La virtualisation, si simple!

par Michel Guy Paiement

Les mardi 15 juin 2010 &
jeudi 17 juin 2010

Securecom Services Conseils inc.
507, Place D'Armes, bureau 1160
Montréal, Québec
H2Y 2W8
Tél: 514 544-0442
info@securesc.ca

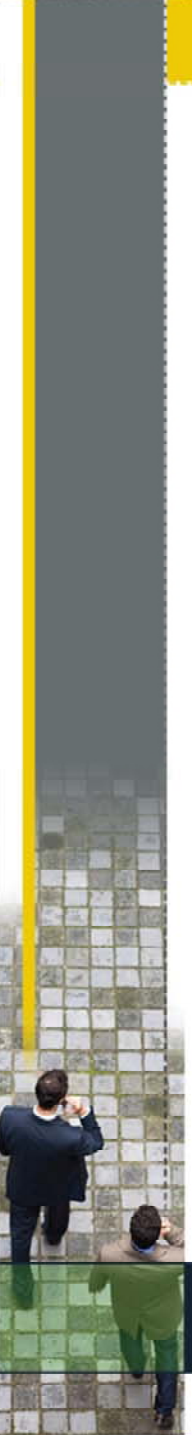
Agenda

- Mise en contexte
- Les types de virtualisation
- Questionnement…
- La sécurité 001
- Évolution dans l'architecture
- Les enjeux de sécurité
  - Les aspects systémique et procédurale
  - Les aspects technologiques
  - Les aspects légaux
- Que nous réserve l'avenir
- En conclusion

Mise en contexte (1/3)

Historiquement

- On est passé de l'ordinateur central (« MainFrame »)
- Au « middleware »
- Aux environnements distribués
- Que l'on a spécialisé et fait évolué avec
  les nouveaux paradigmes informatiques (i.e. SOA)



Mise en contexte (2/3)

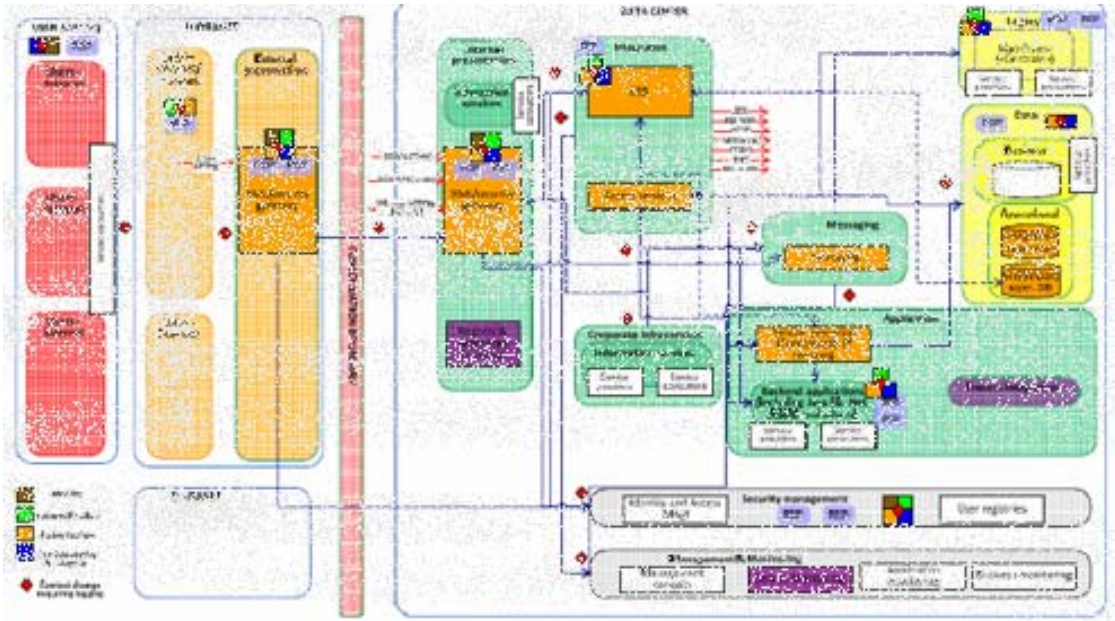
Alors pourquoi virtualiser?

- L'Augmentation des besoins applicatifs des entreprises afin de répondre aux opportunités et/ou aux besoins d'affaires)
- L'augmentation drastique des coûts associés à l'infrastructure
- Le besoin d'être compétitif
- Diminution des coûts associés au matériel

=> Le besoin d'efficience

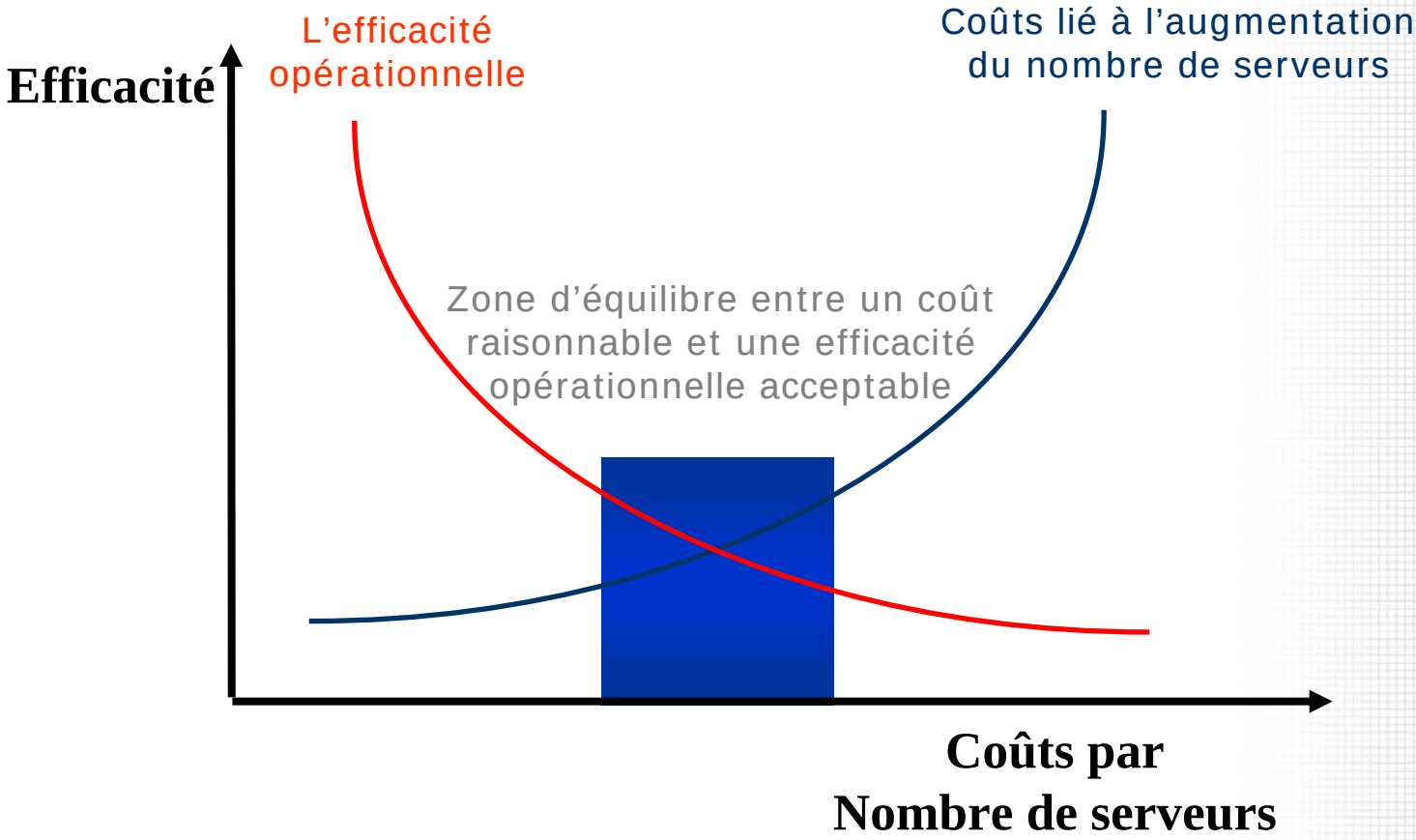
Mise en contexte (3/3)

le besoin d'efficience, parce qu'on est partie d'environnement simple à des environnements tel que :



Mise en contexte (3/3)

Impliquant ainsi :



Type de virtualisation (1/1)

Les principaux modes de virtualisation :

- **Émulation**
  - Simulation intégrale du matériel
  - Ex – Hercule, QEMU, PearPC, Bochs
  - Principe des émulateurs des vieux ordinateurs/consoles de jeu (Amiga, Atari, etc).
- **Virtualisation partielle**
  - Partage de ressources matérielles par abstraction
  - Implémentation répandue telle que l'adressage virtuel des processus
  - Ex - Linux, Windows, etc.
- **Virtualisation complète**
  - Systèmes invités tels quels l'« Emulation » du matériel virtuel
  - Ex - VMware Workstation et VMware Server, Virtual PC, etc.
- **Para-virtualisation et virtualisation assisté par le matériel**
  - Nécessite « l'aide » du système invité
    ou
  - L'aide du matériel spécifique (aujourd'hui répandu)
  - Ex - Hyper-V, ESX/ESXi, Xen.

Questions? (1/1)

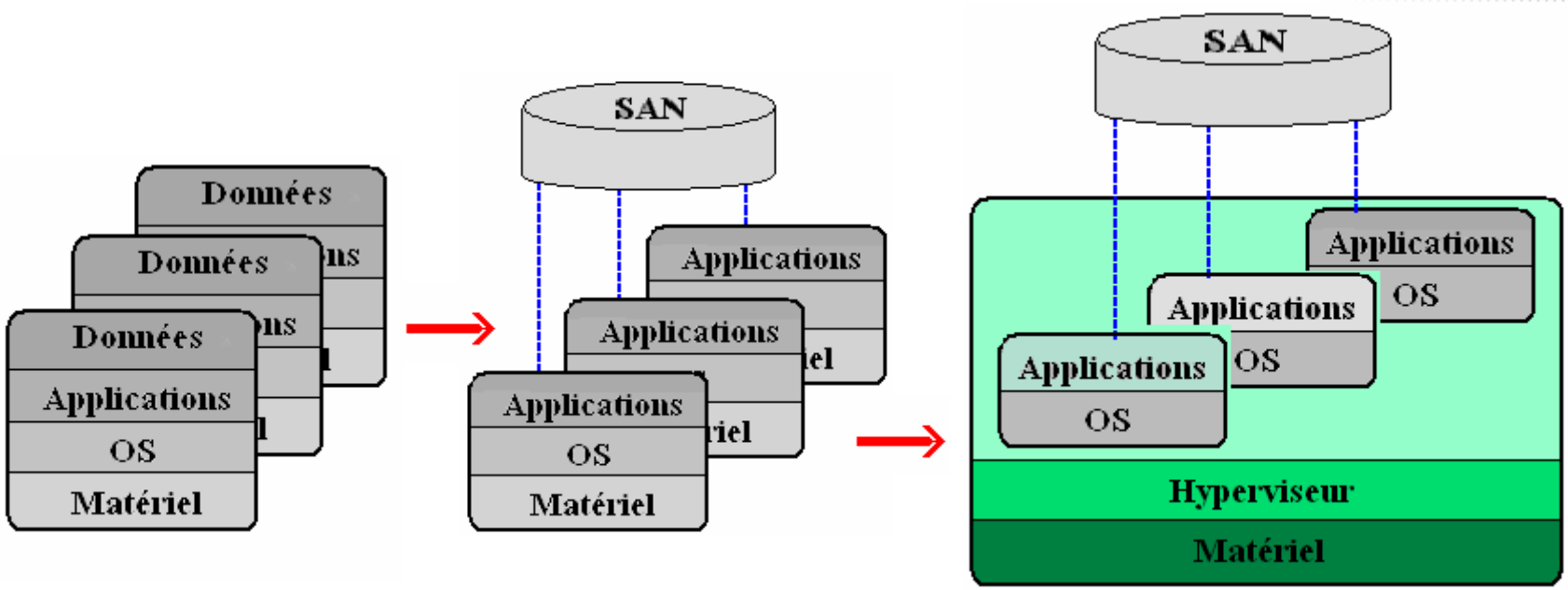
- **Mais cette technologie répond-elle à l'ensemble de nos besoins fonctionnels et non fonctionnels ?**
  (Tels que : Maintenabilité, Opérabilité, Performance, Sécurité, Etc…)
- **À t-on pris en compte ce nouveau niveau d'abstraction dans les processus de l'entreprise?**
- **Voyons d'un peu plus près lorsque l'on parle de sécurité !**

Sécurité – 001

On peut représenter la sécurité et ses mécanismes :

Architecture (1/3)

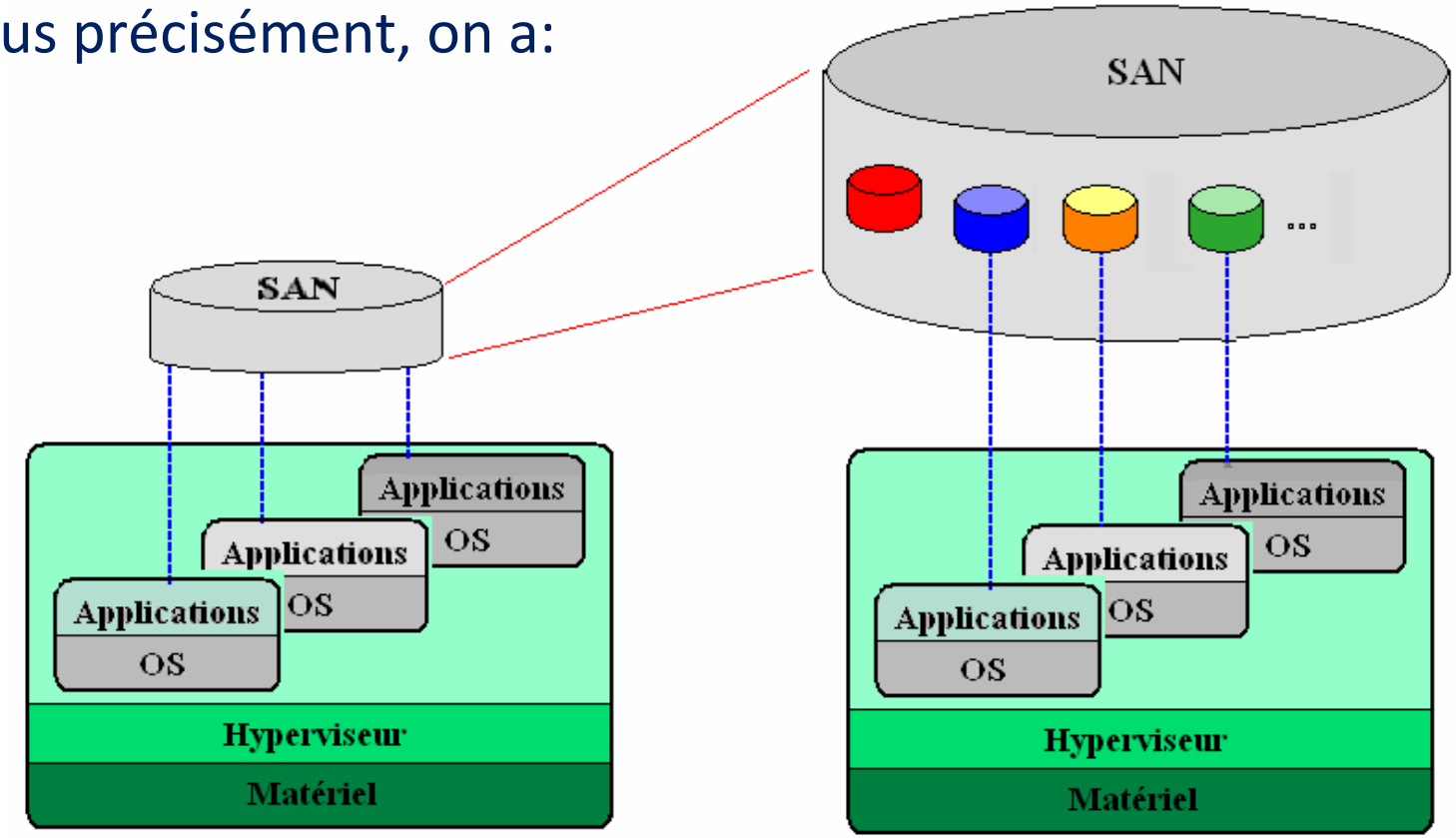
L'architecture a évoluée de la façon suivante:



Au temps 1 Au temps 2 Au temps 3

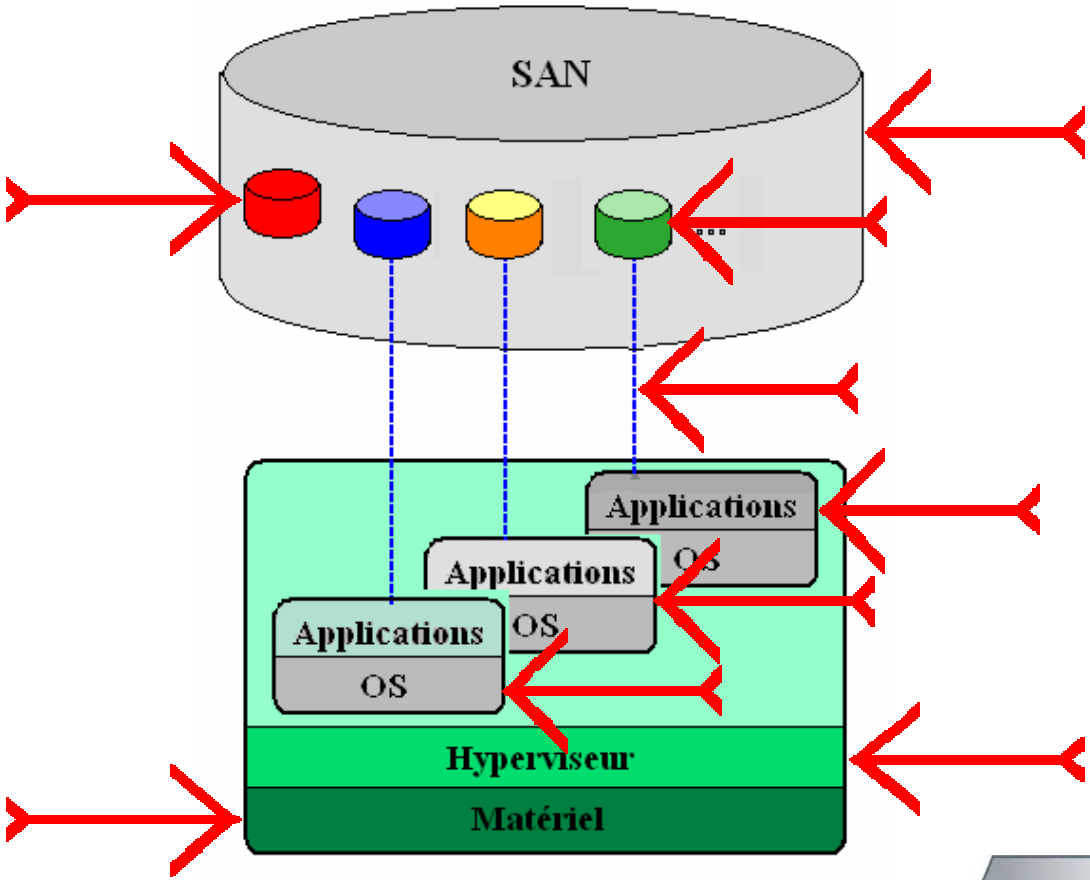
Architecture (2/3)

Plus précisément, on a:



Architecture (3/3)

Vulnérabilités à exploiter :



Les enjeux de sécurité de la virtualisation (1/3)

Aspects systémiques ou procédurales :

- Un niveau d'abstraction supplémentaire
- Concentration de ressources
- Variabilité des états de chacune des instances
- Variabilité du niveau de sécurité de ch. des instances
- Besoin de mise à jour des « politiques, normes, procédures et directives de l'entreprise:
  - Définition des responsabilités (qui fait quoi?)
  - L'encadrement des taches (qui peut faire quoi?)
  - Etc…

Les enjeux de sécurité de la virtualisation (2/3)

Aspects Technologiques :

- Les aspects fonctionnels:
  - Le contrôle d'accès à l'hyperviseur
  - Mise à jour des correctifs
  - Difficultés du « monitoring » des états des instances virtualisées.
- Les aspects non fonctionnels:
  - Mobilité accrue des composantes virtualisées

Les enjeux de sécurité de la virtualisation (3/3)

Aspects légaux & règlementaires :

- PCI-DSS
- Les lois encadrant les aspects financiers telles que : Loi 198, SOX, etc..
- La protection des renseignements personnels
- La protection des ressources de l'entreprise (les aspects liés à l'avoir des actionnaires, etc.)
- Etc…

Et l'avenir

- **Le « cloud computing »**
- **Les organisations virtuelles**
- **Utilisation possible en sécurité**
- **Etc…**

Utilisations possible (en sécurité) :

- Instanciation des mécanismes de sécurité
  (i.e. - identification & authentification, coupe-feux, etc.)
- Consolidation en « backend » d'outils de surveillance et de tableau de bord (i.e. – audit, IPS, IDS)
- Mise en place d'outils de détection et de capture d'intrusion (à la « Honey Pots »)
  (i.e. Collapsar)
- Etc…

En conclusion

La technologie évolue très rapidement, plus rapidement que les divers systèmes existants (entreprises, gouvernements, organisations, etc).

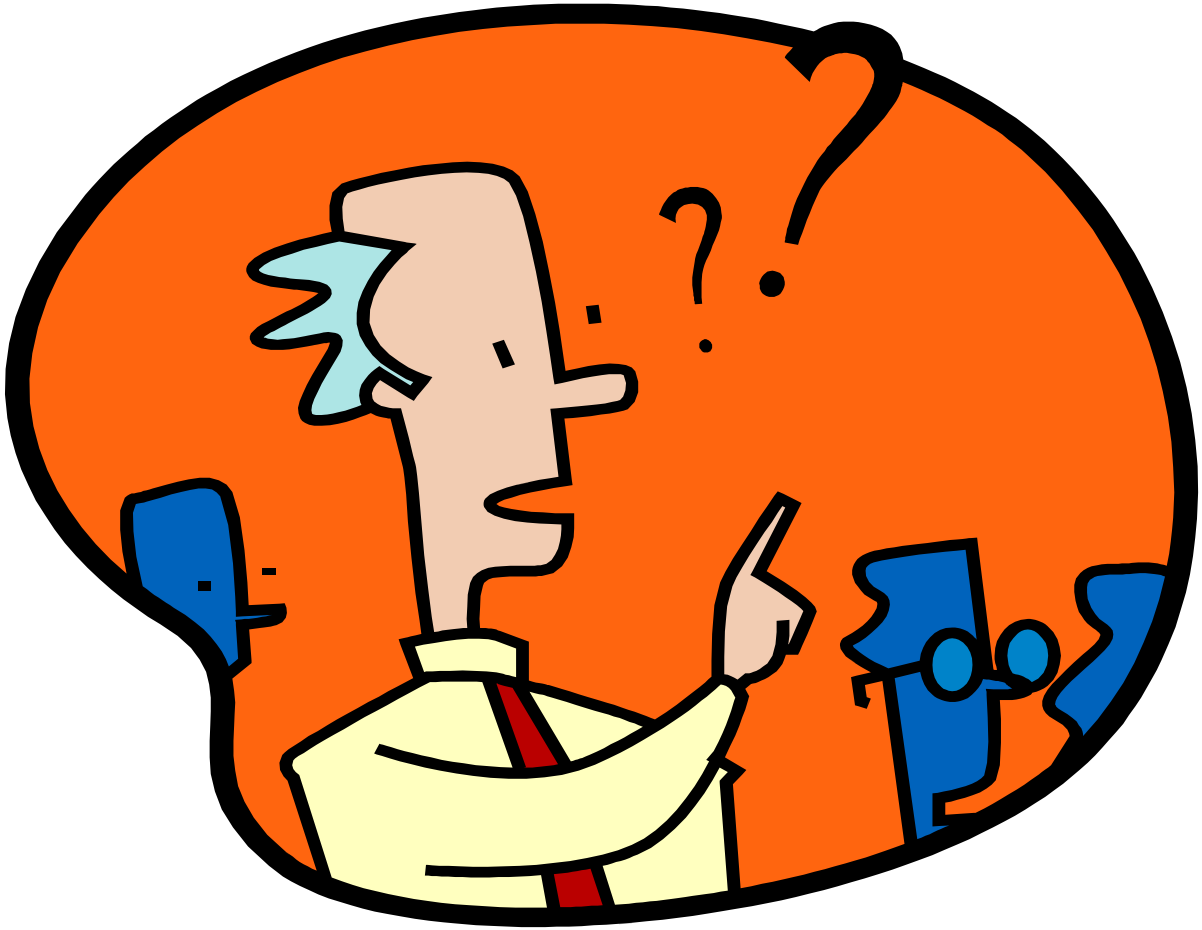
Il importe donc de s'assurer que les aspects non fonctionnels soient pris en compte au tout début de processus d'évolution des besoins technologiques.

Si non, advienne que pourra…

En conclusion (ce qu'il faut faire) :

- Mettre à jour les « Politiques, Normes, directives et procédures » de l'entreprise
- Identifier précisément les rôles et responsabilités de l'infrastructure de virtualisation et des instances y étant installées
- Initier les éléments technologiques dont découleront les mécanismes de sécurité
- Identifier et mettre en place de mesures d'atténuation du risques (de gestion, de techno, etc.)
- Etc…

Questions



Quelques références…

- ***When Virtual is Harder than Real: Resource Allocation Challenges in Virtual Machine Based IT Environments*****,** by Ludmila Cherkasova, Diwaker Gupta, Amin Vahdat, Enterprise Systems and Software Laboratory, HP Laboratories Palo Alto, 2007

- ***Vers une meilleure compréhension de l'organisation virtuelle***, par Becheikh, N. & Zhan, Faculté des sciences de administration, Université Laval, 1999.

- ***Cloud Computing***, by VmWare Corp.
  Voir l'URL : *http://www.vmware.com/solutions/cloud-computing/*
  Consulté le 31 mai 2010.

- ***Collapsar: A VM-Based Architecture for Network Attack Detention Center***, by Xuxian Jiang, Dongyan Xu, Computer Sciences Dept., Purdue University.

- ***PCI-DSS*** *Voir l'URL : https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml*

- ***Cybersecurity Act of 2010 (S. 773)***, consulté le 9 juin 2010, Sénat américain,
  Voir l'URL : *http://commerce.senate.gov/public/?a=Files.Serve&File_id=29daa3d9-291e-46ce-aba9-f2348f4c0d0d*