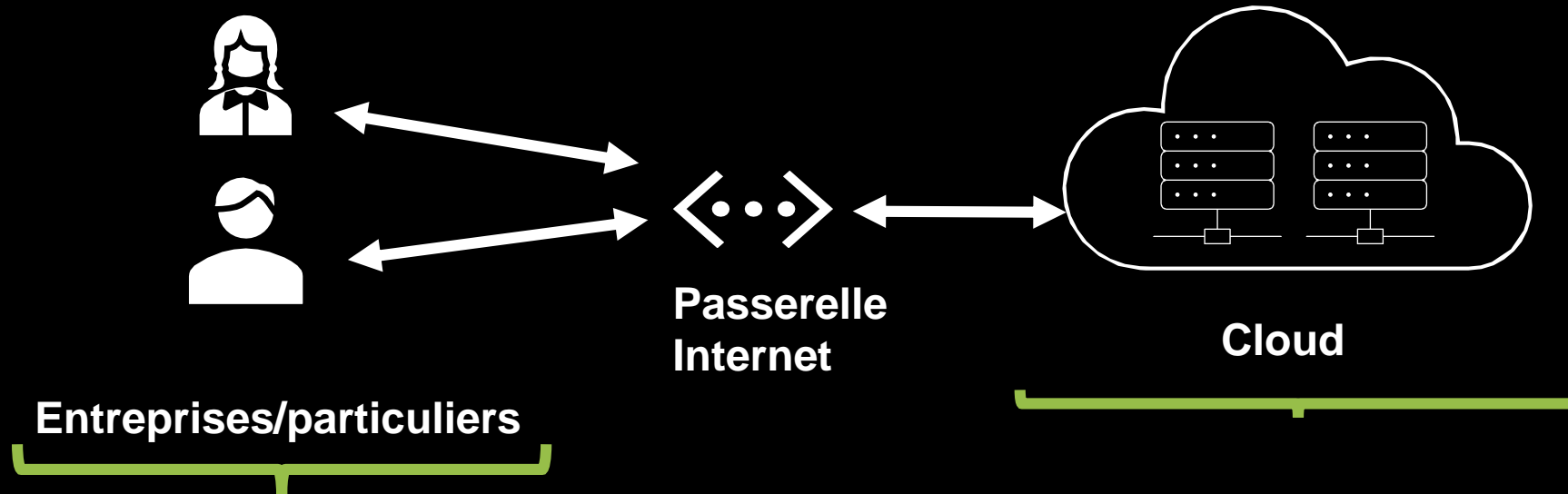


Cloud for IOT - 2

ESIR 3 – 2021/2022

Djob Mvondo

Rappel : Cloud



Apports du Cloud pour les entreprises

- ☐ "Infinité" de ressources (CPU, mémoire, etc...)
- ☐ Passage à l'échelle
- ☐ Taux de disponibilité élevé

Responsabilités des fournisseurs de Cloud

- ☐ Assurer isolation et performance
- ☐ Faire des bénéfices
==> Utilisation efficace des ressources
- ☐ S'appuient sur la **virtualisation**

Rappel: Défis à surmonter

Confidentialité

- Où sont stockées mes données ?
- Quel loi encadre cela ?

SLA/SLOs

- Ce qui est promis doit être garantie
- Le client doit avoir foi en cette garantie

Impact énergétique

- 1.5% of energy is used by datacenters [2010, Jonathan Koumey]

Monitoring précis

- Ma facture doit correspondre à mon utilisation
- Plusieurs utilisateurs

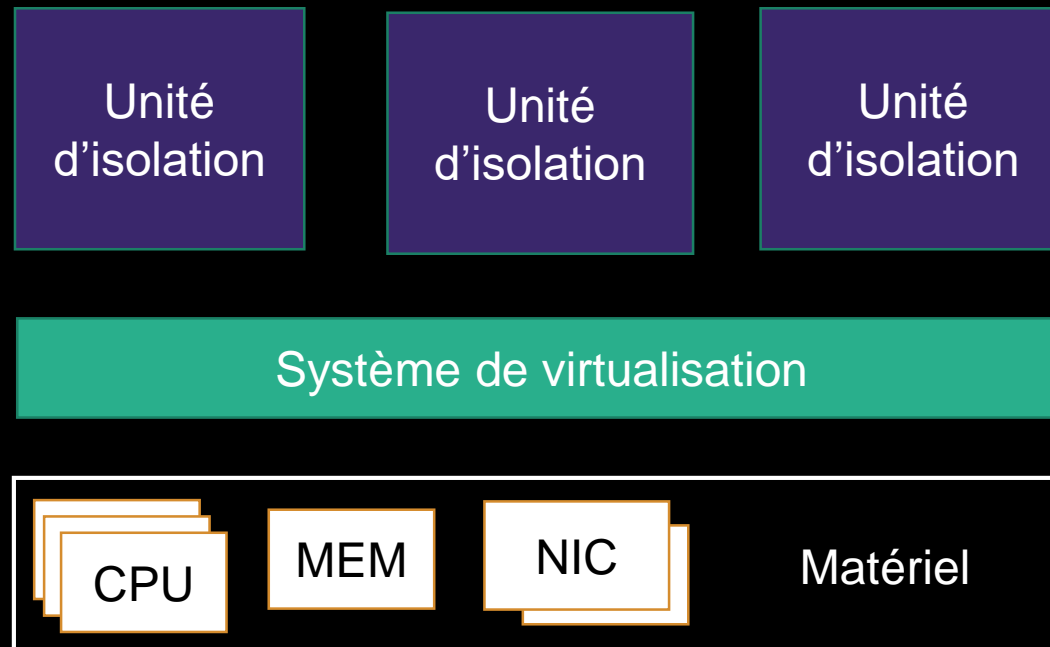
Evoluer avec le matériel

- Besoin d'équipement spécifique
- Être interopérable

Cloud : La virtualisation à la rescousse

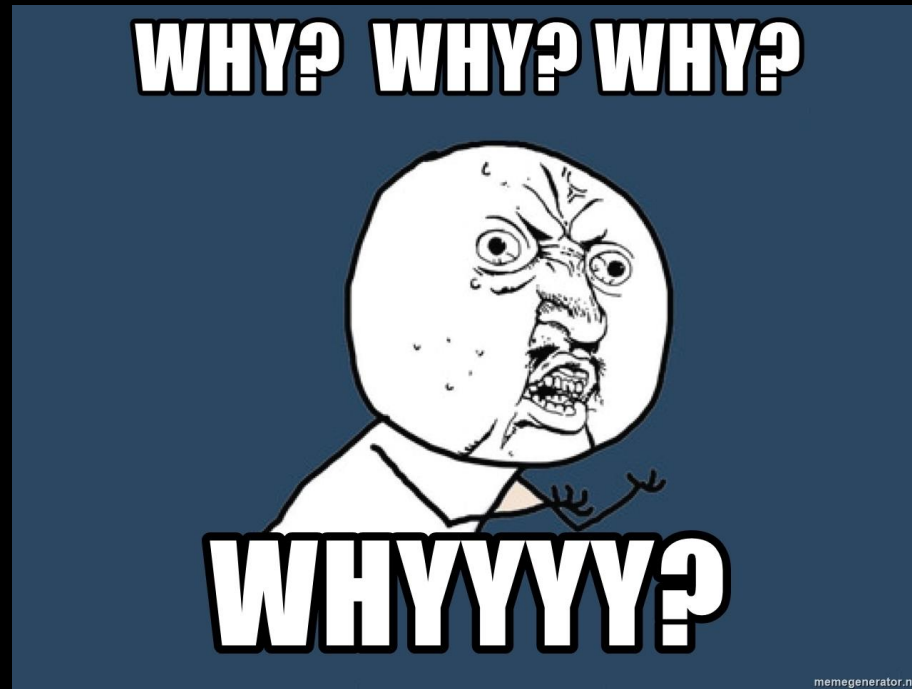
Virtualisation au service du Cloud

- ❑ Plusieurs systèmes parallèles sur un serveur
- ❑ Isolation entre chaque système
- ❑ Tolérance aux pannes grâce à la migration



Ensemble des techniques matérielles et/ou logicielles qui permettent de faire fonctionner simultanément sur une seule machine plusieurs systèmes d'exploitation (appelés machines virtuelles (VMs). Ex.: Xen, VMware, KVM, HyperV, etc

Pourquoi s'y intéresser ?



Pourquoi s'y intéresser ?

1

Maîtriser les technologies sous-jacentes

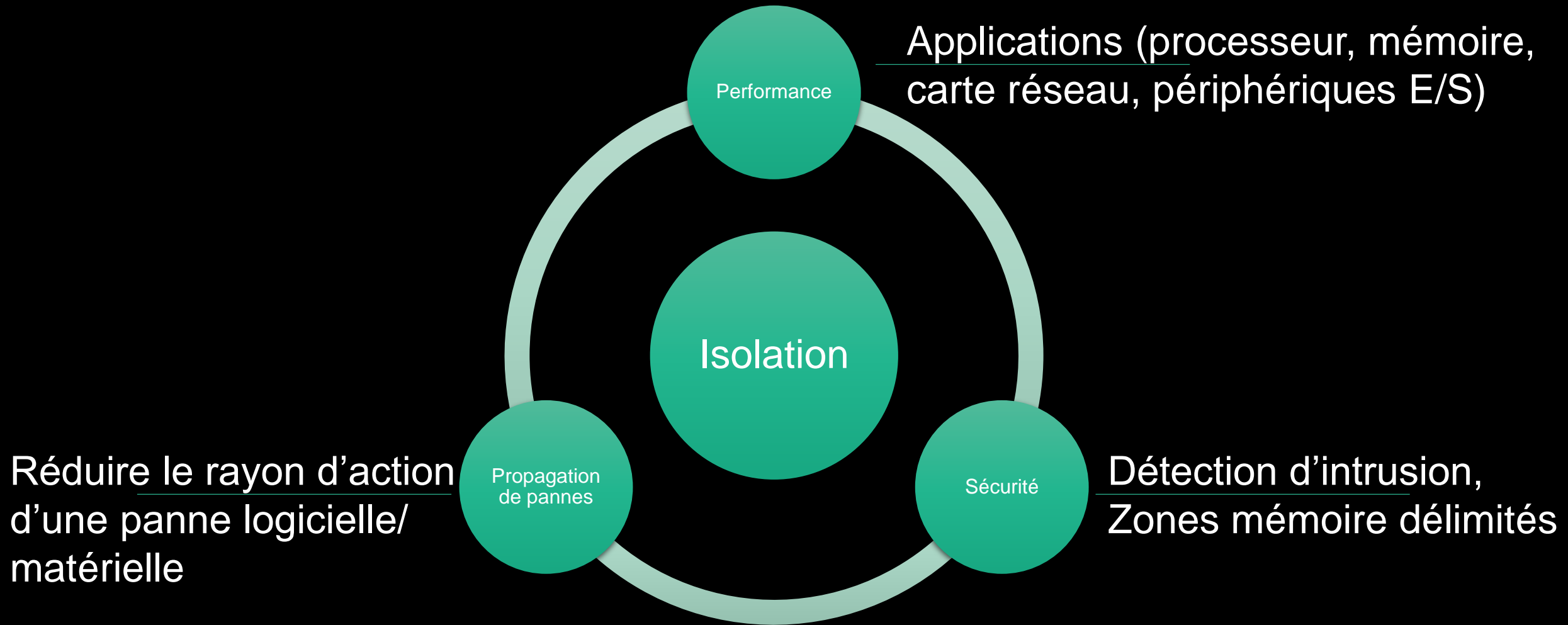
2

Savoir dimensionner et choisir les outils adaptés pour l'écosystème

3

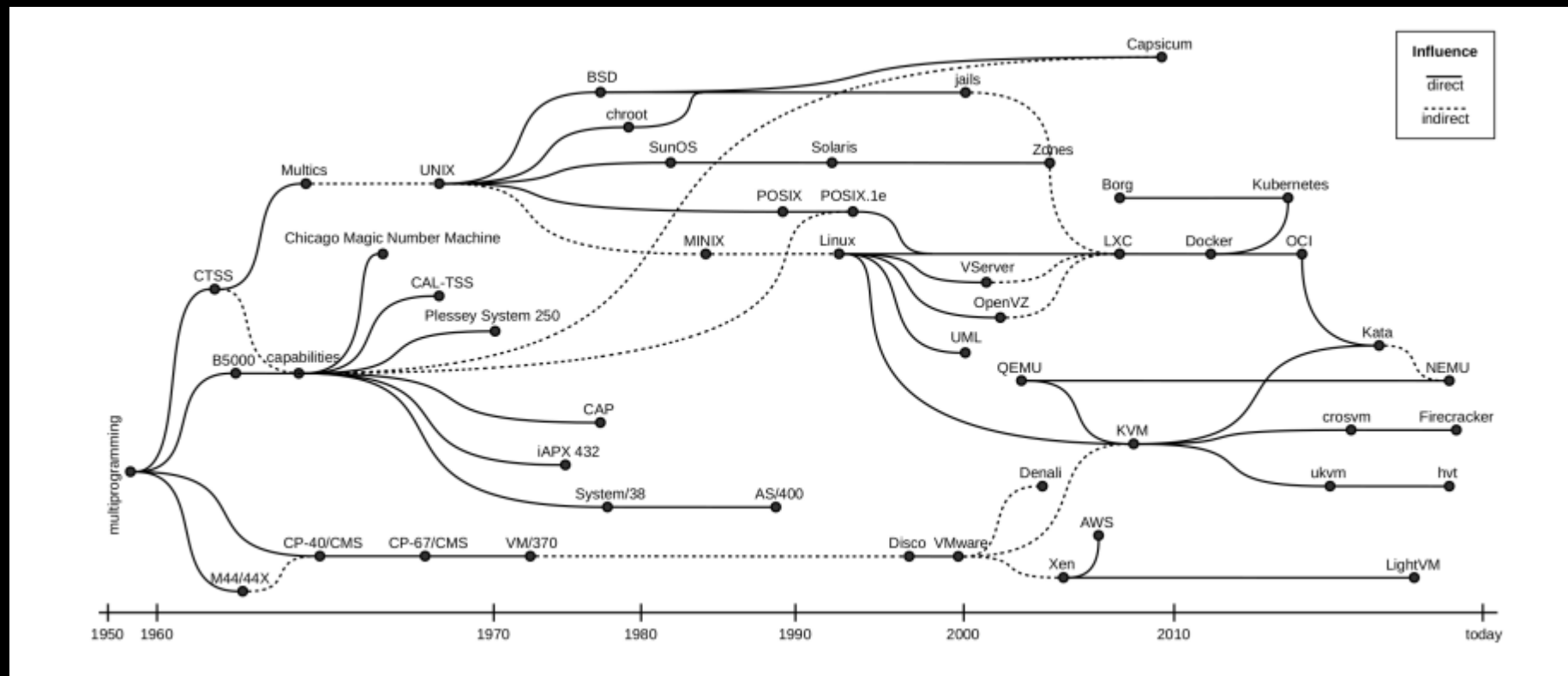
Comprendre les points de défaillances et de dégradation éventuels

Virtualisation : Concepts de base



Virtualisation : Sujet de recherche constant

Les mécanismes de virtualisation évoluent, en fonction de la nature des applications et du **contexte architectural** (x86, ARM, RISC-V, PowerPC, etc.)



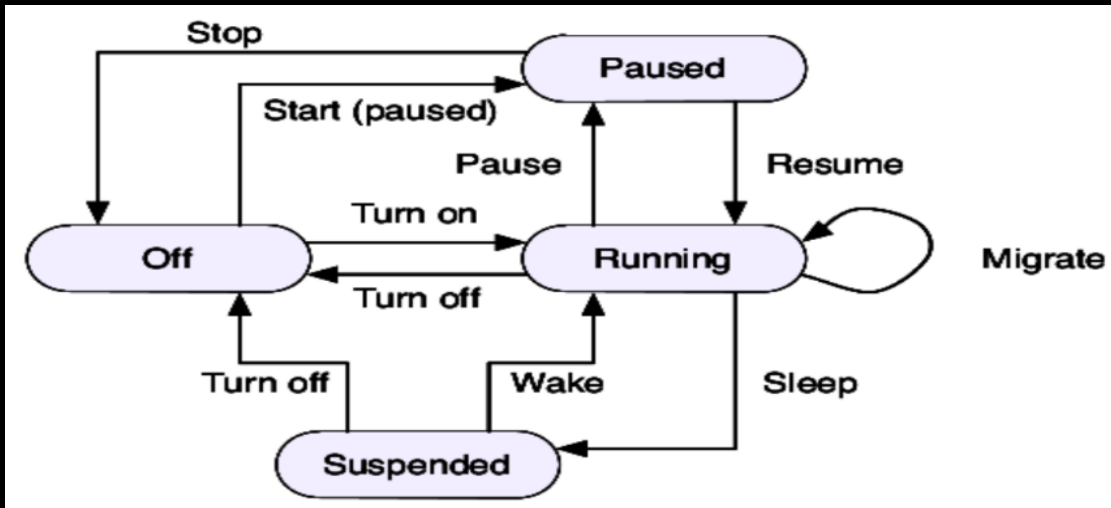
Evolution des systèmes de virtualisation

RANDAL, A. The ideal versus the real : Revisiting the history of virtual machines and containers. ACM Comput. Surv. 53

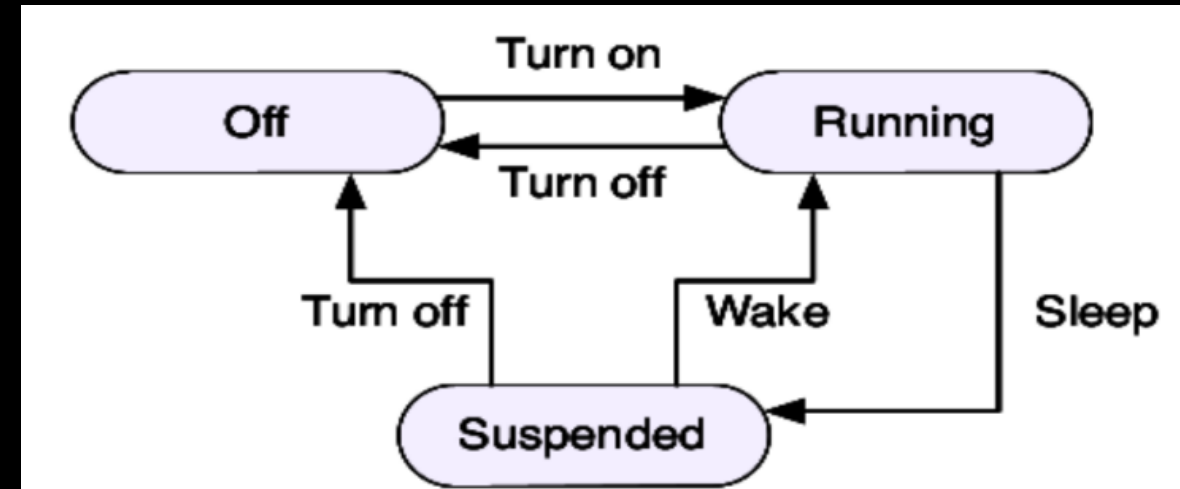
Virtualisation : Différences avec un système traditionnel

Une unité d'isolation peut avoir plusieurs **états** intermédiaires comparé à une machine classique.

====> **Plus de possibilités**



Cycle de vie d'une unité d'isolation

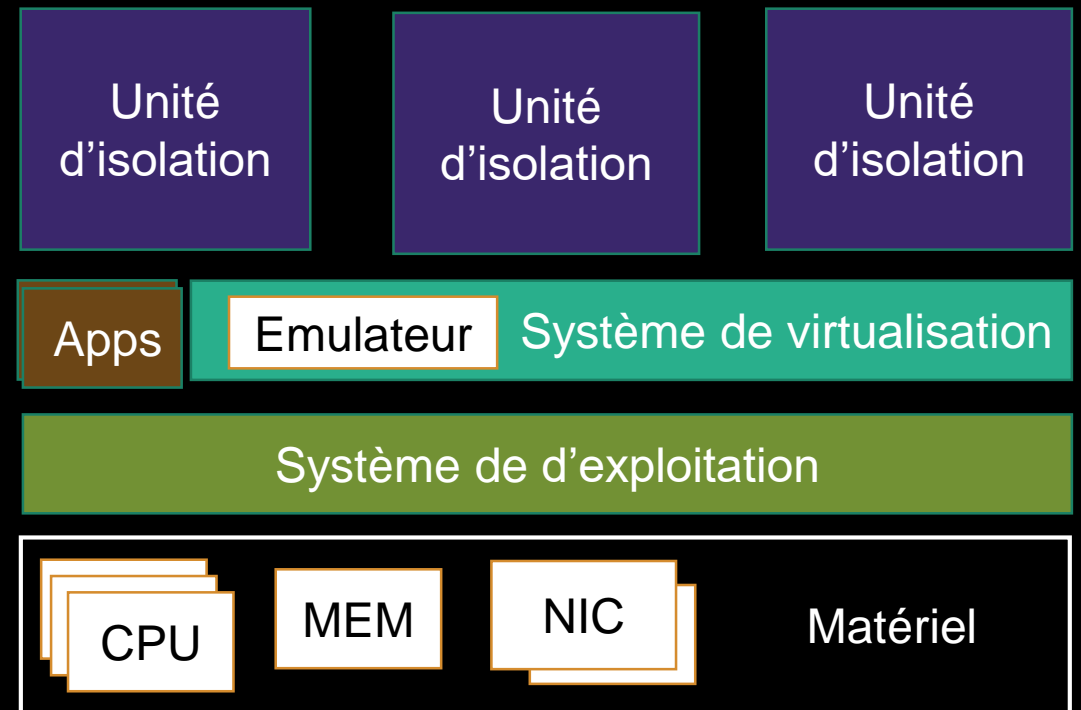


Cycle de vie traditionnel

Virtualisation : Les catégories

❑ Virtualisation complète

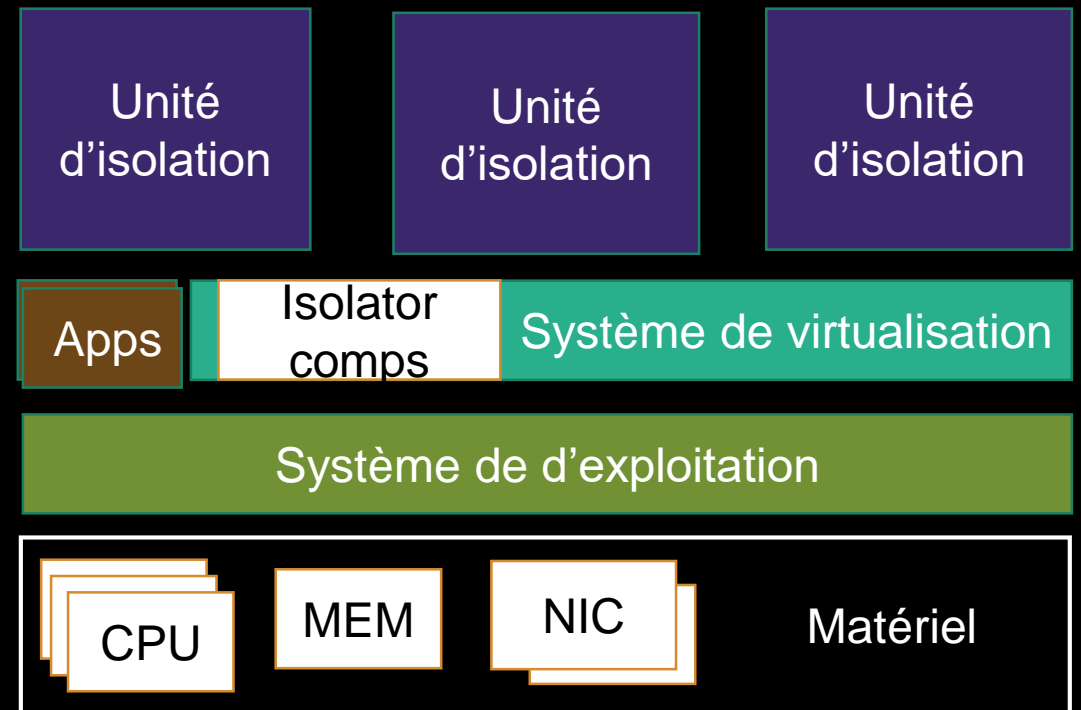
- ❑ Le système de virtualisation **s'appuie** sur un système d'exploitation existant.
- ❑ Toutes les instructions des unités d'isolations sont **émulés**.
- ❑ **Aucune modification** au système d'exploitation requis pour la virtualisation.
- ❑ **Dégradation conséquente** dû à l'émulation.
- ❑ Exemple: VirtualBox, Parallels.



Virtualisation : Les catégories

❑ Virtualisation niveau OS

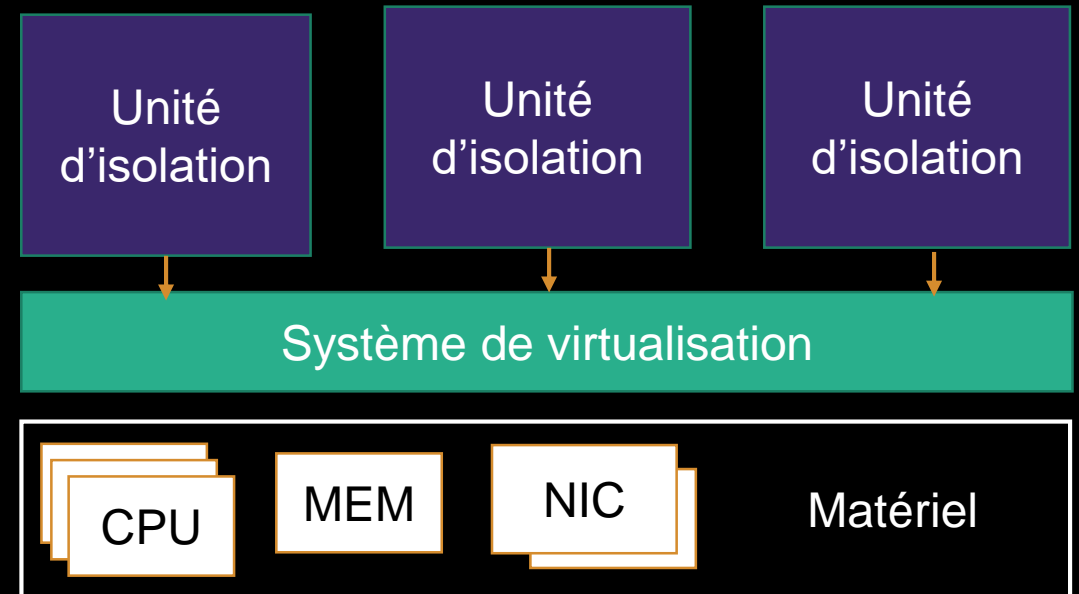
- ❑ Le système de virtualisation **s'appuie** sur un système d'exploitation existant.
- ❑ Des **espaces d'isolations** sont créés pour chaque unité d'isolation (cgroups, seccomp, ...)
- ❑ L'unité d'isolation doit être construite d'une façon spécifique (par ex: container Docker)
- ❑ Isolation pas **très forte**¹
- ❑ Exemple: Docker, LXC, gVisor, etc...



Virtualisation : Les catégories

❑ Para-virtualisation

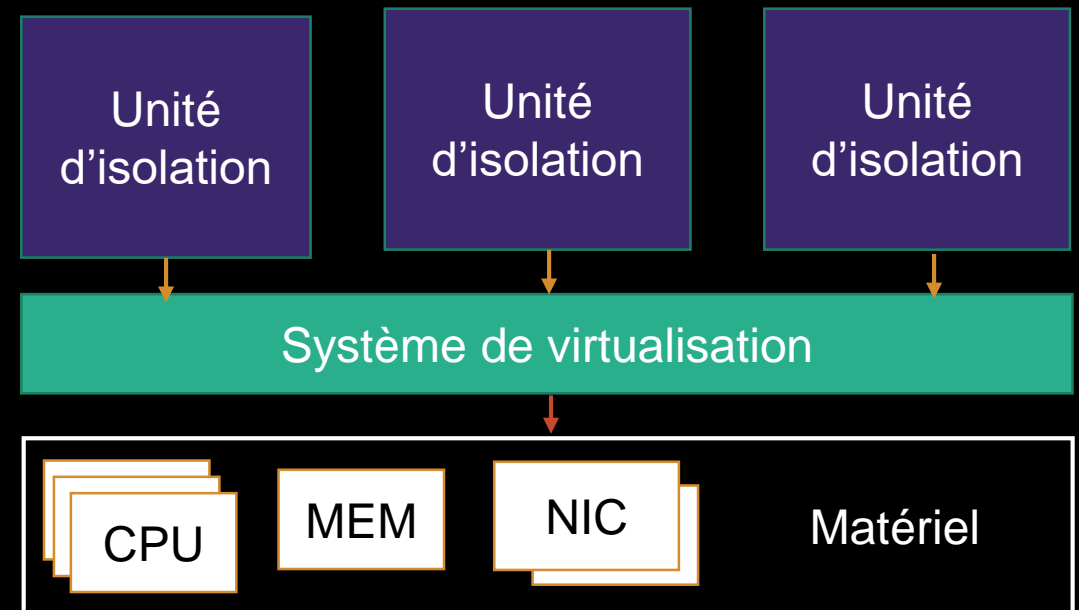
- ❑ Le système de virtualisation **devient** l'hôte
- ❑ Se charge de gérer **l'isolation et l'allocation des ressources** de façon dynamique
- ❑ **Appels système** spécifique (en orange) pour réaliser des opérations privilégiées
- ❑ Isolation **très forte**
- ❑ Exemple: Xen, Hyper-V, VMWare Esxi



Virtualisation : Les catégories

❑ Virtualisation assisté par le matériel (HVM)

- ❑ Le système de virtualisation **exploite** des instructions spécifiques du matériel
- ❑ Se charge de gérer **l'isolation et l'allocation des ressources** de façon dynamique
- ❑ **Appels système** spécifique (en orange) pour réaliser des opérations privilégiées
- ❑ Isolation **très forte**
- ❑ Exemple: Xen, Hyper-V, VMWare Esxi



Virtualisation : Quel catégorie choisir ?

Trois critères à surveiller

Contraintes
fonctionnels,
matérielle

Toolchain pour
construire son unité
d'isolation

Support de la
communauté
(les applications)

Préferer les outils open source

Virtualisation : Concepts techniques

La plupart des concepts techniques ont les mêmes racines.
Nous allons illustrer certains avec le système de virtualisation Xen.

Je vous recommande ces deux livres :

- *The definitive guide to the Xen hypervisor*
- *Hardware and Software Support for Virtualization*

Virtualisation : Concepts techniques

Le système de virtualisation Xen

Crée en 2003, Xen est utilisé par plusieurs fournisseurs de Cloud (ex: Amazon)

Utilisé par plusieurs entreprises industrielles et organisme de recherche.

Très forte communauté autour de l'outil

Supporte la para-virtualisation et assisté par le matériel

Virtualisation : Concepts techniques

Xen : Le démarrage d'une unité d'isolation

BIOS fournit des infos au noyau

- Mémoire, processeur, périphériques, ...

Le noyau se charge en mémoire central

Les structure de données du noyau sont initialisés

Le programme de démarrage est lancé
(init, systemd, ...)

Pipeline standard

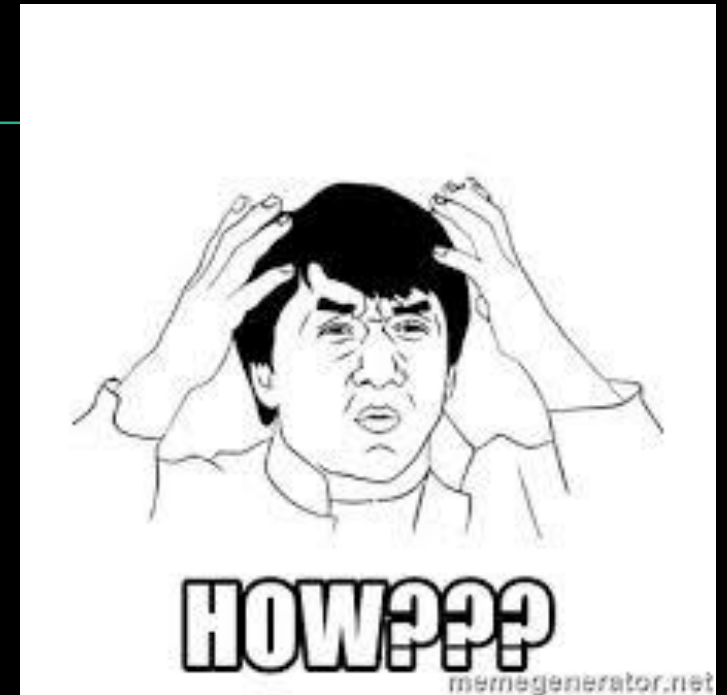
Virtualisation : Concepts techniques

Xen : Le démarrage d'une unité d'isolation

Problématique : Comment faire ?

Les informations du BIOS ne sont
disponible qu'au démarrage de la
machine physique

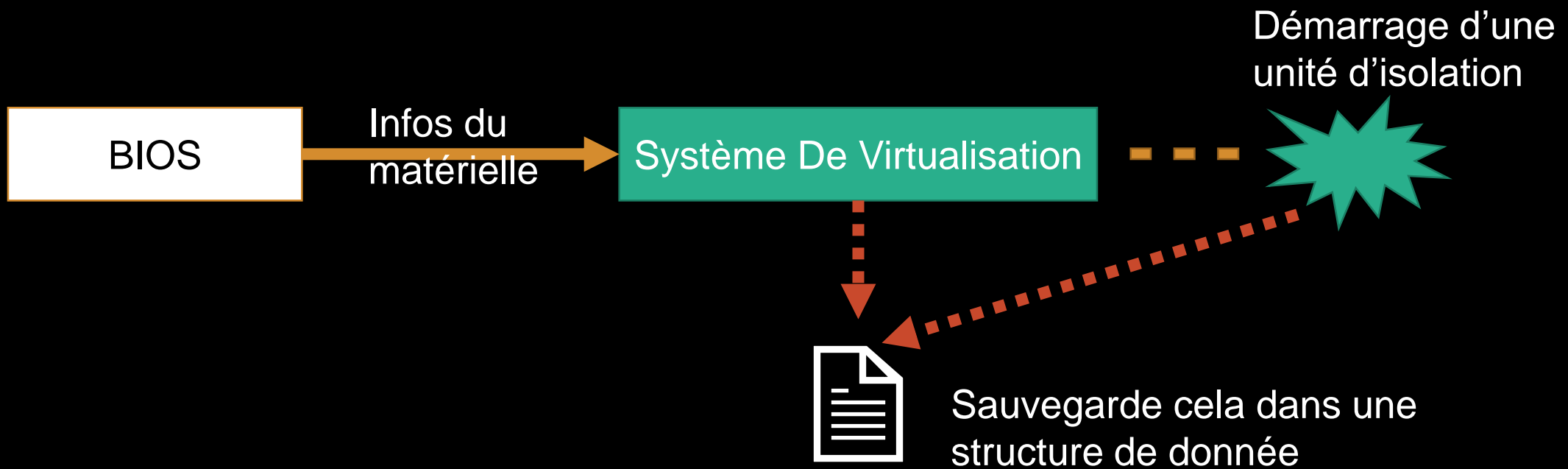
La mémoire a besoin d'être contiguë
pour le démarrage



Virtualisation : Concepts techniques

Xen : Le démarrage d'une unité d'isolation

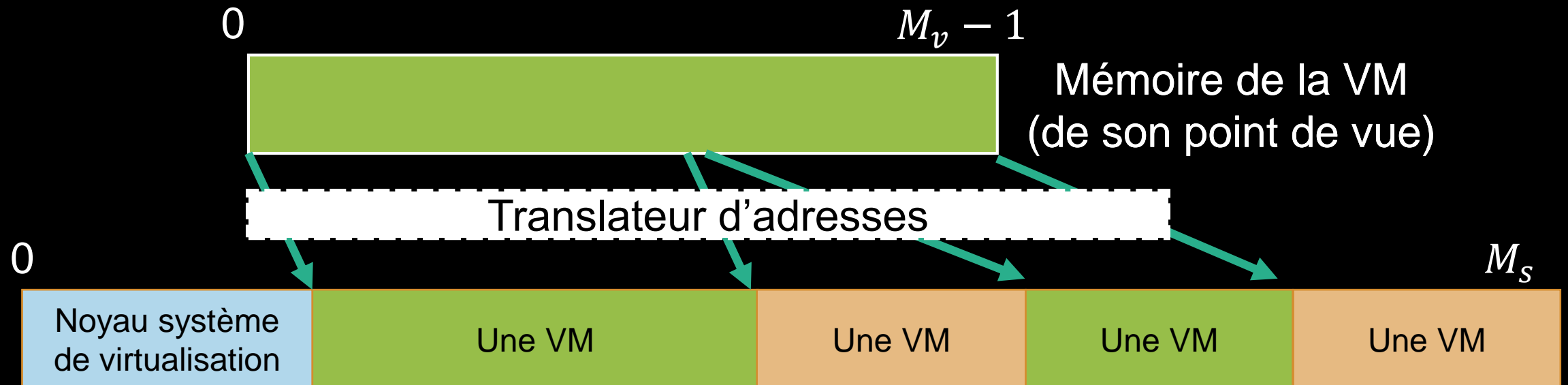
Information du BIOS: Xen sauvegarde l'état dans une structure



Virtualisation : Concepts techniques

Xen : Le démarrage d'une unité d'isolation

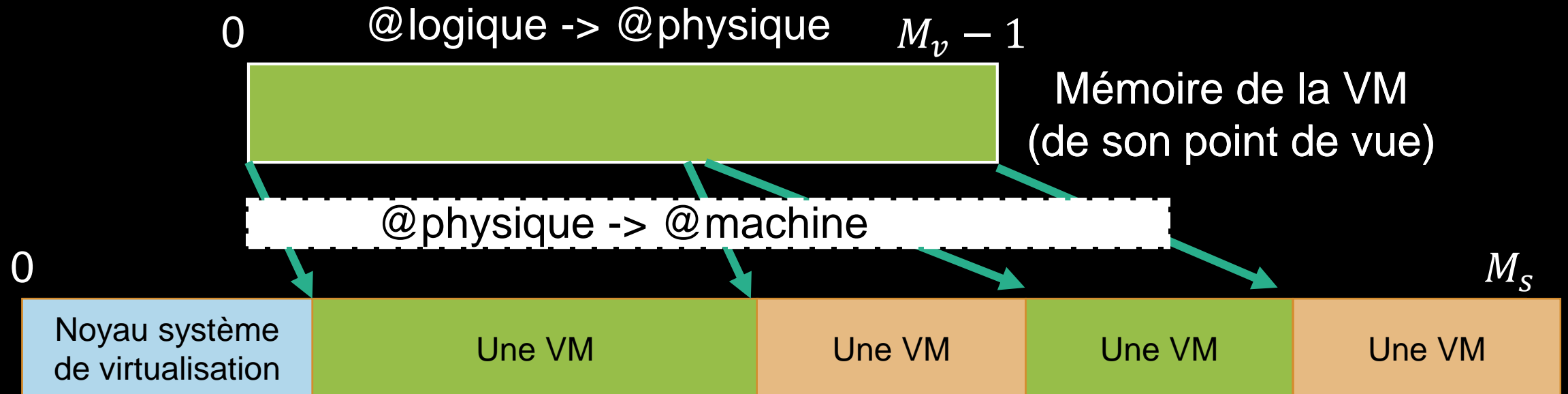
Mémoire contiguë: Xen effectue la translation d'adresse



Virtualisation : Concepts techniques

Xen : Le démarrage d'une unité d'isolation

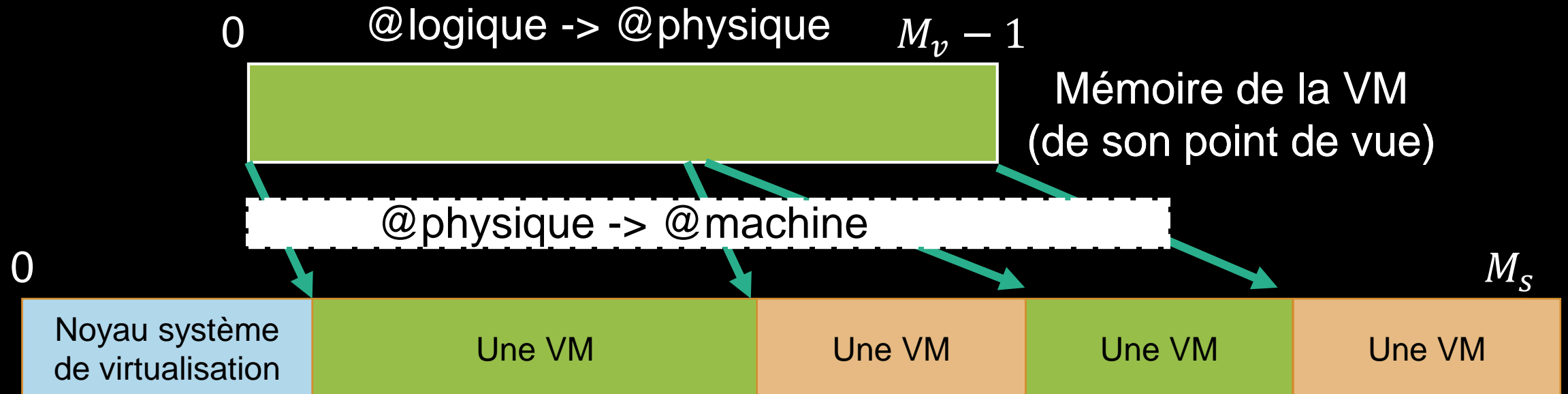
Mémoire contiguë: Xen effectue la translation d'adresse



Virtualisation : Concepts techniques

Xen : Le démarrage d'une unité d'isolation

Mémoire contiguë: Xen effectue la translation d'adresse en interceptant les appels systèmes qui concerne la **table des pages**



Virtualisation : Concepts techniques

Xen : La gestion des périphériques

Architecture « **split-driver** » : similaire au « client-serveur »

- ❑ Exploite le dom0 qui contient les bibliothèques pour accéder au matériel
- ❑ Chaque unité a un représentant qui communique avec le dom0 pour s'échanger les requêtes/réponses.

