TABLES DES MATIERES

C’est quoi une machine virtuelle?

Une machine virtuelle ou VM est un **environnement entièrement virtualisé qui fonctionne sur une machine physique.** Elle **exécute son propre système d’exploitation (OS)** et bénéficie des mêmes équipement qu’une machine physique : CPU, mémoire RAM, disque dur et carte réseau.

L'**hyperviseur** est le logiciel qui permet de séparer les ressources de la machine du matériel et de les approvisionner de manière adéquate pour que la machine virtuelle puisse les utiliser.

Les **machines physiques** sont appelées hôtes (**host**). Les **machines virtuelles** qui utilisent les ressources sont des machines invitées (**guest**).

Les machines virtuelles permettent d'exécuter simultanément plusieurs systèmes d'exploitation sur un seul ordinateur, comme une distribution Linux® sur un ordinateur portable sous MacOS.

Chacun des systèmes d'exploitation s'exécute sur le matériel hôte comme le ferait n'importe quel autre système d'exploitation ou application. **L'expérience de l'utilisateur final émulée au sein de la machine virtuelle est donc quasiment identique à celle offerte par un système d'exploitation exécuté en temps réel sur une machine physique.**

Une machine virtuelle fournit un environnement isolé du reste du système, donc il ne peut y avoir aucune interférence entre les programmes exécutés au sein d'une machine virtuelle et sur le matériel hôte.

Avantages

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.

Désavantages

Toutefois, l’installation d’une machine virtuelle comporte aussi des inconvénients. Notamment au niveau de la sécurité.

- Une machine physique embarquant plusieurs machines virtuelles est **plus vulnérable aux attaques** qu'un ordinateur ne disposant que d'un seul système d'exploitation.
- De la même façon, si cette machine physique vient à tomber en panne, l'accès aux VM devient impossible.
- Enfin, l'ordinateur hôte des machines virtuelles doit être assez puissant pour supporter la virtualisation. Temps de latence et lenteurs sont fréquents si la RAM est trop réduite.

Système d'exploitation OS

Un système d'exploitation se dit Operating System en anglais, que l'on abrège en « OS ».
Voyez-le comme un "super logiciel" qui fait l'interface entre vous et votre ordinateur, pour vous permettre de l'utiliser en gérant ses ressources : processeur, carte graphique, espace de stockage, mémoire vive, etc. On dit qu'**il "exploite" les ressources physiques de l'ordinateur**, d'où son nom : "système d'exploitation".

C'est quoi une distribution?

Comme Linux est un source code ouvert à tout le monde, des communautés ont commencé à se former afin d'adapter le système d'exploitation à des besoins/objectifs spécifiques.

Ces besoins/objectifs spécifiques sont entre-autres:

- Produire des documents;
- Écrire des programmes et créer des logiciels;
- Éditer des images, vidéos, audio;
- Stocker de l'information sensible en sécurisant le système d'opération;
- Surfer le net.

Comme les besoins et les objectifs de chaque communauté étaient différents, ces communautés ont commencé à distribuer des images build de ce système d'exploitation avec tous les outils essentiels installés. Ces images prédéfinies sont appelées `distributions` !

Debian vs. CentOS - différences

	Debian	CentOS
	est une distribution GNU/Linux	est une distribution GNU/Linux
Première version	1993 - Debian est une des plus anciennes et des plus grandes distributions avec une des plus grande communautés.	2002
Type d'organisation	communauté	communauté avec le support de RedHat Enterprise Linux
Niveau	Convient mieux pour des utilisateurs intermédiaires	Pour les utilisateurs à niveau intermédiaire à **avancé**
Basé sur	Le système d'exploitation est composé exclusivement de logiciels libres, développé par le Debian Project.	Tous les paquets sont des paquets compilés à partir des source de la distribution RHEL (Red Hat Enterprise Linux).
Pour quelle utilisation?	Utilisation générale	Utilisations pour les **entreprises** et **servers**
Support des logiciel	**Debian a la plus grande collection de logiciel avec plus de 59'000 paquets.**	
Stabilité	Très stable - Debian est connu pour sa stabilité.	Très stable

aptitude vs apt

apt	Aptitude
Apt ou *Advanced Packaging Tool* est un logiciel libre et à code source ouvert qui **gère** gracieusement l'**installation et la suppression du logiciel.**	Commande qui peut émuler la plupart des arguments de ligne de commande d'apt-get et faire des choses en plus.
Apt est une ligne de commande complète **sans interface graphique.**	Aptitude est un **outil de packaging avancé** qui **ajoute une interface utilisateur** à la fonctionnalité, permettant ainsi à l'utilisateur de rechercher un package de manière interactive, puis de l'installer ou de le supprimer. Il peut fonctionner en mode interface utilisateur interactive à base de texte et même en mode non interactif en ligne de commande.
Initialement créé pour Debain	Initialement créé pour Debain

C'est quoi AppArmor?

AppArmor (Application Armor) est un logiciel de sécurité pour Linux édité sous Licence publique générale GNU.

AppArmor fournit une sécurité de "**contrôle d'accès obligatoire**" (Mandatory Access Control ou MAC) - permet aux développeurs de restreindre les actions que peuvent prendre les processus.

Ce qui rend AppArmor différent des autres outils de sécurité, c'est qu'**il lie les attributs de contrôle d'accès aux programmes plutôt qu'aux utilisateurs individuels.**

Concrètement, le noyau interroge AppArmor avant chaque appel système pour savoir si le processus est autorisé à effectuer l'opération concernée. Ce mécanisme permet à AppArmor de **confiner des programmes à un ensemble restreint de ressources.**

Pour y parvenir, Apparmor installe un module dans le noyau Linux qui surveille l'utilisation des ressources des programmes en fonction de leurs profils.

Vérifier si AppArmor est installé:

```
sudo aa-status
```

C’est quoi un Shell script?

Shell script e un **fichier texte** qui contient une séquence de commandes pour les systèmes d’exploitation basée sur UNIX. Un Shell script est généralement créé pour des séquences de commandes qui doivent être utilisées d’une manière répétitive afin d’économiser du temps.

On l’appelle Shell script parce qu’il combine une séquence de commandes qui autrement devrait être saisie au clavier, une commande après l’autre.

Chaque ligne de commande est entrée avec le signe dollar `$`.

Votre script est un simple fichier texte, par défaut il s'ouvre donc avec l'éditeur de texte défini par défaut. Pour qu'il soit autorisé à se lancer en tant que programme depuis le terminal utilisez la commande `chmod`

```
chmod +x [nom_du_script]
```

Pour lancer le script il suffit de se placer dans le dossier où est le script, et de lancer :

```
bash [nom_du_script]
```

Ou si le fichier script a été rendu exécutable, vous pouvez exécuter le script avec la

```
./[nom_du_script]
```

`wall`

`wall` est une commande qui **affiche un message sur le terminal de tous les utilisateurs connectés**. `wall` est une abréviation de `write all`. Si vous voulez envoyer un message à un utilisateur spécifique, utilisez la commande `write`.

> Pour voir tous les utilisateurs connectés, appliquez la commande `w` ou `who`

Normalement les administrateurs de système envoient des messages pour annoncer la maintenance et demandent les utilisateur de se déconnecter et de fermer tous les programmes. **Le message est affichée à tous les utilisateurs connectés avec un terminal ouvert.** Les utilisateurs qui utilisent un environnement desktop graphique sans avoir un terminal ouvert ne vont pas voir le message.

Le syntaxe de la commande `wall` est:

```
wall [OPTIONS] [<FILE>|<MESSAGE>]
```

La manière la plus simple de diffuser un message est d'invoquer la commande `wall` avec le message comme argument:

```
$ wall "The system will be restarted in 10 minutes."
```

Le partitionnement du disque dur

En micro-informatique, une **partition** est une **partie d'un disque dur destinée à accueillir un système de fichiers.**

Le partitionnement du disque dur sert par exemple à installer des systèmes d'exploitation différents n'utilisant pas le même système de fichiers (avec une machine virtuelle on NE va PAS procéder au partitionnement du disque dur de la machine hôte!). Il y aura donc au minimum autant de partitions que de systèmes d'exploitation utilisant des systèmes de fichiers différents.

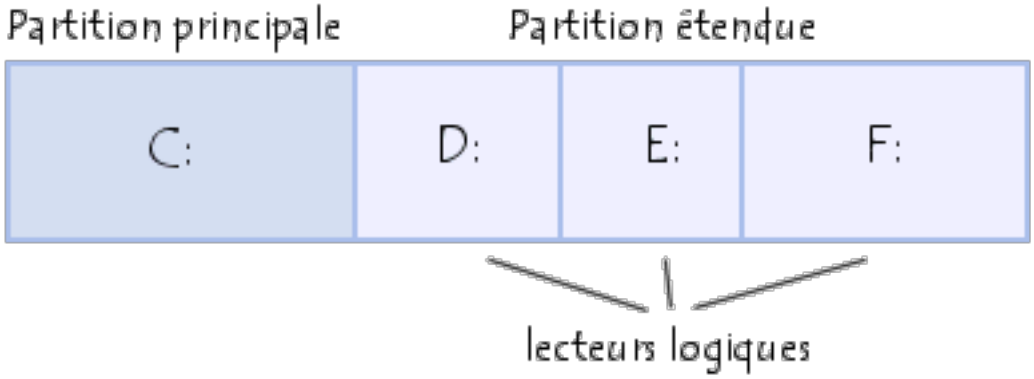
Dans le cas d'un utilisateur d'un système d'exploitation unique, une seule partition de la taille du disque peut suffire, sauf si l'utilisateur désire en créer plusieurs pour faire par exemple plusieurs lecteurs dont les données sont séparées.

Il y a trois sortes de partitions:

- **la partition principale/ primaire**
- **la partition étendue**
- **les lecteurs logiques**.

Dans la partition étendue l'utilisateur peut créer des **lecteurs logiques** (c'est-à-dire **"simuler" plusieurs disques durs de taille moindre**).

La partition étendue donne la possibilité de créer autant de lecteurs logiques que vous désirez dans celle-ci. **Au moins un lecteur logique est nécessaire dans une partition étendue, car vous ne pouvez pas y stocker de données directement.**



Beaucoup de machines sont formatées en une grande partition utilisant l'intégralité de l'espace disponible du lecteur. Ce n'est pourtant pas la solution la plus avantageuse en terme de performances et de capacité. La solution est de créer plusieurs partitions, ce qui va vous permettre :

- d'installer plusieurs systèmes d'exploitation sur votre disque;
- d'économiser de l'espace disque;
- d'augmenter la sécurité de vos fichiers (si le système de fichiers est corrompu, en général une seule partition est affectée);
- d'organiser vos données plus facilement.

Le seul inconvénient qu'il y a à utiliser plusieurs partitions est qu'il est souvent difficile de connaître ses besoins à l'avance. Si vous faites une partition trop petite, vous aurez soit à réinstaller le système soit à déplacer constamment des fichiers pour faire de la place sur la partition trop petite. D'un autre côté, si vous faites une partition trop grande, vous aurez perdu de l'espace.

Partitionnement pour Debian

On appelle **partitionnement** le **processus** qui consiste à écrire les secteurs qui constitueront la **table de partition** (qui contient les informations sur la partition: taille de celle-ci en terme de nombre de secteurs, position par rapport à la partition principale, types de partitions présentes, systèmes d'exploitation installés,…).

```
# lsblk
NAME                    MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
sda                       8:0    0  30.8G  0 disk
├─sda1                    8:1    0   500M  0 part  /boot
├─sda2                    8:2    0     1K  0 part
└─sda5                    8:5    0  30.3G  0 part
  └─sda5_crypt          254:0    0  30.3G  0 crypt
    ├─LVMGroup-root     254:1    0    10G  0 lvm   /
    ├─LVMGroup-swap     254:2    0   2.3G  0 lvm   [SWAP]
    ├─LVMGroup-home     254:3    0     5G  0 lvm   /home
    ├─LVMGroup-var      254:4    0     3G  0 lvm   /var
    ├─LVMGroup-srv      254:5    0     3G  0 lvm   /srv
    ├─LVMGroup-tmp      254:6    0     3G  0 lvm   /tmp
    └─LVMGroup-var--log 254:7    0     4G  0 lvm   /var/log
sr0                      11:0    1  1024M  0 rom
```

Lorsque la partition est créée, on lui donne un nom de volume qui va permettre de l'identifier facilement.

Pour les nouveaux utilisateurs, les machines Debian personnelles ou familiales, et autres systèmes mono-utilisateur, une simple partition / (plus celle d'échange) est sans doute la solution la plus simple. Le type de partition recommandé est ext4. *(partie obligatoire du projet)*

Pour les systèmes avec plusieurs utilisateurs, ou les systèmes avec beaucoup d'espace disque, il vaut mieux placer les répertoires /var, /tmp et /home chacun sur une partition distincte de la partition /. *(projet bonus)*

Le nom des disques et des partitions sous Linux peut être différent des autres systèmes d'exploitation. Vous devez connaître les noms utilisés lors de la création et du montage de partitions. Voici les principales conventions de nommage :

- Le **premier disque dur** détecté est appelé **/dev/sda**.
- Le **second disque dur** détecté est appelé **/dev/sdb**, etc.

Les **partitions sur chaque disque** sont représentées en ajoutant un numéro au nom du disque : **sda1** et **sda2** représentent la première et la seconde partition du premier disque SCSI du système.

Linux représente les partitions primaires par le nom du disque, suivi des **nombres 1 à 4**. Par exemple la première partition sur le premier disque est /dev/sda1.

Les partitions logiques sont numérotées à partir de 5. Donc, la première partition logique sur ce même disque est /dev/sda5. Rappelez-vous que la partition étendue, c'est-à-dire la partition primaire contenant les partitions logiques, n'est pas utilisable en elle-même.

SSH

SSH - serveur shell sécurisé (Secur SHell), qui permet de se connecter à une machine distante et d'y exécuter des commandes sur shell.

Les ordinateurs communiquent entre eux via des réseaux. Par conséquent, les chercheurs en réseau ont défini un ensemble de règles pour communiquer avec d'autres machines et ont commencé à développer des **protocoles qui permettent à un utilisateur de prendre le contrôle d'un autre ordinateur à distance.**

Les commandes que l'utilisateur pourrait exécuter consistent à exécuter des programmes, créer des répertoires, créer/supprimer/transférer des fichiers, démarrer/arrêter des services, etc.

Mais si les protocoles ne sont pas sécurisés, alors n'importe qui au milieu du réseau peut intercepter et lire les données transférées.

SSH est un protocole réseau sécurisé permettant d'accéder à des ordinateurs distants dans un réseau.

SSH utilise une **architecture client-serveur** pour une communication sécurisée sur le réseau en connectant un client ssh au serveur ssh.

Il utilise une technique de cryptographie à **clé publique pour s'authentifier entre le client et le serveur**. De plus, le protocole utilise algorithmes de **cryptage** et de hashing pour l'échange de messages entre le client et le serveur afin d'**assurer la confidentialité et l'intégrité des données.**

La plupart des sessions SSH (période pendant laquelle nous accédons au serveur distant) n'auront que les deux opérations suivantes :

- Authentification
- Exécution de la commande

Le serveur authentifie le client grâce à un mot de passe et une paire de clés SSH. Une fois que le serveur a authentifié le client avec succès, une connexion sécurisée est établie entre eux.

SSH crypte la session de connexion et empêche ainsi tout agresseur de recueillir des mots de passe non-cryptés.

Pour vous connecter à un serveur distant à l'aide de SSH, vous devez savoir au moins deux choses.

- hôte du serveur
- nom d'utilisateur

La syntaxe de la commande ssh de base est :

```
ssh [user-name]@[host]
ssh [user-name]@[host] -p [port-no]
```

La commande de la clé SSH indique à votre système que vous souhaitez ouvrir une connexion Secure Shell cryptée.

`[user-name]` est la machine distante que nous essayons de connecter (et non l'utilisateur sur votre machine locale).

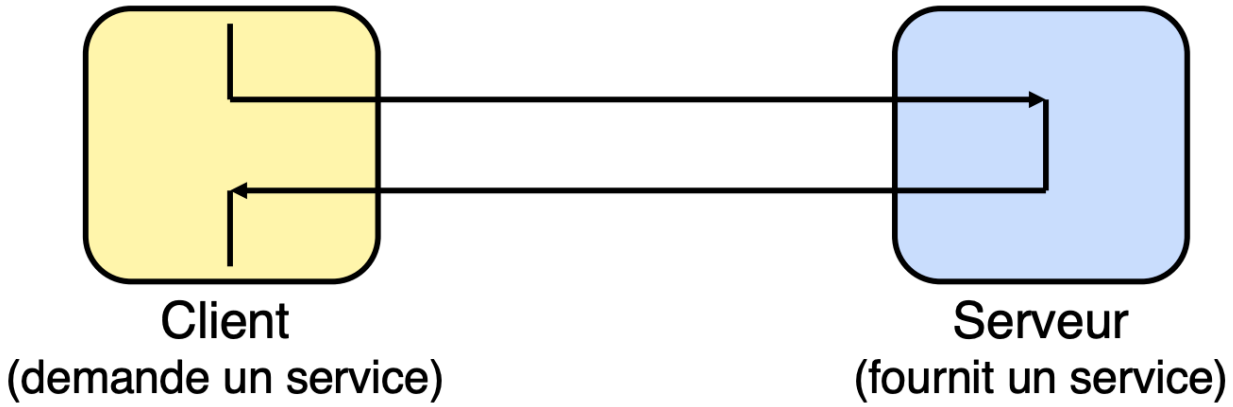
`[host]` fait référence à l'ordinateur auquel vous souhaitez accéder - soit une adresse IP, soit un nom de domaine.

L'option `-p [port-no]` est facultative. Elle permet de désigner un autre port de choix. Si rien n'est précisé, le port 22 sera utilisé par défaut, parce que **toutes les connexions SSH écoutent sur le port 22.**

Lorsque vous appuyez sur Enter, vous serez invité à entrer le mot de passe du compte demandé. Si votre mot de passe est correct, vous serez accueilli avec une fenêtre de terminal à distance.

Lorsque vous souhaitez mettre fin à la session ssh, tapez la commande `exit`.

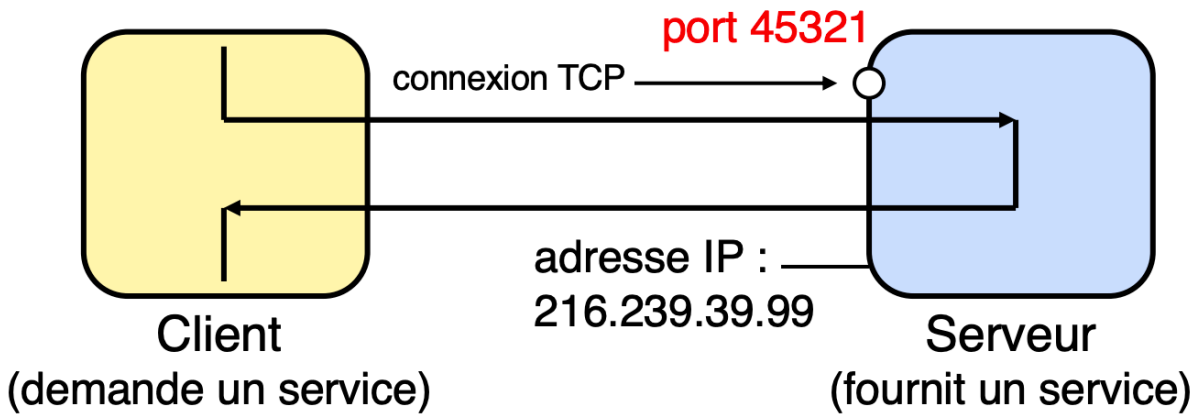
Les ports



Pour le client, un service est souvent désigné par un nom symbolique. Ce nom doit être converti en une adresse interprétable par les protocoles du réseau.

La conversion d'un nom symbolique (par ex. www.google.com) en une adresse IP (216.239.39.99) est à la charge du service DNS

En fait, l'adresse IP du serveur ne suffit pas, car **le serveur (machine physique) peut comporter différents services; il faut préciser le service demandé au moyen d'un numéro de port, qui permet d'atteindre un processus particulier sur la machine serveur.**



L'adresse IP sert à identifier de façon unique une machine sur le réseau tandis que le numéro de port indique le service auquel les données sont destinées.

Un numéro de port comprend 16 bits (0 à 65'535) et est associé à un protocole de transport donné

Le port est en quelque sorte une "porte" qui permet d'attribuer une information à un service du serveur.

UFW

UFW, ou *Uncomplicated Firewall*, est une **interface de gestion de pare-feu simplifiée** qui masque la complexité des technologies de filtrage de paquets. Si vous souhaitez commencer à sécuriser votre réseau, et vous n'êtes pas sûr de l'outil à utiliser, UFW peut être le bon choix pour vous.

C'est quoi un pare-feu?

Un pare-feu (ou coupe-feu, barrière de sécurité ou **firewall**), dans le contexte d'un réseau informatique, est un composant essentiel de la sécurité des réseaux informatiques. Son **but est de protéger un réseau informatique des intrusions indésirables en filtrant les communications autorisées entre deux réseaux informatiques** (généralement dans un contexte domestique : **votre réseau privé domestique et le réseau Internet**).

Le pare-feu pourrait être comparé à un agent de sécurité à l'aéroport. Pour entrer dans votre pays, un visiteur étranger doit passer par un poste-frontière et être contrôlé par un douanier qui, selon des instructions qu'il doit suivre, le laissera passer ou lui fera rebrousser chemin. Pareillement, un habitant de votre pays doit passer un contrôle avant de monter dans un avion vers une destination extérieure ; suite à son contrôle, le voyageur pourra continuer ou non sa route. Le pare-feu joue ce rôle, au niveau informatique : **il filtre les connexions qui arrivent dans votre ordinateur et celles qui sortent de votre ordinateur, et bloque celles qui sont indésirables selon ce que vous lui avez paramétré comme politique de sécurité.**

Un pare-feu se présente essentiellement sous deux formes :

- **Logicielle** : un programme qui fonctionne dans votre ordinateur personnel ou de bureau et assure le rôle de filtrage des connexions. Un pare-feu logiciel doit être installé dans chaque ordinateur ;
- **Matérielle** : un composant physique de votre réseau domestique qui inclut un logiciel de pare-feu. Un pare-feu matériel doit être présent une seule fois dans un réseau informatique – au passage entre un réseau privé et un réseau public.