TP AdminSR – NFS, DNS, LDAP

Auteur : Olivier GLÜCK, Université Lyon 1

1. Packages à installer

Pour NFS :

- **nfs-common** NFS files common to client and server
- **nfs-kernel-server** support for NFS kernel server

Pour les NIS :

- **nis** Clients and daemons for the NIS

Pour le DNS :

- **bind9** Internet Domain Name Server
- **bind9utils** Utilities for BIND
- **bind9-host** Version of 'host' bundled with BIND 9.X
- **libdns58** DNS Shared Library used by BIND
- **liblwres50** Lightweight Resolver Library used by BIND

Pour LDAP :

- **slapd** OpenLDAP server (slapd)
- **lat** ou **jxplorer** ou **luma** ou **gq** un client LDAP graphique
- **ldap-utils** OpenLDAP utilities
- **libnss-ldap** NSS module for using LDAP as a naming service
- **libpam-ldap** Pluggable Authentication Module for LDAP
- **libldap-2.4-2** OpenLDAP libraries

Pour installer un package : `apt-get install nom_pkg`
Pour vérifier que le package est correctement installé, faire un `dpkg -l`
Avant d'installer un package, vous pouvez le supprimer complètement (s'il était déjà installé) par `dpkg --purge nom_pkg`. Pour reconfigurer un package, faire `dpkg-reconfigure nom_pkg`.

2. Organisation pratique

Les binômes se répartissent de manière égale dans les salles TPR1 et TPR2. Vous mettrez en place deux sous-réseaux indépendants : **`192.168.1.0/24`** dans la salle TPR104, **`192.168.2.0/24`** dans la salle TPR106. On imaginera que chacune des salles représente une organisation indépendante de l'Internet avec sa (ou ses) propre(s) zone(s) DNS, son (ou ses) serveur(s) NFS, et son (ou ses) serveur(s) LDAP. **Vous adopterez les conventions suivantes concernant la numérotation des machines : les serveurs DNS utiliseront les adresses IP entre `.10` et `.19`, les serveurs NFS entre `.20` et `.29`, les serveurs LDAP entre `.30` et `.39` ; les machines clientes utiliseront les adresses supérieures. Par exemple, dans la salle TPR1, le serveur DNS primaire utilisera l'adresse `192.168.1.10`, le serveur NFS l'adresse `192.168.1.20`… Dans chaque sous-réseau l'adresse `.1` est réservée à la passerelle qui permettra aux deux sous-réseaux de communiquer : les binômes en charge du DNS devront relier les réseaux des deux ou trois salles par un routeur afin de faire des tests à plus grande échelle.**

Vous utiliserez deux machines distinctes : une pour installer et faire tourner le serveur ; l'autre pour tester le service à partir d'un client.

3. Le service NFS

NOM 1 :	***NOM 2 :***	***Salle : TPR1 TPR2***
Adresse IP du serveur :	***Adresse IP du client :***	

Question

Service rendu par NFS :

3.1. Mise en place du service

Manipulation

Installez les packages nécessaires à la mise en place d'un serveur NFS. Exécutez les commandes suivantes : `cp -a /etc /tmp/etc ; cp -a /home /tmp/home`
Configurez votre machine afin d'exporter :

- *le répertoire* `/tmp/etc` *en lecture à l'ensemble des machines de votre salle*
- *le répertoire* `/tmp/home` *en lecture-écriture à l'ensemble des machines de votre salle ayant une adresse IP supérieure à* `.128`.

Démarrez le serveur NFS.

Question

Mise en place du serveur NFS. Comment faites-vous ?
Comment démarrez-vous le serveur NFS ?
Que fait la commande `exportfs -rv` *?*
Est-ce que le démarrage du serveur exécute cette commande ?
Où se trouvent les logs du serveur NFS ?

APPELLEZ VOTRE ENSEIGNANT

3.2. Test du service

Sur le serveur NFS, taper la commande `chmod 600 /tmp/etc/passwd` *; vous pourrez dans vos tests vérifier si vous pouvez lire ce fichier ou non à partir du client NFS.*

Pour utiliser la commande `showmount` *il faut monter les partitions avec* `nfsvers=3`.

Question et manipulation

Quelle commande vous permet :

- *de vérifier quels sont les services RPC disponibles sur votre serveur,*
- *de vérifier que le service NFS est bien présent sur votre serveur,*
- *de connaître l'ensemble des partitions NFS actuellement exportées par votre serveur ?*

Sur le client ou sur le serveur ?

Question et manipulation

Configurez le client NFS. Comment avez-vous fait ?
Que signifie l'option de montage `auto` *?*
Que fait la commande `mount -a -t nfs` *?*
Proposez plusieurs scénarii permettant de tester <u>*toute*</u> *la configuration avec vérifications exhaustives des droits d'accès. Expliquez les messages d'erreurs NFS rencontrés.*

Question et manipulation

Quels fichiers de `/tmp/etc` sont lisibles
en tant que `root` :
en tant que `moi` :
Expliquez pourquoi

Comment modifier la configuration du serveur pour lire tous les fichiers en tant que `root` ?

APPELLEZ VOTRE ENSEIGNANT

3.3. Étude du protocole

Question et manipulation

Montez le répertoire `/tmp/home` à partir d'une machine cliente autorisée dans le répertoire `/nfshome`. Créez, sur la machine cliente, un compte utilisateur `toto` ayant comme répertoire de connexion `/nfshome/toto` et connectez-vous en tant que `toto`..
Comment avez-vous fait ? Expliquez et commentez.

Question et manipulation

Visualiser avec `wireshark` les échanges entre le client et le serveur NFS.
Quel filtre de capture utilisez-vous ?

Question et manipulation

Exécutez les commandes ci-dessous et observez les échanges. Pour chaque commande, résumez et commentez ce que vous observez : nombre de messages, noms et paramètres des procédures distantes exécutées… :

```
mkdir /nfshome/toto/TMP;

chmod 777 /nfshome/toto/TMP;

cd /nfshome/toto/TMP ;

echo "Bonjour" > /nfshome/tpr/TMP/bj.txt
```

Question et manipulation

Évaluez les performances de NFS par rapport à un accès au système de fichier local pour la copie d'un gros fichier. Idem pour la création et l'extraction d'une grosse archive.

Configurez un deuxième client et vérifiez que si un client verrouille un fichier l'autre client ne pourra pas le verrouiller. Utilisez la commande `flock` pour verrouiller le fichier. Sur le serveur quel processus gère les verrous ?
Redémarrez le serveur NFS, qu'est-ce qui se passe ? Pour les fichiers en cours d'écriture, est-ce que la copie se termine correctement ? Le client a-t-il besoin de refaire le montage ? Les verrous sont-ils déverrouillés ?

Voir questions Thierry sur perf NFS, verrous, `flock` (pour flock il faut statd)

APPELLEZ VOTRE ENSEIGNANT

4. Le service DNS

NOM 1 :	***NOM 2 :***	***Salle : TPR1 TPR2***
Adresse IP du serveur :	***Adresse IP du client :***	

Question

Service rendu par DNS :

On vous propose dans cette partie de :

- mettre en place un serveur DNS primaire qui soit serveur de source autorisée pour la zone de votre salle de TP dont vous avez la charge,
- tester le bon fonctionnement local du serveur à partir des machines clientes de la salle,
- mettre en place un serveur racine (primaire ou secondaire) et tester l'interrogation du serveur DNS de l'autre salle de TP,
- analyser les échanges de requêtes/réponses DNS entre les différents serveurs.

Pour simplifier, les zones DNS seront des TLD (*Top Level Domain*) et les machines seront nommées par le biais de leur adresse IP. Par exemple, les machines de la salle TPR1 seront dans la zone `.tpR1.` et seront référencées dans le serveur DNS de la façon suivante : `m1.tpR1` pour `192.168.1.1`, `m10.tpR1` pour `192.168.1.10`…

Si plusieurs binômes mettent en place un serveur DNS dans la même salle, mettez en place une zone par binôme en vous répartissant les plages d'adresses IP gérées de manière équitable. Si par exemple trois binômes sont en charge du DNS dans la salle TPR2, un binôme sera en charge de la zone `.tpR2A.` un autre de la zone `.tpR2B` le dernier de la zone `.tpR2C.` ; le serveur DNS primaire de la zone `.tpR2A.` référencera les machines ayant comme adresse IP `.1`, `.4`, `.7`, etc. ; celui de la zone `.tpR2B.` référencera les machines ayant comme adresse IP `.2`, `.5`, `.8`, etc ; celui de la zone `.tpR2C.` référencera les machines ayant comme adresse IP `.3`, `.6`, `.9`, etc.

4.1. Mise en place du service

Question et manipulation

Installez et configurez votre machine afin qu'elle soit serveur DNS pour la zone dont vous avez la charge. *Zone DNS :* *Plage IP :*

Que mettez-vous dans le fichier `named.conf` ?

Créez les fichiers de zone adéquats ; le nombre de machines à renseigner étant important, on vous suggère de générer automatiquement vos fichiers de zone. N'oubliez pas de renseigner la zone inverse. Donnez pour chaque fichier de zone un ou deux exemples de chaque type de RR utilisé :

Démarrez le serveur DNS. Pensez à regarder les logs à chaque démarrage du serveur.

Question et manipulation

Donnez des noms plus parlants à certaines machines telles que les serveurs NFS, les serveurs DNS, les serveurs LDAP, et ce sans changer le nom canonique. Comment procédez-vous ?

Mettez en place cette nouvelle configuration en donnant par exemple des noms tels que `dns1.tpR1`, `nfs1.tpR2`… Quelles modifications avez-vous apportées aux fichiers de configuration ?

4.2. Test du service

Question et manipulation

Configurez un client DNS de votre zone avec comme nom de domaine par défaut celui de votre zone et comme serveur DNS local le serveur primaire de la zone (le vôtre !). Comment faites-vous ?

Vérifiez que votre client et serveur fonctionnent. Donnez un exemple de test avec la commande `dig` *et un autre avec la commande* `host`

Question et manipulation

Quelle commande `host` *vous permet :*

- *de vérifier que votre machine cliente est bien enregistrée dans le serveur DNS de votre zone,*
- *de vérifier également qu'elle est bien enregistrée dans la zone inverse,*
- *de lister les serveurs primaire et secondaires de votre zone,*
- *de connaître l'adresse e-mail de l'administrateur de la zone,*
- *de lister tous les alias de votre zone (et uniquement eux),*
- *de connaître l'ensemble des enregistrements référencés par votre serveur DNS ?*

Visualiser avec `wireshark` *les échanges des requêtes/réponses DNS.*

APPELLEZ VOTRE ENSEIGNANT

4.3. Mise en place d'un serveur racine

Question et manipulation

Faites en sorte que tous les clients et serveurs DNS des deux salles se pinguent.
Pour les questions ci-dessous, vous utiliserez la commande `dig` ***sans PUIS avec*** *l'option* `+trace` *pour voir l'enchaînement des requêtes entre les différents serveurs DNS potentiels.*

A partir d'une machine cliente configurée pour interroger votre serveur DNS, que se passe-t-il si vous essayez de résoudre le nom `www.univ-lyon1.fr` *qui n'est référencé dans aucun des serveurs DNS installés ?*

En interrogeant votre serveur DNS, que se passe-t-il si vous essayez de résoudre le nom d'une machine référencée dans un autre serveur DNS que le vôtre ?

Même question en interrogeant directement le serveur DNS de source autorisée.
Qu'en concluez-vous ?

APPELLEZ VOTRE ENSEIGNANT

Question et manipulation

En commun avec les autres binômes, configurez un serveur racine primaire dont l'adresse IP est `192.168.1.19`*. Que faut-il mettre dans* `named.conf` *? Dans le fichier de la zone* `.` *?*

Modifiez le fichier de zone racine de votre serveur DNS pour qu'il référence le serveur racine qui vient d'être mis en place. Refaites les tests de la question précédente. Que concluez-vous ?

APPELLEZ VOTRE ENSEIGNANT

5. Le service LDAP

NOM 1 :	***NOM 2 :***	***Salle : TPR1 TPR2***
Adresse IP du serveur :	***Adresse IP du client :***	

Question

Service rendu par LDAP :

5.1. Mise en place du service

On souhaite mettre en place un annuaire LDAP qui permette :

- la gestion et l'authentification sous Unix des utilisateurs de votre salle de TP,
- la gestion de groupes d'utilisateurs sous Unix,
- la gestion des noms et adresses des machines de la salle.

Réfléchissez au modèle d'information de votre annuaire (c'est à dire les objets dont vous avez besoin et les schémas LDAP que vous allez utiliser) ainsi qu'à l'organisation du DIT (Directory Information Tree) que vous allez mettre en place (modèle de nommage).

Question

Réflexions sur le modèle d'information : Que voulez-vous stocker avec quels objets ? Pourquoi ? Comment voir dans quel schéma un objet est stocké ?

Réflexions sur l'organisation du DIT : Quelle architecture ? Combien de niveaux ? Pourquoi ?

Que prenez-vous comme DN racine ? Pour rappel, il doit être unique et construit à partir du nom de la zone DNS. Il sera donc de la forme `dc=tpR1B`

Faites un schéma du DIT avec les DN :

Question et Manipulation

Installez votre serveur LDAP.
Quelles informations avez-vous données lors de la pré-installation ?

Faites `dpkg-reconfigure slapd` *Vérifiez que votre serveur LDAP est bien démarré.*

Que fait la commande `slapd-config` *?*
Comment redémarrer le serveur ? Quand cela est-il nécessaire ?
Où se trouvent les logs du serveur ?

Question et manipulation

Quels sont les paramètres de connexion d'un client LDAP à votre annuaire ?

Testez la connexion depuis un client LDAP graphique et en ligne de commande.
La connexion a-t-elle réussie ? Si oui, y'a-t-il des entrées dans l'annuaire et lesquelles ?

APPELLEZ VOTRE ENSEIGNANT

5.2. Ajout d'entrées dans l'annuaire

Question et manipulation

Écrivez un fichier au format LDIF contenant une entrée de chacun des types de votre annuaire. Quelle commande `ldapadd` *permet d'ajouter ces entrées dans votre annuaire ?*

Après ajout de ces entrées, vérifiez qu'elles ont effectivement été ajoutées.

Manipulation

En utilisant le client LDAP graphique, en dupliquant l'utilisateur déjà ajouté, ajoutez pour chaque binôme de la salle un utilisateur `b1` *pour le binôme1,* `b2` *pour le binôme2… Vous prendrez comme répertoire de connexion* `/nfshome/b1` *pour le binôme1… Pour l'instant, vous mettrez comme mot de passe, l'uid du binôme en clair.*

Ajoutez un groupe regroupant tous les binômes.

Question et manipulation

Nom de votre zone DNS : *Nom canonique de votre machine :*
Ecrivez un programme ou script qui génère un fichier LDIF décrivant toutes les machines de votre zone DNS. Ajoutez ces entrées dans l'annuaire. Par exemple pour la zone `tpR1`*, il y aurait :* `m1.tpR1/192.168.1.1`*,* `m3.tpR1/192.168.1.3`*, …*

5.3. Interrogation de l'annuaire et utilisation de filtres

Question et manipulation

Citez trois méthodes différentes pour voir tout le contenu de l'annuaire. Indiquez pour chacune d'elles comment faire ainsi que le filtre utilisé :

APPELLEZ VOTRE ENSEIGNANT

Question et manipulation

Utilisez la commande `curl` *pour interroger votre annuaire à l'aide d'une url LDAP :*

```
curl -u USER:PASS 'ldap://url_a_completer'
```

Quelle URL permet d'afficher <u>*uniquement*</u> *:*

- *tous les* `rdn` *de l'annuaire,*
- *la liste des membres (nom, uid) du groupe contenant l'ensemble des binômes de la salle,*
- *la liste des utilisateurs (nom, uid) qui n'appartiennent pas au groupe précédent,*
- *pour chaque machine répertoriée dans l'annuaire, son/ses nom(s) et son adresse IP.*

Question et manipulation

Quelle commande `ldapsearch` *avec l'option* `-LLL` *permet afficher* `uid` *et mot de passe de chaque utilisateur ?*
Qu'affiche la commande si exécutée en tant qu'administrateur :
Qu'affiche la commande si exécutée en tant que l'utilisateur `b1` *:*
Que constatez-vous ? Expliquez.

Question et manipulation

Modifiez la configuration du serveur (`man slapd-config` et `man slapd.access`) afin de faire en sorte que l'attribut `homeDirectory` soit modifiable uniquement par l'administrateur, et lisible que par les utilisateurs authentifiés. Vérifier que cela fonctionne.

5.4. Authentification Unix et résolution de noms via LDAP

Question et manipulation

Comment faire pour permettre aux utilisateurs de la salle de s'authentifier via votre annuaire LDAP et leur permettre de changer leur mot de passe. Quel(s) fichier(s) modifier et comment ? Sur le client ou sur le serveur LDAP ?

Vérifiez que tout fonctionne bien avec les commandes `id`, `su` ou `telnet`, `passwd`, `chown`, `chgrp`... Expliquez et commentez les tests effectués :

Après avoir modifié le mot de passe avec la commande `passwd`, regardez le contenu de l'attribut `userPassword` avec `ldapsearch` ! Commentaire :

Question et manipulation

Comment faire la résolution de noms via l'annuaire LDAP ?
Testez avec la commande `ping`.
Ajoutez un alias dans l'annuaire pour désigner cette machine et refaites un `ping` vers cet alias.
Le `ping` vers cet alias fonctionne-t-il ?

5.5. Etude du protocole

Question et manipulation

Quel filtre de capture utilisez-vous pour visualiser les échanges entre le client et le serveur LDAP? Lancez une capture avec ce filtre dans `wireshark`. Exécutez `id b1` depuis une machine cliente, observez les messages LDAP échangés entre le client et le serveur et expliquez leur contenu.

APPELLEZ VOTRE ENSEIGNANT