EXERCICES DE LA SEANCE 1 :

CONFIGURATION RESEAU STATIQUE

Objectif : acquérir l'adresse nécessaire à la configuration manuelle d'un réseau.
Configuration de départ : un système Linux qui utilise une configuration réseau dhcp.
Mise en situation : le serveur dhcp est en panne ! Vous devez mettre votre station de travail sur le réseau afin de modifier manuellement les fichiers de configuration appropriés et définir une configuration réseau statique.

Sequence 1: définition de l'adresse IP

Mise en situation :
Le serveur dhcp sur votre réseau est en panne. Vous devez alors définir une adresse IP statique afin de pouvoir remettre votre station de travail sur le réseau.

Tâches :

1. Premièrement, désactivez votre interface Ethernet à l'aide de la commande *ifdown* :
   ifdown eth0
2. Ouvrez ensuite le fichier */etc/sysconfig/network-scripts/ifcfg-eth0* dans un éditeur de texte et modifiez son contenu de la façon suivante (où X doit être remplacé par un numéro de votre réseau) :

```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
IPADDR=192.168.0.X
NETMASK=255.255.255.O
GETEWAY=192.168.0.254
```

3. Visualisez le contenu du fichier */etc/resolv.conf*. Vous devriez y retrouver les réglages valides obtenus du serveur dhcp. Si ce n'est pas le cas, faites les modifications nécessaires afin que le tout corresponde à ce qui suit :

```
search  exemple.com
namserver   192.168.0.254
```

4. Activez l'interface que vous venez de configurer à l'aide de la commande *ifup* :
```
ifup  eth0
```

5. Vérifiez vos réglages réseau en appliquant la commande *ping* à server1
6. Redémarrez votre ordinateur et vérifiez de nouveau vos réglages réseau en appliquant la commande *ping* à server1.

Résultat :
Un système configuré de façon à pouvoir fonctionner avec des réglages de réseau statique.

Remise à l'état initial :
Une fois que votre instructeur aura réactivé le serveur dhcp, remettez vos fichiers de configuration à leur état initial, désactivez eth0, puis réactivez-le. Le fichier *ifcfg-eth0* devrait alors ressembler à ceci :

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

Travaux pratiques : installation d'un serveur DNS

PARTIE 1 : INSTALLATION DU SERVEUR

Pour récupérer les adresses IP, on lance un terminal sur chaque une des deux machines et on tape la commande *ifconfig*, on regarde la ligne “inet adr”. On trouve par exemple pour le client : 192.168.108.2 et pour le serveur DNS 192.168.108.1.

Sur la machine serveur on lance le serveur dns en utilisant la commande suivante : /etc/init.d/named start

Sur le serveur DNS :
Dans le fichier /etc/named.conf, on ajoute les lignes suivantes :

```
Domaine.com
      zone "domaine.com" {
      type master;
      file domaine.com.zone";
      };
```

`domaine.com` est le nom de domaine pour lequel le serveur sera primaire (c'est à dire où c'est ce serveur DNS qui sera utilisé), *domaine.com.zone* désigne le fichier où seront stockés les enregistrements de la zone.
On crée le fichier *domaine.com.zone* et on ajoute les lignes suivantes :

```
      $TTL 604800
      domaine.com. IN SOA machine1 root.machine1.domaine.com. (
      1 ; Serial
      604800 ; Refresh
      86400 ; Retry
      2419200 ; Expire
      604800 ) ; Negative Cache TTL
      ;
      domaine.com. IN NS machine1
      machine1 IN A 192.168.108.1.
      machine2 IN A 192.168.108.2.
```

Pour la résolution inverse, dans le fichier *named.conf*, on rajoute :

```
      zone "108.168.192.in-addr.arpa" {
      type master;
      file "Domaine.com.rev";
      };
```

Dans le fichier *domaine.com.rev*, on tape :

```
$TTL 604800
;$ORIGIN 108.168.192.in-addr.arpa.
@ IN SOA machine1 root.machine1.domaine.com (
1 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Negative Cache TTL
;
IN NS machine1.domaine.com.
;
1 IN A machine1
2 IN A machine2
```

Une fois les modifications faites, on tape */etc/init.d/named restart*
Le serveur se relance donc et enregistre les modifications.
Pour voir si le fichier *named.conf* ne comprend pas d'erreur, on tape la commande :
tail /var/log/messages et on repère les lignes des fichiers dans lesquelles il y a des erreurs.
Pour faire l'essai de la résolution directe, on tape sur le serveur la commande :

```
dig @localhost machine1.Domaine.com A
```

Pour tester la résolution inverse on tape :

```
dig @localhost -x 192.168.108.2
```

En résultat nous obtenons :
Avec la première commande nous avons la correspondance IP du nom alors qu'avec la deuxième commande nous avons la correspondance du nom par rapport à l'IP.

Cela atteste que la résolution directe et la résolution inverse fonctionnent.
Pour rajouter des ressources de types CNAME, on rajoute dans le fichier *domaine.com.zone* la ligne :

```
www 86400 IN CNAME machine1.Domaine.com.
```

Pour rajouter des ressources de types MX, on rajoute dans le fichier *domaine.com.rev* la ligne:

```
@ IN MX 5 machine1.domaine.com.
```

CONFIGURATION D'UN CLIENT SOUS LINUX

Par défaut le fichier */etc/resolv.conf* doit contenir l'adresse du serveur de noms que l'on possède et le nom de notre domaine. On peut spécifier plusieurs serveurs de noms grâce à la commande *nameserver*, on peut également positionner notre nom de machine à l'aide la commande *hostname*.
Pour que la commande *ping* réussisse il faut indiquer le serveur DNS que l'on veut utiliser, ici on met la ligne :

```
nameserver 192.168.108.1
```

On teste le ping :
ping machine1.domaine.com, la commande marche le fichier */etc/resolv.conf* est donc bien configuré.
En rajoutant une ressource de type CNAME comme nous l'avons vu au dessus, lorsque l'on tape la commande *ping www.domaine.com*, il y a une réponse de la machine, l'alias fonctionne.

Lorsque l'on lance une capture avec *ethereal* pendant que les pings sont effectués, il y a au niveau des trames :
une demande dns du client vis à vis du serveur pour lui demander l'adresse de *www.domaine.com*, le DNS répond que c'est un alias de machine1 et il donne l'adresse IP de machine1 ensuite le client contacte par un ping l'@ IP de machine1.

PARTIE 2 MISE EN PLACE D'UN SERVEUR SECONDAIRE

Sur le serveur secondaire dans le fichier named.conf, on écrit :

```
zone “domaine.com”{
type slave; //on indique que c'est un serveur secondaire
masters {192.168.108.1};//on indique que le serveur primaire est
192.168.108. 1
};
```

Si on modifie les fichiers de configurations sur le DNS principal, il faut incrémenter le numéro de série, ainsi lors d'une requête DNS en utilisant le serveur secondaire celui ci vérifie si le numéro de série est le même que celui présent dans les fichiers du DNS principal, si ce n'est pas le cas, il met ces fichiers à jours.

Travaux pratiques : installation d'un serveur DHCP

Indications pour la réalisation du TP
L'atelier propose

- d'installer un serveur DHCP sous Linux,
- d'installer un client DHCP sous Linux
- d'installer un client DHCP sous Windows
- de réaliser une phase de test avec les commandes winipcfg et ipconfig de Windows

Matériel nécessaire :
Deux machines en dual boot Linux / Windows en réseau.
Les éléments sur l'analyse de trame, notamment les trames bootp, seront retraités lors des TP sur la métrologie.

Installation du serveur
Les paquets sont déjà installés.
Attention : vous pouvez avoir sur votre distribution, plusieurs serveurs DHCP.
dhcpd est conforme à la RFC 2131. Il fournit un exemple de configuration assez détaillé.
dhcp3, intègre l'inscription auprès d'un DNS Dynamique. C'est ce package que nous allons utiliser dans le TP. Par contre si vous n'avez pas de DNS dynamique sur le réseau, vous devrez mettre en entête du fichier `dhcpd.conf`, la ligne :

```
ddns-update-style none;
```

Configuration du serveur
La configuration consiste à créer 2 fichiers :

- `/etc/dhcp/dhcpd.conf`, ce fichier sert à la configuration même du serveur (plage d'adresses, paramètres distribués),
- `/var/lib/dhcpd/dhcpd.leases`, ce fichier va servir à l'inscription des clients. Chaque client DHCP, génère l'écriture d'un enregistrement dans ce fichier. Cela permet le suivi, les statistiques de l'activité du serveur.

Le fichier de configuration dhcpd.conf
Vous trouverez un exemple de fichier commenté qui permet de réaliser cet atelier dans la documentation de dhcpd sous */usr/share/doc/dhcp**. Vous pouvez créer ce fichier avec un éditeur.

```
$>cat dhcpd.conf

# ici il s'agit du réseau 192.168.0.0
subnet 192.168.0.0 netmask 255.255.255.0 {

#La plage d'adresse disponible pour les clients
range 192.168.0.10 192.168.0.20;

# Les clients auront cette adresse comme passerelle par défaut
option routers    192.168.0.254;

# Ici c'est le serveur de noms, on peut en mettre plusieurs
option domain-name-servers   192.168.0.1;

# Enfin on leur donne le nom du domaine
option domain-name   "freeduc-sup.org";

# Et l'adresse utilisée pour la diffusion
option broadcast-address 192.168.0.255;

# Le bail à une durée de 86400 s par défaut, soit 24 h
# On peut configurer les clients pour qu'ils puissent demander
# une durée de bail spécifique
```

```
default-lease-time  86400;

# On le laisse avec un maximum de 7 jours
max-lease-time 604800;

#Ici on désire réserver des adresses à des machines
group {
#use-host-decl-names indique que toutes les machines dans l'instruction « group »
# auront comme nom, celui déclaré dans l'instruction host.
use-host-decl-names true ;

# ici définir les machines
host m1 {
hardware ethernet 00:80:23:a8:a7:24;
fixed-address 192.168.0.125;
} # End m1

host m2 {
hardware ethernet a0:81:24:a8:e8:3b;
fixed-address 192.168.0.126;
} # End m2

    } # End Group
}     # End dhcp.conf
```

Le fichier */var/lib/dhcp3/dhcpd.leases* peut contenir après l'inscription du premier client :

```
[root@master /etc]# more  /var/lib/dhcpd/dhcpd.leases

lease 192.168.0.10 {

 starts 1 2002/12/14 18:33:45;

 ends 1 2002/12/14 18:34:22;

 hardware ethernet 00:40:33:2d:b5:dd;

 uid 01:00:40:33:2d:b5:dd;

 client-hostname "CHA100";

}
```

On distingue les informations suivantes : Début du bail, Fin du bail, adresse MAC du client, le nom d'hôte du client. Attention ce nom est différent du nom Netbios utilisé sur les réseaux Microsoft.

Activation du serveur

Le serveur est configuré, il n'y a plus qu'à le mettre en route. Utilisez la commande suivante pour arrêter ou activer le service : **/etc/init.d/dhcpd `start | stop`**.
Le script lance le serveur en mode daemon.

Réalisation du TP

1. Installez un serveur DHCP minimal sous Linux et vérifiez le bon démarrage du service
2. Installez un client DHCP sous Linux, vérifiez le bon démarrage du service réseau et l'inscription dans le fichier *dhcpd.leases* du serveur. Testez le renouvellement du bail. Il suffit de relancer le service réseau.
3. Installez un client DHCP sous Windows, vérifiez le bon démarrage du service réseau et l'inscription dans le fichier `dhcpd.leases` du serveur. Testez le renouvellement du bail.
4. Modifiez l'étendue du serveur. Vérifiez le bon fonctionnement de la distribution d'adresses aux clients.
5. Modifiez la configuration du serveur afin qu'il distribue également l'adresse de la passerelle par défaut, l'adresse du serveur de nom. Testez la configuration.
6. Modifiez la configuration du serveur DHCP afin de réserver une adresse au client, vérifiez que le processus a bien fonctionné.

TP Installation/Configuration du service NFS sur GNU/Linux

Objectifs :

- Installer un serveur NFS sur un PC GNU/Linux (RedHat).
- Visiter les principaux fichiers de configuration utiles à NFS.
- Utiliser le service NFS depuis un poste client GNU/Linux.
- Evoquer les aspects de sécurité liés à l'usage de NFS.

1 Configuration réseau des PCs pour le TP

Pour réaliser les TP d'installation des serveurs, il est souhaitable que tous les PCs possèdent une adresse IP fixe. Plusieurs solutions peuvent être envisagées, parmi lesquelles l'utilisation d'un réseau TP possédant une numérotation différente du réseau local. Dans cette optique, on peut par exemple choisir comme adresse réseau : **192.168.x.0**, où la valeur de **x** sera choisie en séance TP pour ne pas interférer avec le réseau local existant (pensez à une interface virtuelle ethx:x).
Le fichier /etc/sysconfig/networkscripts/ifcfg-eth0 devrait ressembler à :

```
DEVICE=eth0
BOOTPROTO=static
IPADDR=192.168.x.y
NETMASK=255.255.255.0
NETWORK=192.168.x.0
BROADCAST=192.168.x.255
ONBOOT=yes
```

Le fichier /etc/sysconfig/network :

```
HOSTNAME=posteX.exemple.com
NETWORKING=yes ...
```

Une fois le réseau configuré, on pourra peupler le fichier */etc/hosts* selon le modèle :

```
#adresse_IP name alias
192.168.x.10 poste10.exemple.com poste10
192.168.x.11 poste11.exemple.com poste11
...
192.168.x.20 poste20.exemple.com poste20
192.168.x.21 poste21.exemple.com poste21
...
```

Remarque : cette étape pourrait être ignorée, mais dans ce cas il faudrait utiliser systématiquement les adresses IP des machines sur le réseau au lieu des nom de machine.

Ne pas oublier de relancer le service **network**. Valider la configuration réseau avec les commandes ifconfig, ping, ssh ...

2 Installation d'un serveur NFS

a - Installation

Utiliser la commande *rpm* pour trouver les paquets *rpm* liés au service NFS
Installer le paquet nfs avec la commande *rpm*.
Visualiser les fichiers du paquet installé.

b - Configuration

La planification des répertoires à exporter est la suivante :

répertoire	***clients autorisés***	***options***
/var/local/data	192.168.x.0/255.255.255.0	rw,sync,root_squash
/var/pub	192.168.x.0/255.255.255.0	rw,sync,root_squash

Créer/modifier si besoin les répertoires comme indiqué ci dessous :

répertoire	***propriétaire***	***groupe***	***modes d'accès***
/var/local/data	nobody	nogroup	rwxrwxrwx
/var/pub	nobody	nogroup	rwxrwxrwx

Editer le fichier /etc/exports en conséquence.
Editer le fichier /etc/sysconfig/nfs : si besoin, on peut augmenter le nombre de processus serveurs NFS à l'aide de la variable NFSDCOUNT (8 par défaut).

c - Lancement des services

+ Vérifier le lancement des services **portmap** et **nfs** pour le *runlevel* courant :
2 façons de visualiser le *runlevel* :
Utiliser un filtre sur la commande 'who a' pour visualiser le *runlevel* courant

Utiliser un filtre sur la sortie de la commande 'ps ax' pour visualiser le *runlevel* courant

Utiliser *chkconfig* pour vérifier sous quels *runlevels* les services portmap et nfs sont lancés

Démarrer le service **portmap**, puis le service **nfs**

d - Vérifications côté serveur

Vérifier le démarrage des services : plusieurs possibilités,

- commande **ps** : ps ax|grep ...
- syslog : tail /var/log/message
- service system V : /etc/init.d/nfs status ou service nfs status ...

A l'aide de la commande 'rpcinfo p', lister les services **portmap** installés pour le serveur NFS :
pour chacun des démons utilisés par NFS , identifier :

- les noms des services **portmap** concernés,
- le numéro de version, le type de transport supporté (tcp ou udp), le numéro de port utilisé ...

Utiliser la commande showmount, sans option. Essayer les option a, d et e.
Comparer le contenu du fichier */etc/exports* et la sortie de la commande *'exportfs -v*'.
Le serveur est maintenant prêt à recevoir des requêtes NFS ...

3 Installation d'un client NFS

L'utilisation standard de NFS sur un poste GNU-Linux ne nécessite pas d'installation particulière puisque les fonctionnalités de montage de ressources distantes via NFS sont intégrées au noyau Linux.

a - Montage nfs à la main

Lister les points de montage du serveur choisi : *showmount –e serveur*

La planification des répertoires à importer par NFS est la suivante : le répertoire /var/pub du serveur NFS 192.168.x.y sera monté sur le répertoire local
/mnt/remote/y/pub
Préparer les points de montage pour les serveurs NFS choisis : mkdir, chmod, ...
Effectuer quelques montages à la main, par exemple :

mount -t nfs 192.168.x.64:/var/local/data /mnt/remote/164/pub

Vérifier les montages NFS : commande « mount –t nfs » ou encore commande df ...
Sous le compte root, créer quelques fichiers, répertoires sous l'arborescence /mnt/remote/x/pub => Vérifier les attributs de création des fichiers (ls -l).
Sous un compte utilisateur, créer quelques fichiers, répertoires sous l'arborescence /mnt/remote/x/pub => Vérifier les attributs de création des fichiers (ls -l).
Créer un compte utilisateur local (inexistant sur le serveur), et utiliser ce compte pour créer quelques fichiers, répertoires sous l'arborescence /mnt/remote/x/pub => Visualiser les attributs de création des fichiers (ls -l) sur le poste client et sur le serveur NFS.
Transférer des fichiers entre postes clients en utilisant le montage NFS.

b - Montages nfs automatisés

Il s'agit de décrire les montages NFS à l'aide du fichier /etc/fstab du poste client :

- Consulter le manuel de la commande mount pour repèrer les options possibles pour le montage d'un *filesystem* de type NFS
- Planifier « quel client va monter quels serveurs » .
- Démonter les montages NFS existant : commande umount
- Les répertoires /var/pub des serveurs NFS d'adresse IP 192.168.x.y seront montés sur les répertoires locaux /mnt/remote/y/pub :
  - les options de montage devront inclure la taille des buffer de lecture/écriture : rsize=8192,wsize=8192
  - les 2 derniers champs (dump et fsck) des entrées NFS dans le fichier /etc/fstab seront nuls
- + Activer les montage NFS décrits dans le fichier /etc/fstab avec la commande mount –a -t nfs
- + Vérifier les montages NFS : commande « mount –t nfs » ou encore commande df ...
- + Vérifier que le service netfs responsable du montage des « fichiers réseaux » est bien démarré en *runlevel* 3, puis rebooter la machine et vérifier les montages NFS.

c - Expérimentation des options de montage NFS : soft, hard, bg

Le but est d'expérimenter l'influence de ces options en cas de panne du serveur NFS.

- Arrêter le serveur NFS utilisé par le client
- Dans le fichier fstab du client, utiliser l'option soft pour les montages NFS
- Rebooter le client et observer ce qui se passe au moment du montage des systèmes de fichier.
- Dans le fichier fstab du client, utiliser l'option hard pour les montages NFS
- Rebooter le client et observer ce qui se passe au moment du montage des systèmes de fichier.
- + Dans le fichier fstab du client, utiliser les options hard,bg pour les montages NFS
- + Rebooter le client et observer ce qui se passe au moment du montage des systèmes de fichier.

TP Service de partage de fichiers Samba

Objectif : Partager des fichiers et des ressources d'imprimante sur le réseau

Séquence 1 : Configuration de Samba pour la connexion des utilisateurs

Tâches :

1- Si nécessaire installer les paquetages samba, samba-common et samba-client et lancer le service smb. Une configuration par défaut est activée. Comment pouvez-vous en observer les détails ?

```
smbclient –L localhost –N
```

2- Créez un groupe nommé *legal* auquel appartiennent les utilisateurs *elies*, *anouar*, *aroua* et *amine*. Ne leur donnez pas de mot de passe ils ne pourront accéder au système que par Samba.

```
groupadd legal
for user in elies anouar aroua amine ; do
   useradd –G legal –s /sbin/nologin $user
done
```

3- Par défaut, Samba est configurer pour recevoir des mots de passe cryptés, mais il n'y a pas encore de mots de passe dans la base de Samba. Pour tester votre serveur vous devez exécuter *smbpasswd* pour chaque utilisateur qui pourra accéder à votre serveur. Ajoutez les utilisateurs de l'étape 2, root et un autre utilisateur de votre choix.

```
smbpasswd –a elies
smbpasswd –a anouar
smbpasswd –a aroua
smbpasswd –a amine
smbpasswd –a root
```

4- Notez que le premier volume partagé défini dans */etc/samba/smb.conf*, [homes], n'a pas de chemin spécifié. Ce partage est configuré pour partager le répertoire personnel d'un utilisateur s'il se connecte et est authentifié. Transférez un fichier dans le volume partagé du répertoire personnel de l'utilisateur elies.

```
smbclient //localhost/elies -U elies
Vous devriez voir maintenant l'invite smb:\>
put /etc/hosts hosts
```

Séquence 2 : Permettre l'accès au répertoire d'un groupe

Scénario :

Il se trouve qu'en plus d'avoir leurs propres privés sur le serveur, nos quatre utilisateurs appartiennent au même département et nécessitent un endroit où stocker leurs fichiers. Nous devons configurer un groupe Linux pour les utilisateurs, créer un répertoire pour qu'ils puissent stocker leur contenu et configurer le serveur Samba pour partager le répertoire.

1- Créez le répertoire */home/depts/legal*. Définissez les propriétés et les permissions de ce répertoire de telle manière que les personnes dans le groupe *legal* puissent ajouter/supprimer des fichiers et personne d'autre.
Définissez également les permissions SGID et Sticky afin que le propriétaire du groupe sur tous les fichiers créés dans ce répertoire soit le propriétaire du répertoire *legal* et qu'un utilisateur ne puisse pas supprimer le fichier d'un autre.

```
mkdir -p /home/depts/legal
chgrp legal /home/depts/legal
chmod 3770 /home/depts/legal
```

2- Créez un partage Samba nommé [legal] dans */etc/samba/smb.conf*. Seuls les membres du groupe *legal* devraient avoir accès au partage. En outre, assurez-vous que les fichiers placés dans le partage [legal] soient créés avec les permissions 0660.

```
[legal]
comment = fichiers de legal
path = /home/depts/legal
publiuc = no
write list = @legal
create mask = 0660

sevice smb restart
```

TP Installation/Configuration du service Apache

Objectifs :

- Installer et configurer un serveur Apache sur un PC GNU/Linux (RedHat).
- Contrôler l'indexation d'un répertoire sur un site.
- Configurer la gestion des pages personnelles.
- Exécuter des scripts cgi ou autres sur le serveur.
- Sécuriser les accès au serveur par authentification ou par source.
- Implémenter plusieurs sites virtuels sur un même serveur.

EXERCICE 1 - Installation et configuration de base

1- Apache est livré dans le paquetage httpd. Est-il installé ? Si oui, quelle est sa version ? Installer (si ce n'est pas déjà fait) le paquetage httpd et assurez vous qu'il est lancé dans les niveaux d'exécution 3, 4 et 5.

2- Le fichier de configuration principal du serveur est /etc/httpd/conf/httpd.conf
Editer ce fichier et répondre aux questions suivantes, qui se réfèrent toutes à la configuration par défaut :

1. Quel directive spécifie le port TCP sur lequel écouter ? Quel est le port par défaut ?
2. Il y a-t-il d'autres fichiers de configuration chargés depuis httpd.conf ? Où sont-ils placés ? Donner leur liste.
3. Quelle est la directive chargeant un module ?
4. Sous quel identité unix (utilisateur et groupe) le serveur va-t-il s'exécuter ? Donner les UID et GID correspondants.
5. Quel est le répertoire racine pour les documents (pages) servis ?
6. Quelle page Apache renvoie-t-il lorsque l'URL demandée correspond à un répertoire ?
7. Comment sont traitées les URLs de la forme http://serveur/cgi-bin/toto ?
8. Quels sont les fichiers de logs générés ? Où sont-ils placés ? Quel est leur format et comment est-il contrôlé ?

EXERCE 2 - Page d'accueil et pages par défaut

1. Comment charger cette page d'accueil du serveur Apache hébergé par votre propre machine ?
2. Pouvez-vous charger la page d'accueil des serveurs Apache des autres groupes ?
3. Observer la page d'accueil : quelle est la version d'Apache ? la documentation d'Apache est-elle installée ?
4. Où se trouve et comment s'appelle cette page d'accueil sur le système de fichiers ? Pour la localiser, trouvez dans le fichier **httpd.conf**, la ligne débutant par **DocumentRoot**, puis lire la page d'accueil.
5. Renommez *index.txt* cette page d'accueil sur votre serveur. Pouvez vous l'obtenir comme précédemment, à partir de la syntaxe *http://serveur/* ? Savez-vous pourquoi ? Qu'obtenez-vous en passant l'URL : *http://serveur/index.txt* ? Expliquez pourquoi. Remettre la page d'accueil d'origine et vérifier.

6. Créez rapidement une petite page HTML portant le nom *index.html* et placez-la à la racine du site
   Qu'obtenez-vous en demandant : *http://serveur/* ? Pourquoi ?
7. Créer une page HTML minimale et la placer à la racine de l'arborescence servie. Lancer le service httpd. Dans quel fichier de log peut-on constater le démarrage ?
8. Accéder à votre page web. Quelle URL utiliser ? Peut-on y accéder depuis une autre machine de la salle ? Avec quelle URL ? Observe-t-on des traces dans les logs ?

Exercive 3 - Contrôler l'indexation d'un répertoire

1. Si cette indexation est bloquée *dans un répertoire*, alors en l'absence d'un quelconque des fichiers par défaut listés à la clause *DirectoryIndex*, on obtient une page d'erreur. En revanche, si cette option d'indexation est activée, on obtient l'affichage du contenu du répertoire demandé.
2. Renommez la page d'accueil en *index.txt*, puis votre page *index.html* en *index.html.old*. Pouvez-vous alors lister le répertoire racine du WEB par *http://serveur/* ?
3. Cherchons la clause qui contrôle cette indexation
   A l'aide d'une commande **grep**, rechercher le numéro de la ligne comportant **"<directory /var/www/html>"**
   Mettre en commentaire la ligne commençant par **Options** et insérer la ligne **Options Indexes FollowSymLinks**
   Enregistrer et relancer le serveur. Vérifier l'effet. Ensuite revenir à la situation initiale et re-bloquer l'indexation du répertoire principal */var/www/html*
4. Créer un sous-répertoire à la racine du WEB */var/www/html*, nommé `webftp`
   Comment permettre à ce répertoire seulement d'être indexé ? Pour cela créer une section :

   ```
   <Directory var/www/html/webftp>
   Options Indexes
   order allow,deny
   allow from all
   </Directory>
   ```

   Placer des pages HTML dans ce répertoire. et vérifier alors qu'affichage et parcours sont autorisés de toutes les stations du réseau

Exercice 4 - Les "pages personnelles"

Comme "webmaster" du site officiel de votre établissement, vous voulez publier les pages personnelles de vos collègues mais pas les gérer vous-mêmes, voire même les laisser gérer eux-mêmes leur site :

1. Vérifier bien la présence de la clause *UserDir public_html* dans le fichier de configuration. Trouvez ce qu'elle signifie
2. Vérifier la présence ou modifier éventuellement pour avoir une directive :

   ```
   <Directory /home/*/public_html>
   order allow,deny
   allow from all
   </Directory>
   ```

Que faut-il alors faire pour permettre à vos utilisateurs de publier et de gérer eux-mêmes leurs "pages persos" ?

3. L'utilisateur *stagex (x=1 ..10)* crée lui-même le répertoire de son site web, et y place une page d'accueil *accueil.html*
4. Peut-il y accéder ?

EXERCICE 5 - Script CGI simple

1- Écrire en shell BASH un script CGI nommé date qui renvoie la date et l'heure dans une page HTML. Où placez-vous le script ? Faut-il configurer quelque chose ?

2- Modifier la configuration pour que toutes les pages suffixées par *.sh* soient considérées comme des CGI et exécutées.

3- Ecrire un CGI qui permette d'afficher la liste des processus appartenant à un utilisateur donné.
http://serveur/listeprocs.sh?user=toto afficherait dans une page HTML la liste des processus de toto s'exécutant sur le serveur.

4- Ecrire une page HTML avec un formulaire simple permettant la saisie du nom de l'utilisateur et qui via un bouton permet de charger le cgi précédent.

EXERCICE 6 - Protection des accès

1- Créez un répertoire secret dans l'arborescence web et placez y une page HTML. Configurez Apache afin que vous ne puissiez accéder au répertoire secret que depuis le serveur lui même.
Quel est le code renvoyé par Apache lorsqu'on tente d'accéder à ce répertoire depuis une autre machine ? Qu'observe-t-on dans les logs ?

2- Protéger l'accès au sous-site privé d'un établissement, supposons qu'il s'agit du sous-répertoire /var/www/html/prive.
Il ne devra être accessible qu'à un ensemble limité de comptes Apache (et non Linux) à créer. Une requête s'adressant à ce répertoire protégé provoquera l'affichage d'une boite de dialogue par laquelle l'utilisateur devra s'authentifier (nom et mot de passe).

1. Créer le répertoire **/var/www/html/prive**, y placer quelques pages HTML.

   Tester leur accessibilité pour tous. Sinon penser à modifier les permissions Linux sur ces fichiers.

2. Créer dans ce répertoire à protéger le fichier .htaccess. En voici une écriture standard :

```
AuthUserFile /etc/httpd/users
AuthName "Accès privé"
AuthType Basic
require valid-user
```

3. Dans ces conditions où se trouvera le fichier d'authentification ?

4. Créer un premier compte Apache avec la commande htpasswd .

```
cd /etc/httpd/
htpasswd -c users admin
   ---> mot de passe demandé (admin), puis confirme.
```

5. Examiner le fichier /etc/httpd/users
   L'utilitaire htpasswd a créé (option -c) le fichier users dans le répertoire courant, ici /etc/httpd, et y a enregistré admin avec son mot de passe crypté.

6. Ajouter un second compte, toto, puis d'autres

```
htpasswd users toto
  ---> mot de passe demandé, puis confirmé
```

7. Tester l'accès au répertoire http://serveur/prive. Pourquoi la protection ne semble-t-elle pas fonctionner ? (remarque : service httpd reload permet de prendre en compte les changements de configuration)
8. Rechercher dans le fichier de configuration la section <Directory /var/www/html> qui fixe des directives par défaut pour le site principal. Par sécurité mettre si nécessaire la clause AllowOverride None
9. Ajouter une directive concernant le répertoire privé

```
<Directory /var/www/html/prive>
   AllowOverride ...
   Options -Indexes
.........
<Directory>
```

10. Retester normalement avec succès ! N'oubliez pas de relancer le navigateur quand on change de compte.
11. Observez le trafic HTTP avec ethereal lors d'un accès au répertoire privé depuis une machine distante. Où se trouve le mot de passe ? Est-il lisible ?

EXERCICE 7 - Serveur "virtuel"

Lorsqu'une machine doit héberger plusieurs sites webs différents et même si elle ne dispose que d'une adresse IP, on utilise la technique des "serveurs virtuels" (Virtual Hosts).

1- Donner plusieurs noms à votre machine (soit via /etc/hosts soit en modifiant le DNS de votre réseau).

2- Configurez Apache, en donnant à chaque hôte virtuel une page d'index différente.

3- Tester votre configuration.

4- Comment séparer les logs d'accès de chaque serveur virtuel ?

Exercice 8 - Réglages d'exécution et suivi

Modifications de paramètres d'exécution

Supposons que le serveur d'établissement soit hébergé par une machine aux ressources limitées, et que le nombre de requêtes qui lui sont adressées n'est jamais considérable.

1. Combien y a t-il de serveurs WEB en exécution lors du démarrage d'Apache, et 150 au maximum simultanément. Comment le vérifiez vous ?
2. Votre capacité mémoire est limitée. Ramenez ces nombres à 4 et à 25. Redémarrez Apache. Vérifiez avec une commande ps

Suivi du journal des accès

1. Passer la commande (à expliquer) : `tail -f /var/log/httpd/access_log`
2. observer le contenu de la console
3. Demander aux groupes voisins de jouer les rôles de clients WEB (avec un browser lynx, Konqueror ou Firefox) et de passer des requetes *http://serveur/*, en direction de votre serveur, et observer les lignes de `access_log` affichées "en direct"
4. Interpréter les champs de chaque ligne, en particulier repérer les renseignements qui concernent le client et les codes de retour des diverses requêtes (200 réussie, 404 "not found" ...)

TP Transfert de fichiers anonyme avec vsftpd

Séquence 1 : Test de l'accès ftp authentifié

L'accès authentifié est simple à mettre en oeuvre.

1. Relevez les ports utilisés par ftp dans /etc/services.

   ```
   grep ftp /etc/services
   ```

2. Démarrez le service vsftpd.

   ```
   service vsftpd start
   ```

3. Vérifiez que le port est bien ouvert avec la commande netstat

   ```
   netstat –ntaupe ¦ grep :21
   ```

4. Faites un test en utilisant un compte système existant.

   ```
   [root@fed12 ~]# ftp localhost
   Trying ::1...
   ftp: connect to address
   Trying 127.0.0.1...
   Connected to localhost (127.0.0.1).
   220 (vsFTPd 2.2.0)
   Name (localhost:user): elies
   331 Please specify the password.
   Password:
   230 Login successful.
   Remote system type is UNIX.
   Using binary mode to transfer files.
   ftp> pwd
   257 "/home/elies"
   ftp> ls
   227 Entering Passive Mode (127,0,0,1,228,126).
   150 Here comes the directory listing.
   226 Directory send OK.
   ftp>
   ```

5. Ajoutez l'utilisateur elies au fichier /etc/vsftpd/ftpusers et refaites la manipulation précédente.

   ```
   [root@fed12 ~]# ftp localhost
   Trying ::1...
   ftp: connect to address ::1Connexion refusée
   Trying 127.0.0.1...
   Connected to localhost (127.0.0.1).
   220 (vsFTPd 2.2.0)
   Name (localhost:user): elies
   331 Please specify the password.
   Password:
   530 Login incorrect.
   Login failed.
   ```

```
ftp>
```

6. Refaites la manipulation de la question 4 mais cette fois-ci avec le compte utilisateur anonyme.

```
[root@fed12 ~]# ftp localhost
Trying ::1...
ftp: connect to address ::1Connexion refusée
Trying 127.0.0.1...
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.2.0)
Name (localhost:user): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/"
ftp> ls
227 Entering Passive Mode (127,0,0,1,80,5).
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Mar 09 11:09 pub
226 Directory send OK.
ftp>
```

Séquence 2 : Autoriser le upload de fichiers pour les utilisateurs anonymes

1- Préparez le répertoire */var/ftp/entrant* pour les fichiers entrants sur le serveur ayant les caractéristiques suivantes :

   a. Le groupe propriétaire doit être ftp
   b. Les permissions seront tout pour le propriétaire, lecture et accès pour le groupe et rien pour les autres.

```
mkdir /var/ftp/entrant
chown root.ftp /var/ftp/entrant
chmod 730 /var/ftp/entrant
```

2- Modifiez le fichier vsftpd.conf pour autoriser les utilisateurs anonymes à effectuer des transferts de fichiers vers le serveur, ces fichiers seront la propriété de l'utilisateur elies et auront les permissions 077.

```
anonymous_enable=YES
anon_upload_enable=YES
chown_uploads=YES
chown_username=elies
anon_umask=077
```

3- Redémarrez le serveur et testez l'envoi de fichiers vers le serveur, puis essayez de lister depuis le client le contenu du répertoire *entrant*.

```
[root@fed12 ~]# ftp localhost
Trying ::1...
ftp: connect to address ::1Connexion refusée
```

```
Trying 127.0.0.1...
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.2.0)
Name (localhost:user): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> ls
227 Entering Passive Mode (127,0,0,1,190,231).
150 Here comes the directory listing.
drwx-wx---    2 0        50            4096 Mar 09 11:07 entrant
drwxr-xr-x    2 0        0             4096 Mar 09 11:09 pub
226 Directory send OK.
ftp> cd entrant
250 Directory successfully changed.
ftp> mput fichier.txt
mput fichier.txt? y
227 Entering Passive Mode (127,0,0,1,112,57).
150 Ok to send data.
226 File receive OK.
6 bytes sent in 0,0002 secs (30,00 Kbytes/sec)
ftp> ls
227 Entering Passive Mode (127,0,0,1,98,122).
150 Here comes the directory listing.
226 Transfer done (but failed to open directory).
ftp>bye

[root@fed12 ~]# ls -l /var/ftp/entrant/
total 4
-rw------- 1 elies ftp 6 avril 19 15:59 fichier.txt
[root@fed12 ~]#
```

Activité séance 6 Installation et configuration de la messagerie

Objectif :

Acquérir les bases de la configuration d'un MTA (Postfix).

Introduction :

Dans les séquences suivantes vous allez :

- Installer et inspecter postfix.
- Ajouter de nouveaux alias à votre installation postfix.
- Configurer votre MTA pour changer son comportement vis-à-vis du relais de mails.
- Installer un serveur POP/IMAP et configurer un client Mail.

Configuration initiale – installation des paquetages nécessaires

```
[root@fed12 ~]# rpm -qa | grep postfix
postfix-2.6.5-2.fc12.i686

sinon vous faites :

yum install postfix
```

Séquence 1 : Configuration de MTA pour recevoir du courrier

Pour des raisons de sécurité, la configuration par défaut de postfix permet l'envoi sur le réseau, mais pas la réception (par défaut elle n'accepte que les connexions sur l'interface loopback). Configurez votre MTA de façon à accepter les connexions entrantes sur toutes les interfaces.

postconf -e "inet_interfaces = all"

Séquence 2 : Démarrage et vérification de MTA

1- Démarrez ou redémarrez le service postfix.

service postfix start ou restart

2- Le service postfix est configuré pour utiliser la fonction syslog pour enregistrer tous les messages dans le fichier /var/log/maillog. Examinez ce fichier et rechercher tout message d'erreur.

tail -f /var/log/maillog

3- Essayez d'envoyer un message de test à root@stationX la station d'un autre utilisateur ayant fait la même manipulation que vous. Vous devriez constater une connexion SMTP cohérente avec votre serveur de relais local.

echo "Bonjour root" | mail -v -s "salut" root@stationX

Si l'échange SMTP se passe bien, c'est que le message a été transmis au serveur de relais local de votre poste.

Quelles options de la commande "mailq" afficheront l'état de la file d'attente de soumission du courrier et la file d'attente d'envoi.

mailq -Ac
et
mailq

4- Relevez les différentes étapes de la connexion SMTP et reproduisez-les avec telnet sur le port 25 du serveur de votre partenaire.

```
[root@fed12 ~]# telnet stationY 25
Trying stationY...
Connected to stationY.
Escape character is '^]'.
220 stationY.domaine.local ESMTP Pstfix; Wed, 14 Apr 2010 11:40:23 +0200
HELO station1.domaine.local
250 fed12.domaine.local Hello localhost [127.0.0.1], pleased to meet you
MAIL FROM: root@fed12.domaine.local
250 2.1.0 root@fed12.domaine.local... Sender ok
RCPT TO: elies@stationY.domaine.local
250 2.1.5 elies@fed12.domaine.local... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
salut
.
250 2.0.0 o3E9eNLd002679 Message accepted for delivery
QUIT
221 2.0.0 fed12.domaine.local closing connection
Connection closed by foreign host.
```

Séquence 3 : Ajouter des Alias

Avant de déterminer la destination d'un message, postfix entreprend une tentative de résolution d'alias.

1- Quel est le fichier utilisé pour l'ajout d'alias?

/etc/aliases

2- Pour optimiser les recherches, postfix génère une tables de hash pour ces définitions d'alias. Quel est le fichier hash des alias et quelle commande le génère?

/etc/aliases.db
La commande : postalias

3- Ajoutez un alias nommé "moi" sur votre compte d'utilisateur, mettez la table de hash à jour et testez un envoi de courrier vers votre alias.

Dans /etc/aliases ajoutez :
moi: votre_compte_utilisateur
Exécutez la commande postalias
Envoi de courrier : echo "Bonjour moi" | mail -s "salut" moi

Séquence 4 : Contrôle du relais

Le relais permet au courrier d'être redirigé vers sa destination à l'aide d'une machine "relais" intermédiaire. Bien qu'il soit parfois utile, le relais est devenu source d'abus sur Internet de la part des spammeurs.
La séquence qui suit va utiliser les hôtes suivants. Remplacez X, Y et Z par les numéros de postes appropriés :

- stationY : la machine source, celle d'où émane le courrier.
- stationX : la machine relais, sur laquelle le courrier est dirigé par l'envoyeur.
- stationZ : la machine de destination finale du courrier.

Cette séquence sous-entend que vous êtes sur stationX, la machine relais, et que vous faites équipe avec quelqu'un qui travaille sur stationY, la machine d'où émane le courrier. Au cours de la séquence, supervisez le fichier /var/log/maillog.
1- Par défaut postfix désactive le relais. Pour activer le relais sur votre sous-réseau quelles commandes doivent être exécutées?

postconf -e "mynetworks_style = subnet"
service postfix restart

2- Faites jouer par votre partenaire le rôle d'un spammeur malintentionné, qui va maintenant pouvoir utiliser votre postfix pour maquiller l'origine de courriers indésirables en faisant directement un telnet sur votre SMTP. Utilisez un identifiant faux lors du HELO et un mail d'origine non valide, destinez le courrier à la machine de destination.

```
[root@fed12 ~]# telnet stationY 25
Trying stationY...
Connected to stationY.
Escape character is '^]'.
220 stationY.domaine.local ESMTP Postfix 8.14.3; Wed, 14 Apr 2010 11:40:23 +0200
HELO mail.cracker.org
250 stationY.domaine.local Hello mail.cracker.org, pleased to meet you
MAIL FROM: spammer@cracker.org
250 2.1.0 spammer@cracker.org... Sender ok
RCPT TO: elies@stationZ.domaine.local
250 2.1.5 elies@stationZ.domaine.local... Recipient ok
DATA
Subject: relayé
354 Enter mail, end with "." on a line by itself
salut
.
250 2.0.0 o3E9eNLd002679 Message accepted for delivery
QUIT
221 2.0.0 stationY.domaine.local closing connection
Connection closed by foreign host.
```

3- Revenez à la configuration postfix par défaut pour interdire à nouveau le relais ou exécutez quelles commandes?

postconf -e "mynetworks_style = host"
service postfix restart

4- Nous voulons maintenant faire du relais sélectif. Quelle commandes permettent le relais depuis l'hôte stationY?

```
postconf -e "mynetworks = 192.168.1.Y,    127/8"
service postfix restart
```

Séquence 5 : Installation et configuration du MDA POP3/IMAP Dovecot

Configuration initiale – installation des paquetages nécessaires

[root@fed12 ~]# rpm -qa | grep dovecot

dovecot-1.2.6-4.fc12.i686

sinon vous faites :

yum install dovecot

1- Editez le fichier /etc/dovecot.conf, recherchez la ligne "protocols" et modifiez-la pour les protocoles POP3 et IMAP, redémarrez ensuite le service dovecot.

```
protocols = imap pop3
```

2- Envoyez un mail à votre utilisateur local. Connectez-vous ensuite au serveur POP par telnet sur le port 110 et utilisez les commandes du protocole POP pour vérifier l'arrivée du message et la lecture de son contenu.

```
telnet localhost 110

S: +OK localhost

Ok vous êtes connecté sur le pop de localhost
C: USER elies
S: +OK
C: PASS elies
S: +OK
On est logué sous le compte elies
C: STAT
S: +OK 5 405560
Il y a 5 messages en attente pour le compte elies@localhost pour un total de 405
560 octets.
C: LIST
S: +OK
S: 1 3499
S: 2 2205
S: 3 3528
S: 4 36612
S: 5 359716
S: .
On a donc cinq courriels numérotés de 1 à 5 avec leur taille respective.
C: TOP 2 10
Nous renvoie l'entête du courriel n°2 et les dix premières lignes.
C: RETR 2
Nous renvoie tous le courriel n°2 (entête et corps du message).
C: DELE 3
S: +OK
Marque le message numéro 3 pour l'effacer.
```

C: **DELE 6**
S: *-ERR*
Le serveur nous renvoie une erreur car il n'y a pas de message n°6.
C: **QUIT**