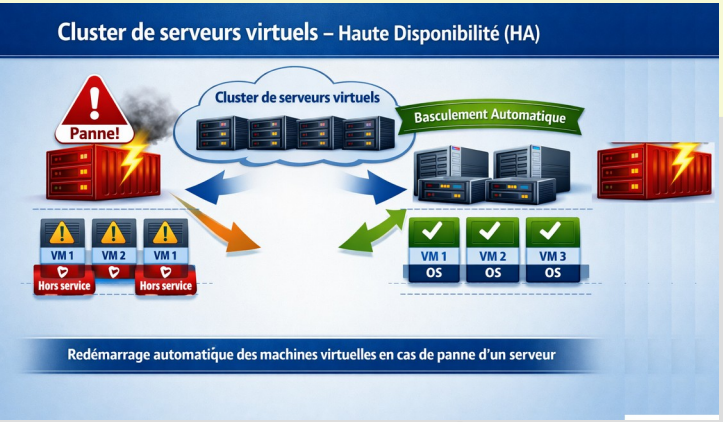
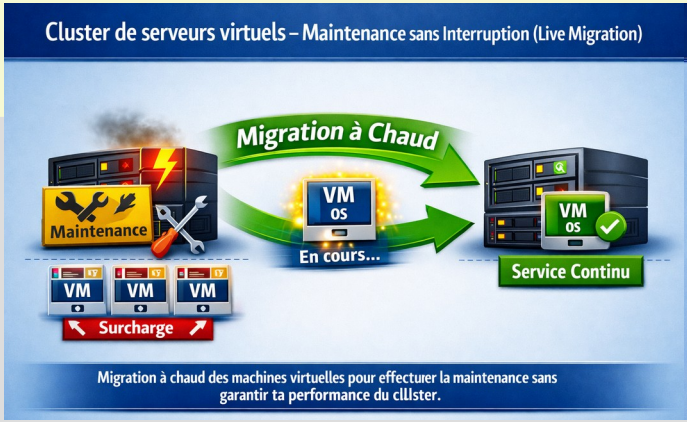
Les contraintes de l’informatique moderne

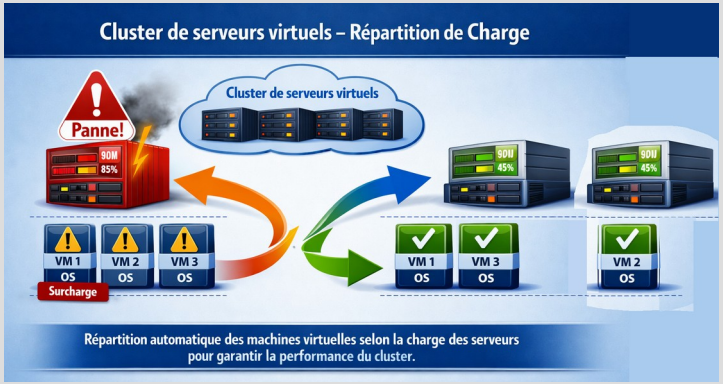


- **1. Haute disponibilité (HA)**
- tes services restent accessibles même en cas de panne matérielle ou logicielle
- **2. Répartition de charge (Load Balancing)**
- Les ressources sont équilibrées entre les hôtes pour éviter la surcharge.



- **3. Maintenance sans interruption**
- Cela permet de mettre à jour ou redémarrer un serveur physique sans impact sur les services.
- **4. Scalabilité**
- On ajoute facilement de nouveaux hôtes au cluster pour augmenter la capacité.

- **5. Tests avant mise en production**
- Valider la stabilité, la performance et la sécurité du cluster avant qu’il ne soit utilisé en environnement réel
- **6. Sécurité et Sauvegarde du Cluster**
- Garantir la protection des données et la résilience du cluster face aux incidents, attaques ou erreurs humaines.



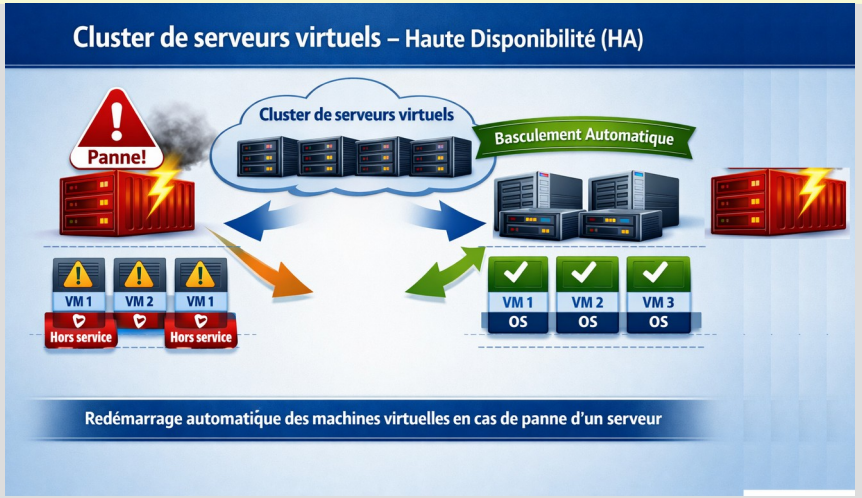
Les contraintes de l’informatique

- **1. Haute disponibilité (HA)**

- c’est ce qui garantit que tes services restent accessibles même en cas de panne matérielle ou logicielle

- La haute disponibilité repose sur un cluster de serveurs capables de se remplacer mutuellement. Si un serveur tombe en panne, les machines virtuelles (VM) qu’il héberge sont automatiquement redémarrées sur un autre hôte du cluster.

- Les VM critiques (serveurs web, bases de données, etc.) sont redémarrées automatiquement sur un autre nœud du cluster en cas de défaillance.
- Exemple : un cluster VMware vSphere ou Hyper-V avec basculement automatique.
-



🔄 Fonctionnement simplifié

Surveillance continue des hôtes du cluster.

Détection de panne (ex. perte de communication, crash matériel).

Basculement automatique des VM vers un autre hôte disponible.

Redémarrage des VM à partir du stockage partagé.

Notification et journalisation de l’événement pour diagnostic.

🧠 Avantages

Disponibilité quasi continue des services.

Réduction du temps d’arrêt (quelques secondes à minutes).

Aucune intervention manuelle nécessaire.

Sécurité accrue pour les environnements critiques (serveurs applicatifs, bases de données, etc.).

Les contraintes de l’informatique

2. Répartition de charge (Load Balancing)

- La répartition de charge consiste à distribuer automatiquement les machines virtuelles (VM) entre les différents hôtes du cluster selon leur niveau d’utilisation des ressources (CPU, mémoire, stockage, réseau). L’objectif est d’obtenir un équilibre dynamique pour maximiser les performances et la stabilité.

🔄 Cycle typique

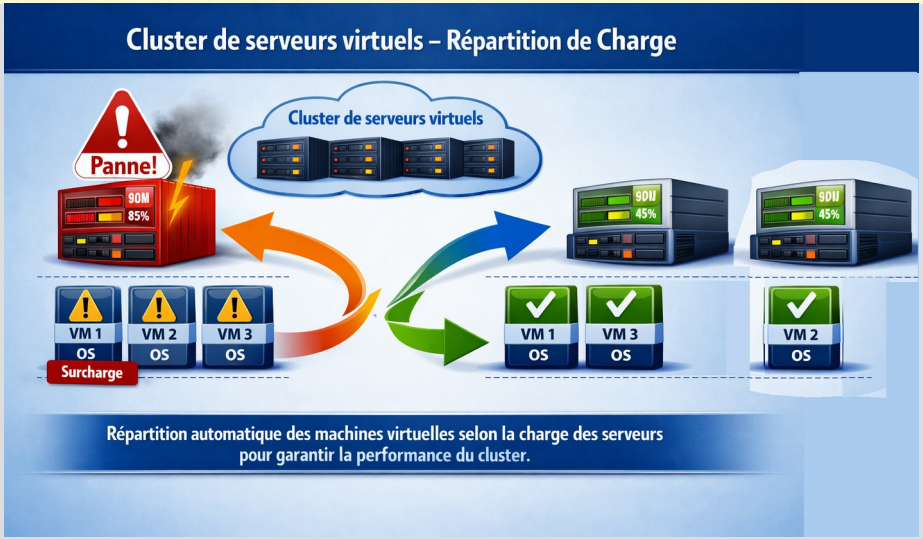
Collecte des données : chaque hôte envoie ses statistiques de charge au contrôleur DRS.

Analyse : le système détecte les déséquilibres (un hôte trop sollicité).

Décision : l’algorithme choisit les VM à déplacer pour rétablir l’équilibre.

Migration à chaud : les VM sont transférées vers un autre hôte sans interruption.

Stabilisation : le cluster retrouve un niveau de charge homogène.



🧠 Avantages

Performance optimisée : chaque VM dispose des ressources nécessaires.

Réduction des risques de surcharge et de ralentissement.

Automatisation complète : pas besoin d’intervention manuelle.

Adaptation dynamique : le cluster s’ajuste en temps réel selon la charge.

Compatibilité avec la haute disponibilité (HA) : les deux mécanismes se complètent.

Les contraintes de l’informatique

3. Maintenance sans interruption

- La Live Migration est l’un des mécanismes les plus impressionnants des environnements virtualisés. Elle permet de déplacer une machine virtuelle (VM) d’un serveur physique à un autre sans l’arrêter, sans coupure réseau, sans impact pour les utilisateurs.
- C’est ce qui rend possible la maintenance d’un hôte en pleine journée, sans perturber la production.

🧩 Ce que la Live Migration permet concrètement

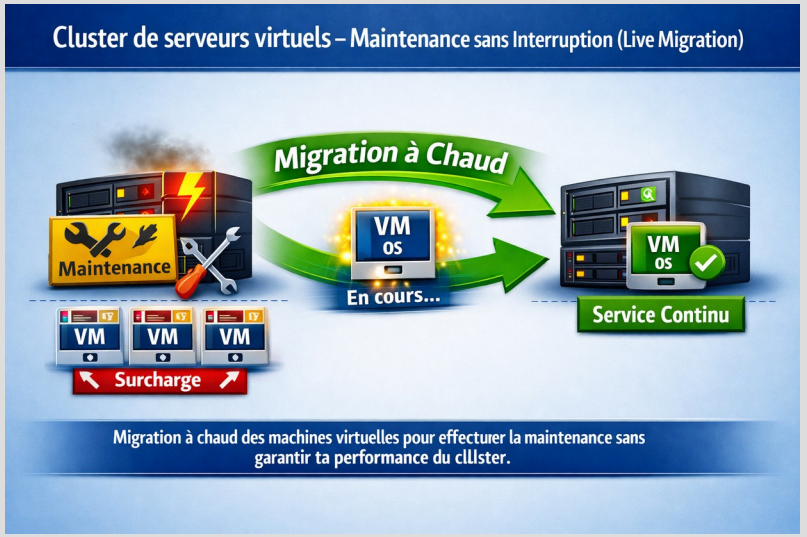
✔️ **Maintenance matérielle**
changement de RAM
remplacement d’un ventilateur
mise à jour du BIOS
nettoyage interne
remplacement d’un disque du serveur

✔️ **Maintenance logicielle**
mise à jour de l’hyperviseur
patch de sécurité
redémarrage de l’hôte

✔️ **Optimisation automatique**
Le cluster peut migrer des VM pour :
équilibrer la charge (DRS),
économiser de l’énergie (consolidation nocturne),
isoler un hôte instable.

🧠 Avantages majeurs

Zéro interruption de service
Aucune action visible côté utilisateur
Maintenance planifiée en journée
Réduction des risques (on évite les interventions en urgence)
Flexibilité totale pour les administrateurs



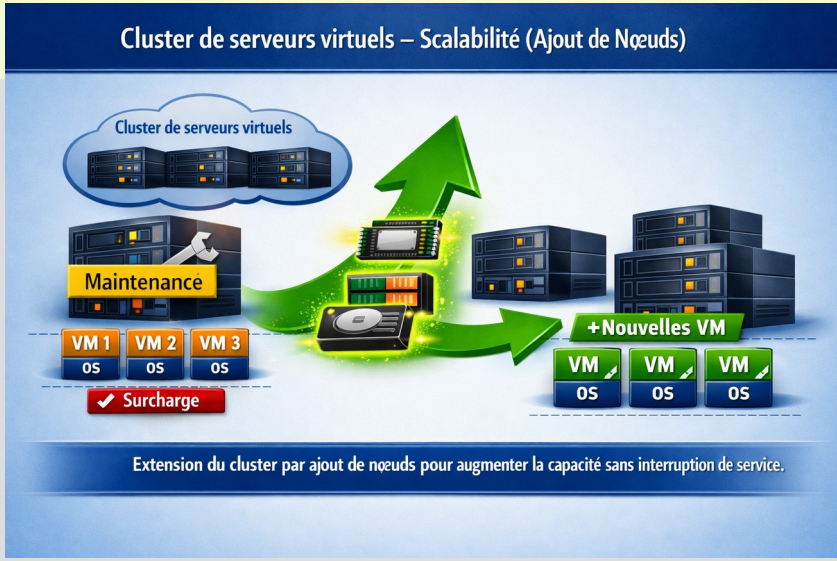
🧠 Pourquoi c’est possible ?

Parce que dans un environnement virtualisé :
La VM n’est pas liée physiquement au serveur.
Son disque dur est stocké sur un stockage partagé (SAN/NAS/ClusterFS).
Son état (mémoire, CPU, connexions réseau) peut être copié en temps réel vers un autre hôte.

Les contraintes de l’informatique

4. Scalabilité

- La scalabilité est la capacité d’un cluster à augmenter sa puissance et sa capacité en ajoutant de nouveaux serveurs (nœuds). C’est ce qui permet à une infrastructure de grandir sans interruption, au rythme des besoins.



🧠 Pourquoi la scalabilité est essentielle ?

Parce que les besoins évoluent :
plus d’utilisateurs
plus d’applications
plus de VM
plus de charge CPU/RAM
plus de stockage
Sans scalabilité, un cluster serait figé et finirait par saturer.

⚙️ Deux types de scalabilité

1️⃣ Scalabilité horizontale (la plus utilisée en virtualisation)

On ajoute des serveurs physiques au cluster.
➡️ C’est ce que tu illustres dans ton image n°4. ➡️ C’est la méthode la plus flexible et la plus fiable.

2️⃣ Scalabilité verticale

On augmente les ressources d’un serveur existant (plus de RAM, plus de CPU).
➡️ Utile mais limitée par le matériel. ➡️ Nécessite souvent un redémarrage → donc pas idéale pour un cluster.

🧠 Avantages majeurs

Aucune interruption de service
Croissance progressive (on ajoute un nœud quand on en a besoin)
Optimisation automatique grâce au DRS
Meilleure résilience (plus de serveurs = plus de tolérance aux pannes)
Coût maîtrisé (on investit au fur et à mesure)

Les contraintes de l’informatique

5. Tests avant mise en production

- Les tests avant mise en production (aussi appelés pré-production, validation, qualification) servent à garantir que ton cluster est stable, performant, sécurisé et conforme avant d’héberger des VM critiques.
- On ne teste pas « pour voir ». On teste pour prouver que le cluster est fiable.

🧠 **Pourquoi c’est critique :**

Un cluster peut sembler stable… jusqu’à ce qu’il soit chargé. Ces tests révèlent les défaut avant qu’ils ne deviennent des incidents.

Tests de basculement

Objectif : vérifier que la haute disponibilité fonctionne réellement.

Scénarios testés :

arrêt brutal d’un hôte
coupure réseau d’un hôte
crash simulé de l’hyperviseur
panne d’alimentation (sur un hôte isolé)

Tests applicatifs

Objectif : vérifier que les applications fonctionnent correctement dans le cluster.

🔍 **Ce qu’on teste :**

base de données
serveurs web
ERP / CRM
services internes
scripts métiers

Tests de migration à chaud

Objectif : s’assurer que les VM peuvent être déplacées sans interruption.

🔍 **Ce qu’on teste :**

migration d’une VM légère
migration d’une VM lourde (RAM > 16 Go)
migration simultanée de plusieurs VM
migration sous forte charge

Tests de sécurité

Objectif : vérifier que le cluster est protégé.

🔍 **Ce qu’on teste :**

segmentation réseau (VLAN, firewall)
accès administrateur (RBAC, MFA)
chiffrement des données (si disponible)
durcissement des hôtes (SSH, services inutile

Tests de compatibilité et cohérence du cluster

Objectif : vérifier que tous les hôtes sont alignés.

🔍 **Points contrôlés :**

versions d’hyperviseur identiques
microcodes CPU compatibles
pilotes réseau / stockage à jour
profils de sécurité identiques
configuration réseau homogène (VLAN, MTU, trunk)

Les contraintes de l’informatique

- **6. Sécurité et Sauvegarde du Cluster**
- Garantir la protection des données et la résilience du cluster face aux incidents, attaques ou erreurs humaines.
- La sécurité vise à empêcher :
- les intrusions,
- les accès non autorisés,
- les attaques réseau,
- les manipulations dangereuses,
- la compromission des VM ou des hôtes.
- Elle se divise en plusieurs couches

1.1. Sécurité réseau (pare-feu, VLAN, segmentation)

🔍 **Objectifs :**

isoler les flux sensibles,
empêcher qu’une VM compromise contamine tout le cluster,
protéger les interfaces de gestion.

1.2. Sécurité des accès (RBAC, MFA, journaux)

🔍 **Objectifs :**

contrôler qui peut faire quoi,
éviter les erreurs humaines,
tracer les actions.

1.3. Durcissement des hôtes (hardening)

🔍 **Objectifs :**

réduire la surface d’attaque,
limiter les services inutiles.

🧠 **Pourquoi c’est critique :**

Une mauvaise segmentation = un cluster vulnérable à une attaque interne ou externe.

80 % des incidents viennent d’un accès mal contrôlé.

Un hyperviseur compromis = toutes les VM compromises.

Les contraintes de l’informatique

- **6. Sauvegarde du Cluster**
- La sauvegarde n’est pas un “plus”, c’est une assurance-vie.
- Elle couvre :
- les VM,
- les configurations du cluster,
- les données applicatives,
- les snapshots,
- les plans de reprise.

2.1. Sauvegarde des machines virtuelles

🔍 **Objectifs :**
pouvoir restaurer une VM complète en cas de panne, erreur ou attaque.

Méthodes :
sauvegarde complète (full)
sauvegarde incrémentale
sauvegarde différentielle
sauvegarde à chaud (sans arrêter la VM)

2.2. Snapshots (instantanés)

🔍 **Objectifs :**
revenir en arrière rapidement avant une mise à jour ou une modification risquée.

🧩 **Caractéristiques :**
rapides
pratiques
mais pas une sauvegarde (risque de corruption si conservés trop longtemps)

🧠 **Bon usage :**
snapshot avant mise à jour
suppression après validation
jamais plus de 24–48h

2.3. Tests de restauration (PRA / PCA)

🔍 **Objectifs :**
vérifier que les sauvegardes fonctionnent réellement
mesurer le temps de reprise (RTO)
mesurer la perte de données acceptable (RPO)

🧠 **Pourquoi c’est critique :**
Une VM sans sauvegarde = une VM déjà perdue.
Une sauvegarde non testée = pas de sauvegarde

2. Les types de virtualisation

1️⃣ Virtualisation de serveurs physiques

C'est la forme la plus répandue.
Les serveurs physiques sont regroupés en un cluster.
Chaque serveur héberge des machines virtuelles (VM) isolées, chacune avec son OS et ses applications.
L'hyperviseur (ESXi, Hyper-V, Proxmox…) distribue CPU, RAM et stockage entre les VM.
Avantages : meilleure utilisation du matériel, haute disponibilité, flexibilité.

2️⃣ Virtualisation logicielle

Elle permet à un système d'exécuter plusieurs environnements logiciels.
Exécution d'un OS invité (ex. Linux dans Windows).
Virtualisation d'applications : une appli tourne dans un conteneur isolé.
Virtualisation de services ou de mémoire.
Avantages : compatibilité, isolation, déploiement simplifié.

3️⃣ Virtualisation des postes de travail (VDI)

Très populaire dans les entreprises.
L'utilisateur accède à son bureau virtuel depuis n'importe où.
Le poste de travail est hébergé dans le datacenter.
Avantages : mobilité, sécurité, maintenance centralisée.

4️⃣ Virtualisation du stockage

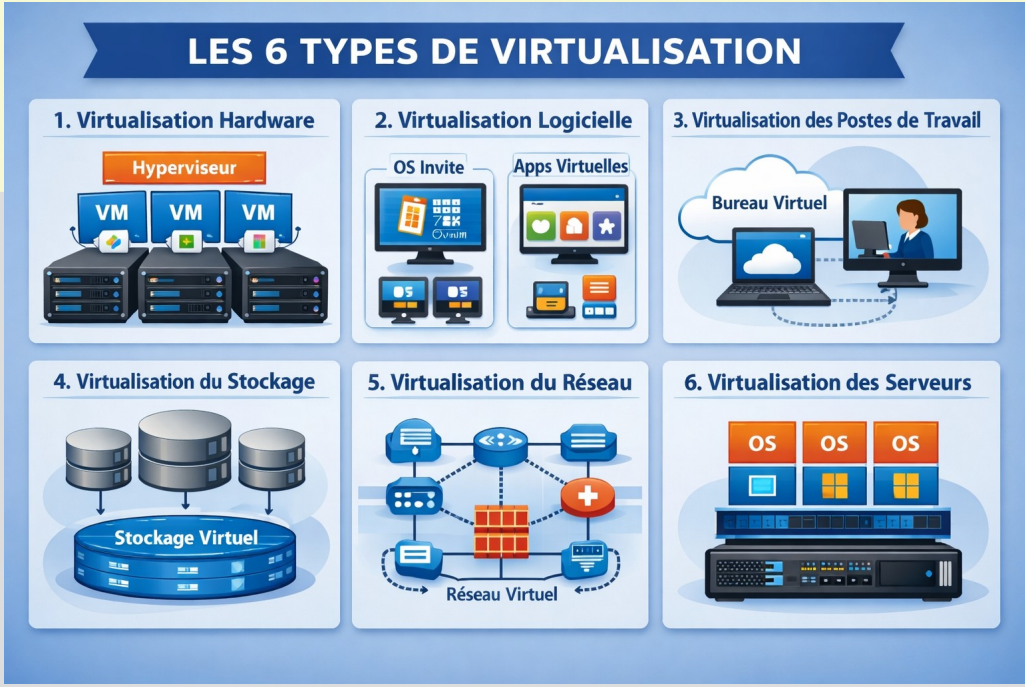
Regroupe plusieurs systèmes de stockage en un espace unifié.
Masque la complexité physique du stockage.
Utilisé pour sauvegarde, archivage, reprise après sinistre.
Avantages : performance, réduction des temps d'arrêt, gestion centralisée.

5️⃣ Virtualisation du réseau

Reproduction logicielle d'un réseau physique.
Division de la bande passante en canaux isolés.
Simplifie la gestion et améliore la sécurité.
Avantages : supervision facilitée, segmentation, isolation des flux.

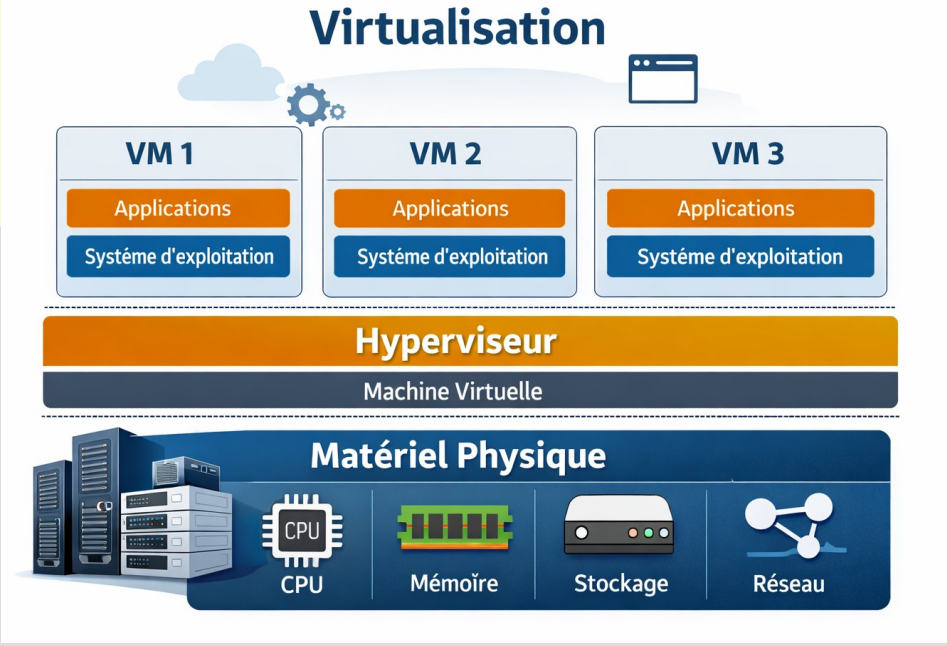
6️⃣ Virtualisation des serveurs

Très proche de la virtualisation hardware, mais centrée sur l'optimisation des serveurs.
Plusieurs OS sur un même serveur physique.
Réduit la prolifération des serveurs physiques.
Avantages : économies importantes, simplification de la gestion, meilleure disponibilité.



La virtualisation est un pilier de l'agilité informatique :
meilleure utilisation des ressources,
réduction des coûts,
haute disponibilité,
flexibilité,
adoption facilitée de nouvelles technologies.
Elle permet de garantir que les applications restent accessibles même en cas de panne d'un serveur, grâce au redémarrage automatique des VM sur un autre hôte.

2. virtualisation



🧩 Définition

La virtualisation permet d'exécuter plusieurs machines virtuelles (VM) sur un même matériel physique, chacune avec son propre système d'exploitation.

Architecture

Matériel physique

OS hôte

Hyperviseur (Type 1 ou Type 2)

VM

OS invité

Applications

Avantages

Isolation forte

Sécurité élevée

Support de plusieurs OS (Linux, Windows…)

Idéal pour serveurs, tests, environnements multiples

Limites

Consommation élevée (RAM, CPU)

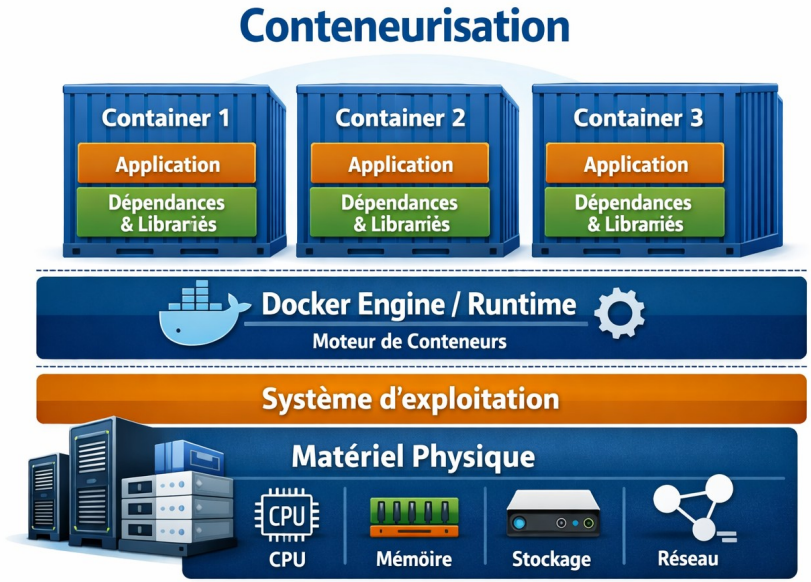
Démarrage lent

Redondance des OS invités

3. Conteneurisation

🧩 Définition

La conteneurisation isole des applications dans des environnements légers partageant le même noyau du système hôte.



Architecture

Matériel

OS hôte

Moteur de conteneurs (Docker, containerd, Podman…)

Conteneurs (processus isolés)

Avantages

Ultra léger

Démarrage instantané

Très portable

Parfait pour DevOps, microservices, CI/CD

Limites

Partage du noyau → moins isolé qu'une VM

Pas adapté aux OS différents

Sécurité dépendante du kernel

4. Émulation

Définition

L'émulation simule un matériel différent (CPU, architecture, périphériques).
Exemples : QEMU, émulateurs ARM, consoles, etc.

Avantages

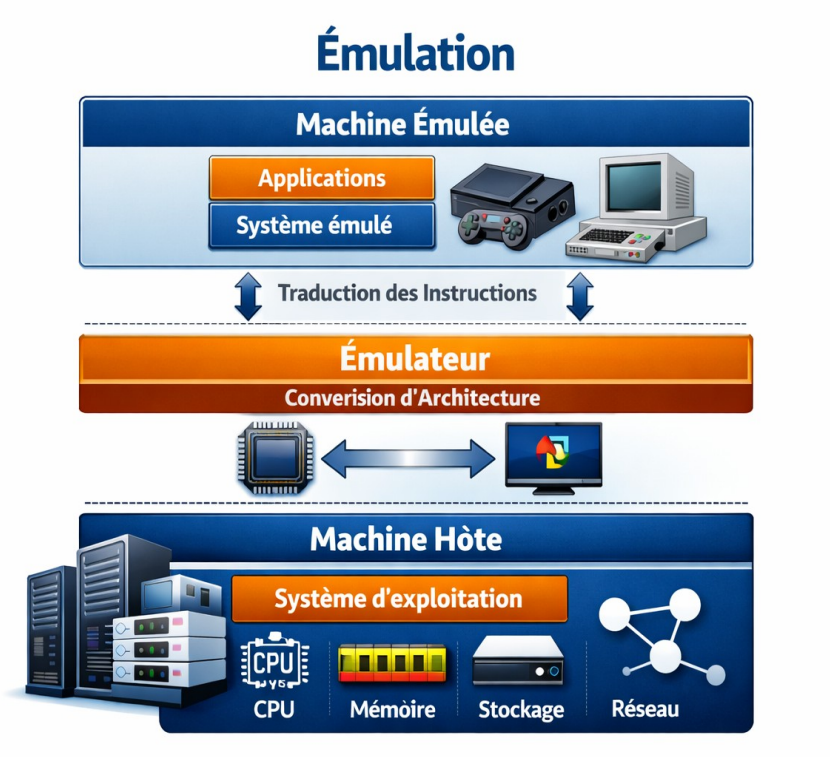
Permet d'exécuter un OS prévu pour un autre matériel

Indispensable pour tests embarqués, rétro-compatibilité, développement ARM/IoT

Limites

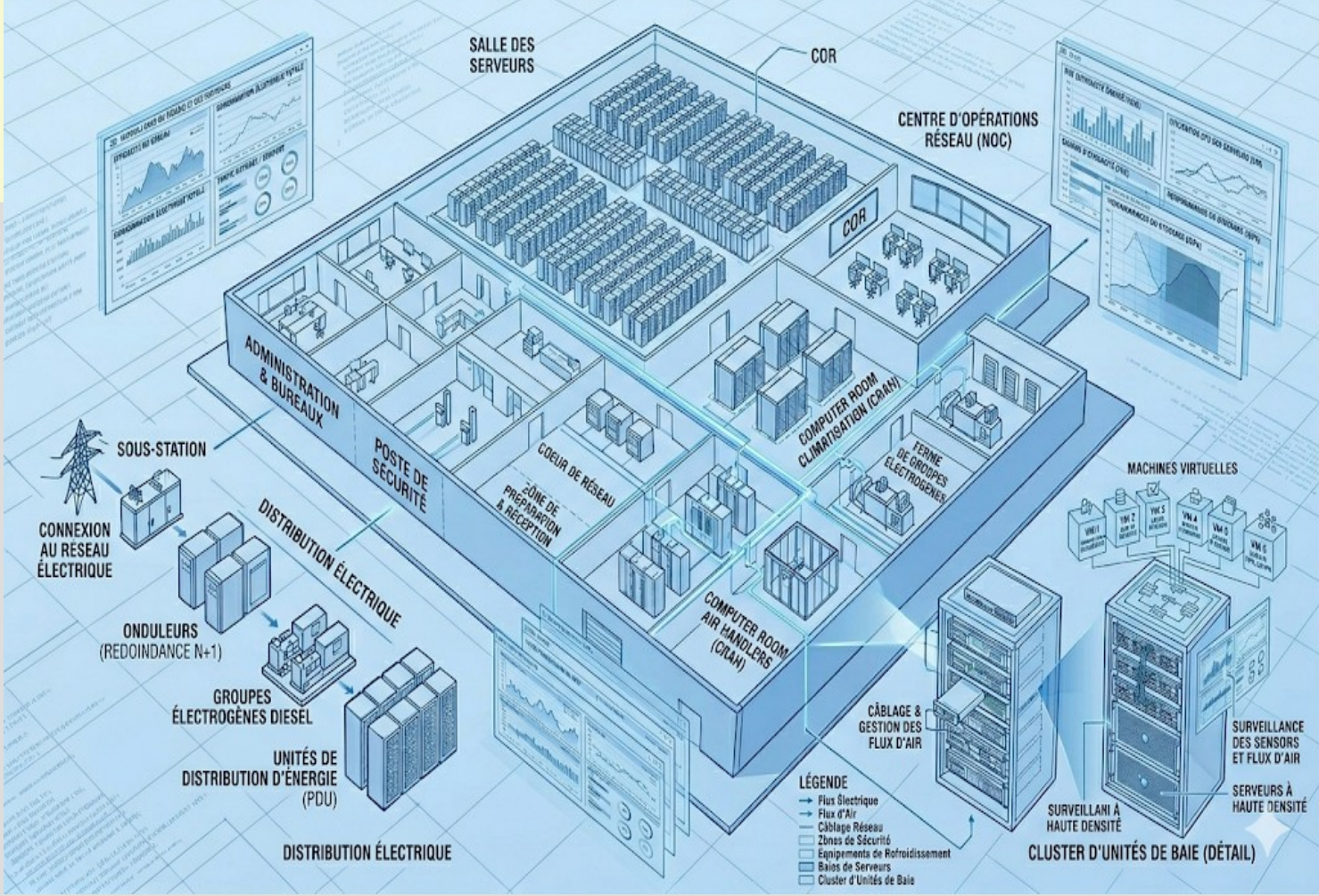
Performances réduites (traduction d'instructions)

Complexité de configuration

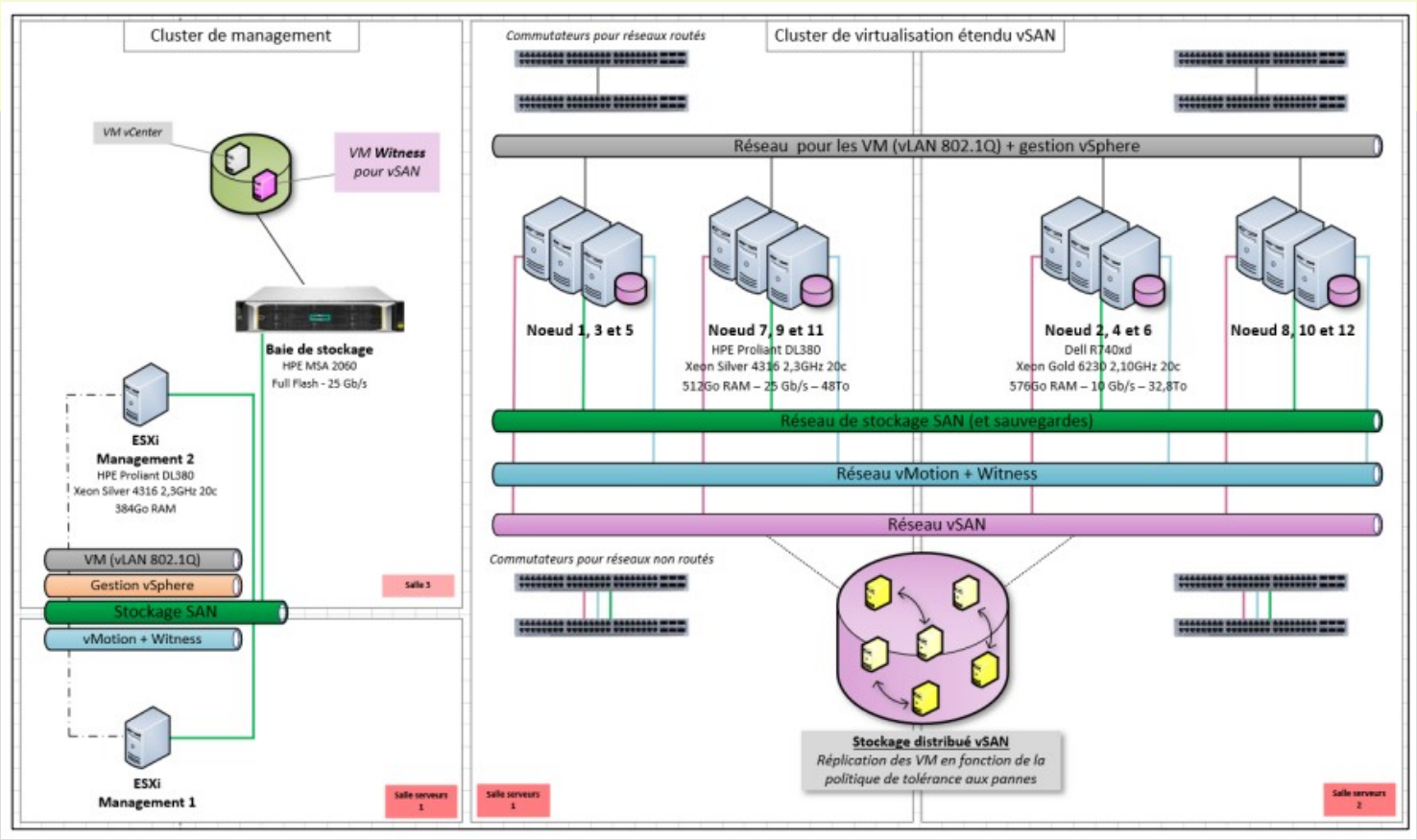


Exemple de virtualisation

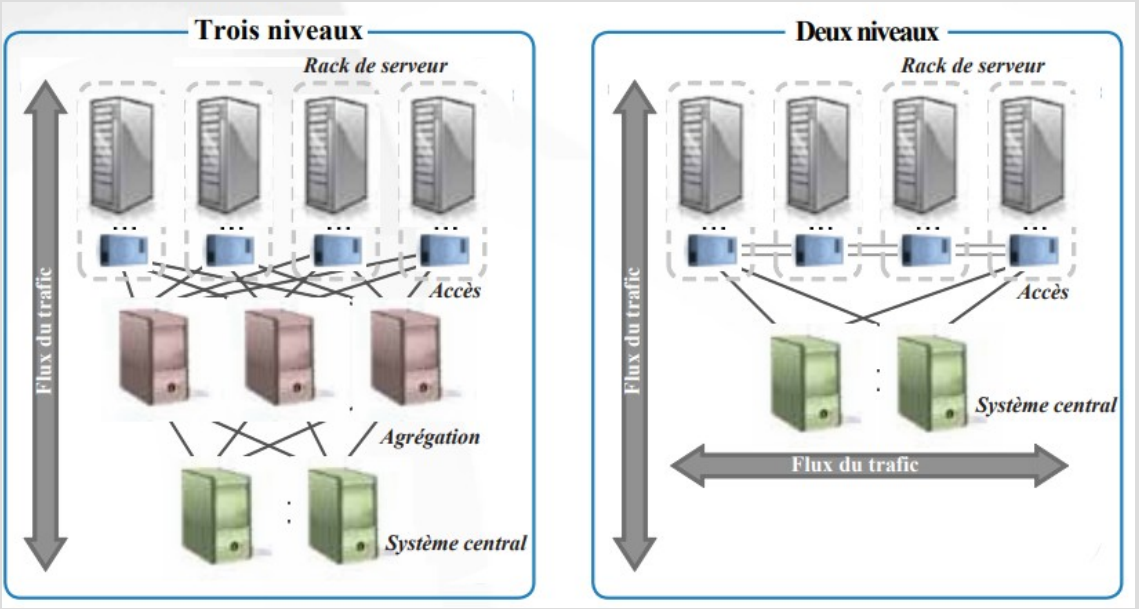
datacenter

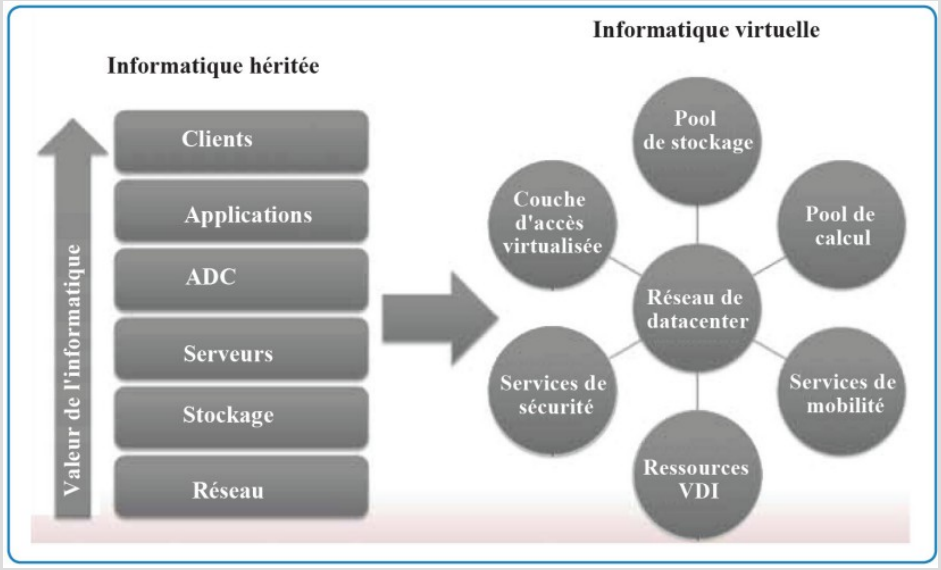

SALLE DES SERVEURS
COR
CENTRE D'OPÉRATIONS RÉSEAU (NOC)
ADMINISTRATION & BUREAUX
POSTE DE SÉCURITÉ
ZONE DE PRÉPARATION & RÉCEPTION
COEUR DE RÉSEAU
COMPUTER ROOM CLIMATISATION (CRAH)
FERME DE GROUPES ÉLECTROGÈNES
MACHINES VIRTUELLES
SOUS-STATION
CONNEXION AU RÉSEAU ÉLECTRIQUE
DISTRIBUTION ÉLECTRIQUE
ONDULEURS (REDOINDANCE N+1)
GROUPES ÉLECTROGÈNES DIESEL
UNITÉS DE DISTRIBUTION D'ÉNERGIE (PDU)
COMPUTER ROOM AIR HANDLERS (CRAH)
CÂBLAGE & GESTION DES FLUX D'AIR
SURVEILLANCE DES SENSORS ET FLUX D'AIR
SERVEURS À HAUTE DENSITÉ
LÉGENDE
Flux Électrique
Flux d'Air
Câblage Réseau
Zones de Sécurité
Equipements de Rofroidissement
Baies de Serveurs
Cluster d'Unités de Baie
DISTRIBUTION ÉLECTRIQUE
CLUSTER D'UNITÉS DE BAIE (DÉTAIL)

datacenter


Cluster de management
VM vCenter
VM Witness pour vSAN
Baie de stockage
HPE MSA 2060
Full Flash - 25 Gb/s
ESXi Management 2
HPE Proliant DL380
Xeon Silver 4316 2,3GHz 20c
384Go RAM
VM (vLAN 802.1Q)
Gestion vSphere
Stockage SAN
vMotion + Witness
ESXi Management 1
Commutateurs pour réseaux routés
Cluster de virtualisation étendu vSAN
Réseau pour les VM (vLAN 802.1Q) + gestion vSphere
Noeud 1, 3 et 5
Noeud 7, 9 et 11
HPE Proliant DL380
Xeon Silver 4316 2,3GHz 20c
512Go RAM – 25 Gb/s – 48To
Noeud 2, 4 et 6
Dell R740xd
Xeon Gold 6230 2,10GHz 20c
576Go RAM – 10 Gb/s – 32,8To
Noeud 8, 10 et 12
Réseau de stockage SAN (et sauvegardes)
Réseau vMotion + Witness
Réseau vSAN
Commutateurs pour réseaux non routés
Stockage distribué vSAN
Réplication des VM en fonction de la politique de tolérance aux pannes

datacenter


Trois niveaux
Rack de serveur
Flux du trafic
Accès
Agrégation
Système central
Deux niveaux
Rack de serveur
Flux du trafic
Accès
Système central
Flux du trafic


Informatique héritée
Informatique virtuelle
Valeur de l'informatique
Clients
Applications
ADC
Serveurs
Stockage
Réseau
Pool de stockage
Couche d'accès virtualisée
Pool de calcul
Réseau de datacenter
Services de sécurité
Services de mobilité
Ressources VDI