

Introduction à la virtualisation

M1 RÉSEAUX & TÉLÉCOMS – RT0702
OLIVIER FLAUZAC



Généralités

Virtualisation

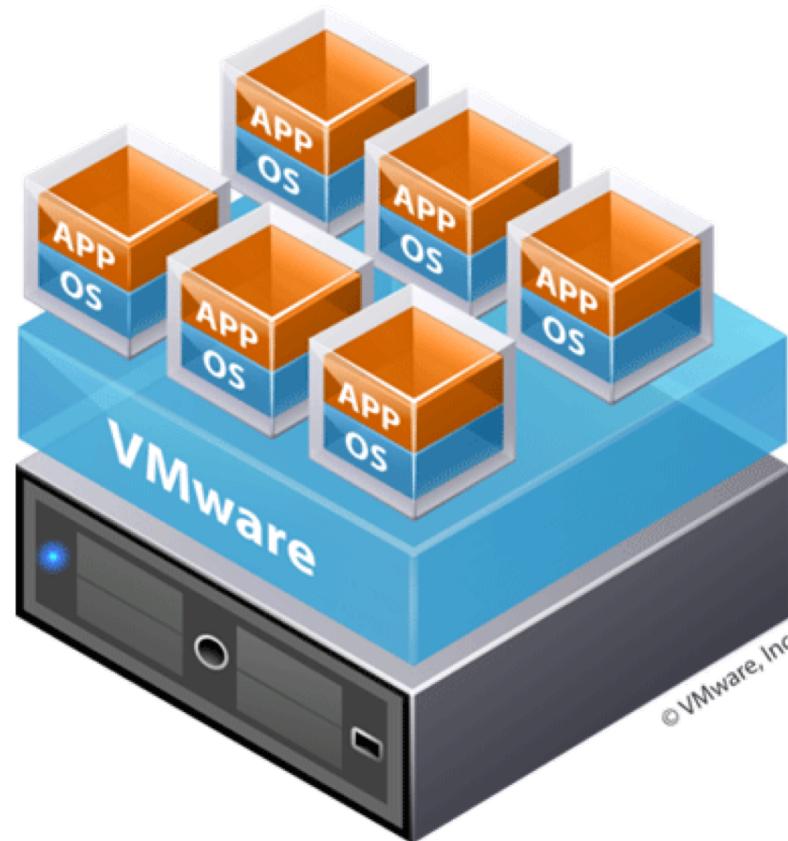
Définition

- Ensemble de techniques visant à faire fonctionner plusieurs systèmes d'exploitation sur le même matériel

Partage

- des ressources
 - bande passante
- du matériel
 - carte réseau

Vue générale



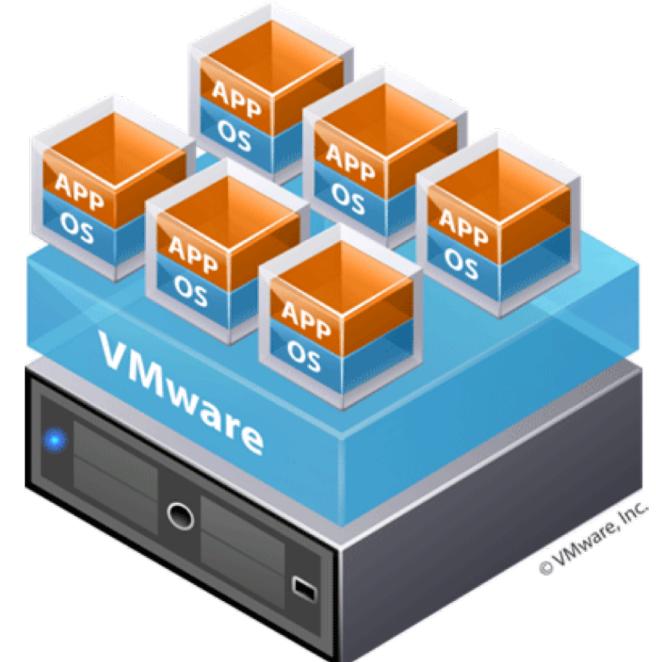
Terminologie

Hôte

- *host*
- Système d'exploitation installé sur le matériel
- « propriétaire » du matériel

Invité

- *guest*
- Système d'exploitation virtualisé



Pourquoi virtualiser ?

Rentabilisation

- Serveur peu chargés
 - serveur de mail
 - serveur de comptabilité
 - ...
- Développement des applications à installation unique
 - 1 application = 1 système / serveur

Virtualiser = exploitation des capacités des serveurs

Pourquoi virtualiser ?

Rationalisation

- Réduction du besoin d'espace
- Réduction des besoins en
 - Énergie
 - climatisation
- Développement des applications à installation unique
 - 1 application = 1 système / serveur

Virtualiser = économiser de la place

Virtualiser = économiser de l'énergie

Pourquoi virtualiser ?

Sécurisation

- Isolation des serveurs
- Isolation des applications
 - Création d'espaces confinés
 - création d'architectures réseau

Virtualiser = sécuriser les services

Virtualiser = sécuriser les applications

Pourquoi virtualiser ?

Dynamicité

- Modulation des ressources
 - modification de la mémoire
 - modification de la puissance de calcul

Virtualiser = optimiser la gestion des besoins

Virtualiser = gérer la montée en charge

Pourquoi virtualiser ?

Déploiement

- Exportation des éléments
 - Système
 - système + application
- Migration des applications

Virtualiser = gérer les installations

Virtualiser = gérer le déploiement

Pourquoi virtualiser ?

Tester

- Test de systèmes d'exploitations
 - Test d'applications
 - Bénéfice pédagogique

Virtualiser = simplifier la veille et le test

Où / Que virtualiser

Où virtualiser ?

Serveur / Data Center

- Installation de systèmes d'exploitations
- Mise en place de services spécifiques
 - service / applications en production
- Définition d'architectures systèmes
 - intégration de services de sécurité
 - intégration de services de gestion des données

Où virtualiser ?

Poste de travail

- Solution locale de virtualisation
- Test
- Utilisation pédagogique
- Création d'environnement de développement similaire à celui de la production
 - intégration de la sécurité
 - intégration des services accessibles

Virtualiser un système complet

Serveur

- Gestion laissé à « l'utilisateur »
 - Installation de logiciels / services
 - Maintenance système

Poste client

- Bureau à distance
 - Problème de bande passante
- Logiciels préinstallés
- Simplicité de gestion
 - Mise à jour
 - Sécurité

Virtualiser un Service spécifique

Solution toute configurée

- Système + service préinstallé
- Serveur Web
- Messagerie
- Téléphonie

Banque de machines

- Téléchargeable à la demande

Ajustement des moyens dans le temps

- Mémoire
- Processeur

Virtualiser le Réseau / un équipement réseau

Réseau interne

- connexion entre machine virtuelles
- connexions via un intégrateur virtuel de connexions

Eléments du réseau

- virtualisation d'un routeur
- virtualisation d'un switch

Gestion étendue des connexions entre machines virtuelles

Mise en place de connexions logique avec des machines physiques

Virtualiser la Sécurité ou l'infrastructure

Systèmes spécialisés avec un service de sécurité

Services de sécurité

- Firewall
- Concentrateur VPN
- Supervision
- Gestionnaire de logs
- ...

Virtualiser le Stockage

Mise à disposition d'espace virtuel

Augmentation de l'espace physique avec le temps

Adaptation à la demande réelle

Exemples

- DropBox, Google Drive, one Drive ...

Espace virtuel disponible > espace physique réel

Virtualiseur

Hyperviseur ?

Plate-forme de virtualisation

Permet à plusieurs OS (*invités*) de travailler sur une même machine physique (*hôte*)

Peut assurer la gestion / partage des ressources

- carte réseau
- carte vidéo
- processeur
- ordonnancement

Hyperviseur de type 1

Bare metal

Positionnement entre le matériel et système

Gestion de l'accès aux composants physiques

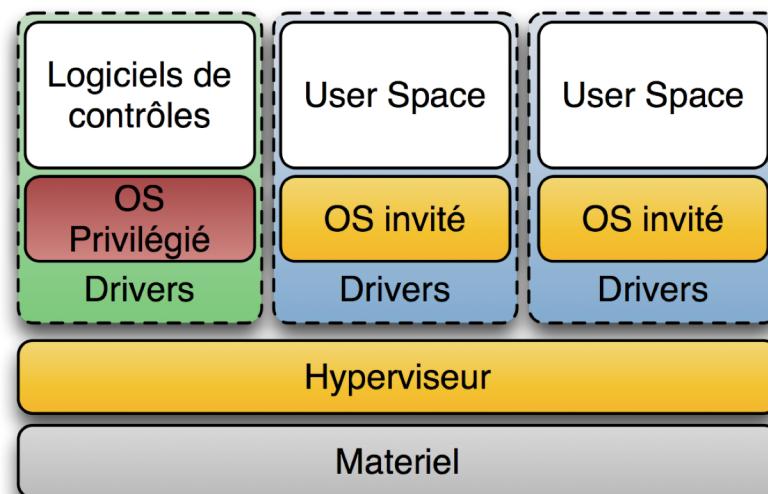
Noyau spécifique optimisé

Administration

- interface de gestion des machines

Gestion sur le matériel

- gain de puissance



Hyperviseurs de type 1

VmWare vSphere

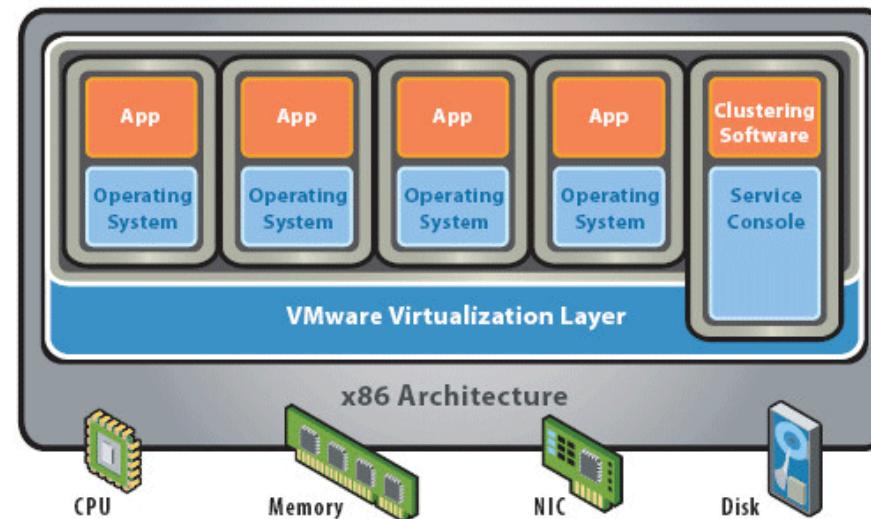
Microsoft Hyper-V

XEN

- Oracle VM server
- Citrix Xen Server

KVM

- le noyau linux = hyperviseur



Hyperviseur de type 2

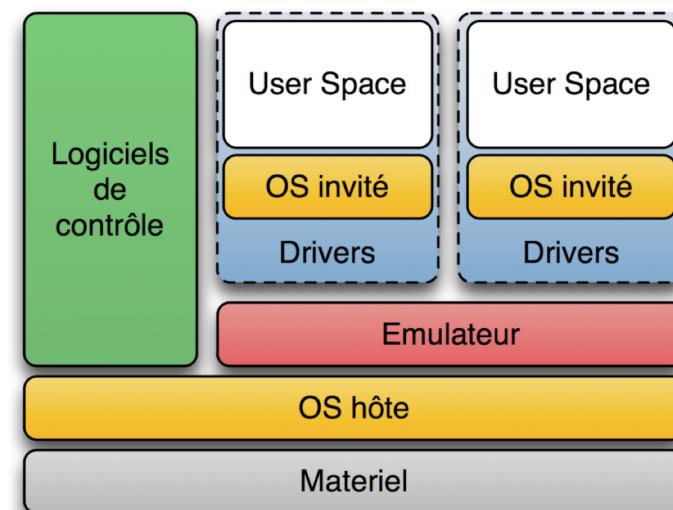
Un système dans un système

Architecture hébergée

Application sur un système d'exploitation

- Émulation possible des composants
 - carte vidéo
 - Processeur
 - carte réseau ...

Couche d'abstraction



Hyperviseur de type 2

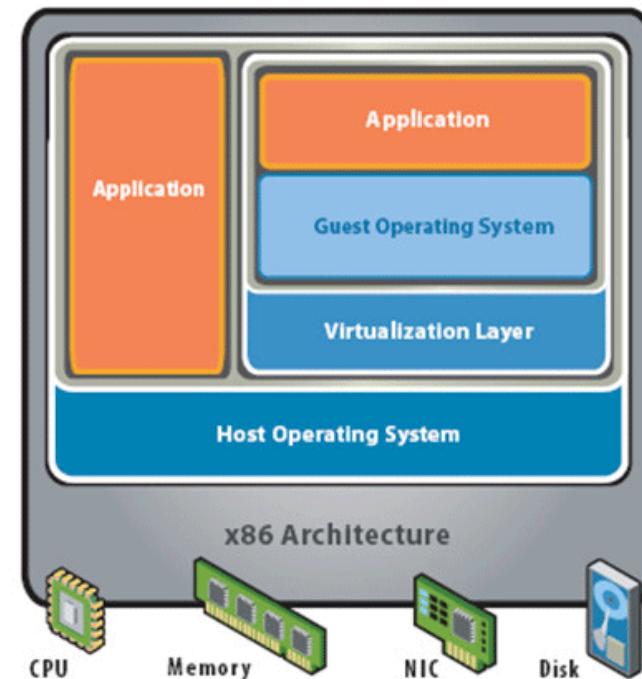
VmWare

- Workstation
- Fusion
- Player

Oracle VirtualBox

Microsoft Virtual PC

QEMU



Isolation

Isolation de l'exécution des application

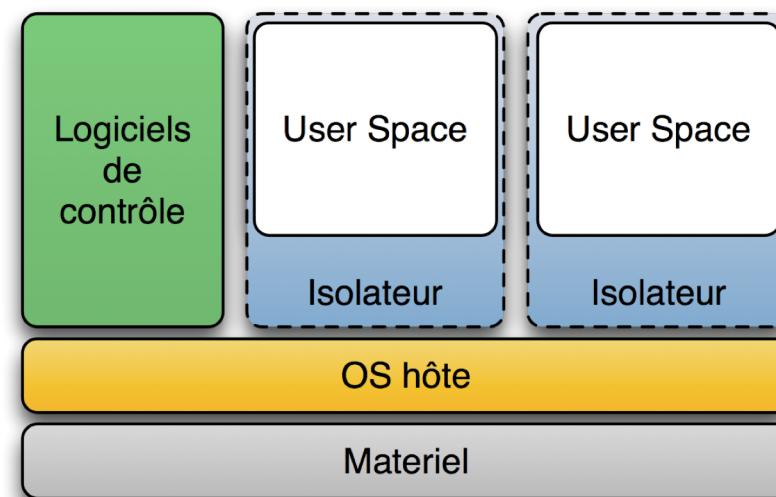
- Gestion de contextes
- Différentes applications des contextes

Isolation partielle

- Partage de noyau
- Séparation des *filesystems*

Exploitation cohérente :

- linux dans linux



Le cas du réseau

Réseau & invités

Quelle utilisation du réseau ?

Quelle configuration ?

- adresse IP
- adresse MAC
- relation avec la machine hôte
- ...

Types de configuration

- Sans réseau
- « Capture » de carte
- *Forward* de port
- Réseau interne
 - NAT
 - Réseau privé
 - bridge

Sans réseau

Machine virtuelle isolée

Accessibilité par l'hyperviseur / l'isolateur

Possibilité de partage de répertoire avec l'hôte

- Dépendant de l'hyperviseur / isolateur

Pas de montage de *filesystem* distant

Comment accéder à l'invité ?

- Pas de connexion réseau possible !
- Pas de SSH, VNC, RDP ...

« Capture » de carte

Attribution d'une interface de l'hôte à l'invité

Perte totale de l'interface dans le système de l'hôte !

Principalement sur LXC

Montage multicartes :

- Réseau filaire : carte de l'hôte
- WIFI : carte de l'invité

Comment accéder à l'invité ?

- Connexions réseaux possible depuis une seconde carte depuis l'hôte vers l'invité !
- Si une seule carte réseau sur l'hôte, pas d'accès réseau possible !

Forward de port

Relai des réceptions sur un port de l'hôte vers un port de la machine virtuelle

Mise en place d'un accès réseau depuis l'extérieur

Configuration lors du lancement de la machine virtuelle

Utilisé pour mettre en place d'une machine virtuelle dédiée à un service

- Serveur WEB

Solution exploitable en local

- draw.io

Problème de multi-instances de services !

- 3 serveurs WEB en virtuel mais un seul port 80

A croiser avec un autre mode réseau pour les connexions en sortie

Réseau interne

Création d'une architecture réseau au sein de l'hôte

Similaire à un réseau filaire classique

- Mise en place de concentrateurs virtuels
- Mise en place de câbles virtuels

Concentrateurs de connexion virtuel

- Système d'exploitation : bridge système
- Switch virtuel : open Vswitch

Câbles virtuels

- Liaisons réseau

Réseau interne

Connexions entre les interfaces des invités et les ports du concentrateur

1. Création sur l'hôte du concentrateur
2. Création des « câbles virtuels » (*tap*)
3. Branchement des câbles virtuels dans les ports du concentrateur
4. Lancement des invités : connexion des câbles virtuels sur les interfaces

Possibilité de créer plusieurs réseaux

Quelle configuration du/des réseau(x) interne(s) et de(s) l'interface(s) de l'hôte ?

Est-il possible de relier l'interface physique de l'hôte à un ou plusieurs réseaux ?

Le réseau privé

Création d'un réseau interne à l'hyperviseur

Isolation entre les invités et l'extérieur

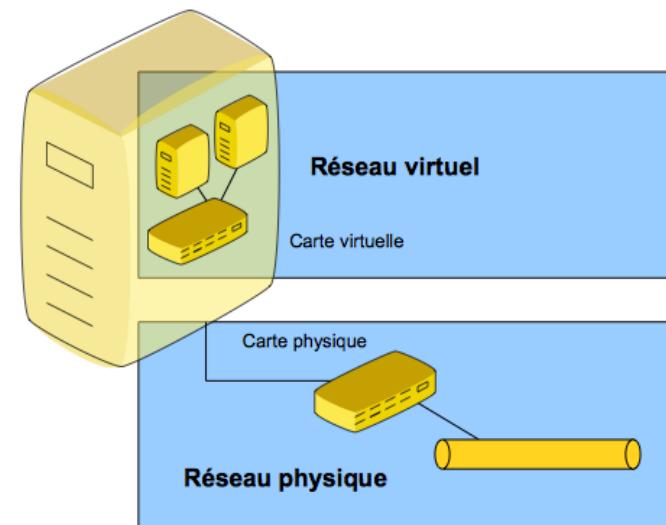
- Pas d'accès ni en entrée ni en sortie

Communication configurable

- entre invités
- entre l'hôte et l'invité

Gestion de l'adressage des invités

Possibilité de *forward* de port



Le réseau privé

Adressage

- Création d'un plan d'adressage par réseau interne
- Exploitation possible d'un invité DHCP
- Possibilité d'avoir plusieurs réseaux, plusieurs plans d'adressage

Le NAT

Mise en place d'un / plusieurs réseau(x) interne(s) dans l'hôte

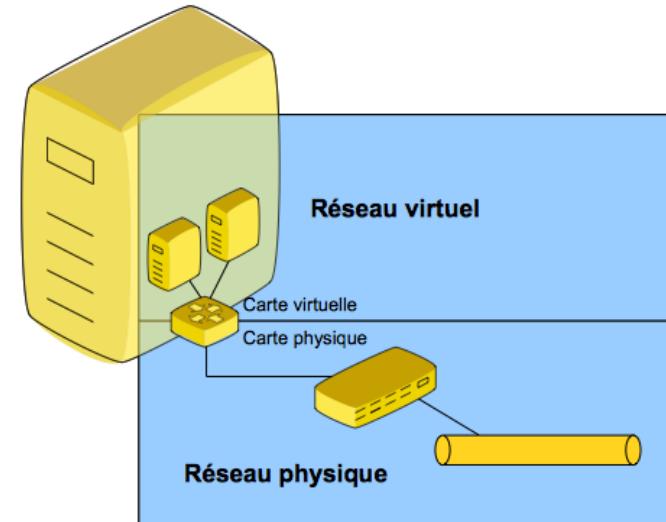
Accès des invités au réseau de l'hôte

Pas d'accès de l'extérieur

Gestion de l'adressage des invités

Possibilité de *forward* de port

Possibilité de mettre plusieurs réseaux internes



Le réseau ponté

Mode *bridge*

Partage des éléments de communication de la carte réseau

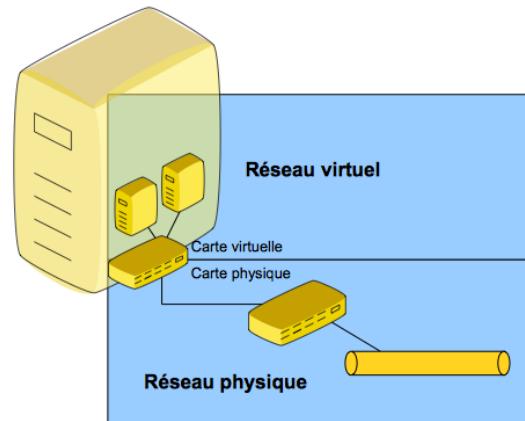
Invité sur le même réseau que l'hôte

Adresse de l'invité : même politique que l'hôte

Accès au réseau comme la machine hôte

Visible par les autres machines du réseau

Gestion des adresses MAC !



Problème de terminologie

Mécanisme permettant de connecter des invité = bridge

Terminologie

- Private bridge : réseau privé
- Bridge NAT : mode NAT
- Full Bridge : réseau ponté

Chaque fondeur à sa définition !

Problématique d'accès

Quel accès entre l'hôte et l'invité ?

- En mode NAT pas toujours d'accès entre l'hôte et l'invité
- En mode réseau privé toujours accès entre l'hôte et l'invité
- Pas toujours de mode bridge configurable (cas d'un portail captif !)

Mise en place de connexions multiples

- Une carte réseau en NAT : accès à l'extérieur
- Une carte réseau en réseau privé : accès hôte / invité en ssh

Connexion aux machines

Problématique

Comment se connecter à un invité

- Depuis l'hôte
- Depuis un autre invité
- Depuis une autre machine du réseau (physique ou virtuelle)

Problème lié au mode réseau

Problème lié à la configuration

- Pas d'adresse IP assignée
- Cas de l'installation

Où se connecter ?

L'hôte

Connexion console à l'hôte

Exécution de commande depuis l'hôte dans l'invité

- Sans connexion à l'invité
- Connexion sans réseau
- *exec* interne

Extension : ouverture d'un terminal dans l'invité

Utilisation avec des conteneurs

- Openvz
- LXC

Où se connecter ?

L'hyperviseur

Connexion distante

Gestion d'un serveur de connexion par l'hyperviseur

- L'hyperviseur assure la liaison avec ma console (terminal) de l'invité

Connexion à la « console » dans laquelle s'exécute la machine

- Comme un accès à une machine physique : clavier / écran

Connexion à une machine non configuré !

Connexion à une machine non installée !

Un port de connexion par machine virtuelle en exécution

Où se connecter ?

L'invité

Nécessité d'installer / configurer un serveur dans la machine virtuelle

Dépendant de la configuration réseau

- Accès total à la machine : *bridge*
- *Forward* de port

Nécessité de configuration de l'invité

Installation et gestion du serveur sur l'invité

Solutions de connexion

Connexion en ligne de commande

- ssh
- telnet

Exportation graphique

- RDP
- VNC
- Spice
- Guacamole
- Google share desktop
- ssh -X

Un premier exemple :
VirtualBox

VirtualBox

Solution de virtualisation pour poste de travail

Développé par Oracle

Gratuit

Hyperviseur de type 2

- Émulation du matériel
- Mais fonctionnalité d'accès direct

Permet la gestion étendue du réseau

Extension pack

Eléments additionnels

Spécifique au système

S'installe sur le système sur lequel est installé virtualBox

Permet

- L'utilisation de l'USB : liaison USB hôte avec l'USB de l'invité
- RDP : connexion console invité
- Cryptage de disque d'invité

Installation d'un invité

Définition du système à installer

Définition de la mémoire

Définition du disque virtuel

Installation

Installation des *guest additions*

Guest additions

Ajout de fonctionnalités au niveau du système invité

Extension entre l'invité et l'hôte

Eléments ajoutés

- Intégration clavier/souris
- Partage de répertoire hôte / invité
- Support graphique étendu
 - Accélération graphique 2D, 3D
- Presse papier partagé hôte / invité

Propriétés

Système

- Gestion mémoire, processeur

Affichage

- Carte vidéo, accès à distance (RDP), capture

Stockage

- Gestion des disques et volumes attachés

Carte son

- Émulation de la carte son

Réseau

- Gestion des interfaces réseau: nombre, types de carte, mode d'accès

USB

- Gestion des connexions et périphériques USB

Dossier partagé

Le réseau

Différents mode réseaux

- Classiques : NAT, bridge ...
- Etendu

Exploitation d'une infratsructure virtuelle

- Switch virtuel
- DHCP

Gestion du réseau de plusieurs machines entre l'hôte et le(s) invité(s)

Gestion des images

Images : disque virtuel sauvegardé

Attention : pas de copie mais une exportation

- Copie = copie de tous les éléments d'une machine (adresse mac !!!)

Importation d'une machine

Création d'une image de base et réexploitation de cette image

Pour le TP 1 installation préalable d'une Debian 9.X (9.5) en version serveur : pas d'interface graphique

Exploitation de VirtualBox

Interface graphique

- gestion de tous les éléments depuis l'hôte

Interface WEB

- gestion de tous les éléments depuis un serveur WEB distant

gestion en ligne de commande

- mise en place de commandes / scripts

Gestion par une API de type Service

- Web services, COM sous Windows, XPCOM (Mozilla)

Commandes

VBoxManage

- createvm : création d'une machine virtuelle
- modifyvm : modification / configuration
- createhd : création d'un disque
- Storagectl, storageattach : gestion des périphériques
- startvm : démarrage d'une VM

VBoxHeadless

- démarrage sans interface graphique

Exemple

```
VBoxManage createvm --name myDeb --ostype "Debian" --register  
VBoxManage modifyvm myDeb --memory 2048  
  
VBoxManage modifyvm myDeb --nic1 bridged  
VBoxManage modifyvm myDeb --bridgeadapter1 eth0  
  
VBoxManage createhd --filename myDeb --size 50000  
VBoxManage storagectl myDeb --name SATA1 --add sata  
VBoxManage storageattach myDeb --storagectl SATA1 --port 0 --device 0  
--type hdd --medium myDeb.vdi  
  
VBoxManage storagectl myDeb --name IDE1 --add ide  
VBoxManage storageattach myDeb --storagectl IDE1 --port 0 --device 0  
--type dvddrive --medium debian-8.2.0-i386-CD-1.iso  
  
VBoxManage startvm myDeb
```