

firewall name=firewall, description=Protection pour serveur
naxsi name=naxsi, description=Un type de firewall

LICENCE ASRALL

EXPOSÉ TECHNIQUE

Fully Automatic Installation

François DUPONT

Florent FILLION

29 janvier 2015

Table des matières

1	Introduction	2
1.1	Objectifs	2
1.1.1	Définition	2
1.1.2	Utilité	2
1.2	Histoire	2
1.2.1	La documentation	3
1.3	Concepts	3
1.3.1	Réseau	3
1.3.2	Système	4
2	Technique	5
2.1	La base	5
2.1.1	DNS, DHCP et PXE	5
2.1.2	Installer fai-quickstart	6
2.1.3	NFSROOT	7
2.1.4	configuration de bases	7
2.2	Configurations avancées et options en tout genres	7
2.2.1	Le Debian mirror	7
3	Alternatives	8
3.1	Jumpstart	8
3.2	Kickstart	11
3.3	Rembo	13
3.4	Clonezilla	13
4	Conclusion	16
5	Sources	17

Chapitre 1

Introduction

1.1 Objectifs

1.1.1 Définition

Fully Automatic Installation ou FAI est un logiciel libre, inspiré de son équivalent SOLARIS, JUMPSTART. Il permet d'installer et de configurer un système d'exploitation Linux sur une ou plusieurs machines, en utilisant une infrastructure client serveur, de façon rapide et automatisée.

Il est à noter que FAI n'est pas interactif contrairement à d'autres logiciels remplissant sensiblement la même fonction. Ce logiciel est également considéré comme mature puisqu'il en est à sa 4^{ème} itération majeure (4.0) et est développé de façon continue depuis 1999.

1.1.2 Utilité

FAI s'adresse particulièrement aux administrateurs ayant à gérer un grand parc de machine sous Linux, que ce parc soit *virtualisé* ou physique (et même des *chroots*). On peut citer EDF qui a récemment utilisé FAI pour déployer son cluster/Super Ordinateur utilisant Debian. (classé dans les 50 premiers mondiaux au moment de son déploiement). De nombreuses universités comme le MIT l'utilisent pour gérer leur parc de machines GNU/Linux en comportant en général des centaines voire des milliers de postes clients.

1.2 Histoire

FAI est née en 1999 alors que Thomas LANGE, Administrateur système expérimenté sur Solaris a dû déployer plusieurs machines Debian/Gnu/Linux. Comme

tous les administrateurs (*compétents ?*), il déteste réaliser des choses répétitives et décide donc de s'atteler à l'automatisation du déploiement de machines Debian. Son projet est un succès, et est maintenant utilisé par de nombreuses administrations, écoles et entreprises. Il est également, depuis, devenu développeur Debian.

Il a depuis été rejoint par d'autres développeurs, notamment Michael PROKOP également développeur Debian et aussi mainteneur du dérivé minimaliste et orienté pour l'administration système GRML. Et par Kerim GUENEY collègue de LANGE à l'Université de Cologne.

1.2.1 La documentation

On peut remarquer que ce projet est assez germano centré, tous les développeurs sont allemands ou bien travaillent dans une université allemande. Cela ne pose pas de grands problèmes dans la mesure où presque toute la documentation disponible est disponible en anglais. Le problème est que cette dernière n'est pas maintenu très à jour (elle est souvent à jour de façon éclaté, wiki à jour mais le guide non, parfois l'inverse). Il existe cependant peu de *talks*, ou documentation externe qui soit à jour ou pas en allemand.

1.3 Concepts

Cette partie pourrait avoir sa place dans le chapitre traitant de la technique à proprement parler, cependant, il nous semble essentiel d'exposer les principes fondamentaux (et simples une fois assimilés) de FAI. Il s'agit ici d'un survol, plus d'informations seront disponibles dans la partie réservée à la technique.

1.3.1 Réseau

Classique

Pour utiliser FAI vous devez avoir un réseau fonctionnel, avec un dhcp configuré, et un DNS fonctionnel. Moins classique, vous DEVEZ utiliser vos machines avec un démarrage réseau par PXE pour l'installation.

Architecture Client Serveur

FAI ne fonctionne qu'en mode client serveur (et pas par exemple en pair à pair). Avec 1 serveur pour N clients. Il faut cependant bien comprendre qu'un serveur peut délivrer plusieurs configurations (une Debian stable, une Debian testing, un Ubuntu ou même un RedHat), tout dépend de la configuration.

1.3.2 Système

L'installation

Une fois votre réseau en place et FAI installé sur un serveur vous pourrez éveiller le client (physiquement, wakeonlan) par PXE, le client ira ensuite s'identifier auprès du serveur. Notre client monte ensuite un partage NFS présent sur le serveur comme sa racine, une fois le noyau chargé, les scripts d'installation FAI suivent leur cours et installe les configurations demandées par l'administrateur. Ces scripts peuvent inclure un partitionnement des disques ou bien formatage, l'installation de logiciels spécifique, gestion du RAID matériel, etc...

Il est possible d'utiliser un système de classe (programmation) pour créer des groupes d'ordinateurs similaires et ainsi faciliter l'industrialisation de notre installation (il serait contre productif d'avoir à un profil par client). Il est possible d'utiliser plusieurs langages pour réaliser les scripts, bash, perl, ruby.

La configuration

La configuration doit être effectué avant de lancer une installation, pour rappel cette dernière n'est pas interactive, en revanche de nombreuses choses sont paramétrables en modifiant les bons fichiers et parfois quelques scripts.

Chapitre 2

Technique

Dans cette partie nous allons expliquer le fonctionnement plus précis de FAI en détaillant chaque composant majeur et dans la mesure du possible les différentes technologies disponibles pour réaliser ces actions ainsi que leurs principes.

2.1 La base

2.1.1 DNS, DHCP et PXE

Pour pouvoir utiliser FAI il faut avoir un DHCP et un DNS fonctionnel, bref rappel de leur utilité, le DHCP attribue une adresse IP à une adresse MAC, le DNS donne un nom à une IP.

La distribution FAI-SERVER propose d'utiliser le serveur `iscdhcp` une implémentation de référence maintenu par l'Internet Systems Consortium qui maintient également BIND (*bref un truc sérieux*). Pour une petite installation il est possible de jouer *old school* et d'utiliser le fichier `/etc/hosts` plutôt que d'utiliser un DNS sérieux, la documentation (et la logique aussi) nous dit que cela fonctionne pareil.

La configuration du DHCP est aisée même quand c'est la première fois et même avec un PXE coté client puisque la documentation interne fournie.

Fonctionnement de PXE

L'amorçage PXE (Pre-boot eXecution Environment) est un environnement de démarrage d'ordinateurs permettant à une machine de démarrer depuis le réseau en récupérant une image de système d'exploitation qui se trouve sur un serveur. L'image stockée sur le serveur PXE peut être un système d'exploitation brut ou bien un système d'exploitation personnalisé avec des composantes logicielles (suite bureautique, utilitaires, packs de sécurité, scripts, etc...). L'image peut ensuite être

installée sur une machine cliente distante (ou un serveur distant) qui a été amorcée en PXE.

Pour activer PXE côté client, il suffit d'activer celui-ci dans le bios de la machine. L'option se trouve fréquemment dans un menu concernant la carte réseau. Cependant, PXE n'est pas toujours disponible notamment sur les machines ne possédant pas de carte réseau suffisamment récente.

Pour qu'une machine puisse utiliser PXE, plusieurs serveurs sont nécessaires : un serveur PXE, un serveur DHCP et un serveur TFTP.

L'amorce par PXE s'effectue ainsi en plusieurs étapes :

1. la machine cliente demande une adresse IP au serveur DHCP
2. une fois l'adresse IP récupérée, le client établit une connexion avec le serveur PXE puis recherche sur ce serveur un programme de démarrage réseau
3. lorsque le programme de démarrage est trouvé, la machine cliente télécharge le fichier à amorcer depuis un serveur TFTP (TFTP étant un protocole de transfert de fichiers fonctionnant en UDP sur le port 69)
4. le fichier étant récupéré, le client l'exécute sur sa machine pour pouvoir "booter" un noyau (noyau Linux par exemple)

2.1.2 Installer fai-quickstart

De façon assez surprenant fai-quickstart (qui est indispensable à l'utilisation de FAI) n'est pas disponible sur la distribution FAI de base.

Ce paquet contient le serveur DHCP cité ci-dessus. Ainsi que le serveur tftp qui sera utilisé pour transférer notre distribution plus tard.

TFTP

TRIVIAL FILE TRANSFERT PROTOCOLE est un protocole de transfert de fichier qui utilise le protocole UDP (rappelons qu'UDP est un protocole de la couche 4 du modèle OSI, la couche transport. Contrairement à TCP, UDP ne fait pas de négociations et ne vérifie pas non plus l'intégrité des données qu'il délivre).

Ce protocole est généralement utilisé pour le streaming vidéo/audio ou encore les jeux en réseaux, plus généralement pour toutes les applications où l'exactitude du message est négligeable devant la nécessité de réactivité. Avec FAI on tire partie de la capacité d'UDP à envoyer très vite beaucoup de données de petites taille. Ce gain de vitesse par rapport à tcp est lié à l'absence de handshake. L'expérience montre que l'UDP utilisé sur un réseau local de QUALITÉ ne présente presque jamais de problèmes d'intégrité.

TFTP en lui même est une version simplifié de FTP (pas de gestion de droits pas de possibilité de ls ou delete dans un répertoire) il est conçu pour la mise à jour ou la copie simple de fichiers.

2.1.3 NFSROOT

2.1.4 configuration de bases

2.2 Configurations avancées et options en tout genres

On peut configurer de nombreuses choses avec FAI

2.2.1 Le Debian mirror

Une des astuces facile voire évidente est l'installation d'un miroir Debian en local (que ce soit ou non sur notre fai-server)

Chapitre 3

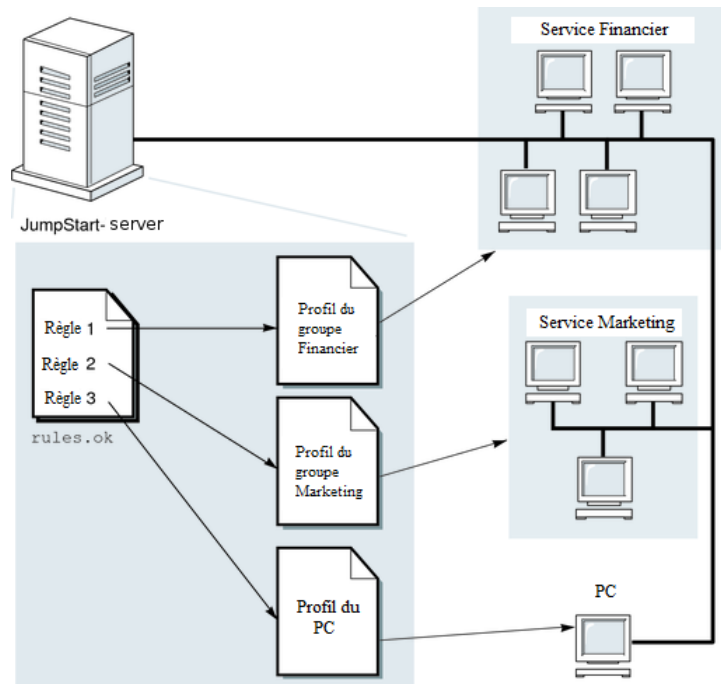
Alternatives

3.1 Jumpstart

Jumpstart a été créé par Sun Microsystems, qui fut ensuite racheté en 2009 par Oracle Corporation. C'est un outil permettant d'automatiser l'installation d'une ou plusieurs machines utilisant Solaris comme système d'exploitation. La configuration de Jumpstart s'effectue à l'aide de plusieurs fichiers :

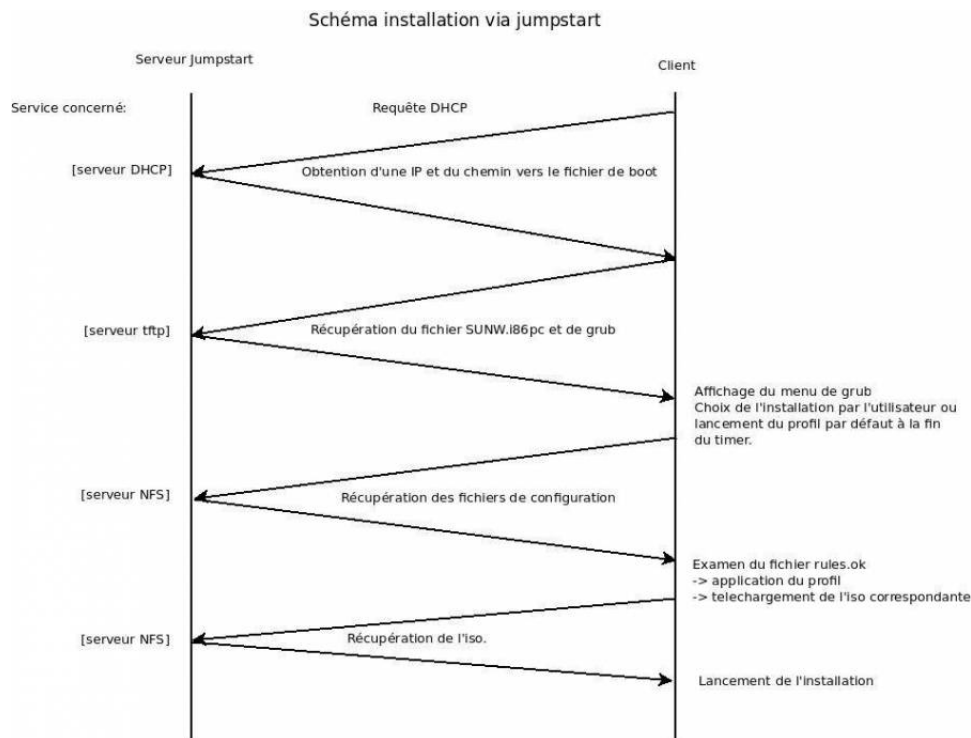
- Le fichier *profile* qui définit les partitions de disques.
- Les fichiers *rules* et *rules.ok* qui définissent les règles correspondant à un profil particulier de client à installer.
- Des scripts s'exécutant avant et après l'installation de la machine cliente.
- Le fichier *sysidcfg* qui définit les informations de configuration du client, comme par exemple son nom d'hôte, son adresse IP, etc...
- Le fichier */etc/bootparams* qui est utilisées par les machines clientes pour démarrer.
- Le fichier */etc/ethers* qui contient les mappages d'adresses MAC pour les clients.

Lors de l'installation, le programme Jumpstart va tenter de faire correspondre le système à installer aux règles définies dans le fichier *rules.ok*. Il lit donc ces règles, de la première à la dernière. Lorsque qu'une correspondance est établie entre un système et une règle, le programme JumpStart interrompt la lecture du fichier *rules.ok* et commence l'installation du système d'après le profil correspondant à la règle associée.



Un serveur DHCP peut également être mis en place sur le serveur Jumpstart afin d'attribuer automatiquement une configuration IP aux machines clientes.

Voici un schéma représentant brièvement les requêtes effectuées entre les clients et le serveur lors du démarrage de l'installation :



Configuration du serveur Jumpstart

Voici la liste des tâches à effectuer lors de la préparation à une installation JumpStart :

- Créer un répertoire JumpStart
- Ajouter des règles pour chaque groupe dans le fichier *rules* :
Chaque règle définit un groupe d'après un ou plusieurs attributs système. La règle lie chaque groupe à un profil.
- Créer un profil pour chaque règle :
Un profil est un fichier texte qui définit l'installation du logiciel Solaris, et indique par exemple le groupe de logiciels devant être installé sur un système. À chaque règle correspond un profil qui définit la procédure d'installation du logiciel Solaris sur un système. Ce profil est utilisé dès qu'une correspondance est établie entre une règle et un système déterminés.
Généralement, on définit un profil pour chaque règle. Le même profil peut toutefois être utilisé dans plusieurs règles.
- Valider le fichier *rules* :

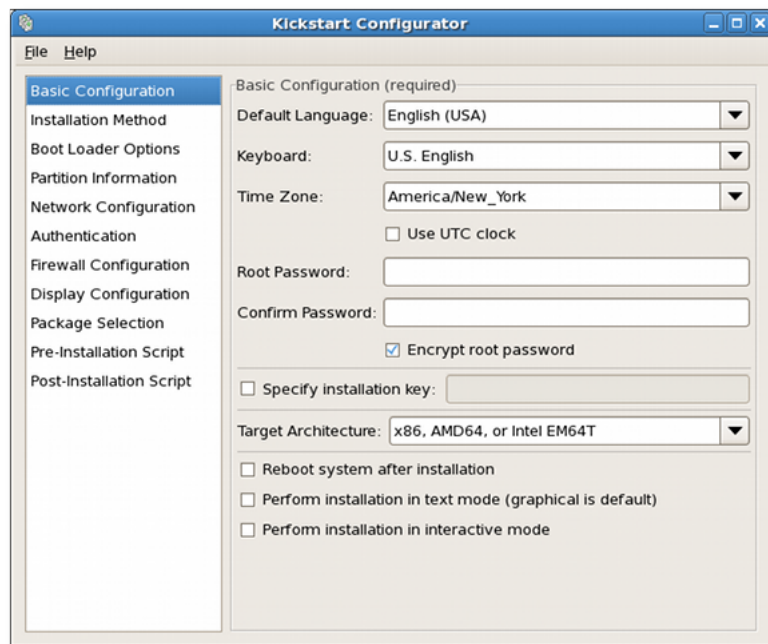
Le fichier *rules.ok* est une version générée du fichier *rules* qu'utilise JumpStart pour détecter le système à installer avec un profil. Le fichier *rules* se valide par l'intermédiaire d'un script *check*.

3.2 Kickstart

Kickstart a été créé par RedHat afin d'automatiser l'installation de Fedora et Red Hat Enterprise Linux. Sa configuration s'effectue dans un fichier kickstart *ks.cfg* unique contenant une liste d'éléments, chacun identifié par un mot-clé. Ces éléments correspondent aux réponses à toutes les questions qui devraient normalement être posées lors d'une installation typique. Ce fichier peut être créé manuellement en partant d'un fichier vierge puis en écrivant les directives une par une.

Cependant, et contrairement à FAI, il existe une interface utilisateur graphique, "Kickstart Configuration", permettant ainsi une configuration plus simple puisque il n'est pas nécessaire de se rappeler de la syntaxe exacte du fichier kickstart à configurer.

Il suffit donc de suivre les étapes les unes après les autres afin de configurer petit à petit le fichier en question :



Si l'on souhaite effectuer une installation plus fine et personnalisée, il est également possible de rajouter des scripts d'installations via l'interface graphique. Ces scripts peuvent être exécuté avant (Pre-Installation Script) ou après l'installation (Post-Installation Script) :

The screenshot shows a graphical user interface for configuring a Pre-Installation Script. On the left is a vertical sidebar with a list of configuration options: Basic Configuration, Installation Method, Boot Loader Options, Partition Information, Network Configuration, Authentication, Firewall Configuration, Display Configuration, Package Selection, Pre-Installation Script (highlighted in blue), and Post-Installation Script. The main area is titled 'Pre-Installation Script' and contains a warning message: 'Warning: An error in this script might cause your kickstart installation to fail. Do not include the %pre command at the beginning.' Below the warning is a checkbox labeled 'Use an interpreter:' followed by an empty text input field. At the bottom of the main area is a large text area with the prompt 'Type your %pre script below:'.

Si l'on souhaite par exemple effectuer manuellement une configuration réseau dans le fichier kickstart, il suffira d'inclure le script dans la zone de texte prévue à cet effet.

En effet, avant le début de l'installation, le fichier kickstart est analysé afin de détecter les différentes commandes à exécuter. Si une configuration réseau est détectée dans le fichier kickstart, avant que la section "Network Configuration" soit traitée, la configuration réseau sera prioritaire et prise en compte.

Pour spécifier un langage de script particulier à utiliser pour exécuter le script, il suffit de sélectionner l'option "use an interpreter" et d'entrer le langage souhaité, par exemple `/usr/bin/python2.7`.

Une fois la configuration terminée, il est tout de même possible de consulter le fichier kickstart avant de le sauvegarder.

Il suffit ensuite de placer le fichier `ks.cfg` généré sur le support de démarrage souhaité, puis de booter la machine cliente sur ce même support de démarrage.

Une commande de démarrage spéciale est à taper à l'invite de démarrage. Le programme d'installation va ainsi rechercher si un fichier kickstart est présent, puis va s'en servir pour procéder à l'installation du système.

3.3 Rembo

Rembo est le successeur de BPBatch. Il a été créé par "Rembo Technology", une société suisse spécialisée dans les outils de gestion applicative et de virtualisation de serveurs, qui fut ensuite rachetée en 2006 par IBM. Rembo est un environnement de déploiement d'applications qui permet d'installer rapidement et en même temps, n machines du même type. Il peut s'exécuter sur Windows, Linux ou encore FreeBSD et s'appuie sur un serveur DHCP. Les machines clientes doivent donc supporter PXE et auront donc exactement la même installation.

L'installation s'appuie sur l'utilisation d'une platine virtuelle, sur laquelle on sélectionne les programmes à installer. La procédure est ensuite entièrement automatique, et personnalisable à l'infini. Une machine virtuelle est créée à chaque installation puis est effacée lorsque le processus est terminé.

.....

3.4 Clonezilla

Clonezilla est un logiciel libre créé par le laboratoire de recherche NCHC pouvant être utilisé sur plusieurs systèmes d'exploitations différents tel que Linux, Windows ou encore MAC OS X par exemple. Il permet de créer une image de sauvegarde d'un disque dur ou d'une ou plusieurs partitions, pour ensuite la restaurer ou la cloner sur une (unicast) ou plusieurs machines clientes (multicast).

Il existe deux versions de Clonezilla, "Clonezilla Live" et "Clonezilla Server" :

- Clonezilla Live est utilisé par l'intermédiaire d'un Live CD, (ou clé usb également). Il permet à l'utilisateur d'effectuer directement depuis la machine une sauvegarde d'un disque ou d'une partition, une restauration d'une image depuis un disque, ou encore un clonage d'une image vers un autre disque. Cependant, ces actions ne peuvent s'effectuer que sur une seule machine à la fois puisque le Live CD est obligatoire.
- Clonezilla Server (ou Clonezilla SE) est utilisé depuis un serveur et autorise plusieurs postes à se connecter simultanément par l'intermédiaire d'un réseau commun. Il n'y a donc pas besoin de Live CD ce qui permet d'effectuer

des sauvegardes/restaurations/clonages sur plusieurs machines à la fois. Un serveur DRBL (Diskless Remote Boot in Linux) est utilisé ce qui permet aux stations esclaves concernées d'effectuer un démarrage PXE.



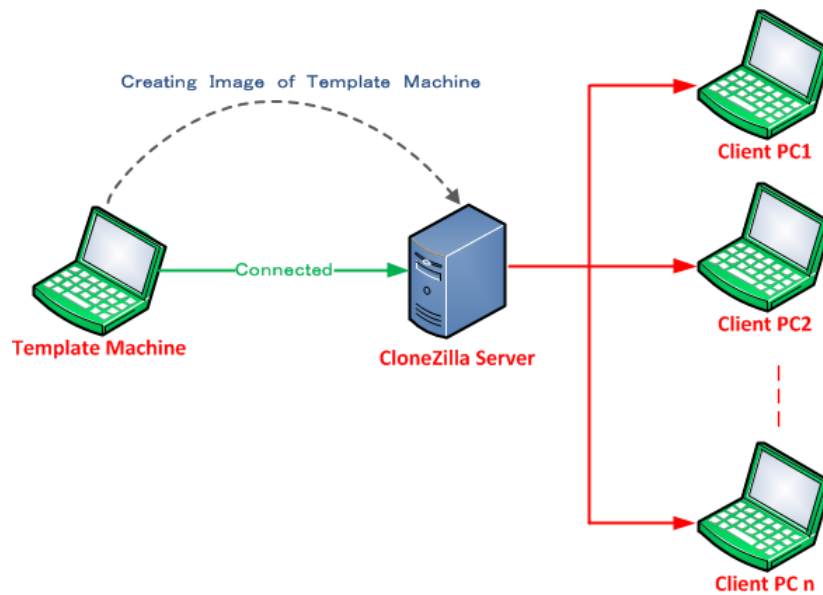
Le serveur DRBL

DRBL permet de mettre à disposition un environnement système léger pour les machines clientes et intègre Clonezilla.

Il est donc utilisé, le plus souvent, pour le clonage massif de postes de travail et le déploiement rapide de salles informatiques. Il s'appuie exclusivement sur des logiciels libres tel que *partimage*, *ntfsclone* ou encore *partclone* pour cloner des disques/partitions, et utilise également *udpcast* pour transférer des données simultanément sur plusieurs destinations via le réseau (unicast/broadcast/multicast).

DRBL supporte les systèmes de fichiers ext2, ext3, ext4, reiser4, xfs, jfs, fat, ntfs, hfs+, ufs, vmfs3 ainsi que LVM2. Les bootloaders syslinux et grub peuvent être installés.

Principe général de fonctionnement de Clonezilla Server



Le serveur Clonezilla a besoin d'une image type, afin qu'il puisse s'en servir par la suite comme référence pour sauvegarder, restaurer ou cloner cette même image sur les différentes machines clientes.

Lors d'un clonage par exemple, une fois l'image disponible sur le serveur, celui-ci va la copier simultanément sur les différentes machines clientes, via le réseaux (PXE).

Chapitre 4

Conclusion

Chapitre 5

Sources

- <http://fai-project.org/>
- <http://www.markus-gattol.name/ws/fai.html>
- <https://github.com/faipproject/fai>
- https://www.linux-magazine.com/w3/issue/100/066-071_FAI.pdf
- <http://grml.org/>
- <https://docs.oracle.com/>
- <https://access.redhat.com/documentation/>
- <http://http://clonezilla.org/>
- <https://www.projet-plume.org/fiche/drblclonezilla>
- http://fr.wikipedia.org/wiki/Preboot_Execution_Environment