ASTIOLAB

VIRTUALISATION ET SÉCURITÉ DES CONTENEURS

INTRODUCTION

PRÉSENTATION ET OBJECTIFS DU MODULE

OBJECTIFS DU MODULE

- Comprendre les concepts fondamentaux de la virtualisation et des technologies de conteneurisation.
- Identifier les différences entre machines virtuelles et conteneurs dans une perspective de sécurité.
- Apprendre à configurer et sécuriser des environnements virtualisés et conteneurisés.
- Identifier et évaluer les risques spécifiques aux conteneurs et aux images non sécurisées.
- Acquérir des compétences pratiques dans la gestion, l'investigation et le durcissement de conteneurs.

PLAN DU MODULE

- Introduction à la Virtualisation et à la Conteneurisation
- Introduction à l'orchestration et à l'écosystème Kubernetes
- Monitoring
- Risques et Défis de Sécurité
- Sécurisation des Environnements Virtualisés
- Sécurisation des Conteneurs
- Atelier Final : Audit et Durcissement d’un Environnement Compromis

MODALITÉS D'ÉVALUATION

- **QCM** réalisé au milieu de la formation et portant sur les trois premières parties.
- **L'atelier final** (pratique) sera évalué.
- **QCM** sur l'intégralité du cours lors des examens de fin de semestre.

INTRODUCTION À LA VIRTUALISATION ET À LA CONTENEURISATION

LIBÉREZ VOS APPLICATIONS, OPTIMISEZ VOS RESSOURCES

PLAN DU COURS

- Cours :
  - Concepts fondamentaux : hyperviseur, VM, conteneur, isolation.
  - Différences clés entre VM et conteneurs.
  - Panorama des technologies : VMware, VirtualBox, Docker, Podman, Kubernetes, …
- Pratique :
  - Premier pas avec la virtualisation / conteneurisation et comparaison

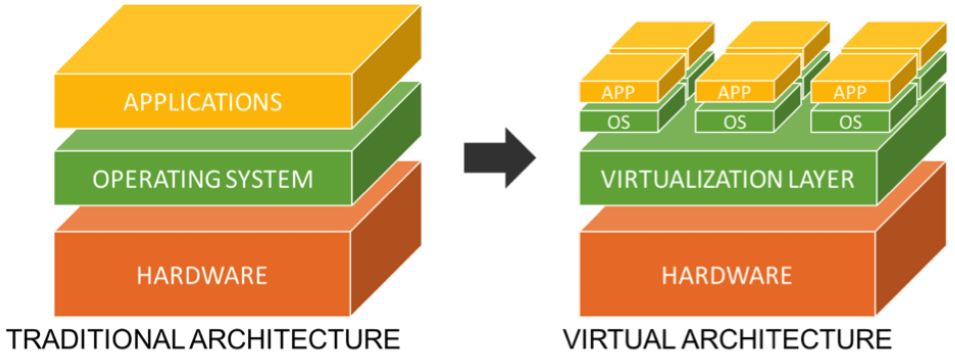
CONCEPTS FONDAMENTAUX

HYPERVISEUR, VM, CONTENEUR, ISOLATION

LA VIRTUALISATION, C'EST QUOI ?

- **Définition**

  Permet de créer une multitude de **machines virtuelles (VM)** sur un seul serveur physique. Chaque VM fonctionne comme un ordinateur indépendant, avec son propre système d'exploitation (OS), ses applications et ses ressources (CPU, RAM, stockage).



LA VIRTUALISATION, C'EST QUOI ?

- **Objectifs principaux**
  - **Optimiser l'utilisation des ressources** (CPU, RAM, stockage).
  - **Isoler** des environnements pour plus de sécurité et de flexibilité.
  - **Simplifier** la gestion et le déploiement d'infrastructures IT.
  - **Réduire les coûts** d'infrastructure et de maintenance.

- **Exemple concret**

  Au lieu d'avoir 10 serveurs physiques sous-utilisés, on peut les regrouper en 1 ou 2 serveurs physiques hébergeant 10 machines virtuelles (VM), chacune avec son propre OS et ses applications.

UN HYPERVISEUR, C'EST QUOI ?

Un hyperviseur pour les contrôler tous !

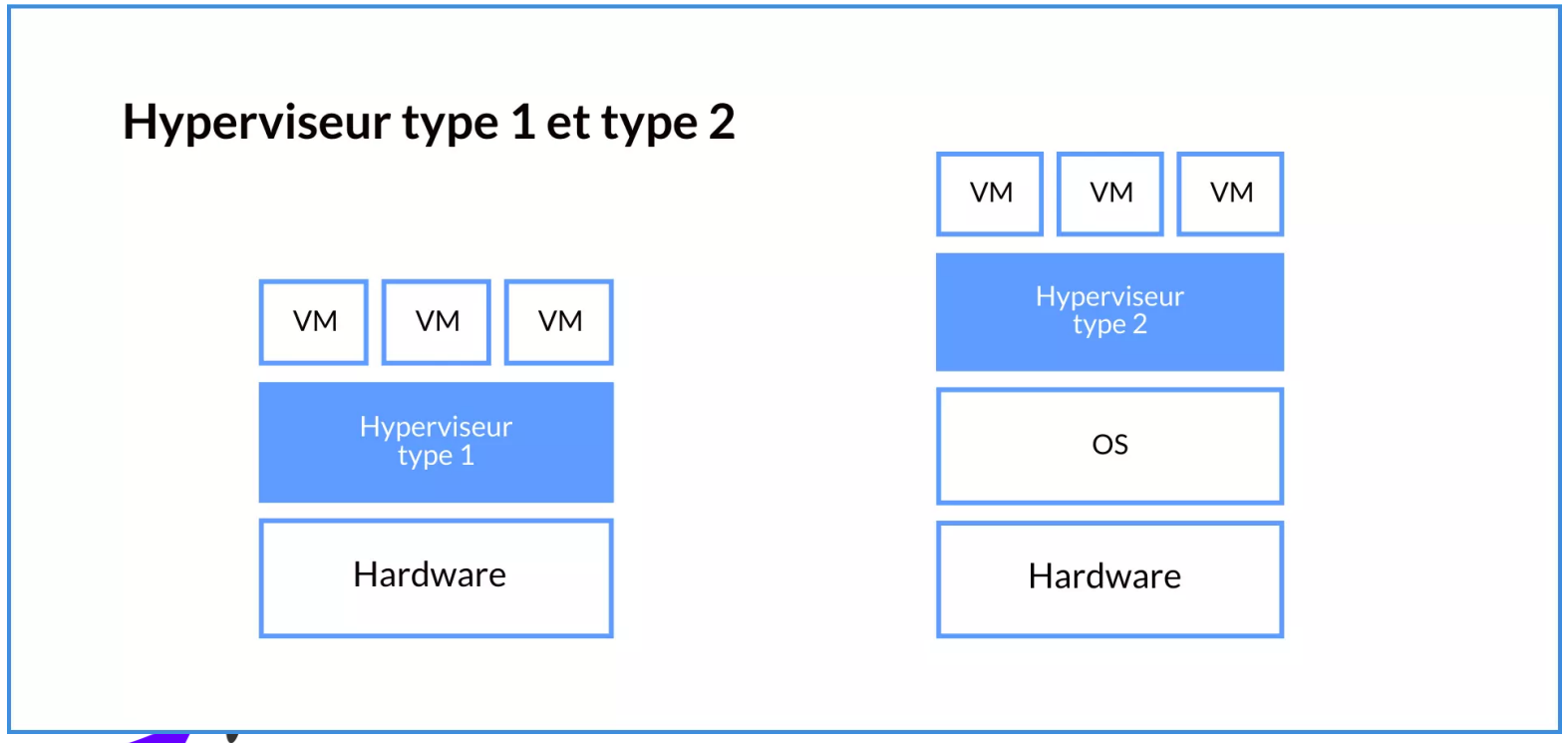
- Cœur de la virtualisation, c'est le moniteur de machine virtuelle.
- Permet de gérer nos machines virtuelles

- Deux types d'hyperviseurs :

  - **Type 1 : Bare-metal :** S'installe directement sur le matériel physique, sans système d'exploitation intermédiaire.

  - **Type 2 : Hosted :** S'exécute comme une application sur un système d'exploitation hôte.

UN HYPERVISEUR, C'EST QUOI ?



Cas d'usage :

Type 1 : utilisés dans les datacenters d'entreprise ou d'autres environnements basés sur un serveur. Ajoute la notion de clustering.

Type 2 : plus adaptés pour les utilisateurs individuels qui souhaitent exécuter plusieurs systèmes d'exploitation sur un ordinateur personnel.

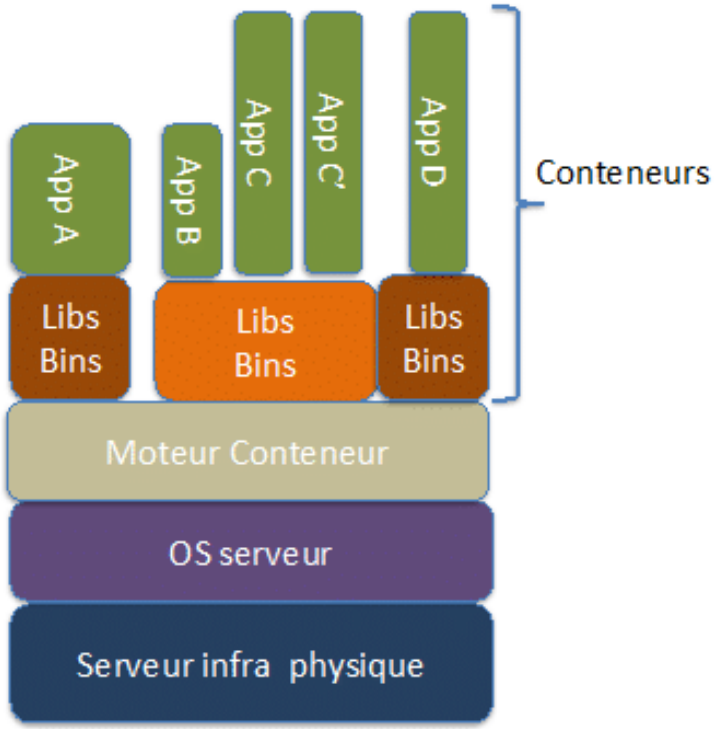
HYPERVISEUR, FONCTIONNALITÉS

Fonctionnalité	Description
Création de VM	Permet de créer, configurer et supprimer des machines virtuelles.
Allocation de ressources	Gère la répartition du CPU, de la RAM, du stockage et du réseau.
Isolation	Assure que chaque VM fonctionne de manière indépendante et sécurisée.
Migration à chaud	Déplace une VM d'un serveur physique à un autre sans interruption.
Snapshots	Permet de « sauvegarder » et restaurer l'état d'une VM à un instant donné.
Gestion du réseau	Configure des réseaux virtuels (NAT, pont, VLAN).

LA CONTENEURISATION, C'EST QUOI ?

- **Définition**

  consiste à regrouper le code logiciel avec uniquement les bibliothèques du système d'exploitation (OS) et les dépendances nécessaires pour exécuter le code afin de créer un seul exécutable léger, appelé conteneur, qui s'exécute de manière cohérente sur n'importe quelle infrastructure.



LA CONTENEURISATION, C'EST QUOI ?

- **Objectifs principaux**
  - **Isoler** les applications pour éviter les conflits.
  - Garantir la **portabilité** (exécution identique sur tous les environnements).
  - **Optimiser l'utilisation des ressources** (pas de surcharge d'un OS complet).

- **Exemple concret**

  Lorsqu'un développeur transfère du code de son ordinateur de bureau vers une machine virtuelle, cela engendre souvent des bugs et des erreurs. La conteneurisation élimine ce problème en regroupant le code l'application avec les fichiers de configuration, les bibliothèques et les dépendances nécessaires à son fonctionnement. Le conteneur est **autonome** et **portable**.

UN ORCHESTRATEUR, C'EST QUOI ?

- Outil essentiel pour **automatiser, gérer et optimiser** le déploiement, la mise à l'échelle et l'exploitation d'applications conteneurisées, surtout dans des environnements complexes ou à grande échelle.

UN ORCHESTRATEUR, C'EST QUOI ?

- Exemples de features possibles :
  - Gestion Automatique des Conteneurs (Déploiement / Redémarrage automatique / Mise à jour sans interruption)
  - Mise à l'Échelle (Scaling)
  - Équilibrage de Charge et Disponibilité
  - Gestion des Réseaux et du Stockage
  - Gestion des Configurations et des Secrets
  - Surveillance et Logging
  - Portabilité et Environnements Multi-Cloud

ISOLATION

- **Conteneurisation :**
  - Niveau OS (partage du noyau)
  - Isolation réduite: sécurité amoindrie (risque de fuite via le noyau partagé)
  - Namespaces : isole des processus, le réseau, etc.
  - Cgroups : limite l'utilisation des ressources (CPU, RAM,R/W disk)

- **Virtualisation :**
  - Niveau matériel (OS complet)
  - Isolation augmentée : sécurité renforcée (chaque VM est indépendante)
  - Chaque VM a son propre OS invité, son CPU virtuel, sa RAM dédiée, et son disque virtuel.

VMS ET CONTENEURS, DIFFÉRENCES

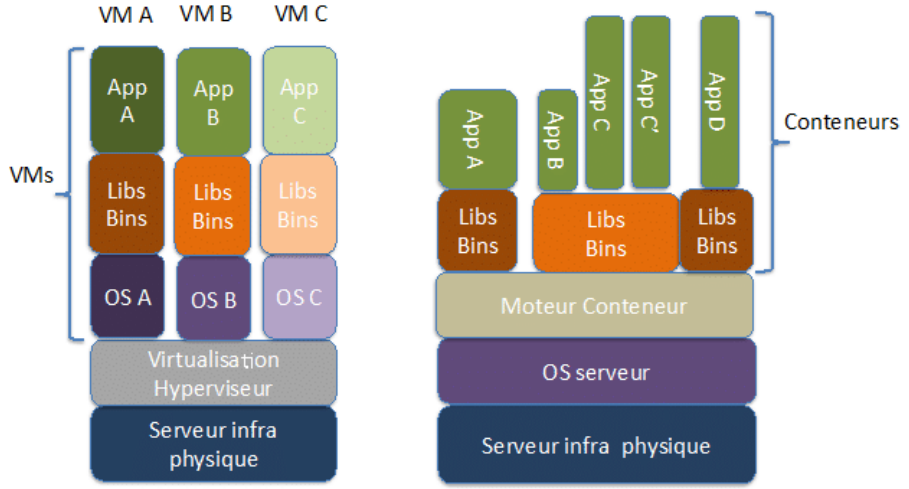
LÉGÈRETÉ CONTRE ISOLATION, LEQUEL CHOISIR POUR VOS APPLICATIONS ?

LES DIFFÉRENCES

Critère	Conteneur	Machine Virtuelle (VM)
Isolation	Niveau OS (partage du noyau)	Niveau matériel (OS complet)
Système d'exploitation	Partage le noyau de l'OS hôte	Chaque VM a son propre OS
Performance	Très léger, démarrage rapide	Plus lourde, démarrage lent
Portabilité	Exécution identique partout	Dépend de l'hyperviseur
Utilisation	Applications, microservices	Systèmes complets, OS multiples
Sécurité	Risque de fuite via le noyau partagé	Isolation totale entre VM
Ressources	Pas de surcharge d'un OS complet	Nécessite un OS complet et des ressources dédiées / VM

LES DIFFÉRENCES

- Les conteneurs sont beaucoup plus légers et plus rapide que les VM et permettent de déployer beaucoup plus d'applications sur un seul serveur.
- Les VM offrent une isolation totale, idéale pour la sécurité et la compatibilité multi-OS.
- Les conteneurs sont parfaits pour les microservices et le cloud, tandis que les VM restent incontournables pour les environnements critiques ou multi-OS



PANORAMA DES TECHNOLOGIES

TOUR D'HORIZON DES SOLUTIONS CLÉS

VIRTUALISATION

- Hyperviseurs de type 1 : Bare-metal

vmware ESXi
Microsoft Hyper-V
PROXMOX
KVM
NUTANIX
Xen Project

VIRTUALISATION

- Hyperviseurs de type 2 : Hosted

vmware Workstation

VirtualBox

KVM

Parallels®

CONTENEURISATION

- Moteurs de conteneurs :

docker

podman

LXC

buildah

containerd

CONTENEURISATION

- Orchestrateurs :

kubernetes

docker SWARM

HashiCorp Nomad

OPENSHIFT

RANCHER BY SUSE

portainer.io

C’EST L’HEURE DE LA PRATIQUE