TP 1-2-3-4 de AdminSR – M2SRIV : Etudes et mises en place de protocoles Client/Serveur

NFS, NIS, DNS, LDAP

Auteur : Olivier GLÜCK, Université Lyon 1

Objectifs

- Apprentissage et mise en place de services utilisés dans l'administration système et réseau d'un parc de machines (NFS, NIS, DNS, LDAP)
- Installation et configuration de ces services sous Linux
- Observation et étude des protocoles de type Client/Serveur associés avec l'utilisation de `tcpdump` et `wireshark`

Pré-requis

Adressage IP, configuration réseau des machines, utilisation d'un miroir *debian* pour l'installation de packages, connaissance des protocoles client/serveur NFS, NIS, DNS et LDAP

NB

Ce TP se déroulera sur 4 séances de 4 heures chacune. Vous répondez à un questionnaire en ligne lors de chaque séance.

1. Introduction (pour vous aider !)

1.1. Outils de capture de paquets

Pour communiquer, les machines échangent des informations sous forme de paquets qui sont l'unité de données échangées sur le réseau. Il est possible « d'écouter » le câble Ethernet et de regarder ce qui se passe quand vous lancez des commandes comme `ping`, `rlogin`, …

Un premier outil permettant d'observer le réseau s'appelle `tcpdump`. Pour écouter le trafic sur l'interface `eth0`, il faut taper la commande `tcpdump -i eth0`.
Par défaut, `tcpdump` écoute en « *promiscuous mode* », c'est à dire qu'il capture et analyse toutes les trames circulant sur le réseau même celles qui ne concernent pas la machine sur laquelle il tourne.

Un deuxième outil, un peu plus convivial que `tcpdump` car utilisable en mode graphique avec un affichage plus lisible, est l'utilitaire `wireshark`. N'oubliez pas de cocher « `Update list of packets in real time` ».

Ces deux outils permettent d'établir des filtres de capture de paquets de manière assez fine. La syntaxe des filtres utilisés et la même pour `wireshark` que pour `tcpdump`. Par exemple, la commande `tcpdump -i eth0 tcp dst port 53` permet de ne capturer sur l'interface `eth0` que les segments TCP dont le port de destination est 53. Pour plus d'informations, consultez la page manuelle de `tcpdump`.

1.2. Comment installer un nouveau package ?

1- faire `apt-get update`
`apt-get install nom_pkg` où nom_pkg est le nom du package à installer
Pour ce TP, les packages qui nous intéressent sont listés ci-dessous.

2- pour vérifier que le package est correctement installé, faire un `dpkg -l` et vérifiez que la ligne correspondant au package commence par `i` ; si tel n'est pas le cas, appelez l'enseignant !

1.3. Liste des packages devant être installés dans le cadre de ce TP

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`

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

Ce TP se déroule sur 4 séances : une séance par service (NFS, NIS, DNS ou LDAP). Lors d'une séance, vous devez traiter un des services que vous n'avez pas encore traité lors des séances précédentes (reportez-vous au tableau de répartition qui vous indiquera pour chaque séance la salle de TP, le service et l'adresse IP de votre serveur).
Il vous est demandé de rendre un compte-rendu de TP à la fin de chacune des séances en répondant aux questions posées dans l'énoncé. Ce compte-rendu est saisi en ligne avec le navigateur `iceweasel` à l'adresse http://demo710.univ-lyon1.fr/cs-x où x=nfs pour NFS, nis pour NIS, dns pour DNS, ldap pour LDAP).
Il ne vous est pas demandé de faire une rédaction très propre mais uniquement de montrer par des réponses brèves et précises que vous avez compris. **Vous n'oublierez pas de bien indiquer sur chaque compte-rendu le nom des binômes concernés, le service traité, la salle de TP et le numéro de la séance.** Pour chacun de ces services, vous devrez : mettre en place le service, capturer et analyser des échanges client/serveur typiques et tester le bon fonctionnement de l'ensemble.

Les binômes se répartissent de manière égale dans chacune des trois salles TPR1, TPR2, TPR3 et ce de façon à avoir à la fin de chaque séance, les quatre services en place dans chacune des salles indépendamment des autres. Vous mettrez en place trois sous-réseaux indépendants : **`192.168.1.0/24`** dans la salle TPR1, **`192.168.2.0/24`** dans la salle TPR2 et **`192.168.3.0/24`** dans la salle TPR3. 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, son (ou ses) serveur(s) NIS 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 NIS entre `.30` et `.39`, les serveurs LDAP entre `.40` et `.49` ; 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 NIS maître l'adresse `192.168.1.30`… 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.

Pour tester le service dont vous aurez la charge, vous pourrez être amenés à vous connecter sur la machine d'un de vos voisins qui vous servira alors de client pour le service que vous mettez en place. On vous suggère alors d'utiliser deux bureaux virtuels différents pour le client et le serveur et de faire un `rlogin` sur l'adresse `10.0.0.xx` : le mieux étant d'avoir un réseau de contrôle en `10.0.0` sur `la carte USB` pour l'installation des packages et les connexions distantes en plus du réseau utilisé pour vos expérimentations.

3. Le service NFS

Question

Rappelez brièvement quel est le service rendu par NFS ainsi que le principal avantage et le principal inconvénient liés à l'utilisation d'un tel protocole.

On vous propose dans cette partie de :

- mettre en place un serveur NFS qui exporte deux partitions avec des droits différents,
- tester le bon fonctionnement du serveur NFS à partir de machines clientes de la salle,
- étudier les échanges entre un client et un serveur NFS.

3.1. Mise en place du service

Question

Notez dans votre compte-rendu les opérations effectuées pour mettre en place les manipulations indiquées ci-dessous (vous ne détaillerez pas la partie installation des packages). Que fait la commande `exportfs -rv` ?

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

Dans la configuration précédente, on vous demande maintenant d'interdire aux stations `.130` et `.131` l'accès à votre serveur NFS. Comment procédez vous ?

3.2. Test du service

Puisque vous aurez besoin de changer d'adresse IP cliente pour faire vos tests, vous utiliserez comme client NFS une machine qui n'est ni serveur NFS, ni serveur NIS, ni serveur DNS, ni serveur LDAP (donc une machine inoccupée !). Sur le serveur NFS, vous taperez 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.

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 ?*

Pour chacune de ces commandes, vous indiquerez si vous l'exécutez sur le client ou sur le serveur.

Question et manipulation

Proposez un ou plusieurs scénarii qui permette(nt) de tester précisément l'ensemble des caractéristiques (mises en place à la section précédente) de votre serveur NFS. Vous décrirez comment vous configurez un client NFS. Vous proposerez une démarche permettant de vérifier que les droits d'accès au serveur NFS sont bien ceux souhaités. Vous noterez dans le compte-rendu les

messages d'erreurs NFS rencontrés en les expliquant. Que signifie l'option de montage `auto` ? Que fait la commande `mount -a -t nfs` ?

Question et manipulation

Montez le répertoire `/tmp/etc` du serveur. Quels sont les fichiers que vous pouvez lire ? Expliquez. Modifiez la configuration du serveur afin de pouvoir lire tous les fichiers.

3.3. Etude du protocole

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`.

Question et manipulation

Mettez en place un moyen de visualiser les échanges entre le client et le serveur NFS. Quel filtre de capture utilisez vous ?

Question et manipulation

Exécutez les commandes suivantes : `mkdir /nfshome/toto/TMP; chmod 777 /nfshome/toto/TMP; cd /nfshome/toto/TMP ; echo "Bonjour" > bj.txt`. Pour chacune d'entre-elles, vous résumerez brièvement et commenterez les échanges observés (nombre de messages, noms et paramètres des procédures distantes exécutées, ...) ?

Question et manipulation

Evaluez les performances de NFS relativement à un accès au système de fichier local pour la copie d'un gros fichier d'une part, la création et l'extraction d'une grosse archive d'autre part.

Question et manipulation

Configurez un deuxième client NFS et vérifiez que si un client verrouille un fichier, l'autre client ne pourra pas le faire. Pour verrouiller le fichier, utilisez la commande `flock`. Quel processus gère les verrous NFS ?

Question et manipulation

Quand vous redémarrez le serveur NFS, que se passe t-il 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 ?

3.4. S'il reste du temps (ce qui devrait être le cas !)…

Question

On suppose que les quatre services sont correctement configurés et que vous êtes promus administrateur de l'ensemble du réseau. Un nouvel utilisateur arrive dans l'organisation avec une machine neuve installée sous Linux. Citez précisément les opérations que vous devez effectuer afin d'intégrer complètement ce nouvel utilisateur et sa machine dans votre réseau (vous donnerez un nom de machine et un nom de login à ce nouvel arrivant). Cet utilisateur devra pouvoir s'authentifier sur n'importe quelle machine du réseau et sa machine devra être accessible aux autres par son nom.
Configurez une machine qui soit à la fois client NFS, client NIS, client LDAP et client DNS. Testez le bon fonctionnement des quatre services. Changez l'ordre d'utilisation des services en configurant le fichier `nsswitch.conf`.

4. Le service NIS

Question

Rappelez brièvement quel est le service rendu par les NIS ainsi que le principal avantage et le principal inconvénient liés à l'utilisation d'un tel protocole.

On vous propose dans cette partie de :

- mettre en place un serveur NIS maître pour les utilisateurs de la salle,
- configurer un client NIS et vérifier le bon fonctionnement du serveur,
- étudier les échanges entre un client NIS et un serveur NIS,
- mettre en place une configuration avancée avec accès restreints au serveur NIS et tester son bon fonctionnement.

Vous choisirez comme nom de domaine `tpR1_nisdomain` ou `tpR2_nisdomain` selon votre emplacement (`tpR1A_nisdomain` ou `tpR1B_nisdomain` si vous êtes plusieurs binômes NIS dans la salle TPR1…).

4.1. Mise en place du service

Question

Quels démons doivent tourner sur le serveur NIS maître sachant que vous ne prévoyez pas pour l'instant la mise en place de serveur NIS esclave mais que vous souhaitez permettre aux utilisateurs de changer leur mot de passe ?

Question et manipulation

ATTENTION DE BIEN EFFECTUER CES OPERATIONS DANS L'ORDRE !

- *Effacez les installations précédentes du package NIS afin de partir d'une configuration propre : `dpkg --purge nis`,*
- *installez le package `nis` nécessaire à la mise en place du serveur NIS (faites `<CTRL-C>` quand le message « `Starting NIS services…` » apparaît),*
- *tuez les démons `yp` qui tournent encore avec `kill` (faire un `ps auxgww` pour vérifier)*
- *redémarrez le portmapper (peut être long) : `/etc/init.d/rpcbind restart`,*
- *positionnez/vérifiez le nom de votre domaine NIS,*
- *renseignez la variable `NISSERVER` du fichier `/etc/default/nis` (vous pourrez éditer le fichier `/etc/init.d/nis` pour voir quelle valeur lui assigner),*
- *configurez votre machine pour qu'elle soit aussi client NIS : vous ferez en sorte que le client NIS ne recherche pas les serveurs NIS par `broadcast` mais plutôt qu'il interroge directement votre serveur NIS,*
- *créez la base NIS à l'aide de la commande `ypinit`,*
- *démarrez votre serveur NIS maître et vérifiez que les bons démons sont bien lancés.*

Pour chacune de ces manipulations, vous indiquerez dans le compte-rendu comment vous avez procédé.

Question

Que fait précisément la commande `ypinit` ? Qu'est ce qu'une carte ? Les cartes sont-elles lisibles par la commande `cat` ? Que fait la commande `make` dans `/var/yp` ?

4.2. Test du service

Puisque vous aurez besoin de changer d'adresse IP cliente pour faire vos tests, vous utiliserez comme client NIS une machine qui n'est ni serveur NFS, ni serveur NIS, ni serveur DNS, ni serveur LDAP (donc une machine inoccupée !).

Question et manipulation

Configurez un client NIS sur une autre machine. Vous indiquerez dans le compte-rendu les différentes manipulations effectuées.

Question et manipulation

Quelle commande vous permet :

- *de vérifier quels sont les services RPC disponibles sur votre serveur,*
- *de vérifier qu'un serveur NIS est bien joignable sur votre serveur,*
- *de vérifier que le service permettant le changement de mot de passe via les NIS est disponible,*
- *de savoir si un client NIS tourne sur une machine,*
- *de connaître, à partir d'une machine cliente, le serveur NIS auquel elle est associée,*
- *d'afficher, à partir d'une machine cliente, le contenu de la carte `passwd` du serveur NIS ?*

Vous exécuterez chacune de ces commandes et vous indiquerez si vous les exécutez sur le client ou sur le serveur.

Question et manipulation

Proposez deux scénarii qui permettent de tester le bon fonctionnement de votre serveur NIS : l'un concernera la carte des noms de machine, l'autre les cartes passwd/group. Vous décrirez précisément comment vous avez mis en place ces deux procédures de test.

4.3. Etude du protocole

Manipulation

Sur le serveur NIS, ajoutez un utilisateur `titi` et donnez un nom à votre machine cliente (`nisclient_xxxx` où `xxxx` sont les initiales du binôme).

Question et manipulation

Mettez en place un moyen de visualiser les échanges entre le client et le serveur NIS. Quel filtre de capture utilisez vous ?

Question et manipulation

Exécutez les commandes suivantes : `ypwhich ; ssh nisclient_xxxx; id titi; yppasswd titi`. Pour chacune d'entre-elles, vous résumerez brièvement et commenterez les échanges observés (nombre de messages, noms et paramètres des procédures distantes exécutées, ...) ?

4.4. Configurations avancées

Question et manipulation

On vous demande maintenant de n'autoriser l'accès à votre serveur NIS qu'à l'ensemble des machines de votre salle ayant une adresse IP supérieure à `.128`, exceptées les stations `.132` et `.133`. Comment procédez vous ? Mettez en place cette configuration.

Question et manipulation

Les utilisateurs du réseau sont désormais séparés en deux catégories : les personnels permanents qui peuvent se connecter depuis n'importe quelle machine autorisée (cf. question précédente) et les personnels nomades qui ne peuvent se connecter que sur les machines autorisées ayant une adresse IP multiple de 10 (`.130`, `.140`, ...). Proposez une solution permettant la mise en œuvre de cette architecture et mettez la en place.

Question et manipulation

Testez le bon fonctionnement des deux configurations précédentes. Vous préciserez dans le compte-rendu la stratégie employée.

4.5. S'il reste du temps…

Question

On suppose que les quatre services sont correctement configurés et que vous êtes promus administrateur de l'ensemble du réseau. Un nouvel utilisateur arrive dans l'organisation avec une machine neuve installée sous Linux. Citez précisément les opérations que vous devez effectuer afin d'intégrer complètement ce nouvel utilisateur et sa machine dans votre réseau (vous donnerez un nom de machine et un nom de login à ce nouvel arrivant). Cet utilisateur devra pouvoir s'authentifier sur n'importe quelle machine du réseau et sa machine devra être accessible aux autres par son nom.

Manipulation

Configurez une machine qui soit à la fois client NFS, client NIS, client LDAP et client DNS. Testez le bon fonctionnement des quatre services. Changez l'ordre d'utilisation des services en configurant le fichier `nsswitch.conf`.

Manipulation

(S'il reste encore du temps !), vous pouvez mettre en place un serveur NIS secondaire, configurer un client NIS pour qu'il recherche le serveur NIS par broadcast et vérifier que si le serveur NIS associé au client tombe en panne, l'autre serveur prend le relais pour répondre au client. Vous pouvez également configurer des accès restreints carte par carte (`man ypserv.conf`).

5. Le service DNS

Question

Rappelez brièvement quel est le service rendu par le DNS ainsi que le principal avantage et le principal inconvénient liés à l'utilisation d'un tel protocole.

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 deux binômes sont en charge du DNS dans la salle TPR2, un binôme sera en charge de la zone `.tpR2A.` et l'autre de la zone `.tpR2B.` ; le serveur DNS primaire de la zone `.tpR2A.` pourra par exemple référencer les machines ayant une adresse IP impaire et l'autre serveur DNS celles ayant une adresse IP paire.

5.1. Mise en place du service

Question

Notez dans votre compte-rendu les opérations effectuées pour mettre en place les manipulations indiquées ci-dessous (vous ne détaillerez pas la partie installation des packages). Vous commencerez par rappeler la zone DNS dont vous avez la charge ainsi que la plage d'adresses des machines que vous devez référencer. Vous pourrez préciser ce que vous avez modifié dans le fichier `named.conf`, les fichiers de zone que vous avez créés et ce que vous y avez mis.

Manipulation

Installez les packages nécessaires à la mise en place d'un serveur DNS. Configurez votre machine afin qu'elle soit serveur DNS pour la zone dont vous avez la charge :

- *Renseignez 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 à l'aide d'un petit programme C ou script shell par exemple. N'oubliez pas de renseigner la zone inverse.*

Démarrez le serveur DNS. Important : pensez à regarder les logs du serveur DNS dans `/var/log` à chaque démarrage du serveur.

Question et manipulation

Dans la configuration précédente, on vous demande maintenant de donner des noms plus parlants à certaines machines telles que les serveurs NFS, les serveurs NIS, les serveurs DNS, les serveurs LDAP, et ce sans changer le nom canonique. Comment procédez vous ? Mettez en place cette nouvelle configuration. On pourra par exemple donner des noms tels que `dns1.tpR1`, `nfs1.tpR2`, `nis2.tpR2A`, … Pour ce faire, vous demanderez aux binômes de votre zone les services qu'ils mettent en place et les adresses IP qu'ils utilisent.

5.2. 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 !). Vous préciserez dans le compte-rendu les manipulations effectuées.

Question

Dans la commande `dig @server name type`, précisez ce que signifie chaque paramètre. Donnez l'équivalent de cette commande en utilisant la commande `host`.

Question et manipulation

Quelle commande 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,*
- *de connaître l'ensemble des enregistrements référencés par votre serveur DNS ?*

Exécutez chacune de ces commandes et indiquez pour chacune d'entre-elles dans le compte-rendu si vous obtenez bien le résultat escompté.

5.3. Mise en place d'un serveur racine et étude du protocole

Manipulation

Entendez-vous avec les autres binômes s'occupant du DNS pour configurer une machine en tant que passerelle entre les deux salles de TP. Vérifier à l'aide de la commande `ping` que vous arrivez à joindre le serveur DNS de l'autre salle. N'oubliez pas de configurer sur les machines clientes la route par défaut vers la passerelle ! Vous prendrez comme passerelle la machine à côté du switch central avec les adresses IP 192.168.1.1 et 192.168.2.1

Question et manipulation

Pour cette question, vous utiliserez la commande `dig` **sans PUIS avec** l'option `+trace` pour voir plus précisément ce qui se passe (enchaînement des requêtes entre les différents serveurs DNS potentiels). Vous préciserez dans le compte-rendu les commandes que vous avez tapées et ce que vous avez constaté pour chacune d'entre elles.
A partir d'une machine cliente configurée pour interroger votre serveur DNS, que se passe t-il si vous essayez de résoudre le nom d'une machine imaginaire (par ex. www.google.fr) qui n'est référencée dans aucun des serveurs DNS installés ? Même question pour une machine qui est référencée dans un autre serveur DNS (par exemple celui de l'autre salle) ? Répétez cette dernière opération en interrogeant directement le serveur DNS de source autorisée de l'autre salle. Qu'en concluez-vous ?

Question et Manipulation

Sur une autre machine que la vôtre (si possible), mettez en place un serveur racine qui référence l'ensemble des zones DNS mises en place. Entendez-vous avec les autres binômes DNS pour savoir si vous êtes serveur racine primaire (zone de type `master`) ou secondaire (zone de type `slave`: `man named.conf`). Vous prendrez comme adresse IP pour votre serveur racine `192.168.2.19` (ou `.18`) si vous êtes dans la salle TPR1 ou `192.168.1.19` (ou `.18`) si vous êtes dans la salle TPR2. Vous préciserez dans le compte-rendu comment vous avez configuré ce

serveur : zones déclarées dans `named.conf` et enregistrements référencés dans les fichiers de zone.

Question et Manipulation

Mettez à jour le fichier de zone racine de votre serveur DNS primaire et relancez le. Vous indiquerez dans le compte-rendu ce que vous avez modifié. Exécutez de nouveau avec la commande `dig` les requêtes que vous avez effectuées juste avant la mise en place du serveur racine. Pour chacune d'entre-elles, faites dans le compte-rendu un schéma qui montre l'enchaînement des requêtes/réponses DNS en précisant bien la nature des serveurs DNS impliqués. Vous préciserez également la nature des requêtes/réponses (itérative ou récursive). Que se passe t-il si vous débranchez le câble réseau du serveur racine primaire ?

Question et manipulation

Sur une machine cliente, ajoutez les suffixes des autres zones DNS dans le fichier `/etc/resolv.conf`. Exécutez la commande ping m138 et notez l'adresse IP correspondante. Changez l'ordre des suffixes et recommencez l'opération. Expliquez dans le compte-rendu ce que vous avez constaté.

Question et manipulation

Vous pouvez maintenant expérimenter les mises à jour des serveurs secondaires (racines dans votre cas). Vous noterez dans le compte-rendu vos conclusions sur les deux expériences ci-dessous :
Expérience 1 : Vous pouvez expérimenter un échange de zones entre un serveur de noms racine primaire et un serveur racine secondaire. Modifiez sur le serveur primaire le numéro de série dans l'enregistrement SOA (comme si vous aviez modifié le fichier de zone) et relancez le service. Relancez ensuite le service sur le serveur de noms secondaire. Que constatez-vous dans le fichier de zone du serveur secondaire ? Regardez également les dates de dernière modification du fichier.
Expérience 2 : Vous pouvez expérimenter une autre procédure d'échange, mais cette fois sans relancer le serveur de noms secondaire. Modifiez d'abord sur les deux serveurs le délai de rafraîchissement (`refresh`) et mettez-le à 2 minutes. Relancez les services. Modifiez sur le serveur primaire le numéro de série et relancez le service. Que constatez-vous au bout de 2 minutes sur le serveur secondaire ?

5.4. S'il reste du temps…

Question et manipulation

Visualiser avec `wireshark` les échanges de requêtes/réponses DNS correspondant à une résolution de nom vers une machine de l'autre salle pour laquelle vous n'avez encore jamais effectué la résolution de nom. Notez dans le compte-rendu le nombre de requêtes/réponses pour cette résolution ainsi que les fanions de la réponse DNS. Réitérez une deuxième fois la même manipulation. Que constatez-vous ? Expliquez.

Question

On suppose que les quatre services sont correctement configurés et que vous êtes promus administrateur de l'ensemble du réseau. Un nouvel utilisateur arrive dans l'organisation avec une machine neuve installée sous Linux. Citez précisément les opérations que vous devez effectuer afin d'intégrer complètement ce nouvel utilisateur et sa machine dans votre réseau (vous donnerez un nom de machine et un nom de login à ce nouvel arrivant). Cet utilisateur devra pouvoir s'authentifier sur n'importe quelle machine du réseau et sa machine devra être accessible aux autres par son nom.

Manipulation

Configurez une machine qui soit à la fois client NFS, client NIS, client LDAP et client DNS. Testez le bon fonctionnement des quatre services. Changez l'ordre d'utilisation des services en configurant le fichier `nsswitch.conf`.

6. Le service LDAP

Question

Rappelez brièvement quel est le service rendu par LDAP ainsi que le principal avantage et le principal inconvénient liés à l'utilisation d'un tel protocole.

On vous propose dans cette partie de :

- mettre en place un serveur LDAP maître et réfléchir à la structuration de votre annuaire qui devra permettre le référencement des machines et utilisateurs de votre salle TP,
- ajouter des entrées dans l'annuaire (manuellement et de manière automatisée),
- tester le bon fonctionnement du serveur en l'interrogeant à partir de clients LDAP et en manipulant les filtres LDAP,
- permettre l'authentification des utilisateurs sous Unix via votre annuaire,
- analyser brièvement les échanges entre un client et un serveur LDAP.

6.1. Mise en place du service

Question

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).
Quelle caractéristique essentielle doit respecter le DN (Distinguish Name) d'une entrée ? Que choisissez-vous comme DN racine ? Pour le choix de votre DN racine, on vous demande de respecter les conseils de l'IETF qui sont de le construire à partir des `dc` *(domain components) correspondant à l'identité de votre zone DNS. Renseignez-vous auprès des binômes en charge du DNS ! Entendez-vous également avec les autres binômes éventuels mettant un annuaire LDAP en place dans la même zone DNS (par exemple, si deux binômes font LDAP dans la salle tpR1, l'un prendra* `dc=tpR1A` *et l'autre* `dc=tpR1B` *comme DN racine).*
Vous ferez un schéma explicatif dans le compte-rendu en indiquant les DN que vous avez choisis. Vous indiquerez dans un tableau, pour chaque type d'entrée (conteneurs ou feuilles) du DIT, les objets dont il dérive (en précisant l'objet structurel) et le schéma LDAP contenant cet objet.

Question et Manipulation

Configurez votre machine pour qu'elle devienne serveur LDAP. Installez les packages nécessaires à la mise en place d'un serveur LDAP en prenant garde à modifier, si nécessaire, les champs déjà pré-remplis lors de la pré-installation. Vous devez reconfigurer votre serveur LDAP avec la commande `dpkg-reconfigure slapd` *.Vous indiquerez dans le compte-rendu les éventuels fichiers que vous avez modifiés et comment. Vérifiez que votre serveur LDAP est bien démarré.*

Question et manipulation

Pour voir si votre serveur LDAP fonctionne, essayez de vous y connecter avec `ldapsearch` *ou le client ldap graphique que vous avez installé. Vous préciserez dans le compte-rendu les paramètres de connexion que vous avez utilisés. Avez-vous réussi à vous connecter à la base ? Si oui, y'a t-il des entrées dans l'annuaire ? Pour savoir comment configurer un client LDAP, vous pouvez consulter la page* `man` *de* `ldap.conf`*.*

6.2. Ajout d'entrées dans l'annuaire

Question et manipulation

Ecrivez un fichier au format LDIF qui contienne les descriptions d'une entrée de chacun des types que vous avez définis à la première question. Vous le reporterez également dans votre compte-rendu.

Question et manipulation

Utilisez la commande `ldapadd` *pour ajouter dans l'annuaire les entrées que vous venez de décrire dans le fichier LDIF. Vous noterez la commande utilisée dans le compte-rendu. Proposez une méthode pour vérifier que les entrées ont effectivement été ajoutées.*

Manipulation

Avec le client ldap en mode graphique et en vous appuyant sur les entrées précédentes, ajoutez dans l'annuaire une entrée par binôme présent dans votre salle de TP et un groupe correspondant à l'ensemble de ces binômes. Vous prendrez comme `uid 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.*

Question et manipulation

Ecrivez un programme ou script qui génère un fichier LDIF décrivant toutes les machines de votre zone DNS. Pour connaître les correspondances nom/adresseIP, reportez-vous à la partie sur le DNS. Par exemple pour la zone `tpR1`*, il y aurait :* `m1.tpR1/192.168.1.1`*,* `m3.tpR1/192.168.1.3`*, …*

6.3. Interrogation de l'annuaire et utilisation de filtres

Question et manipulation

Citez trois méthodes différentes vous permettant de voir tout le contenu de l'annuaire. Vous indiquerez le filtre utilisé (permettant de lister toutes les entrées). Essayez une de ces méthodes pour voir si votre annuaire contient bien ce que vous y avez mis jusqu'à présent.

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'`
Vous noterez dans le compte-rendu l'url qui vous permet d'afficher (uniquement) :

- *tous les* `rdn` *(relative distinguish name) répertoriés dans 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

En utilisant la commande `ldapsearch` *avec l'option* `-LLL`*, affichez pour chaque utilisateur référencé dans l'annuaire son* `uid` *et son mot de passe. Vous noterez cette commande dans le compte-rendu. Vous exécuterez cette requête en tant qu'administrateur de l'annuaire puis 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` *ne soit modifiable que par l'administrateur de la base et ne soit lisible que par les utilisateurs authentifiés. Vous indiquerez les modifications*

apportées dans le compte-rendu. Testez si vos modifications sont bien entrées en vigueur (vous pourrez utiliser le client LDAP en mode graphique pour tenter de changer la valeur de l'attribut).

6.4. Authentification Unix et résolution de noms via LDAP

Question et manipulation

On souhaite maintenant permettre aux utilisateurs de la salle de s'authentifier via votre annuaire LDAP. On souhaite également leur permettre de changer leur mot de passe. Quel(s) fichier(s) faut-il modifier et comment ? Vous indiquerez si ces modifications doivent avoir lieu sur le client ou sur le serveur LDAP. Une fois la configuration terminée, vous contrôlerez le bon fonctionnement avec les commandes `id`*,* `su` *ou* `ssh`*,* `passwd`*,* `chown`*,* `chgrp`*, ... Après avoir modifié le mot de passe avec la commande* `passwd`*, regardez le contenu de l'attribut* `userPassword` *avec* `ldapsearch` *!*

Question et manipulation

On souhaite maintenant permettre la résolution de noms via l'annuaire LDAP. Que suffit-il de faire ? Testez son bon fonctionnement avec la commande `ping` *par exemple. Ajoutez un alias dans l'annuaire pour désigner cette machine et refaites un* `ping` *vers cet alias !*

6.5. Etude du protocole

Question et manipulation

Mettez en place un moyen de visualiser les échanges entre le client et le serveur LDAP. Quel filtre de capture utilisez vous ?

Question et manipulation

Exécutez la commande `id b1` *à partir d'une autre machine que votre serveur LDAP qui soit configurée pour permettre l'authentification Unix via votre annuaire. Résumez brièvement et commentez les échanges LDAP observés entre le client et le serveur (nombre de messages, lisibilité des données véhiculant dans les requêtes/réponses…) ?*

6.6. S'il reste du temps…

Question

On suppose que les quatre services sont correctement configurés et que vous êtes promus administrateur de l'ensemble du réseau. Un nouvel utilisateur arrive dans l'organisation avec une machine neuve installée sous Linux. Citez précisément les opérations que vous devez effectuer afin d'intégrer complètement ce nouvel utilisateur et sa machine dans votre réseau (vous donnerez un nom de machine et un nom de login à ce nouvel arrivant). Cet utilisateur devra pouvoir s'authentifier sur n'importe quelle machine du réseau et sa machine devra être accessible aux autres par son nom.

Manipulation

Configurez une machine qui soit à la fois client NFS, client NIS, client LDAP et client DNS. Testez le bon fonctionnement des quatre services. Changez l'ordre d'utilisation des services en configurant le fichier `nsswitch.conf`*.*

7. Répartition des binômes

Voir tableau de répartition joint