Correction

Project overview

Qu'est ce qu'une VM ?

Une machine virtuelle ou VM (Virtual Machine) est un environnement entièrement virtualisé qui fonctionne sur une machine physique. Elle exécute son propre système d'exploitation (OS) et bénéficie des mêmes équipements qu'une machine physique : CPU, RAM, disque dur et carte réseau. Plusieurs machines virtuelles avec des OS différents peuvent coexister sur le même serveur physique.

Comment fonctionne la VM ?

Le partage des différents environnements virtuels est géré par l'hyperviseur. Il effectue le partitionnement des ressources et alloue une partition à chaque VM. Cela s'effectue à l'aide d'un logiciel installé sur la machine physique.

Quel est les buts/avantages de la VM ?

Il y a plusieurs intérêts à utiliser une machine virtuelle :

- Tester un nouveau système d’exploitation sans avoir besoin de partitionner son disque dur.Le test peut ainsi s’effectuer sans risques d’endommager le disque dur de votre machine.
- Développer un logiciel ou un programme pour un autre système d’exploitation.
- Se servir de logiciels qui ne peuvent pas tourner sur le système d’exploitation de votre machine physique. Vous pouvez ainsi disposer d’une machine virtuelle par système d’exploitation et même de plusieurs versions du même système d’exploitation.
- Réaliser des économies en installant plusieurs machines virtuelles sur un seul support physique plutôt que de multiplier les ordinateurs en service.

Pourquoi choisir Debian plutôt que CentOs ?

Debian est plus approprié pour les débutants et accompagne mieux lors de l'installation et de la configuration de la machine virtuelle.

Quelles est la différence fondamentale entre CentOs et Debian ?

CentOs et Debian sont tous les deux des systèmes d'exploitation Linux. La différence principale est que Debian est destiné aux utilisateurs qui recherchent une distribution stable offrant la meilleure prise en charge logicielle et matérielle tandis que CentOs est destiné aux administrateurs débutants qui souhaitent expérimenter la version communautaire de RHEL de RedHat

CentOs

- Plus stable et est soutenu par une plus grande communauté
- Ne supporte pas beaucoup d'architecture
- Il est difficile de mettre à niveau une version de CentOs localement
- Il n'a pas d'interface graphique facile

Debian

- Moins de préférence sur le marché
- A plus de packages
- La mise à niveau d'une version stable à une autre est facile
- Contient une interface et des applications conviviales pour le bureau

Quelle est la différence entre aptitude et apt ?

Apt et aptitude sont des interfaces de gestion des paquets en ligne qui gèrent l'installation, la mise à jour et la suppression de logiciels. Aptitude est une version améliorée de apt et gère beaucoup mieux les dépendances des packages. Il comprend plus d'options que apt et dispose d'une interface console. De plus, il installe les dépendances suggérées alors que apt n'installe que celles recommandées.

Qu'est ce qu'est AppArmor ?

AppArmor (Application Armor) est un logiciel de sécurité permettant à l'administrateur système d'associer à chaque programme un profil de sécurité qui restreint les accès au système d'exploitation.

Simple setup

```
Connect with mleam

sudo ufw status
sudo service ssh status
head -n 2 /etc/os-release
```

User

```
getent group sudo
getent group user42
sudo adduser pseudo
```

Comment la politique des mots de passe a été mise en place ?

Pour mettre en place la politique des mots de passe fort, il a fallu modifier certaines règles déjà établies dans /etc/login.defs :

- La date d'expiration est passée de 99999 à 30 jours.
- La date minimum avant de pouvoir modifier le mot de passe est passée de 0 à 2 jours
- Le message d'avertissement avant l'expiration du mot de passe est resté à 7 jours

Il a fallu en plus installer le paquet libpam-pwquality permettant de configurer la résistance du mot de passe (nombre d'essai maxium, nombre de caractères minimum, interdiction d'utiliser le nom d'utilisateur ...)

```
sudo groupadd evaluating
sudo adduser pseudo evaluating
getent group evaluating
```

Quels sont les avantages de cette politique de mot de passe ? Quels sont les avantages et les inconvénients de sa mise en oeuvre ?

La politique des mots de passe fort permet d'améliorer la sécurité et de protéger les informations lors d'attaques informatiques.

Hostname and partitions

```
cat /etc/hostname
sudo vim /etc/hostname
sudo reboot
sudo vim /etc/hostname
sudo reboot
lsblk
```

Comment fonctionne LVM et de quoi il s'agit ?

La gestion par volumes logiques (Logical Volume Management ou LVM) est à la fois une méthode et un logiciel de gestion de l'utilisation des espaces de stockage d'un ordinateur. Il permet de gérer, sécuriser et optimiser de manière souple les espaces de stockage en ligne dans les systèmes d'exploitation de type UNIX. Il permet par exemple de diminuer la taille d'un système de fichier pour pouvoir en agrandir un autre, sans se préoccuper de leur emplacement sur le disque.

Sudo

```
dpkg -l | grep sudo
sudo adduser pseudo sudo
getent group sudo
```

Expliquer l'intérêt et le fonctionnement de sudo à l'aide d'exemple au choix

Sudo (abréviation de substitute user do, super user do ou switch user do) est une commande qui permet à un administrateur système d'accorder à certains utilisateurs (ou groupes d'utilisateurs) la possibilité de lancer une commande en tant qu'administrateur, ou en tant qu'autre utilisateur, tout en conservant une trace des commandes saisies et des arguments.

Exemple : Un employé souhaite rentrer dans un bureau dont il n'a pas l'accès. Il demande à son responsable les clés pour y accéder provisoirement.

```
su -
cd /var/log/sudo
ls
cat log_file
sudo touch pouet
cat log_file
exit
```

UFW

```
dpkg -l | grep ufw
sudo ufw status
```

Qu'est ce qu'UFW et à quoi sert-il ?

Un pare-feu est un logiciel et/ou matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données. UFW (Uncomplicated Firewall) est donc une interface vers iptables permettant de simplifier le processus de configuration d'un pare-feu.

```
sudo ufw allow 8080
sudo ufw status
```

```
sudo ufw delete allow 8080
```

SSH

```
dpkg -l | grep ssh
sudo service ssh status
```

Qu'est ce que SSH et a quoi sert-il ?

SSH (Secure Shell) est un terminal qui va permettre de dialoguer avec une machine ou un serveur via l'exécution de différentes commandes qui retourneront des informations. On peut grâce au SSH établir une connection sécurisée entre l'ordinateur et le serveur sur lequel se trouve le site web. Les webmasters peuvent ainsi accéder par Shell au serveur web et y exécuter des commandes. Le transfert des données utilisateurs mais aussi des données est chiffrées.

Il sert à :

- établir une connection sécurisée au serveur web et transférer de façon sécurisé des fichiers
- éditer des fichiers directement sur le serveur web
- sauvegarder des données
- mettre en place des droits de fichiers

```
Ouvrir un terminal
ssh -p 4242 pseudo@127.0.0.1
exit
ssh -p 4242 root@127.0.0.1
```

Script monitoring

```
sudo vim /usr/local/bin/monitoring.sh
```

Comment le script marche ?

Le script va d'abord récupérer les commandes pour les différents arguments avant de les afficher et les envoyer aux différents utilisateurs grâce à la commande wall.

Les différentes commandes :

- uname : affiche les informations système sur la machine sur laquelle elle est exécutée
- grep : cherche la chaîne de caractères choisie à l'intérieur des fichiers ou des répertoires spécifiés et affiche les lignes correspondantes
- sort : permet de trier des fichiers ou leurs contenus
- uniq : affiche les lignes d'un fichier texte en supprimant les multiples occurrences consécutives d'une même ligne
- wc : permet d'obtenir plusieurs informations au sujet de l'entrée standard ou d'une liste de fichiers | wc -l affiche le nombre de ligne
- free : permet d'afficher des informations de disponibilité sur la mémoire vive du système
- awk : permet une recherche de chaîne et l'exécution d'action sur les lignes sélectionnées. Elle est utile pour récuperer de l'information, générer des rapports, transformer des données entre autres.
- df : permet d'afficher la valeur d'espace disque disponible des systèmes de fichier dont l'utilisateur possède l'accès en lecture
- top : permet d'afficher en temps réel la liste des processus et les ressources utilisées. (= gestionnaire des tâches)
- who : permet d'afficher des informations concernant des utilisateurs qui sont connectés

- netstat : permet d'afficher des informations sur les connections réseau, les tables de routage et un certain nombre de statistiques dont ceux des interfaces, sans oublier les connexions masquées, les membres multicast, et enfin, les messages netlink
- hostname : permet de définir ou d'afficher le nom du système hôte en cours
- ip a : permet d'obtenir des informations sur les interfaces réseaux
- echo : permet d'afficher une chaine de caractères passée en paramètre sur le terminal
- wall : abréviation de write to all qui permet d'afficher un message à tous les utilisateurs connectés

Qu'est ce que cron ?

Cron est un programme qui permet aux utilisateurs des systèmes Unix d'exécuter automatiquement des scripts, des commandes ou des logiciels à une date et une heure spécifiée à l'avance ou selon un cycle défini à l'avance.

Comment a été configuré le script pour qu'il s'exécute toutes les 10 minutes à partir du démarrage du serveur ?

```
* * * * * USER_NAME COMMAND / SCRIPT-TO-EXECUTE

| | | | |
| | | | |
| | | | | _________  Jour de la semaine (0 - 6) (0 est dimanche, ou utilisez des noms)
| | | |_____________  Mois (1 - 12), * signifie chaque mois
| | |_______________  Jour du mois (1 - 31), * signifie tous les jours
| |_________________  Heure (0-23), * signifie toutes les heures
|___________________ Minute (0 - 59), * signifie chaque minute
```

```
su -
crontab -e
Modifier */10 par */1
```

```
crontab -e
Ajouter '#' devant la ligne
reboot
ls- l /usr/local/bin/monitoring
```