


R4.A.08 : Virtualisation

BUT 2 – Semestre 4

Volume horaire

- Cours : 4h (dont 1h d'évaluation)
- TD : 6h
- TP : 8h

contact : sautour.iut@gmail.com

Descriptif détaillé

Objectif

L'objectif de cette ressource est de comprendre les principes et enjeux de la virtualisation en informatique et d'être capable de déployer une solution de virtualisation. Cette ressource permettra de découvrir les techniques et outils utilisées pour la virtualisation de systèmes, amenant au déploiement de plateformes facilitant l'intégration et l'administration de services.

Savoirs de référence étudiés

- Types de virtualisation (serveur, application, réseau…)
- Outils de la virtualisation (hypervision, conteneurs…)
- Architectures virtualisées
- Les différents savoirs de référence pourront être approfondis

Indications de mise en œuvre

Cette ressource est largement identique à la ressource R4.B.08 et peut être mutualisée en partie, mais avec des horaires différents.

Virtualisation conteneurs hyperviseur

Introduction

Contexte

- L'approche CI/CD (Continuous Integration/Continuous Deployment) est une méthode permettant aux services IT de renforcer l'automatisation et la surveillance dans leur processus de création de logiciels et applications.

- Le mouvement DevOps consiste à renforcer la collaboration et la communication entre les développeurs d'applications et les équipes chargées des opérations et de la production, en automatisant le processus de livraison de (micro)logiciels et les changements d'infrastructure.

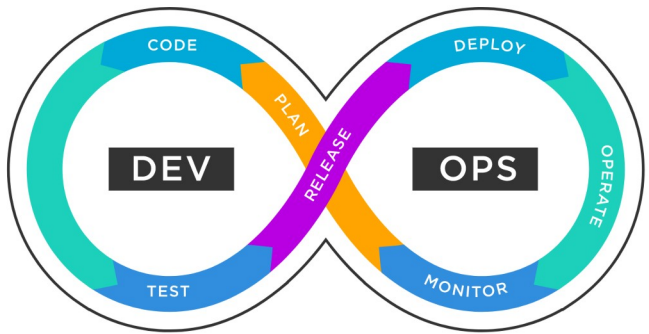
Ils s'appuient sur l'utilisation d'outils performants : GIT, Ansible, Puppet, Chef, Jenkins, Terraform, Docker, Kubernetes, OpenShift, ELK, ...

Objectifs

Découvrir les techniques et outils de la virtualisation

Installer et utiliser un environnement de virtualisation

Dockériser une application web



Introduction

Qu'est-ce que la virtualisation ?

La virtualisation est l'abstraction des ressources informatiques physiques telles que le matériel, les logiciels, le stockage et les composants réseau.

Un « composant » créé par une technique de virtualisation est un composant logique ou virtuel (VNIC, VSwitch, VM, LVM…). Il peut être utiliser, possède les mêmes fonctions et le même fonctionnement que son équivalent bien réel.

Ainsi un élément unique peut apparaître comme plusieurs éléments virtuels

OU

Plusieurs éléments peuvent apparaître comme un unique élément virtuel

Exemples ?

Introduction

Qu’est-ce qui est virtualisé ?

Presque tout…

La virtualisation touche de nombreux domaines comme par exemple :

Les postes de travail, les applications, le stockage, les données, les réseaux, les serveurs, les systèmes d’exploitation, etc.

Virtualisation ≠ Cloud Computing

Un mot sur le cloud

Qu'est-ce que le cloud ?

« Un modèle permettant un accès réseau omniprésent, pratique et à la demande à un pool partagé de ressources informatiques configurables. On cite comme exemples: les réseaux, les serveurs, le stockage, applications et services. Ces derniers peuvent être rapidement provisionnés et libérés avec un effort de gestion minimal ou interaction avec le fournisseur de services.

Ce modèle de cloud est composé de cinq caractéristiques essentielles, trois modèles de service et quatre modèles de déploiement. »

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Un mot sur le cloud

Cinq caractéristiques essentielles

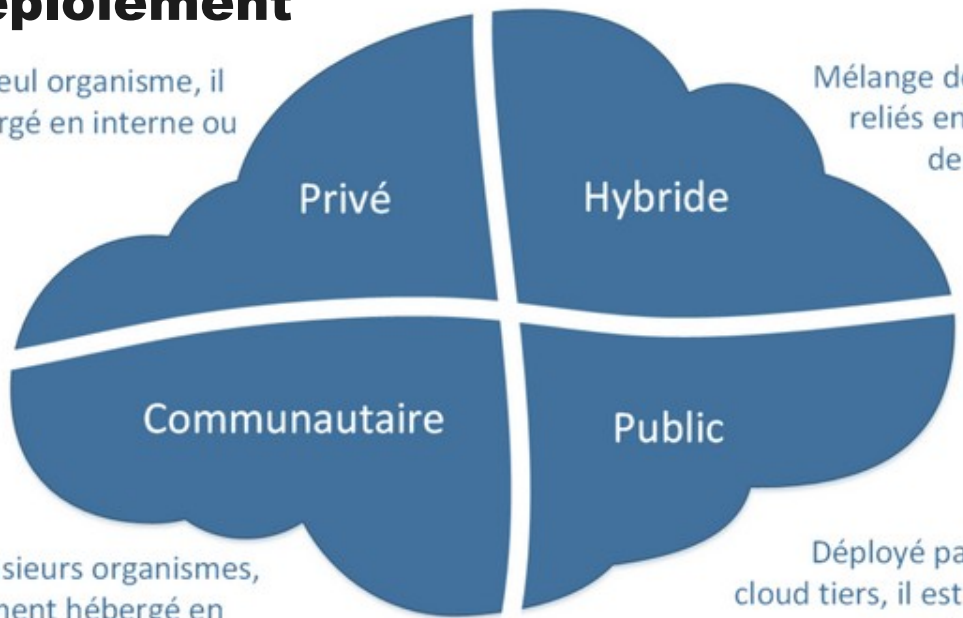
1. **Libre-service à la demande**
2. **Large accès au réseau**
3. **Mutualisation des ressources**
4. **Flexibilité, rapidité**
5. **Service mesuré**

Un mot sur le cloud

Quatre modèles de déploiement

Utilisé par un seul organisme, il peut être hébergé en interne ou en externe.

Mélange de plusieurs modèles de cloud reliés entre eux offrant les avantages des différents environnements.



Partagé par plusieurs organismes, il est généralement hébergé en externe, mais peut être hébergé en interne par un des membres.

Déployé par un fournisseur de cloud tiers, il est ouvert au public et partagé par les utilisateurs.

Un mot sur le cloud (pour AWS)

Modèles de déploiement de cloud computing

Cloud

Une application basée sur le cloud est entièrement déployée dans le cloud. Tous ses composants sont en outre exécutés dans le cloud. Les applications dans le cloud ont été créées dans le cloud ou migrées à partir d'une infrastructure existante pour tirer parti des avantages du cloud computing. Les applications basées sur le cloud peuvent être créées sur des éléments d'infrastructure de niveau inférieur ou utiliser des services de niveau supérieur qui fournissent une abstraction des exigences en matière de gestion, d'architecture et de dimensionnement de l'infrastructure de base.

Hybride

Un déploiement hybride permet de relier une infrastructure et des applications entre des ressources basées sur le cloud et des ressources existantes qui ne se trouvent pas dans le cloud. La méthode la plus courante de déploiement hybride consiste à associer cloud et infrastructure existante sur site pour étendre et développer l'infrastructure d'une organisation dans le cloud tout en connectant les ressources de cloud au système interne. Pour plus d'informations sur la façon dont AWS peut vous aider dans le cadre de votre déploiement hybride, consultez la page relative aux architectures hybrides.

Sur site

Le déploiement de ressources sur site à l'aide de la virtualisation et d'outils de gestion des applications est parfois appelé « cloud privé ». Le déploiement sur site ne présente pas les avantages qu'offre le cloud computing, mais il est parfois souhaité pour sa capacité à fournir des ressources dédiées. Dans la plupart des cas, ce modèle de déploiement est identique à l'infrastructure informatique héritée et fait appel à la gestion des applications et aux technologies de virtualisation pour tester et accroître l'utilisation des ressources.

Un mot sur le cloud

Trois modèles de services

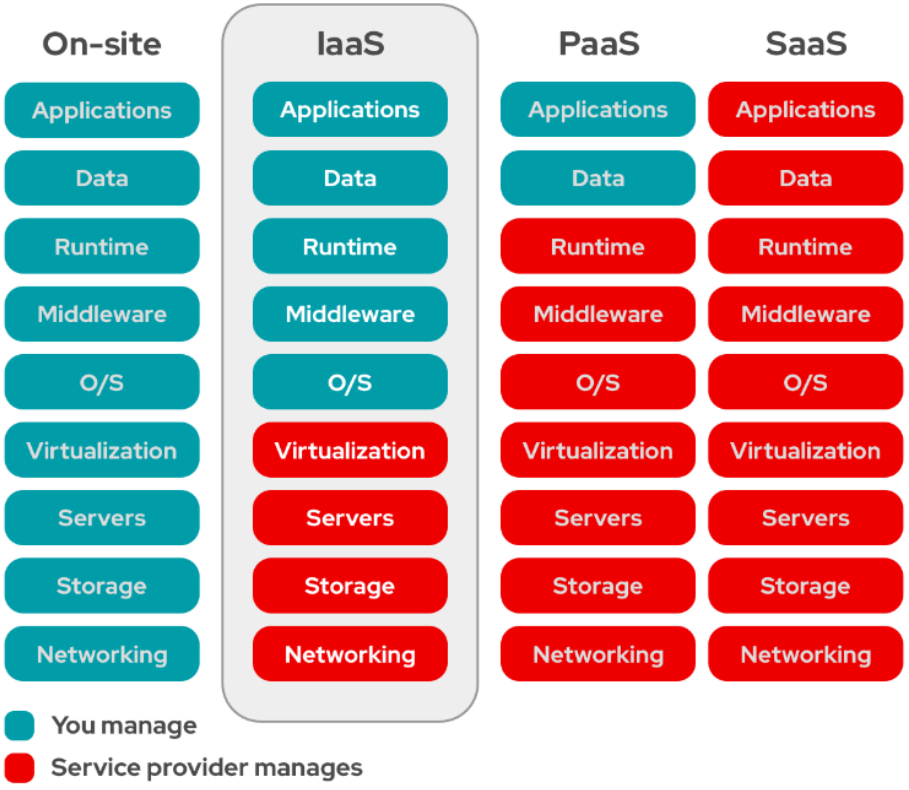
1. **IaaS : Infrastructure as a Service***
2. **PaaS : Platform as a Service**
3. **SaaS : Software as a Service**

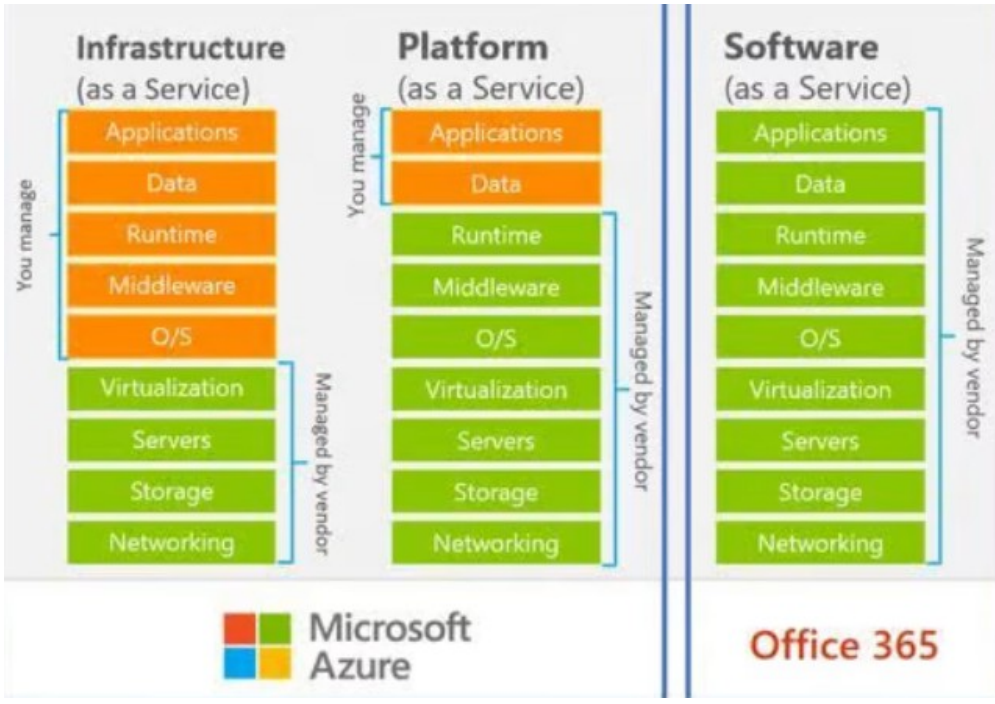
La mode du XaaS… « Everything as a Service », CaaS, DaaS, FaaS, KaaS… bref, on s'y perd.

https://www.auvik.com/franklyit/blog/aas-as-a-service-list/

*** L'expression « as-a-Service » signifie généralement qu'un tiers se charge de gérer un service à votre place, afin que vous puissiez vous concentrer sur des aspects plus importants.**

Un mot sur le cloud





Un mot sur le cloud

IaaS : Infrastructure as a Service

Il apporte aux utilisateurs tous les avantages des ressources informatiques sur site, sans les frais de gestion.

Dans le modèle IaaS, les utilisateurs gèrent :

- Les applications,
- les données,
- le système d'exploitation,
- les middlewares,
- les environnements d'exploitation.

Le fournisseur de solution d'IaaS fournit les fonctions de virtualisation, le système de stockage, les réseaux et les serveurs. Ainsi, l'utilisateur n'a pas besoin d'un datacenter sur site et n'a pas à s'inquiéter des mises à jour physiques ou de la maintenance de ces composants.

Un mot sur le cloud

PaaS : Platform as a Service

Ici, le matériel et la plateforme logiciel-application sont fournis et gérés par un prestataire de services extérieur.

L'utilisateur se charge lui-même de la gestion :

- Des applications,
- des données.

D'abord destiné aux développeurs et aux programmeurs, le PaaS offre à l'utilisateur une plateforme sur laquelle il peut développer, exécuter et gérer ses propres applications, sans avoir à créer ni entretenir l'infrastructure généralement associée au processus.

Un mot sur le cloud

PaaS : Platform as a Service

D'abord destiné aux développeurs et aux programmeurs, le PaaS offre à l'utilisateur une plateforme sur laquelle il peut développer, exécuter et gérer ses propres applications, sans avoir à créer ni entretenir l'infrastructure généralement associée au processus.

Exemple : L'offre PaaS d'Azure : App Service

https://azure.microsoft.com/fr-fr/products/app-service/#overview

**« Créez, déployez et mettez à l'échelle rapidement des applications web et des API selon vos termes.
Utilisez .NET, .NET Core, Node.js, Java, Python ou PHP dans des conteneurs ou exécutés sur Windows ou Linux. »**

Un mot sur le cloud

SaaS : Software as a Service

C’est un service qui permet d'utiliser une application web, gérée par le prestataire de services, généralement à travers un navigateur web et accessible sur des devices différents.

Dans ce modèle de service, l’utilisateur n’a plus rien à gérer.

Les mises à jour logicielles, les corrections de bogues et les autres tâches de maintenance logicielle sont prises en charge par le fournisseur.

Avec le SaaS, plus besoin d'installer une application localement sur l'ordinateur de chaque utilisateur. Ainsi, vous pouvez améliorer les méthodes d'accès au logiciel par un groupe ou une équipe

Un mot sur le cloud (pour AWS)

Infrastructure en tant que service (Infrastructure as a Service, IaaS)

L'infrastructure en tant que service (IaaS) contient les blocs de construction fondamentaux de l'informatique dans le cloud et donne habituellement accès à des fonctionnalités de mise en réseau, à des ordinateurs (virtuels ou sur du matériel dédié) et à de l'espace de stockage de données. Le service IaaS offre le niveau le plus élevé de flexibilité et de contrôle de gestion en ce qui concerne les ressources informatiques. Ce services est très similaire aux ressources informatiques existantes avec lesquelles les services informatiques et les développeurs sont aujourd'hui familiarisés.

Plate-forme en tant que service (PaaS)

Grâce au service PaaS, les entreprises n'ont plus besoin de gérer l'infrastructure sous-jacente (en règle générale, le matériel et les systèmes d'exploitation) et vous pouvez vous concentrer sur le déploiement et la gestion de vos applications. Vous êtes ainsi plus efficace, car vous n'avez pas à vous soucier de l'approvisionnement des ressources, de la planification des capacités, de la maintenance logicielle, de l'application de correctifs ou de toute autre charge indifférenciée liée à l'exécution de votre application.

Logiciel en tant que service (SaaS)

Le logiciel en tant que service offre un produit final qui est exécuté et géré par le prestataire de services. Dans la plupart des cas, les personnes qui font référence au service Saas pensent aux applications des utilisateurs finaux. Avec une offre SaaS, vous n'avez pas à vous soucier de la gestion du service ou de celle de l'infrastructure sous-jacente. Vous devez juste réfléchir à l'utilisation de ce logiciel spécifique. Une messagerie Web dans laquelle vous pouvez envoyer et recevoir des e-mails sans avoir à gérer des ajouts de fonctionnalités ni à effectuer la maintenance des serveurs et des systèmes d'exploitation sur lesquels elle s'exécute est un exemple courant d'application SaaS.

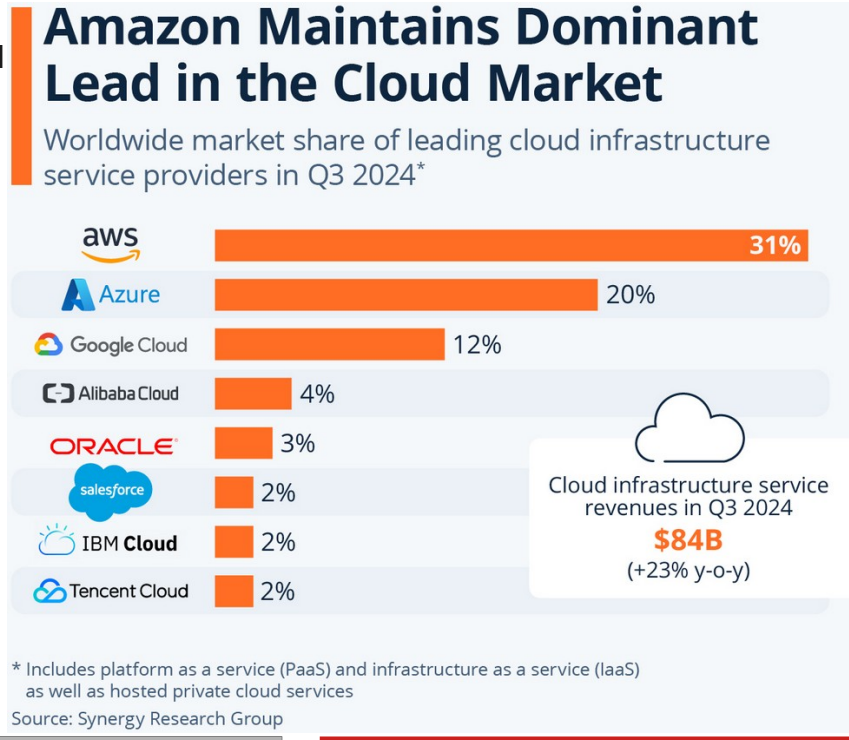
Un mot sur le cloud

Les fournisseurs de cloud sont des entreprises qui mettent en place des clouds publics, gèrent des clouds privés ou proposent des composants de cloud computing à la demande (ou services de cloud computing), notamment des IaaS, des PaaS et des SaaS.

Comparés à un service informatique sur site, les services cloud réduisent le coût des processus métier.

Quelques exemples

AWS (Amazon Web Services), Microsoft Azure, Google Cloud, Alibaba Cloud, IBM Cloud, OVHcloud, Leviia



Un mot sur le cloud

Quelques solutions cloud privé open-source

1. **Open Stack.**
2. **Cloud Stack.**
3. **Open Nebula.**

openstack®

apachecloudstack™
open source cloud computing

Pour faire court

Dans les infrastructures cloud qu'ils fournissent aux utilisateurs, les prestataires de services cloud dissocient les capacités de calcul des composants matériels, en séparant par exemple :

- la puissance de traitement des processeurs (CPU),
- la mémoire vive RAM,
- la puissance de traitement graphique (GPU),
- Le volume du stockage de données, ...

Cette séparation est rendue possible par la virtualisation.

La virtualisation est une technique indispensable à la mise en œuvre d'un service de cloud. Elle est nécessaire mais non suffisante.

La mise en œuvre d'un service de cloud est une application des technologies de virtualisation, mais ce n'est pas la seule.

La virtualisation

La virtualisation touche un grand nombre de domaines

- **Les postes de travail**
- **Les applications**
- **Le stockage**
- **Les réseaux**
- **Les serveurs**
- **Les systèmes d'exploitation**

La virtualisation des postes de travail

Pratique « ancienne » : une entreprise met à disposition d'un employé son propre poste de travail qu'il faut installer, configurer, sécuriser, remplacer, etc.

Il faut donc du temps (humain) et de l'argent (humain + matériel)

Dans un but « d'économies », le concept de virtualisation des postes de travail a vu le jour.

Concept : Diffuser des environnements de bureau par le réseau et centraliser leur gestion, dans un contexte d'entreprise.

La virtualisation des postes de travail

Structure client-serveur, transfert des données par le réseau.

Plusieurs techniques existent :

- **VDI**
- **Poste de travail virtuel sur le client**
- **Streaming d'OS**
- **DaaS***

Plusieurs acteurs :

- Citrix Virtual Apps and Desktops
- Vmware Horizon
- Parallels Remote App Server

- *Amazon WorkSpaces
- *Azure Virtual Desktop

La virtualisation des applications

Infrastructure de postes de travail virtuels : VDI

→ Exécution des postes de travail virtuels sur un serveur

→ Décorrélation du système avec la machine

Le serveur fournit l'environnement de bureau et les applications en cours d'exécution

1 utilisateur = 1 machine virtuelle persistante

Nombreux types de clients possibles (PC, Tablettes, smartphones / Thin-Clients / Zero-Client)

Personnalisation du poste de travail quasiment identique à une machine « locale »

La virtualisation des applications

Autres solutions

1. **Machines virtuelles exécutées sur le client**

   → **Requiert un hyperviseur sur le client**

   → **Synchro régulières avec une image d'OS sur serveur**

2. **Streaming d'OS**

   → **Le système est exécuté sur le client local**

   → **Mais démarré à partir d'une image système récupérée sur un serveur**

La virtualisation des applications

Avantages

- **Administration centralisée et simplifiée des postes de travail**
- **Accès utilisateur à partir d'une multitude de périphériques**
- **Sauvegardes et données centralisées**
- **Réduction des coûts sur le long terme (matériel et gestion)**
- **Infrastructures robustes et redondées**

Inconvénients

- **Connexion constante au réseau, impossibilité d'utilisation du poste non connecté.**
- **Performances des serveurs (calcul et stockage)**
- **Coûts des serveurs et du stockages important**
- **Complexe à déployer**

La virtualisation du stockage

En pratique dans des environnements virtuels (serveurs de virtualisation), le stockage (e.g. des VM) peut être local (DAS) ou en réseau (NAS, SAN).

Dans le cas du DAS, un système hôte (Gestionnaire de volume de l'hyperviseur ou hyperviseur de stockage) présente un système abstrait de lecteurs virtuels aux systèmes invités.

Fonctions de création de lecteurs virtuels disponibles sur tous les OS :

- **Linux : LVM**
- **Windows : LDM**
- **MacOS : CoreStorage**
- **ESXi : Vsphere permet la virtualisation des stockages**

La virtualisation du stockage

Cas des NAS : Network Attached Storage

- → **Serveur de stockage en réseau constitué de :**
  - → **HDD et/ou SSD,**
  - → **Contrôleurs RAID (Redondancy Array of Independant Disks),**
  - → **Un OS (Linux) un logiciel NAS**

But : Fournir une unité de stockage unique et redondée à partir de plusieurs disques logiques

La virtualisation du stockage

Cas des SAN : Storage Area Network

→ Réseau de stockage entre des serveurs et des unités de stockage (HDD, SSD, baies de sauvegarde, lecteurs de bandes)

→ Gestion de stockage virtuel centralisé

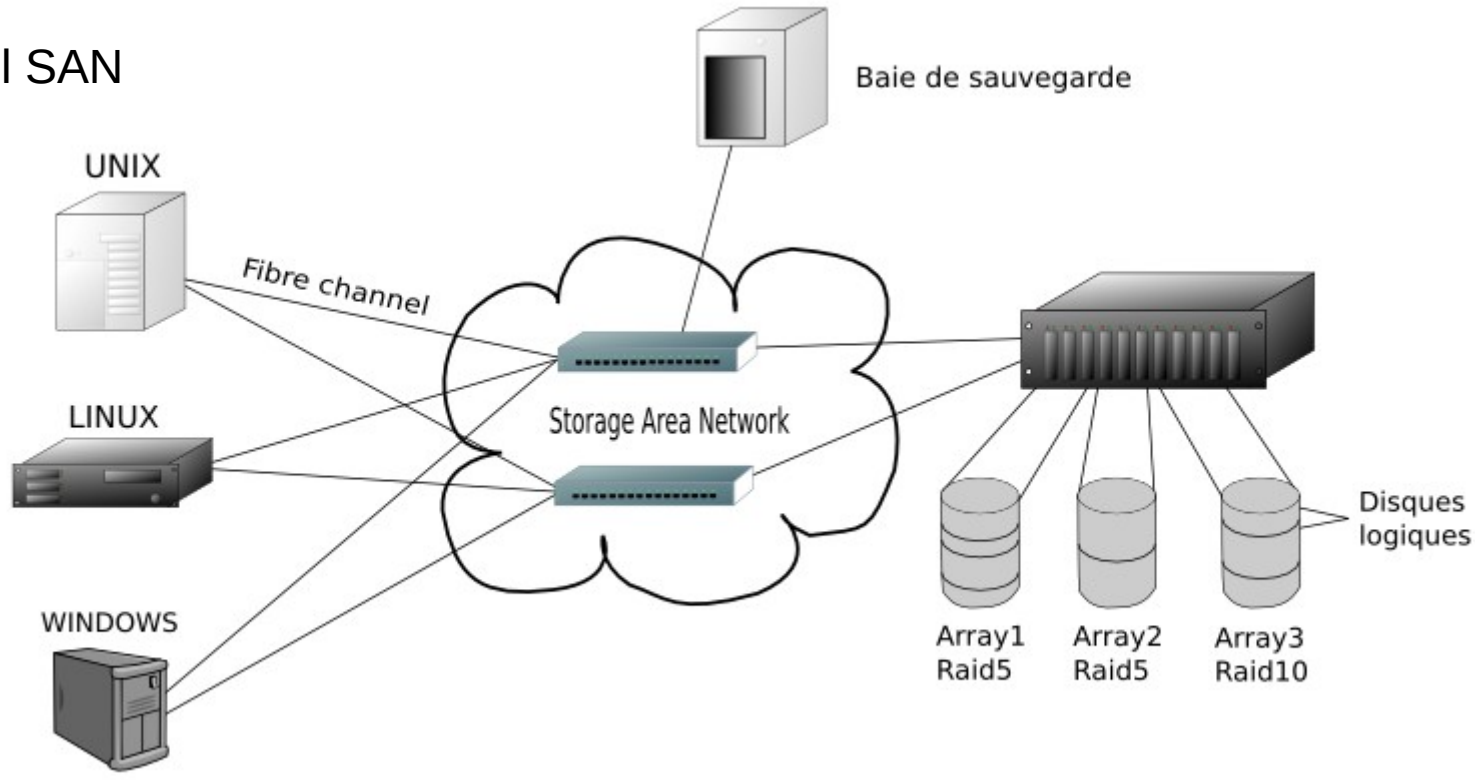
→ Réseau THD : switch fibre + FC

→ Un contrôleur gère l'accès au système de stockage virtuel

→ Forte évolutivité

La virtualisation du stockage

Réseau Fibre Channel SAN



La virtualisation du stockage

Software Defined Storage : SDS

Unifier les différentes ressources de stockage afin de les rendre disponible comme des pools unifiées de stockage pour les utilisateurs et les applications.

Une solution de virtualisation établit ainsi une couche d'abstraction entre les différents supports de stockage physiques et le niveau logique, sur lequel les ressources de stockage combinées peuvent être gérées de manière centralisée par logiciel.

E.g. SANsymphony (Stockage bloc) et vFilo (Stockage Fichier et objets)

La virtualisation du stockage

Avantages

Ressources utilisées plus efficacement

Optimisation des performances

Disponibilité élevée (redondance) → High Availability

Homogénéisation des périphériques de stockage différents

Flexibilité

La virtualisation des réseaux

La virtualisation dans les réseaux

- **VPN : Virtual Private Network**

1998

- **VLAN : Virtual Local Area Network**

2014 +

- **SDN : Software Defined Networking**
- **VXLAN : Virtual eXtensible Local Area Network**
- **NFV : Network Functions Virtualisation**

La virtualisation des réseaux

Juste pour la culture

SDN : Software Defined Networking

Le SDN sépare les deux plans des périphériques réseau, en déplaçant le plan de contrôle qui détermine où envoyer le trafic vers le logiciel, et en laissant le plan de données qui transmet effectivement le trafic dans le matériel.

Une architecture SDN standard est constituée de trois éléments :

1. Applications : elles communiquent des demandes de ressources ou des informations sur l'ensemble du réseau au contrôleur, via une API (e.g. REST))

2. Contrôleurs : ils utilisent les informations provenant des applications pour décider de l'acheminement d'un paquet de données (e.g. Protocole OpenFlow)

3. Périphériques réseau : ils reçoivent des informations du contrôleur sur l'endroit où déplacer les données

La virtualisation des réseaux

Juste pour la culture

NFV : Network Function Virtualisation

La virtualisation des fonctions réseau (e.g. le routage, les pare-feux) désigne le remplacement du matériel des appliances réseau par des machines virtuelles qui exécutent des logiciels et des processus sous le contrôle d'un hyperviseur

En route vers le NaaS...

Initialement utilisées par les opérateurs, ces techniques se popularisent dans les datacenters, la téléphonie mobile, les IoT...

Elles présentent de nombreux avantages : scalabilité, flexibilité, sécurité, réduction des coûts, etc...

Les VLAN (Virtual Local Area Networks)

Limites des réseaux physiques :

- **Architecture dépendante de la couche physique**
- **Évolution difficile**
- **Redondance des liens**
- **Coûts élevés (câblage)**
- **Exploitation lourde**

Les VLAN

1998 : Publication de la norme 802.1q

Idée : S'affranchir des limitations de l'architecture physique en définissant une segmentation logique basée sur un regroupement de machines grâce à des critères (numéros de port, adresses MAC, protocole).

Les VLAN sont donc une segmentation logique d'un réseau physique en plusieurs réseaux virtuels.

Les VLAN

Les buts sont multiples :

- **Réduire les domaines de diffusion / collision*,**
- **Améliorer les performances,**
- **Mise en œuvre simplifiée,**
- **Administration simplifiée,**
- **La réduction des coûts,**
- **Sécurité et confidentialité par séparation des flux.**

Un domaine de collision est une zone logique d'un réseau informatique où les paquets de données peuvent entrer en collision entre eux

Les VLAN

Les VLANS sont créés au niveau des commutateurs (switchs)

On distingue en général 3 types de VLAN :

- **Niveau 1** : VLAN par ports
- **Niveau 2** : VLAN par adresse MAC
- **Niveau 3** : VLAN par protocole de couche 3 (ex : IP)

Les VLAN

Les VLANS de niveau 1 (Par port)

Chaque port physique du commutateur est associé à un VLAN

+ Solution techniquement simple à mettre en place

- Manque de souplesse (Déplacement de machines ?)

Les VLAN

Les VLANS de niveau 2 (Par Adresse MAC)

Une adresse MAC (ou physique/ethernet) : Identifiant unique à chaque périphérique réseau attribuée par le constructeur codée généralement sur 48 bits.

On associe les adresses MAC des clients à un VLAN particulier.

+ Déplacement de machines aisé, souplesse

- Gestion d'une table de correspondance MAC ↔ VLAN

Les VLAN

Les VLANS de niveau 3 (par protocole e.g. IP)

Une adresse IP (plutôt un sous-réseau IP) est associé automatiquement à un VLAN particulier.

+ Solution simple et dynamique

- Problèmes de sécurité (changement IP = changement VLAN)

Les VLAN : un exemple simple

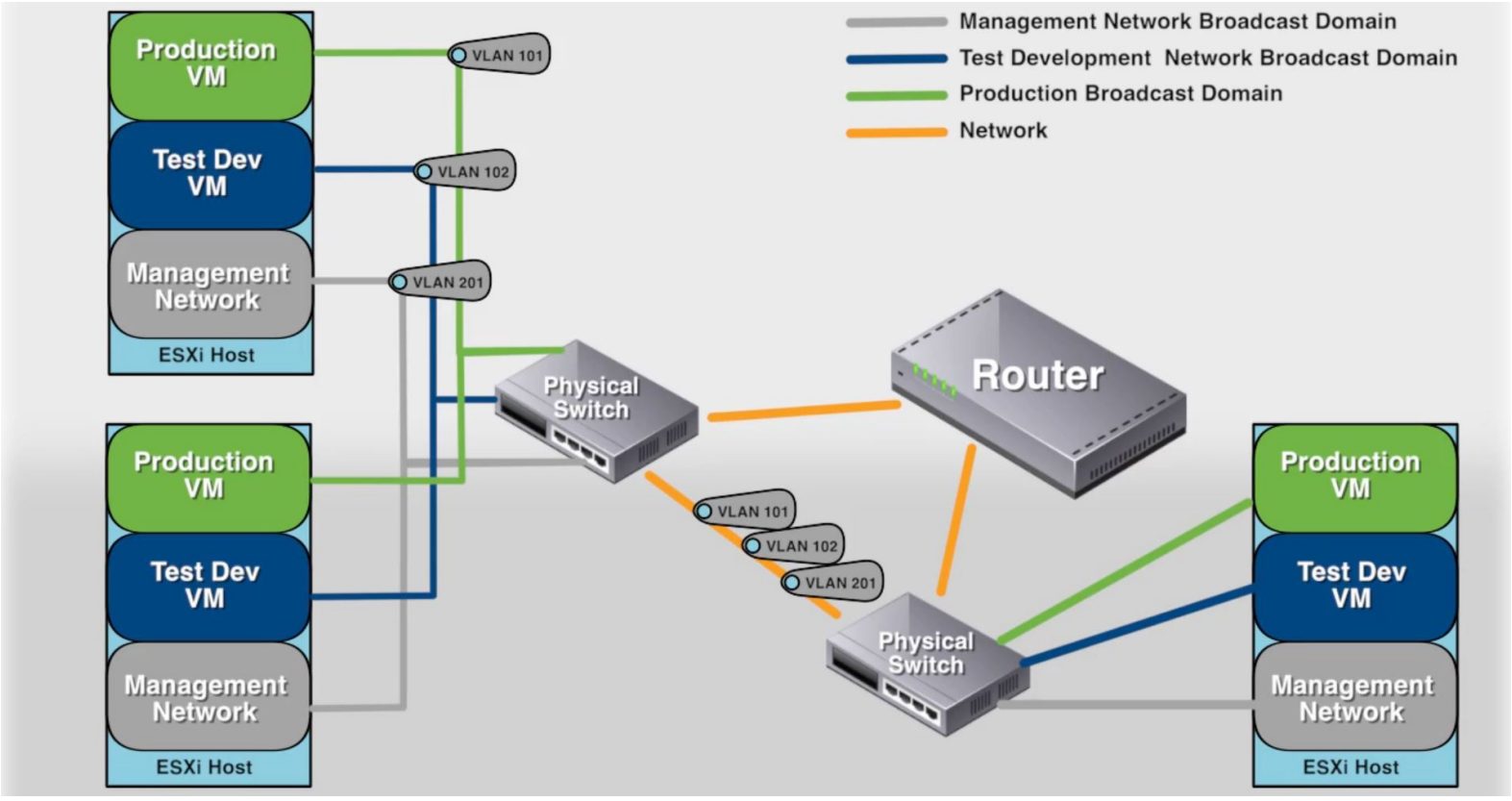


Schéma présentant les VLAN dans une infrastructure virtualisée avec Vmware ESXi

Documentation VMware

Les VLAN : un exemple simple

Un entreprise IT dispose de plusieurs serveurs de virtualisation, chacun d'entre eux contenant plusieurs Machines Virtuelles :

- Des machines de production
- Des machines de test
- Des machines d'administration

Sans VLAN :

- Toutes ces machines sont sur le même domaine de diffusion

- Les trames de diffusion (broadcast) seront diffusées sur tout les ports.

- Une machine de test sera sur la même réseau qu'un serveur en production ou que les machines d'administration.

Les VLAN : un exemple simple

Une solution consisterait à créer un réseau physique pour chaque « groupe de travail » (prod, test, management).

Bien que techniquement possible, bien que ce soit une bonne idée concernant la sécurité, cette solution est très lourde à mettre en place et très peu évolutive, cette solution est financièrement une mauvaise idée...

La solution : les VLAN

Les VLAN : un exemple simple

Dans la typologie par port

Un port = un VLAN, on parle alors de port en mode access (cisco) ou de port non-tagué, non-étiqueté, untagged

Si on reprend l'exemple précédent, on pourrait alors affecter un VLAN sur chaque port des switchs correspondant au réseau souhaité pour la machine connectée.

Il faudrait alors relier les switchs entre eux par plusieurs liens afin de permettre la communication entre les machines d'un même VLAN mais dans des « lieux » différents.

Les VLAN : un exemple simple

Dans cet exemple simple avec 3 machines par switch, 3 VLAN, c'est envisageable, mais imaginons un réseau segmenté en 10, 30, 200 VLAN ?

Dans ce dernier cas, il faudrait relier les switchs entre eux par 200 liens physiques ?

Est-ce vraiment raisonnable ?

Les VLAN : un exemple simple

Un port peut également transporter plusieurs VLAN, on parle alors de trunk (cisco) ou de port tagué, étiqueté, tagged.

Un trunk permet de faire circuler plusieurs VLAN sur le même lien physique, dans le cas ou un équipement voudrait accéder à plusieurs VLAN avec un seule interface physique, ou alors dans le cas de la liaison inter-switch.

Ces deux cas sont présents dans l'exemple.

Les VLAN : un exemple simple

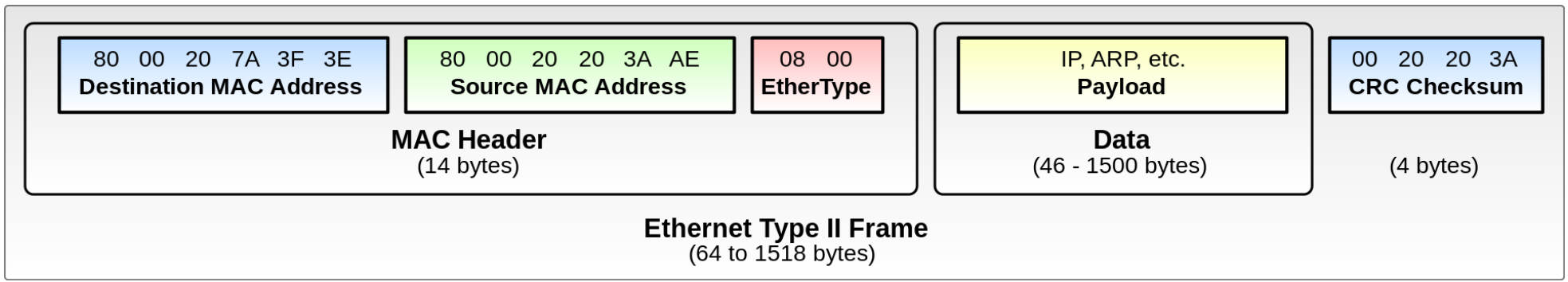
Cependant si plusieurs VLAN circulent sur un même lien physique entre deux switchs, il faut que les switchs sachent à quel VLAN appartient une trame.

Pourquoi ?

La norme 802.1q permet d'inclure un TAG dans les en-têtes ethernet habituelles.

Les VLAN : un exemple simple

Rappel : Format d'une trame ethernet II 802.3 « classique »

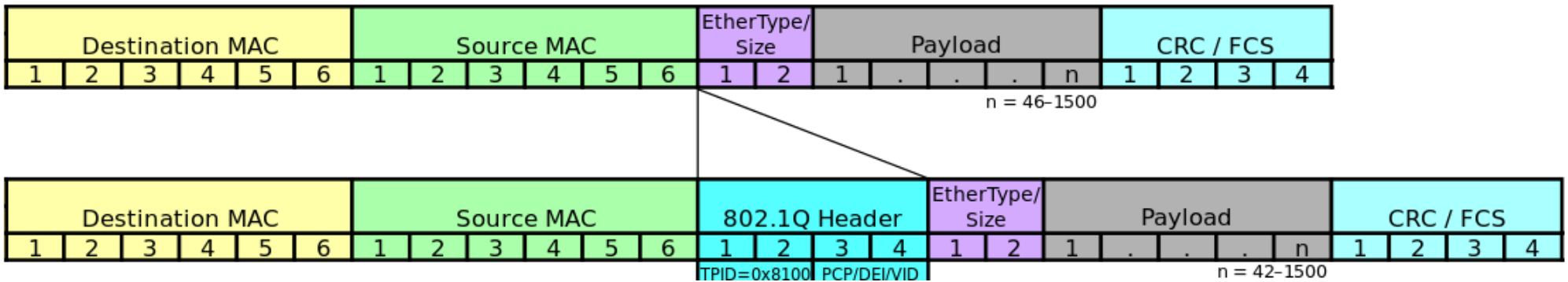


CRC : Contrôle de redondance cyclique

Ethertype : 0800 = IPv4

Les VLAN : un exemple simple

Comparaison avec une trame 802.1q



CRC : Contrôle de redondance cyclique

Ethertype : 0800 = IPv4

Les VLAN : un exemple simple

La balise 802.1q

802.1Q tag format

16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	DEI	VID

- TPID *(Tag protocol identifier)* : Les 16 premiers bits sont utilisés pour identifier le protocole de la balise insérée. Dans le cas de la balise 802.1Q la valeur de ce champ est fixée à 0x8100.

- PCP *(Priority Code Point)* : permet de mettre 8 niveaux de priorité (QoS), comme par exemple pour les applications de ToIP.

- DEI *(Drop Eligible Indicator)* : Indique si un paquet est susceptible de se faire drop en cas de congestion de réseau par exemple.

- VID *(VLAN ID)* : Numéro du VLAN

To be continued...

Partie 2

Virtualisation des serveurs

et

des systèmes d’exploitation

La virtualisation des serveurs

Qu’est ce qu’un serveur ?

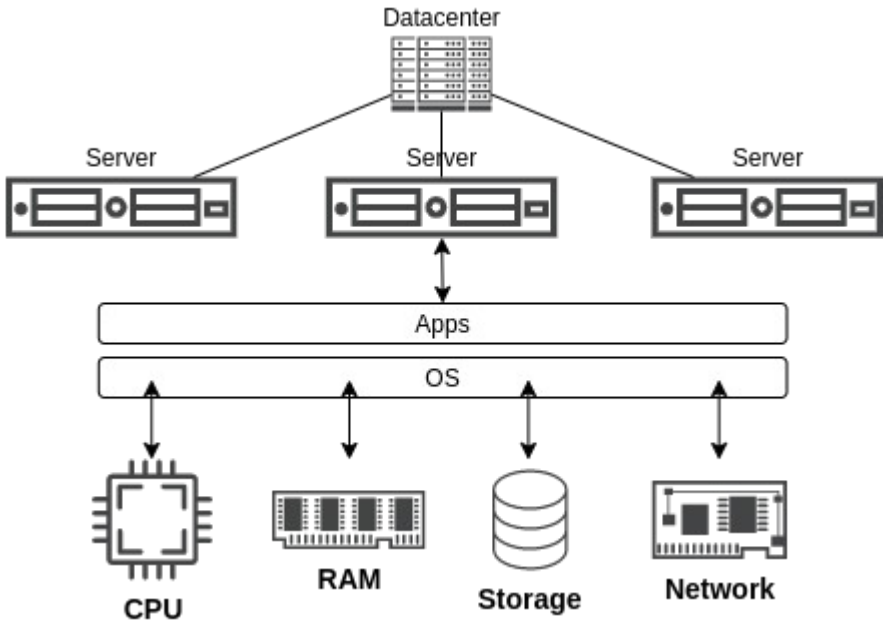
La virtualisation des serveurs

Qu’est ce qu’un serveur ?

Une machine (un ordinateur) dont le rôle est d’offrir un (des) service(s) à des clients

La virtualisation des serveurs

Un serveur est donc constitué des éléments principaux suivants :



CPU (Central Processing Unit): calcul / échange de données entre composants.

RAM (Random Access Memory): stocke temporairement les données nécessaires au processeur.

Stockage: Stocke les données à long terme.

Carte réseau (NIC) : gère et traite le trafic réseau

Différences avec un PC ?

La virtualisation des serveurs

Qu’est ce qu’un OS ?

La virtualisation des serveurs

Qu'est ce qu'un OS ?

Couche logicielle qui assure le lien entre les utilisateurs, les applications et les ressources matérielles.

Il est en charge (entre autre) de la :

- Gestion du processeur (CPU),
- Gestion de la mémoire vive (RAM),
- Gestion des entrées/sorties,
- Gestion des fichiers,
- Gestion du réseau...

La virtualisation des serveurs

Un datacenter ?

La virtualisation des serveurs

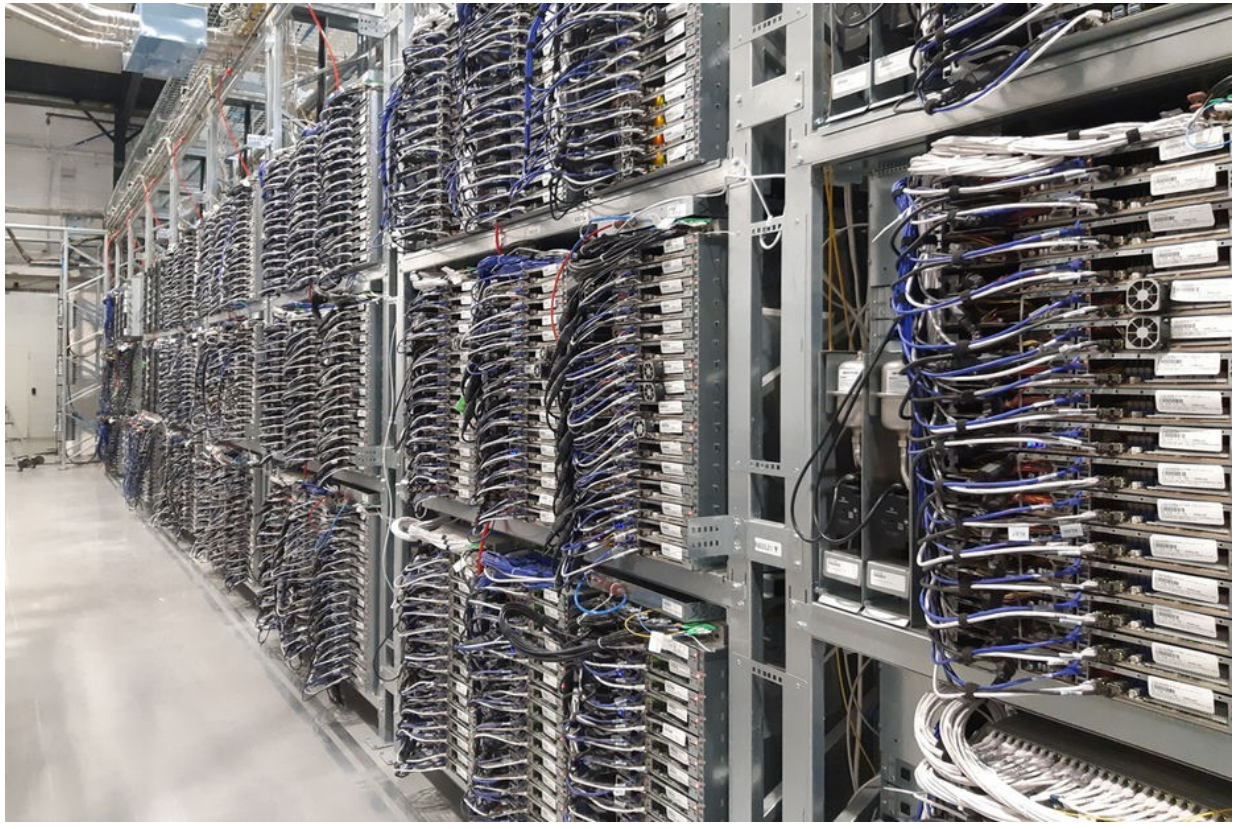
Un datacenter ?

« Un centre de données, ou centre informatique est un lieu (et un service) où sont regroupés les équipements constituants d'un système d'information (ordinateurs centraux, serveurs, baies de stockage, équipements réseaux et de télécommunications, etc.).

Ce regroupement permet de faciliter la sécurisation, la gestion (notamment l'exécution de calculs et le refroidissement) et la maintenance des équipements et des données stockées. »

wikipedia

La virtualisation des serveurs



La virtualisation des serveurs

Un peu d'histoire…

Il y a quelques années (+25), les serveurs possédaient des ressources « limitées ». Ils faisaient tourner 1 OS et une ou plusieurs applications.

Des bonnes pratiques se sont mises en place dans les grandes entreprises :

1 serveur = 1 application / service.

Puis les ressources matérielles ont très vite augmenté

- CPU → Augmentation du nombre de cœurs physique + Hyper-threading (2002)

Nombre de vCPU = Nb CPU x Nb coeurs x 2 (hyper-threading)

Nombre de vCPU = Nb CPU x Nb coeurs x TpC (Thread per Core)

i.e. Un serveur Bi-processeur Intel Xeon Platinum 8380 aura 160 vCPU

La virtualisation des serveurs

Maintenant, il n'est pas rare de trouver des serveurs avec :

- **+ de 100 vCPu**
- **Plusieurs centaines de Go de RAM (voire plusieurs To)**
- **Des dizaines / centaines de To de stockage**
- **Des bandes passantes publiques de +10Gb/s et privées de + 100Gb/s**

Tout ça pour faire tourner un serveur minecraft ?

→ Nope, pour faire de la virtualisation

La virtualisation des serveurs

La virtualisation des serveurs, c'est quoi ?

Ensemble des techniques permettant de faire fonctionner plusieurs systèmes d'exploitation sur une seule machine physique, comme s'ils fonctionnaient sur des machines physiques distinctes.

1 serveur physique → plusieurs serveurs virtuels

+ Optimisation matérielle avec Intel-VT et AMD-V qui permettent une partition du processeur afin d'exécuter plusieurs OS sur une même puce en même temps aidant ainsi les hyperviseurs dans leur gestion des machines virtuelles

https://www.intel.fr/content/www/fr/fr/virtualization/virtualization-technology/intel-virtualization-technology.html

La virtualisation des serveurs

Simulation

≠

Émulation

≠

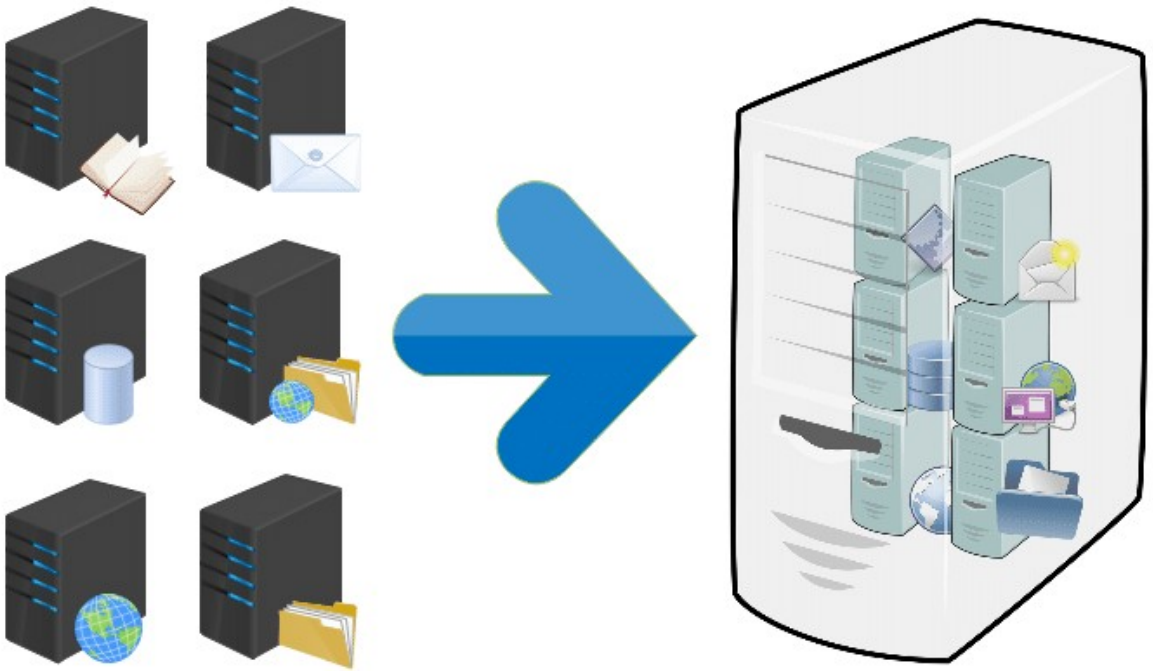
Virtualisation

Imite / modélise / prévoit de manière logicielle le comportement d'un matériel

reproduire de **manière logicielle** à l'identique le comportement d'un matériel

Utilisation du matériel d'un système hôte pour reproduire à l'identique le comportement d'un matériel (bien plus rapide que l'émulation)

La virtualisation des serveurs



Source : https://formip.com/virtualisation/

Idée :

Regrouper différents services sur une seule machine en conservant le cloisonnement qu'offrent des machines physiques séparées

Les applications *(serveurs web, ftp, smtp, db, ldap...)* auront l'« impression » d'être exécutées sur une machine physique dédiée

Comment ?

La virtualisation des serveurs

Un hyperviseur (ou gestionnaire de machines virtuelles) est un outil qui permet de créer, exécuter, gérer des machines virtuelles.

Il permet de partager « *virtuellement* » les ressources de la machine physique sur laquelle il est installé à plusieurs machines virtuelles.

Il assure une correspondance entre le CPU, la RAM et les périphériques de la machine hôte et ceux de la machine invitée.

La virtualisation des serveurs

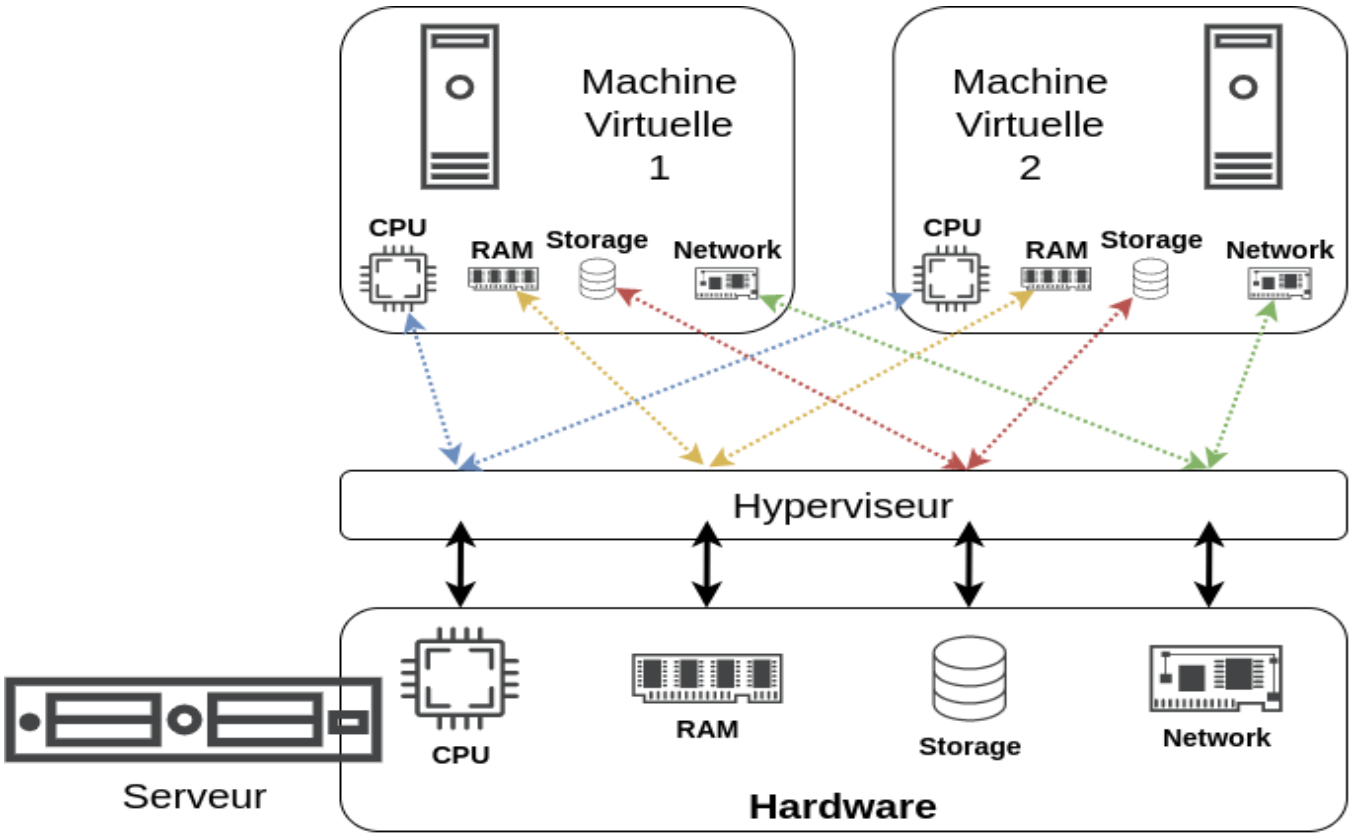
- Hyperviseur (hypervisor): Plateforme logicielle de virtualisation qui permet la création et l'exécution de plusieurs systèmes d'exploitation isolés sur une même machine physique.

- Système Hôte (host) = machine physique sur laquelle s'exécute l'hyperviseur et les machines virtuelles.

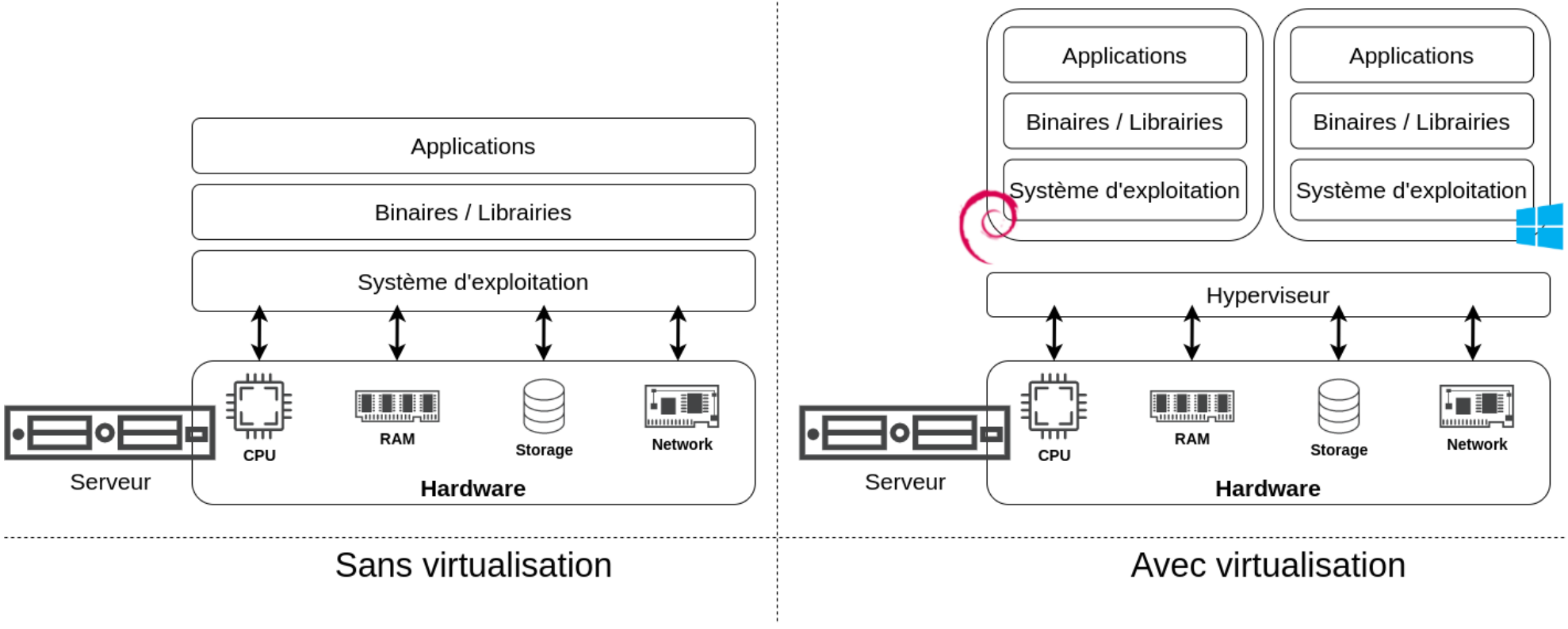
- Système Invité (guest) = Machine virtuelle créée par l'hyperviseur ou système d'exploitation installé à l'intérieur d'une machine virtuelle.

- Machine Virtuelle (VM) : Environnement entièrement virtualisé qui exécute son propre système d'exploitation et bénéficie des mêmes composants « virtuels » qu'une machine physique (CPU, RAM, Disques durs, NIC, etc...)

La virtualisation des serveurs



La virtualisation des serveurs



La virtualisation des serveurs

De nombreux buts à la virtualisation

1. **Une meilleure utilisation des ressources (Consolidation, mutualisation)**

Les serveurs ont de plus en plus de ressources et faire tourner quelques (voire une) applications sur un serveur est devenu *« overkill »*.

Des serveurs non virtualisés utilisent 10 % de leurs ressources.

Un serveur virtualisé peut les exploiter de manière plus efficiente (> 70 %)

Source : « trust me »

La virtualisation des serveurs

2. Réduction des coûts en tout genre (> 30%)

- **Les coûts des machines**
- **Les coûts d'exploitation et de maintenance**
- **La consommation électrique**
- **La climatisation**
- **Les câbles et équipements réseaux**
- **L'immobilier**
- **Licences**

La virtualisation des serveurs

3. Facilité de gestion et d'administration

- **Installation (des systèmes) beaucoup plus rapide**
- **Déploiement plus rapide et facile**
- **Sécurisation facilitée par l'isolement**
- **Gestion des Backups / snapshots**
- **Gestion du réseau (SDN, NFV)**

La virtualisation des serveurs

4. Amélioration des performances

- **Migration aisée d'une VM vers un autre serveur (à chaud - i.e. vMotion)**
- **Load balancing**
- **Réplication/redondance → haute disponibilité (HA)**
- **Scalabilité**
- **Flexibilité**
- **Automatisation (provisioning) → agilité**

La virtualisation des serveurs

5. Tests

- **Exécuter plusieurs OS différents en même temps**
- **Développer une application pour un autre système d'exploitation**
- **Tester le déploiement d'une application dans un environnement différent de l'environnement de développement**
- **Bidouiller un système d'exploitation sans risque**
- **Tester de nouveaux services**
- **Réaliser des POC (tester la faisabilité d'un projet)**
- **Réaliser des tests de PRA**

La virtualisation des serveurs

Quelques inconvénients / risques

- Le décloisonnement

→ Sortir de la Machine virtuelle et prendre la main sur la machine hôte

- Les attaques DDoS

→ Une VM se fait DDoS, c'est possiblement l'ensemble des VM qui trinquent...

- Un point unique de défaillance (SPOF)

→ Panne, mauvaise configuration = ...

→ Nécessite la réplication, load-balancing, la HA

La virtualisation des serveurs

Il existe plusieurs types de virtualisation dont :

Virtualisation « lourde »

→ Hyperviseur de type 1

→ Hyperviseur de type 2

Virtualisation « légère »

→ ou isolation

→ ou conteneurisation

La virtualisation des serveurs

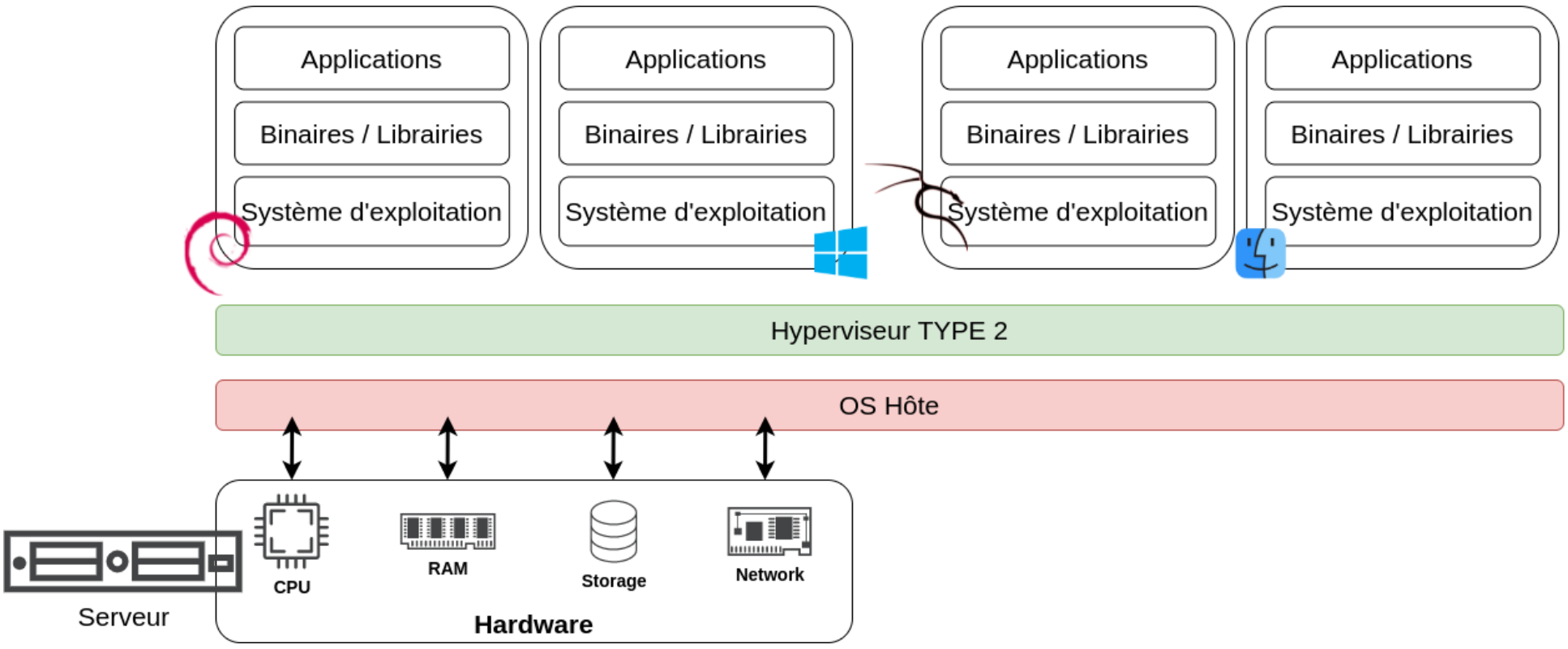
Hyperviseur de type 2 : « Hyperviseur hébergé »

C’est un logiciel (installé et exécuté sur un système d’exploitation) permettant de créer, gérer des machines virtuelles

Exemples : Celui que vous utilisez tous les jours → VirtualBox

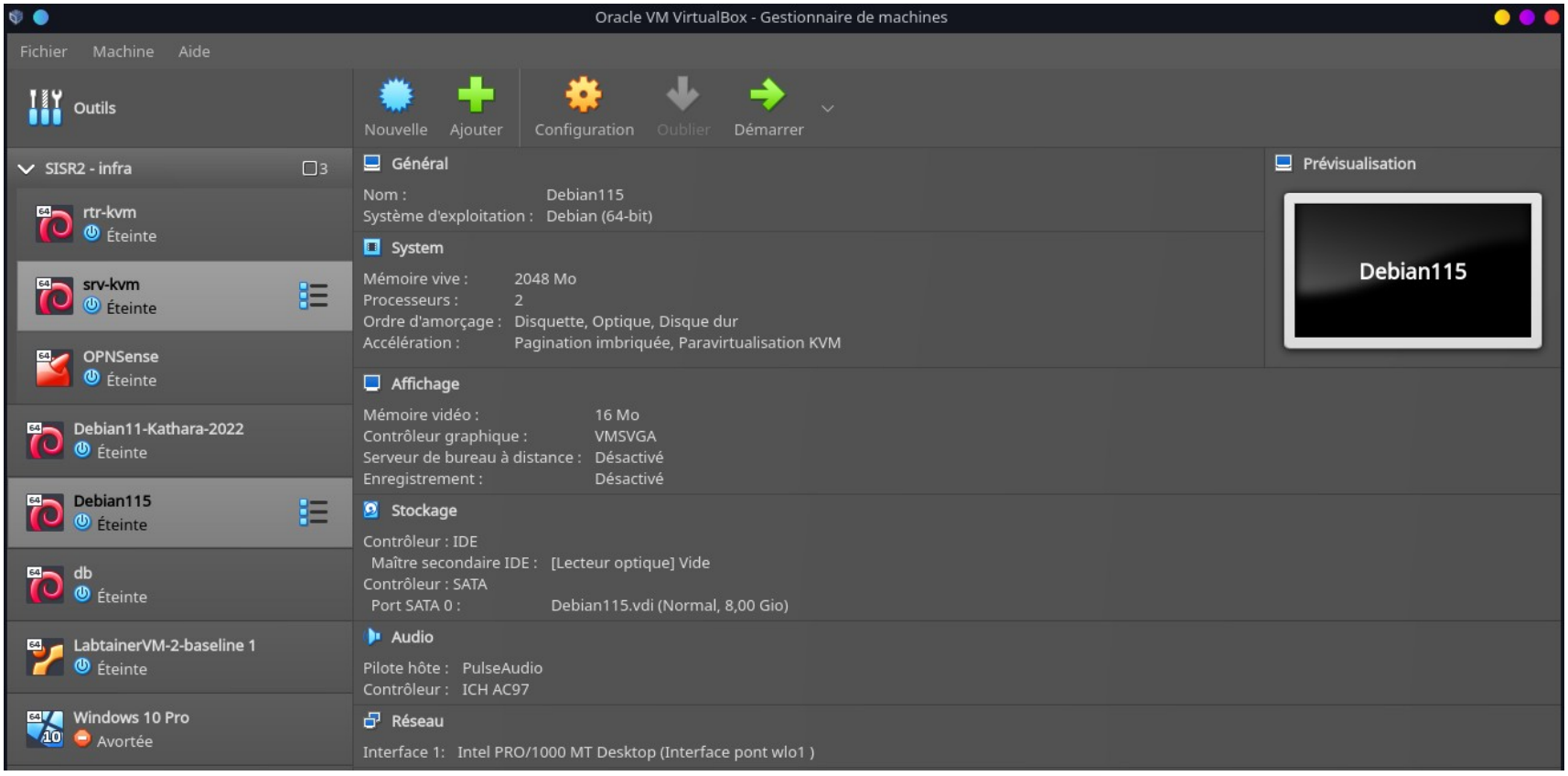
- **Vmware Workstation**
- **Vmware Fusion**
- **Microsoft VirtualPC (dead)**

La virtualisation des serveurs



La virtualisation des serveurs

Oracle VirtualBox Type 2



La virtualisation des serveurs

Hyperviseur de type 1 : « Hyperviseur natif ou bare-metal »

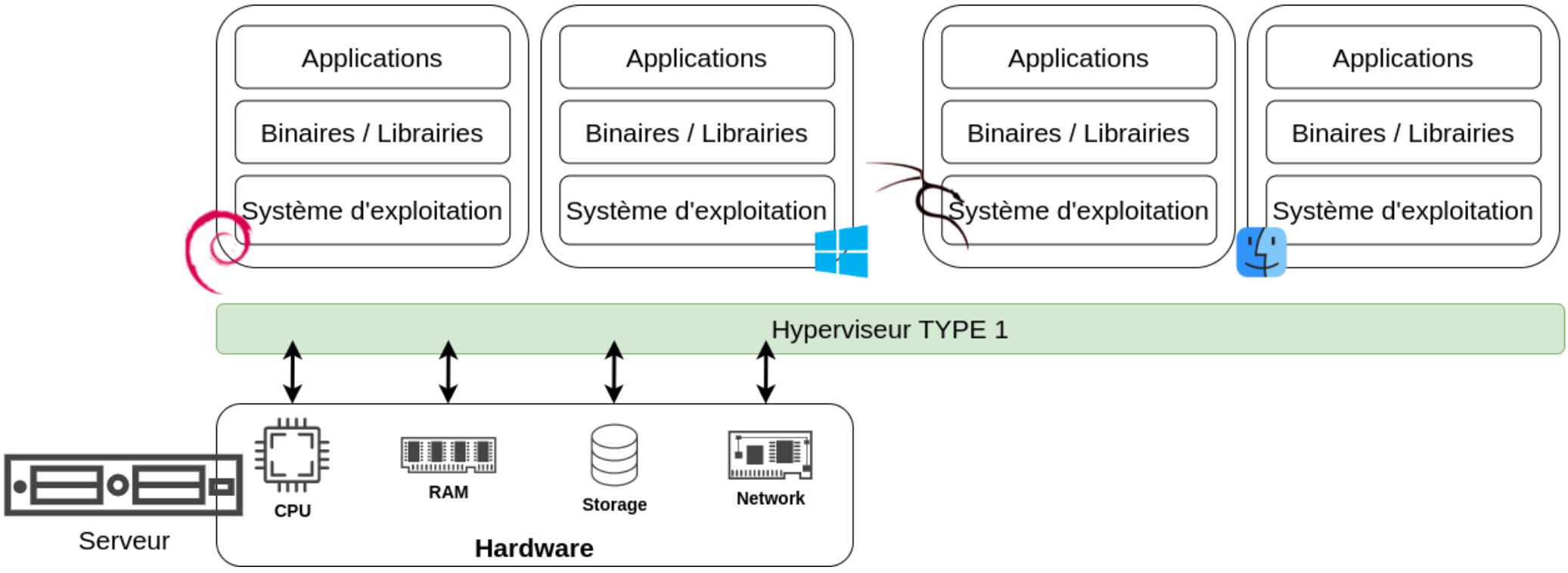
C’est une famille d’hyperviseur qui interagissent et s’installe directement sur le matériel (d’où le bare-metal)

Il n’ont pas besoin d’un OS pour être installés (Ah bon ?)

Exemples :

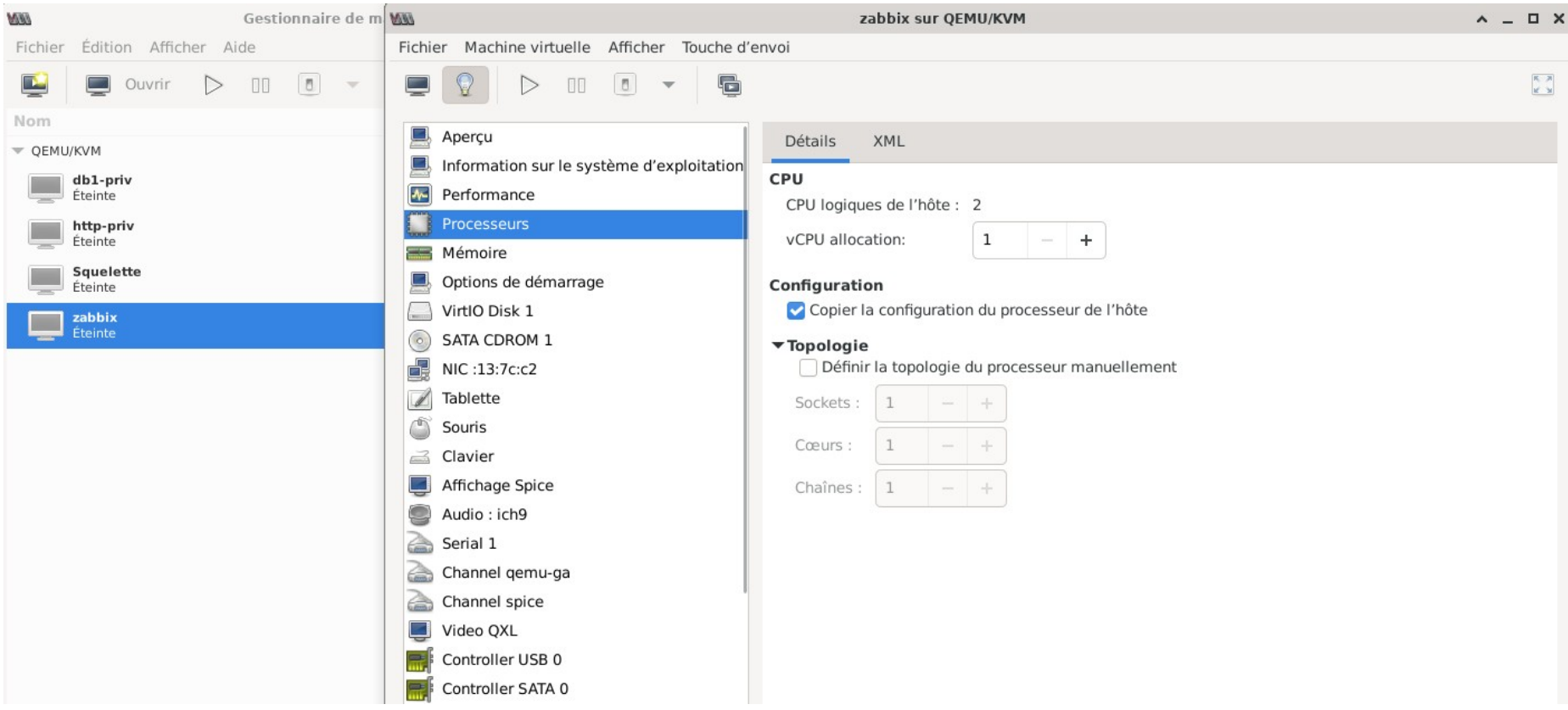
KVM, Microsoft Hyper-V, *ProxMox*, Citrix XenServer et le leader incontesté pour l’instant vmware Esxi (suite vSphere)

La virtualisation des serveurs



La virtualisation des serveurs

KVM
Type 1



La virtualisation des serveurs

Quelques usages des hyperviseurs

Type 1 : Virtualisation de serveurs en entreprise, cluster de production, environnements de déploiement, datacenter, cloud (IaaS)

Type 2 : Faire tourner / tester plusieurs OS sur une machine sans risques, réalisation de tests de compatibilité, s'adonner à la cybersécurité, s'amuser !, ...

Les conteneurs

Les conteneurs sont une forme de virtualisation légère, sauf qu'à la différence de ce qu'on a vu précédemment, ce n'est pas la machine qui est virtualisée, mais le système d'exploitation.

Un conteneur est un espace d'exécution dédié à (en général) une application, un logiciel.

Le noyau du système d'exploitation utilisé est celui de la machine hôte, seules les applications et ce dont elles ont besoin pour fonctionner (binaires/librairies) sont isolées dans un conteneur.

Ce qui signifie ?

Les conteneurs

Pourquoi ?

Une application n'utilise pas forcément l'ensemble des ressources d'une machine virtuelle (ressources fixes)

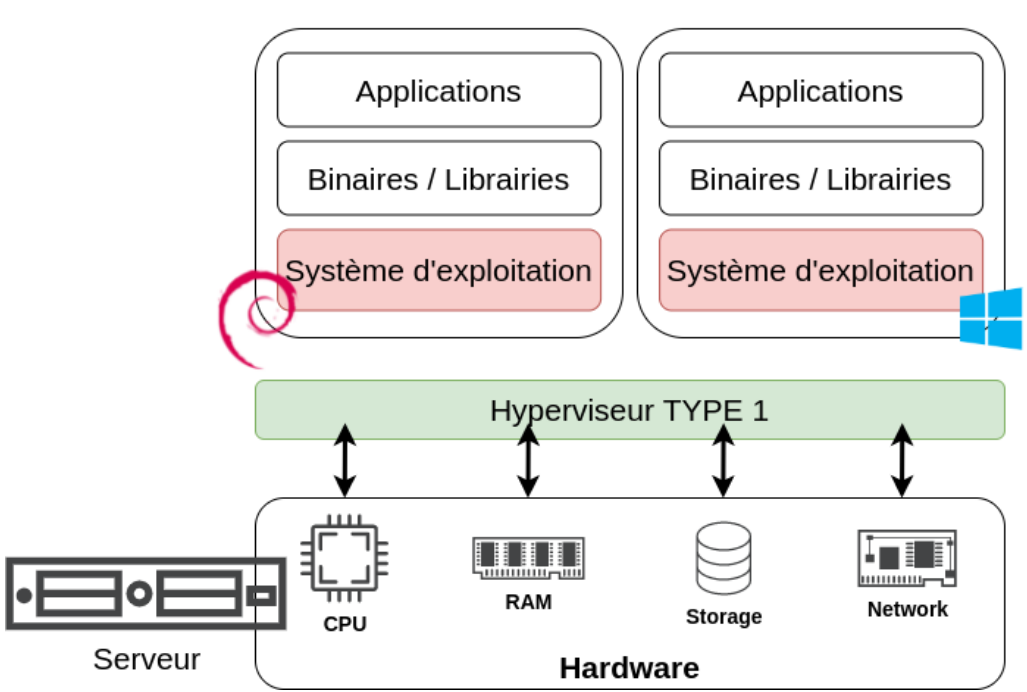
Besoin de développer des applications/fonctionnalités portables rapidement.

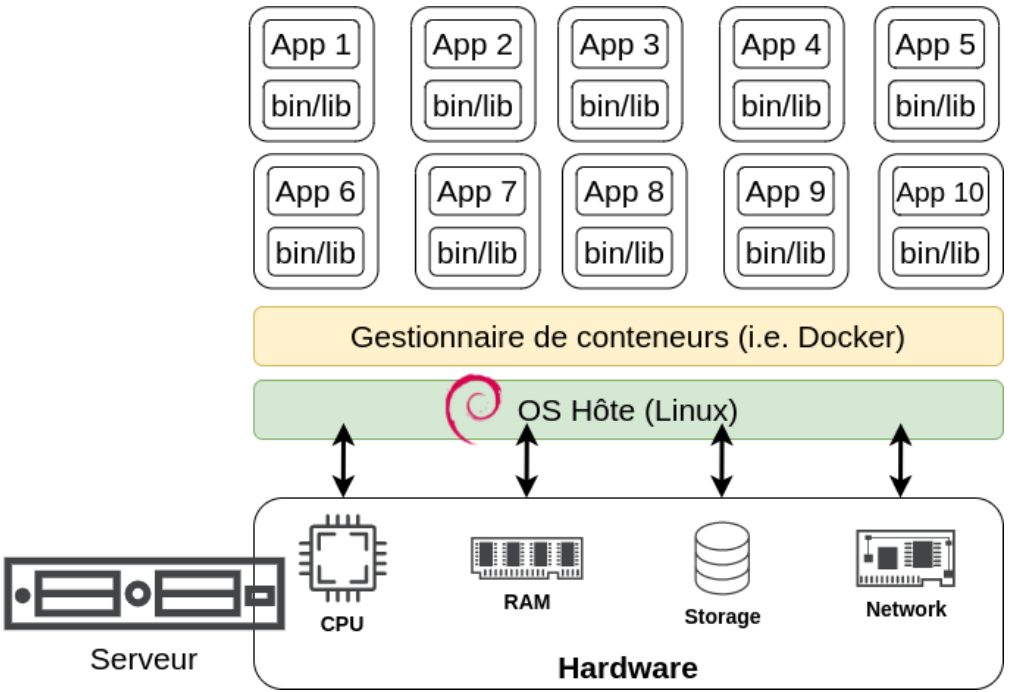
→ Essor des conteneurs (facilité de mise en œuvre, rapidement de démarrage). Docker est la star (pour l'instant).

Outils : LXC/LXD, Docker, CoreOS RKT, CRI-O, runC, crun, containerd.

Et Swarm / Kubernetes / RH OpenShift ? → Ce sont des outils d'orchestration.

Les conteneurs





Les conteneurs

Comment sont « isolés » les conteneurs Linux ?

- Par isolation des processus grâce à une fonctionnalité du noyau Linux : les Namespaces

- L'allocation de ressources est gérée par une autre fonctionnalité : les Cgroups.

Les conteneurs

Namespace (pid, net, mnt, uts, ipc, user)

Ils permettent une séparation logique des conteneurs.

Les processus des différents conteneurs sont gérés par l'hôte dans des espaces de noms différents de ceux de l'hôte et des autres conteneurs.

Les conteneurs

Namespace NET :

Séparation des

- **Interfaces réseau,**
- **Table de routage,**
- **Règles de pare-feu,**
- **Sockets**

Un processus ne partage ses éléments qu'avec les autres processus appartenant au même namespace.

Les conteneurs

Namespace UTS (Unix Time-Sharing) : Nom d'hôte/domain de la machine

Namespace Time : Isolation de l'heure système.

Namespace USER : mapping des iud/gid

i.e. uid 0 → 9999 d'un container => uid 10000 => 19999 sur l'hôte

Root dans un conteneur n'est pas root sur l'hôte

Namespace IPC (InterProcess Communication) : pour éviter les conflits de mémoire partagée entre des processus de namespaces différents.

Namespace MNT (MouNT) : contrôle des points de montage. Un rootfs par namespace.

Namespace PID : Isolation des PID. PID 1 (init) sur l'hôte ≠PID 1 (init) dans le namespace. Tous les processus apparaissent dans le namespace par défaut (de l'hôte) mais avec des numéros différents.

Les conteneurs

Les Cgroups (Control groups) : fonctionnalité du noyau Linux pour limiter, compter et isoler l'utilisation des ressources (processeur, mémoire, utilisation disque, etc.).

Cgroups permet de :

- Limiter les ressources à certains groupes

- Prioriser certains groupes (CPU, BW, I/O)

- Mesurer les ressources consommées par certains groupes

...

Chaque processus est placé dans un cgroup. Les nouveaux sont placés dans le cgroup de leur parent.

Bilan

	Machines virtuelles	Containers
Pros	Technologie éprouvée	Légers (dizaines/centaines de Mo)
	Lancer des OS différents indépendamment du matériel	Ressources nécessaires réduites
	Portabilité et migration facilitées	Démarrage « instantané »
	De nombreux outils professionnels	Nombre de conteneurs élevé
	Sécurité	Approche CI/CD / DevOps
Cons	Une VM = plusieurs dizaines de Go	Dépendants du Kernel de l'hôte
	Ressources élevées → Nombre de VM réduit	Sécurité (isolation moindre)
	Plusieurs minutes à démarrer	En constante évolution. Quid docker ?

Bilan

Alors conteneurs ou VM dans le futur ?

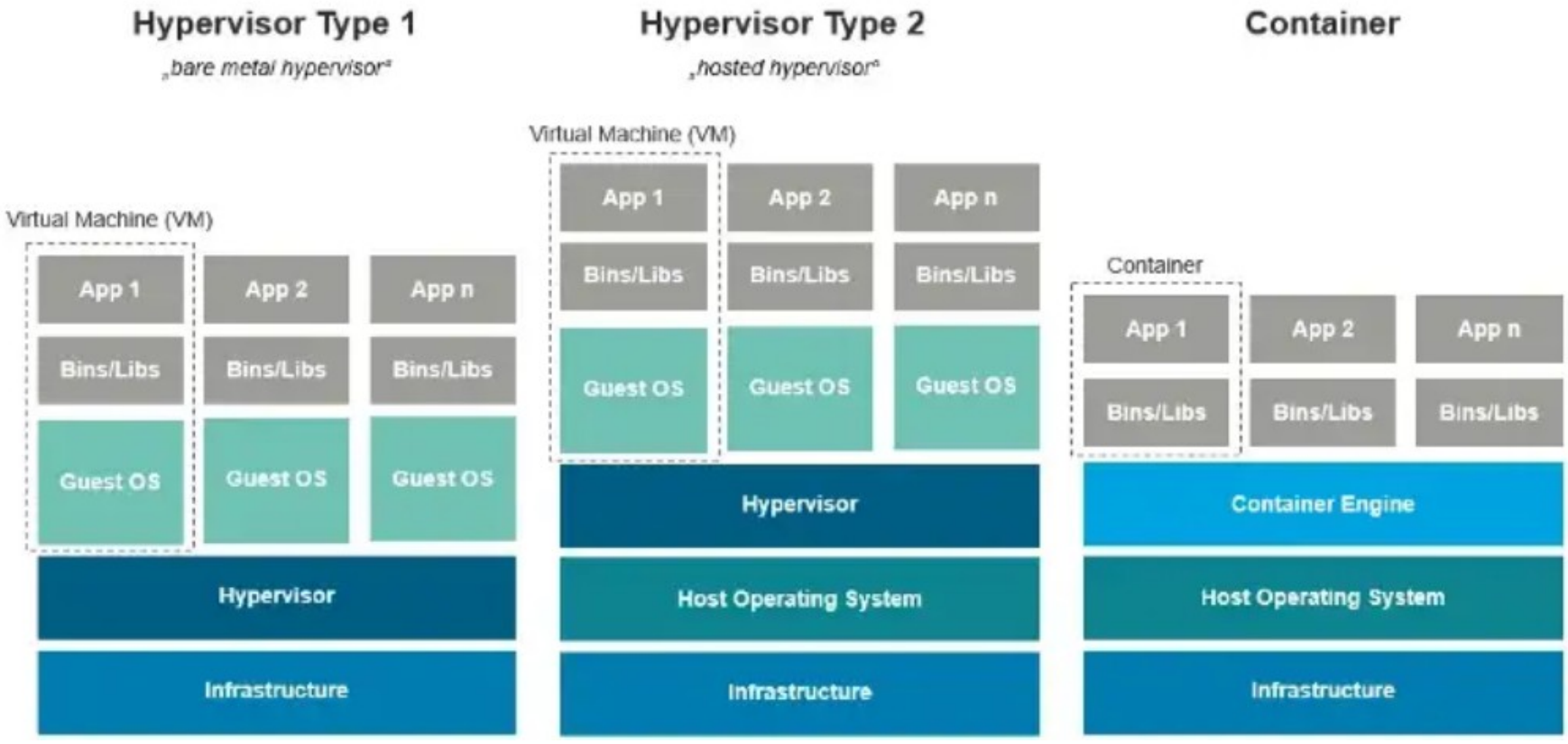
→ Les deux.

Les conteneurs et les machines virtuelles continueront à jouer des rôles importants.

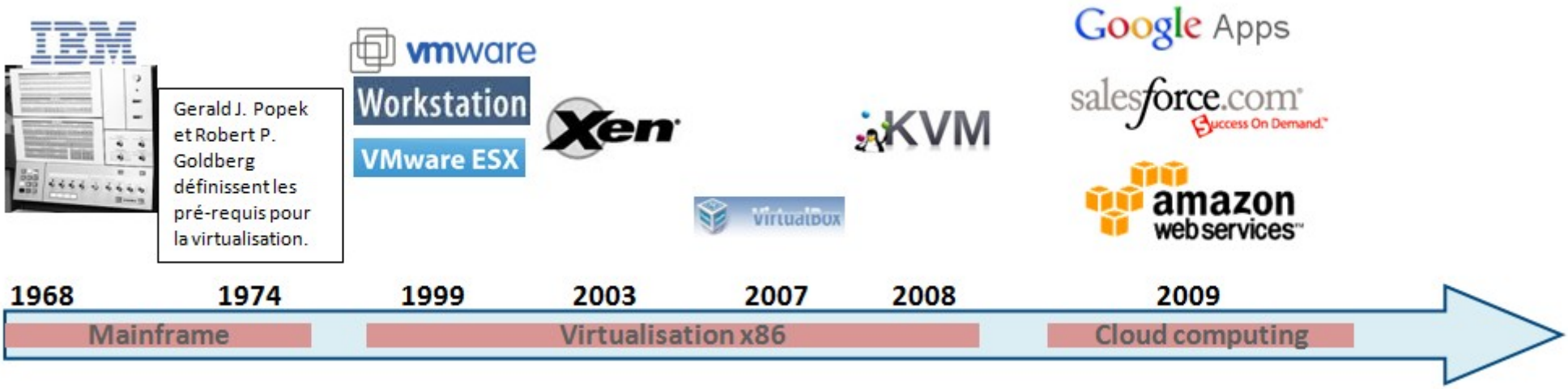
Les conteneurs peuvent s'exécuter sur des VMs, permettant à une organisation de tirer parti de ses outils existants pour l'automatisation, la sauvegarde et la surveillance. Les conteneurs sur les VMs permettent également aux équipes IT expérimentées en matière de VMs de gérer un environnement conteneurisé. Les VMs auront de nouveaux cas d'utilisation lorsque les entreprises chercheront à utiliser la puissance de leur infrastructure ou le cloud pour prendre en charge les charges de travail lourdes des applications et du réseau.

vmware

Bilan


Hypervisor Type 1
„bare metal hypervisor"
Virtual Machine (VM)
App 1
App 2
App n
Bins/Libs
Bins/Libs
Bins/Libs
Guest OS
Guest OS
Guest OS
Hypervisor
Infrastructure
Hypervisor Type 2
„hosted hypervisor"
Virtual Machine (VM)
App 1
App 2
App n
Bins/Libs
Bins/Libs
Bins/Libs
Guest OS
Guest OS
Guest OS
Hypervisor
Host Operating System
Infrastructure
Container
Container
App 1
App 2
App n
Bins/Libs
Bins/Libs
Bins/Libs
Container Engine
Host Operating System
Infrastructure

Bilan



https://fr.wikibooks.org/wiki/Les_syst%C3%A8mes_d%27exploitation/Virtualisation_et_machines_virtuelles

VM vs Containers

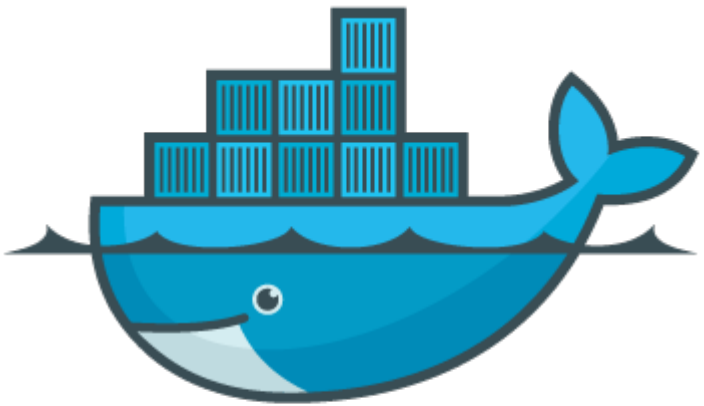
« Virtual Machines (VMs) and Containers are complimentary and similar – both improve IT efficiency, application portability, and enhance DevOps. However, understanding the difference between them is a key component of developing an agile, cloud-native, application-driven strategy. »

(vmware)

Les machines virtuelles et les conteneurs sont complémentaires et similaires - tous deux améliorent l'efficacité des outils informatiques, la portabilité des applications et améliorent l'approche DevOps. Cependant, comprendre la différence entre eux est un élément clé du développement d'une stratégie agile, native du cloud et axée sur les applications.

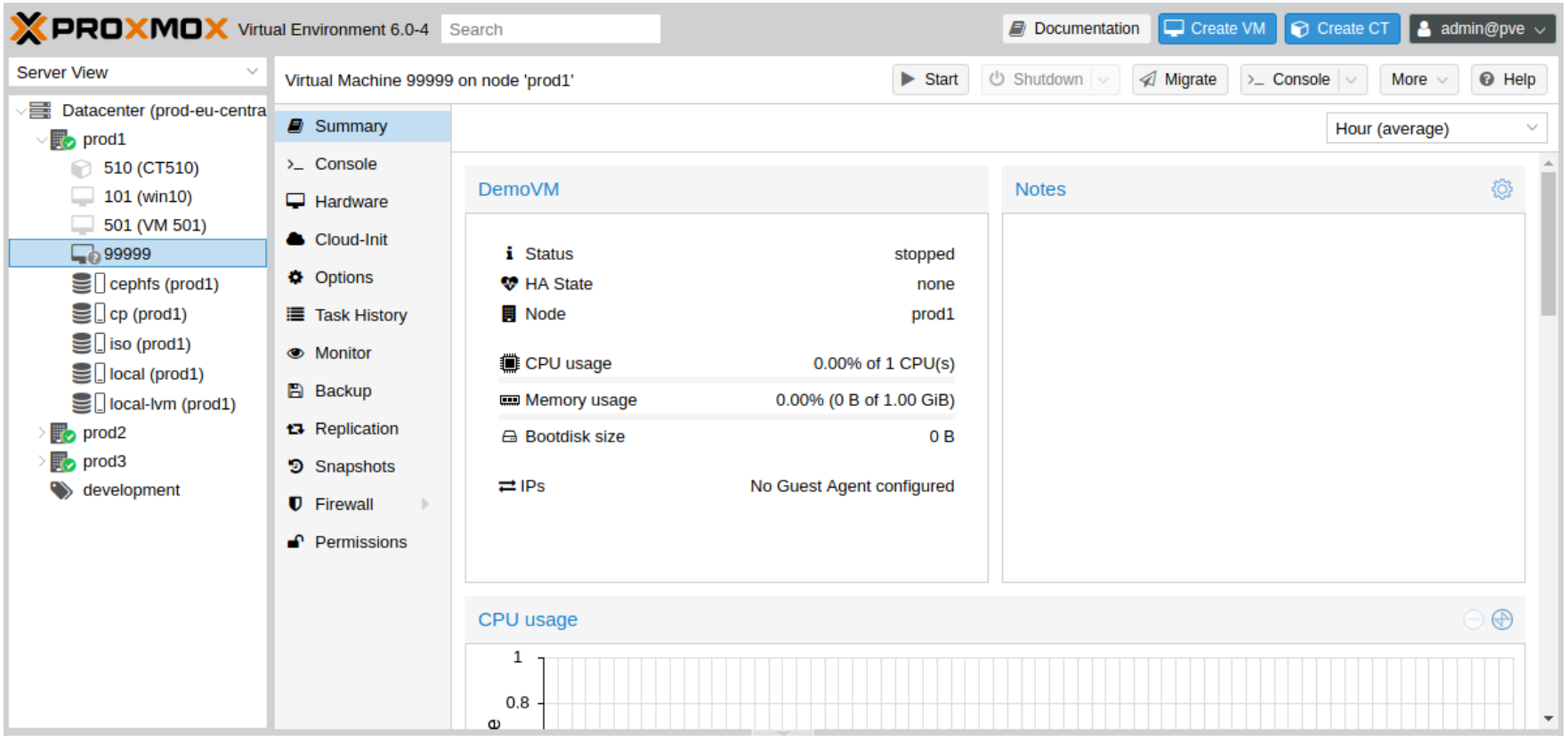
Pour la suite en TD/TP

PROXMOX

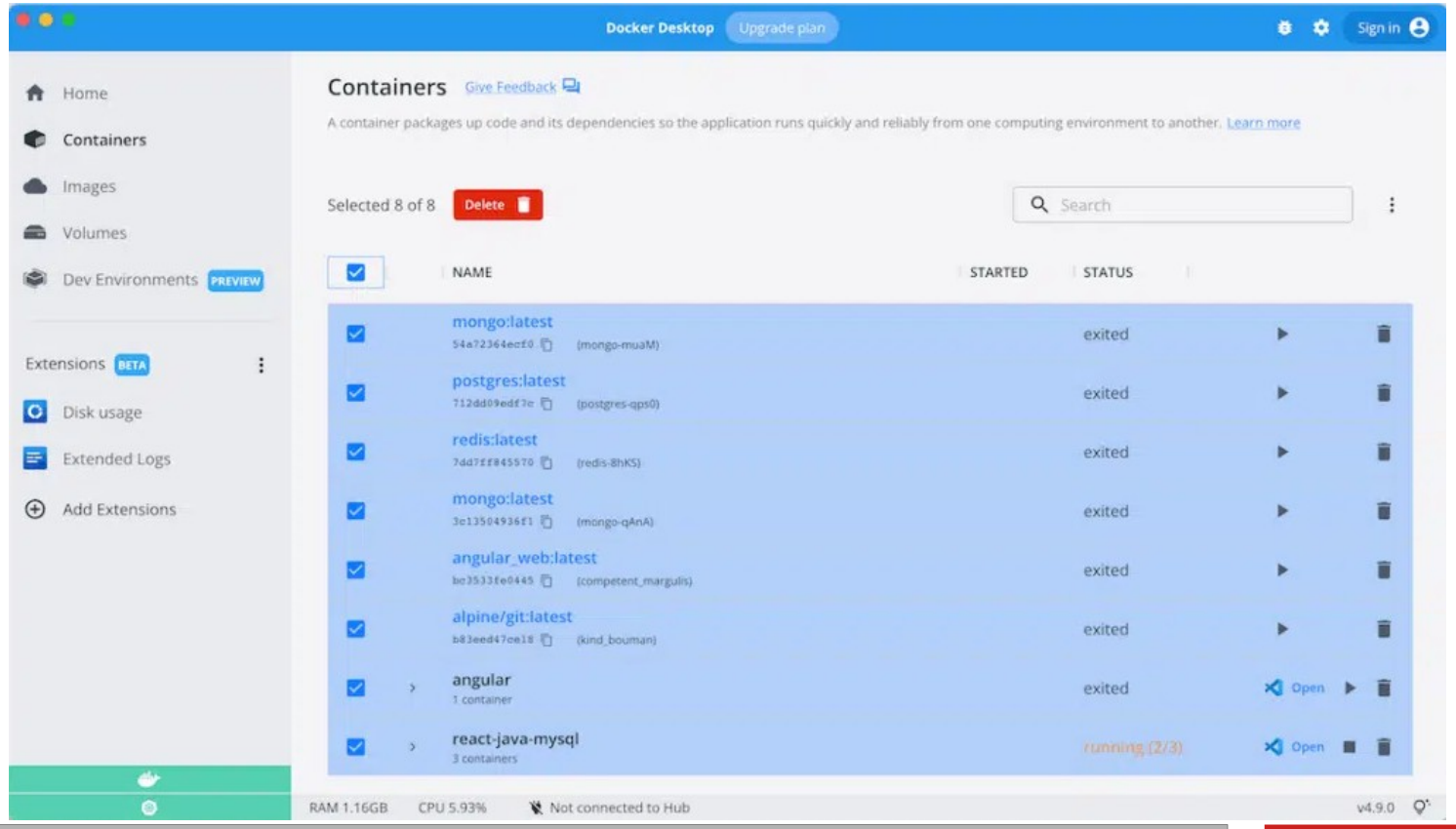


docker

ProxMox VE


PROXMOX Virtual Environment 6.0-4
Search
Documentation
Create VM
Create CT
admin@pve
Server View
Datacenter (prod-eu-centra
prod1
510 (CT510)
101 (win10)
501 (VM 501)
99999
cephfs (prod1)
cp (prod1)
iso (prod1)
local (prod1)
local-lvm (prod1)
prod2
prod3
development
Virtual Machine 99999 on node 'prod1'
Start
Shutdown
Migrate
Console
More
Help
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Backup
Replication
Snapshots
Firewall
Permissions
Hour (average)
DemoVM
Status stopped
HA State none
Node prod1
CPU usage 0.00% of 1 CPU(s)
Memory usage 0.00% (0 B of 1.00 GiB)
Bootdisk size 0 B
IPs No Guest Agent configured
Notes
CPU usage
1
0.8

Docker


Docker Desktop
Upgrade plan
Sign in
Home
Containers
Images
Volumes
Dev Environments
PREVIEW
Extensions
BETA
Disk usage
Extended Logs
Add Extensions
Containers
Give Feedback
A container packages up code and its dependencies so the application runs quickly and reliably from one computing environment to another. Learn more
Selected 8 of 8
Delete
Search
NAME
STARTED
STATUS
mongo:latest
54a72364ecf0 (mongo-muaM)
exited
postgres:latest
712dd09edf7e (postgres-qps0)
exited
redis:latest
7dd7ff845570 (redis-8hKS)
exited
mongo:latest
3c13504936f1 (mongo-qAnA)
exited
angular_web:latest
bc3533fe0445 (competent_margulis)
exited
alpine/git:latest
b83eed47ce18 (kind_bouman)
exited
angular
1 container
exited
Open
react-java-mysql
3 containers
running (2/3)
Open
RAM 1.16GB
CPU 5.93%
Not connected to Hub
v4.9.0

Le réseau dans VirtualBox

Il existe plusieurs mode réseau dans VirtualBox :

- **NAT**
- **NAT Network**
- **Bridged**
- **Internal Network**
- **Host-only**

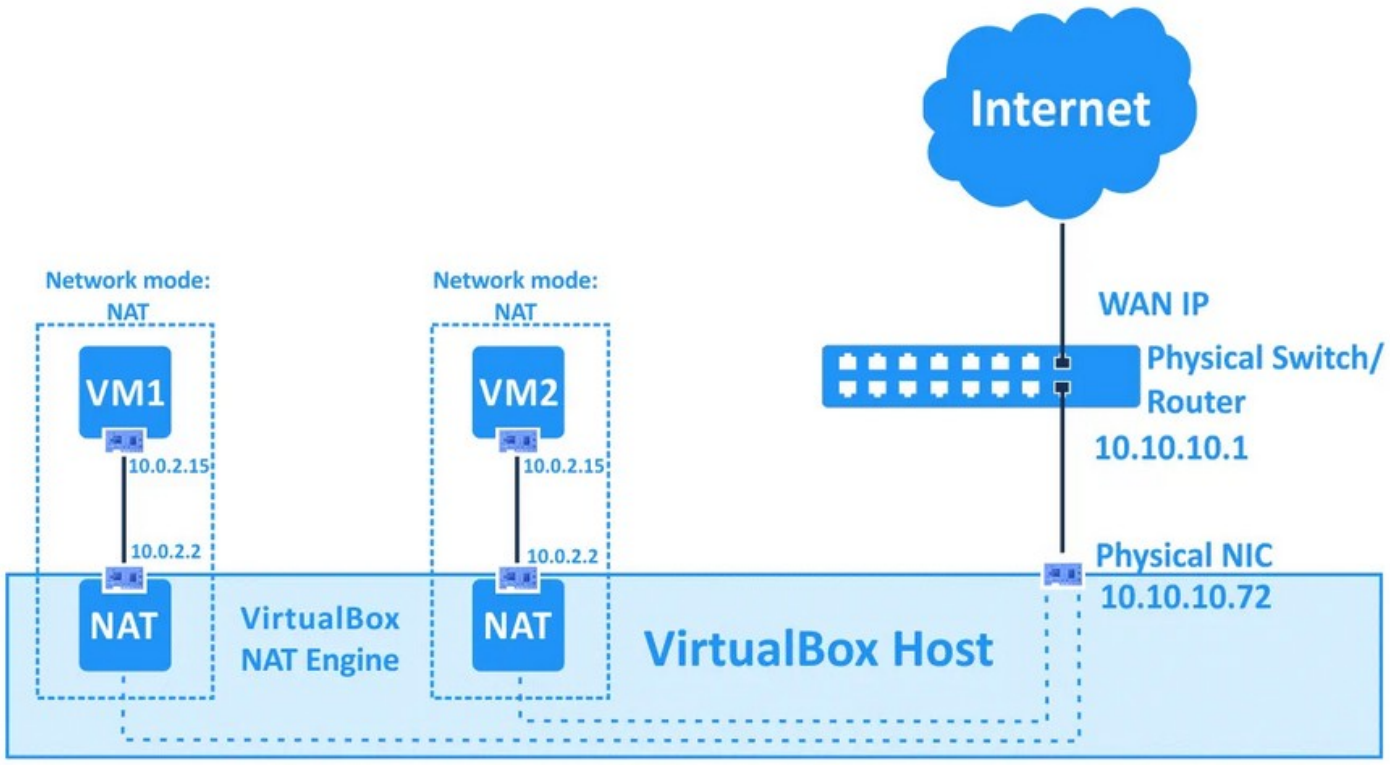
...

Il est possible de faire la même chose ou équivalent avec UTM sous Mac.

Le réseau dans VirtualBox

Fonctionnement du mode **NAT** dans VirtualBox

Toutes les VM en NAT ont la même adresse IP (10.0.2.15) et sont isolées les unes des autres par le moteur NAT de VirtualBox

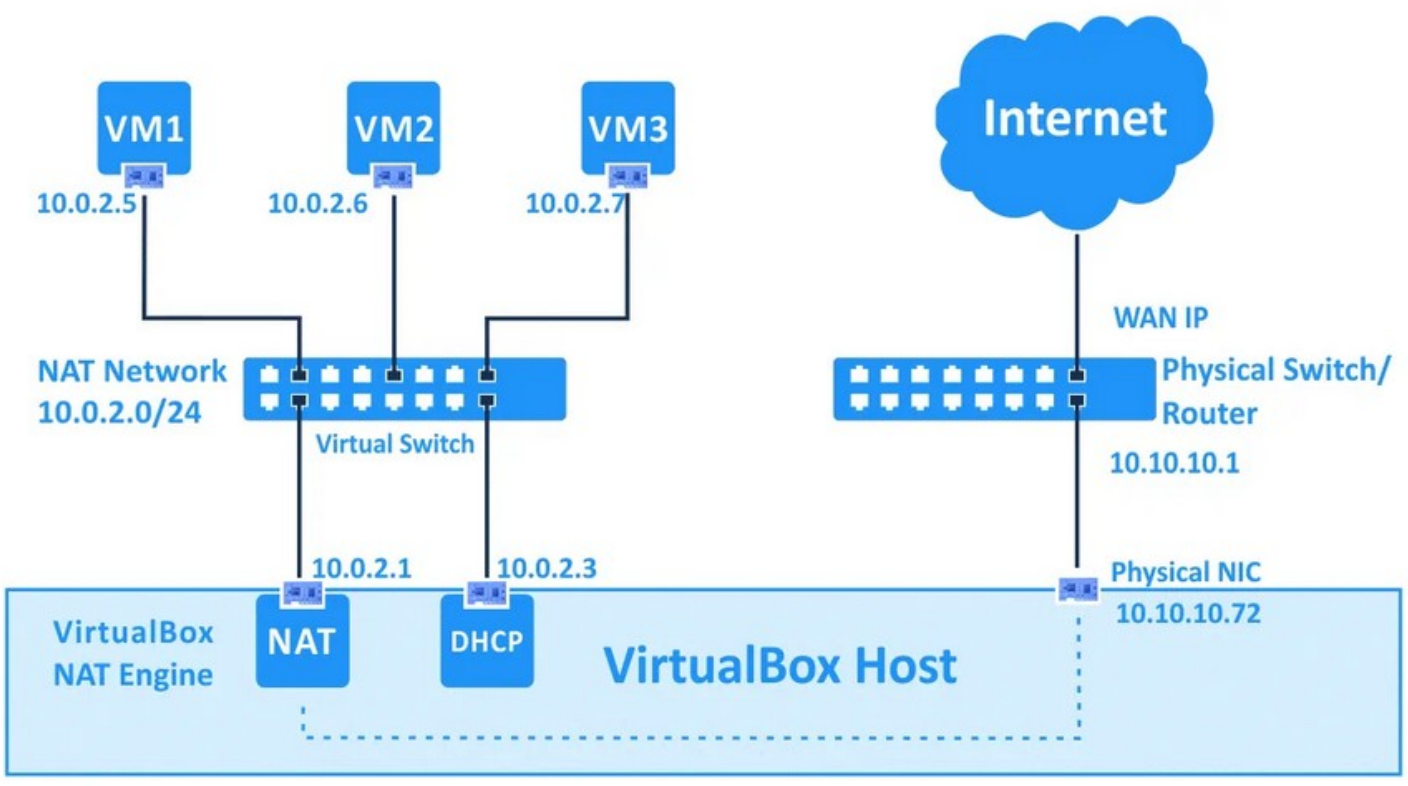


Le réseau dans VirtualBox

Fonctionnement du mode **NAT Network** dans VirtualBox

Toutes les VM en réseau NAT ont une adresse IP différente sur le réseau NAT utilisé (10.0.2.0/24 par défaut)

Il est possible de créer plusieurs réseau NAT

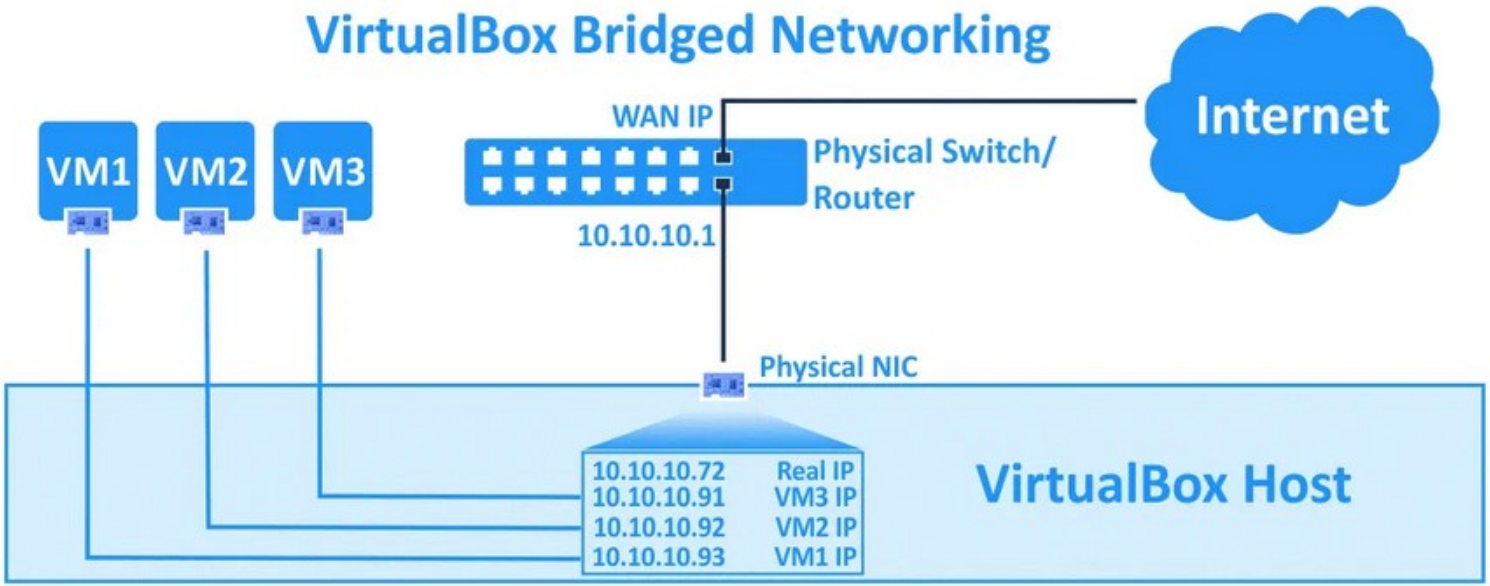


Le réseau dans VirtualBox

Fonctionnement du mode **bridged** dans VirtualBox

Un driver filtre les paquets reçus sur l'interface réseau de l'hôte et les répartir entre les VM.

Une VM an mode bridge apparaît comme un équipement physique sur le réseau de l'hôte

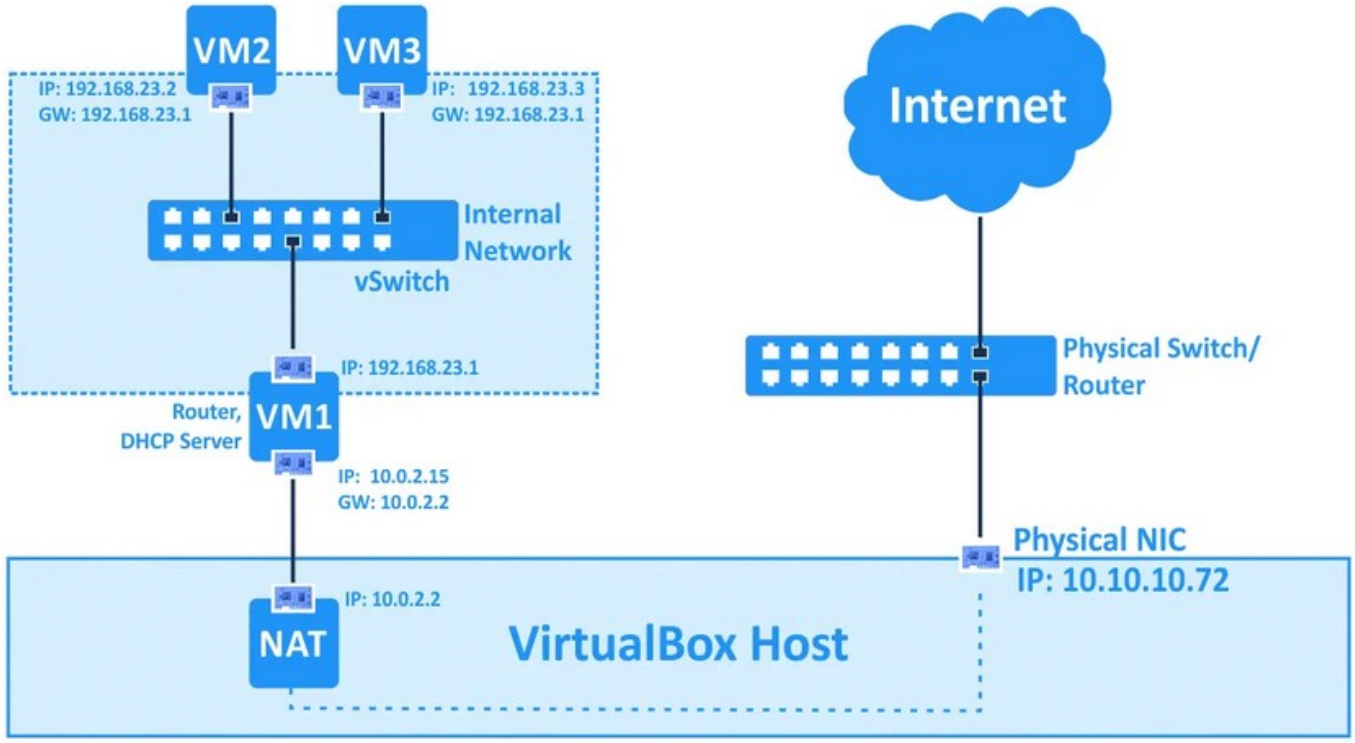


Le réseau dans VirtualBox

Fonctionnement du mode **internal network** dans VirtualBox

Crée un réseau interne de VM dans VirtualBox.

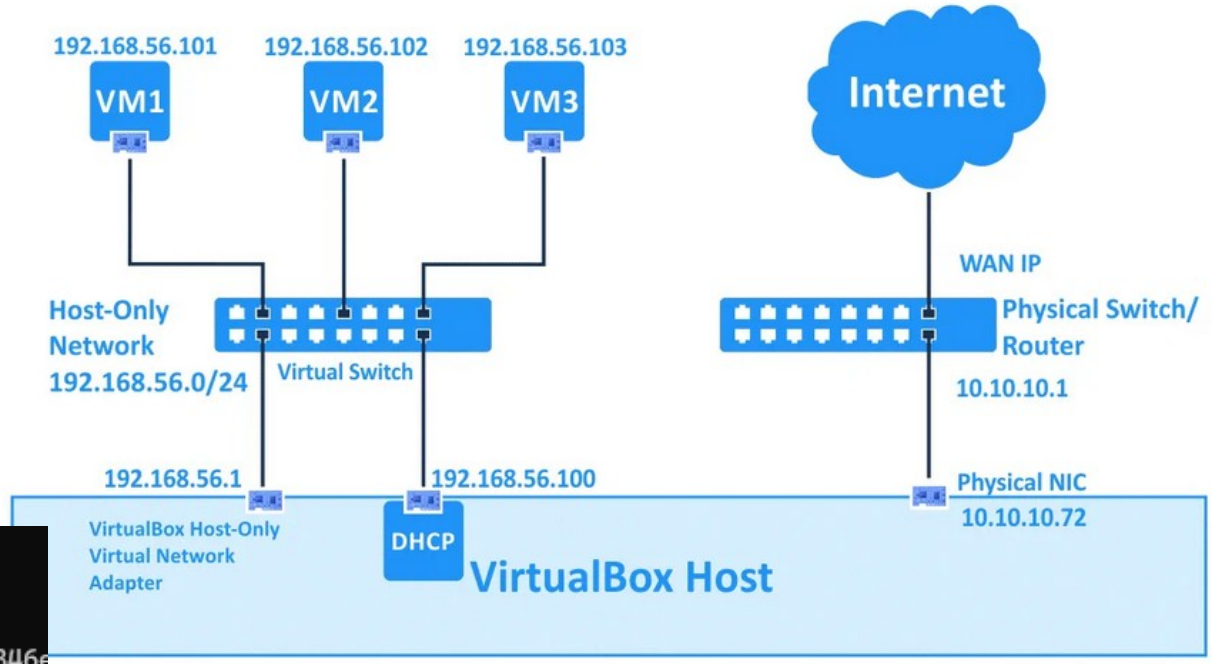
Des machines connecté à un même réseau interne pourront communiquer, mais seront isolées les unes des autres.



Le réseau dans VirtualBox

Fonctionnement du mode **Host-only** dans VirtualBox

Les machines sont placées sur un réseau particulier créé par l'hôte, par défaut 192.168.56.0/24




```
Carte Ethernet VirtualBox Host-Only Network :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::5380:846e
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.56.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :
```

Le réseau dans VirtualBox

Tableau de communication en fonction du mode réseau utilisé

	VM ↔ VM	VM → Host	VM ← Host	VM → LAN	VM ← LAN
Not attached	–	–	–	–	–
NAT	–	+	Port Forward	+	Port Forward
NAT Network	+	+	Port Forward	+	Port Forward
Bridged	+	+	+	+	+
Internal Network	+	–	–	–	–
Host-only	+	+	+	–	–

Source des images : https://www.nakivo.com/blog/virtualbox-network-setting-guide/

Installation d’une Debian avec VirtualBox

Une petite démo sur une VM debian

NAT
NAT Network
Bridge ?

Port forwarding

Sources

https://www.hebergeurcloud.com/definition-cloud-computing-selon-nist/

https://www.redhat.com/fr/topics/cloud-computing/what-is-multicloud

https://aws.amazon.com

https://azure.microsoft.com/

https://www.redhat.com/

https://www.openstack.org/

https://www.ionos.fr/digitalguide/serveur/configuration/la-virtualisation/

https://visionarymarketing.com/fr/2020/04/poste-de-travail-virtuel-vdi/

https://www.padok.fr/en/blog/container-docker-oci