Installation de logiciels

Par les sources

```
# wget http://www.siteweb.com/folder/archive.tar.gz           sous Unix, tar ne gère pas gzip
# gunzip -c archive.tar.gz > archive.tar                    -c conserver et stdout = écran
# tar xvf archive.tar
# cd archive
# less INSTALL
# less README
# ./configure                                               crée un fichier Makefile (si sources GNI, besoin de GCC)
# make
# make install | tee archive-install.log                     pour un log détaillé
```

Gestionnaire de paquets (pkgadd)

<http://sunfreeware.com> puis sélectionner x86 – Solaris9 (indique les dépendances)

Installer :

```
wget http://www.siteweb.com/folder/package.gz
gunzip -c package.gz > package
pkgadd -d paquet                                           -d : indiquer que le chemin est le répertoire de la commande
```

Désinstaller :

```
pkgrm paquet-logiciel
```

Infos :

```
pkginfo -l <nom du paquet>  nombreuses infos
pkgchk <paquet>             listes des modifications du paquet
-v                           liste des fichiers créés
-l -p <fichier>             provenance d'un fichier
```

11 Configuration TCP/IP sous Unix

11.1 Afficher les informations

`ifconfig -0` lo0 (loopback) et pcn0 (ou dnet/qfe/hme)

Modification temporaire et dynamique :

`ifconfig pcn0 <adresse IP> <masque>`

activer/désactiver une interface réseau :

`ifconfig pcn0 down|up` <UP ... > (! Pas évident à trouver)

Informations diverses :

`netstat -i` statistiques

`-r` table de routage

`-n` désactive la résolution de noms

`snoop [poste1 poste2] -v -V [-o output-file-bin] [-i input-file-bin]` sniffeur de trames

11.2 Fichiers de configuration TCP/IP

```
/etc/init.d/network start|stop|restart
```

Attribuer définitivement une adresse IP :

1. `/etc/hostname.pcn0` pcn0 (nom de la carte à modifier)

```
poste1
```

2. `/etc/hosts`

```
10.27.15.10 poste1 loghost    envoie les logs vers la machine contenant le service loghost
10.27.15.10 poste1.stagiaires.local sur une ligne à part pour lisibilité (pas nécessaire)
127.0.0.1 localhost
10.27.255.254 gw-27                passerelle
```

3. `/etc/netmask`

```
10.27.0.0 255.255.0.0        sinon choisit le masque correspondant à la classe RSO
```

4. `/etc/defaultrouter` (passerelle par défaut)

```
gw-27
```

5. `/etc/gateways` (table de routage)

```
net 192.168.0.0 gateway 10.27.255.253
```

6. `/etc/networks` (nommer les réseaux _ pas indispensable du tout !)

```
salle207 10.27.0.0
salle206 10.26.0.0
```

Attribuer temporairement une table de routage (dynamique) :

`route add net 176.16.0.0 10.27.2.5`

`route delete net default 10.27.0.254` supprimer la route 10.27.0.254

`route add net default 10.27.255.254` changer la route par défaut

IP aliasing : ajouter une adresse IP à une carte (pour du load balancy par exemple)

Dynamique : `ifconfig pcn0 addif 172.16.0.1 up | iconfig pcn0 removeif 172.16.0.1`

Statique : `/etc/hostname.pcn0`

```
poste1
addif 172.16.0.1
```

Changer définitivement le “hostname” :

Changer toutes les occurrences du hostname par le nouveau nom de machine dans les fichiers :

```
/etc/nodename  
/etc/hostname.pcn0  
/etc/hosts  
/etc/net/ticlts/hosts  
/etc/net/ticotsord/hosts  
/etc/net/ticots/hosts
```

Puis relancer les services de réseaux (/etc/init.d/inetinit et (/etc/init.d/network)

Sys-unconfig :

Equivalent de sysprep : réinitialise les identifiants uniques + config. clavier/souris/vidéo

```
# sys-unconfig
```

Client DHCP :

Dynamique :

- `ifconfig pcn0 auto-dhcp start|stop|release|drop`

Statique :

- `touch /etc/dhcp-pcn0`
- Pour résoudre (en partie) le bug du “hostname”
- `vi /etc/init.d/network`

```
« dhcp » ) hostname=`/sbin/dhcpinfo Hostname` ;;  
« dhcp » ) hostname=`/bin/cat/etc/nodename` ;;
```

La résolution de noms DNS :

```
/etc/nsswitch.conf
```

```
hosts:files dns [nis ldap nisplus] (ordre de résolution = de gauche à droite)
```

files = résolution locale, qui utilise /etc/hosts et /etc/netmasks

```
/etc/resolve.conf
```

```
nameserver 10.0.0.1  
nameserver 10.0.0.2  
search stagiaires.local eni-ecole.fr (sert dans le cas d'un ping cd001)
```

La commande dig : résolution inverse de nom

Marche à suivre en cas de doute sur l'authenticité d'un site internet bancaire :

```
dig www.mabanque.com adresse IP du serveur www.mabanque.com  
dig nic.fr ns serveur DNS 'officiel' internet  
dig @ns.nic.fr www.mabanque.com utiliser un serveur dns spécifique pour dig
```