


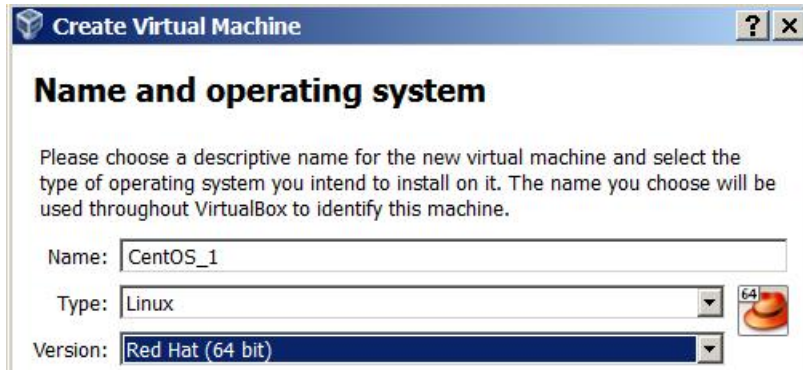
Laboratoire Vbox-Jour 1 (45 min)

§0	Introduction	sudo ./c 2
Objectifs	Comprendre les bases de la virtualisation avec l'excellent outil Virtual Box https://www.virtualbox.org/ qui est simple, gratuit et disponible pour les systèmes d'exploitation Windows, Linux et Mac. Ce travail pratique comprend les étapes suivantes : §1 LiveCD §2 Appliances §3 Réseau virtuel	
Prérequis	Avoir effectué le labo Linux du cours Sécurité des SI http://www.tdeig.ch/ITI2_Secu/33_Lab_Linux.pdf	
Cadre	Les machines virtuelles utilisées sont basées sur la distribution CentOS 6.4 CLI	
Manuel	Le texte mis en bleu est un extrait du manuel présent dans le dossier partagé	
Session	Ouvrir une session Windows 7 administrateur : compte=albert password=admin	
Action	Copier sur le bureau le dossier partagé \\10.2.1.1\doclabo\Virtu\Vbox1 contenant les fichiers utiles Lancer VirtualBox (raccourci bureau) Principales commandes dont les 3 boutons : New VM – Settings VM – Start VM	
		Action
§1	Utiliser CentOS-6.4-x86_64-minimal.iso	10 min

Manuel	page 44 → Emulation ... if you provide VirtualBox with the image of a CD-ROM in an ISO file, VirtualBox can present this image to a guest system as if it were a physical CD-ROM. 5.9 CD/DVD support The virtual CD/DVD drive(s) by default support only reading. The medium configuration is changeable at runtime. You can select between three options to provide the medium data : <ul style="list-style-type: none">• Host Drive defines that the guest can read from the medium in the host drive.• Image file (typically an ISO file) gives the guest read-only access to the data in the image.• Empty stands for a drive without an inserted medium.	
Choix	Utiliser l'émulation du CD afin d'éviter de devoir graver un CD	

But 1.1 Créer une nouvelle VM

Action Bouton **New**



Conserver les valeurs par défaut pour créer cette VM

But 1.2 Fichiers utiles

Action Clic-droit sur la VM – Show in Explorer
2 fichiers de configuration de 7 KB ont été créés ainsi que le fichier pour le disque virtuel CentOS.vdi

Remarque Vbox offre une interface CLI dont les commandes **vboxmanage** sont décrites au §8 du manuel

Action Ouvrir une console dans le dossier `C:\Program Files\Oracle\VirtualBox`
Exécuter `vboxmanage showvminfo "Centos"` pour accéder au détail de la configuration de cette VM

Lancer Notepad++ pour constater que ces 2 fichiers sont au format XML

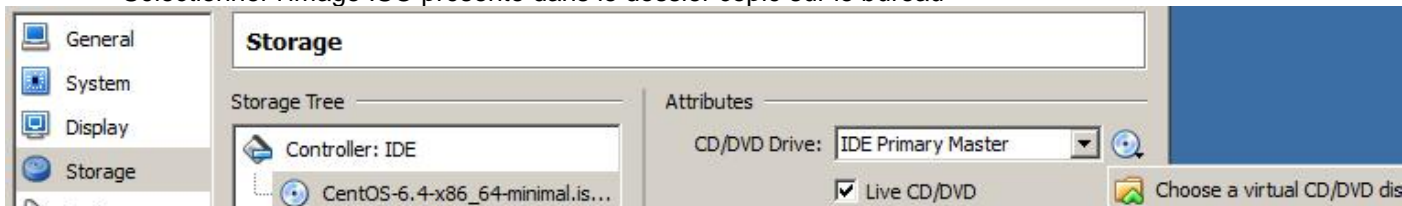
But 1.3 Configurer le virtual BIOS pour démarrer sur le CD virtuel

Action Sélectionner cette VM
Settings – System – Motherboard



OK (ne pas oublier)

Settings – Storage
Sélectionner l'image ISO présente dans le dossier copié sur le bureau



OK (ne pas oublier)

Action Démarrer cette VM
Ignorer le message d'erreur

But 1.4 Parcourir avec la souris les icônes du bas de la fenêtre



a) A quoi sert Ctrl Droite ?

Fermer la fenêtre pour stopper (Power Off) le chargement (et gagner du temps)

Manuel**page 31**

OVF is a **cross-platform standard** supported by many virtualization products which allows for creating ready-made virtual machines that can then be imported into a virtualizer such as VirtualBox.

VirtualBox makes OVF **import** and **export** easy to access and supports it from the Manager window as well as its command-line interface.

This allows for packaging so-called virtual **appliances: disk images together with configuration settings that can be distributed easily.**

This way one can offer complete ready-to-use software packages (operating systems with applications) that need no configuration or installation except for importing into VirtualBox.

But 2.1 Importer une appliance

Action File – Import Appliance – CentOS (situé dans le partage)

Remarque Ce fichier compressé de 282 MB contient un système CentOS 6.4
Il a été obtenu en terminant l'installation précédente du §1 puis File – Export

But 2.2 Retrouver les informations utiles

Action Sélectionner cette VM – Settings puis parcourir ces champs



- a) Quelles sont les valeurs username – password ?
- b) Quelle est la taille de l'espace RAM émulé ?
- c) Combien de vCPU sont émulés ?
- d) Combien de vCPU peuvent être émulés au maximum ?
- e) Quel est le type de contrôleur disque ?
- f) Où se trouve le fichier du disque virtuel ?
- g) Quelle est sa taille ?

Remarque File – Virtual Media Manager donne accès à tous les disques virtuels

Manuel

5.2 Disk image files (VDI, VMDK, VHD, HDD)

Disk image files reside on the host system and are seen by the guest systems as hard disks of a certain geometry.

When a guest OS reads from or writes to a hard disk, VirtualBox redirects the request to the image file.

Like a physical disk, a virtual disk has a size (capacity), which must be specified when the image file is created.

As opposed to a physical disk however, VirtualBox allows you to expand an image file after creation, even if it has data already; see §8.22

VirtualBox supports four variants of disk image files:

- Normally, VirtualBox uses its own container format for guest hard disks – **Virtual Disk Image (VDI)** files.

In particular, this format will be used when you create a new VM with a new disk.

- VirtualBox also fully supports the popular and open **VMDK** container format that is used by **VMware**

- VirtualBox also fully supports the VHD format used by Microsoft.

- Image files of Parallels version 2 (HDD format) are also supported

If you create a **fixed-size image**, an image file will be created on your host system which has roughly the same size as the virtual disk's capacity.

So, for a 10G disk, you will have a 10G file.

Note that the creation of a fixed-size image can take a long time depending on the size of the image and the write performance of your hard disk.

For more flexible storage management, use a dynamically allocated image.

This will initially be very small and not occupy any space for unused virtual disk sectors, but will grow every time a disk sector is written to for the first time, until the drive reaches the maximum capacity chosen when the drive was created.

While this format takes less space initially, the fact that VirtualBox needs to expand the image file consumes additional computing resources, so until the disk file size has stabilized, write operations may be slower than with fixed size disks.

However, after a time the rate of growth will slow and the average penalty for write operations will be negligible.

But 2.3

Déterminer le type de périphérique émulé

Action

Démarrer cette VM

lspci pour les voir tous

h)

Quel est le type du contrôleur SATA émulé ?

lspci | grep SATA

Manuel

5.1 Hard disk controllers: IDE, SATA (AHCI), SCSI, SAS

In a real PC, hard disks and CD/DVD drives are connected to a device called hard disk controller which drives hard disk operation and data transfers.

VirtualBox can emulate the four most common types of hard disk controllers typically found in today's PCs: IDE, SATA (AHCI), SCSI and SAS.

Lien

http://www.linuxtopia.org/online_books/linux_kernel/kernel_configuration/ch09.html

Manuel**6.2 Introduction to networking modes**

Each of the **eight networking adapters** can be separately configured to operate in one of the following modes :

- **Not attached**

In this mode, VirtualBox reports to the guest that a network card is present, but that there is no connection – as if no Ethernet cable was plugged into the card. This way it is possible to “pull” the virtual Ethernet cable and disrupt the connection, which can be useful to inform a guest operating system that no network connection is available and enforce a reconfiguration.

- **Network Address Translation (NAT)**

If all you want is to browse the Web, download files and view e-mail inside the guest, then this default mode should be sufficient for you, and you can safely skip the rest of this section.

- **Bridged networking**

This is for more advanced networking needs such as network simulations and running servers in a guest. When enabled, VirtualBox connects to one of your installed network cards and exchanges network packets directly, circumventing your host operating system’s network stack.

But 3.1**Mode par défaut de cette VM**

a) Quel est le mode par défaut du réseau ?

Manuel**6.3 Network Address Translation (NAT)**

The virtual machine receives its network address and configuration on the private network from a DHCP server integrated into VirtualBox.

The IP address thus assigned to the virtual machine is usually on a completely different network than the host.

As more than one card of a virtual machine can be set up to use NAT, the first card is connected to the private network 10.0.2.0, the second card to the network 10.0.3.0 and so on.

b) Qu’apprenez-vous grâce à la commande `ifconfig` ?

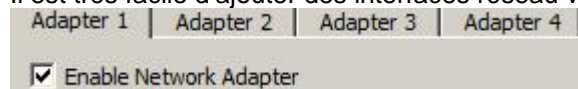
c) Dans quel mode (statique ou dynamique) d’adressage IP le système CentOS est-il configuré ?

d) Quel est le type de contrôleur Ethernet présent sur la carte mère du PC ?

e) Quel est le type de contrôleur Ethernet émulé par Vbox et présenté au système CentOS ?

Remarque

Il est très facile d’ajouter des interfaces réseau virtuelles



But 3.2 Configurer le mode Bridge

Manuel

6.4 Bridged networking

With bridged networking, VirtualBox uses a device driver on your host system that filters data from your physical network adapter. This driver is therefore called a “net filter” driver.

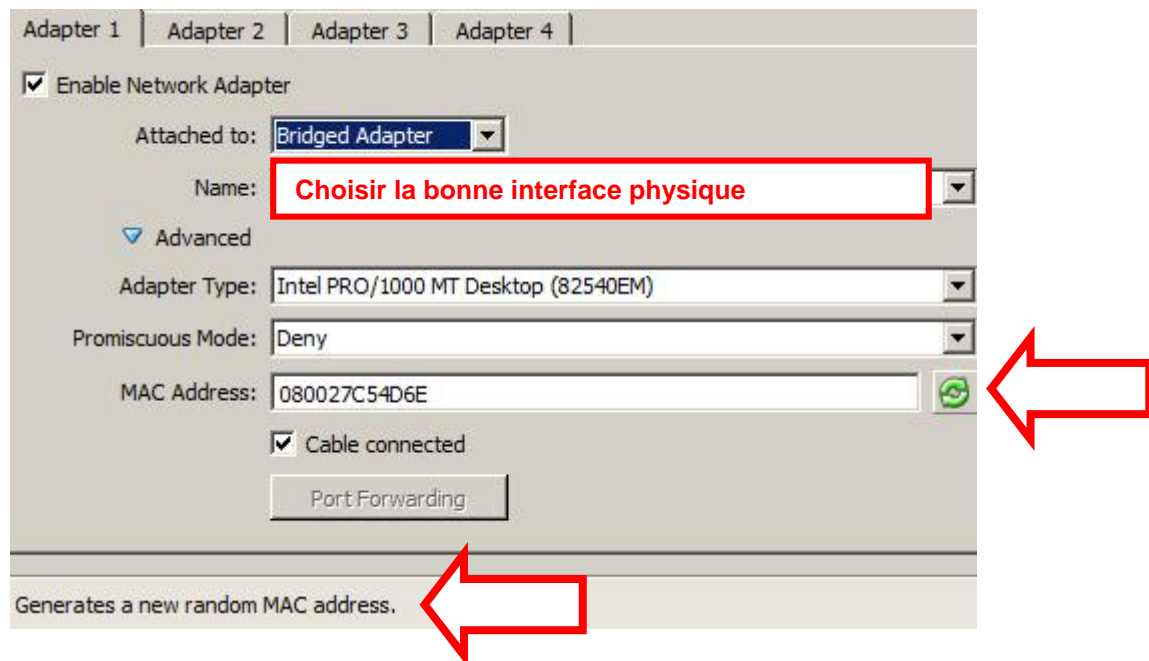
This allows VirtualBox to intercept data from the physical network and inject data into it, effectively creating a new network interface in software.

When a guest is using such a new software interface, it looks to the host system as though the guest were physically connected to the interface using a network cable: the host can send data to the guest through that interface and receive data from it.

This means that you can set up routing or bridging between the guest and the rest of your network. For this to work, VirtualBox needs a device driver on your host system.

Remarque Le système CentOS, configuré par défaut en mode DHCP, va utiliser le serveur DHCP du labo utilisant l'intervalle 10.2.3.X

Action Arrêter la VM utilisée au §3.1 avec Power Off
Configurer l'interface comme indiqué dans la figure



Remarque Lors d'opération de clonage, il est souvent nécessaire de modifier l'adresse Ethernet

f) Quelle est la nouvelle adresse Ethernet ? Noter la valeur =

Action Démarrer cette VM

g) Quelle est l'adresse IP obtenue ? Noter la valeur =

Remarque Lors du changement d'adresse Ethernet, udev désactive l'interface qu'il croit absent
<http://alexcline.net/2011/11/15/reconfiguring-network-interfaces-in-centosrhel-systems-cloned-with-vcenter/>

Action `rm -f /etc/udev/rules.d/70-persistent-net.rules`
`nano /etc/sysconfig/network-scripts/ifcfg-eth0`
`HWADDR=08:00:27:c5:4d:6e`
`cat /etc/sysconfig/network-scripts/ifcfg-eth0`
`reboot`

dans cet exemple
pour contrôler

h) Quelle est l'adresse IP obtenue ? Noter la valeur =

i) Avez-vous la connexion réseau (ping) entre les 2 systèmes (Win7 et CentOS) ?

But 3.3 Comprendre le mécanisme de capture et l'architecture utilisée par tcpdump

Quels sont les modules noyau chargés lors du démarrage

```
lsmod | more
```

La liste est longue

j) Déterminer les éléments liés à Ethernet à partir des logs produit lors du démarrage

```
dmesg | grep eth
```

k) Observer le changement de mode du pilote suite à la commande tcpdump

```
tcpdump -i eth0
```

<Ctrl+C> pour stopper l'acquisition

```
dmesg | grep eth0
```

Utiliser 2 terminaux pour effectuer un ping et tcpdump

```
tcpdump -i eth0
```

Terminal 1

```
<CTRL+Alt+F2>
```

Ouvrir Terminal 2

```
ping
```

```
<CTRL+Alt+F1>
```

Pour basculer dans Terminal 1

l) Statistiques avec netstat

```
netstat -i
```

m) Déterminer la signification des compteurs [MTU](#), [RX-OK](#), [RX-ERR](#), [RX-DRP](#), [RX-OVR](#), ...

But 3.4 Comprendre la gestion des adresses Ethernet

Action Utiliser Wireshark (Win7)
Répéter i) Ping depuis Win7

n) Quelles sont les valeurs des adresses Ethernet ?

Remarque Wireshark ne voit pas les paquets de cette VM qui communiquerait vers l'extérieur

Synthèse Quels sont les principaux paramètres d'une machine virtuelle ?

Où sont-ils mémorisés ?

Que contient un fichier ova ?

Labo terminé

Toutes les unités centrales seront éteintes avec un script
Tous les écrans seront éteints depuis le tableau électrique

Laboratoire Vbox-Jour2 (45 min)

§4	Introduction	<code>sudo ./c 2</code>
----	--------------	-------------------------

Session Ouvrir une **session Windows 7** administrateur : compte=**albert** password=**admin**

Action Copier sur le bureau le dossier partagé <\\10.2.1.1\doclabo\Virtu\Vbox2>
Lancer **VirtualBox**

§5	Configuration Client – Serveur avec Internal Network	20 min
----	--	--------

Objectifs Vous disposez de l’appliance **CentOS_C.ova** (Client) pour réaliser cette configuration :



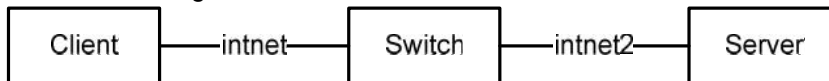
Cette VM est basée sur Linux CentOS 6.4 et préconfigurées : adresse IP, ...

Tester avec ping

a) Quelle est la marche à suivre ?

§6	Commutateur Ethernet basé sur noyau Linux	20 min
----	---	--------

Objectifs Réaliser la configuration suivante



Le commutateur Ethernet est basé sur noyau Linux Microcore 4.0 → <http://tinycorelinux.net/>

Action Configurer le switch virtuel à partir de la slide 41

a) Quelle est la marche à suivre ?

b) Le test du ping est-il positif depuis la VM Client ?

Action Utilisez tcpdump dans la VM Server pour comprendre le dysfonctionnement
`tcpdump -i eth0 arp`

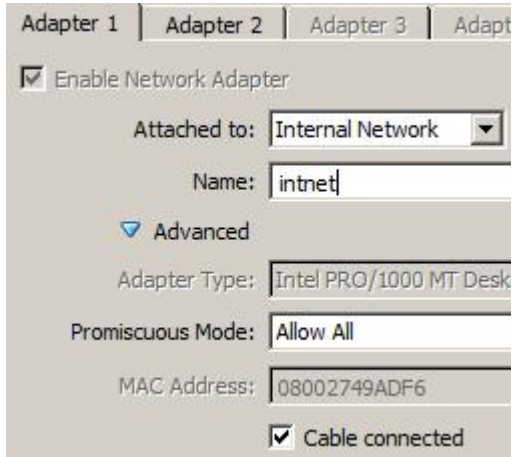
c) Le paquet ARP request émis par le Client est-il reçu par le Serveur ?

d) Le Serveur envoie-t-il un paquet ARP response ?

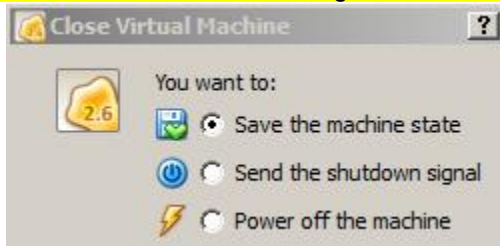
Action Utilisez tcpdump dans la VM Switch pour comprendre le dysfonctionnement
`tcpdump -i eth1 arp`

e) Quel est le trafic ARP sur le port eth1 du commutateur ?

Action Placer les interfaces de la VM Switch en mode Promiscuous



Action Pour rendre effectif ce changement, sauvegarder l'état de la machine puis la restaurer avec Start



Remarque Les 2 autres choix redémarrent la VM et perdent la configuration effectuée auparavant.

f) Le test du ping est-il positif depuis la VM Client ?

Action `brctl showmacs b1` pour connaître la liste des adresses Eth et les durée de vie

Remarque Les commandes brctl sont dans l'Annexe

Synthèse Quel est l'intérêt de Internal Network ?

Expliquer le mode Promiscuous activé au labo §6

Labo terminé

Toutes les unités centrales seront éteintes avec un script
Tous les écrans seront éteints depuis le tableau électrique

Annexe 1

brctl - ethernet bridge administration

<http://linux.die.net/man/8/brctl>

From <http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge>

brctl	addbr	<bridge>	add bridge
	delbr	<bridge>	delete bridge
	addif	<bridge> <device>	add interface to bridge
	delif	<bridge> <device>	delete interface from bridge
	setageing	<bridge> <time>	set ageing time
	setbridgeprio	<bridge> <prio>	set bridge priority
	setfd	<bridge> <time>	set bridge forward delay
	sethello	<bridge> <time>	set hello time (spanning tree protocol)
	setmaxage	<bridge> <time>	set max message age (stp)
	setpathcost	<bridge> <port> <cost>	set path cost (stp)
	setportprio	<bridge> <port> <prio>	set port priority (stp)
	show		show a list of bridges
	showmacs	<bridge>	show a list of mac addrs
	showstp	<bridge>	show bridge stp info
	stp	<bridge> {on off}	turn stp on/off

Annexe 2

Niveau CentOS

df -T → **Système de fichier Ext4**

```
Filesystem      Type      1K-blocks      Used Available Use% Mounted on
/dev/mapper/vg_centos-lv_root
                ext4      13973860      773308  12490716    6% /
tmpfs           tmpfs      510268         0      510268    0% /dev/shm
/dev/sda1       ext4      495844        31954   438290    7% /boot
```

fdisk -l | more → **1 disque de 17 GByte et des secteurs de 512 bytes**

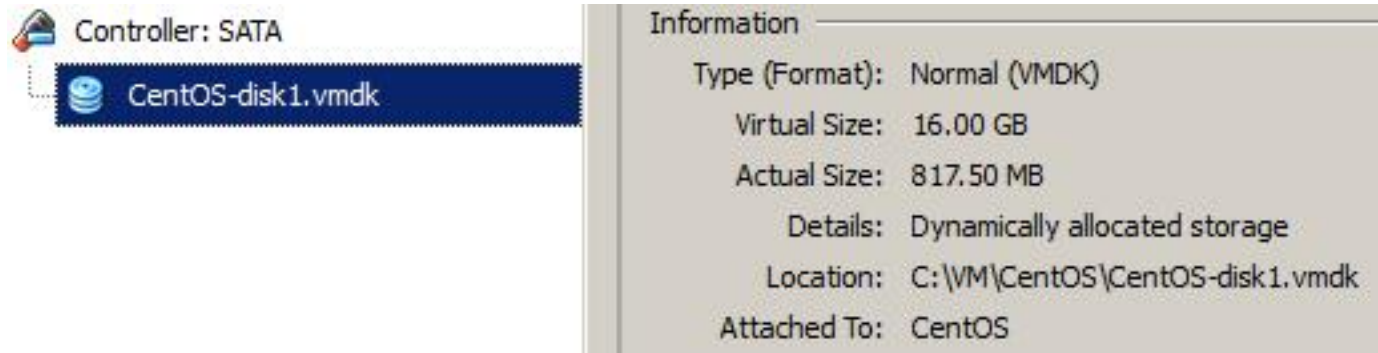
```
Disk /dev/sda: 17.2 GB, 17179869184 bytes
255 heads, 63 sectors/track, 2088 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

lspci | grep SATA → **contrôleur Intel 82801**

```
SATA controller: Intel 82801HM/HEM (ICH8M/ICH(M-E) SATA Controller [AHCI mode])
```

Niveau VBox → **Virtual Disk de 16 GB + Controller SATA**

Fichier C:\...\CentOS-disk1.vmdk de 818 MB



Controller: SATA

CentOS-disk1.vmdk

Information

- Type (Format): Normal (VMDK)
- Virtual Size: 16.00 GB
- Actual Size: 817.50 MB
- Details: Dynamically allocated storage
- Location: C:\VM\CentOS\CentOS-disk1.vmdk
- Attached To: CentOS

Niveau Win7

Disk Management → **Système de fichiers NTFS avec taille de 298 GB**

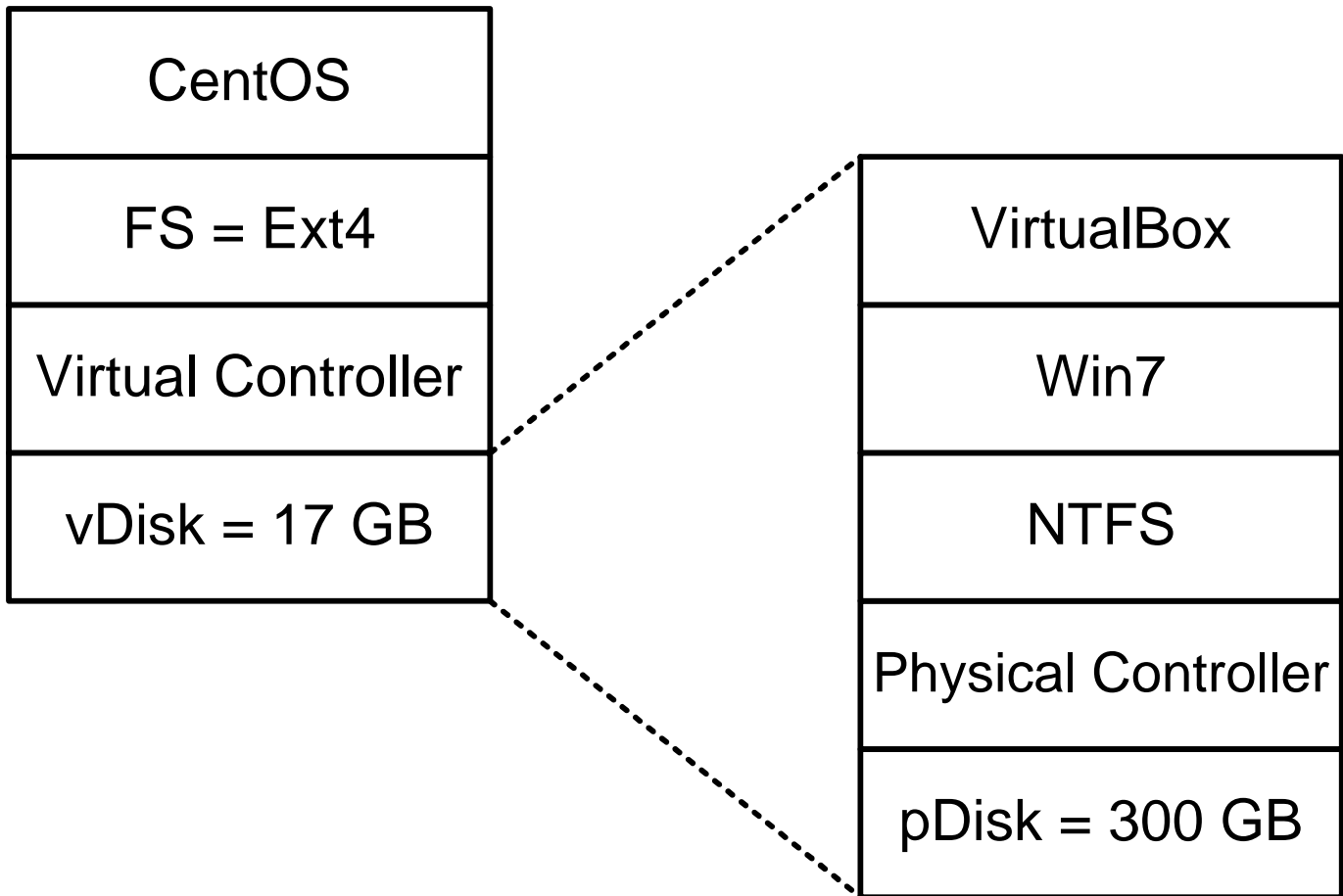
Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
Windows (C:)	Simple	Basic	NTFS	Healthy (System, Boot, Page File, Active, Crash Dump, Primary Partition)	298.09 GB	282.49 GB	95 %

C:\> **fsutil fsinfo ntfsinfo c:** → **secteurs physiques de 512 bytes (échange NTFS de 4096 byte)**

```
Bytes Per Sector : 512
Bytes Per Cluster : 4096
```

Device Manager → **contrôleur Intel 82801**

Intel(R) 82801GB/GR/GH (ICH7 Family) Serial ATA Storage Controller - 27C0



Analyse du code par Khaled Basbous – 1 oct 2013

J'ai fouillé le code de Virtualbox → <https://www.virtualbox.org/wiki/Downloads>

Ma conclusion c'est que la fragmentation se fait au niveau de CentOS par la couche file system. Ensuite le fichier du disque virtuel est à nouveau fragmenté par Win7.

```
-->VDI.cpp <--
```

Dans le code source du format VDI nous avons vraiment la description d'un disque physique avec les cylindres, têtes de lectures et secteurs avec la taille du secteur.

```
pGeometry->cCylinders = pLCHSGeometry->cCylinders;
pGeometry->cHeads = pLCHSGeometry->cHeads;
pGeometry->cSectors = pLCHSGeometry->cSectors;
pGeometry->cbSector = VDI_GEOMETRY_SECTOR_SIZE;
```

```
-->VDICore.cpp <--
```

```
#define VDI_GEOMETRY_SECTOR_SIZE (512)
```

Le contrôleur SATA du guest OS discute avec le AHCI controller device disk (virtual device ou nous pouvons brancher des vDisk SATA).

```
-->DevAHCI.cpp <--
```

```
nous pouvons brancher jusqu'à 30 disques ou lecteurs CD-Rom
/** Maximum number of ports available.
#define AHCI_MAX_NR_PORTS_IMPL 30
```

```
This component implements an AHCI serial ATA controller. The device is split
* into two parts. The first part implements the register interface for thesu
* guest and the second one does the data transfer.
* Implements the AHCI standard 1.1
```

Le contrôleur AHCI est fait à partir des spécifications 1.1 faite par Intel. Tout y est jusqu'à la led du disque qui clignote !

Il y a du cache lors d'une écriture disque sur le guest et sur le host. Par défaut sur le guest le caching est désactivé pour éviter la perte de données si la VM plante.

Laboratoire Vbox-Jour3 (45 min)

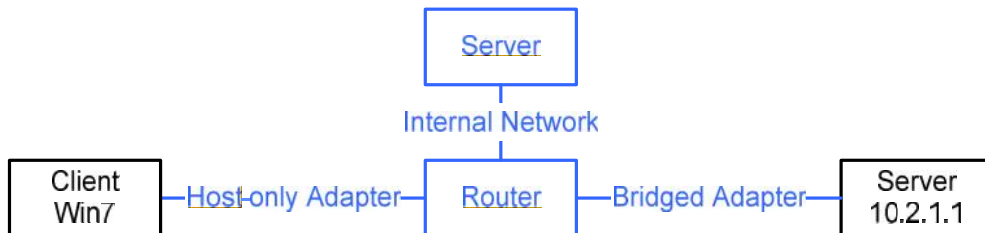
§7	Introduction	<code>sudo ./c 2</code>
----	--------------	-------------------------

Session Ouvrir une **session Windows 7** administrateur : compte=**albert** password=**admin**

Action Copier sur le bureau le dossier partagé <\\10.2.1.1\doclabo\Virtu\Vbox3>
Lancer **VirtualBox**

§8	Configuration avec routeur	40 min
----	----------------------------	--------

Objectifs Vous disposez de l'appliance CentOS_S (Server) pour réaliser cette configuration :

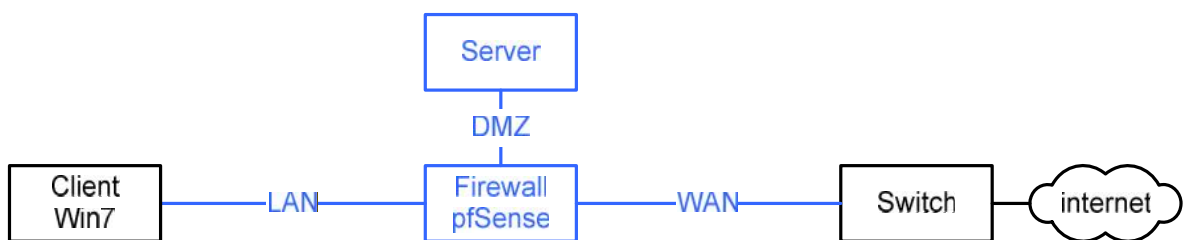


a) Quelle est la marche à suivre pour un test (ping) depuis Win7 sur le serveur virtuel ?

b) Pourquoi le test (ping) depuis Win7 sur le serveur 10.2.1.1 sera négatif ?

§9	Firewall pfSense virtuel	En réserve
----	--------------------------	------------

Objectifs Réaliser la configuration suivante
Tester les configurations du firewall pfSense dans cette **architecture virtualisée**



Labo terminé	Toutes les unités centrales seront éteintes avec un script Tous les écrans seront éteints depuis le tableau électrique
---------------------	---