Cheatsheet : Virtualisation et Conteneurisation

1. Virtualisation

Définition

- Technique permettant d'exécuter plusieurs systèmes d'exploitation (OS) sur une même machine physique.
- Utilisation d'un hyperviseur pour gérer les machines virtuelles (VM).

Types de Virtualisation

1. **Virtualisation complète** : Chaque VM fonctionne indépendamment avec son propre OS.
2. **Paravirtualisation** : L'OS invité est modifié pour collaborer avec l'hyperviseur.
3. **Virtualisation au niveau du système d'exploitation** : Partage du noyau de l'OS hôte entre les conteneurs.

Hyperviseurs

- **Type 1 (bare-metal)** : Fonctionne directement sur le matériel physique.
    - Exemples : VMware ESXi, Proxmox, Microsoft Hyper-V, Xen
- **Type 2 (hosted)** : Fonctionne au-dessus d'un OS hôte.
    - Exemples : VMware Workstation, VirtualBox

Concepts avancés des Hyperviseurs

- **Load Balancing (Répartition de charge)** : Répartition automatique des charges de travail entre les hyperviseurs pour optimiser l'utilisation des ressources.
- **High Availability (HA - Haute Disponibilité)** : Configuration permettant le redémarrage automatique des VMs sur un autre hôte en cas de panne d'un hyperviseur.
- **Fault Tolerance (FT - Tolérance aux pannes)** : Technique qui duplique une VM sur un second hyperviseur pour assurer la continuité du service sans interruption.
- **Maintenance des hyperviseurs** : Utilisation de clusters d'hyperviseurs pour transférer les VMs en direct (live migration) avant maintenance.
- **Backup de VM** : Sauvegarde régulière des images des VMs via des solutions comme Veeam, snapshots VMware, ou Azure Backup.

2. Conteneurisation

Définition

- Exécution d'applications dans des environnements isolés partageant le même noyau.
- Léger, rapide et portable comparé aux VM.

Technologies

- **Docker** : Standard de facto pour la conteneurisation.
- **Podman** : Alternative à Docker sans daemon.
- **LXC (Linux Containers)** : Solution de conteneurisation bas niveau.
- **Kubernetes** : Orchestration de conteneurs à grande échelle.

Avantages des Conteneurs vs VMs

Critère	Conteneurs	Machines Virtuelles
Isolation	Modérée	Complète
Performance	Rapide	Plus lourd
Stockage	Léger	Nécessite un OS complet
Portabilité	Élevée	Moyenne

3. Types de solutions proposées par les Cloud Providers

IaaS (Infrastructure as a Service)

- Provisionnement de ressources virtuelles (VMs, stockage, réseaux).
- Exemples : AWS EC2, Google Compute Engine, Azure VMs.

PaaS (Platform as a Service)

- Environnements gérés pour le développement et le déploiement d'applications.
- Exemples : AWS Elastic Beanstalk, Google App Engine, Azure App Services.

CaaS (Containers as a Service)

- Services managés pour exécuter des conteneurs.
- Exemples : AWS Fargate, Google Kubernetes Engine, Azure Kubernetes Service.

SaaS (Software as a Service)

- Logiciels accessibles via le cloud sans gestion d’infrastructure.
- Exemples : Google Workspace, Microsoft 365, Dropbox.

4. Stockage

RAID (Redundant Array of Independent Disks)

- **RAID 0** : Répartition des données sans redondance (performance accrue, mais pas de tolérance aux pannes).
- **RAID 1** : Miroir des disques (tolérance aux pannes, mais capacité réduite).
- **RAID 5** : Parité distribuée (bonne tolérance aux pannes, nécessite au moins 3 disques).
- **RAID 10** : Association de RAID 1 et RAID 0 (performances et redondance accrues).

NAS (Network Attached Storage)

- **Accès Direct au Système de Fichiers** : Les utilisateurs et applications accèdent directement aux fichiers sur le NAS via des protocoles de partage de fichiers (comme NFS ou CIFS/SMB).
- Idéal pour le partage de fichiers entre plusieurs machines.
- Facile à gérer mais limité en performance pour des besoins critiques.

SAN (Storage Area Network)

- **Accès aux Blocs de Données** : Les serveurs accèdent aux données sous forme de blocs bruts via des protocoles de stockage bloc (comme SCSI sur Fibre Channel ou iSCSI).
- **Gestion des Métadonnées par le Serveur** : Le serveur doit gérer le système de fichiers et les métadonnées. Le SAN ne gère que le stockage des blocs de données.
- **Performances Élevées** : Idéal pour les applications nécessitant des performances élevées et une faible latence, car les opérations de lecture/écriture de blocs sont très rapides.
- Convient aux bases de données et aux applications critiques.

Object Storage

- **Objets** : Dans un Object Storage, les données sont stockées sous forme d'objets. Chaque objet est composé de trois parties principales :
    - **Données** : Le contenu réel de l'objet, comme un fichier ou un blob de données.
    - **Métadonnées** : Informations sur l'objet, telles que le type de contenu, la taille, et les permissions.
    - **Identifiant Unique** : Un identifiant unique qui permet d'accéder à l'objet, souvent sous la forme d'une URL ou d'une clé.
- Utilisé pour stocker des données massives comme des sauvegardes et des archives.
- Exemples : Amazon S3, Google Cloud Storage, Azure Blob Storage.

5. Réseau et Cloisonnement des VMs

Cloisonnement réseau des VMs

Lorsque plusieurs entreprises utilisent le même serveur physique (bare-metal), il est essentiel d'isoler les réseaux pour éviter toute fuite de données.

- **VLAN (Virtual Local Area Network)** : Segmente le réseau pour chaque entreprise en séparant les flux de données.
- **VXLAN (Virtual Extensible LAN)** : Étend le VLAN en permettant un cloisonnement sur un réseau distribué.
- **SDN (Software Defined Networking)** : Permet une gestion dynamique du réseau via des contrôleurs centralisés.
- **Firewall et ACLs** : Définition de règles strictes pour restreindre les communications entre VMs appartenant à différentes entreprises.
- **Micro-segmentation** : Contrôle du trafic au niveau des workloads individuels avec des outils comme VMware NSX ou Calico.

6. Outils et Technologies Cloud

Technologie	Description
Terraform	Infrastructure as Code (IaC)
Ansible	Automatisation de configuration
OpenStack	Cloud privé open-source
Kubernetes	Orchestration de conteneurs
Helm	Gestion de packages Kubernetes

7. Sécurité et Meilleures Pratiques

- **Sécuriser les hyperviseurs** : Accès restreint, mises à jour régulières.
- **Utiliser des images conteneurs sûres** : Scanner et éviter les images non vérifiées.
- **Gestion des permissions** : Limiter les accès aux VM et conteneurs.
- **Surveillance et logs** : Utiliser Prometheus, Grafana, ELK Stack pour la supervision.