

## Examen de 2<sup>ème</sup> session du module 3I015

Durée : 2 heures

*Seuls documents autorisés :*

*Une feuille A4 recto-verso*

---

### Exercice 1 (20 points) — *Étude de cas Linux*

---

Le contexte de l’étude de cas est celui d’un laboratoire de recherche en informatique. Celui-ci est localisé sur deux sites différents : un site *A* principal disposant d’une centaine de machines, nommées M1 à M100, et un site *B* secondaire, plus petit, disposant de cinquante machines nommées M101 à M150. Toutes ces machines sont accessibles par l’ensemble des chercheurs du laboratoire. Les sites *A* et *B* possèdent chacun leur propre réseau et doivent donc communiquer via des passerelles. Le site *A* possède une salle dédiée contenant les serveurs suivants, utiles au fonctionnement du parc informatique :

- la machine nommée *S1* sert de serveur LDAP. Elle permet l’authentification de tous les chercheurs du laboratoire, qu’ils travaillent sur le site *A* ou sur le site *B*.
- la machine nommée *S2* sert de serveur NFS pour les comptes des chercheurs travaillant uniquement sur le site *A*. Elle exporte ainsi un répertoire `/siteA/users` contenant les *home directories* des chercheurs du site *A* vers toutes les machines M1 à M150 ainsi que vers les serveurs qui en ont besoin.
- la machine nommée *S3* sert de backup. Les comptes des chercheurs travaillant sur le site *A* (c’est-à-dire les sous-répertoires de `/siteA/users` exportés par le serveur *S2*) sont sauvegardés dans un répertoire `/backups/siteA`. Les comptes des chercheurs travaillant sur le site *B* (les sous-répertoires de `/siteB/users` exportés par un serveur nommé *S4*) sont sauvegardés dans un répertoire `/backups/siteB`. Les restaurations de tous les fichiers et répertoires sauvegardés, qu’ils concernent le site *A* ou le site *B*, seront réalisées uniquement sur le serveur *S1*.
- la machine nommée *gateA* sert de passerelle afin de communiquer avec le site *B*.

Le site *B*, quant à lui, possède un petit local contenant les serveurs suivants :

- la machine nommée *S4* sert de serveur NFS pour les comptes des chercheurs travaillant uniquement sur le site *B*. Elle exporte ainsi un répertoire `/siteB/users` contenant les *home directories* des chercheurs du site *B* vers toutes les machines M1 à M150 ainsi que vers les serveurs qui en ont besoin.
- la machine nommée *S5* sert de serveur NFS et exporte uniquement vers les machines M101 à M150 un répertoire `/Vrac` dans lequel tout utilisateur peut écrire des fichiers et ces derniers ne peuvent être supprimés que par leur propriétaire.
- la machine nommée *gateB* sert de passerelle afin de communiquer avec le site *A*.

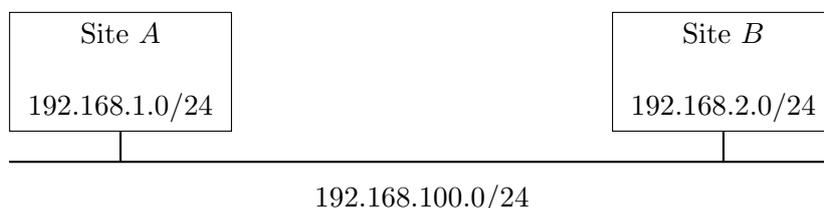
Toutes les machines, *S1* à *S5*, M1 à M150, *gateA* et *gateB* sont équipées d’un système d’exploitation Linux Debian 8.1. Excepté les passerelles, elles sont toutes dotées d’une carte réseau d’interface `eth0`. Les passerelles sont dotées de deux cartes réseaux d’interfaces respectives `eth0` et `eth1`.

Toutes les machines sont dotées d’un disque dur `/dev/sda` de 100 gigaoctets partitionné en une partition primaire `/dev/sda1` de 30Go contenant le système d’exploitation et une autre partition primaire `/dev/sda2` de 10Go contenant un espace de swap. De plus, tous les serveurs NFS sont également dotés d’un deuxième disque dur `/dev/sdb` non partitionné de 16 teraoctets dédié aux fichiers des comptes utilisateurs. Enfin le serveur de sauvegarde *S3* est doté, en plus de `/dev/sda`, de deux disques durs non partitionnés de 16 teraoctets `/dev/sdb` et `/dev/sdc` : le premier sert pour les sauvegardes des fichiers des chercheurs du site *A* tandis que le deuxième sert pour les sauvegardes des fichiers des chercheurs du site *B*.

**Quelques conseils pour la suite :**

- Choisir de façon raisonnable toute information utile qui ne serait pas indiquée dans l'énoncé.
- Répondre à CE sujet et non selon les travaux associés aux séances passées de TME.
- Être très précis quant aux réelles informations manipulées, y compris pour les contenus de fichiers demandés.
- Quand des lignes de fichiers sont strictement égales, numéroter la première occurrence de telles lignes, dans la marge, et utiliser par la suite ce numéro.
- Quand des lignes de fichiers sont similaires (même structure, mais quelques champs de valeurs différentes à cause d'un numéro de poste différent, par exemple, ou autre variation régulière, ...), écrire complètement la première ligne de la série, puis des points de suspension, puis complètement la dernière ligne de la série.

**Q 1.1** Le réseau du site *A* est le 192.168.1.0/24. Celui du site *B* est le 192.168.2.0/24. La liaison entre ces deux sites est un réseau d'adresse 192.168.100.0/24, comme le montre la figure ci-dessous :



Les adresses IP des machines du site *A* sont les suivantes :

- 192.168.1.201 pour *S1*,
- 192.168.1.202 pour *S2*,
- 192.168.1.203 pour *S3*,
- 192.168.1.*x* pour les machines *Mx*, avec  $x = 1, \dots, 100$ ,
- *gateA* a deux adresses : 192.168.1.254 et 192.168.100.1.

Les adresses IP des machines du site *B* sont les suivantes :

- 192.168.2.204 pour *S4*,
- 192.168.2.205 pour *S5*,
- 192.168.2.*x* pour les machines *Mx*, avec  $x = 101, \dots, 150$ ,
- *gateB* a deux adresses : 192.168.2.254 et 192.168.100.2.

Indiquez les fichiers système que vous devez configurer pour que toutes les machines puissent communiquer entre elles et avec internet en utilisant le service **networking**. Vous préciserez le contenu de ces fichiers **uniquement** pour la machine *M1*. Quelle commande doit-on exécuter pour que le service **networking** soit démarré automatiquement à chaque redémarrage des machines ?

Il faut éditer le fichier `/etc/default/networking` et préciser que :

```
CONFIGURE_INTERFACES=yes
```

Ensuite, il faut éditer le fichier `/etc/network/interfaces`. Pour *M1*, cela revient à ajouter les lignes :

```
auto eth0
iface eth0 inet static
    name eth0
    address 192.168.1.1
    network 192.168.1.0
    netmask 255.255.255.0
    gateway 192.168.1.254
    broadcast 192.168.1.255
```

Pour que le service `networking` soit démarré automatiquement à chaque redémarrage des machines, il faut que `root` exécute :

```
systemctl enable networking
```

**Q 1.2** Indiquez le contenu des fichiers de la question précédente pour la machine `gateB`. On supposera que les instructions permettant le routage (statique) entre les deux sites *A* et *B* ont déjà été écrites, vous n'avez donc pas à en tenir compte dans votre réponse.

Il faut éditer le fichier `/etc/default/networking` et préciser que :

```
CONFIGURE_INTERFACES=yes
```

Ensuite, il faut éditer le fichier `/etc/network/interfaces` :

```
auto eth0
iface eth0 inet static
    name eth0
    address 192.168.2.254
    network 192.168.2.0
    netmask 255.255.255.0
    broadcast 192.168.2.255
auto eth1
iface eth1 inet static
    name eth1
    address 192.168.100.2
    network 192.168.100.0
    netmask 255.255.255.0
    gateway 192.168.100.254
    broadcast 192.168.100.255
```

Ici, il faut bien comprendre que, lorsqu'une machine *M<sub>x</sub>* du site *B* veut communiquer avec une machine *S<sub>y</sub>* du site *A*, d'après la question précédente, *M<sub>x</sub>* va transmettre son paquet à `gateB`. La passerelle `gateB` doit alors transmettre ce paquet à `gateA` afin qu'il soit acheminé vers la machine *S<sub>y</sub>* du site *A*. La configuration ci-dessus permet à `gateB` et `gateA` de communiquer. En revanche, rien n'indique que, pour joindre *S<sub>y</sub>*, `gateB` doit transmettre le paquet d'abord à `gateA`. Pour obliger cela, il suffit de rajouter une instruction de routage statique dans le fichier `/etc/network/interfaces`. Cela se fait via l'ajout d'une ligne similaire à :

```
up route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.100.1
```

Mais cela n'est pas au programme du module 3I015.

**Q 1.3** On suppose que les fichiers ci-dessus ont été correctement configurés pour les deux interfaces réseau du serveur `gateB`. Quel fichier supplémentaire faut-il éditer pour que `gateB` devienne une passerelle du site *B*? Indiquez ce qu'il faut mettre à jour dans ce fichier.

Il faut éditer le fichier `/etc/sysctl.conf` en décommentant la ligne :

```
net.ipv4.ip_forward = 1
```

**Q 1.4** On souhaite maintenant que toutes les machines, postes clients et serveurs, passerelles, puissent « pinguer » les autres machines des deux sites en ne spécifiant plus leurs adresses IP mais leurs noms (M1,...,M150, S1,...,S5, gateA, gateB). Indiquez quels fichiers vous éditeriez pour cela et précisez leur contenu.

Il faut éditer le fichier `/etc/hosts`. Son contenu est :

```
192.168.1.201 S1
192.168.1.202 S2
192.168.1.203 S3
192.168.2.204 S4
192.168.2.205 S5

192.168.1.1 M1
.....
192.168.1.100 M100
192.168.2.101 M101
.....
192.168.2.150 M150

192.168.1.254 gateA
192.168.2.254 gateB
```

**Q 1.5** Dans un tableau, indiquez pour chaque machine (Mx, x = 1, ..., 150, S1, ..., S5, gateA, gateB) ayant besoin de partitions supplémentaires, celles que vous devez créer. Vous préciserez leur nom (par exemple `/dev/sda1`), leur taille, leur type (primaire, logique, etc.), et leur point de montage.

machine	partition	taille	type	point de montage
S2	<code>/dev/sdb1</code>	16To	primaire	<code>/siteA/users</code>
S3	<code>/dev/sdb1</code>	16To	primaire	<code>/backups/siteA</code>
	<code>/dev/sdc1</code>	16To	primaire	<code>/backups/siteB</code>
S4	<code>/dev/sdb1</code>	16To	primaire	<code>/siteB/users</code>
S5	<code>/dev/sdb1</code>	16To	primaire	<code>/Vrac</code>

**Q 1.6** Indiquez l'ensemble des commandes (formatage, etc.) à effectuer dans l'état actuel de S2 afin d'installer le répertoire `/siteA/users`, c'est-à-dire afin que l'administrateur puisse se déplacer dedans et y ajouter des fichiers, y compris après un redémarrage de la machine.

1. Il faut passer root avec la commande `su -`.
2. Il faut utiliser `fdisk /dev/sdb` afin de créer la partition primaire `/dev/sdb1` de 16To.
3. Soit on exécute `partprobe`, soit on reboote la machine afin que le système reconnaisse la partition `/dev/sdb1`.
4. On formate la partition : `mkfs -t ext4 /dev/sdb1`.
5. On crée le point de montage `mkdir /siteA/users`.
6. On rajoute dans `/etc/fstab` la ligne :  
`/dev/sdb1 /siteA/users ext4 defaults 0 2`

7. On effectue le montage : `mount /siteA/users`.

**Q 1.7** Indiquez les contenus des fichiers `/etc/exports` des serveurs S1 à S5.

S1 n'est pas un serveur NFS, son `/etc/exports` reste donc vide.

Le fichier de S2 :

```
/siteA/users 192.168.1.203(ro,no_root_squash)
/siteA/users 192.168.1.0/24(rw,root_squash)
/siteA/users 192.168.2.0/24(rw,root_squash)
```

Le fichier de S3 :

```
/backups/siteA 192.168.1.201(ro,no_root_squash)
/backups/siteB 192.168.1.201(ro,no_root_squash)
```

Le fichier de S4 :

```
/siteB/users 192.168.1.203(ro,no_root_squash)
/siteB/users 192.168.1.0/24(rw,root_squash)
/siteB/users 192.168.2.0/24(rw,root_squash)
```

Le fichier de S5 :

```
/Vrac 192.168.2.0/24(rw,root_squash)
```

**Q 1.8** Indiquez les lignes à ajouter au fichier `/etc/fstab` de la machine M101 du site B afin de pouvoir monter les répertoires qui lui sont exportés. Indiquez également les répertoires que vous envisagez de créer afin de pouvoir réaliser les montages.

```
S2:/siteA/users /siteA/users nfs defaults,bg,soft 0 0
S4:/siteB/users /siteB/users nfs defaults,bg,soft 0 0
S5:/Vrac /Vrac nfs defaults,bg,soft 0 0
```

On doit créer les répertoires de montage, c'est-à-dire `/siteA/users`, `/siteB/users`, `/Vrac`.

**Q 1.9** Faites de même pour la machine M1 du site A.

```
S2:/siteA/users /siteA/users nfs defaults,bg,soft 0 0
S4:/siteB/users /siteB/users nfs defaults,bg,soft 0 0
```

On doit créer les répertoires de montage, c'est-à-dire `/siteA/users`, `/siteB/users`.

**Q 1.10** On souhaite que, dans le répertoire `/Vrac` de S5, tout utilisateur puisse écrire des fichiers et que ces derniers ne puissent être supprimés que par leur propriétaire. Que faut-il faire dans l'état actuel de S5 pour parvenir à cela.

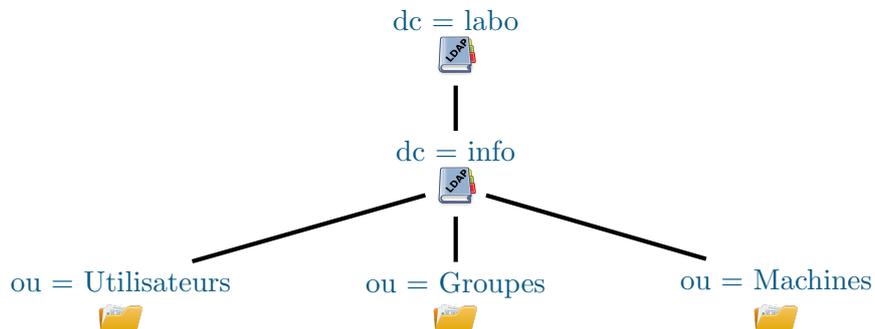
Si le répertoire `/Vrac` n'a pas été créé, on le crée. Ensuite, il faut donner les droits d'accès en lecture/écriture à tous les utilisateurs et mettre à « on » le sticky bit :

```
mkdir /Vrac
mount /Vrac
chmod 1777 /Vrac    ou    chmod a+rw,+t /Vrac
```

**Q 1.11** On souhaite mettre en place sur S1 un serveur LDAP. La base de l'arborescence doit être « `dc=info,dc=labo` » et le mot de passe de l'administrateur LDAP doit être « `LINFO` ». Le package `slapd` est déjà installé sur la machine S1. Quelle commande doit-on utiliser pour reconfigurer ce package et quelles réponses doit-on fournir aux questions du programme de configuration.

On doit exécuter `dpkg-reconfigure slapd`.  
 À la question « nom de domaine », répondre : `info.labo`  
 À la question « Nom d'entité », toute réponse est OK  
 À la question « Mot de passe de l'administrateur », répondre `LINFO`  
 Pour toutes les autres questions, choisir la réponse par défaut.

**Q 1.12** On souhaite avoir l'arborescence suivante sur le serveur LDAP :



Indiquez précisément ce qu'il faut faire pour obtenir cette arborescence.

Il faut créer le fichier `arbo.ldif` suivant :

```
dn: ou=Utilisateurs,dc=info,dc=labo
objectClass: organizationalUnit
ou: Utilisateurs
```

```
dn: ou=Groupes,dc=info,dc=labo
objectClass: organizationalUnit
ou: Groupes
```

```
dn: ou=Machines,dc=info,dc=labo
objectClass: organizationalUnit
ou: Machines
```

puis exécuter la commande `ldapadd -x -D cn=admin,dc=info,dc=labo -W -f arbo.ldif`.

**Q 1.13** Sur la machine M101 du site *B*, quelles actions doit-on précisément effectuer afin que les utilisateurs puissent être identifiés via le serveur LDAP de la machine S1.

On doit installer les packages `libnss-ldap` et `pam-ldap`. Il faut les configurer : il faut indiquer que le serveur LDAP est « `ldap://S1` » et que le mot de passe de l'administrateur est « `LINFO` ». Enfin, il faut éditer le fichier `/etc/nsswitch.conf` et y indiquer :

```
passwd: files ldap
group: files ldap
shadow: files ldap
gshadow: files ldap
```