A retenir

TP00 : Virtualisation des architectures et environnements de travail

A. Introduction à la virtualisation

La **virtualisation** est une technique permettant d'exécuter ***plusieurs systèmes d'exploitation (OS) et applications sur une seule machine physique***, créant des versions virtuelles de serveurs, réseaux, ou environnements de travail. Cette approche ***optimise les ressources, réduit les coûts matériels, et offre plus de flexibilité pour gérer des environnements de test ou de production***.

B. Avantages principaux :

- **Réduction des coûts matériels** : Une seule machine physique peut héberger plusieurs machines virtuelles.
- **Optimisation des ressources** : Allocation dynamique de CPU, mémoire et stockage.
- **Flexibilité** : Possibilité de créer, cloner, et restaurer des environnements sans impact sur l'infrastructure physique.
- **Isolation des environnements** : Les systèmes virtuels sont séparés les uns des autres, augmentant la sécurité.

C. Exemples de virtualisation

1. **Virtualisation de serveur** : Créer plusieurs serveurs virtuels sur une machine physique (Hyperviseurs comme VirtualBox, VMware, Hyper-V).
2. **Virtualisation de réseau** : Diviser un réseau physique en segments virtuels indépendants.
3. **Virtualisation de stockage** : Agréger et gérer plusieurs ressources de stockage comme s'il s'agissait d'un seul appareil.

D. Types de virtualisation (Hyperviseur)

Logiciel qui permet de gérer les machines virtuelles (VM). On distingue deux types :

1. **Type 1** : Installé directement sur le matériel, comme VMware ESXi ou Hyper-V.
2. **Type 2** : Fonctionne à l'intérieur d'un OS, comme VirtualBox.

E. Les principaux acteurs du marché

1. **Oracle VirtualBox** : Solution open-source, idéale pour créer et gérer des environnements virtuels pour le développement ou le test.
2. **VMware vSphere** : Suite professionnelle pour les entreprises permettant de gérer des infrastructures virtuelles.

3. **Microsoft Hyper-V** : Outil intégré aux systèmes Windows Server, utilisé dans les environnements d'entreprise.
4. **Recherche sur le fonctionnement de *Proxmox* et la configuration d'une machine virtuelle sous *Proxmox*** ??

F. Etape de création d'un environnement virtuel

1. **Installation de l'hyperviseur** : Téléchargez et installez VirtualBox ou VMware Workstation sur votre machine.
2. **Création de la VM** (Une simulation logicielle d'un ordinateur physique avec un système d'exploitation complet et des applications) :
    - La création consiste à configurer les ressources (CPU, RAM, Espace disque, périphériques, …)
        1. Définissez les paramètres de base (nom, OS, version).
        2. Configurez la mémoire, cpu et le stockage alloué à la VM.
        3. Démarrez la VM et installez le système d'exploitation de votre choix (ex. : Ubuntu, Windows).
    - Une fois la VM démarrée, installez vos applications et testez vos scénarios sans affecter votre machine physique.
    - Vous pouvez également cloner la VM pour créer un environnement identique.

G. Configuration réseau pour la virtualisation (NAT, Bridge, etc.)

1. NAT (Network Address Translation)

Avec **NAT**, les machines virtuelles utilisent l'adresse IP du réseau hôte pour accéder à Internet. Les VM partagent l'IP externe, ce qui les rend invisibles depuis l'extérieur. C'est simple à configurer et convient aux environnements de test où l'accès externe n'est pas nécessaire.

- **Avantage** : Isolation des VM par rapport au réseau externe.
- **Inconvénient** : Les services hébergés par les VM ne sont pas accessibles depuis le réseau externe sans configuration de port forwarding.

2. Bridge (Pont réseau)

Le mode **Bridge** permet aux machines virtuelles de se comporter comme des appareils physiques sur le réseau local. Chaque VM obtient sa propre adresse IP sur le réseau local, la rendant directement accessible aux autres machines.

- **Avantage** : Les VM peuvent interagir directement avec les autres appareils sur le réseau.

3. Réseau Privé

Ce mode crée un réseau isolé entre les VM sur le même hôte, sans connexion avec l'hôte ou l'extérieur comme s'il s'agit d'un VLAN.

- **Avantage** : Utile pour des environnements de développement ou des tests isolés.
- **Inconvénient** : Aucune connexion Internet ou au réseau hôte sans passerelle ou routeur virtuel.

4. **Host-only**

En mode **Host-only**, les machines virtuelles ne peuvent communiquer qu'avec l'hôte et les autres VM du réseau. Il n'y a pas d'accès Internet, mais elles peuvent échanger des données avec l'hôte.

- **Avantage** : Utile pour des environnements de développement locaux, où la sécurité est cruciale.
- **Inconvénient** : Pas de connexion au réseau externe.

5. **Récapitulatif des possibilités selon le mode choisi :**

Type de connexion	**Pont/Bridge**	**NAT**	**Host Only**	**Réseau privé**
VM vers hôte	OUI	OUI	OUI	OUI
VM vers LAN	OUI	NON	NON	NON
VM vers Internet	OUI	OUI	NON	NON
VM vers autre VM sur même hôte	OUI si les 2 en mode pont/bridge	OUI	NON	OUI si même réglage
VM vers autre VM sur autre machine	OUI si les 2 en mode pont/bridge	NON	NON	NON
VM vers autre machine du réseau	OUI	NON	NON	NON

H. Gestion des ressources

- **Snapshot** : Capture d'une image d'une VM à un instant précis, permettant de restaurer le système en cas de problème.
- **Migration** : Déplacement des VM entre différents serveurs physiques sans interruption.
- **Scalabilité** : Ajout de ressources (CPU, mémoire) à une VM sans redémarrage.

I. Sécurité et performances

a) **Isolation** : Les VM sont isolées les unes des autres, ce qui renforce la sécurité.

b) **Pare-feu virtuel** : Implémentation de règles de sécurité directement au niveau de la couche de virtualisation.

c) **Performance** : La virtualisation ajoute une légère surcharge, mais les avantages en matière de gestion et d'évolutivité compensent ce coût.