Salle informatique "Administration Systèmes & Services Réseaux"

Ivan MADJAROV
Aix Marseille Université,
IUT, Département Réseaux et Télécommunications,
Marseille, France
ivan.madjarov@univ-amu.fr

ABSTRACT

La spécialité "Réseaux et Télécommunications" forme des techniciens supérieurs capables de s'insérer dans les secteurs des réseaux informatiques, télécommunications et du web, ou de poursuivent leurs études en licence professionnelle orientée vers la sécurité et l'administration des réseaux informatiques (ASUR). Le programme pédagogique national a nettement mis l'accent sur l'administration des systèmes et des services de l'Internet en l'affectant d'une charge d'environ 700 heures réparties sur 7 modules dans les 3 premiers semestres. D'une part, parce que ce type d'enseignement est très difficile à mener dans des salles informatiques banalisées, d'autre part, parce que la mise en place d'une pédagogie par projet nous semble être un gage d'une formation de qualité, il nous semble donc important la mise en place du matériels adéquats (Serveurs, Stations de travail, Unités mobiles) à vocation purement pédagogique pour l'équipement d'une salle de travaux pratiques afin de mettre en œuvre une solution répondant aux exigences pédagogiques de nos modules d'enseignements. Ainsi, dans ce papier nous présentons la solution technique mise en place dans notre département R&T pour favoriser la pédagogie par projet et l'évaluation par compétences dans les modules administration systèmes et services réseaux.

Keywords

Administration systèmes ; Administration des services réseaux ; Développement d'applications hybrides.

1. INTRODUCTION

Le diplômé en Réseaux et Télécommunications exerce dans toutes les entreprises utilisant les Nouvelles Technologies de l'Information et de la Communication (NTIC) [1]. Le porteur d'un diplôme DUT R&T et LP ASUR est donc présent dans les métiers:

- Administration des systèmes d'exploitation,
- Informatique ubiquitaire ou spécifique aux communications,
- Administration des services Internet et de la téléphonie,
- Développement d'applications natives et hybrides pour les smartphones et les tablettes,
- Domotique,
- Objets connectés (Internet of Things).

2. LE CONTEXTE

Les locaux du département Réseaux et Télécommunications de l'IUT d'Aix-Marseille Université accueillent quatre formations:

- DUT "Réseaux et Télécommunications" (BAC+2),
- Licence Pro "Administration et Sécurité des Réseaux" - ASUR (BAC+3),
- Master ISIC option réseau (BAC+5),
- Licence Technologique (BAC+3).

Ces quatre formations ont toutes en commun l'étude des réseaux et l'administration des systèmes et des services Internet. Environ 250 étudiants sont concernés par promotion. Pour enseigner au mieux l'aspect administration et services, nous avons utilisé une solution de virtualisation dans des salles informatiques banalisées gérées par la Direction Opérationnelle du Système d'Information (DOSI) [2]. Malheureusement, cette solution nous a posé de nombreux problèmes techniques (installation réelle des systèmes, impossibilité d'être administrateur, identification de l'accès au réseau, stockage des images systèmes, temps d'exécution, etc.) qui rendent complexe, voire inefficace l'apprentissage des étudiants. Or, il est important de souligner que ces formations sont à vocation professionnelle et qu'à ce titre elles se doivent de tout mettre en œuvre pour augmenter l'insertion professionnelle des étudiants en les rendant immédiatement "opérationnels" pour nos partenaires professionnels.

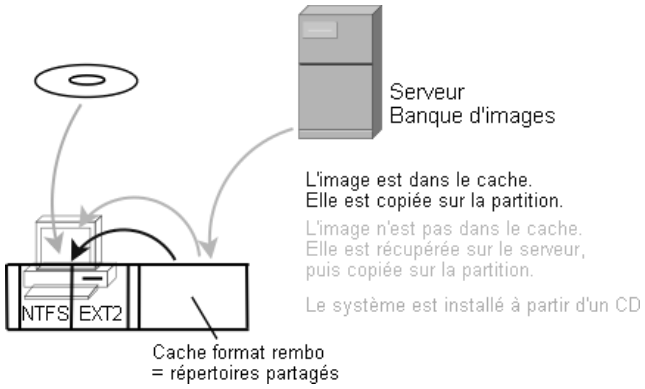

Figure 1 : Le schéma NoRabbit

La Figure 1 montre la solution technique appelée NoRabbit mise en place par les services techniques de l'université pour les travaux pratiques des modules d'administration afin de créer un environnement autorisant les droits d'administrateur sur les ressources systèmes et informatiques.

Un ordinateur soumis à NoRabbit n'a pas de système d'exploitation préinstallé. L'installation d'un système se fera par restauration d'image. Le disque dur de ces machines est partitionné de manière fixe en 4 :

- DOS
- Linux (~ 10 Go)
- Swap
- Windows (~ 10 Go)

L'espace restant est pour le cache. D'autres disques physiques peuvent être présent pour le stockage du travail en cours.

Le système d'exploitation est installé sur l'ordinateur par restauration d'une image stockée dans le cache, sur le serveur ou encore à partir d'un CD. L'intérêt principal de cette solution est qu'elle permet à l'étudiant d'être administrateur sur la machine.

En principe, une machine n'est pas dédiée à une personne mais chaque personne peut installer sur une machine un environnement informatique (système d'exploitation et logiciels), enregistrer et retrouver cet environnement par simple restauration d'image (iso). La pratique nous a démontré que l'utilisation du disque local dans le cadre d'exercice de virtualisation fige l'étudiant sur une machine donnée. La sauvegarde systématique n'affecte pas cette partition supplémentaire, alors la restauration est accompagnée d'erreurs. Impossible dans ces conditions de suivre le séquencement pédagogique des TP évolutifs.

Cette solution de salles informatiques semi-banalisées posent par ailleurs des problèmes techniques et pédagogiques diverses et variés :

- Des ordinateurs de configuration standard qui opèrent des ressources insuffisantes :
  - Une taille limitée pour la mémoire vive ;
  - Un quota limité pour le volume de stockage,
- Les droits d'accès sont définis par la pré-installation,
- Le choix du logiciel de virtualisation est prédéfini et limité,
- La sauvegarde personnalisée est souvent accompagnée d'erreurs. Alors, la restauration devient inefficace.
- Perte de temps considérable pour la restauration et la sauvegarde personnalisée au début et à la fin du TP.
- Complexification de l'apprentissage,
- Pédagogie par projet peu convaincante,
- Évaluation par compétences difficilement applicable.

Pour ces raisons, nous avons envisagé de mettre en place une salle de travaux pratiques avec le matériel informatique appropriés (Serveurs, Stations de travail, Unités mobiles, matériel réseau) pour apporter à moyen terme une solution autonome satisfaisant les modalités pédagogiques des modules d'administration et autres.

3. NOTRE PROJET

3.1 Les objectifs pédagogiques

Le métier de l'administrateur systèmes et réseaux est actuellement fortement apprécié surtout en liaison avec la sécurité des services Internet. Objectif principal du projet est l'organisation et l'équipement d'un espace d'enseignement autonome pour mieux assurer l'acquisition des compétences telles que :

- Connaître le rôle des systèmes d'exploitation et manipuler les systèmes de fichiers ;
- Apprendre à automatiser et à fiabiliser les tâches répétitives ;
- Comprendre et mettre en œuvre des systèmes virtualisés,
- Optimiser les systèmes informatiques et faciliter l'administration des utilisateurs ;
- Comprendre et savoir déployer un service de configuration automatique d'une station ;
- Savoir installer, sécuriser, exploiter et maintenir un serveur Web ;
- Apprendre à installer, configurer et maintenir un annuaire d'un système d'exploitation réseau ;
- Comprendre et savoir déployer un service DNS, Configurer et exploiter un bureau distant ;
- Configurer et exploiter une messagerie électronique ;
- Comprendre et apprendre la gestion d'erreur et la manipulation de journaux d'évènements ;
- Apprendre à sécuriser des services.

Pour atteindre ces objectifs pédagogiques on se base sur la ligne directrice de ce projet qui permettra aux étudiants d'avancer avec une pédagogie par projets la mieux adaptée à l'acquisition de ces compétences.

L'objectif pédagogique développé dans le PPN des départements R&T des IUT pointe les compétences dans le secteur des réseaux informatiques et les télécommunications. A l'intersection de ces compétences se trouve la maitrise de l'administration des services générés par les activités du cœur de métier. L'acquisition de ce savoir-faire demande des heures de travaux pratiques dans un environnement proche de la réalité de l'entreprise.

Pour se rapprocher le plus possible des conditions de l'entreprise, nous souhaitons que les étudiants puissent travailler en équipe sur un sujet précis, lui-même faisant partie d'un projet plus général mené par l'ensemble du groupe. Après une explication des bases théoriques et principes de fonctionnement en cours, une étude globale du projet en travaux dirigés, les étudiants, durant les séances de travaux pratiques, concevront et bâtiront une architecture apportant les solutions au sujet proposé. D'une séance de travaux pratiques à l'autre, le projet global sera conservé mais les différents sous-projets seront traités par des équipes différentes d'étudiants. A titre d'exemple, nous pourrions définir comme projet général la mise en place de l'architecture système d'une entreprise, et décomposer celui-ci en plusieurs tâches comme l'installation du serveur WEB, du serveur DNS, du serveur DHCP, etc.

Ainsi, il nous semble important de pouvoir étaler un projet complexe sur la totalité des modules dédiés à l'administration, tels que :

- M1103 - Architecture des équipements informatiques,
- M1105 - Bases des systèmes d'exploitation,
- M2102 - Administration système,
- M2106 - Bases des services réseaux,
- M3104 - Gestion d'annuaires unifiés,
- M3105 - Services réseaux avancés,
- M3206 - Automatisation des tâches d'administration,
- ATW01 - Administration et supervision avancées,
- Les modules similaires en LP et/ou Master Réseau,
- Les modules similaires dédiés à la Licence technologique

Ce dispositif devant fonctionner pour plusieurs formations comportant elles même plusieurs groupes devant travailler en parallèle, nous devrons disposer de machines puissantes dotées d'une forte capacité disque et mémoire.

Le besoin en ressources est explicitement défini dans les objectifs des modules concernés dont une partie importante est notamment la mise en œuvre des étapes d'exploitation des systèmes :

- Windows
- Linux

Pour placer les étudiants en situation proche d'une entreprise, il est judicieux de mettre en place des travaux pratiques évolutifs. Ainsi, notre projet vise une salle autonome regroupant les ressources

informatiques pour mettre en œuvre les étapes de l'administration des systèmes informatiques et les services réseaux. Notamment :

- Installation
- Configuration
- Automatisation
- Sécurisation

3.2 Les paramètres techniques

Les paramètres techniques et la configuration des machines ont été choisis pour favoriser la virtualisation et le stockage de données dans le cadre des TP évolutifs. Le TP est fait sur machine virtuelle, l'étudiant sauvegarde son travail sur disque dur ou sur disque amovible. L'accès réseaux est configuré au travers des cartes virtuelles et filtré par un routeur autorisant l'accès Internet (Figure 2).

Ainsi, la salle est équipée de 17 machines serveurs d'entrée de gamme configurées comme suit :

- Base : PowerEdge T130
- Processeur : Processeur Intel E3-1240v5 à 3.5 GHz 4 cœurs 8 Mo cache 80W Turbo
- Mémoire : 2133MT/s 32Gb UDIMMs, en 4 x 8Go 2133 Mhz UDIMM - Faible Voltage
- Configuration du châssis : jusqu'à 4 disques durs câblés 3.5 pouces et Embedded SATA
- Disque dur principal : 2To Nearline SAS 6 Gbps 7200 Tpm format 3.5" - câblé (carte SAS additionnelle)
- Disque dur additionnel : 2To Nearline SAS 6 Gbps 7200 Tpm format 3.5" - câblé (carte SAS additionnelle)
- Carte réseau : On-Board LOM 1 GBE Dual Port (BCM5720 GbE LOM)
- Carte réseau supplémentaire : Broadcom 5720 Dual ports gigabit

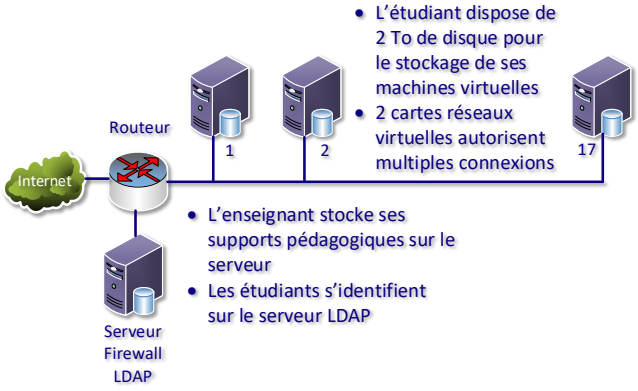

Figure 2 : L'architecture réseau de la salle

L'amorçage initial du système d'exploitation se fait avec OS Linux (Debian). L'enseignant-responsable de la salle est le seul ayant les droits d'administrateur. L'étudiant est identifié par le système d'annuaire mis en place (LDAP). Le TP est fait sur machine virtuelle à l'aide de logiciel de virtualisation, l'étudiant sauvegarde son travail sur le second disque (2To) ou sur disque amovible (1To).

3.3 Les prérequis des travaux pratiques

En informatique, une machine virtuelle (MV) est une illusion d'un appareil informatique créée par un logiciel d'émulation par exemple Hyper-V, Virtual Box, VMware, KVM, etc.

Le logiciel d'émulation simule la présence de ressources matérielles et logicielles telles que la mémoire, le processeur, le disque dur, le système d'exploitation, les pilotes, le switch et la connexion réseau, permettant d'exécuter des programmes dans les mêmes conditions que celles de la machine simulée (physique).

KVM (*Kernel-based Virtual Machine*) est un hyperviseur libre de type I pour Linux. Il est désormais intégré dans le noyau Linux depuis la version 2.6.20. KVM permet de faire fonctionner des machines virtuelles aux OS variés, Windows, Linux, BSD. KVM est une instance de QEMU.

QEMU est un émulateur de diverses architectures. Combiné au pilote KVM, il permet de réaliser de l'accélération Hardware (HVM). L'outil de base `qemu-img` permet de créer et de gérer des images disque. En format local les images disques peuvent se trouver en formats `raw`, `qcow2`. Par ailleurs, on peut utiliser directement des volumes logiques LVM.

Lors de la création d'un fichier de disque dur virtuel pour KVM avec `qemu-img`, l'option `-f` permet de spécifier le format à utiliser parmi `raw`, `qcow(2)`, `vmdk`, etc. Si aucun format n'est précisé, l'image est créée en `raw`. Ce format ne permet cependant pas de bénéficier de certaines fonctionnalités qui font la souplesse de KVM. L'outil intègre une fonction de conversion permettant de transformer un disque virtuel d'un format vers un autre.

Les étapes à suivre dans le TP :

- Création de disque virtuel avec `qemu-img`
- Installation du système d'exploitation avec `kvm`
- Choix du mode de communication Hôte-MV-Réseau.
- Lancement de la machine virtuelle avec `kvm`

Le mode de connexion réseau pour la machine virtuelle (MV) est configuré en fonction des modalités du TP.

3.3.1 Le mode bridge [3]

Le mode établi conçoit un "bridge" de la carte réseau virtuelle à une carte réseau physique de l'hôte. Dans le schéma de la Figure 3 les adresses IP sont fournies par le serveur DHCP. L'hôte et la MV peuvent communiquer. La MV communique comme une machine réelle de la même façon que l'Hôte communique avec les autres machines du réseau.

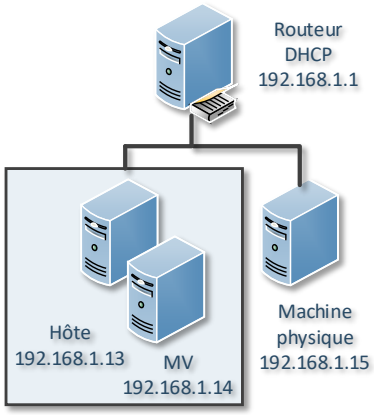

Figure 3 : Mode bridge

La carte réseau virtuelle étant associée à une carte réseau physique de l'Hôte on aura donc deux adresses IP,

- L'adresse IP dédiée à l'Hôte (`192.168.1.13`),
- L'adresse IP dédiée à la MV (`192.168.1.14`).

Le DHCP du réseau fournit une adresse IP à la MV de la même façon que pour l'Hôte. A l'absence de DHCP, la carte réseau de l'Hôte et/ou de la MV peuvent être en IP fixe. Ainsi, les machines sont sur le même réseau avec chacune leur adresse IP. Dans le cas d'une communication entre l'Hôte et la MV au niveau IP, la stack IP du système d'exploitation enverra les paquets à la bonne destination : l'Hôte ou la MV, de la même façon que pour l'accès entre deux cartes réseau sur la même machine.

3.3.2 Le mode NAT [3]

Le mode NAT (*Network Address Translation*) est par défaut sur les logiciels de virtualisation VirtualBox et VMWare. En mode NAT la MV utilise la translation d'adresse. La machine Hôte effectue une translation d'adresse avant d'envoyer les paquets de la MV vers le réseau. La machine Hôte met son adresse IP en source du paquet et tient à jour une table de translation. Une réponse reçue, la machine Hôte met à jour le paquet à destination de la MV avant de le transmettre à la MV.

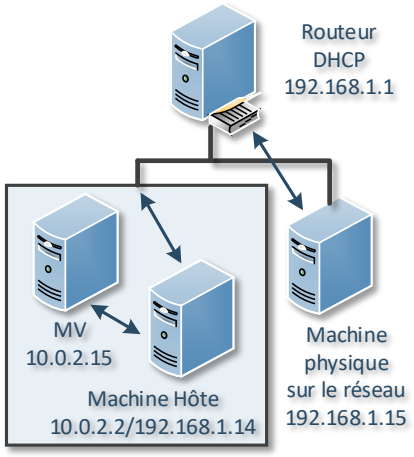

Figure 4 : Le mode NAT

- L'adresse IP dans la MV est obtenue de l'Hôte par DHCP du logiciel de virtualisation (`10.0.2.15`),
- L'adresse IP de la passerelle par défaut dans la MV est obtenue par l'Hôte (`10.0.2.2`),
- La MV communique avec le réseau via l'Hôte.

Une autre machine que l'Hôte ne pourra pas accéder à la MV. La carte réseau virtuelle de l'Hôte ne comporte pas de passerelle vers les autres ordinateurs du réseau, uniquement une passerelle entre lui et ses MV. Si plusieurs machines doivent communiquer avec la MV, il faut utiliser le mode pont.

Pour s'assurer du bon fonctionnement, un ping sur `10.0.2.2` doit aboutir, un ping sur `192.168.1.14` aussi. Ces deux adresses correspondent aux deux cartes réseau de l'Hôte, l'une réelle et l'autre virtuelle créée par le logiciel de virtualisation. Un ping de la MV vers l'adresse `192.168.1.1` répond en assurance du bon fonctionnement de la passerelle de l'Hôte. Un ping de la MV vers une autre machine du réseau (`192.168.1.15`) fonctionne toujours grâce à la passerelle et son NAT.

3.3.3 Création de disque virtuel

Pour le bon fonctionnement d'une MV un espace disque dédié est nécessaire. A l'aide de l'outil `qemu-img` on crée le fichier image disque qui va être utilisé comme disque dur virtuel :

```
qemu-img create -f qcow2 vm/iv.qcow2 40G
```

- `iv.qcow2` est le nom du fichier image disque.
- `qcow2` est l'extension du fichier image disque qui n'est pas indispensable mais indique le type de fichier image. Le format `qcow2` est un format d'espace de stockage optimisé, c'est à dire que l'espace sera occupé par le fichier image disque dynamiquement.
- `vm` est le nom du répertoire qui abrite le fichier de l'image du disque virtuel Il faut songer à sa création.
- `40G` sera la taille virtuelle de l'espace disponible dans le disque virtuel.

3.3.3.1 Installer un système d'exploitation depuis un CD-ROM

```
kvm -m 2G -cpu host vm/img.qcow2 -cdrom
/dev/cdrom -boot d
```

- `-m 2G` paramètre et attribut pour définir la quantité de `2GiB` de mémoire RAM qui sera utilisable par la MV.
- `-cpu host` indique que le microprocesseur de la machine virtuelle aura les mêmes caractéristiques que celles du microprocesseur de la machine hôte.
- `-cdrom` est le lecteur de CD ROM.
- `-boot d` indique que le périphérique d'amorce sera le lecteur de CD ROM.

3.3.3.2 Installer un système d'exploitation depuis une image-ISO

```
kvm -m 2G -cpu host vm/img.qcow2 -cdrom
NomDuFichier.iso -boot d
```

- `-m 2G` est la quantité de 2GiB de mémoire RAM utilisable par la MV.
- `-cpu host` indique que le microprocesseur de la machine virtuelle aura les mêmes caractéristiques que celles du microprocesseur de la machine hôte.
- `-cdrom` est le lecteur de cd-rom, ou un fichier image-ISO.
- `-boot d` indique que le périphérique de d'amorce sera le lecteur de cd-rom, ou le fichier image-ISO.

Exemple : Appel à la machine virtuelle avec installation de Windows 2012 Serveur.

```
kvm –m 4G –hda vm/w10srv.qcow2 –cdrom
/baru/local/src/
fr_windows_server_2012_x64_dvd_915480.iso
```

3.3.3.3 Démarrage de la MV

Une fois l'installation terminée, on peut démarrer la machine virtuelle avec la ligne de commande pour lancer le système d'exploitation virtualisé.

```
kvm -m 2G -cpu host iv/img.qcow2
```

Pour sécuriser le travail et de pouvoir reprendre en cas de besoin, il est préférable de s'assurer avec une copie de la MV avant toutes autres actions sur le sujet du TP. Faire une copie de la MV (fichier)

```
cp NomFichier NomFichier.archive
```

Lancer deux machines virtuelles avec changement d'adresses MAC pour les cartes réseaux virtuelles et attribution d'adresses IP fixes (sans DHCP).

```
kvm -m 4G -hda w10srv.qcow2 -k fr -net
nic,macaddr=42:01:02:03:04:05 -net
vde,sock=/var/run/vde2/kvmnodhcp0.ctl
```

Enlever le firewall pour tester la commande `ping`.

Mettre des adresses IP fixes `192.168.1.15` pour l'une et `192.168.1.16` pour l'autre, si on veut faire communiquer deux machines virtuelles. Dans ce cas de configuration on n'a plus accès Internet.

Certains exercices concernant l'administration de Windows 2016 Server, installé en virtuel sur KVM, demandent l'installation d'une machine virtuelle à la base de Hyper-V, c.à.d. une deuxième machine virtuelle pour la gestion de Nano-Serveur par exemple. Après un ajustement paramétrique du KVM le test effectué a été concluant.

4. CONCLUSION

Le présent projet a été financé entièrement par l'IUT d'Aix-Marseille Université à la hauteur de 25000€ dans le cadre du programme FIP (Fonds d'Intervention Pédagogique) en 2017. La Figure 6 présente une vue panoramique de la salle.

Le projet s'inscrit également dans une volonté du département R&T de développer des actions de formation continue dans les domaines des réseaux informatiques, de l'administration système et des technologies web. En effet, l'équipe pédagogique de notre département possède un savoir-faire reconnu et une expérience pédagogique approuvée ces derniers 20 ans. La mise en place de cet équipement est un atout de qualité pour convaincre les entreprises en demande de formation.

La satisfaction des étudiants est exprimée par le sondage annuel mené par l'université (voir Figure 5).

La solution technique réalisée dans cette salle de TP informatique a, par ailleurs, attiré l'attention de la DOSI par les résultats pédagogiques obtenus et les retours positifs des enseignants intervenants dans les divers modules d'administration sur plusieurs formations confirment son efficacité. Ainsi, à leur initiative la solution que nous avons proposée et réalisée dans notre département sera étendue sur l'ensemble des salles semi-banalisées durant l'année 2019.

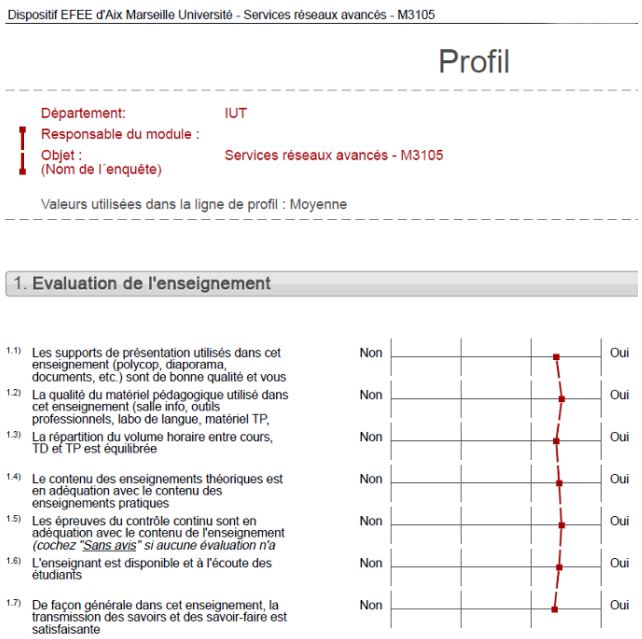

Figure 5. Résultat de l'évaluation de l'enseignement pour le module M3105

5. REFERENCES

[1] PPN RT 2013, Ministère de l'enseignement supérieur et de la recherche, 2013, http://www.enseignementsup-recherche.gouv.fr.

[2] DOSI, Direction Opérationnelle des Systèmes d'Information, https://dosi.univ-amu.fr/.

[3] La Gestion réseau dans une machine virtuelle, https://chrtophe.developpez.com/tutoriels/gestion-reseau-machine-virtuelle/.

[4] KVM, https://www.linux-kvm.org/page/Documents.

Figure 6 : La salle de 17 postes