

Administration et sécurisation des infrastructures virtualisées

5.1. Comprendre la virtualisation : concepts fondamentaux

La virtualisation consiste à **faire fonctionner plusieurs systèmes d'exploitation ou environnements applicatifs sur une même machine physique**, via un **hyperviseur**. Cela optimise l'utilisation des ressources, améliore la flexibilité, et permet une meilleure isolation.

Types de virtualisation :

- **Virtualisation de serveurs** : VM sur hyperviseur (VMware, Hyper-V, Proxmox)
- **Virtualisation de postes de travail** : VDI (Virtual Desktop Infrastructure)
- **Virtualisation du réseau** : VLAN, VXLAN, SDN
- **Virtualisation du stockage** : SAN, NAS, VSAN
- **Conteneurisation** : Docker, Podman

Modèles de déploiement :

- **On-premise** (infrastructure locale)
 - **Cloud privé/public/hybride**
 - **Modèles de services** : IaaS, PaaS, SaaS
-

5.2. Les hyperviseurs : rôle et administration

Types :

- **Type 1 (bare metal)** : VMware ESXi, Hyper-V Server
- **Type 2 (hébergé)** : VirtualBox, VMware Workstation (pour test)

Tâches administratives :

- Création de VM, affectation CPU/RAM
 - Gestion des snapshots, clones
 - Paramétrage des réseaux virtuels (vSwitch, bridges)
 - Surveillance des ressources hôtes
 - Application des correctifs (patching hyperviseur)
-

5.3. Gestion du stockage virtualisé

L'infrastructure virtualisée repose sur des dispositifs de stockage **hautement disponibles et scalables**.

Type	Description
SAN	Réseau de stockage en fibre ou iSCSI
NAS	Partages en réseau (SMB, NFS)
VSAN	Stockage distribué entre hyperviseurs
DAS	Disques locaux à un serveur (limité)

Outils :

- VMware vSAN
 - Windows Storage Spaces
 - FreeNAS, TrueNAS
 - Azure Disk Storage
-

5.4. Réseaux virtualisés et sécurité réseau

Concepts :

- Réseaux internes, bridgés, NAT
- Groupes de ports (VMware), vSwitch
- Tagging VLAN
- Contrôle du trafic est-ouest

Sécurité :

- Pare-feu virtuels (pfSense, NSX)
 - Micro-segmentation
 - IDS/IPS en VM
 - Bastions d'accès aux VM
 - Réplication réseau (HA)
-

5.5. Sauvegarde et restauration des environnements virtualisés

Outils de sauvegarde spécialisés :

- **VEEAM Backup & Replication**
- **Veritas NetBackup**
- **Nakivo Backup & Recovery**
- **Bacula / UrBackup** (Open Source)

Bonnes pratiques :

- Stratégie 3-2-1 : 3 copies, 2 supports, 1 distant

- Tests réguliers de restauration
 - Chiffrement des sauvegardes
 - Segmentation réseau du trafic de sauvegarde
-

5.6. Administration dans le cloud (AWS, Azure)

L'administrateur AIS doit également gérer des **ressources virtualisées dans le cloud** :

Plateforme	Services clés
AWS	EC2 (VM), VPC, IAM, EBS, CloudWatch
Azure	VM, NSG, Azure AD, Resource Groups

Compétences :

- Création et gestion de VM
 - Sécurisation des accès (firewall NSG, RBAC)
 - Monitoring (CloudWatch, Azure Monitor)
 - Sauvegardes (Snapshots, Vaults)
 - Automatisation (ARM, CloudFormation, Terraform)
-

5.7. Conteneurisation : Docker et Kubernetes

Conteneurs :

- Images légères, portables, isolées
- Infrastructure-as-code
- Déploiement rapide

Compétences clés :

- Docker : installation, images, volumes, réseaux
- Docker Compose : orchestration légère
- Kubernetes : orchestration avancée, scalabilité, redondance

Sécurité :

- Vérification d'intégrité des images
 - Moindre privilège (non-root containers)
 - Sécurisation des secrets (Vault, KMS)
-

5.8. Haute disponibilité et continuité de service

L'architecture virtualisée permet de mettre en œuvre des **solutions de résilience** :

Solution	Fonction
Cluster HA	Reprise automatique d'une VM sur autre hôte
vMotion / Live Migration	Déplacement à chaud sans coupure
Plan de reprise (PRI/PCI)	Relance des services critiques
Snapshots	Points de restauration rapides

5.9. Supervision et logs dans les environnements virtualisés

Outils :

- vSphere Monitor, Azure Monitor, AWS CloudTrail
- Prometheus, Grafana, ELK Stack
- Centralisation Syslog, journaux de conteneurs

Points de contrôle :

- Disponibilité des VM et hôtes
 - Consommation CPU/RAM/Disque
 - Réplication des machines critiques
 - Alertes de sécurité
-

5.10. Activités pratiques et évaluation

Projets :

- Installation d'un hyperviseur + création de VMs
- Mise en place d'un réseau virtuel isolé
- Déploiement d'une architecture Docker 3-tiers
- Sauvegarde + restauration d'une VM avec VEEAM
- Création d'une VM Azure + politique de sécurité NSG

Évaluations :

- **QCM** : typologie des hyperviseurs, architecture cloud
- **Étude de cas** : sécurisation d'une infrastructure virtuelle
- **Projet** : documentation complète d'une plateforme virtualisée sécurisée