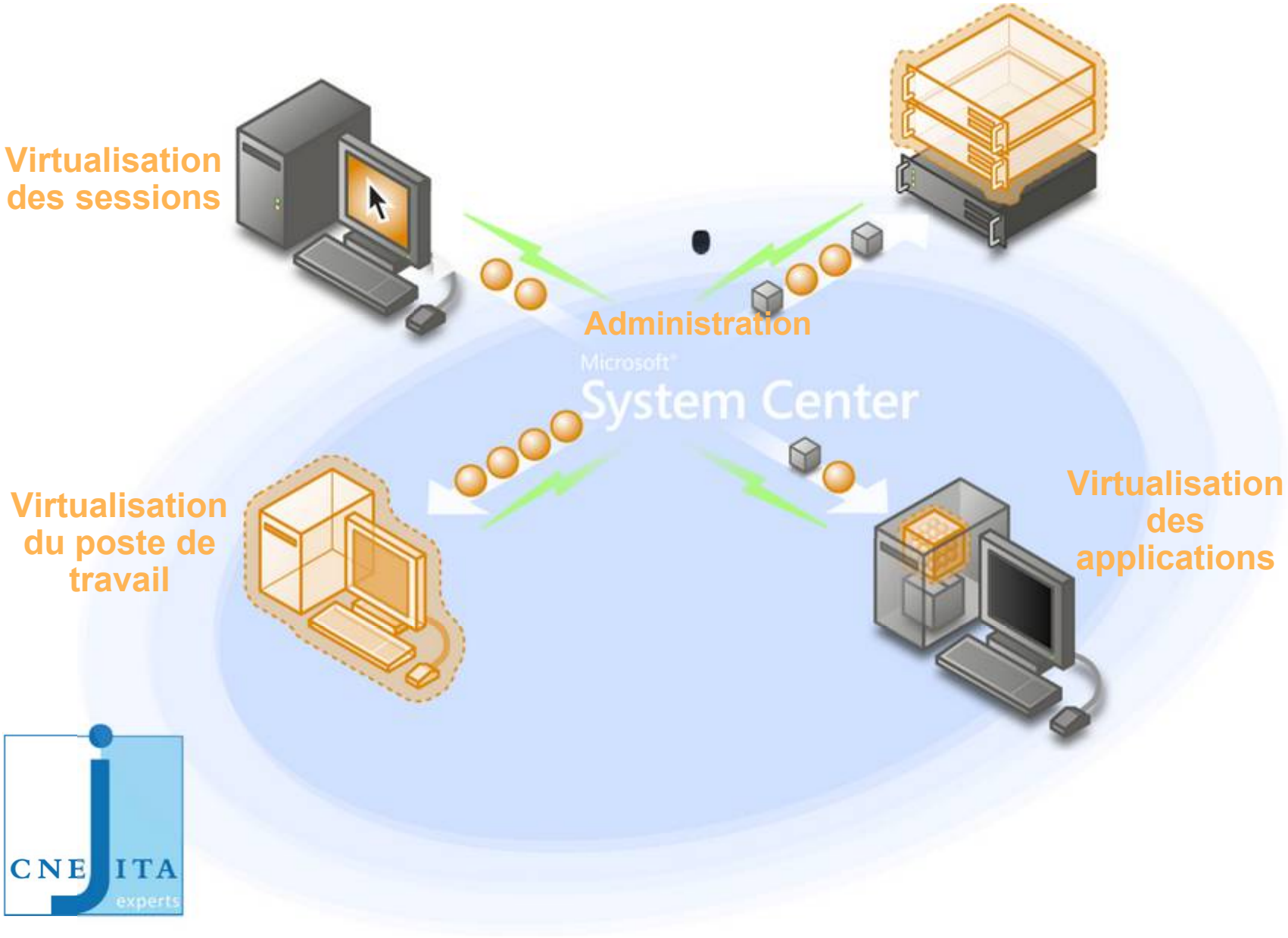
JT du 22/01/13
Virtualisation

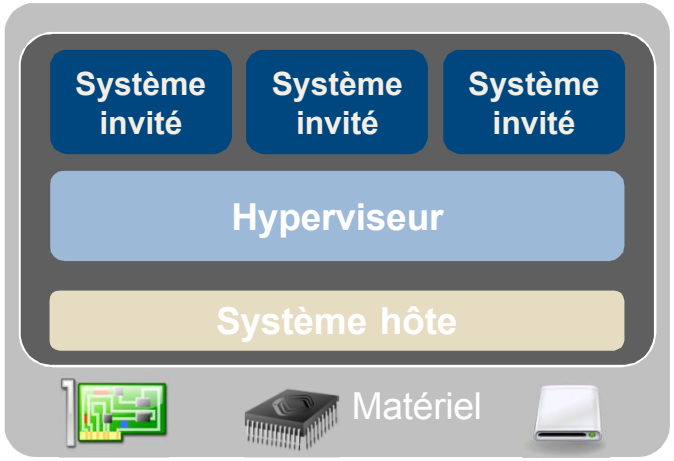
Eric LAURENT-RICARD

Virtualisation



Virtualisation

Logiciels de virtualisation du poste de travail :
VMWare Workstation ; Parallels Desktop ; Microsoft Virtual PC
Virtual Box (Oracle)…



Hyperviseurs remplaçant l'OS:
VMWare ESX
Xen
Microsoft Hyper V

Détection de machines virtuelles

- Logiciel de virtualisation installé (registre…)
- Présence de fichiers de VM (*.vmx ; *.pvm…)
- Fichiers de taille importante (disques virtuels ?)
- Utilitaires de type ‘TCHUNT’
- Accès distants

Copie de machines virtuelles

- Copie du dossier complet de la VM
- Ouverture et analyse « live » / copie des fichiers
- Attention aux systèmes protégés (pwd ; crypto)

Montage de machines virtuelles

- Liveview
- OSFmount et autres logiciels forensic

Questions - Débat

Merci de votre attention