

# Installation scriptée de PCs pédagogiques sous Fedora 28

## Frédéric Amrein

Service informatique Polytech Clermont  
2 avenue Blaise Pascal  
63170 AUBIERE

## Pierre-Philippe Chapon

Service informatique Polytech Clermont  
2 avenue Blaise Pascal  
63170 AUBIERE

## Résumé

*Notre système d'installation automatisée des postes pédagogiques de Polytech Clermont-Ferrand se base sur une approche très industrialisée du déploiement. Notre idée est de proposer un service fiable, optimisé et simplifié pour les installations et ré-installations de salles. Ainsi, nous savons répondre au mieux aux besoins pédagogiques de l'école.*

*Nos PCs sont installés sous distribution linux Fedora via un boot PXE et un script « kickstart ». Ce script permet une installation très personnalisée du système, il se décompose en trois phases :*

- définition des paramètres d'installation du système d'exploitation ;*
- définition des paquets que l'on souhaite installer et ceux que l'on souhaite supprimer ;*
- application des scripts post installation qui permettent une personnalisation avancée du système ;*

*Par la suite, les tâches régulières de maintenance comme les installations de nouveaux paquets seront exécutées en bloc via ParallelSSH.*

*Ce système répond à une très grande partie des besoins pédagogiques mais pas tous : les étudiants ont besoin de certaines applications natives Windows. Ainsi, nous distribuons également sur l'ensemble du parc une machine virtuelle Windows accessible à tous les utilisateurs connectés via un serveur Bitorrent.*

## Mots-clefs

*Gestion de parc, installation scriptée, kickstart.*

## 1 Contexte

Polytech Clermont-Ferrand est une école d'ingénieurs interne de l'Université Clermont Auvergne. Elle est membre du réseau Polytech (15 écoles en France), compte six diplômes d'ingénieurs et regroupe plus de mille élèves et apprentis-ingénieurs. Elle est habilitée par la Commission des Titres de l'Ingénieur.

D'un point de vue informatique, Polytech Clermont-Ferrand représente plus de 500 PCs, 50 serveurs virtuels, 22 salles informatiques. Parmi ces machines, 160 sont paramétrées via la méthode que nous allons présenter ici.

## 2 Les objectifs

Les objectifs sont multiples mais nous cherchons avant tout une réponse fiable et performante aux attentes formalisées de la pédagogie de l'école. Nous nous devons de proposer à nos élèves un parc de machines uniformes disposant d'une offre logicielle homogène. Ces PCs doivent être accessibles toute la journée, que ce soit pour les cours ou pendant les accès en libre-service : les salles ne sont jamais fermées. Pour cela nous devons mettre en œuvre un processus d'installation automatisée facile à déployer et indépendante des différentes générations de hardware.

## 3 Les solutions envisagées

A l'époque de la rénovation du parc de PCs pédagogiques, nous avons envisagé trois solutions pour remplacer nos anciennes salles.

### 3.1 PC Windows avec clonage

Cette solution présente l'avantage de pouvoir réutiliser les postes informatiques déjà présents dans les salles, par contre elle a l'inconvénient de ne pas être robuste au changement de hardware et nécessite de créer plusieurs images pour chaque génération de PC : c'est lourd à mettre en œuvre et très chronophage.

### 3.2 Virtualisation du poste de travail

Le VDI (Virtual Desktop Infrastructure) via la solution VMware Horizon implique des coûts élevés en termes de licences et la nécessité d'une infrastructure système et réseau lourde à notre échelle. De plus, cela entraîne pour nous une dépendance au constructeur que nous avons jugée trop importante lors de nos tests.

### 3.3 PC Linux avec installation scriptée

Avec un tel choix, on peut réutiliser les PC déjà acquis. L'installation du système d'exploitation s'adapte au hardware quand celui-ci est largement répandu. L'automatisation très avancée du déploiement nous permet d'être très réactifs lors du renouvellement de postes pédagogiques.

## 4 Solution retenue

En 2012, lorsque nous choisissons la solution de déploiement de PC sous Linux via une installation scriptée de Fedora, nous savons que pour mener à bien ce projet nous aurons énormément de travail et que nous rencontrerons de nombreuses difficultés. En effet, il nous faudra bâtir de toutes pièces un environnement logiciel (services et serveurs) nécessaire à une automatisation maximum. C'est à cette époque que nous virtualisons l'intégralité de nos serveurs sous VMware et que nous entamons la rénovation de toute notre infrastructure réseau. Ce choix sera principalement guidé par les grandes compétences techniques de nos collaborateurs de l'époque, Pierre Mondié et Jérémie Rodriguez.

## 5 Les aspects serveurs

Notre solution d'installation scriptée repose sur un ensemble de serveurs hébergés sur notre infrastructure virtualisée sous VMware. Celle-ci est composée de deux serveurs ESXi (256Gb de RAM, 50 serveurs, 2 baies de disques).

### 5.1 Boot PXE

Les installations des postes de travail sont réalisées via le réseau (Pre-boot eXecution Environment). Initialement, nous avons un serveur proposant uniquement un boot PXE en mode BIOS legacy via PXELinux, cela nous convenait parfaitement. Avec l'avènement de l'UEFI, cette solution ne nous

permettait plus de booter depuis un disque local en mode legacy. Nous avons alors dû nous tourner vers une solution de “boot loader” compatible UEFI en implémentant un Grub.

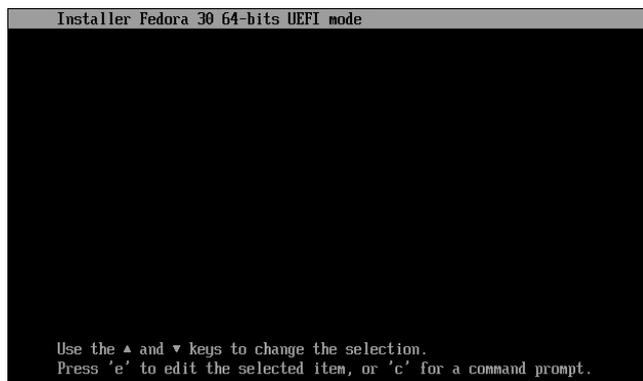


Figure 1 - Menu de boot UEFI

```
menuentry 'Installer Fedora 30 64-bits UEFI mode' --class fedora
--class gnu-linux --class gnu --class os {
echo 'Message de grub.cfg : chargement du noyau vmlinuz'
linuxefi (tftp)/FC30/vmlinuz ip=dhcp
root=live:http://172.16.5.55/FC30/install.img
inst.ks=http://172.16.5.55/fc30_64_uefi.ks
echo 'Message de grub.cfg : chargement du système de fichiers
initial'
initrdefi (tftp)/FC30/initrd.img
echo 'Message de grub.cfg : Initialisation du processus d
installation'
```

## 5.2 DHCP

Lors de sa présentation aux JRES de 2011 nous avons été séduits par Netdot (logiciel d'IP Management (<https://github.com/cvicente/Netdot>)) et l'avons depuis déployé à Polytech Clermont.

C'est le point d'entrée pour la configuration des serveurs DHCP et DNS. Outre le fait que l'on associe les adresses MAC / IP et le nom de chaque machine, Netdot fournit les options DHCP *next server* et *filename* qui sont indispensables au bon fonctionnement du boot PXE. En effet l'option *next server* indique l'adresse IP du serveur proposant un boot PXE et l'option *filename* indique le fichier de configuration pour initialiser l'installation par le réseau. Cela nous a permis de résoudre le problème suivant : pour installer un OS en UEFI il faut le booter en UEFI mais nos postes les plus anciens ne sont pas compatibles avec un boot réseau de ce type. Nous avons donc modifié notre configuration DHCP pour que l'option *filename* s'adapte en fonction de la requête de l'émetteur. Ainsi dans le cas d'un boot UEFI on indique notre fichier grub.cfg ; dans le cas d'un boot legacy on indique notre fichier pxelinux.

```
if option arch = 00:07 {
    filename "boot/grub/x86_64-efi/core.efi";
} else if option arch = 00:09 {
    filename "boot/grub/x86_64-efi/core.efi";
```

```
} else {
    filename "/gpxelinux.0";
}
```

## 5.3 TFTP

Les options *next server* et *filename* précédentes indiquent donc l'adresse IP et l'emplacement TFTP (Trivial File Transfer Protocol) du fichier qui lancera l'installation du système d'exploitation. Que ce soit pour une installation en mode UEFI ou une installation en mode BIOS, on fait appel aux mêmes sources :

- *vmlinuz* qui contient le noyau ;
- *initrd.img* qui contient les modules nécessaires au noyau ;
- *install.img* qui contient des sources d'installation en lecture seule ;
- fichier *kickstart*.

Les trois premiers fichiers sont issus de l'image iso de Fedora, le fichier *kickstart* est quant à lui paramétré par nos soins.

## 5.4 Fichier kickstart

À l'origine, c'est une solution d'automatisation d'installation de RedHat.

Le contenu de ce fichier est décomposable en trois parties que nous allons détailler dans ce chapitre :

- description de la configuration générale ;
- logiciels à installer ;
- scripts post installation.

### 5.4.1 Description de la configuration générale

Ici, on indique les réponses aux questions que l'on retrouve lors de l'installation d'un système d'exploitation : langue utilisée, mot de passe root, création d'un compte local, source des paquets...

Les instructions de partitionnement étant différentes suivant le mode d'installation, nous avons donc un fichier kickstart pour le BIOS mode et un autre pour le mode UEFI.

```
url --url="http://172.16.25.0/fc30/releases/30/Everything/x86_64/
os/"
# Root password
rootpw --iscrypted $1$Ap74dMQa$ppcZ9EfGurkKjKmBlvRhm.
# System keyboard
keyboard fr
# System langage
lang fr_FR
# Create a fallback local user.
user --name=etu --groups=etu --homedir=/home/etu --
password=$1$FYCWcvOF$virDko4pLHcjfBNLdAg3h0 -iscrypted
# System timezone
timezone Europe/Paris
```

### 5.4.2 Logiciels à installer

Dans cette seconde partie, on renseigne la liste des paquets ou groupes de paquets (précédés d'un @) que l'on souhaite installer ou désinstaller (en les précédant d'un -).

```
# Section [packages]
%packages
@libreoffice
libreoffice-langpack-fr
libreoffice-base
...
-@gnome-desktop
-evolution
-evolution-help
```

### 5.4.3 Scripts post installation

Ici, nous pouvons ajouter toutes les lignes de commande nécessaires afin de façonner comme on le souhaite notre environnement Fedora. Voici quelques exemples issus de cette longue partie :

```
# Section [post-installation]
# On définit l'adresse IP de notre serveur d'impression dans le
fichier de configuration de CUPS
echo "ServerName 172.16.5.1" >> /etc/cups/client.conf
echo "post-Murray" >> /root/progress.log

# On ajoute le montage NFS pour les profils utilisateurs dans
fstab
mkdir -p /Polytech
echo -e "datastore.epucfe.eu:/home/Polytech /Polytech nfs4
x-systemd.automount,auto,rw,_netdev,nfsvers=4.0 0 0" >>
/etc/fstab

# On ajoute la clef publique de notre serveur Dalton à la liste
des clefs autorisées
mkdir -p /root/.ssh
wget http://172.16.5.55/fedora-scripts/id_rsa_dalton.pub -O
/root/.ssh/id_rsa_dalton.pub
cat /root/.ssh/id_rsa_dalton.pub >> /root/.ssh/authorized_keys

#On copie la configuration du fichier SSSD pour pointer vers nos
serveurs Active Directory
wget http://172.16.5.55/fedora-scripts/sss2.new -O /tmp/sss2.new
cat /tmp/sss2.new > /etc/sss/sss.conf
chmod 0600 /etc/sss/sss.conf

# On installe l'application VMWare player
dnf -y install gcc make binutils perl kernel-devel-`uname -r`
wget http://172.16.5.55/vmware/VMware-Player-15.1.0-
13591040.x86_64.bundle -O /tmp/Vmware-Player.bundle
```

```

chmod +x /tmp/Vmware-Player.bundle
/tmp/Vmware-Player.bundle --console --required --eulas-agreed -
ignore-errors
rm -f /tmp/Vmware-Player.bundle

# On Copie en local un fichier d'aide à destination des
utilisateurs
wget http://172.16.5.55/fedora-scripts/AidePolytech.desktop -O
/usr/share/applications/AidePolytech.desktop
wget http://172.16.5.55/fedora-scripts/AidePolytech.pdf -O
/usr/share/doc/AidePolytech.pdf
wget http://172.16.5.55/fedora-scripts/logo-polytech.png -O /usr/
share/logos/logo-polytech.png
chmod +r /usr/share/doc/AidePolytech.pdf
chmod +x /usr/share/applications/AidePolytech.desktop
chmod +r /usr/share/logos/logo-polytech.png

#Pour le nommage des PC on se réfère à nos serveur DNS qui sont
alimentés par NetDot.
rm -f /etc/hostname
hostnamectl --transient > /etc/hostname

```

## 5.5 Les données utilisateurs

Les profils utilisateurs sont stockés sur un serveur de fichiers auquel les postes Fedora accèdent en NFS version 4 via les montages fstab. Ceci permet aux utilisateurs de retrouver leurs données depuis n'importe quel poste.

## 5.6 L'Authentification

Pour l'authentification des utilisateurs, nous nous appuyons sur nos serveurs Active Directory qui sont alimentés par les serveurs LDAP de l'université. Ceci nous assure une intégrité complète des données d'authentification : pas de comptes locaux, uniquement ceux de l'Université Clermont Auvergne des utilisateurs « autorisés ».

Nos postes Fedora interrogent nos AD via un SSSD (System Security Service Daemon). Ci-dessous notre fichier sssd.conf.

```

[domain/default]

## Manually configured
access_provider = simple
enumerate = False

ldap_default_bind_dn = cn=anonymous,cn=Users,dc=epucfe,dc=eu
ldap_default_authtok = 2B4fh45dcfyJX9C
ldap_default_authtok_type = password

ldap_group_search_base = dc=epucfe,dc=eu

```

```
ldap_user_search_base = dc=epucfe,dc=eu
ldap_group_object_class = group
ldap_user_object_class = user
ldap_user_name = samAccountName
ldap_user_uid_number = uidNumber
ldap_user_gid_number = gidNumber
ldap_user_home_directory = unixHomeDirectory
ldap_user_search_filter = (&(objectCategory=User)(uidNumber=*))
## End of manual configuration
ldap_schema = rfc2307bis
ldap_search_base = ou=utilisateurs,dc=epucfe,dc=eu
krb5_realm = EPUCFE.EU
krb5_server = venturi.epucfe.eu,watt.epucfe.eu
id_provider = ldap
auth_provider = krb5
chpass_provider = krb5
ldap_uri = ldap://venturi.epucfe.eu,ldap://watt.epucfe.eu
krb5_kpasswd = venturi.epucfe.eu,watt.epucfe.eu
cache_credentials = True
ldap_tls_cacertdir = /etc/openldap/cacerts
[sssd]
services = nss, pam
config_file_version = 2
domains = default
[nss]
[pam]
```

## 5.7 Rtorrent et machines virtuelles

Notre environnement Fedora et ses applications répondent à bon nombre des attentes de la pédagogie. Néanmoins, certaines applications requises pour des TP sont exclusives au monde Windows ou requièrent un environnement très spécifique. Dans ces cas-là nous faisons appel à des machines virtuelles que l'on exécute sur les postes pédagogiques via l'application VMWare Player. Ces machines virtuelles sont configurées en mode « non persistant », ce qui nous assure de les retrouver en état de fonctionnement après chaque utilisation. La mise en pause est désactivée et le fichier de configuration vmx est synchronisé avec un fichier de référence.

Ces VMs sont copiées en local sur chaque poste via le protocole bittorrent. Coté serveur nous avons un tracker bitstorm et côté client nous avons rtorrent. Ce dernier ne requiert aucune interface graphique et fonctionne avec des quotas afin que le transfert des VMs puisse se faire en arrière-plan.

## 5.8 Maintenance des postes pédagogiques

Dans notre kickstart, nous intégrons l'installation de Fusion Inventory qui alimente notre inventaire GLPI. Avec les informations issues de GLPI nous pouvons générer deux types de listes. Une première liste qui va regrouper les adresses MAC des postes Fedora, afin de faire du Wake On Lan. La seconde liste concerne le nom des postes fonctionnant sous Fedora 30 ce qui nous permet de faire du PSSH (Parallel SSH). Grâce à la clef publique de notre serveur PSSH qui a été ajoutée à la liste des clefs autorisées lors de l'installation, nous sommes en mesure de pousser des commandes avec privilèges en simultanément sur tous les postes concernés.

```
parallel-ssh -t 20 -l root -h hosts-sept2019.txt 'ls
/Torrents/Complete/Windows10_V4.1'
```

```
[120] 13:37:29 [SUCCESS] e006-5v17rg2
[121] 13:37:29 [SUCCESS] e006-6gsdrg2
[122] 13:37:29 [SUCCESS] e006-6gy5rg2
[123] 13:37:29 [FAILURE] b116-jlj38c2 Exited with error code 255
[124] 13:37:29 [FAILURE] b118-fn97lg2 Exited with error code 255
```

Figure 2 - Résultat d'une commande PSSH, le code 255 correspond à un PC injoignable

## 6 Déploiement d'un poste client

Voici les différentes étapes pour la mise en service d'un poste pédagogique sous Fedora.

### 6.1 Déballage et paramétrage du BIOS

En premier lieu il nous faut paramétrer le BIOS du PC pour le rendre compatible avec notre système d'installation réseau :

- On active le boot sur le réseau (mode UEFI network stack si possible)
- On active le Wake On Lan (mode lan only)
- On désactive le Deep Sleep Control
- On définit un mot de passe admin du BIOS

On en profite aussi pour noter l'adresse MAC de la machine.

### 6.2 Réserver une adresse IP dans Netdot

Depuis l'interface web de Netdot, on réserve une adresse IP sur notre réseau pédagogique en associant l'adresse MAC récupérée plus haut à l'adresse IP. On renseigne également le nom de machine sous la forme Num\_salle-ServiceTAG (b116-1x7l9x1).

24.162	24.163	24.164	24.165	24.166
24.178	24.179	24.180	24.181	24.182
24.194	24.195	24.196	24.197	24.198
24.210	24.211	24.212	24.213	24.214
24.226	24.227	24.228	24.229	24.230
24.242	24.243	24.244	24.245	24.246
25.2	25.3	25.4	25.5	25.6
25.18	25.19	25.20	25.21	25.22
25.34	25.35	25.36	25.37	25.38
25.50	25.51	25.52	25.53	25.54

Figure 3 - Interface web de Netdot

### 6.3 Boot PXE et installation système

Une fois l'installation lancée, elle va suivre le script et se terminer en environ 40 minutes sur un poste récent équipé d'un SSD. Attention au nombre d'installations simultanées, on constate des erreurs quand on lance plus de 12 postes en même temps.

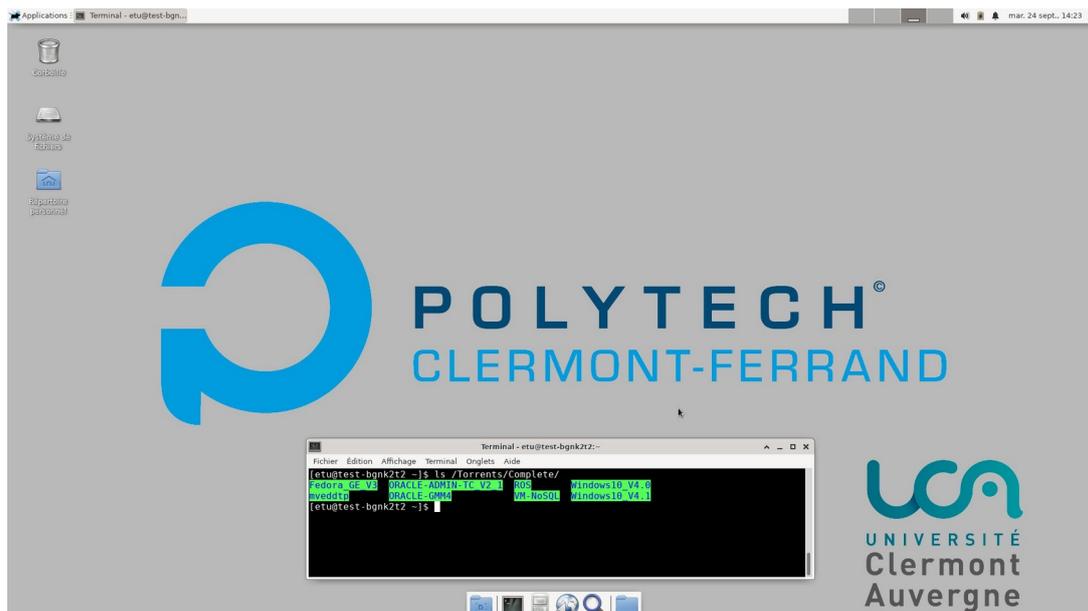


Figure 4 - Bureau par défaut sous xfce

## 6.4 Téléchargement des machines virtuelles

Une fois le système Fedora installé, le poste devient fonctionnel. Les utilisateurs peuvent se connecter et travailler sur leurs espaces personnels. Par contre la machine ne sera pleinement opérationnelle que quand elle aura fini de télécharger les machines virtuelles via RTorrent. Étant donné le volume actuel de la machine virtuelle Windows 10 (environ 100Gb), il faut compter au moins 24 heures pour que celle-ci soit disponible sur tout le parc.

## 7 Les résultats

Cette solution est en place à Polytech Clermont-Ferrand depuis plus de 7 ans, les utilisateurs sont très satisfaits de trouver un environnement de travail identique quel que soit le poste où ils se connectent.

Concernant la maintenance du parc, on peut rencontrer quelques surprises lors de la création d'un nouveau script kickstart (principalement lors de la montée de version de Fedora). Une erreur dans le script entraîne évidemment une erreur sur chaque poste déployé. Il est alors possible, via le PSSH, de passer une commande où un script massivement sur tous les postes.

Une réunion « Informatique pédagogique » est organisée chaque année en juin pour faire le bilan de l'année et prendre en compte les nouvelles demandes de logiciels. Un PC maquette est alors mis à disposition des enseignants pour qu'ils testent leurs logiciels, s'ensuit alors le déploiement de l'ensemble du parc.

## 8 Remerciements

Nous tenons tout particulièrement à remercier nos anciens collègues Pierre Mondié (décédé prématurément il y a deux ans) et Jérémie Rodriguez qui sont les initiateurs de cette solution de déploiement à Polytech Clermont Ferrand.

Nous remercions les JRES pour nous avoir permis de rédiger cet article et de présenter notre poster.