

Mutualisation de la configuration de postes de travail GNU/Linux dans un environnement multi départements

Manuel Sabban

Télécom ParisTech
46 rue Barrault
75 013 Paris

Ariel Vives

Télécom ParisTech
46 rue Barrault
75 013 Paris

Frédéric Pauget

Télécom ParisTech
46 rue Barrault
75 013 Paris

Résumé

Pour leurs missions d'enseignement et de recherche, une partie de nos enseignants-chercheurs a besoin d'une solution de travail sous GNU/Linux. Elle doit être adaptée à leurs besoins en terme de postes de travail fixes ou mobiles, de salles de travaux pratiques mutualisées ou dédiées à des domaines scientifiques donnés ("réseau" par exemple). De plus, cette solution technique étant déployée dans un contexte délicat de mutualisation et de regroupement progressif des personnels techniques au sein de la DSI, l'attractivité et la performance de la solution ont été particulièrement soignées.

Pour répondre à ce besoin, Télécom Paristech a déployé une plateforme d'installation automatique basée sur un démarrage par le réseau, l'installateur de la version stable/wheezy de Debian GNU/Linux, et un serveur bcfg2. Un système de distribution pair à pair est également utilisé pour déployer les fichiers volumineux.

Le présent article présente les besoins des utilisateurs avant d'aborder les aspects plus techniques du déploiement des postes. Il a également fallu apporter une réponse aux usagers de Windows sans pour autant proposer de machines à double démarrage ; une solution basée sur l'utilisation de machines virtuelles (VirtualBox) a été choisie.

Le système est aujourd'hui déployé dans 13 salles de TP, soit 234 postes et aussi sur 190 postes de travail de configurations matérielles différentes. Les spécificités matérielles de chaque poste ou salle sont respectées. Ce système fonctionne depuis un peu plus d'une année. Les retours des utilisateurs sont positifs, de plus en plus de salles sont migrées vers ce système.

Mots clefs

bcfg2, pair à pair, machine virtuelles, stations de travail, salle de TP, Debian GNU/Linux, VirtualBox

1 Introduction : motivation et besoins des usagers

1.1 Situation initiale

Télécom Paristech est composée de quatre départements et plusieurs services administratifs. Les quatre départements scientifiques sont les suivants :

- SES (sciences économiques et sociales) ;

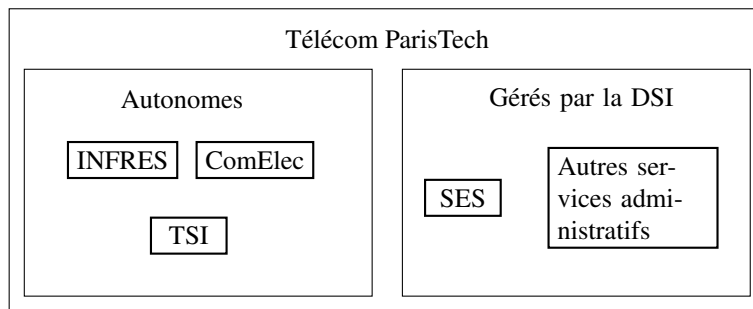


Figure 1 - Organisation initiale de l'informatique à Télécom ParisTech

- TSI (traitement du signal et de l'image) ;
- INFRES (informatique et réseau) ;
- COMELEC (communications et électronique).

Avant 2010, le personnel informatique était réparti entre trois départements scientifiques (COMELEC, TSI et INFRES) et la DSI (voir figure 1). Les systèmes de gestion existants étaient plutôt hétérogènes en terme de solutions techniques choisies et l'interopérabilité très perfectible. Les services DHCP, serveurs de fichiers et serveurs web étaient et restent à la charge des départements.

En 2010, le personnel informatique dédié de COMELEC a été intégré à la DSI, et en 2012 une partie de celui de TSI. À l'occasion de cette intégration, les pratiques et usages ont été homogénéisés et les services mutualisés. Cela a permis de limiter la répétition de nombreuses tâches, et nous cherchons à pousser cette logique jusqu'aux configurations utilisateurs, sans toutefois diminuer les fonctionnalités proposées.

1.2 Centralisation et mutualisation des services

Chaque entité doit pouvoir disposer d'une configuration adaptée à ses besoins, tout en mutualisant les services et la main d'oeuvre. En parallèle, les moyens humains se redéplient au cours du temps au sein de la DSI. C'est un argument fort pour une solution fortement mutualisée et configurable. Du point de vue de l'utilisateur, la configuration reste la même, il accède aux mêmes fichiers et aux mêmes programmes. Il peut ainsi garder ses habitudes quelque soit son lieu de travail.

1.3 Besoins

Nous avons identifiés les besoins suivants :

- intégrer des configurations préexistantes dans un système centralisé sans changer les habitudes des usagers ;
- pouvoir déployer automatiquement des logiciels et faire évoluer les configurations selon les demandes utilisateur ;
- permettre aux utilisateurs de retrouver toujours leur environnement de travail sur toutes les stations ;
- prendre en compte les spécificités matérielles de manière la plus simple possible ;
- automatiser le système.

2 Postes de travaux pratiques et stations de travail

La mise en service d'un poste client sur le parc se déroule en trois phases. Nous installons d'abord un système d'exploitation minimal, puis nous configurons le système et enfin nous le personnalisons.

2.1 Installation d'un système d'exploitation

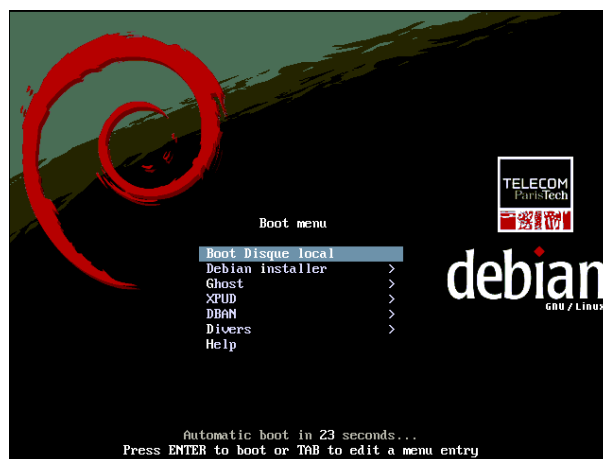


Figure 2 - Menu de démarrage

2.1.1 Démarrage

La procédure d'installation débute par un démarrage sur le réseau : une requête DHCP est d'abord émise. La réponse à cette requête renseigne le serveur TFTP et le fichier à utiliser. La machine à installer télécharge et exécute alors `syslinux`. Ceci présente à la personne chargée de mener l'installation un menu comportant toutes les entrées utiles au fonctionnement de l'établissement (figure 2) :

- démarrage sur le disque local (Par défaut après 10s) ;
- installateur Debian. Cette entrée propose un sous-menu qui liste toutes les installations de la distribution Debian GNU/Linux que nous proposons. En plus de l'installation décrite ici, il est possible d'utiliser l'installateur standard ou lancer une install automatique de serveur ;
- Ghost pour les installations Windows ;
- système de secours sous GNU/Linux (XPUD) ;
- Dban pour les effacements de disques durs ;
- d'autres outils regroupés dans un sous menu «Divers».

2.1.2 Installation

Nous nous servons de l'installateur Debian en mode non-interactif. Un fichier de préconfiguration est utilisé afin de répondre aux questions de l'installateur automatiquement. Plusieurs choix présentés par le menu lancent le même installateur, mais avec des préconfigurations différentes. Ces différences sont principalement une adaptation de la configuration des disques et des partitions. Pour les portables, une installation du système d'exploitation sur un système de fichier racine chiffré est possible. L'exécution de l'installateur s'achève avec la mise à disposition d'un système Debian GNU/Linux minimal. La suite de l'installation se déroule après le redémarrage à l'aide d'un script dédié. Ce script est téléchargé et remplace le fichier `/etc/rc.local`.

2.2 Configuration du système en utilisant `bcfg2`

Après le premier reboot, notre `/etc/rc.local` est exécuté. Ce script installe `bcfg2` et l'exécute.

`Bcfg2` est un outil de gestion de configuration. La philosophie de `bcfg2` est de décrire précisément l'état souhaité pour chaque machine et d'effectuer les opérations nécessaires pour arriver à cet état. Un état correspond à un ensemble de paquets installés, de fichiers en place, et de services démarrés. La spécification se découpe en trois parties utilisant une syntaxe XML simple :

1. Définition des méta-données
2. Définition formelle
3. Configuration littérale

2.2.1 Bcfg2 : définition des méta-données

Méta-données statiques un profil est associé à chaque machine. À ce profil, sont affectés des groupes et des Bundles. Les groupes permettent l'organisation des configurations à obtenir, tandis que les Bundles sont des objets utilisés pour la spécification de la configuration formelle expliquée plus tard dans cet article (voir 2.2.2).

L'affectation d'un profil à une machine est définie dans le fichier Metadata/clients.xml :

```
<Clients version="3.0">
  <Client profile="tp" name="c124-01.enst.fr"/>
  [...]
</Clients>
```

La définition des profils se trouve dans le fichier Metadata/groups.xml.

```
<Group name="tp" profile="true" public="true">
  [...]
</Group>
<Group name="tsi_tp" profile="true" public="true">
  <Group name="tp"/>
  <Bundle name="tsi-printers"/>
</Group>
```

Un groupe peut être inclus dans un autre groupe, auquel cas, il hérite des configurations de ce dernier. Une machine reçoit toutes les configurations de tous les groupes auxquels elle appartient. Dans notre exemple précédent, on peut voir que les machines du groupe tsi_tp appartiennent au groupe tp.

La configuration installée dépend de l'utilisation de la machine (machine de bureau, machine de salles de TP, serveur de calcul), et de l'entité dont dépend la machine (TSI, ComElec ou DSI). La gestion se fait de manière matricielle. Modifier la configuration des machines de bureau aura une influence dans tous les départements tandis que modifier la configuration liée à un département n'impactera que celui-ci.

Affectation dynamique d'une machine à des groupes : Bcfg2 peut effectuer une affectation dynamique de machines à des groupes via l'exécution de scripts. Nous avons écrit des sondes pour prendre en compte les hétérogénéités matérielles de notre parc et installer tous les pilotes et les logiciels utiles lorsque cela s'avère nécessaire. Ci-après un exemple de sonde pour le matériel nvidia, on peut voir qu'il s'agit d'un très simple script shell.

```
#!/bin/sh
if which lspci >/dev/null 2>&1; then
  lspci -nmmd 10de: | uniq -f6 | \
  awk '($2=="\0300\" || $2=="\0302\"") {print "group:probe_nvidia"}'
fi
```

Le script est stocké sur le serveur bcfg2, et exécuté par le client au moment du lancement de bcfg2. Son exécution aura pour effet de placer la machine dans le groupe probe_nvidia si le script a renvoyé group:probe_nvidia.

2.2.2 Bcfg2 : configuration formelle

On peut spécifier quatre types de configurations dites formelles

- installation d'un paquet ;
- chemin ou système de fichier (répertoire, lien, fichier ou permission) ;
- démarrage d'un service ;
- exécution d'une commande.

```

<Bundle name="X11" version='2.0'>
  <Service name="mdm"/>
  <Group name="probe_nvidia">
    <Package name="nvidia-kernel-dkms"/>
    [...]
    <Path name="/etc/modprobe.d/nvidia-kernel-common.conf"/>
  </Group>
</Bundle>

```

Dans l'exemple proposé ci-dessus, on voit que dès qu'un ordinateur se trouve dans le groupe `probe_nvidia`, le paquet `nvidia-kernel-dkms` doit être installé et le fichier `/etc/modprobe.d/nvidia-kernel-common.conf` doit exister. De même, on peut également remarquer, que dès qu'une machine installe le Bundle `X11` le service `mdm` doit être configuré.

Ces directives formelles que constituent ces bundles sont rangées dans un répertoire `Bundler`.

La manière dont chaque directive (ici `Path`, `Package` et `Service`) est traitée se trouve décrite dans la configuration littérale. Plusieurs extensions fournissent les outils qui permettent de construire cette configuration littérale.

2.2.3 Bcfg2 : configuration littérale

Paquets : le logiciel `bcfg2` est muni d'un pilote pour gérer l'installation de paquetage sur les grandes distributions GNU/Linux (basées sur `rpm`, sur `apt`, sur `portage`, ...), sur `FreeBSD`, sur `OpenBSD`, sur `MacOS X`, sur `Solaris`, ... Le fonctionnement de `bcfg2` impose que lorsqu'un paquet est défini pour être installé, il faut en spécifier la version. Nous n'utilisons que `Debian GNU/Linux`, ce qui a conduit à une légère modification de `bcfg2`. En effet, le gestionnaire de paquets de `Debian` étant particulièrement efficace, nous l'utilisons aussi pour gérer les versions des paquets à installer. `Bcfg2` est modifié pour installer la version préconisée par la configuration d'`apt` ainsi que ses dépendances. L'administrateur n'a donc ni besoin de préciser le numéro de version de chaque programme à installer, ni de dresser la liste complète des dépendances nécessaires. Cela simplifie grandement l'utilisation de `bcfg2`.

Cfg : ce répertoire contient les fichiers de configuration à déployer. Chaque fichier se trouve dans un répertoire qui porte son propre nom. Ce même répertoire est placé dans une arborescence analogue au système final. Par exemple, pour le fichier `xorg.conf`. Cette configuration se trouve définie dans le répertoire `<config_dir>/Cfg/etc/X11/xorg.conf`. `Cfg` permet aussi de gérer les cas particuliers. `Bcfg2` définit des priorités sur les fichiers :

1. le fichier est suffixé par `H_fqdn` ;
2. le fichier est suffixé par `GXX_group` ou `XX` est compris entre 0 et 100. L'entrée est d'autant plus prioritaire que `XX` est faible ;
3. le fichier n'est suffixé par rien du tout.

```

$ pwd
/srv/bcfg2/Cfg/etc/X11/xorg.conf
$ ls
xorg.conf                xorg.conf.H_c130-01.enst.fr    [...]
xorg.conf.G50_probe_nvidia  xorg.conf.H_c124-05.enst.fr

```

L'exemple présenté ci-dessus présente un fichier particulier pour le groupe `probe_nvidia` et pour quelques machines. Les permissions liées à la création du fichier des configurations sur la machine cible sont définis par un dernier fichier `:info` dans le même répertoire. Dans notre exemple, ce fichier `:info` n'existe pas, les fichiers de configurations sont donc créés avec les droits par défaut (644) et appartiennent à `root:root`.

`Bcfg2` embarque également deux langages de template : *cheetah* et *genshi*. Les priorités définies ci-dessus sont conservés permettant ainsi de gérer au mieux les cas particuliers. Il suffit pour cela de suffixer le nom du fichier par le type de template. On pourrait avoir dans notre exemple un fichier `xorg.conf.G50_probe_nvidia.cheetah` pour un template qui ne s'applique qu'à un groupe.

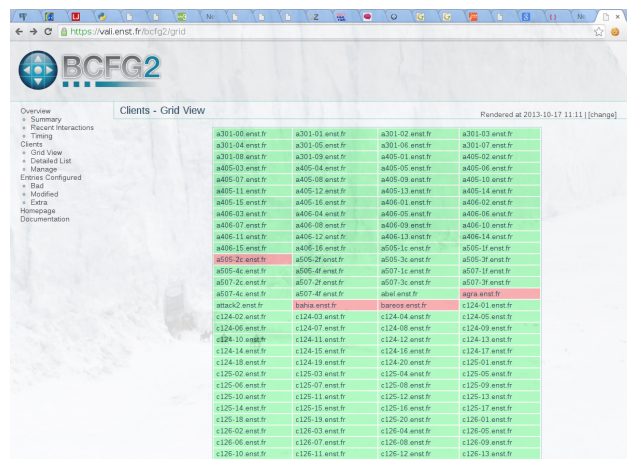
Rules : ce plugin permet de décrire des services, des liens, des répertoires et des permissions. Par exemple d'installer un service en spécifiant s'il doit être lancé ou non.

L'exemple ci-après spécifie le nom d'un service Debian, qui doit être lancé. L'attribut mode="default" signifie que le service doit être installé lors de l'installation du paquet, puis exécuté. La target="reload" définit qu'une modification du Bundle dans lequel se trouve le service entraînera une réexécution du service. Relancer le service pourrait être désagréable pour un utilisateur en train d'utiliser l'ordinateur.

```
<Rules priority="0">
  <Service name="mdm" type="deb" status="on" mode="default" target="reload"/>
</Rules>
```

SSHBase : ce plugin permet de gérer les clés ssh de toutes les machines, et de générer le fichier /etc/ssh/known_hosts pour chaque poste qui en découle.

Statistics : bcfg2 est fourni avec des outils de visualisations graphiques et de rapports d'actions, très pratique pour obtenir une vision de l'état du parc (voir figure 3).



The screenshot shows the BCFG2 web interface in a browser window. The page title is "Clients - Grid View" and it was rendered on 2013-10-17 11:11. The main content is a grid of client information. The grid has 4 columns and many rows. Each row represents a client and contains four entries, each with a unique ID and the text "enst.fr". For example, the first row contains "a301-00 enst.fr", "a301-01 enst.fr", "a301-02 enst.fr", and "a301-03 enst.fr". The grid is mostly green, indicating a successful state, but some rows are highlighted in red, such as the row containing "a507-3c enst.fr" and "a507-3d enst.fr".

Figure 3 - Rendu de la page de rapports

2.3 Personnalisation du système final

Debian GNU/Linux ne fournit pas tous les éléments nécessaires aux besoins pédagogiques et d'enseignement. En effet, il reste à installer tous les logiciels nécessitant des licences particulières et possédant des procédures d'installation propres. Il s'agit en particulier de matlab, des logiciels de mesures et de simulations scientifiques. Un script exécute simplement les procédures d'installation de ces logiciels, sur les clients là où c'est nécessaire et où les licences desdits logiciels le permettent (matlab, maple, ...). Nous ne pouvons utiliser bcfg2 car il n'est pas adapté à la distribution de nombreux fichiers binaires.

3 Virtualisation

3.1 Motivations

Pour certains besoins pédagogiques, les utilisateurs doivent disposer d'une installation de Windows ou d'un accès administrateur à leur poste. Pour adresser cette problématique, l'école a d'abord eu des salles munies de postes à double démarrage (Windows et GNU/Linux). Cela s'est révélé compliqué à maintenir, la faute à la gestion de deux systèmes

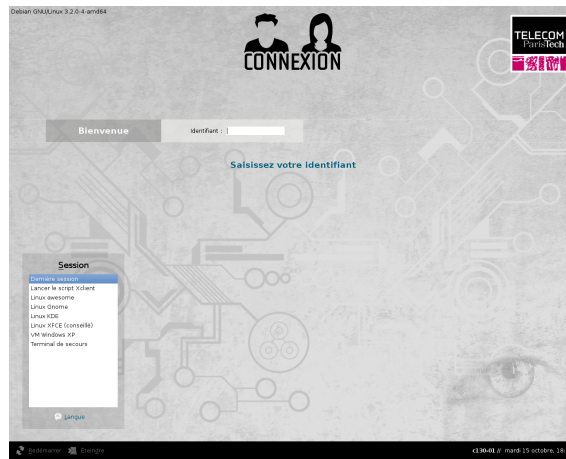


Figure 4 - Fenêtre de login

d'exploitation dont un seul est accessible à la fois à un instant donné. Cela peut également nécessiter une intervention directement sur le poste, alors que la préférence est donnée à l'administration distante pour gagner du temps.

Les salles ont ensuite été dédiées à un seul système d'exploitation (salle sous environnement Windows, et salles sous environnement GNU/Linux). Cela posait d'importantes contraintes en termes d'emploi du temps.

Nous souhaitons une solution qui permette d'adresser tout ces problématiques et lever toutes ces contraintes.

3.2 Virtualisation : VirtualBox

La virtualisation adressait point par point à toutes ces problématiques. En effet, les données des machines virtuelles restent accessibles depuis l'hôte, que celle-ci soit allumée ou éteinte. Cela permet à la fois de mettre à jour l'hôte et la machine virtuelle depuis l'hôte.

Pour le choix de la technologie, il fallait une interface graphique simple n'exigeant pas une élévation de privilège à disposition des utilisateurs. Cela disqualifiait de facto nombre de solutions de virtualisation. Il ne restait plus que VirtualBox et les solutions VMware comme choix possibles. Du fait des restrictions dues à la licence des logiciels proposés par VMware, VirtualBox a été retenu. De plus, les solutions VMware ne nous permettaient pas d'obtenir la configuration réseau souhaitée. Les disques durs des machines virtuelles sont en lecture seule. Chaque utilisateur peut posséder sa propre image de machine virtuelle sous forme d'un fichier de différences par rapport à la version de référence distribuée par la DSI.

En cas de problèmes, possibilité est donnée à l'utilisateur de réinitialiser sa propre machine virtuelle. Ce mécanisme est particulièrement intéressant pour pouvoir donner un accès administrateur aux utilisateurs. Ainsi, ils peuvent faire ce qu'ils veulent dans la machine virtuelle sans impact avec le système hôte. Une seule restriction : afin de protéger le réseau de l'hôte des attaques de type « arp cache poisoning » et d'écoutes utilisant l'interface de l'hôte, VirtualBox a été modifié pour empêcher de donner un accès direct via un pont sur l'interface réseau de l'hôte. Pour les enseignements traitant spécifiquement de réseau une interface virtuelle a été ajoutée. Celle-ci est connectée à un vlan dit « bac à sable ». Cela autorise entre autres, la création de service (serveur web, ftp,...), le sniffing/scanning, et ainsi mettre en évidence certaines attaques réseau à des fins pédagogiques.

Pour la simplicité d'usage, une machine virtuelle sous Windows XP est proposée directement dans le gestionnaire de login (voir la figure 4). Pour les autres machines virtuelles, proposées soit par les enseignants, soit par la DSI, un menu dédié est ajouté.

Ainsi par exemple, il a été possible de proposer une solution permettant à la fois la programmation d'un circuit imprimé grâce à une machine virtuelle sous Windows, et l'organisation de mesures sur le même circuit imprimé depuis l'hôte sous GNU/Linux. La souplesse obtenue dans le système final est très satisfaisante.

3.3 Distribution pair-à-pair

La machine virtuelle Windows déployée a été construite en capturant une image Windows tournant sur les postes de travail dans les salles de TP. Beaucoup de logiciels ont été installés pour des besoins pédagogiques (dont certains hors actualité

aujourd'hui). Avec le temps, l'image de la machine virtuelle a atteint environ 50Go.

À l'origine ces images étaient déployées par simple copie depuis un partage nfs. Cela avait pour conséquence un impact fort sur le serveur nfs, spécialement si plusieurs machines étaient en cours d'installation en même temps. Seuls quatre postes étaient alors instanciables simultanément. Cela limitait de fait les possibilités d'évolution du système pour mettre en place une mise à jour des machines virtuelles.

Nous avons donc mis en place un système de distribution de ces fichiers par un service pair à pair. Le logiciel utilisé sur le serveur de machines virtuelles est bittornado. Ce produit s'articule autour de deux démons principaux : un tracker et un client. Il est configuré pour ne «partager» les fichiers que d'un seul répertoire dans lequel se trouvent les images à distribuer. Pour la création du fichier «torrent» sur le tracker, à effectuer à chaque nouvelle mise à jour des machines à distribuer, il suffit d'exécuter simplement la commande suivante

```
cd /srv/vms/archives/VMcatalog/  
btmakemetafile.bittornado http://nfs-vms.enst.fr:6969/announce <Dossier>
```

Pour la partie cliente, le tracker n'est pas nécessaire. Les fichiers «torrent» sont distribués à l'aide de bcfg2. La mise à jour d'un fichier torrent entraîne la mise à jour de la machine virtuelle associée.

Au niveau de l'efficacité réseau, plus le nombre de machines à installer (ou déjà installées) en même temps est élevé, plus le temps de téléchargement des machines virtuelles s'en trouve globalement réduit.

4 Évolution des configurations

Nous utilisons également bcfg2 pour faire évoluer notre parc en tenant compte des nouveaux besoins. Il permet de maintenir les configurations des postes clients : l'installation de nouveaux logiciels et les évolutions de configurations sont totalement gérées par le serveur.

En pratique chaque poste exécute un script tous les jours (anacron) qui effectue la mise à jour du système (avec les outils apt) et exécute bcfg2.

Par contre, une contrainte apparaît sur les machines virtuelles en raison de la place qu'elles occupent sur les postes clients ; une toute petite modification de la machine virtuelle nécessitant de la recopier sur tous les postes. Bcfg2 est utilisé pour mettre à jour le fichier torrent ayant pour effet de remplacer la machine virtuelle par sa nouvelle version.

Pour les salles de travaux pratiques, un environnement virtuel est importable rapidement à la demande d'un enseignant.

5 Conclusion

Notre solution a permis la mise en place d'un système centralisé automatique répondant à un grand nombre de besoins d'un établissement d'enseignement supérieur et de recherche :

- la configuration personnalisée des postes clients adaptée à leur utilisation (poste de bureau, poste de salles de travaux pratiques et poste pilote d'instrumentation) ;
- la possibilité d'utiliser des machines virtuelles en tant qu'administrateur ;
- la possibilité d'utiliser un système d'exploitation windows sur les postes ;
- une solution facilement administrable et adaptable à un environnement avec beaucoup de besoins différents.

L'accent a été mis sur la simplification des configurations pour un accès facilité pour le plus grand nombre. La procédure de lancement est assez simple pour que les personnels, même non spécialistes de GNU/Linux puissent procéder à une installation.