UV TMRI-1 - Systèmes en réseaux

Introduction au système Linux

—

Correction de l'examen final

Rémi LEBLOND

6 août 2004

1 Déploiement de stations Linux

Une entreprise souhaite déployer Linux sur 30 postes de travail reliés à un réseau local Ethernet à 100Mb/s. Elle désire permettre à chaque utilisateur de se connecter indifféremment sur tout poste en retrouvant son environnement de travail. Pour des raisons de sécurité, elle souhaite que les données manipulées par les utilisateurs et leurs applications ne soient pas stockées sur les postes clients, mais se retrouvent centralisées sur un serveur. Tous les postes de travail doivent pouvoir être inter-changés. Ainsi, en cas de défaillance de l'un d'entre eux, un utilisateur doit pouvoir continuer son travail tout autre poste du réseau en retrouvant intactes ses données.

1.1 Mise en place de l'infrastructure générale

1. Décrivez rapidement une infrastructure permettant de répondre à ces besoins. Justifier vos choix.

Solution :

Pour mettre en oeuvre l'infrastructure décrite, nous devrons disposer de 30 PC de type bureautique (Pentium II avec 128 Mo de RAM et 4Go de disque dur minimum) et d'un serveur principal (Pentium II avec 512 Mo de RAM et 20Go de disque SCSI). Pour améliorer la disponibilité de ce serveur, il est fortement recommandé de disposer d'un onduleur, d'un sous-système disque RAID (0 ou 5), d'une alimentation redondante et de deux cartes réseau.

Éventuellement un serveur secondaire pourra relayer le serveur principal sur les fonctions critiques (serveur de nom, serveur NIS) et prendre en charge des fonctions secondaires. La configuration de ce serveur peut être équivalente à celle d'un poste de travail.

Tous ces postes de travail sont reliés à un réseau Ethernet à 100Mb/s.

2. Comment centraliser le contrôle d'accès au système informatique (nom des utilisateurs et mots de passe) ? Proposez une solution en la décrivant précisément.

Solution :

Nous proposons de mettre en oeuvre un serveur NIS pour répondre à ce besoin.

Le serveur NIS s'installe de la façon suivante :

- *Installation du paquet contenant le programme serveur (cas d'une distribution Debian) :*
  `apt-get install nis`
- *Il est nécessaire, avant de commencer le paramétrage du serveur NIS, de déclarer le nom du domaine qui sera servi par le serveur. Ce paramétrage se fait à l'aide de la commande* `nisdomainname`*. Généralement, cette phase n'est pas nécessaire, car elle est déjà réalisée par le programme* `apt-get`*.*
  ```
  # nisdomainname cnam-strasbourg-nis
  ```
- *Il faut ensuite lancer le serveur NIS, à l'aide de la commande* `ypserv`*, et l'initialiser en temps que serveur NIS principal, à l'aide de la commande* `ypinit` *avec l'option 'm' (comme "master")*[1]*.*
  ```
  # ypserv
  # /usr/lib/yp/ypinit -m
  ```
  Le programme `ypinit` *va vous demander la liste des serveurs NIS à maintenir. Pour le moment, nous ne disposerons que d'un seul serveur NIS. Utilisez "CTRL" + "D" pour sortir de la liste.*
- *Une fois que le serveur NIS est actif, il faut constituer sa base de données. Cette dernière est stockée dans des fichiers situés dans le répertoire* `/var/yp`*. La construction de la base NIS se fait à partir des fichiers de configuration du serveur, sur la base du fichier de construction* `/var/yp/Makefile`*.*
  Pour publier uniquement les fichiers `/etc/passwd` *et* `/etc/group`*, on modifiera le fichier Makefile, afin d'obtenir la ligne suivante :*
  ```
  ALL = passwd group
  ```
- *Ensuite, il faut se rendre dans le répertoire* `/var/yp` *et lancer la commande* `make`*.*

[1] Pour lancer un serveur secondaire, on utilisera l'option 's', comme "slave".

```
# cd /var/yp
# make
```

On remarque que cette manipulation a créé un sous-répertoire de `/var/yp` *portant le nom du domaine ("cnam-strasbourg-nis", par exemple). Ce dernier contient les différentes informations publiées par NIS, qui sont extraites des fichiers de configuration du serveur sur lequel s'exécute NIS, conformément au fichier de configuration* `/var/yp/Makefile`.

La commande `make` *devra être lancée, depuis le répertoire* `/var/yp`*, dès qu'une modification des fichiers de configuration du serveur NIS devra être publiée.*

- *A partir de maintenant, le serveur NIS est configuré et fonctionne.*
- *Pour que le serveur NIS soit lancé à chaque démarrage du serveur, il faut modifier le fichier* `/etc/default/nis`*, pour changer la valeur suivante :*

  `NISSERVER=master`
- *Sur les clients, il est nécessaire d'installer les paquetages NIS, de la même façon que pour le serveur, en précisant le même nom de domaine NIS.*

3. Comment permettre à l'utilisateur de retrouver son répertoire de travail sur tout poste du réseau sur lequel il se connecte ? Précisez la configuration à mettre en oeuvre.

Solution :

Pour répondre à ce besoin, il est nécessaire de partager le répertoire `/home` *du serveur en utilisant le service NFS.*

On installera le serveur NFS à l'aide de la commande suivante : On utilisera le programme `apt-get` *de Debian pour installer les packages NFS sur le serveur (debian1). Pour ce faire, on exécute la commande suivante :*

```
# apt-get install nfs-user-server nfs-common
```

Pour déclarer les répertoires à exporter, on ajoute l'entrée suivante dans le fichier `/etc/exports` *afin d'exporter le répertoire* `/home` *en lecture et écriture pour les machines du réseau :*

```
/home   *(rw,root_squash)
```

Ensuite, on lance le serveur et les utilitaires NFS, à l'aide des commandes suivantes :

```
# /etc/init.d/nfs-user-server start
# /etc/init.d/nfs-common start
```

Par la suite, en cas de modification du fichier `/etc/exports`*, il suffira de lui dire de relire son fichier de configuration à l'aide de la commande suivante :*

```
# /etc/init.d/nfs-kernel-server reload
Re-exporting directories for NFS kernel daemon...done.
```

Sur les postes client, on installera les utilitaires NFS à l'aide de la commande suivante :

```
# apt-get install nfs-common
```

Pour monter un export NFS, on procède de la même façon que pour les autres systèmes de fichiers, à l'aide de la commande `mount`.

```
# mount -t nfs serveur:/home /home
```

A partir de ce moment, on retrouve le répertoire `/home` *du serveur sur les postes clients. Les utilisateurs peuvent donc désormais se connecter sur n'importe poste client et y retrouver leur répertoire personnel. Le tour est joué !!!*

Pour retrouver ce montage NFS après un redémarrage d'un poste client, on ajoute la ligne suivante dans le fichier `/etc/fstab` *:*

```
serveur:/home /home nfs soft,timeo=5,intr,
                        rsize=8192,wsize=8192 0 0
```

4. Comment centraliser la configuration du réseau et le plan de nommage des machines ?

Solution :

Il est possible de centraliser la configuration du réseau en mettant en oeuvre un serveur DHCP. La centralisation du plan de nommage nécessite les services d'un serveur de noms. Nous installerons respectivement "dhcp3" et "bind" pour répondre à ces besoins.

L'installation du serveur DHCP est réalisé à l'aide de la commande suivante :

```
# apt-get install dhcp3-server
```

A l'installation, il vous demande d'entrer la liste des interfaces réseaux sur lesquelles le serveur DHCP doit écouter (séparées par des espaces). Cette information est ensuite stockée dans le fichier /etc/default/dhcp3-server.

Dans notre cas, nous désirons uniquement que le serveur DHCP écoute l'interface "eth1", qui correspond à celle qui est reliée au réseau local.

Comme vous l'indiquent les messages d'avertissement affichés par `apt-get`*, le serveur DHCP n'est pas fonctionnel avec la configuration par défaut, pour des raisons de sécurité (c'est une habitude chez Debian). On modifiera donc le fichier* `/etc/dhcp3/dhcpd.conf`.

```
option domain-name "cnam-strasbourg.org";
option domain-name-servers 192.168.1.1;
# Durée du bail en secondes
default-lease-time 6000;
max-lease-time 6000;
authoritative;

# Déclaration du sous-réseau 192.168.0.0/255.255.255.0
subnet 192.168.1.0 netmask 255.255.255.0 {
  # Adresse du routeur
  option routers 192.168.1.1;
  # Plage d'adresses pour les machines non déclarées
  range 192.168.1.100 192.168.1.200;
}

# Déclaration des machines à adresse fixe
host station_travail1 {
  # Adresse MAC de la machine
  hardware ethernet 00:0C:29:33:24:00;
  # Adresse IP à attribuer
  fixed-address 192.168.1.10
```

Une fois que le fichier de configuration est au point, il est nécessaire de relancer le serveur DHCP à l'aide de la commande suivante :

`# /etc/init.d/dhcp3-server restart`

Lorsque le service DHCP est démarré sur le serveur, il est nécessaire de reconfigurer les interfaces réseau des station de travail, de façon à ce qu'elles récupèrent leur configuration depuis le serveur DHCP.

Ainsi, il faudra modifier les fichiers `/etc/network/interfaces` *afin d'y trouver :*

```
auto eth0
  iface eth0 inet dhcp
```

Après avoir modifié ce fichier, il est nécessaire de relancer le support du réseau pour récupérer la configuration des interfaces réseau depuis le serveur DHCP.

```
# /etc/init.d/networking restart
```

Le serveur de noms s'installe à l'aide de la commande suivante :

```
# apt-get install bind9
```

Les fichiers de configuration de Bind se trouvent dans le répertoire `/etc/bind/`.
Pour configurer une zone primaire correspondant à notre serveur local, nom ajouterons la ligne suivante au fichier `named.conf` *:*

```
zone "cnam-strasbourg.org" {
        type master;
        file "cnam-strasbourg.org.zone";
};
```

Où `cnam-strasbourg.org.zone` *désigne le fichier, situé dans le répertoire* `/var/cache/bind/`*, où seront stockés les enregistrements de la zone.*
L'écriture de ce fichier est, de loin, la phase la plus complexe de la configuration d'un serveur de noms.
En dehors des lignes d'en-tête, nous devrons retrouver les informations suivantes dans le fichier de zone :

```
; ENREGISTREMENTS "NS"
cnam-strasbourg.org.    IN      NS      debian1

; ENREGISTREMENTS "A"
debian1         IN      A       192.168.1.1
debian2         IN      A       192.168.1.2
debian3         IN      A       192.168.1.3

; ENREGISTREMENTS "CNAME" : Alias DNS
nfs             IN      CNAME   debian1
mailhost        IN      CNAME   debian1
nis             IN      CNAME   debian1

; ENREGISTREMENTS "MX" : Serveur de messagerie
cnam-strasbourg.org.    IN      MX      10      debian1
```

Pour forcer Bind à relire son fichier de configuration, nous utiliserons la commande suivante :

```
# /etc/init.d/bind9 reload
```

Une fois que le serveur de noms est opérationnel, il est nécessaire de diffuser son adresse aux stations de travail. Cette diffusion peut se faire facilement à l'aide du serveur DHCP. Il nous suffit de modifier le fichier de configuration du serveur DHCP (ligne "option domain-name-servers" du fichier `/etc/dhcpd3/dhcpd.conf`*, puis de relancer le serveur DHCP pour diffuser cette information.*

5. L'administrateur système souhaite pouvoir intervenir à distance sur tous les postes et serveurs depuis sa machine. Comment peut-il faire ? Expliquer précisément la configuration a mettre en oeuvre.

Solution :

Pour que l'administrateur puisse se connecter sur les stations de travail depuis sa machine, il est possible d'utiliser le service "ssh".

Chaque station devra exécuter le serveur ssh (`sshd`) et la machine de l'administrateur disposera uniquement des outils "ssh" client.

L'installation de "ssh" se fait à l'aide de la commande suivante :

```
# apt-get install ssh
```

Le paquet "ssh" va se charger d'installer à la fois les outils client et serveur (`sshd`) d'OpenSSH. Le programme `apt-get` se charge de configurer ces derniers. Vous pouvez normalement accepter les valeurs proposées par défaut. Il vous est ensuite demandé si vous désirez exécuter le service serveur de ssh (sshd). Répondez "oui" sur les stations de travail et "Non" sur la machine de l'administrateur.

En installant ce paquet sur chaque machine du réseau, vous devriez être en mesure de vous connecter d'une machine à l'autre. Ainsi, pour ouvrir une nouvelle session sur "debian1" à partir de "debian2", il suffit d'utiliser la commande suivante :

```
# ssh debian1
```

1.2 Mise en place de droits d'accès particuliers

La principale application utilisée dans cette entreprise est le logiciel de comptabilité. Ce dernier est nommé "compta", ses fichiers exécutables sont situés dans /usr/compta, ses fichiers de paramétrage dans /opt/compta et elle stocke ses données dans /var/compta/data.

Certains utilisateurs (groupe "compta_modif") doivent pouvoir mettre à jour les données de la comptabilité, d'autres (groupe "compta_consult") ne peuvent que les consulter et, enfin, les utilisateurs restants ne doivent pouvoir accéder à aucune de ces informations.

6. Comment peut-on répondre à ces besoins ? Décrivez précisément l'infrastructure et la politique de gestion des droits permettant de répondre à ces contraintes (partage de l'information et droits d'accès aux données).

Solution :

– *Créer les groupes "compta_consult" et "compta_modif" à l'aide des commandes suivantes :*

```
groupadd compta_consult
groupadd compta_modif
```

- *Créer le répertoire de données à l'aide de la commande suivante :*
  `mkdir -p /var/compta/data`
- *Affecter le répertoire* `/var/compta` *au groupe "compta_consult", à l'aide de la commande suivante :*
  `chgrp compta_consult /var/compta`
- *Affecter le répertoire* `/var/compta/data` *au groupe "compta_modif", à l'aide de la commande suivante :*
  `chgrp compta_modif /var/compta/data`
- *Modifier la matrice de droits du répertoire* `/var/compta` *afin de ne permettre l'accès qu'aux membres du groupe, à l'aide de la commande suivante :*
  `chmod 750 /var/compta`
- *Modifier la matrice de droits du répertoire* `/var/compta` *afin de permettre la consultation par les utilisateurs étrangers, à l'aide de la commande suivante :*
  `chmod 775 /var/compta/data`
- *Ajouter les membre du groupe "compta_modif" dans le groupe "compta_consult", en modifiant le fichier* `/etc/group`*.*

7. Certains utilisateurs du système utilisent exclusivement le programme de comptabilité. Ils ne doivent pas pouvoir faire autre chose du système informatique. Proposez une solution permettant de limiter l'accès de ces utilisateurs au seul programme de comptabilité.

Solution :

Pour que l'utilisateur ne puisse utiliser que le programme de comptabilité il faut indiquer, dans le fichier `/etc/passwd`*, le chemin du logiciel en question (à la place de celui de l'interpréteur de commandes).*

Cela est effectué en remplaçant, dans le fichier `/etc/passwd`*, une ligne de la forme :*

```
util1:x:500:500:Utilisateur 1:/home/util1:/bin/bash
```

par :

```
util1:x:500:500:Utilisateur 1:/home/util1:/usr/compta/compta
```

8. Certains postes sont accessibles en libre service. Pour des questions de confidentialité et de sécurité, on désire éviter que quiconque puissent entrer ou sortir des informations numériques (fichiers) du système informatique depuis ces postes. La politique de sécurité à mettre en place doit donc interdire l'utilisation du lecteur de disquettes de ces postes.

Proposez une solution permettant de mettre en oeuvre cette politique.

Solution :

Pour ne pas permettre l'utilisation du lecteur de disquette par les utilisateurs des stations de travail, il est possible de supprimer l'entrée correspondante dans le fichier `/etc/fstab`*. Ainsi, seul l'administrateur du système pourra monter le lecteur de disquette, en utilisant la commande "mount" complète.*

2 Cohabitation avec Windows

L'entreprise dispose de vingt postes fonctionnant avec Windows NT qu'il souhaite raccorder au réseau que vous avez mis en place. Chaque utilisateur, qu'il se connecte indifféremment à une station Windows ou Linux, doit systématiquement retrouver :

– le contenu de son répertoire de connexion,
– le contenu du répertoire utilisé par le logiciel de compta, en lecture seule.

9. Proposez une solution permettant aux utilisateurs de se connecter sur ces postes Windows avec les mêmes comptes que ceux utilisés pour les machines Linux.

Solution :

Nous allons mettre en oeuvre un serveur Samba pour répondre à ce besoin.

On utilise la commande suivante pour installer les paquetages nécessaires à Samba :

```
apt-get install samba
```

Le paramétrage de Samba est centralisé sur un seul fichier : /etc/samba/smb.conf. Modifiez le fichier existant pour obtenir :

```
[global]
   netbios name = serveur
   server string = Serveur de fichier %h (Samba %v)
[homes]
   comment = Répertoire personnel de %u
   writable = Yes
   browseable = No
[compta]
  comment = Répertoire comptabilité
  path = /var/compta/data
  writable = No
  browseable = Yes
  create mode = 0777
```

3 Ouverture d'un accès Internet

L'entreprise souhaite faire bénéficier certaines machines de son réseau d'un accès Internet ciblé : accès aux sites institutionnels, aux pages jaunes et aux sites d'information en dehors des heures de travail.

10. Proposez une solution, basée sur Linux, permettant de satisfaire ce besoin.

Solution :

Nous partagerons l'accès Internet à l'aide d'un serveur mandataire[2]*, qui nous permettra une optimisation des télé-chargements et un contrôle des sites accessibles. Nous utiliserons pour cela le programme* `squid`*, qui est un standard dans le monde Unix.*

Pour des questions de sécurité, il est préférable de ne pas installer la passerelle internet sur un serveur critique. Nous installerons donc ce service sur un serveur secondaire, situé en amont du réseau local, dans une zone démilitarisé (DMZ) et équipé de deux cartes réseau : une reliée à Internet et une autre, au réseau local.

L'installation du serveur squid est réalisé à l'aide de la commande suivante :

```
apt-get install squid
```

La configuration du serveur mandataire `squid` *se fait à l'aide du fichier* `/etc/squid.conf`*, qui doit au moins contenir les lignes suivantes :*

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl all src 0.0.0.0/0.0.0.0
acl machines_ok src 192.168.1.0/255.255.255.0

# Autorisation de l'accès HTTP aux seules machines
                                        du réseau
http_access allow machines_ok
http_access deny all

# Utilisation du serveur mandataire de l'IUT
cache_peer 130.79.80.33 parent 8080 3130 no-query
                                      proxy-only
```

Pour que cette configuration soit prise en compte, il faut relancer le serveur mandataire à l'aide de la commande suivante :

```
# /etc/init.d/squid restart
```

[2] Souvent appelé "serveur proxy".

A présent, le serveur mandataire est actif sur le serveur et rend la navigation possible depuis les stations de travail, à condition de paramétrer le proxy sur ces dernières.