Administration Système UNIX
Travaux Pratiques

Installation

Installer **Ubuntu Server** dans une nouvelle machine virtuelle. Avant de lancer l'installation, configurez la carte réseau de votre machine virtuelle en mode pont (*bridge*).

Quelques impératifs seront à respecter. Il faut :

- Ne pas utiliser LVM (*Logical Volume Manager*).
- Ne pas chiffrer le répertoire personnel.
- N'installer que le minium (système de base, pas de paquets supplémentaires à part le serveur SSH).
- Ne pas faire les mises à jour pendant l'installation.

Lancez l'installation. Une fois celle-ci terminée :

– connectez-vous sur la machine virtuelle à l'aide du compte créé à l'installation.

– récupérez l'adresse IP de la machine virtuelle à l'aide de la commande suivante :
`ifconfig | grep addr:`

– connectez-vous à l'aide d'un outil SSH (commande `ssh`, Putty, ...) à cette adresse IP.

– vérifiez dans les fichiers de *logs* d'installation si tout c'est bien passé.

Gestion des logiciels

Avec la commande **dpkg** :

– Combien de packages sont installés sur votre système ?

– Est-ce que le package `xpdf` est installé ? `bash` ?

– Affichez toutes les informations du package installé `cron` (informations, fichiers, dépendances, ...)

Avec le système **APT** :

– Trouvez les packages correspondant à des logiciels ayant un rapport avec le JDK de Java

– Installer la dernière version d'OpenJDK

– Mettez à jour le catalogue des *packages* puis mettez à jour votre système.

Démarrage du système

– Arrêtez, testez puis redémarrez le service réseau.

– Trouvez le niveau (*runlevel*) courant.

– Utilisez la commande **`shutdown`** pour arrêter le système dans 2 minutes tout en affichant un message d'avertissement aux utilisateurs connectés.

La sécurité du système

– Ajoutez un groupe "**mesusers**" (en ligne de commande).

– Ajoutez à ce groupe deux utilisateurs "**user1**" et "**user2**" et fixez deux mots de passe différents pour ces utilisateurs (en ligne de commande). L'utilisateur user1 doit avoir par défaut le *shell* **`bash`** et l'utilisateur user2 le shell **`csh`**.

– Les mots de passe identiques donnent-ils les mêmes résultats cryptés ?

– Essayez d'ouvrir une session avec chacun de ces utilisateurs.

– Bloquez le compte le l'utilisateur **user2** (en ligne de commande). Testez. Qu'est ce qui a changé dans le fichier **`/etc/shadow`** ?

– Forcez l'utilisateur **user1** à changer son mot de passe à la prochaine ouverture de session (en ligne de commande).

– Supprimez l'utilisateur **user2** et son espace personnel.

– Connectez-vous en temps que **root** (vous devez lui donner un mot de passe avant avec la commande **`sudo passwd root`**). A l'aide de la commande **`id`**, listez tous les groupes auxquels appartient le super utilisateur.

– Connectez-vous en temps que **user1** et endossez l'identité de **root** à l'aide de la commande **`su`**.

– Utilisez les commandes **`id`**, **`whoami`** et **`who am i`**. Que constatez-vous ?

– Connectez-vous par **`ssh`** en tant que **user1** sur la machine de votre voisin et afficher l'historique des connexions.

Les fichiers d'initialisation

– Modifiez les fichiers d'initialisation de l'utilisateur **user1** : le fichier d'initialisation de *login* doit afficher le message "**login**" et celui de lancement doit afficher le message "**lancement**". Effectuez plusieurs connexions puis en exécutez un *shell* manuellement. Que constatez-vous ?

– Effectuez ces modifications dans les fichiers correspondants dans **`/etc/skel`**. Créez un utilisateur **user3** (dans le même groupe que les deux autres), puis connectez-vous avec cet utilisateur pour valider votre modification.

Les permissions étendues

– Endossez l'identité du super utilisateur et vérifiez la valeur de **`umask`**.

– Trouvez à quel endroit cette valeur par défaut est définie.

– Créez un répertoire **`/home/public`** dans lequel tous les utilisateurs pourront créer des fichiers mais ne pourront pas effacer les fichiers des autres. Testez avec les utilisateurs **user1** et **user3**.

– Quelles seraient les conséquences si la commande **`/bin/cat`** possédait le bit **SETUID** ?

– Installez le paquet **acl**, créez un répertoire nommé **`/home/projet`** puis modifiez les droits pour que seuls aient l'accès :

– L'utilisateur **user1** en lecture et écriture

– L'utilisateur **user3** en lecture seule

Contrôle des processus

– Trouvez le numéro de processus (**PID**) *shell* que vous êtes en train d'utiliser.

– Trouvez le numéro de processus père (**PPID**) de ce *shell*. Puis recommencez de proche en proche pour remonter la hiérarchie des processus. Quel est le processus le plus haut de la hiérarchie ?

– Ouvrez une deuxième session, et fermez-la en utilisant la commande **`kill`** sur le processus *shell* (**`bash`**) correspondant à cette session, à partir du premier shell.

– Ouvrez plusieurs sessions et tentez de toutes les fermer en une seule commande.

– Installez le paquet **mailutils**.

– Faites en sorte que soit envoyé par *mail* à votre utilisateur le message « **A la bouffe !** », à 12h10. Vérifiez que vous avez bien programmé l'affichage du message. Utilisez la commande **`mail`** pour cela. Voici un exemple d'utilisation de cette commande :

```
echo " le message " | mail -s " le sujet " utilisateur
```

– Faites en sorte que soit envoyé par mail à votre utilisateur le message « **La pause s'impose** » du lundi au vendredi à 10h30 et 15h00, seulement pendant les mois de janvier et février. Vérifiez que vous avez bien programmé l'affichage du message.

Configuration et partitionnement des disques

– Trouvez le modèle, la taille et le nom (nom logique, tel que désigné sous Linux) du disque de *boot* de votre machine.

– Quel est le nom logique de la partition de *swap* ? A quelle adresse commence-t-elle ? Quelle est sa taille ?

– Quel est le type de la partition **`sda1`** ? Quel est son système de fichiers ?

– Réfléchissez à la question suivante : supprimer une partition de la table des partitions (à l'aide d'un outil comme **`fdisk`**) supprime-t-il les données ?

– Ajoutez trois partitions sur un disque supplémentaire : une de 100 Mo, une de 500 Mo puis une de 50Mo. La première sera utilisée comme partition **FAT32**, les deux autres comme partition **Linux** (ne vous occupez pas du système de fichiers, juste des partitions).

– Redémarrez puis vérifiez que vos partitions ont bien été créées.

– Supprimez la dernière partition, celle de 50Mo.

Les systèmes de fichiers

– Créez un nouveau système de fichiers ***ext2*** sur la partition de 500Mo que vous avez créé précédemment, puis un système de fichiers **FAT32** sur la partition de 100Mo.

– Montez la partition manuellement, copiez-y des fichiers, puis démontez les.

– Faites en sorte que les nouvelles partitions soient montées automatiquement au démarrage. Vérifiez que vos modifications fonctionnent avant de redémarrer. Après le redémarrage, vérifiez que les partitions sont bien montées.

Surveillance et audits du système

– Utilisez la commande **`tail`** pour surveiller en temps réel le journal des connexions.

– Consultez le journal du service **`ssh`** puis celui des erreurs.

– Récupérez les dates et heures des 5 derniers *reboots* de votre machine.

Swap et autres systèmes de fichiers

– Vérifiez l'utilisation de la *swap*.

– Ajoutez une zone de *swap* de 50 Mo à l'aide d'une partition supplémentaire (cette zone de swap doit être disponible à chaque démarrage).

– Ajoutez une zone de *swap* de 50 Mo à l'aide d'un fichier placé dans le répertoire `/` (cette zone de *swap* doit être disponible à chaque démarrage).

– Ajoutez un *ramdisk* d'au maximum 100 Mo (ce *ramdisk* doit être disponible à chaque démarrage).

L'environnement réseau

– Passez la configuration réseau de votre machine de **DHCP** en configuration **statique** (ceci inclut TOUTE la configuration réseau). Pour cela, n'oubliez pas de récupérer toutes les informations de configuration réseau avant toute modification.

Raspberry Pi

– Installez une distribution ***Raspbian*** sur votre Raspberry Pi. Réalisez une installation *headless*.

– Identifiez la version de la distribution installée, les caractéristiques du processeur, la quantité de mémoire et la taille du swap, les partitions et systèmes de fichiers installés.

– Terminer la configuration de votre système en utilisant **`raspi-config`**.

– Mettez à jour le catalogue des *packages* puis mettez à jour votre système.

– Testez les E/S du **GPIO** en commandant une Led.

– Listez les services actifs de votre système avec **`systemctl`**.

– Journalisez le message « **Système ok** » et vérifiez sa présence dans le *log*.

– Créez un service de surveillance de la température du processeur avec une visualisation par Led et une journalisation des dépassements des seuils.

– Prenez le contrôle à distance de votre Raspberry Pi via **VNC**.

– Installez le package **sshfs**, puis montez en **sshfs** le répertoire distant **`/home/pi`**. Testez le montage en écrivant un fichier dans le répertoire monté. Terminez en démontant le répertoire.

Vous travaillerez maintenant avec deux machines : votre machine virtuelle et la Raspberry Pi.

Services réseau

– Installez et configurez un serveur **DNS** sur la machine « serveur ». Ce serveur DNS doit avoir, dans sa base de données, uniquement les noms et adresses IP des deux machines « serveur » et « client ». Choisissez un nom de domaine qui vous soit unique. La résolution doit marcher dans les deux sens (nom -> adresse et adresse -> nom) depuis le « serveur » et le « client ».

– Installez et configurez un serveur **DHCP** sur la machine « serveur ». Ce serveur DHCP doit permettre la configuration automatique de la machine « client » (et uniquement celle-ci). Choisissez une adresse de réseau qui vous soit unique. Modifiez la configuration réseau de la machine « client » pour tester.

– Créez un utilisateur « **user1** » sur les machines « client » et « serveur » (avec le même UID, mes des mots de passe différents). Vous donnerez à cet utilisateur le répertoire **`/home/user1`** comme répertoire personnel. Testez sur les deux machines en ouvrant une session avec cet utilisateur.

– Sur la machine « client », supprimez le répertoire **`/home/user1`**. Sur la machine « serveur », partagez sur le réseau à l'aide de NFS le répertoire **`/home`**. Configurez la machine « client » pour que ce partage réseau soit monté sur **`/home`** au démarrage et que l'on puisse ouvrir une session avec **user1** sur les deux machines, avec le même répertoire physique.

Samba

– Installez et configurez **Samba** en temps que serveur de fichiers.

– Créez sur le serveur un groupe nommé **partage** auquel appartiennent les utilisateurs **toto1** et **toto2**. Ne leur donnez pas de mot de passe ils ne pourront accéder au système que par Samba. Les utilisateurs **toto1** et **toto2** doivent pouvoir accéder à leur répertoire personnel par Samba.

– Créez sur le serveur les espaces supplémentaires **`/mnt/apps`**, **`/mnt/partage`** et **`/mnt/public`**. Le premier est en lecture uniquement, les deuxième et troisième en lecture/écriture.

– Définissez les propriétés et les permissions du répertoire **`/mnt/partage`** de telle manière que les personnes dans le groupe partage 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 et qu'un utilisateur ne puisse pas supprimer le fichier d'un autre.

– Créez les partages Samba pour les deux répertoires **`/mnt/apps`** et **`/mnt/partage`**. Seuls les membres du groupe **partage** devraient avoir accès à ces partages. En outre, assurez-vous que les fichiers placés dans le partage **[partage]** soient créés avec les permissions **0660**.

– Créez le partage Samba pour le répertoire **`/mnt/public`** dans lequel on pourra accéder en anonyme (sans mot de passe).

– Tester avec des machines clientes.

Serveur Web

– Installez un serveur web **Apache**. Créez un page d’accueil et testez à partir d’une machine cliente.

Serveur FTP

– Installez le serveur FTP **`vsftpd`**. Configurez le serveur afin de permettre aux utilisateurs authentifiés de télécharger des fichiers dans le répertoire **`/var/vsftp`**. Testez à partir d’une machine cliente (commande **`ftp`** ou FileZilla).

Mode Kiosque

– Configurer votre Raspberry Pi en mode kiosque afin de démarrer automatiquement un navigateur web vers une page d’accueil ou le site web de l’Esimed.

LDAP

– Sur la machine « client », supprimez l'utilisateur **user1**.

– Installez et configurez le service **LDAP** sur la machine « serveur ». Utilisez votre nom de domaine DNS comme nom de domaine LDAP. Configurez les deux machines en tant que client de ce service LDAP. Vous devez pouvoir ouvrir une session avec l'utilisateur **user1** depuis les deux machines (le serveur doit donc aussi être un client LDAP).