Examen de 2ème 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'une entreprise localisée sur quatre sites différents : un site S dédié à des serveurs, un site A disposant de 10 postes clients destinés aux secrétaires de l'entreprise, un site B disposant de 20 postes clients destinés aux ingénieurs, et enfin un site C disposant de 10 postes clients destinés aux commerciaux de l'entreprise.

- Les serveurs du site S ont une adresse IP du réseau 132.227.100.0/24. Ce site contient notamment un serveur nommé `S1`, d'adresse IP 132.227.100.1, permettant de sauvegarder et de restaurer les comptes des utilisateurs des sites A, B et C (les restaurations se font uniquement sur `S1`). Il contient également un serveur NFS `S2` d'adresse IP 132.227.100.2 pour les comptes des secrétaires et des ingénieurs. Il y a aussi un serveur NFS `S3` d'adresse IP 132.227.100.3 pour les comptes des commerciaux. Le site S contient aussi un serveur LDAP `S4` d'adresse IP 132.227.100.4 permettant l'authentification de tous les utilisateurs des trois sites A, B et C. Il est aussi équipé d'un serveur `S5` d'adresse IP 132.227.100.5 permettant d'exporter via NFS vers le site A un répertoire `/communA`, vers le site B un répertoire `/communB` et vers le site C un répertoire `/communC`. Ces répertoires peuvent être utilisés en lecture/écriture par tout utilisateur d'un même site mais l'ingénieur système de l'entreprise garantit que seul le propriétaire d'un fichier peut le supprimer et il garantit également que les utilisateurs peuvent remplir chacun des répertoires `/communA`, `/communB` et `/communC` à hauteur de 6 teraoctets. Enfin, une passerelle nommée `gate` permet d'accéder aux trois sites A, B, C.
- Le site A est pourvu de 10 postes clients nommés `A1` à `A10` d'adresses IP **fixes** 132.227.200.1 à 132.227.200.10. Toute secrétaire et seulement une secrétaire peut se connecter via LDAP/NFS sur n'importe quel poste.
- Le site B est pourvu de 20 postes clients nommés `B1` à `B20` d'adresses IP **fixes** 132.227.300.1 à 132.227.300.20. Tout ingénieur et seulement un ingénieur peut se connecter via LDAP/NFS sur n'importe quel poste.
- Le site C est pourvu de 10 postes clients nommés `C1` à `C30` d'adresses dynamiques du réseau 132.227.400.0/24 obtenues par DHCP. Tout commercial et seulement un commercial peut se connecter via LDAP/NFS sur n'importe quel poste.

Afin de créer son parc informatique, l'entreprise a acheté un lot de 60 PC munis de processeurs Intel Core I7 et de disques durs vierges de 1 teraoctet ainsi qu'un lot de 8 disques durs de 20 teraoctets chacun et un lot de 100 cartes réseau.

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 Indiquez quels matériels (PC, disques durs, cartes réseau) vous devez affecter à chacun des serveurs et des postes clients des sites afin que le parc puisse fonctionner correctement (c-à-d que les utilisateurs peuvent se connecter aux postes clients, accéder à leurs comptes, ces derniers sont sauvegardés, *etc*). Si vous avez besoin de serveurs supplémentaires, indiquez-le.

Chaque poste client des sites A, B et C correspond à un PC standard muni de son disque dur interne de 1 teraoctet et d'une carte réseau. Notez qu'il n'y a pas besoin de passerelle spécifique à chaque site puisque la machine `gate` du site S sert déjà à cet effet.
Sur le site S, le serveur `S1` est un PC standard muni d'une carte réseau. Afin que les utilisateurs de chaque site puissent avoir un maximum d'espace de sauvegarde, on affecte pour les sauvegardes des home directories de chaque site un disque dur de 20 teraoctets. Donc `S1` contient on disque dur de 1 teraoctet + 3 disques de 20 teraoctets. Le serveur `S2` est un PC standard muni d'une carte réseau, de son disque de 1 teraoctet + 2 disques de 20 teraoctets, ces derniers servant aux comptes utilisateurs des sites A et B. Le serveur `S3` est un PC standard muni d'une carte réseau, de son disque de 1 teraoctet et d'un disque de 20 teraoctets servant aux comptes utilisateurs du site C. Pour le serveur LDAP `S4`, il suffit d'un PC standard muni d'une carte réseau et d'un disque dur de 1 teraoctet. Le serveur `S5` est un PC standard muni d'une carte réseau, de son disque de 1 teraoctet et d'un disque de 20 teraoctets pour l'ensemble des répertoires `/communA`, `/communB` et `/communC` (étant donné qu'en tout, l'entreprise possède 8 disques de 20 teraoctets, elle ne peut pas utiliser un disque par espace commun de site, car il lui faudrait alors 9 disques dur de 20 teraoctets et elle n'en possède que 8). Il faut ajouter un serveur DHCP `S6`. Cette machine est un PC standard muni de son disque dur interne de 1 teraoctet et d'une carte réseau. Enfin, il faut une passerelle nommée `gate` afin de communiquer avec les sites A, B et C. Cette machine est un PC standard muni de son disque dur interne de 1 teraoctet et de quatre cartes réseau (1 sur le réseau de chaque site).

Q 1.2 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 `S1` et pour la machine `A1`. Enfin, 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 `S1`, en supposant que la passerelle du site S a pour adresse IP 132.227.100.254 sur le réseau du site S, cela revient à ajouter les lignes :

```
auto eth0
iface eth0 inet static
  name eth0
  address 132.227.100.1
  network 132.227.100.0
  netmask 255.255.255.0
  gateway 132.227.100.254
  broadcast 132.227.100.255
```

Pour `A1`, en supposant que la passerelle `gate` a pour adresse IP 132.227.200.254 sur le réseau du site A, cela revient à ajouter les lignes :

```
auto eth0
iface eth0 inet static
  name eth0
  address 132.227.200.1
  network 132.227.200.0
  netmask 255.255.255.0
  gateway 132.227.200.254
  broadcast 132.227.200.255
```

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

```
systemctl enable networking
```

Q 1.3 Indiquez le contenu des fichiers de la question précédente pour la machine `C1`.

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 dhcp
```

Q 1.4 On souhaite maintenant que tous les postes clients du site A puissent « pinger » l'ensemble des machines du site S en ne spécifiant plus leurs adresses IP mais leurs noms (`S1`, *etc.*). Indiquez quels fichiers vous éditeriez pour cela et précisez leur contenu.

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

```
132.227.100.1   S1
132.227.100.2   S2
132.227.100.3   S3
132.227.100.4   S4
132.227.100.5   S5
132.227.100.6   S6

132.227.100.254 gate
```

Q 1.5 Dans un tableau, indiquez pour chaque disque dur de chacune des machines de chacun des sites quelles partitions vous devez créer (on rappelle que tous les disques sont actuellement vierges). Pour chaque partition, 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
S1	/dev/sda1	100Go	primaire	/
	/dev/sdb1	20To	primaire	/sauvegardeA
	/dev/sdc1	20To	primaire	/sauvegardeB
	/dev/sdd1	20To	primaire	/sauvegardeC
S2	/dev/sda1	100Go	primaire	/
	/dev/sdb1	20To	primaire	/homeA
	/dev/sdc1	20To	primaire	/homeB
S3	/dev/sda1	100Go	primaire	/
	/dev/sdb1	20To	primaire	/homeC
S4	/dev/sda1	20To	primaire	/
S5	/dev/sda1	100Go	primaire	/
	/dev/sdb1	6To	primaire	/communA
	/dev/sdb2	6To	primaire	/communB
	/dev/sdb3	6To	primaire	/communC
S6	/dev/sda1	100Go	primaire	/
Ax, Bx, Cx,	/dev/sda1	100Go	primaire	/
passerelles	/dev/sda1	100Go	primaire	/

Q 1.6 Indiquez les contenus des fichiers `/etc/exports` des serveurs `S1` à `S5`.

`S1` n'est pas un serveur NFS puisque les sauvegardes et restaurations sont effectuées entièrement sur `S1`.
Le fichier de `S2` :

```
/homeA    132.227.200.0/24(rw,root_squash)
/homeA    132.227.100.1(rw,no_root_squash)
/homeB    132.227.300.0/24(rw,root_squash)
/homeB    132.227.100.1(rw,no_root_squash)
```

Le fichier de `S2` :

```
/homeC    132.227.400.0/24(rw,root_squash)
/homeC    132.227.100.1(rw,no_root_squash)
```

`S4` n'est pas un serveur NFS.
Le fichier de `S5` :

```
/communA    132.227.200.0/24(rw,root_squash)
/communB    132.227.300.0/24(rw,root_squash)
/communC    132.227.400.0/24(rw,root_squash)
```

Q 1.7 On a installé les systèmes d'exploitation Linux Debian sur les machines `S2` et `A1`. Indiquez les lignes à ajouter au fichier `/etc/fstab` de ces machines pour que toutes les fonctionnalités du parc informatique soient effectives.

Sur la machine `S2`, on doit rajouter :

```
/dev/sdb1   /homeA   ext4   defaults  0   2
/dev/sdc1   /homeB   ext4   defaults  0   2
```

Sur la machine `A1`, on doit rajouter :

```
S2:/homeA     /homeA     nfs   defaults,bg,soft   0   0
S5:/communA   /communA   nfs   defaults,bg,soft   0   0
```

Q 1.8 Actuellement, seule la partition du système d'exploitation de `S5` a été créée. On souhaite que, dans le répertoire `/communA` de `S5`, tout utilisateur puisse écrire des fichiers et que ces derniers ne puissent être supprimés que par leur propriétaire. Que faut-il faire sur `S5` pour parvenir à cela. Vous détaillerez bien les opérations à effectuer.

1. Il faut passer root avec la commande `su -`.
2. Il faut utiliser `fdisk /dev/sdb1` afin de créer la partition primaire de 20To.
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 /communA`.
6. On rajoute dans `/etc/fstab` la ligne :
   `/dev/sdb1   /communA   ext4   defaults   0   2`
7. On effectue le montage : `mount /communA`.
8. On donne les droits d'accès en lecture/écriture à tous les utilisateurs et on met à « on » le sticky bit : `chmod 1777 /communA` ou `chmod a+rwx,+t /communA`.

Q 1.9 Indiquez le contenu du fichier `/etc/dhcp/dhcpd.conf` du serveur DHCP fournissant les adresses IP au site C.

```
authoritative; # serveur DHCP officiel du réseau

subnet 132.227.400.0 netmask 255.255.255.0 {
  option routers 132.227.400.254;            # la passerelle du site C
  option broadcast-address 132.227.400.255;  # le broadcast
  default-lease-time 3000;
  max-lease-time 7200;
}
```

Q 1.10 On souhaite mettre en place des IP tables afin de sécuriser le parc informatique de l'entreprise. On part d'une configuration où il n'y a qu'une politique par défaut mise en place, qui est égale à `DROP` sur l'ensemble des chaînes. Quelles lignes faudrait-il écrire dans les IP tables du serveur `S2` afin que les fichiers des utilisateurs du site A puissent être exportés sur les machines de ce site. Indiquez de même les lignes à rajouter au client `A1`.

Sur le serveur `S2`, on doit ajouter :

```
-A OUTPUT -o eth0 -p tcp --sport 2049 -s 132.227.200.0/24 -j ACCEPT
-A INPUT  -i eth0 -p tcp --dport 2049 -d 132.227.200.0/24 -j ACCEPT
```

Sur le client `A1`, on doit ajouter :

```
-A OUTPUT -o eth0 -p tcp --dport 2049 -d 132.227.100.2 -j ACCEPT
-A INPUT  -i eth0 -p tcp --sport 2049 -s 132.227.100.2 -j ACCEPT
```

Q 1.11 Actuellement, on a uniquement installé le système d'exploitation sur la machine passerelle du site S, sans configurer son réseau. Quelles sont les opérations à effectuer et les fichiers à modifier afin que cette machine remplisse bien son rôle de passerelle. Vous préciserez le contenu de ces fichiers.

Il faut commencer par configurer les 4 cartes réseau de la machine. Pour cela, il faut éditer le fichier `/etc/default/networking` et préciser que :

```
CONFIGURE_INTERFACES=yes
```

Ensuite, il faut éditer le fichier `/etc/network/interfaces` et ajouter les lignes :

```
auto eth0
iface eth0 inet static
  name eth0
  address 132.227.100.254
  network 132.227.100.0
  netmask 255.255.255.0
  broadcast 132.227.100.255

auto eth1
iface eth1 inet static
  name eth1
  address 132.227.200.254
  network 132.227.200.0
  netmask 255.255.255.0
  broadcast 132.227.200.255

auto eth2
iface eth2 inet static
  name eth2
  address 132.227.300.254
  network 132.227.300.0
  netmask 255.255.255.0
  broadcast 132.227.300.255

auto eth3
iface eth3 inet static
  name eth3
  address 132.227.400.254
  network 132.227.400.0
```

```
  netmask 255.255.255.0
  broadcast 132.227.400.255
```

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

```
systemctl enable networking
```

Enfin, il faut éditer le fichier `/etc/sysctl.conf` en décommentant la ligne :

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