Environnements de TP pour la sécurité

Bruno Martin

RESSI'19, le 16 mai

Contenu

Présentation générale

Buts visés

Permettre aux étudiants d'utiliser :

- une distribution d'audit (Kali, BlackArch, Parrot) en étant `root` sur la distribution et sur le(s) réseau(x)
- un serveur (passerelle sous Ubuntu) pour ajouter des services
- un client sous BSD

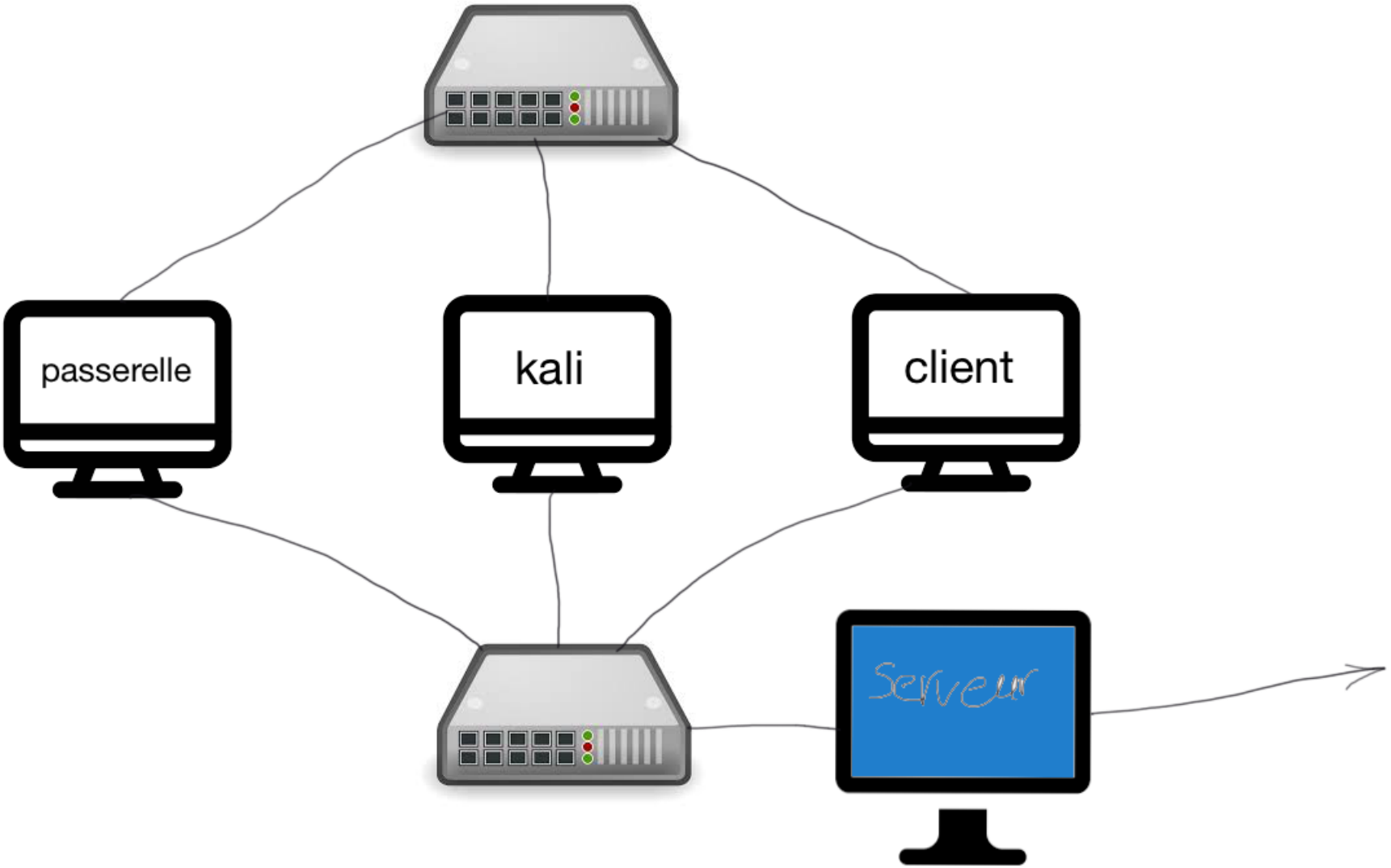
Toutes ces machines reliées sur 1 (ou 2) LAN et en toute sécurité.

Exemples de TP à réaliser

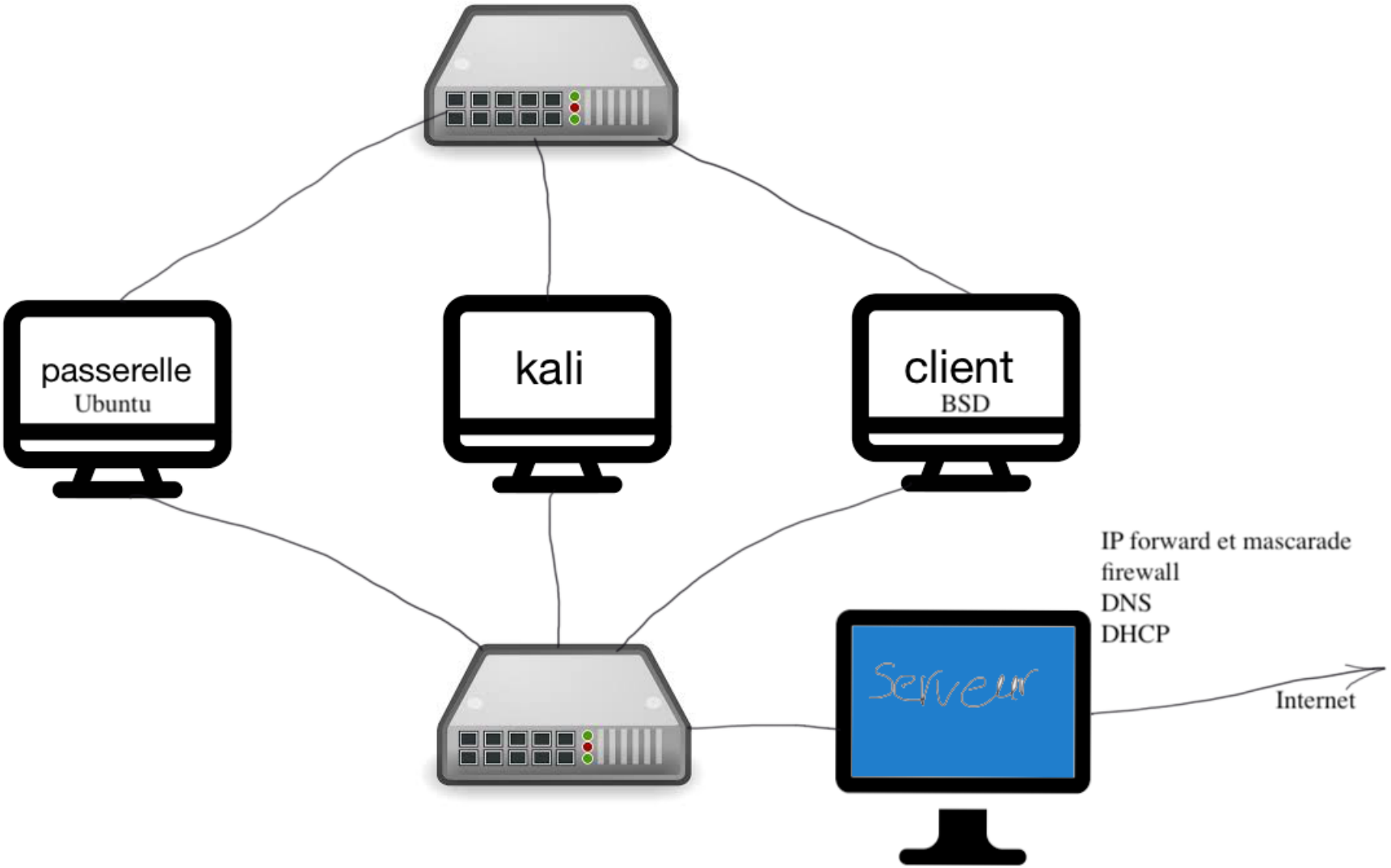
- Utiliser le serveur relié à 2 interfaces réseau comme passerelle (IP forwarding, IP masquerading)
- Installer un serveur web (`http` et `https`), publier un formulaire de login et réaliser une attaque MIM (démo)
- Installer un serveur `smtp`, `imap(s)`, configurer le `smtp` client, réaliser des attaques MTA et sur le serveur `imap(s)` ; utiliser `GPG`
- Mettre en place `openVPN` en mode routé puis ponté, tenter de réaliser des attaques
- Réaliser un mini audit sur le serveur en utilisant `OpenVAS`, `nmap` et `Metasploit`

En mettant en place au fur et à mesure les règles de firewall et en assurant la sécurité

Environnement de TP



Environnement de TP



Implémenter l'environnement

Au moins 4 façons de réaliser l'environnement de TP :

- physiquement : avec un serveur, des commutateurs réseaux, des machines physiques
- virtuellement sur un ordinateur personnel avec :
  - un hyperviseur de type 2
  - un hyperviseur de type 1 virtualisé
- virtuellement sur un serveur de virtualisation

Environnement physique

Environnement physique

Entre 2000 et 2009 dans une salle séparée du réseau par un serveur, un parc de 24 machines (12 avec 2 NIC, 12 avec 1 NIC) sur un réseau commuté reconfigurable.

+ Réinstallation rapide (technique de kickstart de Fedora)
+ Possibilité d'ajouter des équipements (routeur wifi)
- Salle dédiée non utilisable pour d'autres TP
- (Seulement) 2 machines par étudiant : passerelle et client
- Mises à jour laborieuses
- Plus de services sur le serveur (reconfiguration réseau, . . .)
- Coût élevé

Pas de remplacement des machines $\mapsto$ passage à la virtualisation.

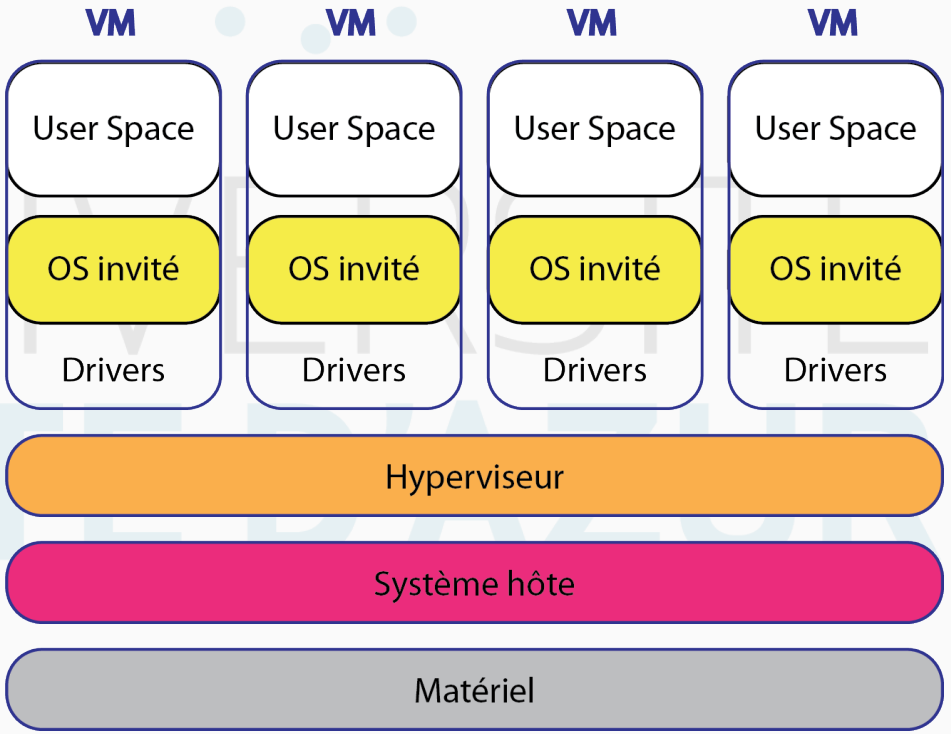
Techniques de virtualisation

Machine virtuelle – Hyperviseur de type 2

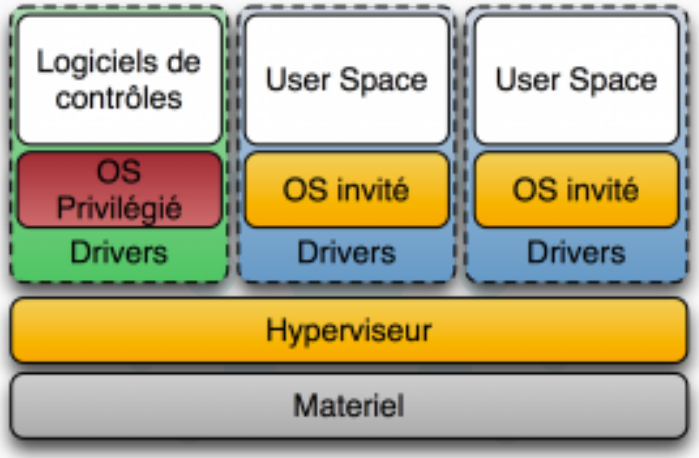
Un logiciel émule le matériel et permet de lancer plusieurs OS invités sur le système hôte physique. La mémoire et le CPU sont directement accessibles aux VM. On parle d'hyperviseur de type 2.

Technique qui fait cohabiter plusieurs OS isolés qui communiquent par un réseau émulé.

- KVM
- QEMU
- **VMware**
- VirtualBox
- VirtualPC
- Bochs



Hyperviseur de type 1



L'hyperviseur est un noyau système léger et optimisé pour la gestion de noyaux des SE invités directement au dessus de la couche matérielle. On parle d'hyperviseur de type 1 ou natif ou baremetal.

- **VMware** ESX, ESXi
- Xen qui est utilisé en particulier dans QubesOS

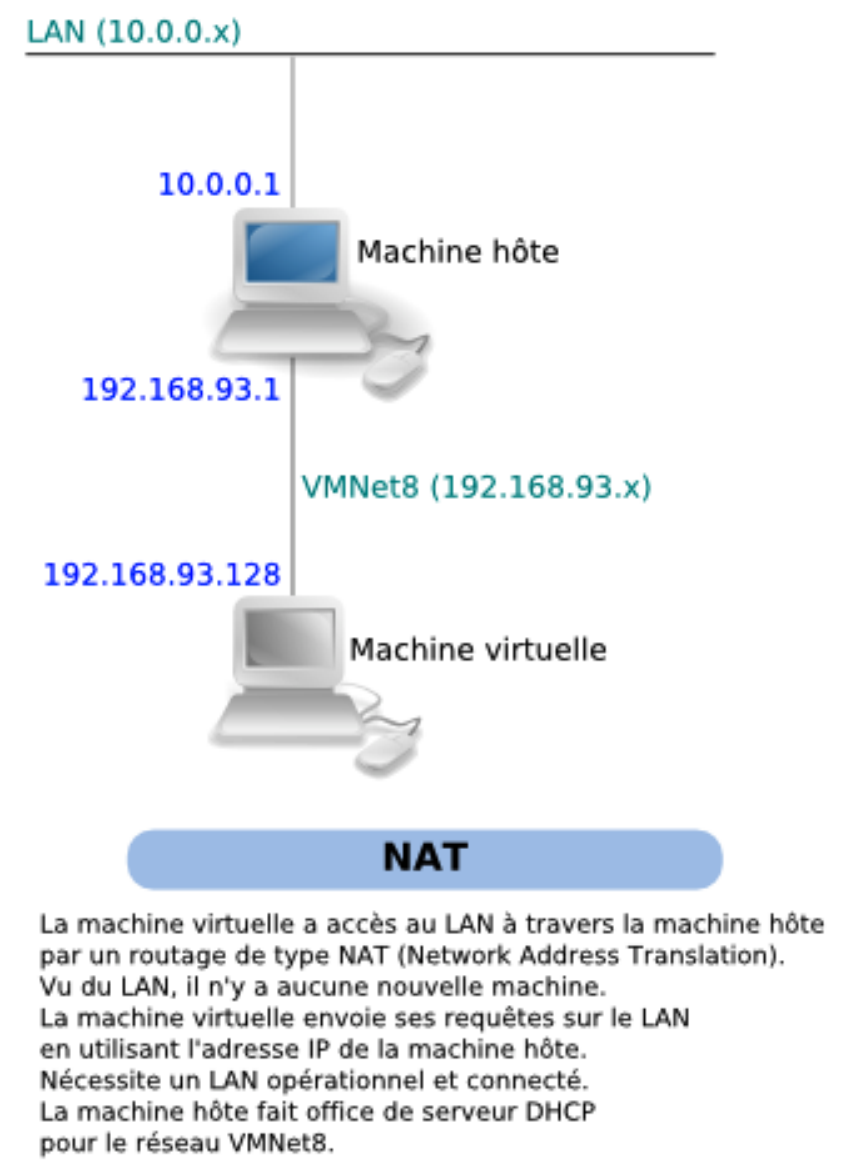
Machines virtuelles : mise en réseau

3 modes de fonctionnement principaux

- **NAT** : fonctionnement le plus simple. La VM se comporte comme un hôte connecté à un routeur qui acquiert son IP par `dhcp`. Le logiciel de virtualisation sert de routeur.
- **Host only** : la VM ne peut communiquer qu'avec d'autres VM hébergées sur le même hôte, comme si elles étaient connectées par un commutateur.
- **Bridge** : partage l'interface physique de la machine hôte. La VM acquiert son IP par un serveur externe à l'hôte.

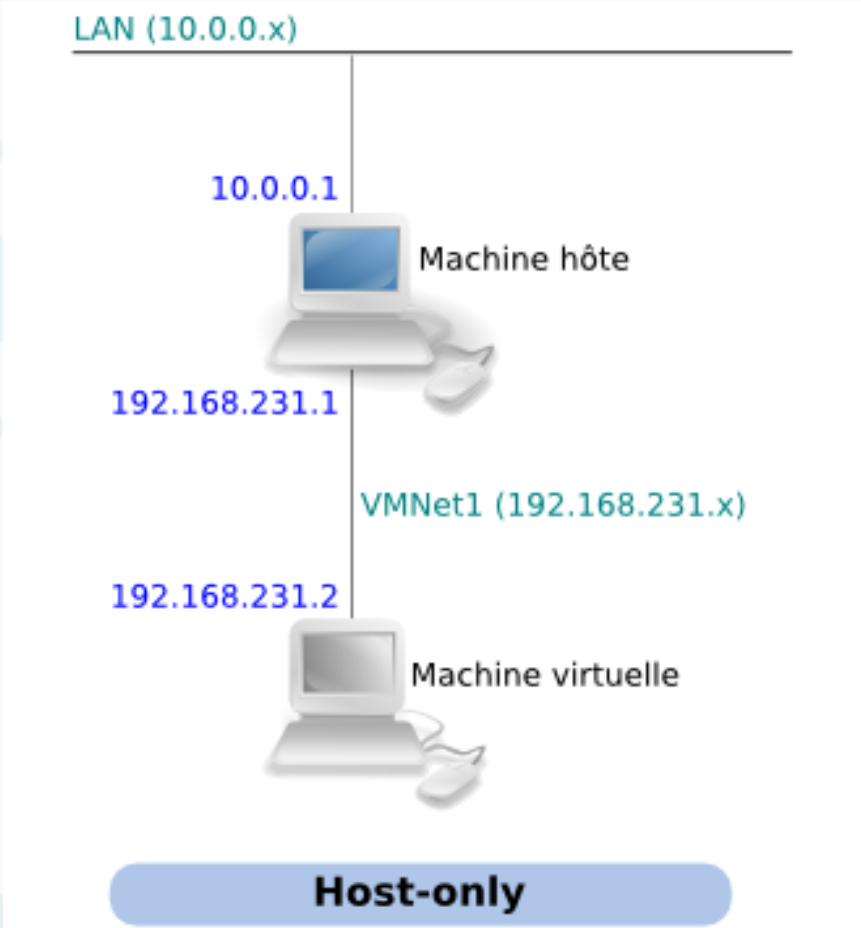
	accès au LAN	adr. IP de LAN
host only	NON	NON
NAT	OUI	NON
Bridge	OUI	OUI

Mise en réseau NAT & Host only



NAT

La machine virtuelle a accès au LAN à travers la machine hôte par un routage de type NAT (Network Address Translation).
Vu du LAN, il n'y a aucune nouvelle machine.
La machine virtuelle envoie ses requêtes sur le LAN en utilisant l'adresse IP de la machine hôte.
Nécessite un LAN opérationnel et connecté.
La machine hôte fait office de serveur DHCP pour le réseau VMNet8.

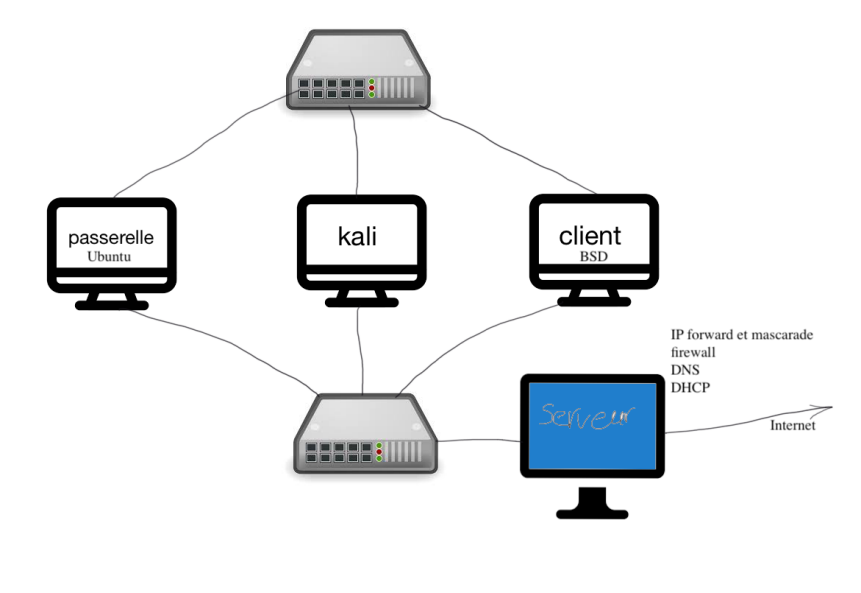


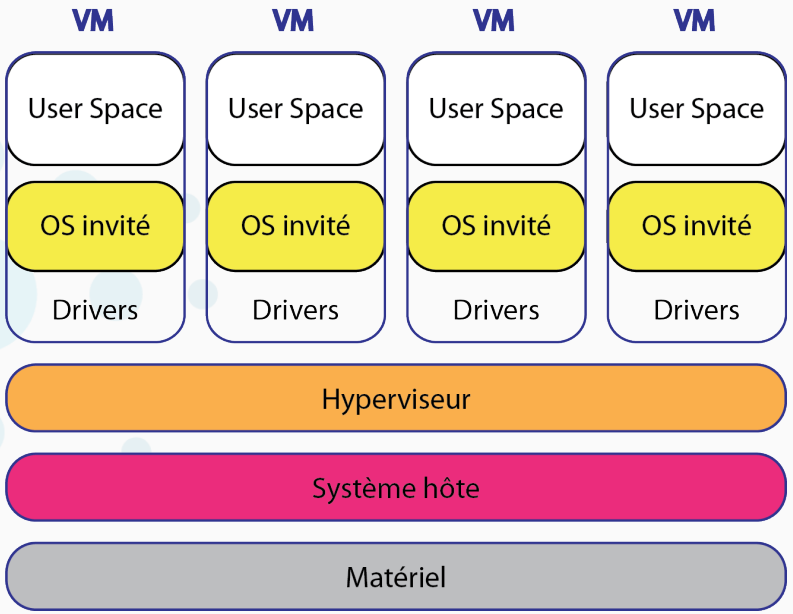
Host-only

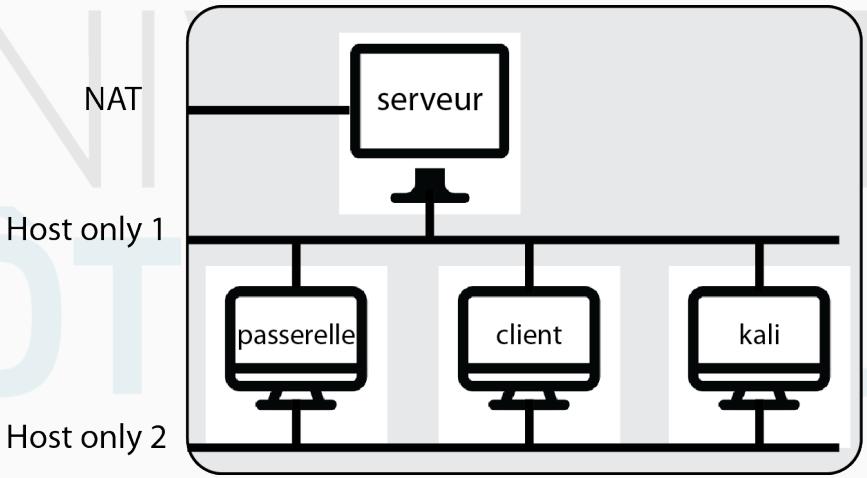
La machine virtuelle a accès uniquement à la machine hôte sur un réseau privé virtuel (VMNetX).
Vu du LAN, il n'y a aucune nouvelle machine.
La machine hôte fait office de serveur DHCP pour le réseau VMNet1.

Hyperviseur de type 2

Virtualisation “simple” de l’environnement





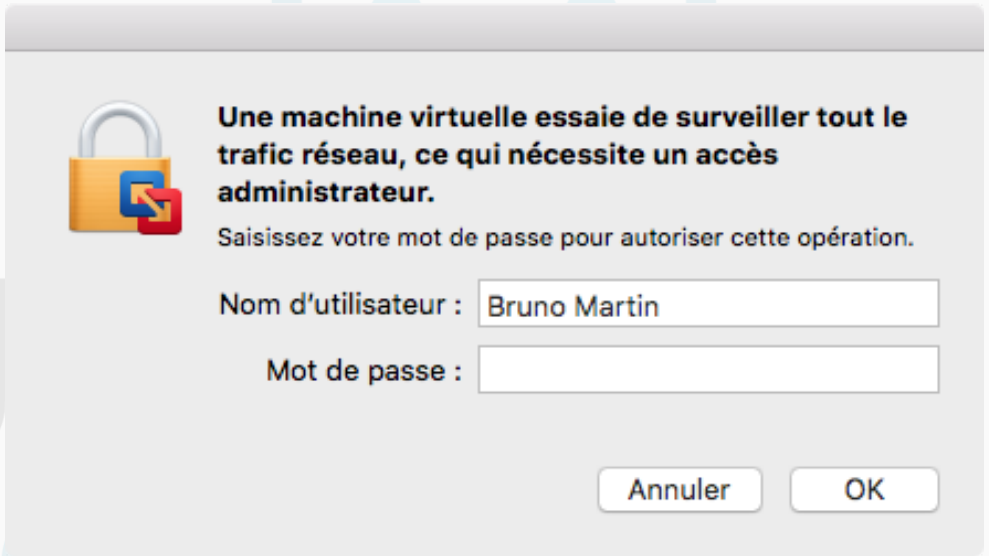


Hyperviseur de type 2

+ Réalisable facilement
+ Coût quasi-nul (VMWare Player gratuit)
- Très difficile à déployer sur un parc (installation par machine)
- Utilisation du réseau incertain (admin sur la machine)

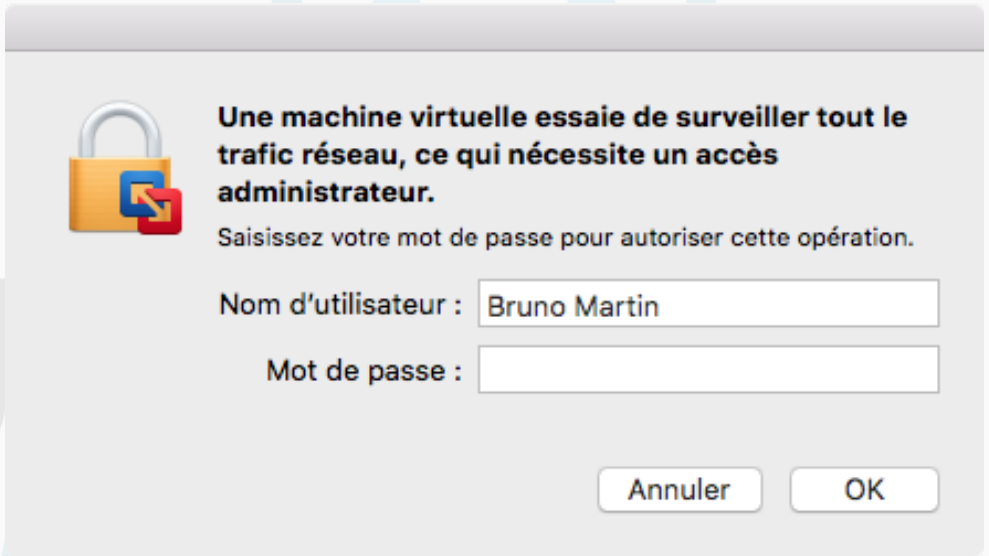
Hyperviseur de type 2

+ Réalisable facilement
+ Coût quasi-nul (VMWare Player gratuit)
- Très difficile à déployer sur un parc (installation par machine)
- Utilisation du réseau incertain (admin sur la machine)



Hyperviseur de type 2

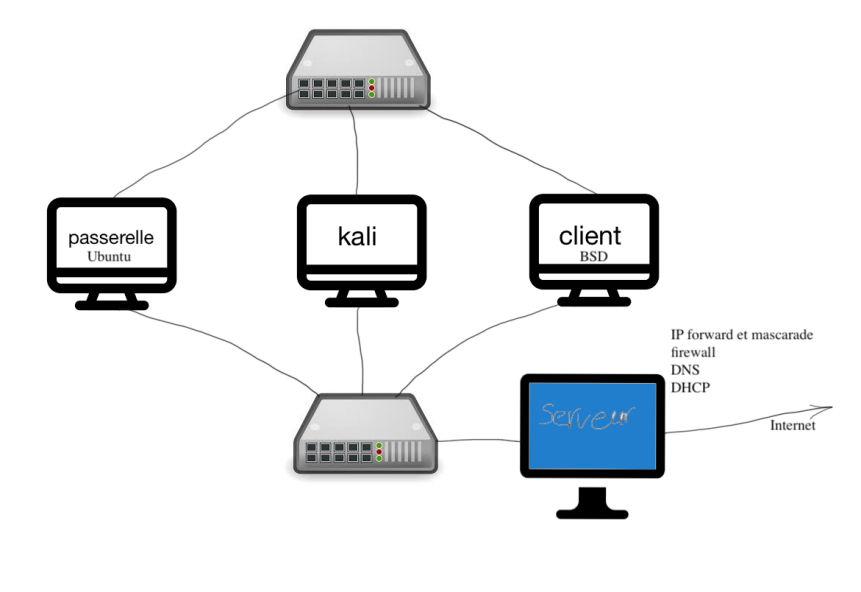
+ Réalisable facilement
+ Coût quasi-nul (VMWare Player gratuit)
- Très difficile à déployer sur un parc (installation par machine)
- Utilisation du réseau incertain (admin sur la machine)

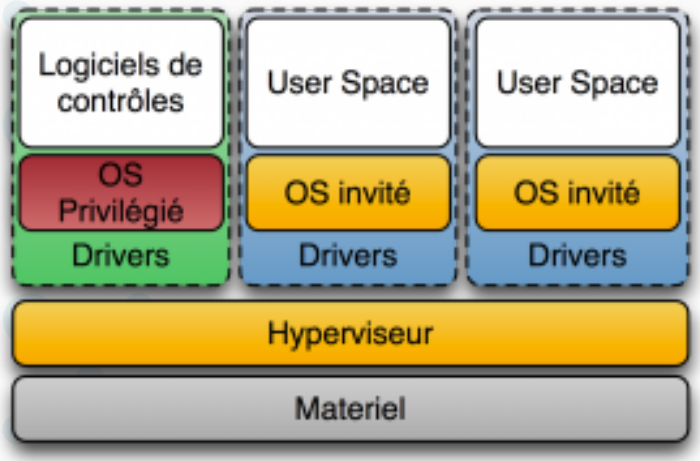


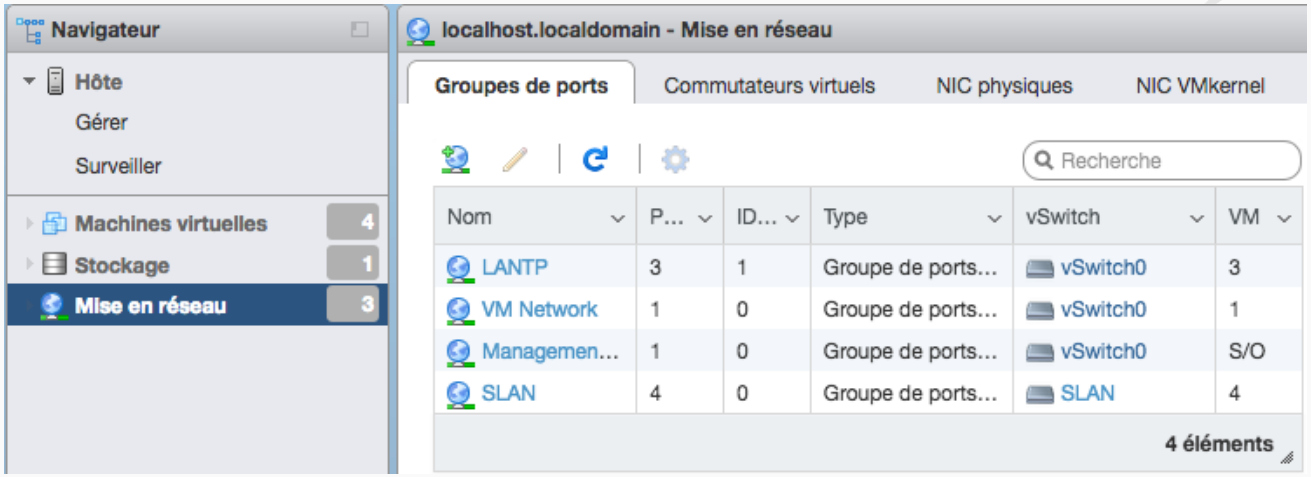
Remède : ajouter une couche de virtualisation !

Hyperviseur de type 1 virtualisé

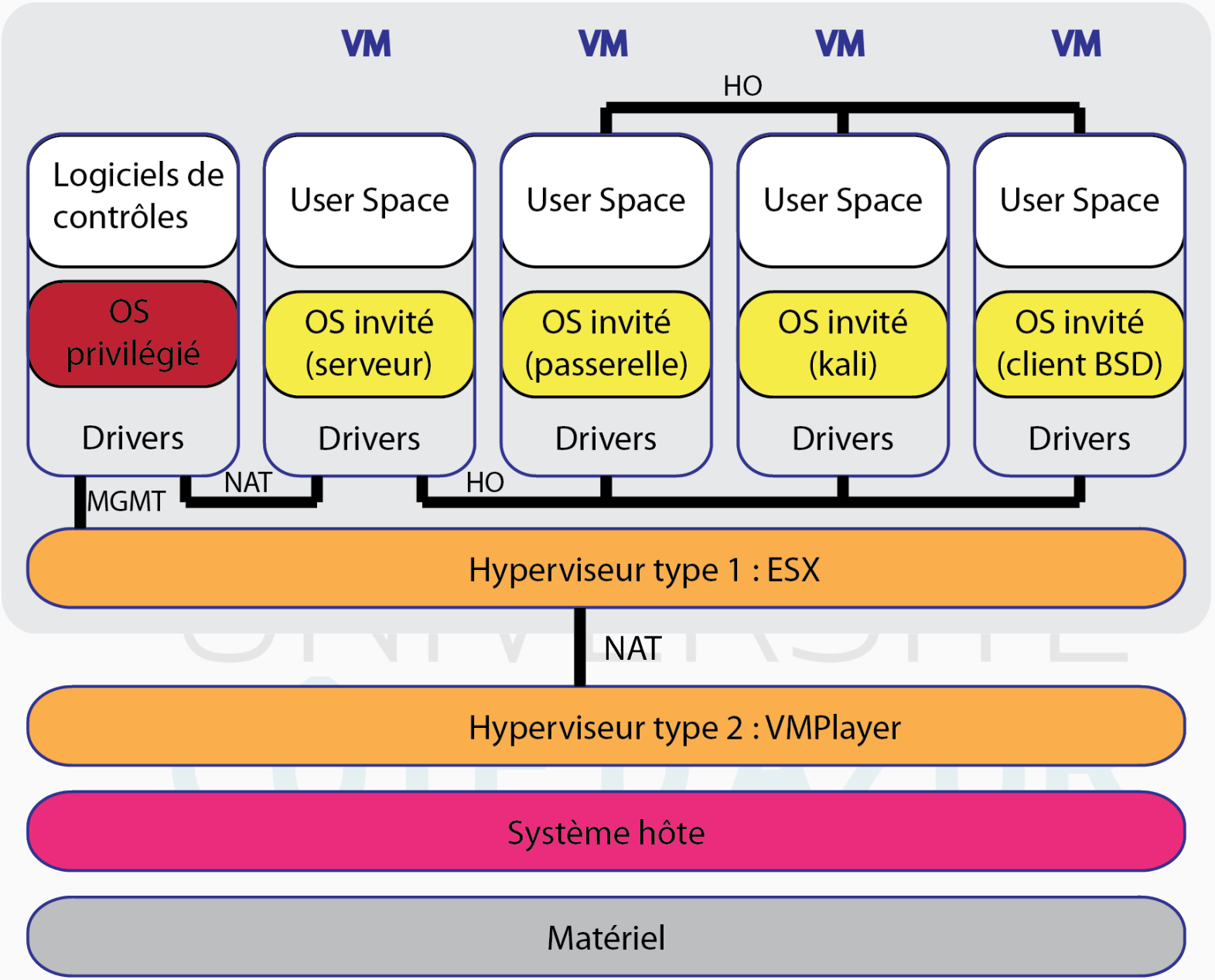
Virtualisons les VM !



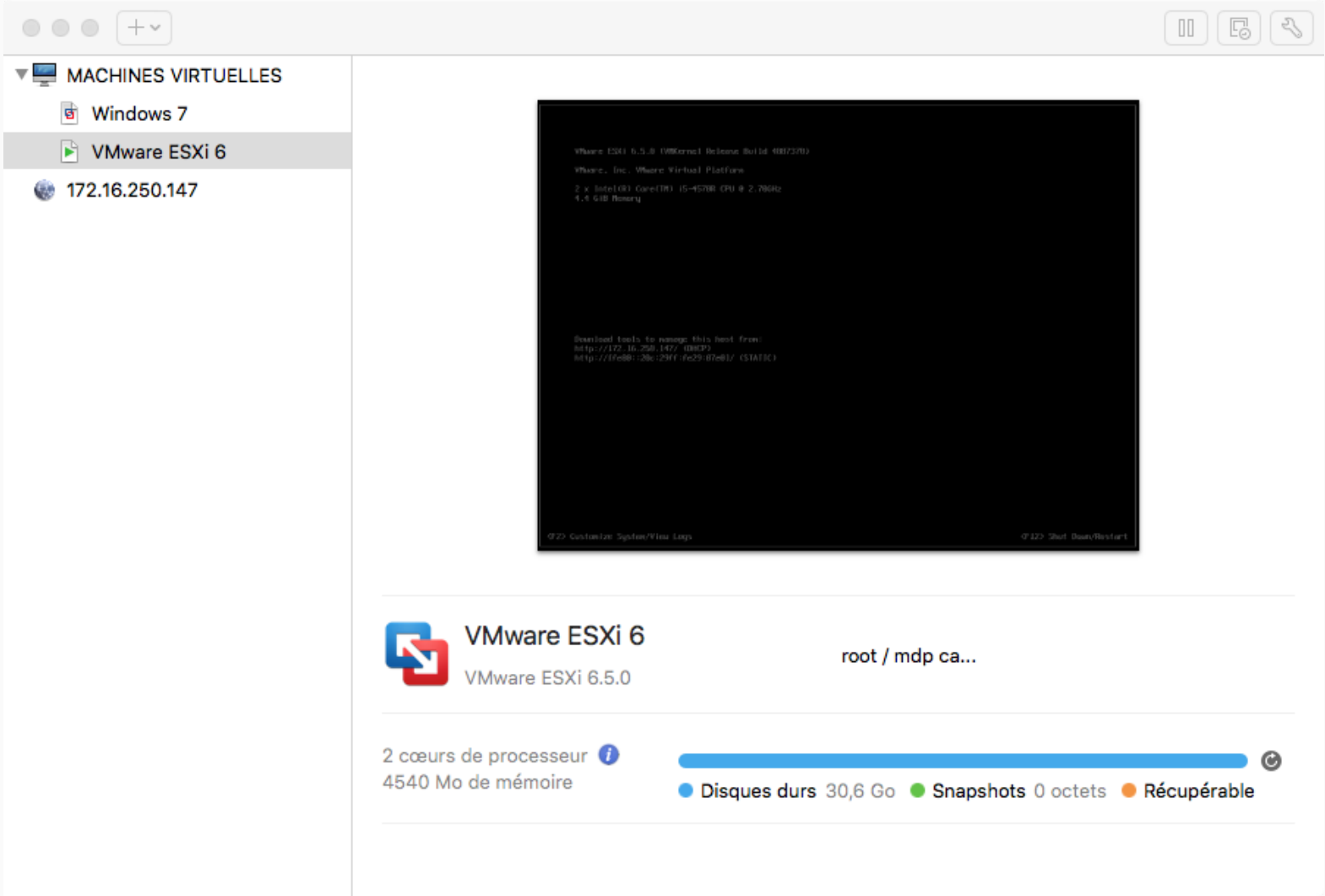




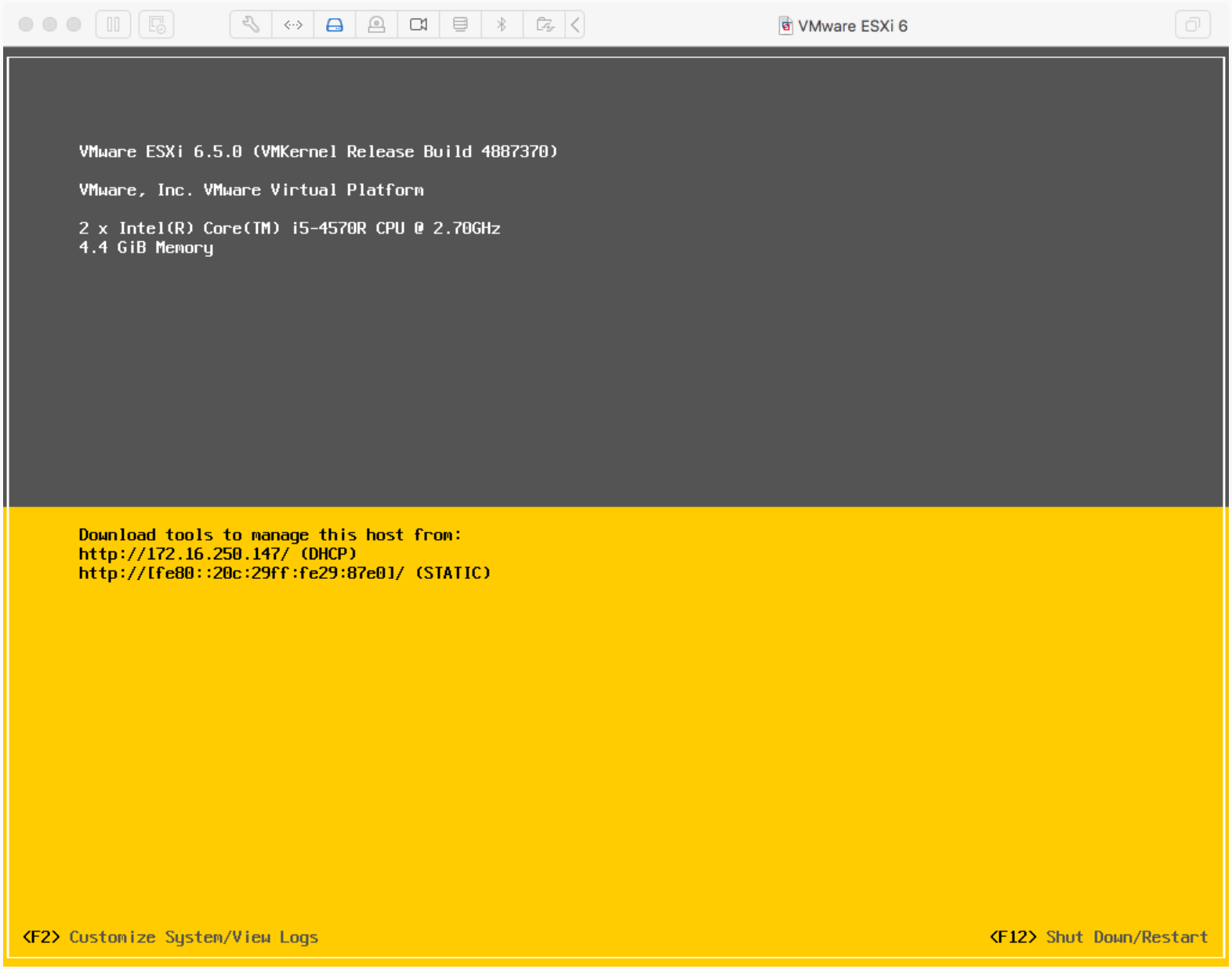
Ajout d'une couche de virtualisation



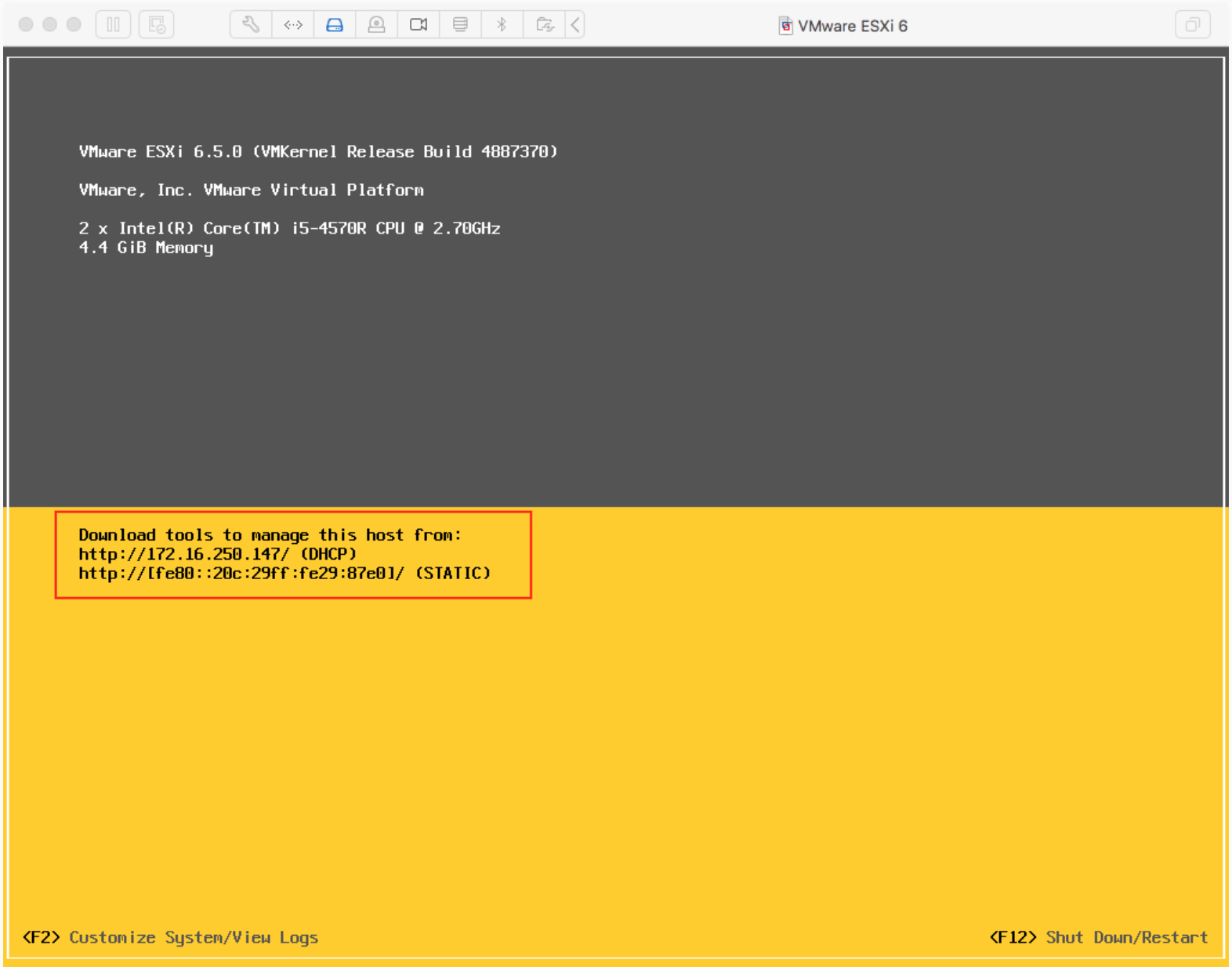
Ajout d'une couche de virtualisation : résultat



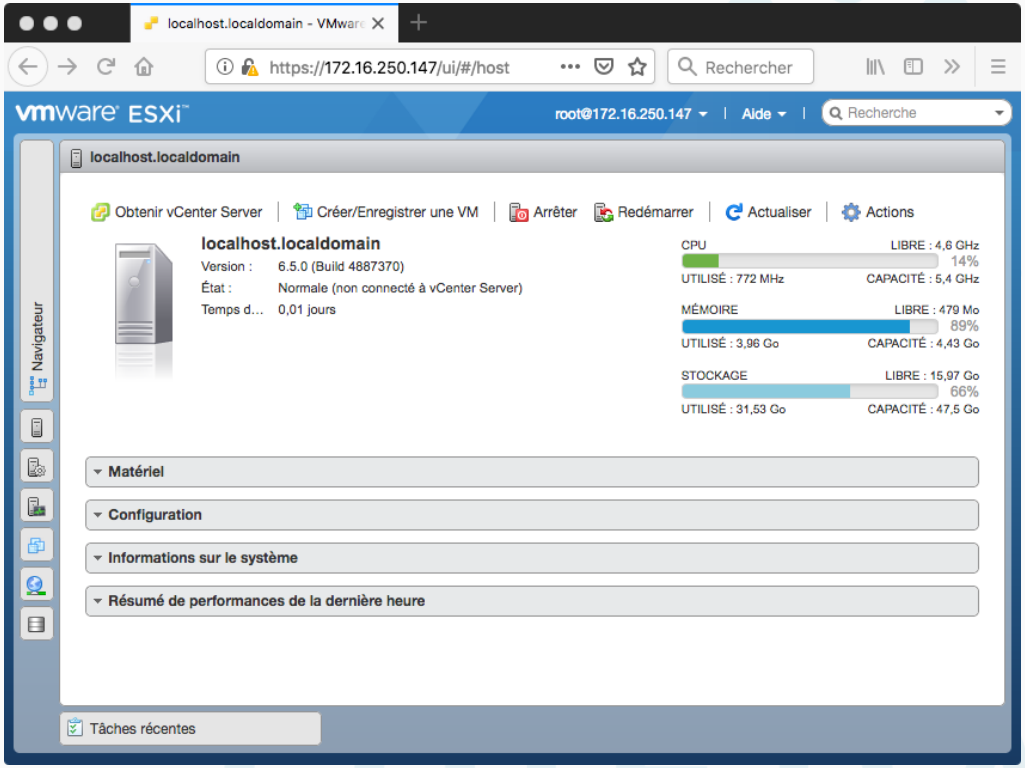
Ajout d'une couche de virtualisation : ESXi

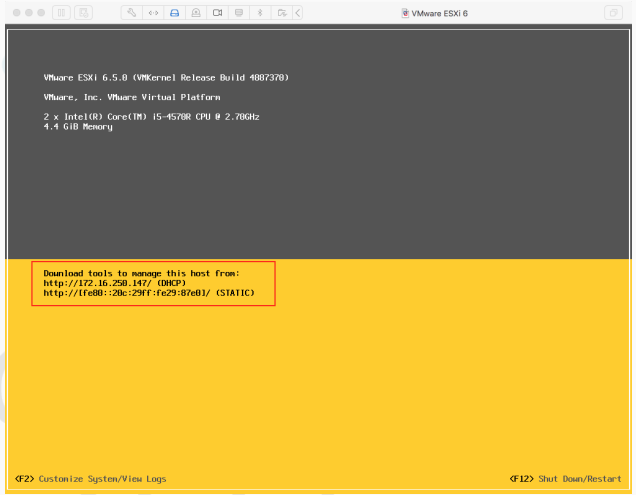


Ajout d'une couche de virtualisation : ESXi

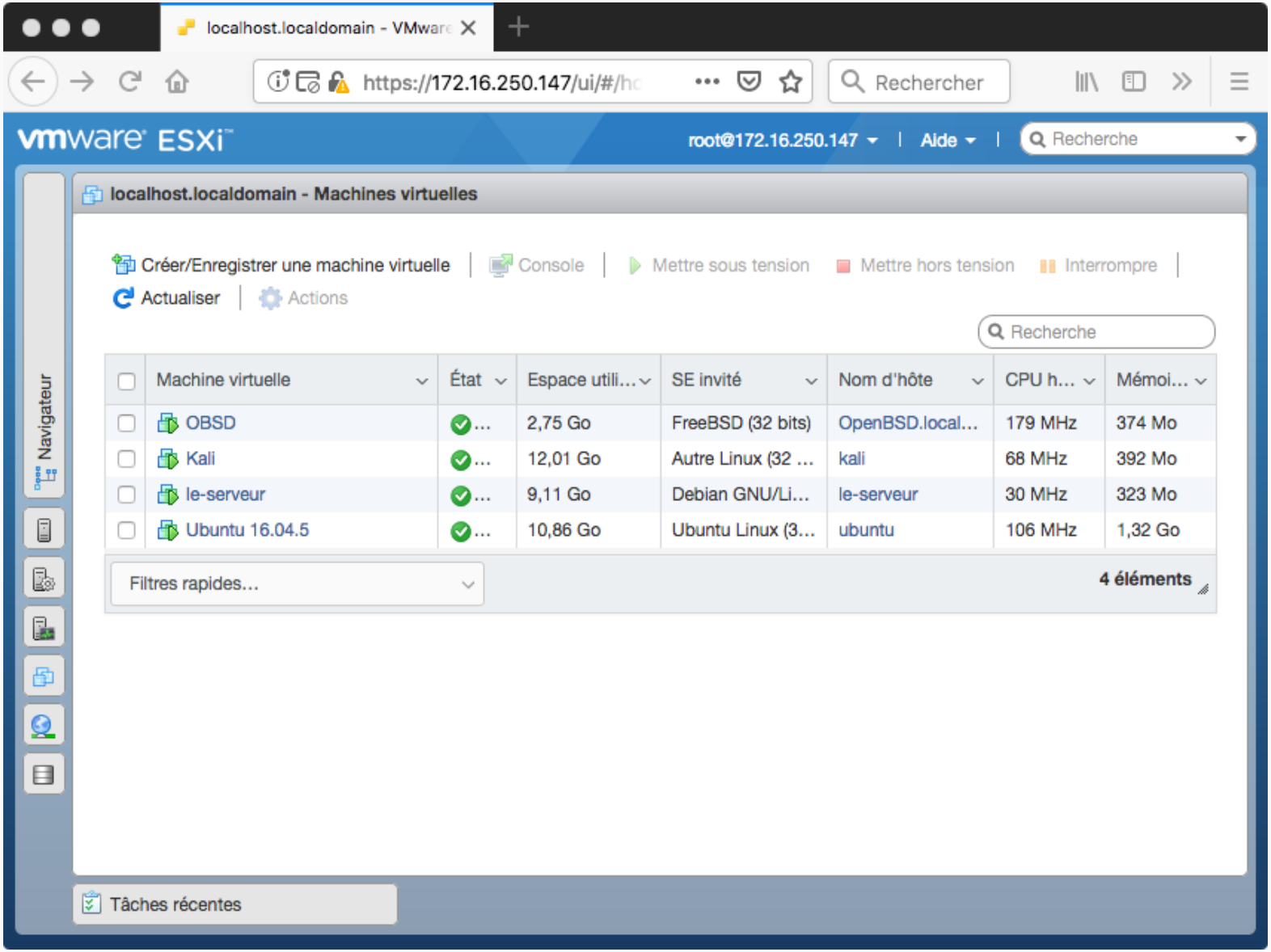


Connexion à l'ESXi

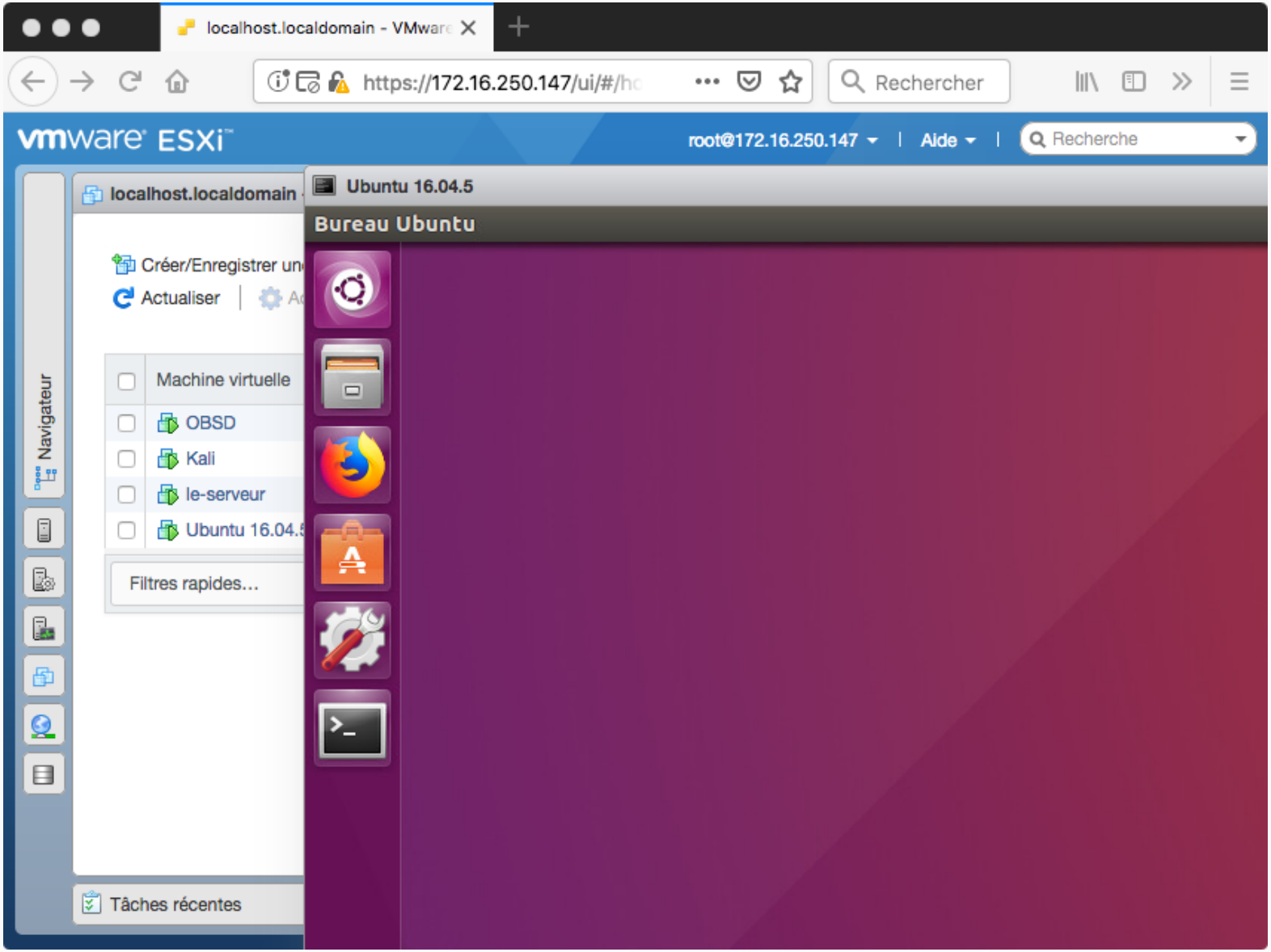




Connexion à l'ESXi : accès aux VM



Connexion à l'ESXi : accès aux VM

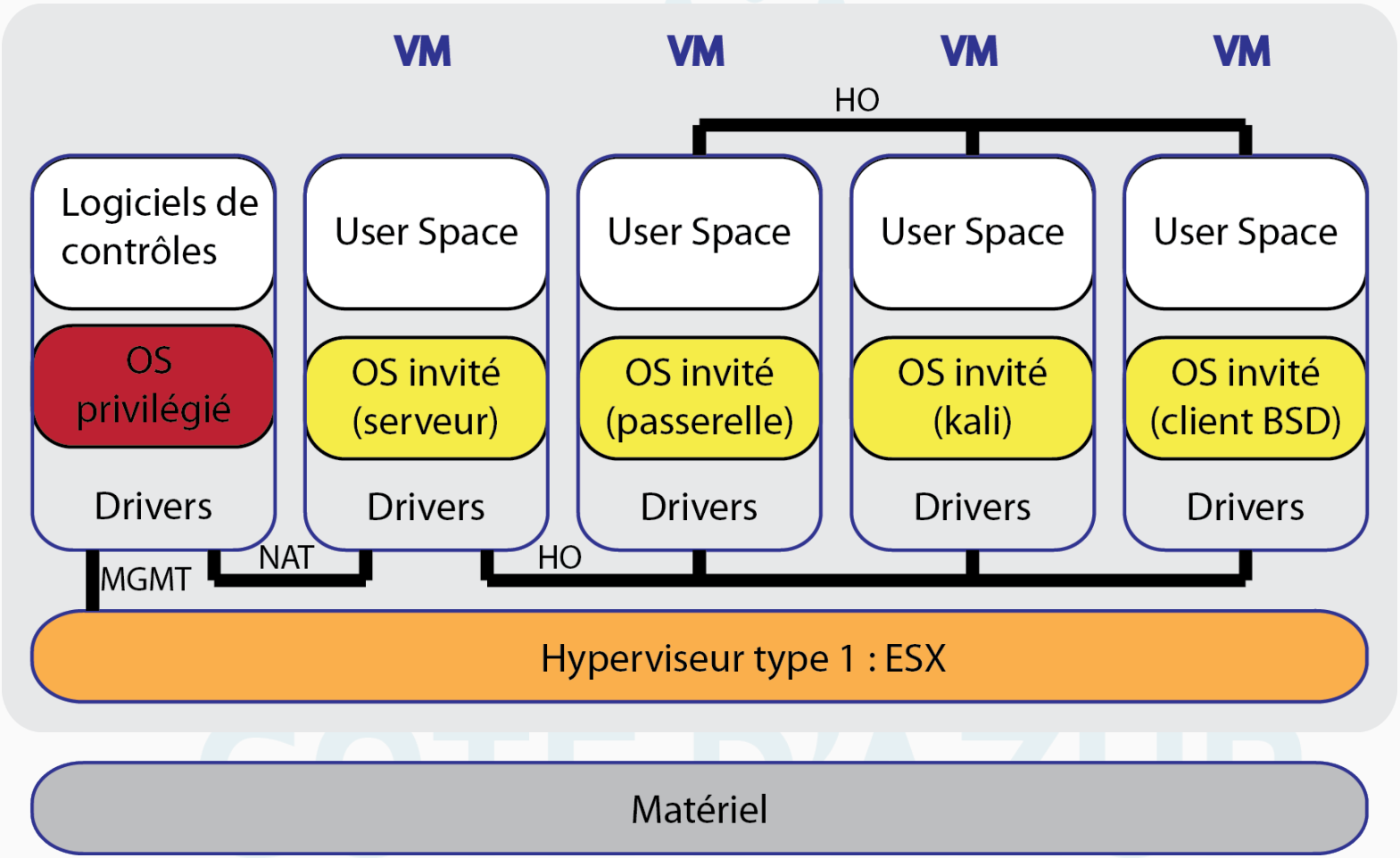


Hyperviseur de type 1 virtualisé

+ Coût quasi-nul (VMWare Player gratuit, licence ESXi gratuite)
+ Utilisation du réseau sûre (pas admin sur l'ESXi, $\neq$ rôles)
+ Utilisable sur plusieurs OS hôtes (Win, MacOS, linux)
- Réalisation assez technique
- Laborieux à déployer sur un parc (recopie de gros volumes)
- Limitation aux images 32 bits des distributions
- Mise à jour laborieuse
- Gestion de plusieurs groupes successifs quasi-impossible

Hyperviseur de type 1 (serveur)

Avec un serveur de virtualisation



Hyperviseur de type 1 non virtualisé

+ Utilisation du réseau sûre (pas admin sur l'ESXi)
+ Utilisable sur plusieurs OS hôtes (Win, MacOS, linux)
+ Pas de problème de déploiement
+ Pas de limitation aux images 32 bits des distributions
+ Possibilité d'interconnecter tout le monde (MAN)
+ Mises à jour facilitées
- Coût important (achat serveur, licence ESXi payante)
- Support technique (IE ou IR)
- Réalisation assez technique

Conclusion

Conclusion

	salle	type 2	type 1V	type 1
coût	€€€	0	0	€€
droits	root	root hôte	user	user
déploiement	⋆	⋆⋆	⋆	⋆⋆⋆
portabilité	-	⋆	⋆⋆	-
flexibilité	-	⋆⋆⋆	⋆⋆	⋆⋆⋆⋆
technicité	⋆⋆⋆	⋆	⋆⋆	⋆⋆
DNS local	oui	non	oui	oui
support	IE/IR	-	-	IE/IR
màj	⋆	⋆⋆⋆	⋆⋆	⋆⋆⋆
32/64	oui	oui	non	oui

Annonce

http://univ-cotedazur.fr/events/ecole-cybersecurite-2019