RCSO-TIC

h e p i a

Haute école du paysage, d'ingénierie et d'architecture de Genève

Sécurité d'une architecture virtualisée

§2 Analyse

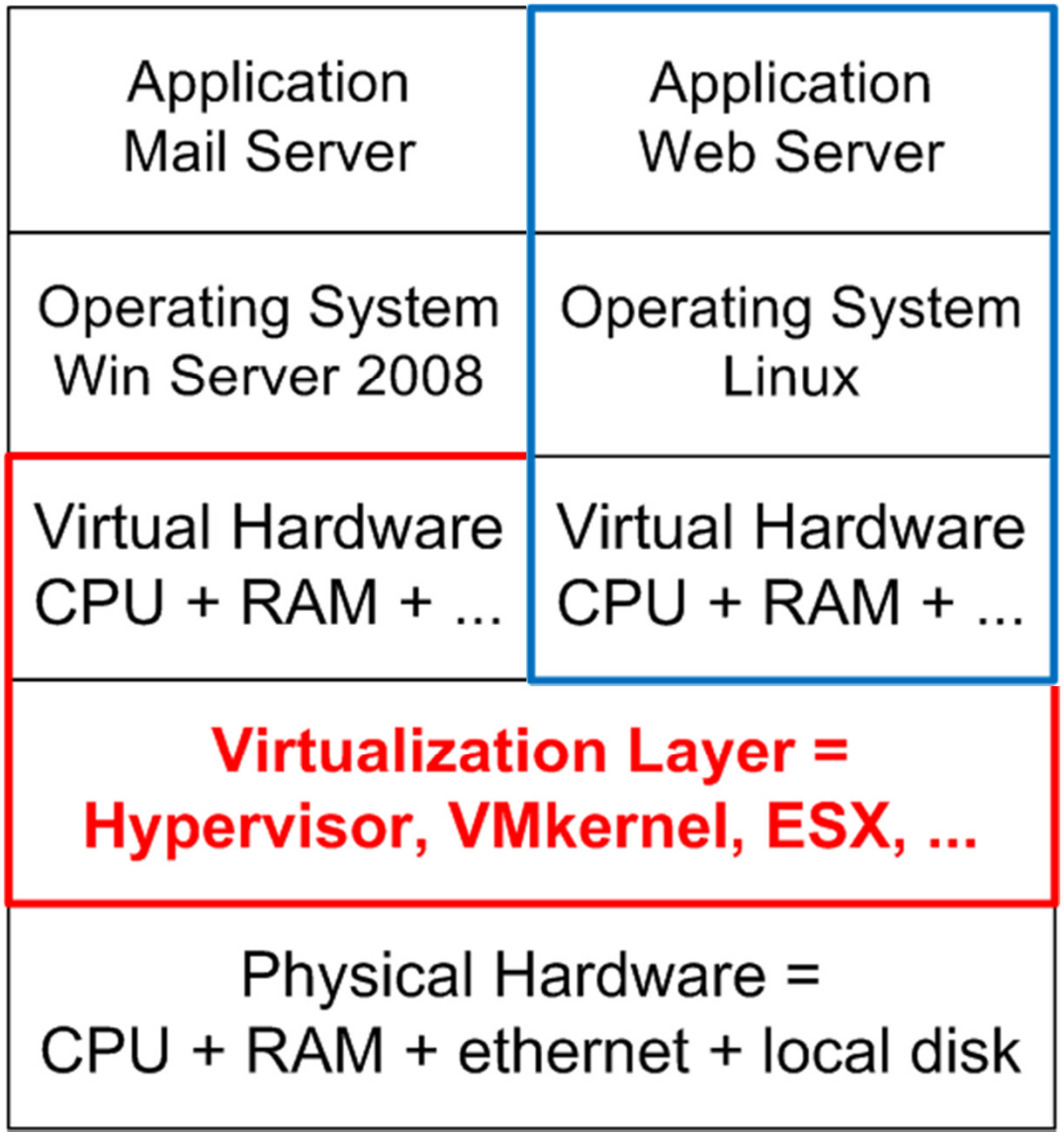
§3 Best Practices (modèle générique)

§4 Hyperviseur ESXi 4.0 (Cédric Penas)

Rapport :

http://www.tdeig.ch/visag/Security.pdf

Que signifie virtualisation ?



Virtual Machine

Chaque machine virtuelle croit posséder seule le matériel disponible

- Compatibilité binaire (OS + applic)
- Transparence (performance)
- Cloisonnement (sécurité)

Arguments commerciaux

- Meilleure utilisation du matériel → **Consolider** des serveurs
  Economie du matériel, de l'énergie consommée, des surfaces, …

- Facilité d'ajouter une machine virtuelle supplémentaire
  Souplesse d'exploitation : ajouter, tester, supprimer, sauvegarder, ..
  Technologie pour le Cloud Computing & Grid

- Gartner prédisait l'installation de 4 Mio de machines virtuelles en 2009, mais que **60% sera moins bien sécurisée** qu'avec une architecture traditionnelle

- IBM proposait la virtualisation (VM/370) **dès 1964**

Performances & disponibilité

Pour le responsable technique :

- Connaître les besoins (cahier des charges, SLA, …)
- Trouver le meilleur compromis entre coût et performances
- Surveiller certains indicateurs : charge CPUs, occupation RAM, accès disque, charge réseaux
- Choix du système de stockage, prise en compte des exigences de sécurité (pas traité dans ce projet)
- Redondance (pas traité dans ce projet)

Pour l'utilisateur :

- Serveur virtualisé doit présenter des caractéristiques semblables au serveur physique

5 principaux domaines d'un système virtualisé (§2.2)

- Réseau

  séparation, défense périmétrique

- Système

  comptes actifs, services, logs

- Management

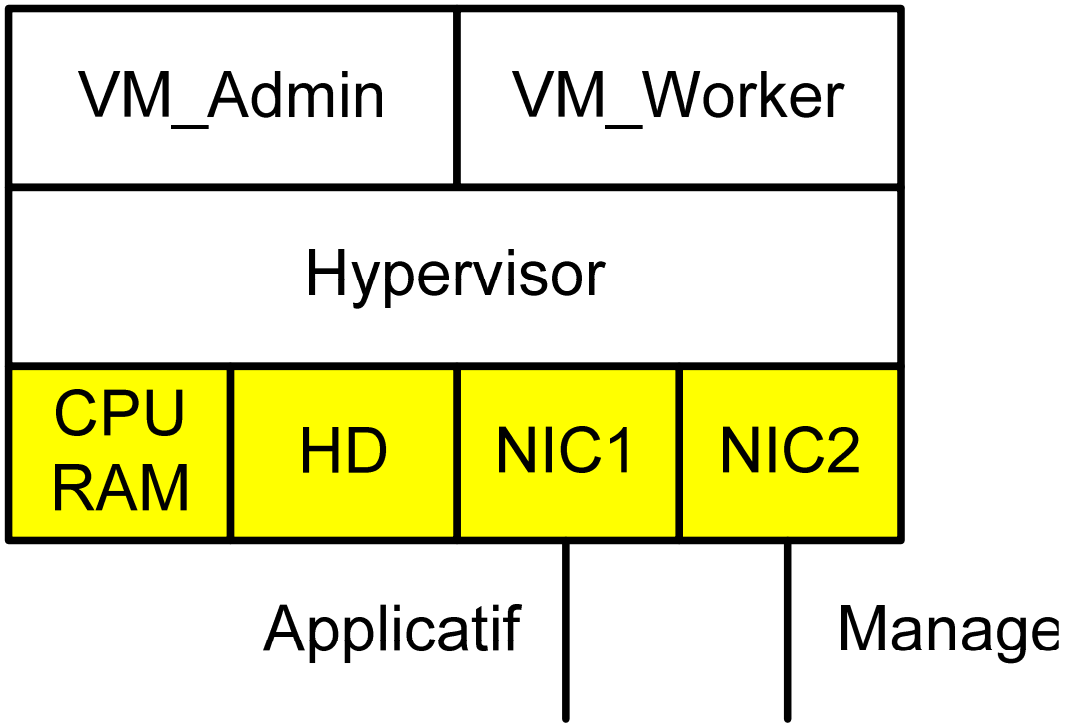
  accès distant, backup, …

- Virtualisation

  cloisonnement des VMs, …

- Applicatif

  flux, …



Risques

- Disponibilité - §2.3.1

  Réservation des ressources CPU, RAM, … QoS → ESXi 5.0

  Denial of Service

    Une VM peut monopoliser toutes les ressources → *Single point of failure*, *High value target*

    Mêmes solutions que pour le monde physique

    + limiter le nb de vCPU, ajuster des limites de charge CPU, …

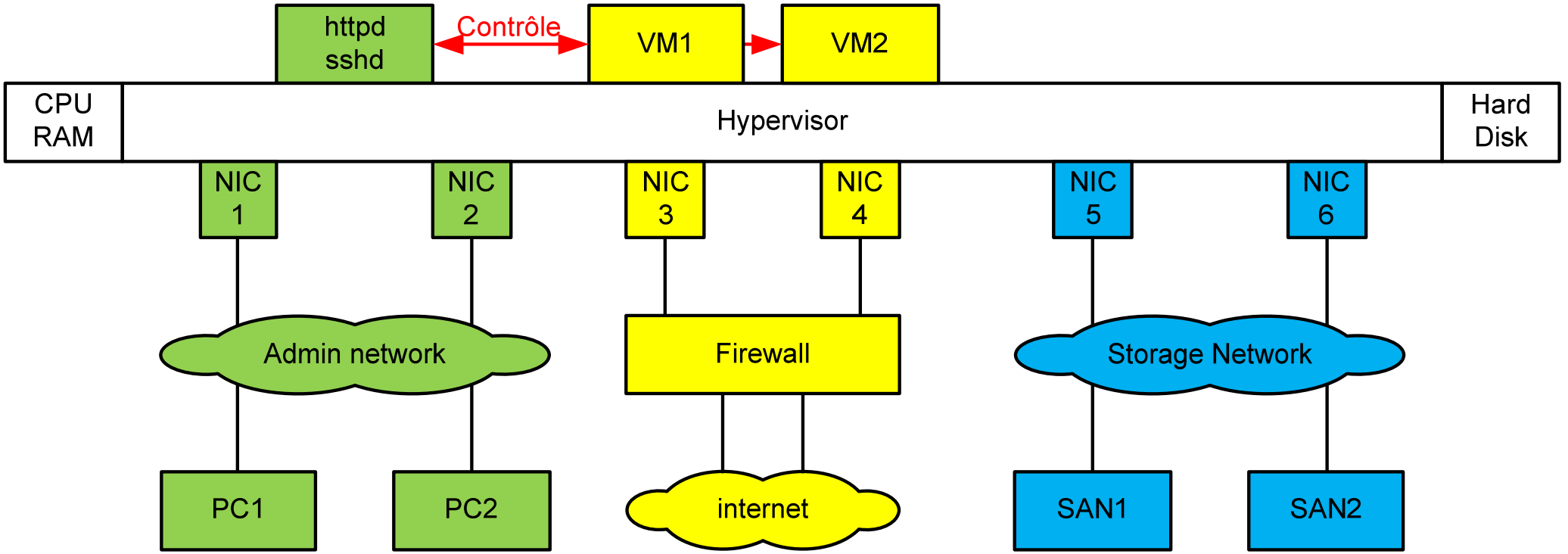
- Intégrité - §2.3.2

  Confiance dans la couche de virtualisation, les OS, les applic., …

- Confidentialité - §2.3.3

  Les méthodes classiques (séparation physique, échanges sécurisés avec SSL/TLS, IPSec, …) restent valables

Redondance et séparations physiques (§3)

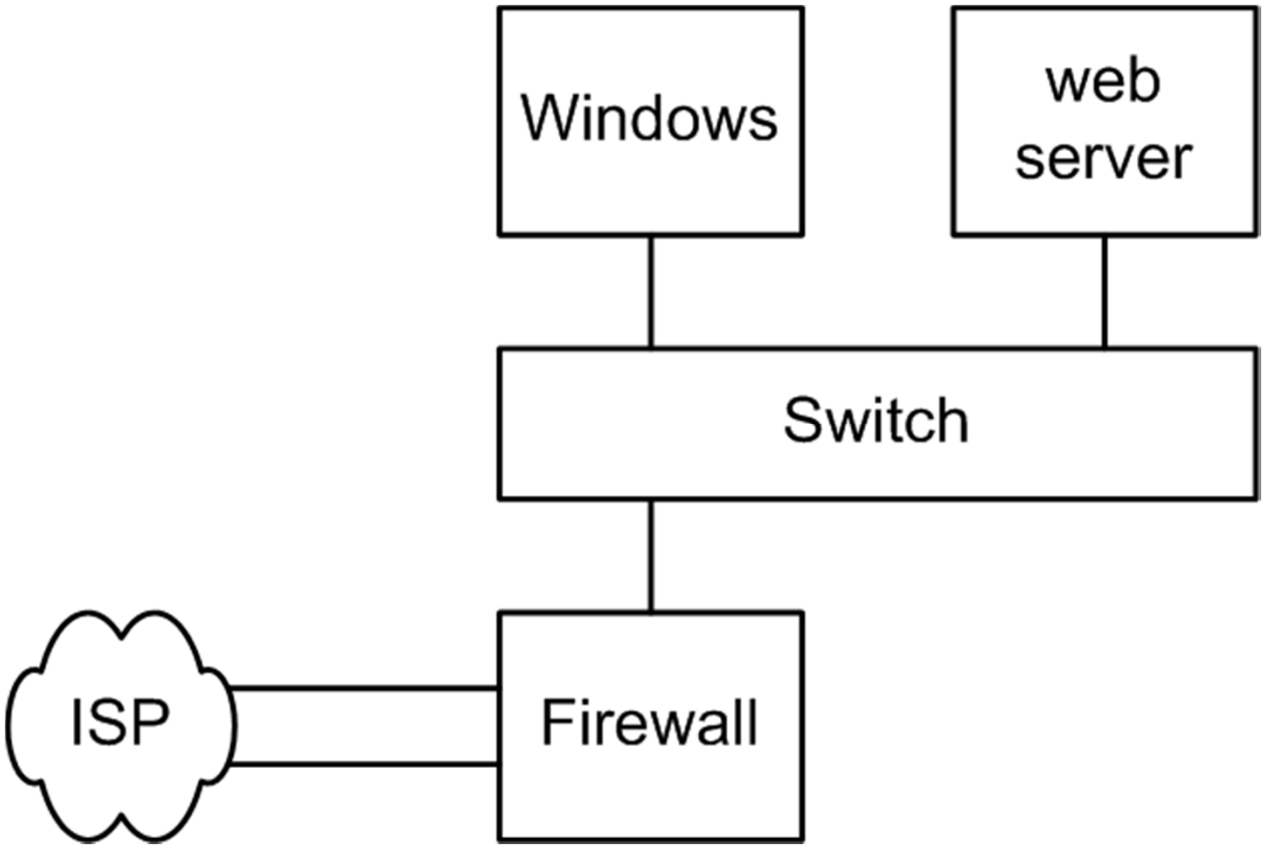


- Administration via un réseau (des hommes) de confiance
- *Storage Area Network* digne de confiance
- Risques au niveau des VMs (services) offerts sur internet

  Utiliser les bonnes pratiques sécuritaires du monde physique !

Architecture physique

Spécialistes



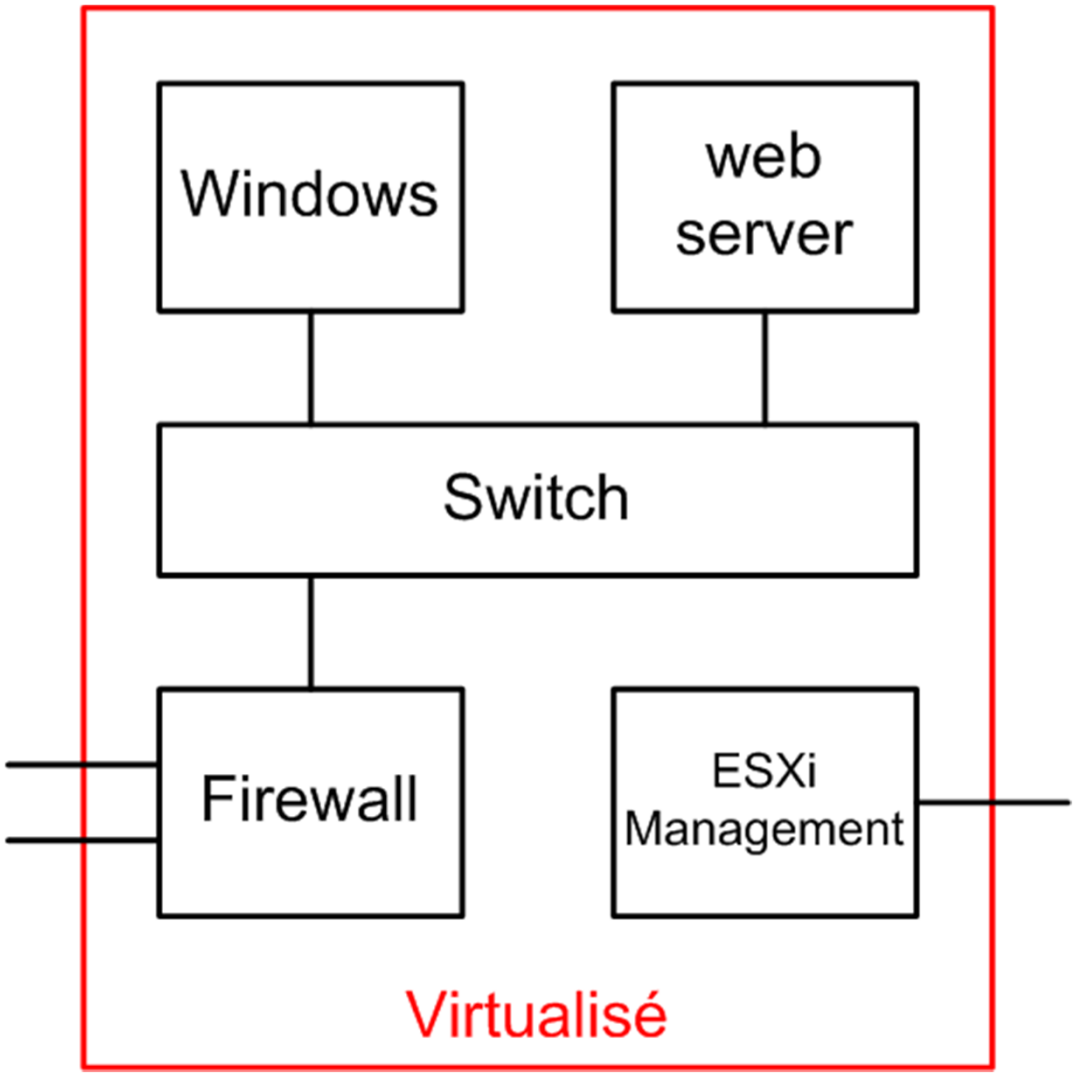
Serveurs,
Contexte applicatif

Réseau

Sécurité

Taille de l'entreprise

Architecture virtualisée



Risques

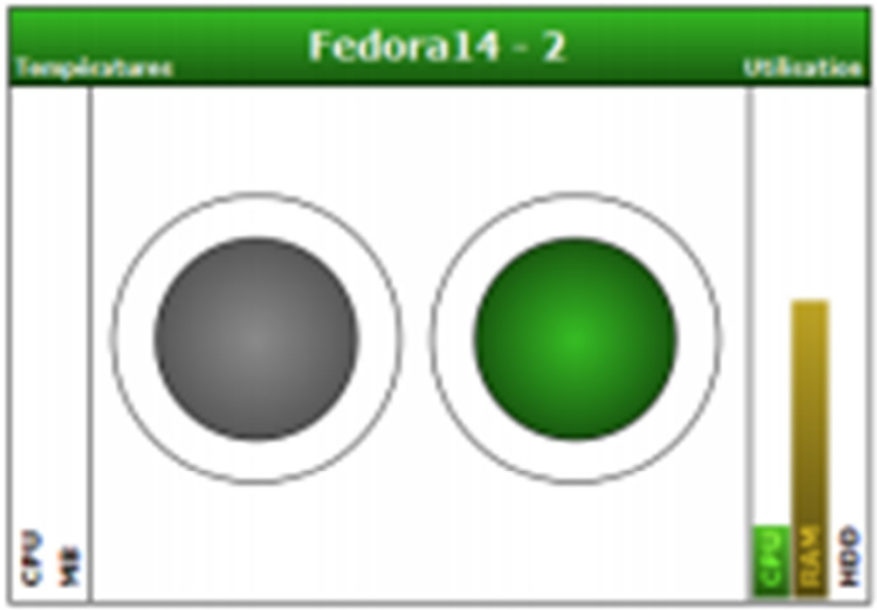
- *Misconfiguration*
- Eviter que chaque spécialiste s'occupe de problématique qu'il ne maîtrise pas
- Comprendre la virtualisation
- Très (trop) facile d'ajouter une VM de test, …

Taille de l'entreprise

Liste Machines

Nom	CPU	RAM	Disque	Température CPU	Température MB
Fedora14 - 2	14.32	58.48	0.00	0.00	0.00
VM-Fedora14-2	5.86	0/0			
VM-Fedora14-1	0.00	0/0			
Fedora14	43.08	57.55	0.00	38.00	34.00
5-Fedora-14-64bits	0.00	2047/2047			
4-Fedora-14-64bits	0.00	512/512			
3-Fedora-14-64bits	11.25	512/512			
2-Fedora-14-64bits	11.68	1024/1024			
1-Fedora-14-64bits	0.00	1024/1024			

Lionel Schaub : Enoncé Résumé Mémoire Présentation Documents

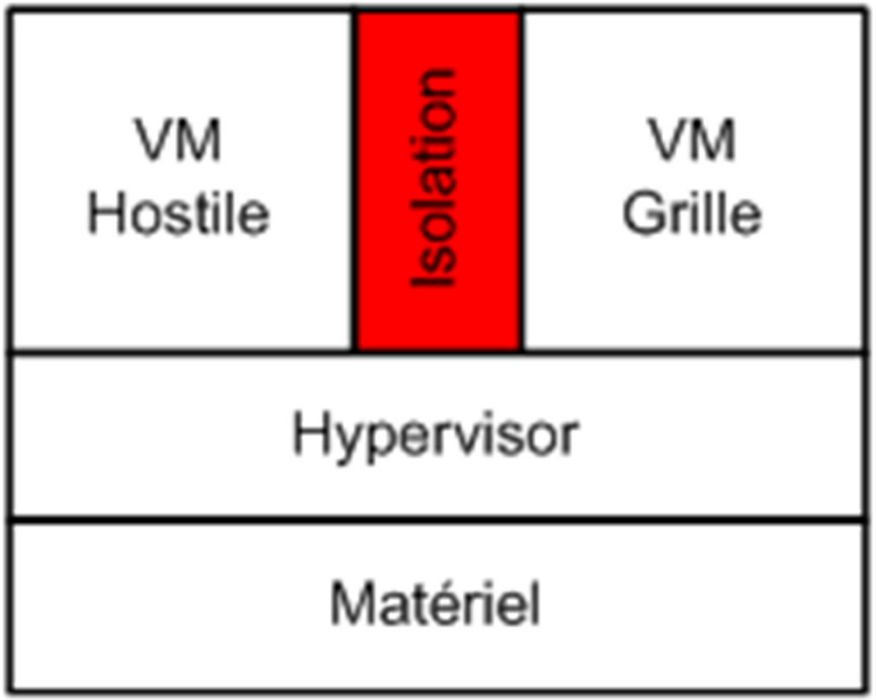


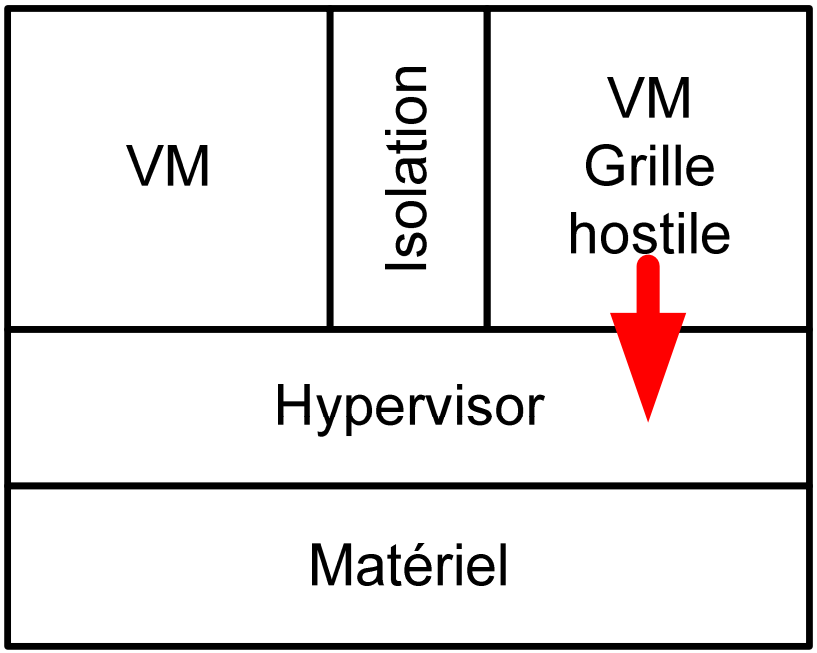
Options | Afficher les machines en bonne santé | Taille: 8% | Zoom: 100%

Connecté

Risques liés à la couche de virtualisation (§2.4)

- La virtualisation a-t-elle un impact négatif sur la sécurité ?
- Peut-on auditer une architecture virtualisée selon les principes utilisés pour le monde physique ?
- La virtualisation peut-elle augmenter la sécurité ?
- Intégrité de calcul *(VM Hopping)* et de l'hyperviseur *(VM Escape)*





Conclusion

- Hyperviseurs (ESXi, Linux-KVM) sont des composants éprouvés
  Pas d'attaque publiée sur VM Hopping ou VM Escape
  Attaque du processus web sur un processus DNS par injection DLL

- Principaux risques sont humains
  Mauvaise configuration, VMs fantômes ?, …
  Documentation à jour
  Connaître le profil (min – moy – max) des charges → références !

- Difficulté d'agir lors d'un problème (affirmation VMware)
  La couche de virtualisation complexifie le système
  Outils de supervision, formation, training (mise en condition, …)

Activités & Publications 2011

- Formation VMware 2011 suivies par 40 personnes : : Introduction & Bonne gestion

Services=20	Formation=10	Banque=8	Industrie=2
50%	25%	20%	5%

- Premier Labo Linux-KVM pour les étudiants Bachelor
- Travail de Bachelor de **Lionel Schaub** : Enoncé Résumé Mémoire
- Etude de **Raphaël Babel** & **Amine Ouadahi**
- Projet Visag : Descriptif Security_Analysis Flyer
- Projet de semestre Bachelor de **Benoit-Georges Chalut** : Enoncé F
- Projet de semestre Bachelor de **Justin-Karim Mbongueng** : Enonce
- Projet d'approfondissement Master de **Sébastien Pasche** : Enoncé