Enterprise Server 5

Enterprise Server 5
Publié 2010-10-01

par Loïc Vaillant, Christophe Potigny, Andreas Hasenack, Rafaël Garcia Suarez, Emmanuel Cohen, Vincent Cuirassier, Anne Nicolas, Antoine Ginies, Yann Droneaud, Anthoine Bourgeois, Cédric Delfosse, Nicolas Perrin, et Séverine Wiltgen

Notice légale

Table des matières

Liste des tableaux

Préface

1. À propos de Mandriva Linux

Mandriva Linux est une distribution GNU/Linux développée par Mandriva S.A. La société Mandriva est née sur Internet en 1998. Son ambition première demeure de fournir un système GNU/Linux convivial et facile à utiliser. Les valeurs de Mandriva sont la simplicité, l'ouverture et l'innovation.

Le 7 avril 2005, la société Mandrakesoft a modifié son nom d'entreprise pour refléter sa fusion avec Conectiva, leader GNU/Linux du Brésil. Par conséquent, le produit phare Mandrakelinux a lui aussi changé de nom pour Mandriva Linux.

1.1. Communiquer avec la communauté Mandriva Linux

Nous présentons ci-dessous plusieurs liens Internet pointant vers de nombreuses ressources liées à Mandriva Linux. Si vous souhaitez en savoir plus sur la société Mandriva, consultez notre site Web (`http://www.mandriva.com/`)

Mandriva Expert (`http://expert.mandriva.com/`) est la plate-forme d'aide en ligne de Mandriva. Elle propose une nouvelle façon de partager les savoirs, basée sur la confiance et le plaisir de récompenser son prochain pour son aide.

Vous êtes également invité à participer aux nombreuses listes de diffusion (`http://lists.mandriva.com/`), où la communauté Mandriva Linux déploie tout son enthousiasme et sa vivacité.

Enfin, n'oubliez pas de vous connecter sur la page sécurité (`http://www.mandriva.com/security/`) (en anglais), qui rassemble tout ce qui traite de la sécurité des distributions Mandriva Linux. Vous y trouverez notamment des avertissements de bogues et de sécurité, ainsi que des procédures de mise à jour du noyau, les différentes listes de diffusion concernant la sécurité auxquelles vous pouvez vous inscrire. Ce site est incontournable pour tout administrateur système, ou tout utilisateur soucieux de sécurité.

1.2. Acheter des produits Mandriva

Vous pouvez acheter des produits Mandriva en ligne sur le Mandriva Store (`http://store.mandriva.com`). Vous y trouverez non seulement des logiciels Mandriva Linux, des systèmes d'exploitation (Free, One, PowerPack) et des clés usb « live » (Flash), mais aussi des offres spéciales d'abonnement, de l'assistance, des logiciels tiers et des licences, des manuels et des livres GNU/Linux, ainsi que d'autres gadgets Mandriva.

Pour nos offres destinées aux professionnels, vous pouvez consulter notre site (`http://www.mandriva.com/enterprise/fr`) ou contacter notre service commercial à **sales@mandriva.com**.

1.3. Contribuer à Mandriva Linux

Quels que soient vos talents, vous êtes encouragé à participer à l'une des nombreuses tâches requises à la construction du système Mandriva Linux :

- **Paquetages.** Un système GNU/Linux est principalement constitué de programmes rassemblés depuis Internet. Ils doivent être mis en forme de façon à ce qu'ils puissent fonctionner ensemble, si tout se passe bien.
- **Programmation.** Une foule de projets est directement développée par Mandriva : trouvez celui qui vous intéresse le plus et proposez votre aide au développeur principal.
- **Internationalisation.** Vous pouvez nous aider à traduire des pages de nos sites Web, des programmes et leur documentation respective.

Consultez la page projets en développement (`http://www.mandriva.com/fr/communaute/contribuer`) pour découvrir comment participer à l'évolution de Mandriva Linux.

2. Conventions utilisées dans ce manuel

2.1. Conventions typographiques

Exemple formaté	Signification
inode	Signale un terme technique.
`ls -lta`	Type utilisé pour une commande et ses arguments (voir la section Section 2.2.1).
`un_fichier`	Type utilisé pour les noms de fichier. Il peut aussi représenter un nom de paquetage RPM.
ls(1)	Référence à une page de manuel (aussi appelée page de `man`). Pour consulter la page correspondante, tapez `man 1 ls` dans une ligne de commande.

Exemple formaté	Signification
`$ ls *.pid`	Ce style est utilisé pour une copie d'écran texte de ce que vous êtes censé voir à l'écran, comme une interaction utilisateur-ordinateur ou le code source d'un programme.
`localhost`	Données littérales qui ne correspondent généralement pas à une des catégories précédemment définies : un mot clé tiré d'un fichier de configuration, par exemple.
OpenOffice.org	Désigne le nom des applications. Selon le contexte, une application et la commande qui la représente peuvent être formatées différemment. Par exemple, la plupart des noms de commande s'écrivent en minuscule, alors que les noms d'application commencent par une majuscule.
Fichier	Entrée de menu ou label des interfaces graphiques. La lettre soulignée, si présente, indique le raccourci clavier, auquel vous pouvez accéder en appuyant sur la touche **Alt** et la lettre soulignée.
Once upon a time...	Citation en langue étrangère.
Attention !	Type réservé pour les mots que nous voulons accentuer. Lisez-les à voix haute !

Cette icône introduit une note. Il s'agit généralement d'une remarque dans le contexte courant, pour donner une information complémentaire.

Cette icône introduit une astuce. Il peut s'agir d'un conseil d'ordre général sur la meilleure façon d'arriver à un but spécifique ou une fonctionnalité intéressante qui peut vous rendre la vie plus facile, comme les raccourcis clavier.

Soyez très attentif lorsque vous rencontrez cette icône. Il s'agit toujours d'informations très importantes sur le sujet abordé.

2.2. Conventions générales

2.2.1. Synopsis d'une commande

L'exemple ci-dessous présente les symboles que vous rencontrerez lorsque nous décrivons les arguments d'une commande :

```
commande <argument non littéral> [--option={arg1,arg2,arg3}
      [argument optionnel...]
```

Ces conventions étant standardisées, vous les retrouverez en bien d'autres occasions (dans les pages de `man`, par exemple).

Les signes « < » (inférieur) et « > » (supérieur) indiquent un argument **obligatoire** qui ne doit pas être recopié tel quel mais remplacé par votre texte spécifique. Par exemple : `<fichier>` désigne le nom d'un fichier ; si ce fichier est `toto.txt`, vous devrez taper `toto.txt`, et non `<toto.txt>` ou `<fichier>`.

Les crochets (« [ ] ») indiquent des arguments optionnels que vous déciderez ou non d'inclure dans la ligne de commande.

Les points de suspension (« ... ») signifient qu'un nombre illimité d'arguments peut être inséré à cet endroit.

Les accolades (« { } ») contiennent les arguments autorisés à cet endroit. Il faudra obligatoirement en insérer un à cet endroit précis.

2.2.2. Notations particulières

De temps à autre, il vous sera demandé d'appuyer sur les touches **Ctrl**-**R**, cela signifie que vous devez maintenir la touche **Ctrl** enfoncée pendant que vous appuyez sur la touche **R**. Il en va de même pour les touches **Alt** et **Shift**.

Nous utilisons des lettres majuscules pour représenter les touches clavier. Ceci n'implique pas que vous deviez les utiliser en majuscule. Toutefois, dans certaines applications, il est possible que le fait de taper **R** ou **r** n'ait pas le même effet. Nous vous le signalerons lorsque ce sera le cas.

De même, à propos des menus, aller sur l'entrée de menu Fichier→Relire la configuration utilisateur (**Ctrl-R**) signifie : cliquez sur le label Fichier du menu (généralement en haut et à gauche de la fenêtre) puis sur le menu vertical qui apparaît, cliquez sur Relire la configuration utilisateur. De plus, vous pouvez également utiliser la combinaison de touches **Ctrl**-**R**, comme décrit ci-dessus pour arriver au même résultat.

2.2.3. Utilisateurs système génériques

Chaque fois que cela est possible, nous utilisons deux utilisateurs génériques dans nos exemples :

Reine Pingusa	reine	C'est notre utilisateur par défaut, que nous utilisons dans la plupart des exemples de ce manuel.
Pierre Pingus	pierre	Cet utilisateur peut ensuite être créé par l'administrateur système. Nous l'utilisons quelques fois afin de varier le texte.

Démarrer une installation en toute tranquillité

Mandriva Linux reconnaît un très grand nombre de périphériques matériel, et la liste est bien trop longue pour que nous la citions en intégralité. Néanmoins, certaines démarches détaillées dans ce chapitre vous permettront de vous assurer de la compatibilité de votre matériel et, le cas échéant, de pouvoir configurer certains des périphériques non reconnus.

Clause de non-responsabilité légale : la liste de matériel agréé par Mandriva Linux contient des informations à propos des périphériques matériel qui ont été testés ou ont été signalés comme fonctionnant correctement sous Mandriva Linux. Du fait de la grande variété des configurations, Mandriva ne peut pas garantir qu'un périphérique spécifique fonctionnera correctement sous votre système.

Chapitre 1. Les différentes méthodes d'installation

1.1. Avant l'installation

Vous allez installer Mandriva Enterprise Server 5. Voici quelques conseils avant de démarrer et quelques pistes à explorer en cas de difficulté au début de l'installation.

Si l'installation se fait sur une nouvelle plate-forme, il est important de s'assurer de la bonne reconnaissance par la distribution. Vous disposez à cet effet de bases de données consultables en ligne qui peuvent vous aider à faire votre choix :

- Les fiches de certification officielles (`http://www.mandriva.com/hardware`) : ensemble des matériels certifiés officiellement par Mandriva
- base communautaire (`http://hcl.mandriva.com`) : base hardware communautaire constituée des informations collectées auprès des utilisateurs de la distribution.

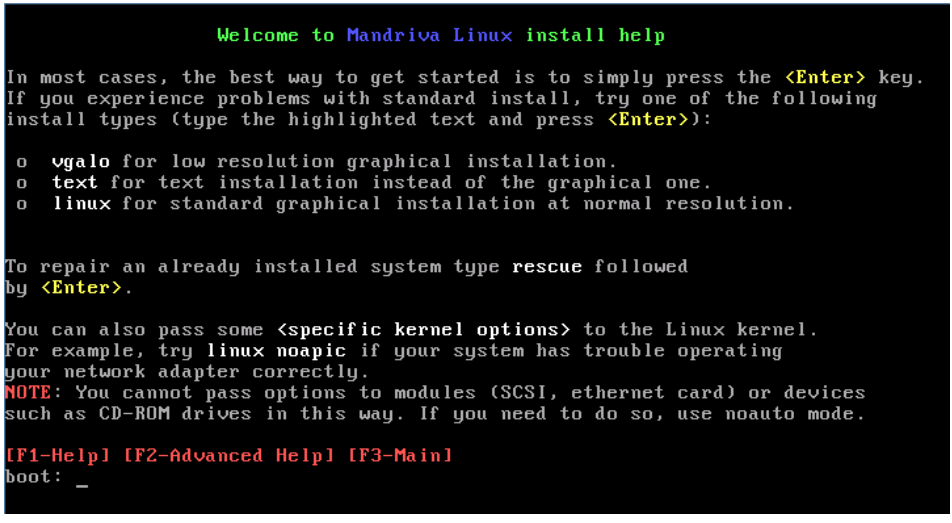
Afin d'assurer une installation complète et sans embûches, vérifiez que tous vos périphériques soient bien branchés et sous tension. DrakX détectera et configurera automatiquement tous les appareils ainsi reliés à votre serveur lors de l'installation de Mandriva Linux

Vous allez pouvoir choisir différents types d'installation de Mandriva Enterprise Server 5 : en local (au moyen de CD ou DVD), par le réseau (PXE, FTP, HTTP). Quel que soit le moyen utilisé, c'est DrakX, l'installeur graphique de Mandriva qui va vous guider dans cette procédure d'installation.

1.2. Installation via CD/DVD

Insérez le CD/DVD Mandriva Enterprise Server 5 dans le lecteur CD/DVD de votre serveur. Démarrez celui-ci. Si le démarrage s'est bien effectué sur le support amovible, l'écran ci-après apparaît. Sinon, modifier la séquence de démarrage définie dans le BIOS afin de définir le lecteur CD/DVD prioritaire (voir le manuel de votre matériel).

Le lancement de l'installation se fait par défaut en mode graphique. Toutefois, vous pouvez passer en installation en mode texte. Tapez alors `Esc` avant le chargement de l'interface graphique.



L'écran vous propose alors une interface en mode texte et la possibilité de définir des options spécifiques de démarrage. Listons les plus utilisés :

- `vgalo` : si vous avez essayé une installation normale et qu'il vous a été impossible de voir l'interface graphique, vous pouvez essayer d'utiliser une résolution d'écran plus basse. Cela peut arriver avec certaines cartes graphiques, de sorte que Mandriva Linux vous donne la possibilité de contourner ce problème dû le plus souvent à des cartes obsolètes. Pour essayer l'installation en basse résolution, tapez vgalo à l'invite de commande.
- `text` : si vous utilisez une très vieille carte vidéo et que l'installation en mode graphique refuse de démarrer, le mode texte vous permettra de poursuivre l'installation.
- Le mode `noauto` : dans certains cas isolés, la détection du matériel peut bloquer le démarrage. Si cela arrive, vous pouvez ajouter le mot `noauto` comme paramètre pour que l'installation ne lance pas de détection matériel. Mais sachez que vous devrez alors fournir l'ensemble des paramètres de votre matériel manuellement. Le paramètre noauto peut être utilisé conjointement aux modes précédents, vous pouvez donc spécifier `vgalo noauto` pour lancer une installation en basse résolution sans détection automatique du matériel.
- options du noyau : la grande majorité des machines n'ont pas besoin d'options spécifiques sur le noyau. Cependant du fait d'erreurs de conception ou de BIOS défectueux, certaines cartes mères ne reconnaissent pas correctement la quantité de mémoire installée. Si vous devez spécifier manuellement la quantité de RAM installée, utilisez l'option mem=xxxxM. Par exemple, pour démarrer une installation en mode standard sur un PC ayant 512 Mo de mémoire vive, entrez la commande Linux `mem=512M`. Vous pouvez également utiliser des paramètres comme `noapic`, `nolapic` pour gérer les problèmes liés aux interruptions ou aux modes de communication du processeur.

Durant l'installation, vous allez avoir la possibilité de basculer en mode console, vous donnant ainsi l'accès aux logs système détaillés, mais aussi à un environnement shell. Dans cet environnement, outre les commandes traditionnelles, vous avez à votre disposition la commande `bug` qui permet de sauvegarder sur un support amovible un ensemble de logs et d'informations système fort utiles en cas de nécessité de dépannage.

1.3. Installer via PXE

Ce chapitre décrit les étapes nécessaires pour installer votre Mandriva Enterprise Server 5 en utilisant PXE (*Pre-boot eXecution Environment*). Vous verrez

comment configurer les parties serveur et client.

1.3.1. Qu'est-ce que PXE ?

PXE est un protocole développé par Intel permettant aux ordinateurs de démarrer à partir d'un réseau. PXE est conservé dans la mémoire ROM des cartes réseau récentes. Au moment du démarrage, le BIOS charge la mémoire ROM PXE et l'exécute. À partir du menu proposé, choisissez une entrée et l'ordinateur démarrera sur le système d'exploitation disponible sur le réseau.

PXE est implémenté par les fabricants de cartes réseau selon la spécification d'Intel. Le diagramme suivant illustre le fonctionnement de PXE utilisant un serveur DHCP et un serveur TFTP.

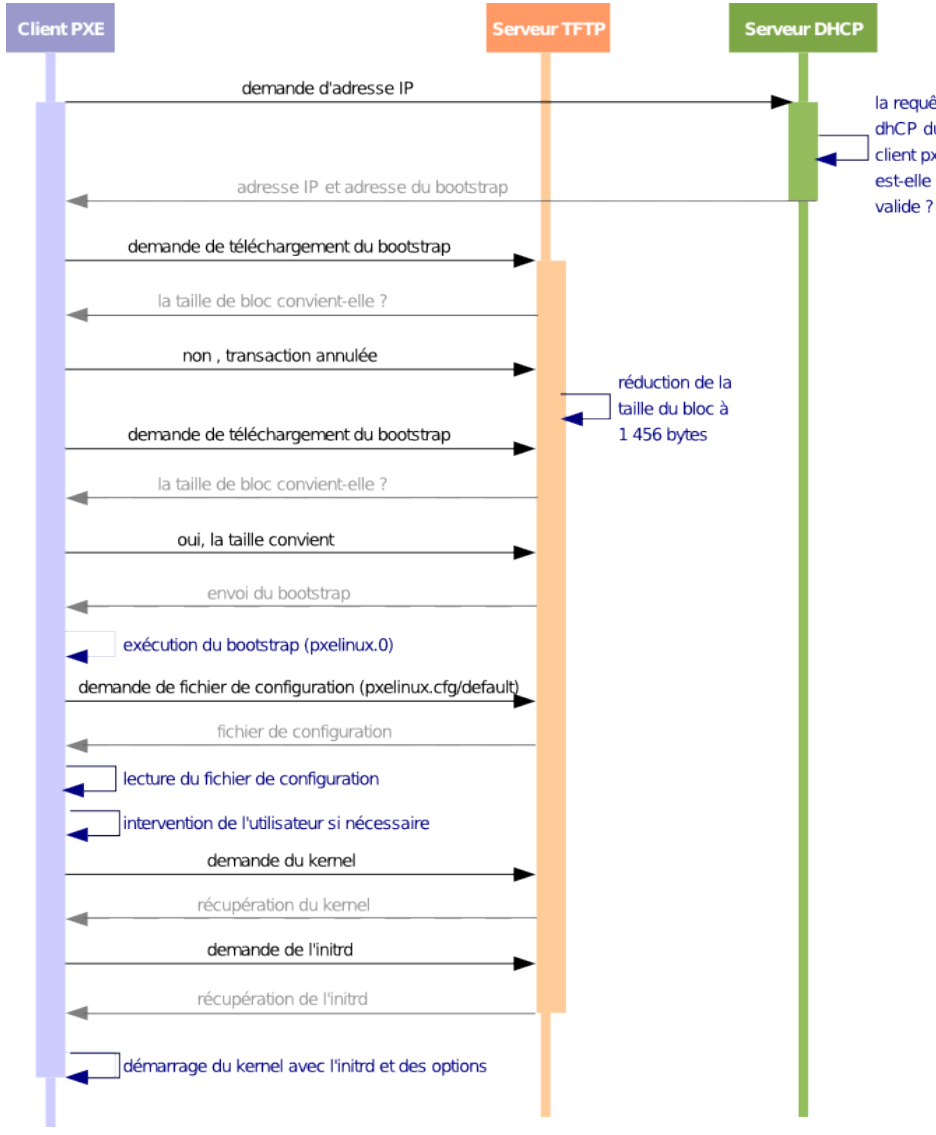


Figure 1-1. Fonctionnement de PXE

PXE suit trois étapes pour le démarrage :

- Obtention d'une adresse IP du serveur DHCP
- Télécharger une amorce (*bootstrap*) sur le serveur TFTP.
- Exécution de l'amorce.

1.3.2. Utiliser PXE pour installer Mandriva Enterprise Server 5

L'utilisation de PXE est relativement simple. Suivez ces étapes :

Vérification de votre matériel

Vérifiez d'abord si votre matériel supporte PXE. Il n'y a pas de façon universelle pour répondre à cette question. En théorie, la documentation de votre carte réseau ou celle de votre carte maîtresse devrait vous informer à ce chapitre. Vous pouvez également vérifier les paramètres de votre BIOS, particulièrement pour une carte réseau sur la carte mère. Vous pourrez alors activer ou désactiver une « option ROM » pour du matériel réseau (la formulation exacte risque de varier selon les BIOS). Enfin, vérifiez également l'ordre de démarrage (*boot order*) afin que le démarrage réseau précède le démarrage sur le disque.

Les ordinateurs récents vous proposent le démarrage réseau simplement en appuyant sur la touche F12 au démarrage.

Démarrer votre système

Si votre serveur est bien configuré, durant le démarrage, vous devriez voir les 3 étapes présentées précédemment. Vous verrez alors `boot:`. Entrez le nom du système que vous voulez démarrer, et c'est tout.

1.3.3. Configurer votre serveur PXE

Préparer les fonctionnalités de PXE :

- serveur DHCP
- serveur TFTP
- amorce PXElinux
- serveur NFS ou HTTP, nous suggérons NFS.

1.3.3.1. Configuration du serveur DHCP

Ce serveur répond à une requête DHCP spéciale du client PXE, selon la classe du client PXE. Le répertoire du fichier de log variera selon la configuration du serveur. Vous pourrez les trouver dans `/var/log/messages`. Le fichier de configuration par défaut est sauvegardé dans le répertoire `/etc`.

1.3.3.1.1. Options de dhcpd.conf

Voici les options que vous devez configurer :

Permettre le démarrage (*Allow booting*)

> L'option de démarrage indique si le DHCP répond ou non a une requête d'un client particulier. Ce mot clé a de l'importance seulement lorsqu'il apparaît dans la configuration client. Par défaut, le démarrage est permis. S'il est désactivé pour un client particulier, celui-ci ne pourra pas obtenir d'adresse du serveur DHCP.

Non autoritaire

> Si le serveur n'est pas valide pour un segment, il enverra un message `DHCPNACK`. C'est un paramètre important si vous avez d'autres serveurs DHCP. Si vous installez un serveur PXE dans un réseau qui a déjà un serveur DHCP, l'activation de cette option vous assurera que les réponses DHCP seront toujours considérées après celle du serveur autoritaire. Cette option est généralement utilisée avec un bassin (*pool*, voir plus bas) restreint de configuration PXE.

Pool

> Cette section de `/etc/dhcpd.conf` définit un bassin contenant une plage d'adresses IP. Dans notre exemple, le serveur DHCP accepte les membres de la classe PXE et refuse les membres des autres classes. L'exemple de configuration (voir plus bas) restreint le bassin d'adresses aux clients PXE. Ceci vous assure que votre serveur DHCP ne répondra pas aux demandes courantes pour le DHCP. Vous pourrez ainsi installer un serveur PXE sans entrer en conflit avec le serveur DHCP autoritaire. Si vous voulez répondre aux demandes DHCP et PXE, vous avez simplement à commenter la ligne « Allow member of PXE ».

Afin de fonctionner adéquatement, le serveur de démarrage de PXE nécessite également des options spécifiques pour le serveur DHCP :

Classe

> Dans notre exemple, nous allons créer une classe PXE pour établir des options spécifiques.

Option vendor-class-identifier

Si l'option `vendor-class-identifier` de la requête DHCP équivaut à PXEclient, cette classe est compatible.

Vendor-option-space

Cette option est définie pour permettre des options spécifiques à la classe.

Filename

L'option `filename` détermine l'amorce client à récupérer. Le serveur TFTP est en mode chroot, donc seulement le chemin est relatif au répertoire de chroot. Habituellement, le fichier représente l'amorce PXElinux. Il est fréquemment nommé « linux.0 » ou « pxelinux.0 ».

Next-server

Elle définit l'IP de votre serveur TFTP qui peut stocker l'amorce et sa configuration.

Définir vendor_class_identifier

Définis le champ vendor-class-identifier à PXEclient dans la réponse du DHCP. Si ce champ n'est pas défini, le client PXE ignorera la réponse.

1.3.3.1.2. Exemple de fichier `dhcpd.conf`

```
ddns-update-style ad-hoc;
allow booting;
allow bootp;
not authoritative;

 # Definition of PXE-specific options
option space PXE;
option PXE.mtftp-ip code 1 = ip-address;
option PXE.mtftp-cport code 2 = unsigned integer 16;
option PXE.mtftp-sport code 3 = unsigned integer 16;
option PXE.mtftp-tmout code 4 = unsigned integer 8;
option PXE.mtftp-delay code 5 = unsigned integer 8;
option PXE.discovery-control code 6 = unsigned integer 8;
option PXE.discovery-mcast-addr code 7 = ip-address;

class "PXE" {
match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
#filename "/PXEClient/pxegrub";
filename "/PXEClient/pxelinux.0";
option vendor-class-identifier "PXEClient";
vendor-option-space PXE;
option PXE.mtftp-ip 0.0.0.0;
next-server 192.168.200.1;
}
```

```
class "known" {
match hardware;
one-lease-per-client on;
ddns-updates on;
ddns-domainname = "mandriva.com";
ddns-hostname = pick-first-value(ddns-hostname, option host-name);
option fqdn.no-client-update on;
set vendor_class_identifier = option vendor-class-identifier;
}

shared-network "mynetwork" {
subnet 192.168.200.0 netmask 255.255.255.0 {
option subnet-mask 255.255.255.0;
option routers 192.168.200.1;
default-lease-time 28800;
max-lease-time 86400;

pool {
range 192.168.200.1 192.168.200.192;
allow members of "PXE";
}

}
}
```

1.3.3.2. Configuration du serveur TFTP

Le serveur TFTP contient les fichiers d'amorce et de configuration. Le serveur TFTP est lancé au démarrage par le démon xinetd. Habituellement, l'installation RPM par défaut fonctionne sans changement, sauf que ce service n'est pas activé par défaut. Comme TFTP est gérer par xinetd, vous devez spécifier à xinetd d'ouvrir un port dédié. La configuration de xinetd pour TFTP est située dans `/etc/xinetd.d/tftp`. Ouvrez ce fichier, changez `disable=yes` par `disable=no`. Enfin, redémarrez xinetd pour que les changements soient pris en compte : `servicexinetdrestart`.

1.3.3.3. Configuration de PXElinux

PXElinux est l'amorce de PXE. Cette amorce est téléchargée par le ROM PXE du client et exécutée localement. Le but de l'amorce PXE est de retourner une interface minimale permettant de choisir le système que vous voulez démarrer. PXElinux est un projet de SYSLINUX. L'amorce est fréquemment nommée « pxelinux.0 » ou « linux.0 ». Voici ses principales fonctionnalités :

- Vous pouvez définir un fichier de configuration pour chaque adresse IP de client PXE
- La répertoire racine de TFTP contient pxelinux.0
- Est conforme aux demandes du vendor-class-identifier
- Démarre une image disque (ex. : image floppy)

1.3.3.3.1. Arbre PXElinux

```
/var/lib/tftpboot
   |-- X86PC
 |-- linux
  |-- help.txt
  |-- images
  |   |-- 2009.0
  |       |-- all.rdz
  |       `-- vmlinuz
  |-- linux.0
  |-- memdisk
  |-- messages
  |-- pxelinux.cfg
       |-- default
```

Tous les fichiers de configuration sont stockés dans le répertoire `/X86PC/linux/` du serveur TFTP :`/var/lib/tftpboot`. Vous pouvez créer un sous-répertoire contenant l'ensemble des fichiers requis par le client PXE. Le client est stocké dans `/var/lib/tftpboot/X86PC/linux` (PXEPATH). Donc, votre `linux.0` devrait être dans `PXEPATH` et activé dans votre fichier de configuration DHCP. Créez ensuite un répertoire `pxelinux.cfg` dans `PXEPATH` (CFGPATH).

Le répertoire de configuration contient tous les fichiers de configuration (un par adresse IP de client PXE) ou un fichier de configuration « par défaut ». Pour nommer vos fichiers, convertissez les adresses IP en format hexadécimal : `192.168.200.1` vous donnera le nom « C0A8C801 » pour votre fichier de configuration (CFGFILE). Ce fichier contient des options pour le client PXE afin qu'il passe sa requête avec son adresse IP `192.168.200.1`. Vous pouvez utiliser le script `gethostip` pour faire cette conversion.

Dans PXEPATH, créez un répertoire `images` avec un sous-répertoire pour chaque système d'exploitation (ex. : `linux` pour une image Linux ou un noyau et son fichier `initrd`). Chaque fichier contient une image d'amorce ou un noyau et un fichier `initrd`, ainsi qu'un fichier d'aide.

1.3.3.3.2. Configurer PXElinux dans pxelinux.cfg

Le client PXE télécharge l'amorce (`linux.0` dans notre exemple), l'exécute localement et tente ensuite de télécharger son fichier de configuration CFGFILE. Ce fichier contient des options générales et les définitions des images de démarrage. En voici les options principales :

`DEFAULTkerneloptions(optionspardéfautdunoyau)`

Règle la ligne de commande par défaut. Si PXELINUX démarre automatiquement, il prendra en charge les paramètres après `DEFAULT` comme s'ils avaient été entrés à l'invite de commande `boot`, en ajoutant l'option `auto`, indiquant le démarrage automatique.

`DISPLAYnomdefichier`

Affiche le fichier indiqué au démarrage, avant l'invite de commande `boot`.

`TIMEOUTdurée`

Indique combien de temps attendre avant le démarrage. Cette durée est annulée dès que l'usager entre une donnée (n'importe laquelle), la présomption étant que celui-ci complétera sa commande. Un `TIMEOUT` de zéro désactive l'attente complètement. Il s'agit de la valeur par défaut.

`F[1-9]fichier`

Si l'usager appuie sur `F[1-9]`, le fichier est affiché avant de retourner à l'invite de commande. Il s'agit d'une manière simple de fournir de l'aide à propos des images fournies sur le serveur.

Après avoir configuré les options générales du noyau, nous devons maintenant définir les images fournies par le serveur PXE. Chaque image définie débute par l'option `label`. Elle contient une chaîne de caractères qui peut être entrée au démarrage. Voyons d'abord une image spécifique permettant de démarrer un système localement en forçant le client PXE à quitter.

```
label local
     LOCALBOOT 0
```

La syntaxe générale est `LOCALBOOTtype`. Cela exécute un démarrage de disque local au lieu de démarrer un noyau. L'argument **0** signifie de lancer un démarrage normal sur la prochaine amorce. L'argument **4** lancera un démarrage avec le pilote *Universal Network Driver Interface* (UNDI) toujours présent en mémoire. Finalement, l'argument **5** lancera un démarrage local avec l'ensemble de la pile (*stack*) PXE, incluant le pilote UNDI, toujours présent en mémoire. Toutes les autres valeurs ne sont pas définies. Si vous ne savez pas

ce que sont UNDI ou la pile PXE, ne vous inquiétez pas, vous n'en avez donc pas besoin : spécifiez **0**.

```
label label
     KERNEL image
     APPEND options...
```

Si `label` est entré au démarrage du noyau, PXE devra démarrer `image`, et l'option `APPEND` sera utilisée au lieu de celles spécifiées dans la section globale du fichier.

PXE peut également vous permettre de démarrer le noyau directement. Le client PXE télécharge (avec TFTP) le noyau à partir du chemin spécifié dans `KERNEL`, puis il télécharge `initrd` de l'adresse spécifiée dans l'option `APPENDinitrd=`.

Puis, le client PXE exécute le noyau avec le `initrd` et l'option passée par `APPEND`.

1.3.3.3.3. Utilisez PXE pour tester la mémoire

Si vous avez des problèmes à installer ou à démarrer un serveur, il peut être pertinent de vérifier la mémoire principale. PXE peut vous aider en fournissant cette fonctionnalité.

Obtenez les binaires pour memtest en installant le paquetage `memtest86+` :

```
# urpmi memtest86+
```

Copiez ensuite le binaire dans l'arborescence de PXElinux :

```
# cp /boot/memtest.bin /var/lib/tftpboot/X86PC/linux/images/memtest
```

Ajoutez finalement une nouvelle entrée dans la configuration de PXElinux :

```
label memtest kernel
     images/memtest
```

C'est tout! Vous avez simplement à démarrer votre ordinateur pour tester sur un périphérique réseau et à entrer `memtest` à l'invite de commande `linux`.

1.3.3.3.4. Exemple de fichier de configuration

Ce fichier doit être conservé dans `CFGPATH` et nommé comme un fichier `CFGFILE` (ex. : /var/lib/tftpboot/X86PC/linux/pxelinux.cfg/default)

```
PROMPT 1
DEFAULT local
```

```
DISPLAY messages
TIMEOUT 50

label local
LOCALBOOT 0

label linux
KERNEL memdisk
APPEND initrd=images/linux/network.img

label memtest
KERNEL images/memtest

label autoinstall
KERNEL images/autoinstall/vmlinuz
APPEND initrd=images/autoinstall/network.rdz ramdisk=32000 vga=788
kickstart=Mandrake/base/auto_inst.cfg.pl useless_thing_accepted
automatic=method:nfs,network:dhcp,interface:eth0,dns:192.168.100.11,
server:192.168.200.1,directory:/install root=/dev/ram3

F1 images/local/help.txt
F2 images/autoinstall/help.txt
```

Chapitre 2. Principales étapes de l'installation

2.1. Choix de la langue

La première étape consiste à choisir votre langue.

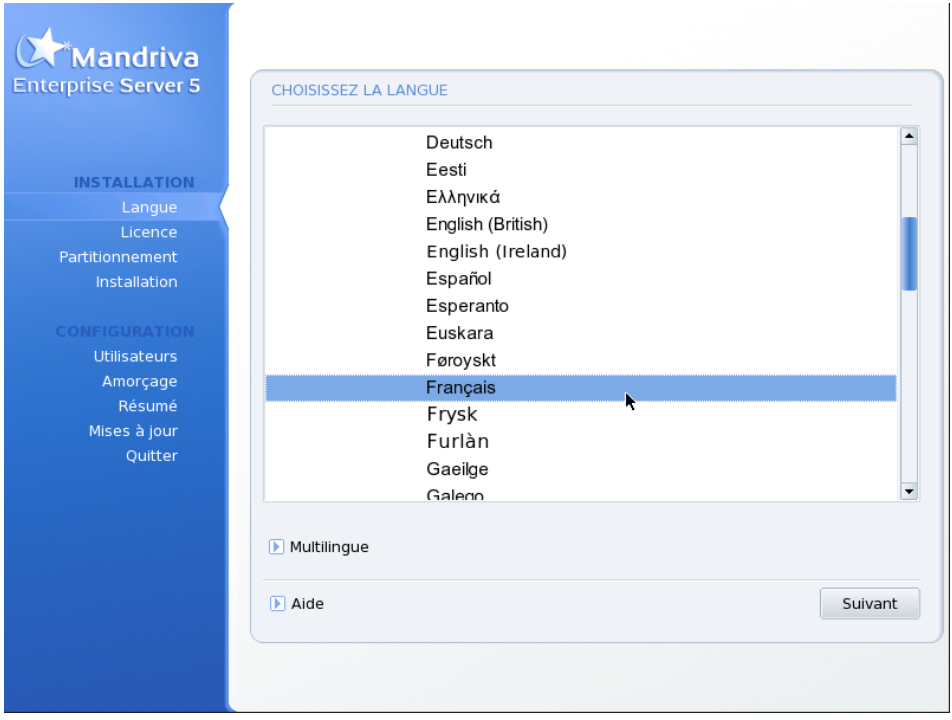


Figure 2-1. Choix de la langue par défaut

Premièrement, ouvrez l'arborescence relative au continent sur lequel vous habitez, puis choisissez votre langue. Le choix de la langue sera appliqué au programme d'installation, à la documentation et au système en général.

Utilisez la liste accessible par le bouton Multi languages pour choisir d'autres langues à installer sur votre poste. Ainsi, vous installerez toute la documentation et les applications nécessaires à l'utilisation de ces langues.

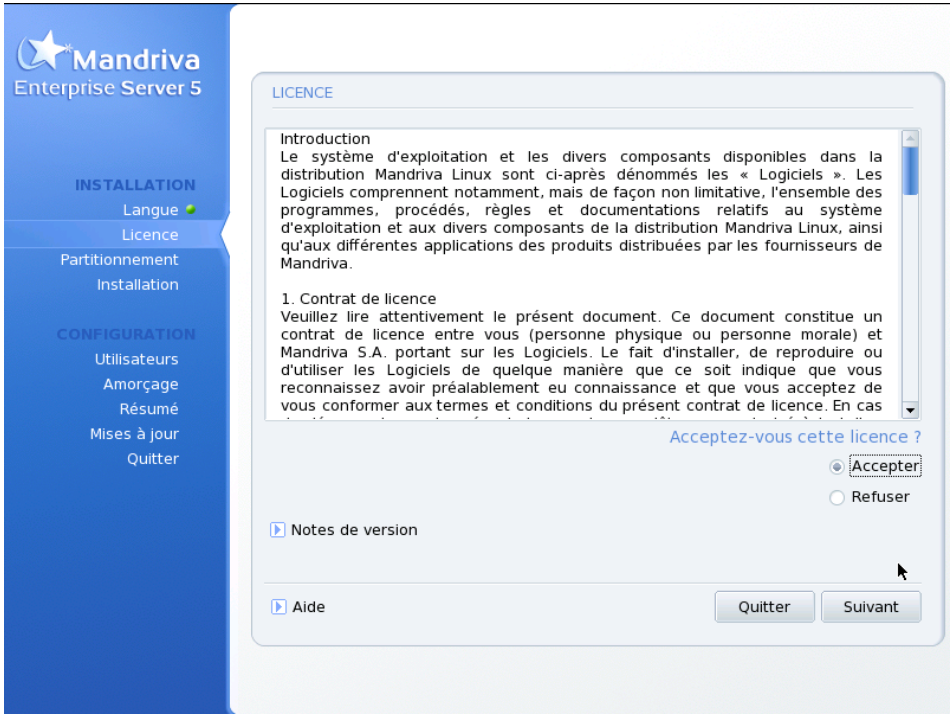
À propos de l'encodage UTF-8 (unicode) : Unicode est un système d'encodage des caractères censé couvrir toutes les langues existantes. Cependant, son intégration dans GNU/Linux est encore imparfaite. Pour cette raison, Mandriva Linux l'utilisera ou non selon les critères suivants :

1. Si vous choisissez une langue avec un encodage ayant une longue histoire (langues associées au `latin1`, russe, japonais, chinois, coréen, thaï, grec, turc, et la plupart des langues `iso-8859-2`), l'encodage historique sera utilisé.
2. Les autres langues entraîneront l'utilisation d'Unicode par défaut.
3. Si vous demandez l'installation de plus d'une langue, et que ces langues n'utilisent pas le même encodage, alors Unicode sera utilisé pour tout le système.
4. Enfin, Unicode peut aussi être utilisé quel que soit votre configuration des langues à utiliser, en sélectionnant l'option Utiliser Unicode par défaut.

Remarquez que vous n'êtes pas limité à une langue supplémentaire. Vous pouvez en choisir plusieurs, ou même les installer toutes en choisissant Toutes les langues. Choisir le support pour une langue signifie ajouter les traductions, les polices, correcteurs orthographiques, etc. Installez **maintenant** toutes les langues qui pourraient vous être utiles dans le futur. Il sera en effet difficile d'installer leur support par la suite, en dehors de l'installation initiale du système.

Pour passer d'une langue à l'autre, vous pouvez lancer l'utilitaire `localedrake` en tant que `root` pour changer la langue utilisée dans tout le système : connectez-vous en simple utilisateur pour ne changer que la langue de cet utilisateur.

2.2. Licence de la distribution

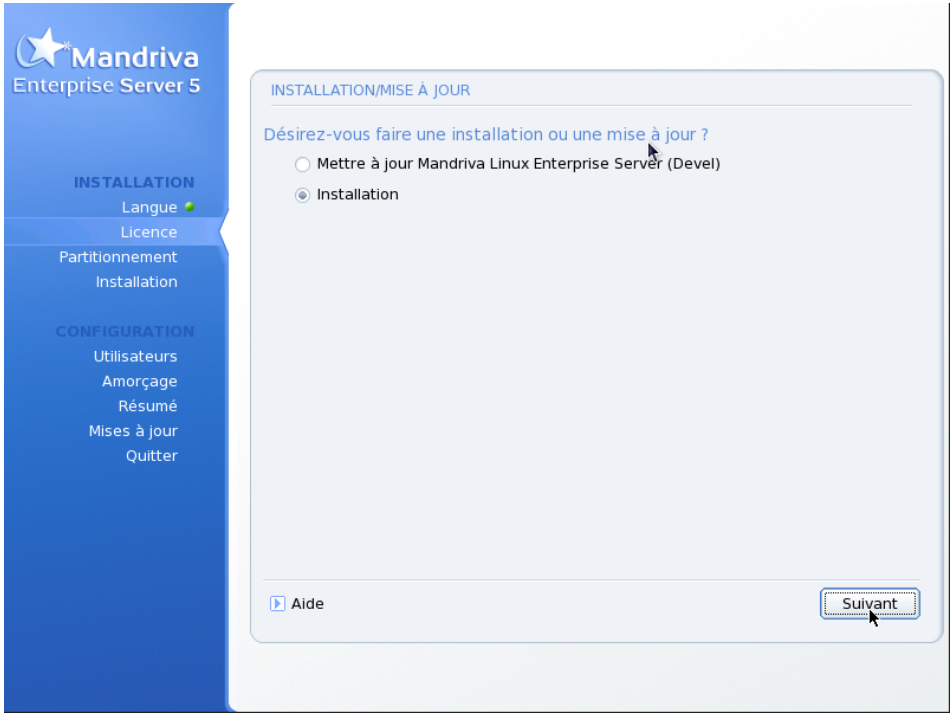


Avant d'aller plus loin, nous vous recommandons de lire attentivement les termes et conditions d'utilisation de la licence. Celle-ci régit l'ensemble de la distribution Mandriva Linux. Si vous en acceptez tous les termes, cochez la case Accepter puis cliquez sur Suivant. Sinon, cliquez sur le bouton Quitter pour redémarrer votre ordinateur.

Si vous êtes curieux des évolutions techniques effectuées depuis la dernière version, cliquez sur les Notes de version.

2.3. Classe d'installation

Cette étape s'affiche uniquement si une partition GNU/Linux préexistante est détectée sur votre machine.



DrakX doit maintenant savoir si vous désirez lancer une Installation ou une Mise à jour d'un système Mandriva Linux déjà installé :

Mise à jour

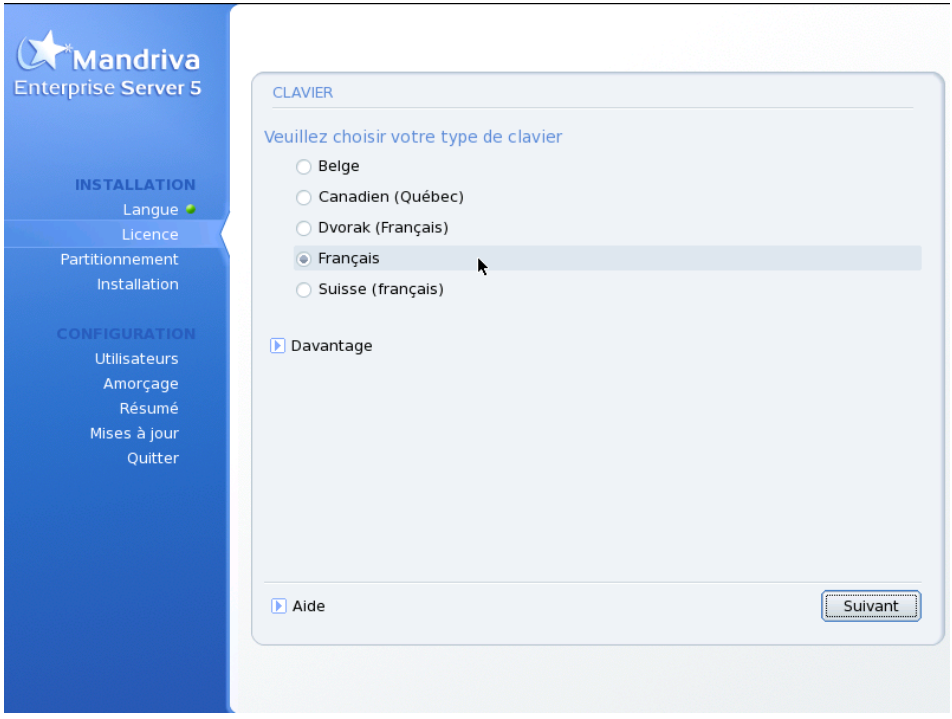
Cette classe d'installation vous permet uniquement de mettre à jour les paquetages qui composent votre système Mandriva Linux. Elle conserve les partitions existantes ainsi que la configuration des utilisateurs. La plupart des autres étapes d'une installation classique sont accessibles.

Installation

Cette option revient pratiquement à écraser l'ancien système. Cependant, selon votre table de partitions, vous pouvez éviter l'effacement de vos données existantes (notamment les répertoires `/home`).

2.4. Configuration du clavier

Votre clavier est automatiquement configuré en fonction de la langue que vous avez choisie. Si cette dernière propose plusieurs configurations possibles de clavier, vous devrez alors sélectionner la vôtre.



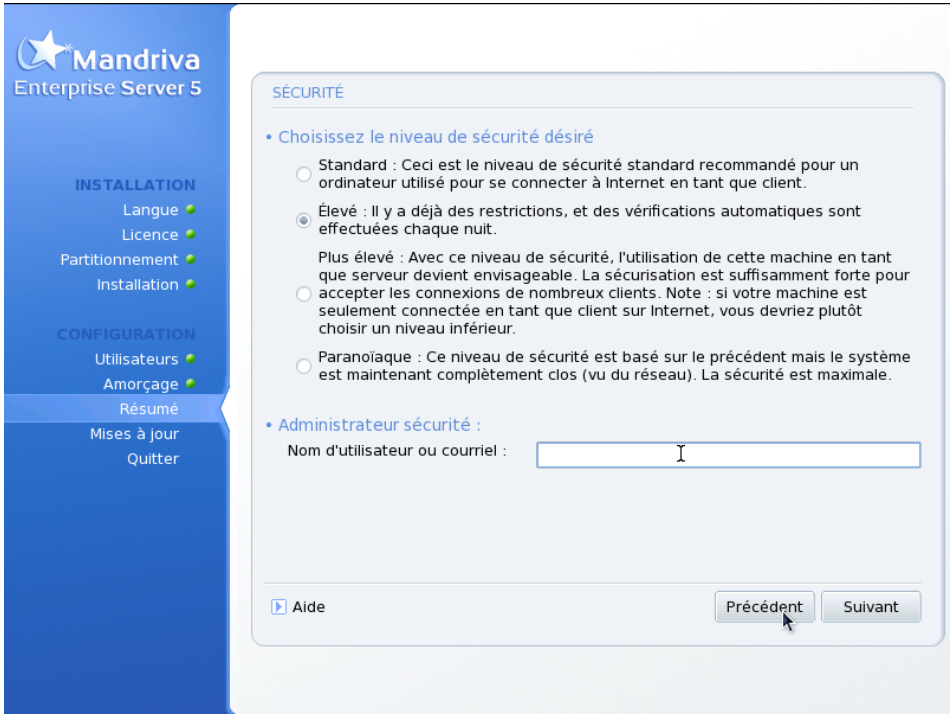
Selon la langue principale que vous avez choisie (Section 2.1), DrakX sélectionne le clavier approprié. Vérifiez que cela correspond à votre configuration de clavier ou choisissez-en une autre dans la liste.

Cela dit, il est possible que vous ayez un clavier ne correspondant pas exactement à votre langue d'utilisation. Par exemple, si vous habitez le Québec et parlez le français et l'anglais, vous pouvez vous trouver dans la situation où votre langue et votre configuration de clavier ne sont pas les mêmes. Dans ces cas, cette étape vous permet de sélectionner un autre clavier à partir de la liste.

Cliquez sur Davantage pour voir toutes les options proposées.

Si vous choisissez un clavier basé sur un alphabet **non latin**, il vous sera demandé de choisir la combinaison de touches permettant d'alterner entre les configurations de clavier au prochain écran.

2.5. Niveau de sécurité

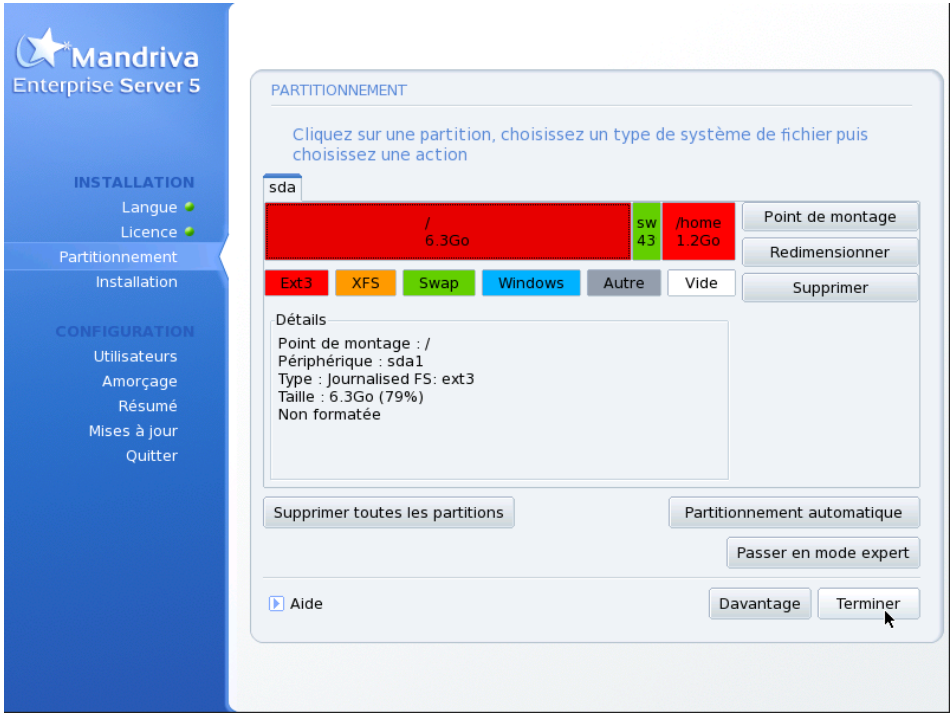


À cette étape, DrakX vous permet de choisir le niveau de sécurité requis pour votre système. Il se détermine en fonction de l'exposition du système à d'autres utilisateurs (s'il est connecté directement sur Internet, par exemple) et selon le niveau de sensibilité de l'information contenue dans le système. Sachez toutefois que plus la sécurité d'un système est élevée, plus il est complexe à utiliser.

Si vous ne savez pas quel niveau choisir, gardez la sélection par défaut. Vous pouvez le modifier ultérieurement avec draksec, qui se trouve dans le Centre de contrôle Mandriva Linux.

Remplissez le champ Administrateur sécurité avec l'adresse de courrier électronique du responsable de la sécurité. Les messages de sécurité lui seront adressés.

2.6. Création des partitions



Vous devez maintenant décider où installer Mandriva Linux sur votre disque dur. Partitionner un disque consiste à y effectuer des divisions logiques et, dans le cas qui nous concerne, créer l'espace requis pour l'installation de votre nouveau système Mandriva Linux.

Comme les effets du partitionnement sont irréversibles (l'ensemble du disque est effacé), cette étape est généralement intimidante et stressante pour un utilisateur inexpérimenté. Heureusement, un assistant a été prévu à cet effet. Avant de commencer, lisez la suite de ce document et surtout, prenez votre temps.

Selon la configuration de votre disque, plusieurs options sont disponibles :

Utiliser l'espace disponible

Cette option tentera simplement de partitionner automatiquement l'espace inutilisé de votre disque. Il n'y aura pas d'autre question.

Utiliser les partitions existantes

L'assistant a détecté une ou plusieurs partitions Linux existantes sur votre disque dur. Si vous voulez les utiliser, choisissez cette option. Il vous sera

alors demandé de choisir les points de montage associés à chacune des partitions. Les anciens points de montage sont sélectionnés par défaut, et vous devriez généralement les garder. DrakX vous demandera aussi quelles partitions doivent être formatées ou conservées.

Effacer tout le disque

Si vous voulez effacer toutes les données et les partitions présentes sur votre disque, choisissez cette option. Soyez prudent, car ce choix est irréversible.

En choisissant cette option, **l'ensemble** du contenu de votre disque sera détruit.

Partitionnement personnalisé

Permet de partitionner manuellement votre disque. Soyez prudent, car bien que plus évoluée, cette option est dangereuse. Vous pouvez facilement perdre l'ensemble du contenu d'un disque. C'est pourquoi cette option n'est recommandée que si vous possédez des connaissances sur la notion de partitionnement.

Par défaut, Mandriva Enterprise Server 5 ajoute le support des Listes de contrôle d'accès avancées (ACL) pour gérer les droits des usagers sur les partitions ext3.

2.6.1. Utilisation des fonctionnalités avancées de DiskDrake

DiskDrake vous permet de créer des partitions selon vos besoins précis.

2.6.1.1. L'interface

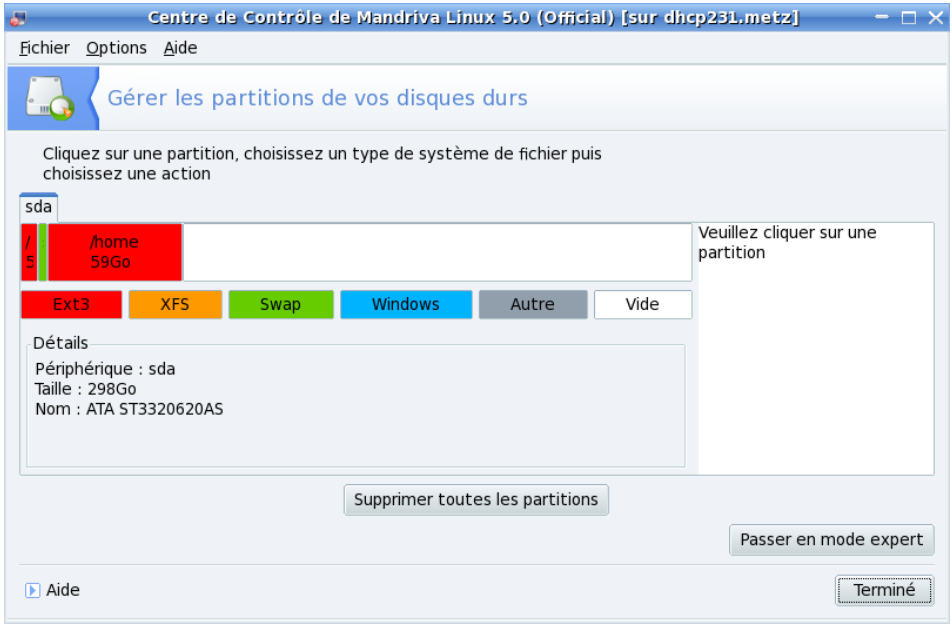


Figure 2-2. Menu principal de DiskDrake

DiskDrake permet de configurer chaque disque physique sur votre serveur. Si vous avez seulement un disque IDE, vous verrez seulement un onglet nommée sda sous Types de système de fichier. Si vous avez plus d'un disque, chaque disque aura son propre onglet et celui-ci sera nommé en fonction du nom alloué par le noyau pour ce disque. DiskDrake vous permet de gérer le partitionnement de chaque disque.

La fenêtre principale (consultez Figure 2-2) se divise en quatre zones :

- En haut se trouve la structure de votre disque dur. Au démarrage de DiskDrake, la structure actuelle de votre disque sera affichée. DiskDrake rafraîchira cet affichage en fonction des changements que vous appliquerez.
- À gauche. Un menu relatif à la partition sélectionnée dans la structure précédente.
- À droite. Une description des partitions sélectionnées.
- En bas. Les boutons pour effectuer les actions générales. Consultez la section suivante.

2.6.1.2. Les boutons d'action de DiskDrake

Supprimer toutes les partitions

En cliquant sur ce bouton, vous effacerez toutes les partitions existantes sur le disque sélectionné.

Davantage

Affiche une petite fenêtre proposant trois boutons pour :

Sauvegarder la table des partitions. Permet de faire une copie de sauvegarde de la table des partitions actuelle dans un fichier sur un disque (disquette en général). Cela peut être utile en cas de problème (notamment une erreur lors du repartitionnement).

Charger une table des partitions. Permet de récupérer une table de partitions sauvegardée à l'aide de l'option précédente. La récupération de la table des partitions peut vous permettre de récupérer vos données perdues dans la mesure où vous n'avez pas reformaté les partitions, car le processus de formatage détruit les données.

Deviner automatiquement la table des partitions. Si vous avez perdu votre table des partitions et n'avez pas de sauvegarde, cette fonction parcourt votre disque pour essayer de reconstruire une table de partitions.

Aide

Affiche cette documentation dans la fenêtre d'un navigateur.

État précédent

Annule la dernière action. La plupart des modifications faites sur vos partitions ne sont rendues effectives que lorsque DiskDrake vous en avertit. Ce bouton vous permet donc d'annuler vos modifications sur les partitions jusqu'à la dernière écriture de la table.

Passer en mode expert

Ce bouton permet d'avoir accès aux fonctions du mode expert. Elles peuvent s'avérer dangereuses pour l'utilisateur novice.

Terminer

Enregistre les changements et met fin à l'utilisation de DiskDrake.

2.6.2. Utilisation de la gestion dynamique des partitions

Voici un exemple concret d'utilisation de DiskDrake pour obtenir la liste des partitions de votre machine. Votre serveur est destiné à devenir un serveur de fichiers. En conséquence, il doit avoir beaucoup d'espace disponible afin de pouvoir augmenter la taille des partitions lorsque l'une d'elle est complètement utilisée :

- Gestion dynamique des partitions : nous allons utiliser `LVM` (*Logical Volume Manager*). Si le système de fichier le permet, ceci vous donne la possibilité de redimensionner des partitions à la volée, fournissant ainsi un système de fichiers sans limites physiques.
- Listes de contrôle d'accès (ACL) avancées pour gérer les droits des usagers : nous avons besoin de droits supplémentaires comme sur des systèmes de fichiers Windows®. Le système de fichier `XFS` permet d'accroître sa dimension à la volée.
- Informations diverses : l'espace disque total sera de 350 Go, en utilisant 2 disques. Ce système de fichier sera monté sur la partition `/data`.

Dans DiskDrake, choisissez Partitionnement personnalisé. Supposons que vous avez déjà créé vos partitions système. Au bas de l'écran, cliquez sur Passer en mode expert. Suivez les étapes suivantes pour obtenir les partitions désirées :

1. Obtenir de l'espace du disque système.

   Nous avons 50 Go disponibles sur le disque système. Cliquez dessus puis sur Créer. Choisissez la taille afin de pouvoir utiliser tout l'espace disponible. Puis, dans la liste de type de système de fichiers, choisissez Linux Logical Volume Manager. Après avoir validé votre sélection, vous êtes retourné au menu principal. Gardez votre partition sélectionnée et cliquez sur Add to LVM. Dans le champ LVM name field, entrez le nom de cette partition virtuelle. Nommons-la `data`. Vous devriez maintenant voir un onglet nommé data.

2. Ajout d'espace à partir d'un second disque

   Utilisons maintenant le second disque pour ajouter de l'espace disponible. Cliquez l'onglet correspondant, puis sur espace disponible. Cliquez sur Créer et choisissez tout l'espace disque. Dans la liste de Type de système de fichiers, sélectionnez Linux Logical Volume Manager. De retour au menu principal, cliquez sur Add to LVM une seconde fois. L'écran suivant vous proposera 2 items : data étant le premier groupe créé, et new. Comme nous voulons augmenter la taille de la partition data, sélectionnez-la. Vous pouvez vérifier que cette opération est complétée : cliquez sur l'onglet data. La taille du volume devrait maintenant être augmentée.

3. Création d'une partition virtuelle et d'un système de fichier

Maintenant que votre volume global est prêt, vous devez y créer des partitions logiques à l'intérieur. Dans l'onglet data, cliquez sur l'espace disponible, puis sur Créer. Nous utiliserons 200 Go des 250 Go disponibles. Ajustez la taille dans ce champ. Choisissez `xfs` dans Type de système de fichiers. Dans le champ Point de montage, entrez `/data`. Entrez également cette valeur dans Logical volume name.

4. Optimiser un système de fichier

   Maintenant que votre partition et votre système de fichiers sont prêts, il faut optimiser quelques paramètres :

   - `noatime` : en utilisant cette option, le temps d'accès des inodes du système de fichiers ne sera pas mis à jour. L'accès aux données sera encore plus rapide.
   - `grpquota` et `usrquota` : permettent de limiter les quotas pour les usagers et les groupes d'usagers en fonction de l'espace utilisé par usager ou par groupe.

Pour simplifier l'administration, vous devriez utiliser des noms significatifs pour toutes les étapes du partitionnement.

Votre système de fichier est maintenant prêt. Vous pouvez modifier des options et augmenter l'espace disponible en utilisant la ligne de commande ou l'outil `harddrake` disponible à travers le Mandriva Linux Control Center.

2.7. Choix des paquetages à installer

Abordons maintenant l'installation des paquetages logiciels. Cette phase consiste à sélectionner les medias d'installation puis les paquetages à installer.

2.7.1. Gestion des medias

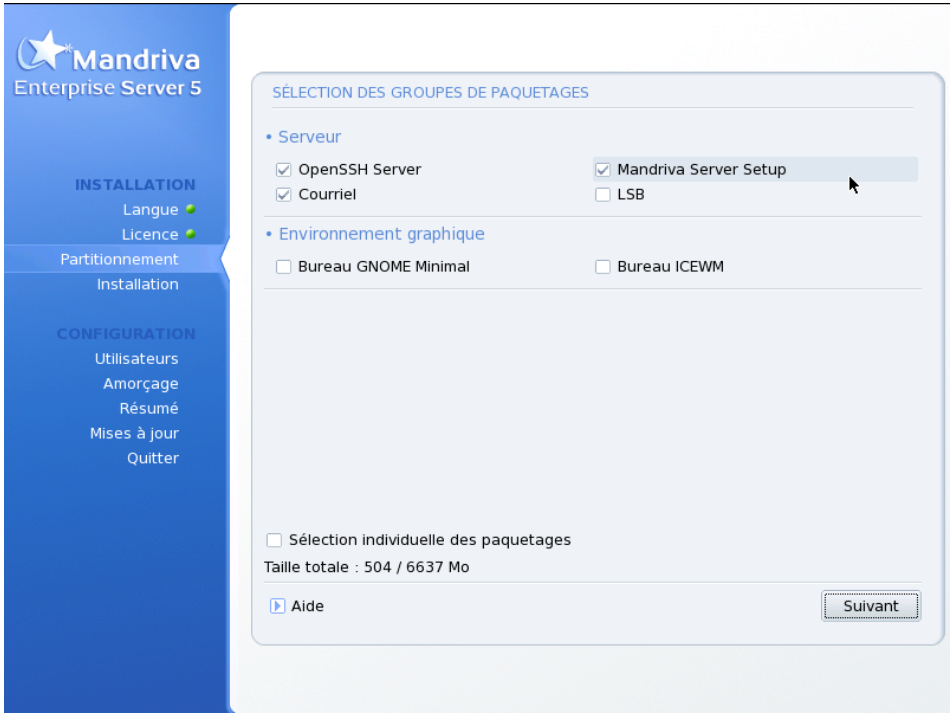
Si vous réalisez une installation à partir d'un CD, vous devrez sélectionner ceux que vous possédez.

Il vous est aussi proposé de copier tous les paquetages sur votre disque dur.

Nous vous recommandons de copier les paquetages sur le disque dur. Cette méthode accélère l'installation et vous facilitera les installations de paquetages logiciels une fois votre serveur installé puisque les paquetages seront déjà disponibles sur le disque dur.

Si vous ne copiez pas les paquetages sur le disque dur, vous aurez besoin des CD d'installations pour chaque nouveau paquetage que vous installerez. Cette opération pourra toutefois être réalisée plus tard (voir chapitre "Configuration d'un dépôt local").

2.7.2. Choix des groupes de paquetages à installer



Mandriva Enterprise Server 5 propose une méthode d'installation différente. Ce volet est exécuté en deux étapes principales :

Durant l'installation principale vous pouvez choisir et installer des paquetages qui concernent le système de base. Ce qui signifie la pile du noyau, une pile réseau minimale, une pile courriel minimale et un environnement graphique.

L'environnement graphique n'est pas nécessaire au bon fonctionnement d'un serveur. Néanmoins, de nombreux outils d'administration ne sont accessibles qu'à partir d'un environnement graphique.

Voici ce que vous pouvez installer durant le processus d'installation :

- Serveur : un serveur d'accès distant (`OpenSSH`) et un Mail Transport Agent (MTA) minimal (`postfix`) sont proposés.

  Mandriva Server Setup (paquetage mmc-wizard) est l'assistant d'installation pour Mandriva Linux Enterprise Server. Il vous aidera à activer les piles dont vous avez besoin pour votre serveur à travers une interface web.

- Environnement graphique : par défaut, Mandriva Enterprise Server 5 propose d'installer un environnement graphique Gnome allégé. Vous pouvez également choisir un environnement encore plus léger tel que IceWM.

En plaçant votre souris au-dessus du nom d'un groupe, vous verrez apparaître une courte description de ce groupe.

Vous pouvez enfin cocher l'option Sélection individuelle des paquetages. Cette option est utile si vous connaissez exactement le paquetage désiré ou si vous voulez avoir le contrôle total de votre installation.

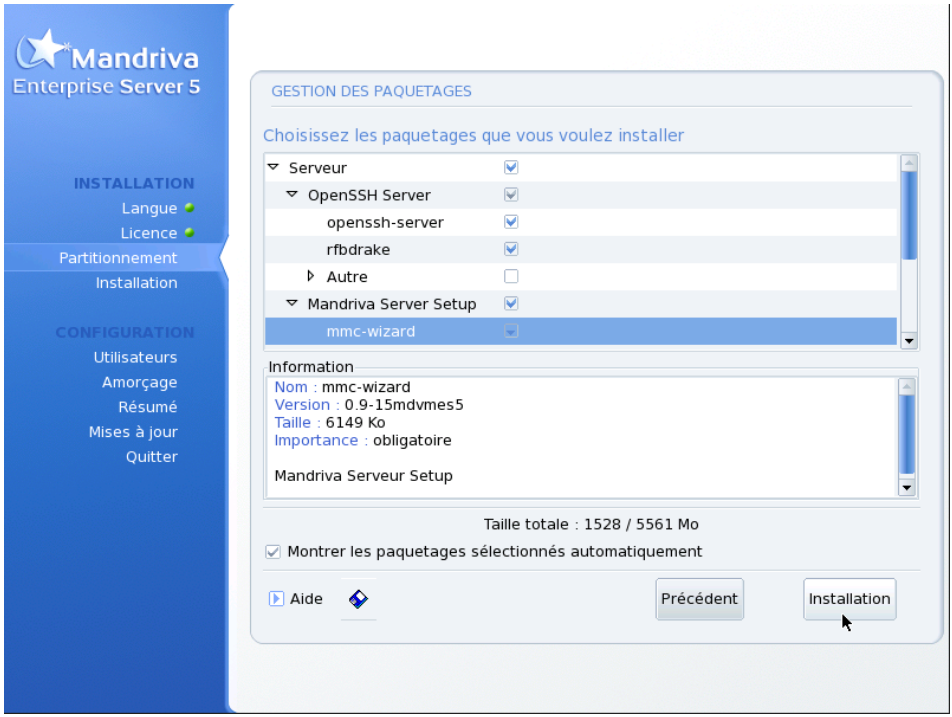
Si vous avez démarré l'installation en mode mise à jour, vous pouvez désélectionner tous les groupes afin d'éviter l'installation de nouveaux programmes. Cette option est très utile pour restaurer un système défectueux ou le mettre à jour.

Installation minimale

Si vous désélectionnez tous les groupes lors d'une installation standard (en opposition à une mise à jour), une boîte de dialogue apparaîtra après avoir cliqué sur Suivant, et vous proposera différentes options pour une installation minimale :

- Avec X : installe le moins de paquetages possible pour avoir un environnement de travail graphique ;
- Avec la documentation de base : installe le système de base plus certains utilitaires de base et leur documentation. Cette installation est utilisable comme base pour monter un serveur ;
- Installation vraiment minimale : installe le strict minimum nécessaire pour obtenir un système GNU/Linux fonctionnel en ligne de commande. urpmi ne sera pas installé !

2.7.3. Choix des paquetages individuels à installer



Enfin, si vous avez choisi de sélectionner individuellement les paquetages à installer, DrakX vous présentera un arbre contenant tous les paquetages classés par groupes et sous-groupes. En vous déplaçant dans l'arbre, vous pouvez sélectionner des groupes, des sous-groupes ou des paquetages individuels.

Dès que vous sélectionnez un paquetage dans l'arbre, une description apparaît à droite.

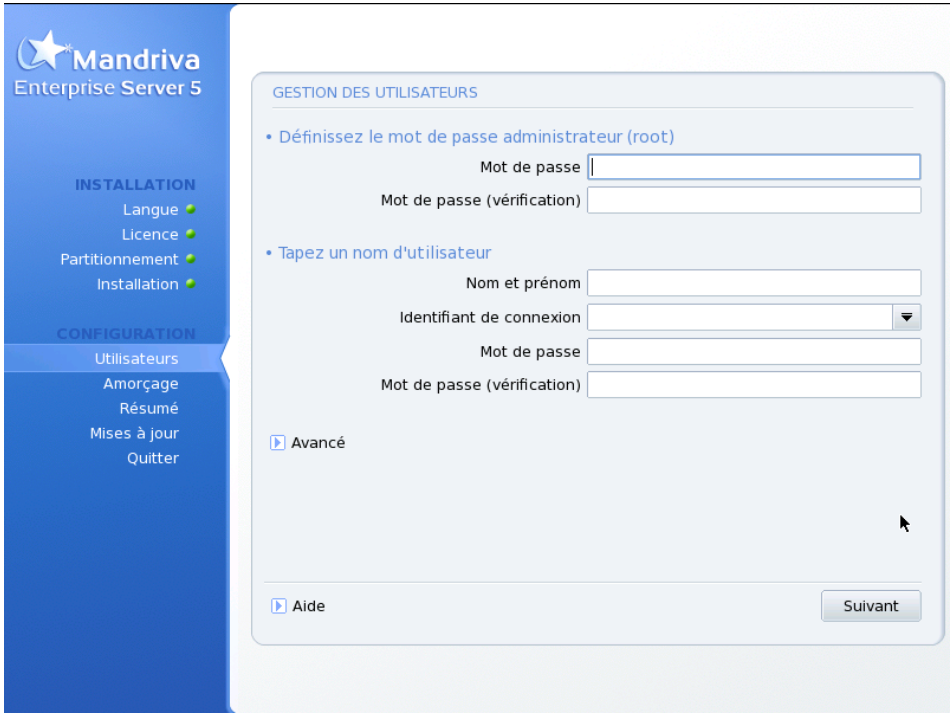
Si un paquetage serveur a été sélectionné, vous devrez confirmer que vous voulez vraiment que celui-ci soit installé. Sous Mandriva Linux, par défaut, tous les services installés sont lancés au démarrage. Malgré tous les efforts investis pour vous livrer une distribution Linux sécurisée, il est possible que certaines failles de sécurité affectent les serveurs installés au-delà de la date de publication. Si vous ne savez pas précisément à quoi sert un service en particulier ou pourquoi il est installé, cliquez sur NON.

L'option Montrer les paquetages sélectionnés automatiquement sert à désactiver les messages d'avertissement. Ceux-ci apparaissent lorsque l'installeur sélectionne automatiquement un nouveau paquetage dont le système dépend. Certains paquetages sont dépendants les uns des autres, donc l'installation d'un

paquetage peut engendrer l'installation d'un autre (paquetage). DrakX peut déterminer quels paquetages sont requis pour résoudre les conflits dus aux dépendances et installer le système avec succès.

L'icône de disquette qui apparaît au bas de la liste permet de charger ou sauvegarder la liste de paquetages. Cette option est utile si vous possédez plusieurs machines et que vous désirez les configurer de façon identique. Cliquez sur cette icône et choisissez entre la Charge ou la Sauvegarde de votre liste de paquetages. Puis, sélectionnez le média dans l'écran suivant et cliquez sur OK.

2.8. Ajout d'un utilisateur



GNU/Linux est un système multiutilisateurs, ce qui signifie généralement que chaque utilisateur peut avoir des préférences différentes, ses propres fichiers, etc. Contrairement à `root` qui a tous les droits, les utilisateurs que vous ajouterez n'auront que la permission d'agir sur leurs propres fichiers et la personnalisation de leurs applications. Ainsi les fichiers et configurations système sont implicitement protégés contre toute altération accidentelle ou intentionnelle.

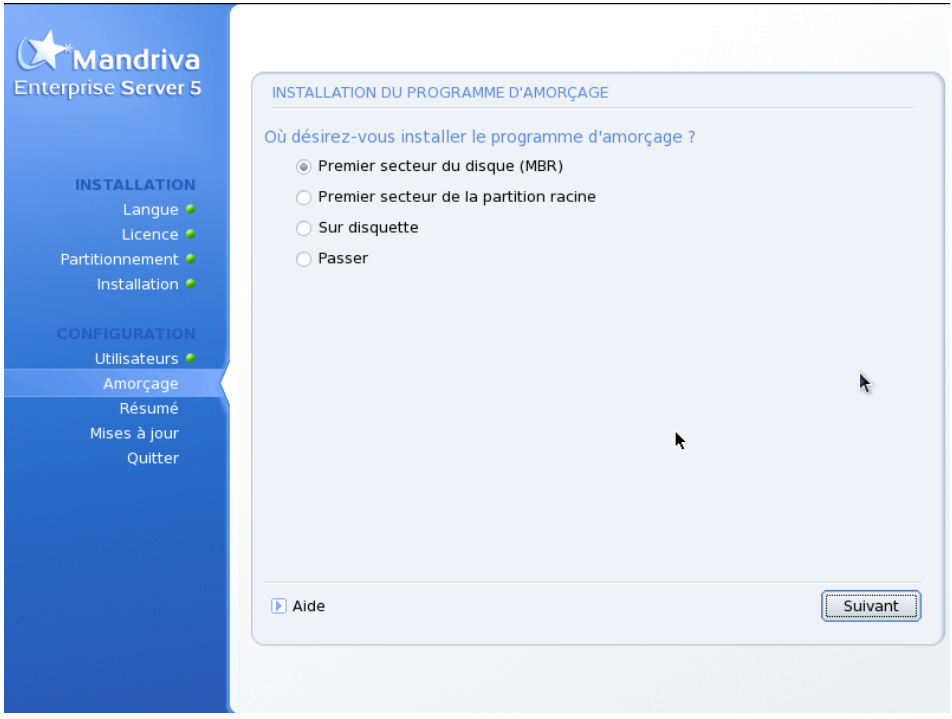
Vous devez vous créer au moins un compte utilisateur pour vous-même, que vous utiliserez pour l'utilisation quotidienne du système. Car, bien qu'il soit pratique de se connecter en tant que `root` et avoir tous les accès, cette situation peut également engendrer des situations désastreuses si un fichier est détruit par inadvertance. Un utilisateur normal n'ayant pas accès aux fichiers sensibles ne peut causer de dommages majeurs.

Il faut d'abord entrer le vrai nom de la personne. DrakX prend le premier mot inséré et le transpose, en minuscule, dans le champ Nom de login. C'est le nom que l'usager doit utiliser pour se connecter au système. Entrez ensuite un mot de passe, deux fois (pour confirmation). Celui-ci n'est pas aussi crucial que le mot de passe de `root`, mais ce n'est pas une raison pour le négliger et utiliser un mot évident. Après tout, ceci mettrait **vos** fichiers en péril.

Après avoir cliqué sur Accepter l'utilisateur, il vous sera possible d'ajouter d'autres utilisateurs. Créez un utilisateur différent pour chaque personne devant utiliser votre ordinateur. Une fois chaque utilisateur défini, cliquez sur Suivant.

En cliquant sur Avancé, vous pourrez sélectionner un `shell` différent pour cet utilisateur (bash est assigné par défaut) et choisir manuellement l'ID utilisateur et de groupe pour cet usager.

2.9. Installation du gestionnaire de démarrage

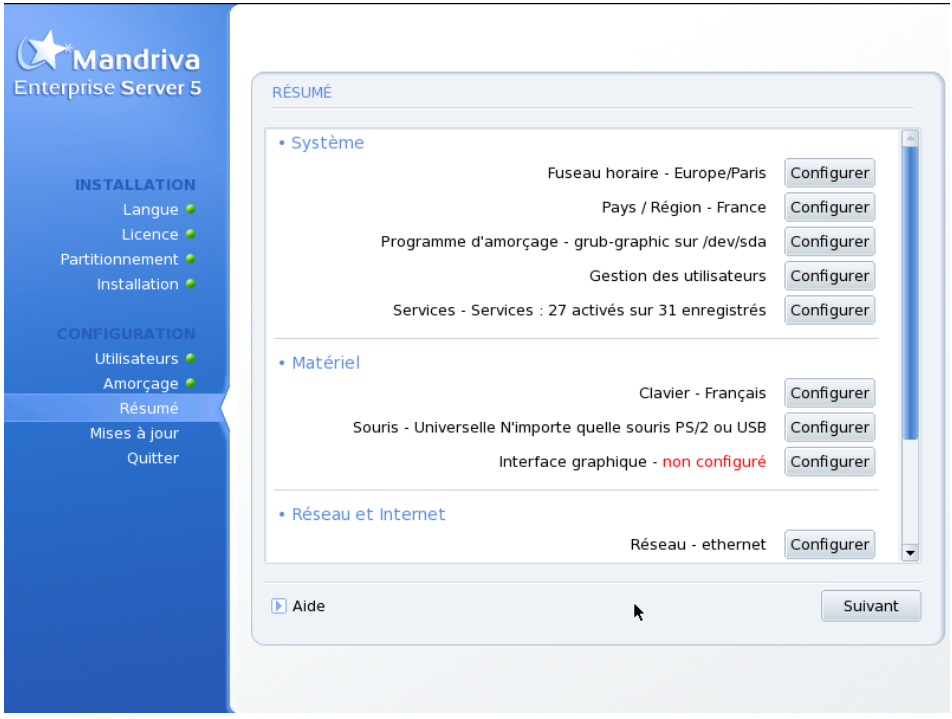


Le gestionnaire de démarrage est un petit programme lancé par la machine à l'amorce. Il est en charge du démarrage du système. Normalement, l'installation d'un gestionnaire de démarrage est complètement automatique. DrakX analyse le secteur de démarrage (*Master Boot Record* ou MBR) et agit en fonction de ce qu'il peut y lire. Il vous demandera s'il doit remplacer le chargeur de démarrage. Généralement, le Premier secteur du disque (MBR) est l'endroit le plus sûr.

Choisissez Passer et aucun gestionnaire de démarrage ne sera installé. Utilisez cette option à vos risques et périls.

2.10. Résumé de l'installation courante

2.10.1. Résumé



Diverses informations sont présentées au sujet de la configuration actuelle. Selon le matériel installé, certaines entrées seront présentes et d'autres pas. Sur chaque ligne apparaît le nom du paramètre suivi de sa valeur actuelle. Cliquez sur le bouton Configurer correspondant pour effectuer un changement.

- Clavier : vérifiez la configuration choisie pour le clavier.
- Pays / Région : vérifiez la sélection du pays. Si vous ne vous trouvez pas dans ce pays, cliquez sur le bouton Configurer et choisissez le bon. Si votre pays ne se trouve pas dans la première liste, cliquez sur Autres pays pour obtenir la liste complète.
- Fuseau horaire : Par défaut, DrakX configure le fuseau horaire selon le pays dans lequel vous vous trouvez. Cliquez sur le bouton Configurer si ce n'est pas le bon.
- Souris : pour vérifier la configuration actuelle de la souris et la modifier si nécessaire.

- Imprimante : l'outil de configuration d'impression sera démarré en cliquant sur Configurer.
- Carte son : si vous remarquez que la carte configurée n'est pas celle qui se trouve effectivement sur votre système, vous pouvez cliquer sur le bouton pour choisir un pilote différent.
- Interface graphique : par défaut, DrakX applique une résolution correspondant le mieux à votre combinaison de carte graphique et d'écran. Si cela ne vous convient pas ou si DrakX n'arrive pas à la configurer automatiquement, cliquez sur Configurer pour changer la configuration de votre interface graphique. Vous pouvez cliquer sur le bouton Aide depuis l'assistant de configuration pour consulter l'aide en ligne.
- Réseau : pour configurer votre accès Internet ou réseau local dès maintenant. Lisez la documentation fournie ou exécutez Centre de contrôle Mandriva Linux après l'installation pour avoir droit à une aide en ligne complète.
- Proxy : permet de configurer les adresses proxy (mandataire en français) HTTP et FTP si la machine que vous installez se trouve derrière un serveur proxy.
- Niveau de sécurité : vous pouvez y redéfinir votre niveau de sécurité.
- Pare-feu : si vous avez l'intention de connecter votre ordinateur à Internet, c'est une bonne idée de le protéger des intrusions grâce à un pare-feu.
- Chargeur de démarrage : pour changer la configuration par défaut de votre chargeur de démarrage. À réserver aux utilisateurs expérimentés. Lisez la documentation fournie ou l'aide en ligne sur la configuration du chargeur de démarrage présente dans le Centre de contrôle Mandriva Linux.
- Services : pour contrôler finement les services disponibles sur votre machine. C'est une bonne idée de vérifier ce paramétrage pour vous assurer des services dont vous avez **réellement besoin**.

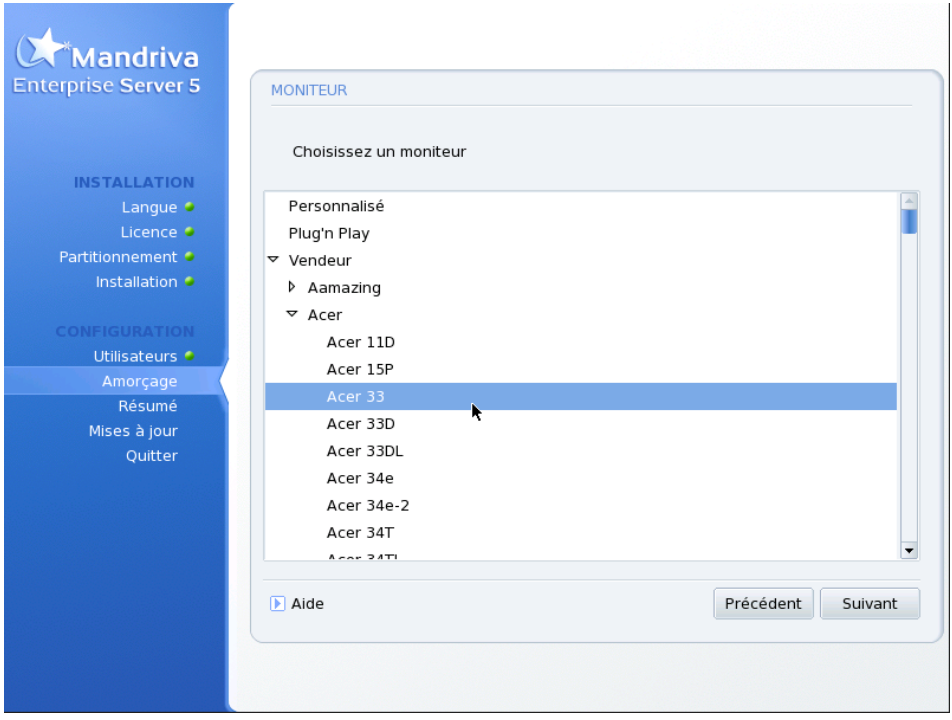
2.10.2. Options de fuseau horaire

Cet outil permet d'affiner le fuseau horaire dans lequel vous êtes situé. Après avoir choisi l'endroit le plus proche de votre fuseau horaire, deux options supplémentaires s'offrent à vous.

Horloge système réglée sur le méridien de Greenwich. GNU/Linux manipule l'heure au format GMT (*Greenwich Mean Time*) et la convertit en temps local selon le fuseau horaire choisi. Si l'horloge de votre ordinateur est réglée sur l'heure locale, vous pouvez désactiver cela en dé-sélectionnant cette option de façon à ce que GNU/Linux sache que l'horloge matérielle est la même que celle du système. C'est particulièrement utile si la machine accueille un autre système d'exploitation.

Synchronisation automatique. Cette option permet de régler l'heure automatiquement en se connectant à un serveur de temps sur Internet. Dans la liste proposée, choisissez un serveur géographiquement proche de vous, ou plus simplement l'entrée World Wide qui sélectionne automatiquement le serveur le plus approprié. Vous devez bien entendu avoir une connexion Internet pour que cela fonctionne. Un serveur de temps local sera installé sur votre machine et pourra, en option, être lui-même utilisé par d'autres machines de votre réseau local.

2.10.3. Configuration de X, le serveur graphique



Si vous avez choisi d'installer un environnement graphique, il vous est demandé de configurer X. X (qui signifie « le système X Window ») est le cœur de votre interface graphique sous GNU/Linux. Tous les environnements graphiques (KDE, GNOME, WindowMaker etc.) présents sur Mandriva Linux dépendent de X.

Vous verrez une liste de divers paramètres à changer pour obtenir un affichage optimal :

Carte graphique

Le programme d'installation détecte et configure automatiquement la carte graphique présente sur votre machine. Si ce n'est pas le cas, vous pouvez choisir dans cette liste la carte que vous utilisez.

Moniteur

Le programme d'installation détecte et configure automatiquement les moniteurs connectés à votre unité centrale. Si ce n'est pas le cas, vous pouvez choisir dans cette liste celui que vous utilisez.

Résolution

Vous pouvez choisir la résolution et le nombre de couleurs parmi celles disponibles pour votre matériel. Choisissez la configuration optimale pour votre utilisation (vous pouvez la modifier après l'installation). Un échantillon de la configuration choisie apparaît à l'écran.

Test

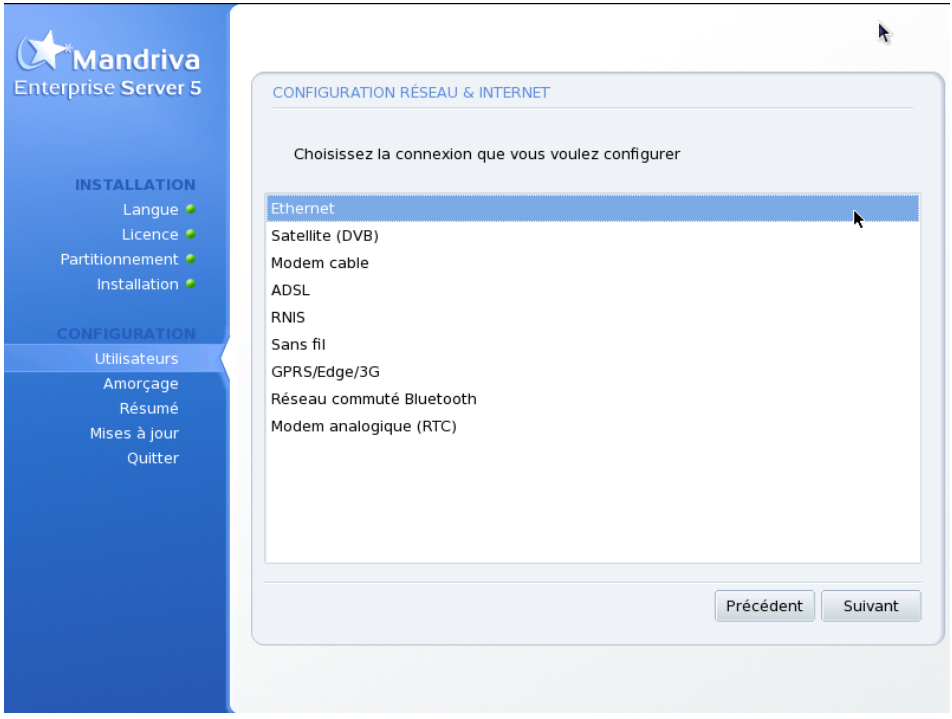
Selon votre matériel, cette option peut ne pas apparaître.

Le système essaie d'ouvrir un écran graphique à la résolution choisie. Si vous pouvez voir le message pendant le test, et répondez Oui, alors DrakX passe à l'étape suivante. Si vous ne pouvez pas voir de message, cela signifie que vos paramètres sont incompatibles, et le test se termine automatiquement après quelques secondes. Changez la configuration jusqu'à ce que vous obteniez un affichage correct lors du test.

Options

Cette étape vous permet de sélectionner un démarrage en mode graphique dès le début. Évidemment, il est préférable de choisir Non si vous êtes en train d'installer un serveur, ou si vous n'avez pas réussi à configurer l'écran correctement.

2.10.4. Configuration réseau



Si vous désirez connecter votre système à un réseau ou à Internet, cliquez sur OK. L'auto-détection des périphériques réseau et modem sera alors lancée. Si cette détection échoue, décochez la case Utiliser l'auto-détection. Vous pouvez aussi choisir de ne pas configurer le réseau, ou de le faire plus tard. Dans ce cas, cliquez simplement sur Annuler.

Les types de connexion supportés sont : modem traditionnel, Winmodem, modem ISDN, connexion ADSL, modem câble ou simplement LAN (réseau Ethernet).

Nous ne détaillerons pas dans cette section chacune des configurations possibles. Assurez-vous seulement que vous avez toutes les informations de votre fournisseur de service Internet à portée de main.

2.10.5. Installation d'un programme d'amorçage

Vous pouvez ajuster le programme d'amorçage :

- Programme d'amorçage à utiliser vous propose les choix suivants :

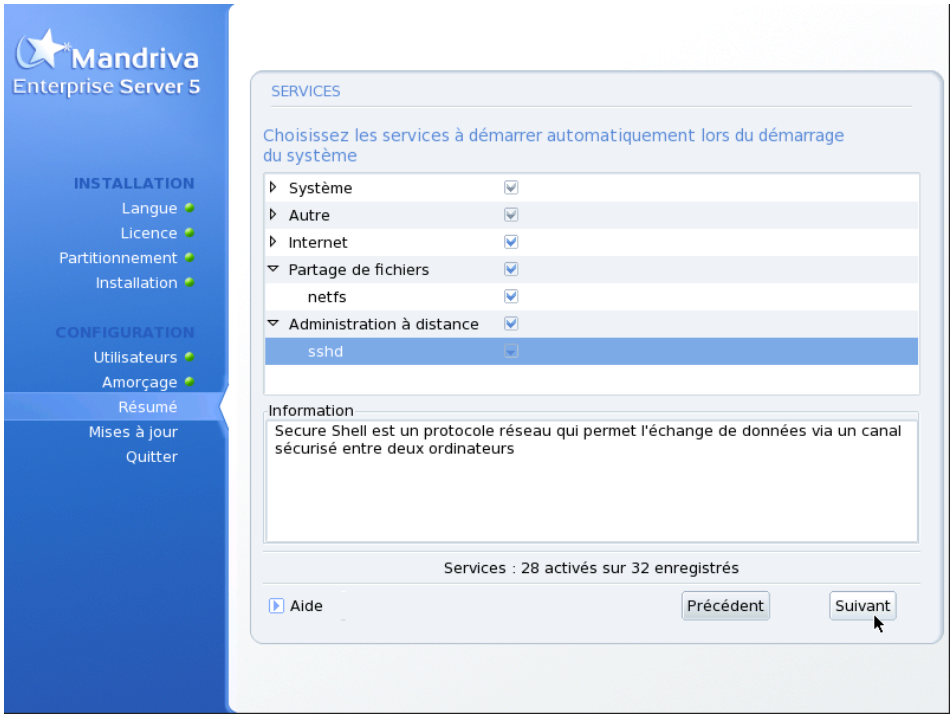
  1. GRUB : si vous préférez GRUB (menu texte).
  2. GRUB en mode graphique : si vous préférez GRUB avec une interface graphique.
  3. LILO en mode texte : si vous préférez la version texte de LILO.
  4. LILO en mode graphique : si vous préférez l'interface graphique.

- Périphériques de démarrage : dans la plupart des cas, vous n'aurez pas à changer le disque par défaut (/dev/sda), mais si vous le désirez, le programme d'amorce peut être installé sur un second disque, /dev/sdb, ou même sur une disquette, /dev/fd0.
- Délais avant l'activation du choix par défaut : au redémarrage de l'ordinateur, il s'agit du temps accordé à l'utilisateur pour démarrer un autre système d'exploitation.
- Activer l'ACPI : pour la gestion d'énergie, surtout pour les portables. Si vous savez que votre matériel est compatible ACPI, cochez cette case.
- Forcer sans APIC : si vous avez remarqué auparavant des problèmes matériel sur votre machine (conflits IRQ, instabilités, blocages machine, etc.), vous pouvez essayer de désactiver l'APIC en cochant cette case.

Prenez garde, si vous décidez de ne pas installer de programme d'amorce (en cliquant sur Passer), vous devez vous assurer d'avoir une méthode pour démarrer le système. Aussi, assurez-vous de bien savoir ce que vous faites si vous modifiez les options.

En cliquant sur Avancée, vous aurez accès à plusieurs options de configuration supplémentaires. Sachez que celles-ci sont réservées aux experts en la matière.

2.10.6. Sélection des services disponibles au démarrage



Vous pouvez maintenant choisir les services disponibles au démarrage de votre système.

Tous les services disponibles sont présentés. Faites une bonne vérification et enlevez tout ce qui n'est pas absolument nécessaire au démarrage du système.

Vous pouvez obtenir une courte explication des services en les sélectionnant spécifiquement. Cela dit, si vous ne savez pas à quoi sert exactement un service, conservez les paramètres par défaut.

À cette étape, soyez particulièrement attentif dans le cas d'un système destiné à agir comme serveur. Dans ce cas, vous voudrez probablement permettre exclusivement les services nécessaires. Souvenez-vous que certains services peuvent s'avérer dangereux s'il sont activés sur un serveur. En général, n'installez que les services dont vous avez **absolument** besoin.

Chapitre 3. Mandriva Server Setup (mmc-wizard)

3.1. Utiliser Mandriva Server Setup

Mandriva Server Setup est l'assistant d'installation pour Mandriva Enterprise Server 5. Il permet d'installer simplement les fonctionnalités de base du serveur et d'activer des services supplémentaires.

Si vous ne l'avez pas sélectionné à l'installation du système, vous pouvez toujours l'installer ultérieurement. Il s'agit du paquetage mmc-wizard.

Une fois installé, Mandriva Server Setup est accessible via un navigateur web à l'adresse https:/IP_server_MES5/mmc-wizard/

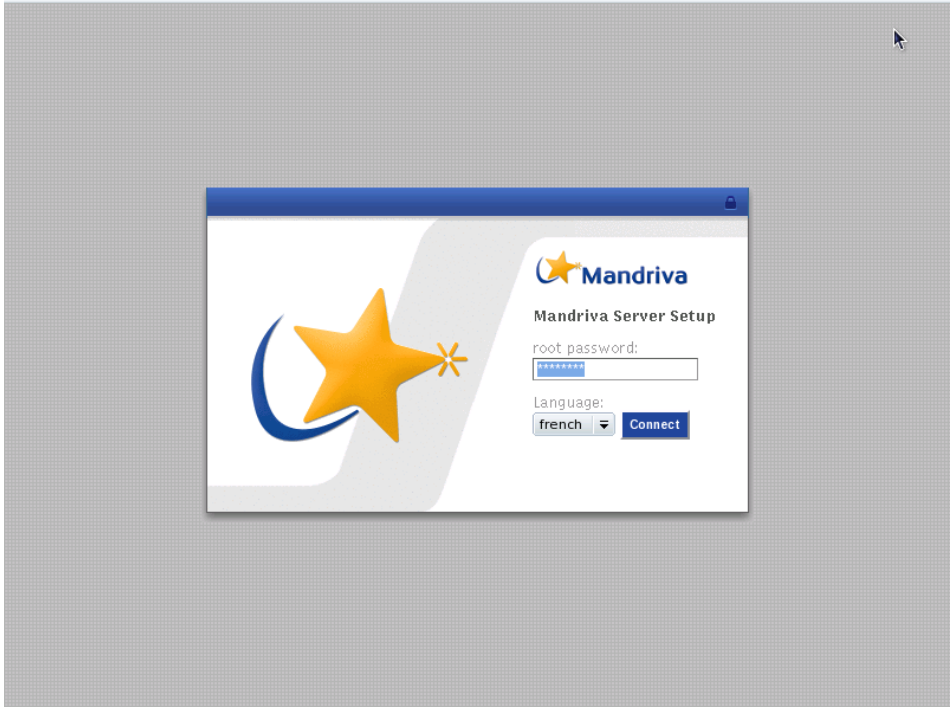


Figure 3-1. Login Mandriva Server Setup

On ne peut s'y connecter qu'avec l'utilisateur root.

Figure 3-2. Accueil Mandriva Server Setup

Mandriva Server Setup est divisée en 2 grandes parties:

- Configuration simplifiée avec Mandriva Directory Server: permet d'installer simplement et de configurer automatiquement Mandriva Directory Server, l'annuaire d'entreprise basé sur OpenLDAP. Mandriva Directory Server étant conçue de façon modulable, les différents parties constituantes de MDS peuvent être choisies. -> voir "Stack Mandriva Directory Server"
- Configuration avancée: Vous y retrouverez les stacks middleware/serveur et services communément installés sur des serveurs. Les stacks proposées dans cette partie ont une configuration minimale. De plus, elles ne sont pas automatiquement intégrées à MDS.

Certaines piles applicatives se retrouvent à la fois dans les 2 parties de Mandriva Server Setup. Si tout ou partie d'une stack est déjà installée, les stacks correspondantes de la seconde partie ne seront plus accessibles (cases à cocher grisées).

3.2. Stacks MDS et configuration simplifiée

3.2.1. Concept général

Mandriva Directory Server est un annuaire d'entreprise basé sur OpenLDAP

permettant de gérer les comptes et profils des utilisateurs d'un parc informatique, ainsi que différents services réseaux communément utilisés (Samba, dns, dhcp, mail...).

Pour une utilisation simplifiée, Mandriva Directory Server se pilote par le biais d'une interface web moderne et conviviale. Le chapitre Mandriva Directory Server de cette documentation aborde l'utilisation de l'interface.

Pour une vue d'ensemble de Mandriva Directory Server, visitez le site du projet (`http://mds.mandriva.org/`) .

3.2.2. Installation et configuration

Figure 3-3. Page d'installation de Mandriva Directory Server

3.2.2.1. Composant principal : Mandriva Directory Server

Les paquets et la configuration de base de Mandriva Directory Server. Coché par défaut, ce composant est nécessaire aux autres modules liées à Mandriva Directory Server.

Lors de l'installation de ce composant, un fenêtre apparait. Cliquez sur le bouton Détails pour visualiser la console.

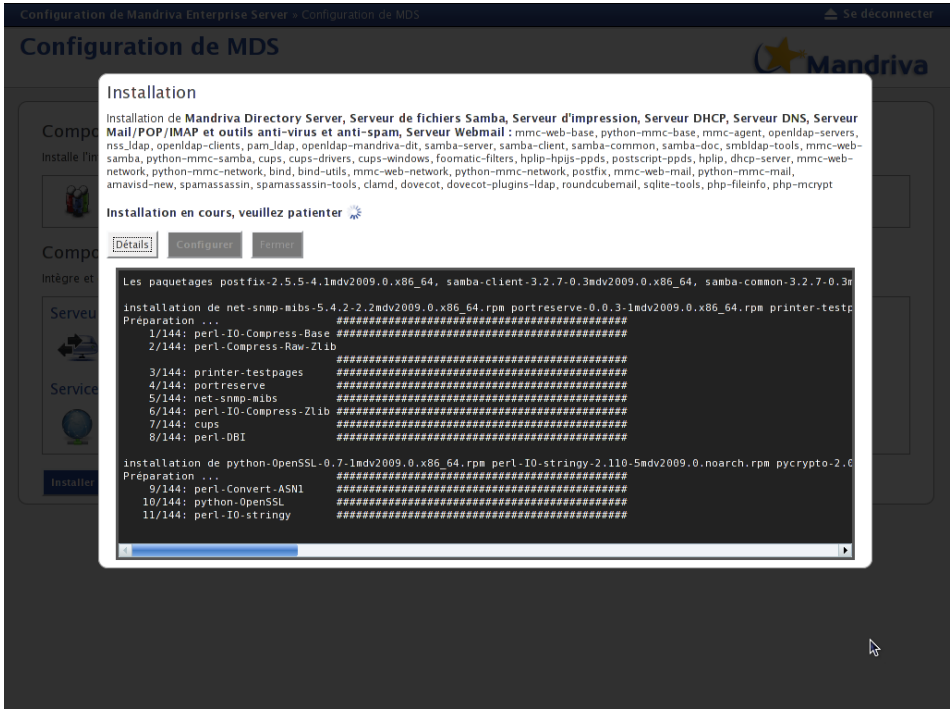


Figure 3-4. Détails de l'installation: vue console

À l'issue de l'installation, cliquez sur Configurer.

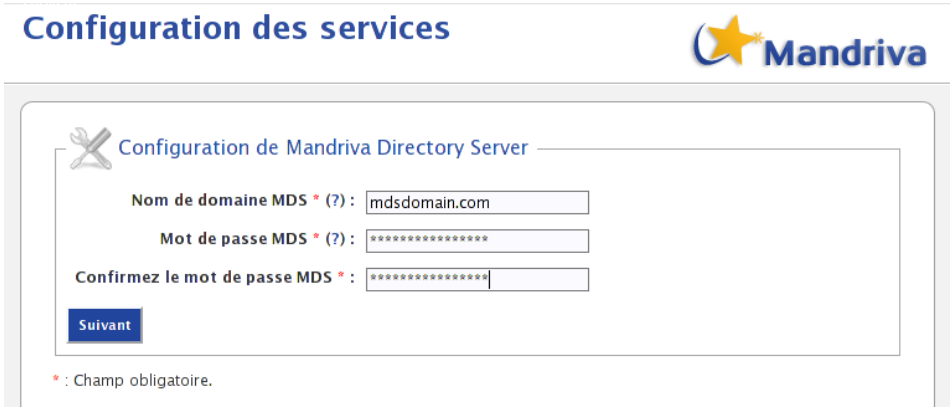


Figure 3-5. Page de configuration de Mandriva Directory Server

Il vous est alors demandé de renseigner le nom de domaine (par exemple: domain.com) géré par Mandriva Directory Server et un mot de passe d'administration spécifique à Mandriva Directory Server. Celui-ci sera demandé pour toute installation de modules Mandriva Directory Server.

Un récapitulatif de la configuration est ensuite affiché.

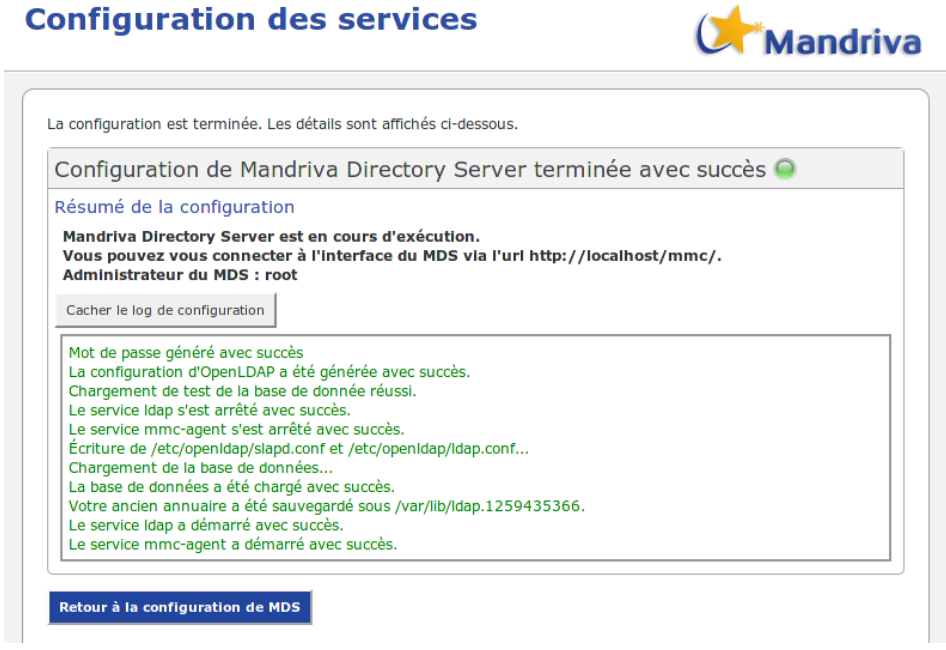


Figure 3-6. Page de résultat de la configuration de Mandriva Directory Server

Suite à la configuration vous pouvez remarquer que l'interface du MDS est accessible via l'URL http://IP_serveur_MES5/mmc/. L'utilisateur administrateur du MDS est root.

Si vous ne pouvez pas vous connecter à l'interface MDS depuis un autre poste que le serveur, vérifiez que votre firewall autorise les requêtes de type "web" (ports 80 et 443).

Voici la liste des paquets installés par ce composant :

- `mmc-web-base`
- `python-mmc-base`
- `mmc-agent`
- `openldap-servers`
- `nss_ldap`
- `openldap-clients`

3.2.2.2. Serveur d'impression et de fichiers

Ce composant contient les paquets et la configuration du module Mandriva Directory Server permettant d'administrer les partages de fichiers et d'imprimantes pour les réseaux Microsoft.

3.2.2.2.1. Serveur de fichiers Samba

Lors de la configuration il vous sera demandé de renseigner le nom de domaine Samba ainsi que le nom du serveur Samba dans le domaine Microsoft. Enfin, il faut définir un mot de passe administrateur Samba.

Le service Samba est configuré en tant que contrôlleur de domaine principal pour votre réseau Microsoft. Des machines clientes Windows pourront se joindre au domaine que vous spécifiez lors de l'étape de configuration. L'utilisateur "admin" créé lors de l'installation vous permettra d'administrer le domaine.

Pour que vos utilisateurs puissent s'authentifier sur le domaine, ils doivent appartenir au groupe "Domain Users". Après l'installation de ce composant, tous les utilisateurs nouvellement créés seront placés automatiquement dans le groupe "Domain Users".

Voici la liste des paquets installés pour le serveur de fichiers Samba :

- `samba-server`
- `samba-client`

- samba-common
- samba-doc
- smbldap-tools
- mmc-web-samba
- python-mmc-samba

3.2.2.2.2. Serveur d'impression Cups

Le serveur d'impression Cups permet de partager les imprimantes que vous installez sur votre serveur.

Voici la liste des paquets installés pour le serveur d'impression Cups :

- cups
- cups-drivers
- cups-windows
- foomatic-filters
- hplip-hpijs-ppds
- postscript-ppds
- hplip

Plus d'informations sur le paquetage cups-windows:

```
The cupsaddsmb command will use the CUPS v6 PostScript printer driver
for Windows available in this package.
To complete the installation, you have to put the Microsoft Postcript
driver files in the /usr/share/cups/drivers directory. These files can
be found on any system running Windows 2000 or higher in the folder:
%WINDOWS%\SYSTEM32\SPOOL\DRIVERS\W32X86\3

After this step, your /usr/share/cups/drivers directory should contain
these files:
cups6.inf
cups6.ini
cupsps6.dll
cupsui6.dll
ps5ui.dll (from your Windows system)
pscript.hlp (from your Windows system)
pscript.ntf (from your Windows system)
pscript5.dll (from your Windows system)
```

3.2.2.3. Services réseaux

Ce composant contient les paquets et la configuration du module Mandriva Directory Server permettant de créer et de gérer un LAN (zones DNS et sous-réseaux DHCP).

Lors de la configuration du module de serveur DNS, vous pouvez configurer les réseaux qui pourront faire des requêtes récursives sur votre DNS. Une requête récursive a pour objet un nom de domaine d'une zone que votre serveur DNS ne connait pas. Le serveur DNS doit alors contacter d'autres serveurs DNS pour résoudre la requête.

Pour ce qui est de la résolution des zones configurées sur votre serveur DNS, il n'y a pas de restriction concernant l'origine des clients.

Vous pouvez également spécifier de forwarder toutes les requêtes DNS externes vers un autre serveur DNS. Votre serveur DNS ne résoudra alors que les zones que vous avez configuré.

Le composant DHCP ne nécessite aucune configuration dans le Mandriva Serveur Setup.

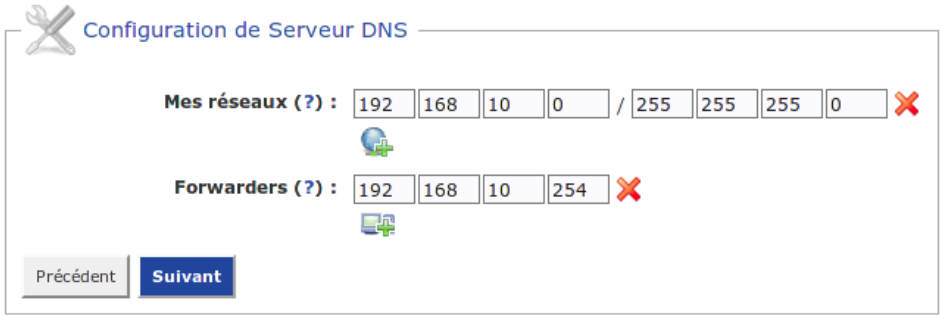


Figure 3-7. Page de configuration du service DNS :

Les paquets installés pour ces composants sont :

- **Serveur DHCP.** : `dhcp-server`, `mmc-web-network`, `python-mmc-network`
- **Serveur DNS.** : `bind`, `bind-utils`, `mmc-web-network`, `python-mmc-network`

3.2.2.4. Serveur de mail

3.2.2.4.1. Serveur Mail/POP/IMAP et outils anti-virus et anti-spam

Ce module installe et configure pour MDS un serveur SMTP (envoi et récep-

tion des mails), un serveur POP3/IMAP (consultation des mails) ainsi que des outils de détection des spams et virus. Cette configuration vous permet de gérer autant de domaines mails que vous désirez.

À l'issue de l'installation, il vous sera demandé de renseigner le hostname/FQDN du serveur smtp (par exemple: smtp.domain.com). Spécifiez ensuite quels réseaux sont autorisés à envoyer des mails à travers Postfix, par exemple le réseau local 192.168.0.0 de masque 255.255.255.0.

Choisissez enfin les protocoles que le serveur Dovecot fournira: imap imaps, pop3 pop3s ou à la fois imap imaps et pop3 pop3s.

Pour finir, n'oubliez pas d'ouvrir les ports nécéssaires sur le firewall (SMTP: 25, SMTPS: 465, POP3S: 995, IMAPS: 993). Notez que les protocoles IMAP et POP3 en mode non sécurisé ne sont pas actifs sur les interfaces externes.

- Les paquets installés pour ce composant sont :
- `postfix`
- `mmc-web-mail`
- `python-mmc-mail`
- `amavisd-new`
- `spamassassin`
- `spamassassin-tools`
- `clamd`
- `dovecot`
- `dovecot-plugins-ldap`

3.2.2.4.2. Serveur Webmail

Cette stack n'est pas directement liée à Mandriva Directory Server. Elle installe le webmail Roundcube, qui permettra à vos utilisateurs d'avoir leur messagerie en ligne. Il suffit d'activer le module mail sur vos utilisateurs depuis l'interface du MDS si ce n'est déjà fait. Les utilisateurs pourront s'authentifier avec le couple mail/mot de passe sur http://IP_serveur_MES5/roundcubemail.

- Les paquets installés pour ce composant sont :
- `roundcubemail`
- `sqlite-tools`
- `php-fileinfo`
- `php-mcrypt`

3.3. Stacks middleware/serveur et services ("Configuration avancée")

3.3.1. Concept général

Cette partie permet d'installer des stacks serveur sans configuration particulière.

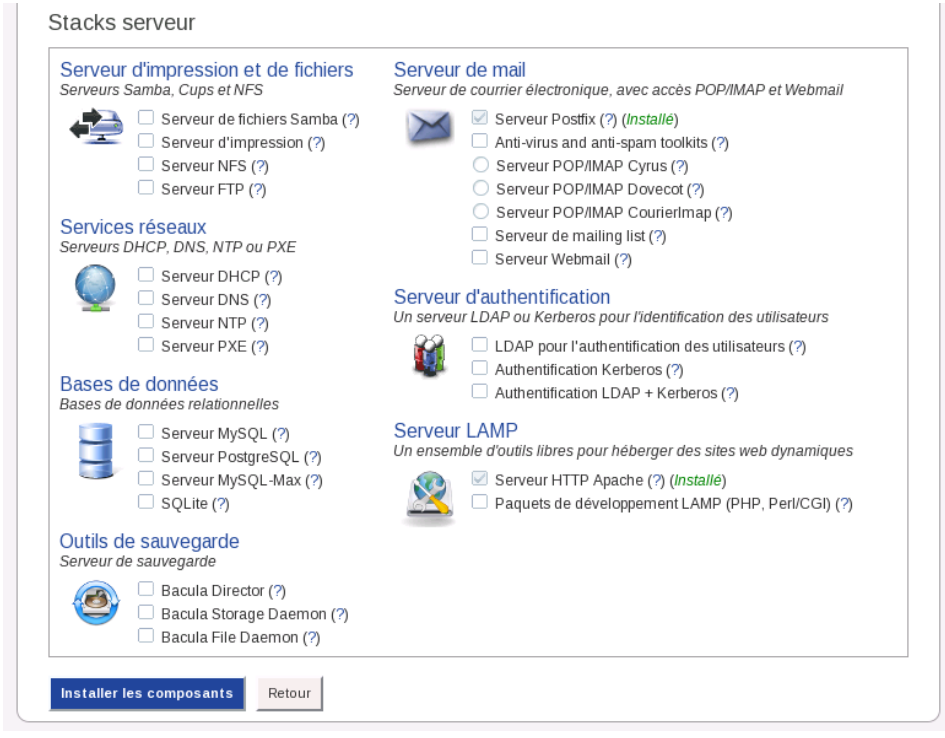


Figure 3-8. Page Stacks serveur

Certaines stacks peuvent être grisées et donc impossibles à cocher si certaines stacks déjà installées sont en conflits.

3.3.2. Survol des piles

Serveur d'impression et de fichiers

Serveurs Samba, CUPS et NFS

- Serveur de fichiers Samba

  Partage de fichiers et d'imprimantes pour les réseaux Microsoft .

  `samba-server`

  `samba-client`

  `samba-common`

  `samba-doc`

  `smbldap-tools`

  `samba-winbind`

- Serveur d'impression

  Installation et configuration d'imprimantes réseau avec CUPS .

  `cups`

  `cups-drivers`

  `cups-windows`

  `foomatic-filters`

  `hplip-hpijs-ppds`

  `postscript-ppds`

  `hplip`

- Serveur NFS

  Partage de fichiers par NFS

  `nfs-utils`

  `nfs-utils-clients`

Services réseaux

Serveurs DHCP, DNS, NTP ou PXE

- Serveur DHCP

  Fourni les paramètres IPs aux machines clientes.

  `dhcp-server`

- Serveur DNS

Résolution des noms de machine sur le réseau.

`bind`

`bind-utils`

- Serveur NTP

  Serveur de temps

  `ntp`

- Serveur PXE

  Cette option va installer un serveur PXE (Preboot eXecution Environment).

  `pxelinux`

  `tftp`

  `tftp-server`

  `syslinux`

  `dhcp-server`

Bases de données

Insatllation de diverses bases de données relationnelles.

- Serveur MySQL.

  `mysql`

  `mysql-client`

  `phpmyadmin`

- Serveur PostgreSQL.

  `postgresql8.3-server`

  `postgresql8.3-pl`

  `phppgadmin`

- Serveur MySQL-Max

  Serveur MySQL alternatif, compilé avec le support de fonctionnalités avancées (tables transactionnelles, etc.).

  `mysql-Max`

  `mysql-client`

  `phpmyadmin`

- SQLite

Outils en ligne de commandes pour manager la librairie libsqlite.

`sqlite-tools`

`phpsqliteadmin`

Serveur de mail

Serveur de courrier électronique, avec accès POP/IMAP et Webmail.

- Serveur Postfix

  Serveur de mail

  `postfix`

- Anti-virus and anti-spam toolkits

  Installation de AMaVis, ClamAV and SpamAssassin.

  `amavisd-new`

  `spamassassin`

  `spamassassin-tools`

  `clamd`

- Serveur POP/IMAP

  Au choix:

  Serveur POP/IMAP Cyrus

  `cyrus-imapd`

  `cyrus-imapd-utils`

  `cyrus-sasl`

  `libsasl2-plug-plain` ou `lib64sasl2-plug-plain`

  `libsasl2-plug-login` ou `lib64sasl2-plug-login`

  Serveur POP/IMAP Dovecot

  `dovecot`

  `dovecot-plugins-ldap`

  Serveur POP/IMAP CourierImap

  `courier-imap`

  `courier-base`

- Serveur de mailing list

  Installation de Sympa.

`sympa`

- Serveur Webmail

  Installation du webmail roundcube.

  `roundcubemail`

  `sqlite-tools`

Serveur d'authentification

Un serveur LDAP ou Kerberos pour l'identification des utilisateurs.

- LDAP pour l'authentification des utilisateurs.

  OpenLdap pour l'authentification des utilisateurs.

  `openldap-servers`

  `nss_ldap`

  `openldap-clients`

  `pam_ldap`

  `openldap-mandriva-dit`

- Authentification Kerberos

  Serveur d'authentification Kerberos.

  `krb5-server`

  `krb5-workstation`

- Authentification LDAP + Kerberos

  Serveur d'authentification LDAP avec Kerberos.

  `openldap-servers`

  `nss_ldap`

  `openldap-clients`

  `pam_ldap`

  `openldap-mandriva-dit`

  `krb5-server`

  `krb5-workstation`

  `libsasl2-plug-gssapi` ou `lib64sasl2-plug-gssapi`

Serveur LAMP

Un ensemble d'outils libres pour héberger des sites web dynamiques.

- Serveur HTTP Apache

  Installation d'un Serveur Web.

  `apache-base`

  `apache-mpm-prefork`

  `apache-conf`

  `apache-modules`

  `apache-mod_ssl`

- Paquets de développement LAMP (PHP, Perl/CGI)

  Un ensemble d'outils libres pour héberger des sites web dynamiques (langages de script, php modules, ...).

  `apache-mod_perl`

  `apache-mod_php`

  `php-dom`

  `php-simplexml`

  `php-xml`

  `php-xmlrpc`

  `php-xsl`

  `php-cli`

  `php-mysql`

  `php-pgsql`

  `php-sqlite`

Outils de sauvegarde

Bacula est un ensemble de programmes qui vous permet de gérer vos sauvegardes, restaurations ou vérifications de données d'un ordinateur sur un réseau hétérogène.

La version incluse dans Mandriva Enterprise Server 5 est Bacula 3. Pour plus d'informations sur le projet, visitez le site officiel (`http://www.bacula.org`) .

"It comes by night and sucks the vital essence from your computers."

- Bacula Director

Le service Bacula Director est le programme qui supervise toutes les opérations de sauvegarde, restauration, vérification et archivage.

`bacula-common`

`bacula-dir-common`

`bacula-dir-mysql`

- Bacula Storage Daemon

  Bacula Storage Daemon Transfère les données et les attributs de fichiers aux média physiques ou aux volumes et les restitue lors de restaurations. Le storage Daemon est responsable des opérations de lecture et d'écriture sur vos cartouches (ou autres média de stockage).

  `bacula-sd`

- Bacula File Daemon

  Bacula File Daemon est l'application à installer sur les machines clientes à sauvegarder. Elle est chargée de fournir les attributs des fichiers et les données requis par le Director.

  `bacula-fd`

3.4. Limiter l'accès au Mandriva Server Setup

Après avoir configuré votre serveur avec le Mandriva Server Setup nous vous conseillons de limiter son accès étant donné que ce service peut accéder à des parties sensibles de votre système. Pour cela, deux méthodes peuvent être employées.

3.4.1. Désactiver le servive mmc-wizard

En désactivant le service mmc-wizard, vous empêchez quiquonque d'effectuer des opérations sur votre serveur via l'interface de configuration.

Pour désactiver le service vous pouvez utiliser le centre de contrôle Mandriva (MCC) en vous rendant dans la section Système->Gérer les services, ou bien en lancant depuis une ligne de commande en root, l'outil drakxservices. Arrêtez le service manuellement et décochez l'option "Au démarrage".

3.4.2. Interdire l'accès à l'interface Web de configuration depuis le réseau

Cette méthode à l'avantage de laisser le service mmc-wizard actif, mais il ne pourra être utilisé uniquement que depuis le serveur. Toute connection depuis un poste du réseau sera refusée.

Pour cela, éditez le fichier `/etc/httpd/conf/webapps.d/mmc-wizard.conf` et remplacez la ligne

```
Allow from all
```

par

```
Allow from 127.0.0.1
  Deny all
```

Chapitre 4. Auto-installation

4.1. Gestion de l'installation automatique

Mandriva Enterprise Server 5 vous offre une méthode d'installation automatisée. Elle reproduit un scénario d'installation donné, que vous pouvez personnalisé en tout ou en partie. Cette méthode vous propose donc de choisir le degré d'interactions voulu lors de l'installation. Cette section présente les fonctionnalités d'installation automatique de votre Mandriva Enterprise Server 5.

La documentation complète est disponible dans le paquetage `drakx-autoinstall-doc`. Il contient de la documentation détaillée sur la configuration de l'auto-installation et son utilisation.

La fonction d'installation automatisée de DrakX est contrôlée par le contenu du fichier `auto_inst.cfg`. Ce fichier se trouve généralement dans la disquette de démarrage. PXE peut aussi le fournir pour que vous puissiez installer automatiquement.

Le contenu du fichier `auto_inst.cfg` comprend une déclaration *Perl Scalar Structure (o)*. DrakX utilise généralement la déclaration `$o = {...};` pour prérégler certaines options et sélections. Entre les accolades ouverte et fermée se trouve une série de déclarations simples ou composées représentant vos sélections.

Lors d'une installation manuelle, les différentes déclarations sont créées et les champs appropriés sont remplis au fur et à mesure que vous faites vos choix. Ensuite, lorsque vous créez votre disquette Automatique ou Rejouée (*Replay*), des portions sélectionnées de cette structure sont simplement déposées sur un fichier, qui contrôlera les actions de DrakX lorsqu'une installation Automatique ou Rejouée sera faite.

Une installation automatique requiert que tous les choix soient présélectionnés en utilisant soit un fichier généré par DrakX, ou manuellement (par vous). Durant chaque installation, DrakX crée un modèle basé sur vos choix appelé `/root/drakx/auto_inst.cfg.pl`. Vous pouvez l'éditer et modifier certaines valeurs.

L'installation automatique vous permet de gérer:

- les partitions ;
- le choix de paquetages ;
- la configuration réseau ;

- la création d'utilisateurs ;
- l'authentification ;
- la configuration de X
- etc.

Vous pouvez aussi ajouter des actions supplémentaires à être exécutée une fois l'installation complétée. Pour ce faire, utilisez des commandes `bash`.

Voici un court extrait d'un fichier d'auto installation, à titre d'exemple.

```
$o = {
 'printer' => {
  'configured' => {}
},
 'default_packages' => [
  'kernel-2.6.12.26mdk',
  'vim-enhanced',
  'grub',
  'lilo',
  'vim-minimal',
  ...
  ]
  'net' => {
 'zeroconf' => {
  'hostname' => undef
 },
 'network' => {
  'NETWORKING' => 'yes',
  'DHCP' => 'yes',
  'NET_DEVICE' => 'eth0',
  'NET_INTERFACE' => 'eth0'
  },
  ...
  }
```

Dans cet exemple, les imprimantes ne sont pas configurées, ni zeroconf. Les choix de paquetages par défaut contiennent des paquetages comme `grub` et `vim-enhanced`. Le réseau est configuré à travers `dhcp` sur l'interface `eth0`.

Une fois que votre fichier est prêt, vous pouvez l'utiliser de différentes manières :

- en utilisant le CD ou le DVD d'installation et une disquette : copiez `auto_install.cfg` sur la disquette. Ensuite, démarrez avec un médium d'installation et la disquette. Au premier écran, tapez **F1** et à l'invite, utilisez cette commande : `linux kickstart=floppy`.
- en utilisant PXE : vous pouvez définir une image spécifique pour qu'elle prenne en compte le fichier d'auto-installation. Par exemple : le serveur PXE et les données sont stockés sur un partage NFS.

Vous devriez ensuite copier `auto_install.cfg` dans le répertoire `install` de votre dépôt. Vous pouvez le renommer `testauto`, par exemple. Puis, si le client utilise l'image `mes5auto`, il utilisera automatiquement le fichier d'auto-installation sans utiliser d'autre média.

Vous pouvez facilement vérifier la syntaxe de `auto_inst.cfg.pl` en utilisant un outil de vérification perl. Utilisez la commande suivante :

```
# perl -cw /root/drakx/auto_inst.cfg.pl
auto_inst.cfg.pl syntax OK
```

Administrer les services sur Mandriva Enterprise Server 5

Mandriva Enterprise Server 5 propose un certain nombre d'outils graphiques qui vous apporteront une aide précieuse pour la configuration du système et des services. Nous vous présentons rapidement deux d'entre eux : Centre de contrôle Mandriva Linux et Mandriva Server Setup. L'objectif de ce chapitre est d'approfondir la configuration du système et des services peu importe le mode de gestion (outil graphique ou ligne de commande).

1. Utiliser le Centre de contrôle Mandriva

Le Centre de contrôle Mandriva Linux permet à l'administrateur système de configurer le matériel et les services utiles à tous les utilisateurs.

Accédez au Centre de contrôle Mandriva Linux par le menu principal dans Système+Configuration→Configurer votre ordinateur.

Quelques outils du Centre de contrôle Mandriva Linux sont aussi accessibles par la ligne de commande en mode texte en lançant `drakconf`.

Figure 1. Fenêtre principale du centre de contrôle

Voici maintenant quelques-unes des entrées de menu disponibles :

- **Options→Affichage des journaux.** Cette option permet d'afficher une fenêtre Actions des outils au bas de la fenêtre principale. Ce cadre affichera toutes les actions prises par les différents outils de configuration lancés depuis le Centre de contrôle Mandriva Linux.
- **Options→Mode expert.** Vous donne accès aux outils avec des options plus avancées.
- **Profils.** Vous permet de sauvegarder des profils de configuration.
- **Aide→Aide.** Ouvre le navigateur d'aide et affiche de la documentation sur cet outil de configuration.
- **Aide→Signaler un bogue.** Ouvre un dialogue pour vous permettre de signaler une erreur à l'équipe de développement.

Les outils sont classés selon différentes catégories. Nous citons ci-dessous tous les outils avec la référence vers la section du manuel correspondante.

D'autres catégories apparaissent si le paquetage drakwizard est installé. La documentation pour ces assistants est intégrée. Ces assistants permettent une configuration de base des services LAN les plus courants, comme les serveurs Web ou FTP, les serveurs de courriers et de base de données.

Chapitre 5. Système de base

Paramétrer un serveur Mandriva Enterprise de base

L'objectif de ce chapitre n'est pas de refaire une revue complète des bases du fonctionnement d'un système GNU/Linux, mais plutôt, de vous faire découvrir les nouvelles fonctionnalités et les points clés de votre système Mandriva Enterprise Server 5. La définition du système de base repose sur le schéma qui sous-tend l'architecture de la distribution.

Ce chapitre traite d'outils de geston de paquetages (Section 5.1), de l'implantation de machines virtuelles à travers une virtualisation (Section 5.3), et la répartition de charge (Section 5.2).

5.1. Outils de gestion des logiciels

Une fois l'installation de votre serveur complété, vous aurez sans doute besoin d'installer ou d'enlever des logiciels. Avec Mandriva Enterprise Server 5, vous avez 2 options pour accomplir ces tâches : en mode graphique avec Rpmdrake (voir Section 5.1.4) ou en mode texte. La dernière option se compose de urpmi pour l'installation et la mise à jour, de urpme pour retirer des paquetages RPM, `urpmf` et `urpmq` pour faire des recherches dans la base de données RPM. Ces logiciels sont également la fondation dernière Rpmdrake.

5.1.1. Configuration d'un dépôt local

Afin de se faciliter les installations de paquetages logiciels, il est possible de créer un dépôt de paquetages directement sur le disque dur de votre serveur.

Pre-requis

- Vous devez disposer d'un espace disque de minimum 3 Go.
- Vous devez disposer du CD/DVD d'installation.

5.1.1.1. Configuration d'un dépôt local en mode graphique

Voici comment procéder pour configurer un dépôt local avec des outils graphiques.

- Insérer le CD/DVD d'installation.
- Une icône représentant le media apparaît sur le bureau. Double-cliquer sur celle-ci pour explorer le contenu du DVD.
- Copier le répertoire `i586` (ou `x86_64`) sur votre disque dur à l'emplacement désiré.
- Une fois que la copie est terminée, lancer le Centre de Contrôle Mandriva Linux.

Figure 5-1. Le Centre de Contrôle Mandriva Linux

- Cliquer sur Configurer les sources pour installer et mettre à jour les logiciels
- Dans Fichier, choisir Ajouter un media personnalisé.

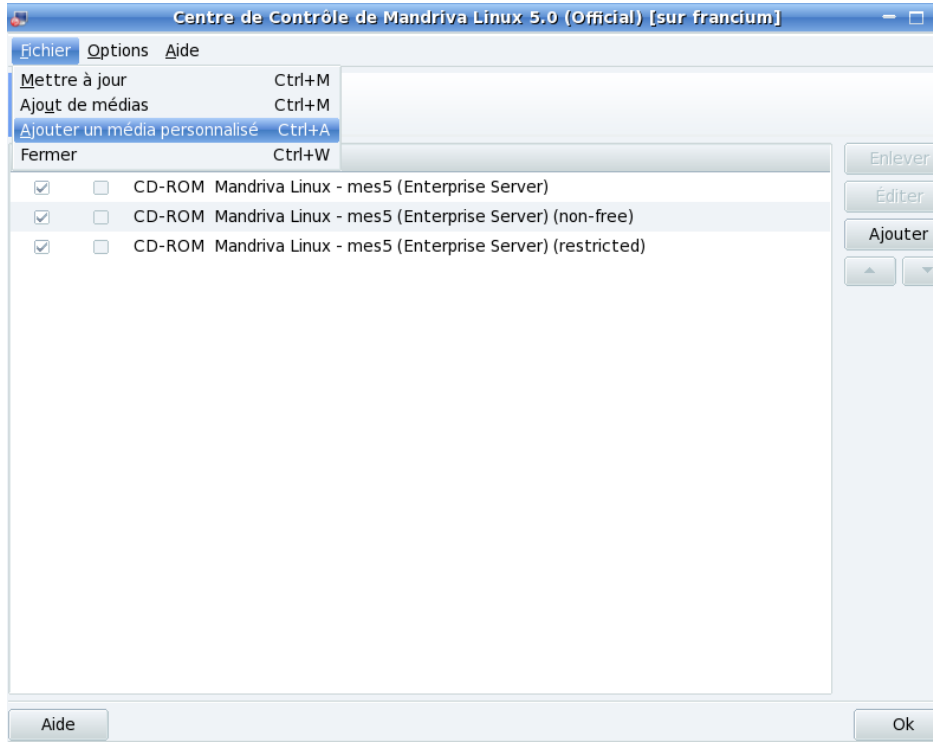


Figure 5-2. Ajout de dépôts

- Remplir les champs.

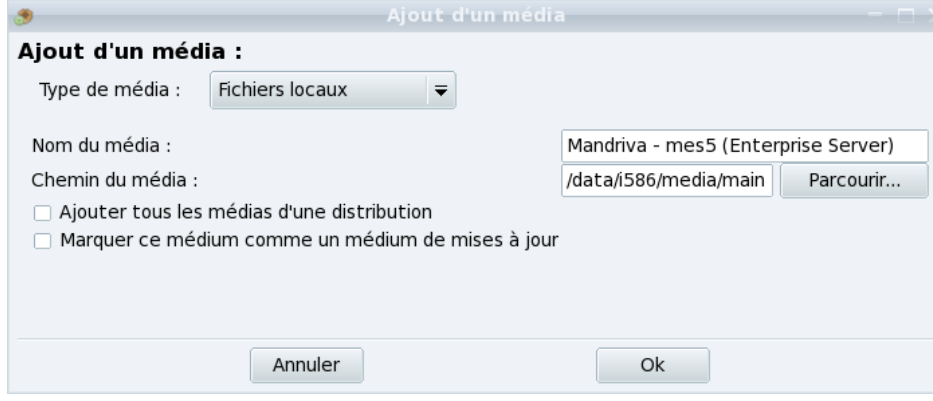


Figure 5-3. Ajout d'un dépôt personnalisé

Il y a 3 dépôts à configurer :

- media main

nom du media : Mandriva - mes5 (Enterprise Server)

Chemin du media : `/data/i586/media/main/`

- media non-free

nom du media : Mandriva - mes5 (Enterprise Server) non-free

Chemin du media : `/data/i586/media/non-free/`

- media restricted

nom du media : Mandriva - mes5 (Enterprise Server) restricted

Chemin du media : `/data/i586/media/restricted/`

Dans notre exemple, le répertoire `i586` du DVD a été copié dans `/data`

- Désactiver les medias CDROM : décocher la case activé.

5.1.1.2. Configuration d'un dépôt local en mode ligne de commande

Voici comment procéder pour configurer un dépôt local en ligne de commande.

- Insérer le CD/DVD d'installation.
- Le CD/DVD est monté dans `/mnt/cdrom`
- Copier le répertoire `i586` (ou `x86_64`) sur votre disque dur (par exemple dans `/data`):

```
cp -r /media/cdrom/i586 /data/
```

- Supprimer les anciens media:

```
urpmi.removemedia -a
```

- Ajouter les medias:

```
urpmi.addmedia "Mandriva - mes5 (Entreprise Server) main" file://data/i586/media/
urpmi.addmedia "Mandriva - mes5 (Entreprise Server) non-free" file://data/i586/me
urpmi.addmedia "Mandriva - mes5 (Entreprise Server) restricted" file://data/i586/
```

- Mettre à jour les medias ajoutés:

```
urpmi.update -a
```

5.1.2. Installation et mise à jour de RPM avec urpmi

5.1.2.1. Notions de base

Le but principal de urpmi est de simplifier le téléchargement et l'installation de paquetages RPM. Les logiciels RPM contiennent souvent des dépendances : urpmi reconnaît ces dépendances, télécharge les paquetages requis et retire les paquetages déjà installés susceptibles d'entrer en conflit.

urpmi récupère la liste des RPM disponibles et les RPM à partir d'un média source. Pour simplifier, un média source se décrit par un nom et une location spécifiée par un URL. Actuellement, les médias supportés incluent les disques locaux, des disques amovibles tels que des CD, des images ISO, et des médias réseau via différents protocoles (http, ftp, ssh et rsync). Les partitions réseau montées via NFS sont traitées comme des disques locaux.

5.1.2.2. Installer des RPM

Voici les options des base de urpmi:

```
urpmi <liste de noms de RPM>
```

Cette commande demande à urpmi d'aller chercher et d'installer tous les paquetages et leurs dépendances à partir du média configuré. Dans ce processus, urpmi peut demander des questions. Par exemple, si un paquetage déjà installé a besoin d'une mise à jour, urpmi vous demandera d'accepter cette mise à jour. Si certains paquetages doivent être retirés (à cause de conflit avec le RPM que vous voulez installer), vous devrez aussi le confirmer. Dans certains cas, urpmi vous proposera également des choix entre différentes alternatives, habituellement la « meilleure » proposition sera choisie par défaut.

Une autre fonctionnalité très utile de urpmi est de mettre à jour tous les paquetages à la dernière version disponible sur le média. Pour ce faire, utilisez la commande suivante :

```
urpmi --auto-update
```

urpmi peut également installer des fichiers RPM directement. Plutôt que d'utiliser `rpm -i foobar.rpm`, vous pouvez passer le chemin du fichier RPM à urpmi et celui-ci tentera de résoudre les dépendances requises :

```
urpmi /home/user/foobar.rpm
```

Voici quelques options utiles pour urpmi :

--auto

Mode automatique : urpmi ne pose pas de question et choisit toujours la sélection par défaut.

--test

Pour tester l'installation de paquetages sans installer ou modifier le système.

--media *media1,...,mediaN*

Cette option force urpmi à utiliser le média spécifié, plutôt que la sélection par défaut (tous les médias). Vous pouvez également utiliser une sous-chaîne de caractères afin que urpmi utilise tous les médias contenant cette sous-chaîne dans leur nom. Par exemple, `urpmi --auto-update --media sous-chaîne` cherchera des mises à jour sur des médias contenant « update » dans leur nom.

Consultez le *man page* de `urpmi(8)` pour plus d'informations.

5.1.2.3. Gestion des médias avec urpmi

5.1.2.3.1. Ajouter un média

urpmi est utilisable seulement lorsqu'au moins un média est défini. Habituellement, l'installation du système configure une sélection prédéfinie de médias, correspondant à la méthode d'installation utilisée : les CD d'installation, un serveur HTTP ou FTP si vous installez depuis un réseau. Pour ajouter des médias, utilisez `urpmi.addmedia` :

```
urpmi.addmedia [options] <name> <url> [with hdlist]
```

Dans cet exemple, <name> est le nom du nouveau média, <url> est l'URL où se trouvent les RPM, et le paramètre « with » permet de spécifier le fichier de description du contenu du média.

Les URL supportées peuvent être : `http://`, `ftp://`, `rsync://`, `ssh://` (qui utilisera `rsync` sur `ssh`), `file://`, et `removable://`. `removable://` fonctionne comme `file://`, en indiquant à urpmi que le répertoire est monté à partir d'un média amovible comme un CD ou un DVD. Si le média requiert une authentification, vous pouvez utiliser la syntaxe usuelle URL :

```
<scheme>://<login>:<pass>@host/path
```

Ces informations ne seront pas conservées dans un fichier humainement lisible.

Dans certains cas, si votre média pointe vers un serveur HTTP ou FTP externe, vous aurez peut-être besoin de passer par un mandataire (*proxy*). Utilisez les options `--proxy` et `--proxy-user`, la seconde étant requise si votre serveur nécessite une authentification.

5.1.2.3.2. Supprimer un média

Il s'agit d'un opération très simple. Pour supprimer un média nommé `foo`, utilisez simplement la commande :

```
urpmi.removemedia foo
```

5.1.2.3.3. Mise à jour des médias

Certains médias ne changent jamais, le CD-ROM par exemple. Par contre, d'autres médias, typiquement les mises à jour, sont en croissance. De nouveau RPM sont ajoutés et les obsolètes sont retirés. En conséquence, avant de les utiliser, vous devez indiquer à urpmi que leur contenu peut avoir été changé.

Pour ce faire, utilisez le programme `urpmi.update`. Vous pouvez mettre à jour tous les médias :

```
urpmi.update -a
```

Vous pouvez également spécifier le média à mettre à jour :

```
urpmi.update updates-one updates-two
```

5.1.2.3.4. Créer votre propre média

La façon la plus simple de créer votre propre média consiste à laisser `urpmi.addmedia` le faire pour vous. Par contre, cette procédure fonctionnera seulement si vous avez un petit nombre de RPM sur votre disque ou sur un disque réseau partagé par NFS. Pour ce faire, en assumant que vos RPM sont dans un répertoire `/var/my-rpms`, tapez la commande :

```
urpmi.addmedia my-media /var/my-rpms
```

Pour un média contenant une vaste quantité de RPM ou si vous voulez placer votre média sur un serveur partagés, vous devrez utiliser l'outil `gendistrib`. Celui-ci est disponible dans le paquetage rpmtools. Il génère un arbre miroir pour un ou plusieurs médias.

Un dépôt média typique, sous le répertoire racine /ROOT/, possède la structure suivante (nous avons 2 médias, nommés « first » et « second ») :

```
ROOT/ - media/
|- first/
|   `- media_info/
|- second/
|   `- media_info/
`- media_info/
```

Les RPM sont placés dans les sous-répertoires first et second. Le dépôt de métadonnées est conservé dans le répertoire de premier niveau media_info. Les métadonnées par média sont contenues dans les sous-répertoires first/media_info et second/media_info.

Les métadonnées par média sont composées d'un fichier hdlist.cz contenant une en-tête compressée (*gzipped*) des RPM du média, un fichier synthesis.hdlist.cz (beaucoup plus petit que hdlist) contenant seulement les informations nécessaires à urpmi pour résoudre les dépendances, et si nécessaire, un fichier pubkey si les RPM sont signés (pour que urpmi puisse vérifier que les RPM qu'il télécharge sont signés avec la clé associée à ce média.)

Avant d'utiliser gendistrib, vous devez créer un fichier media_info/media.cfg pour décrire ce dépôt. La syntaxe de ce fichier rappelle celle d'un fichier .ini. Il contient un fichier par média

```
[first] hdlist=hdlist_first.cz name=First
    supplementary media
```

Dans l'exemple précédent, first est le répertoire, hdlist_first.cz est le nom du fichier hdlist qui sera créé (il devra se terminer par .cz), et name= donne une description du média.

Ensuite, vous pouvez lancer gendistrib. Vous devriez lui passer comme paramètre le répertoire /ROOT/. Il générera ensuite les fichiers hdlist et synthesis et tous les autres fichiers requis pour l'opération adéquate d'un dépôt.

Pour en savoir plus, consultez la *man page* gendistrib(1).

5.1.2.4. Commande d'installation en parallèle : urpmi-parallel

urpmi-parallel est un ajout utile à urpmi pour installer des paquetages sur plusieurs hôtes d'un réseau. Il lance une commande urpmi en parallèle sur un nombre défini de clients. Plus précisément, la machine sur laquelle vous lancez la commande (le serveur) teste les résultats sur chaque machine du groupe (les clients) un par un, télécharge les paquetages nécessaires pour

chaque machine, distribue les paquetages appropriés à chaque machine, puis appelle urpmi sur la machine pour effectuer l'installation.

urpmi doit être installé sur chaque client, mais il n'est pas nécessaire que chaque client ait un média défini.

Pour l'utiliser :

1. Assurez-vous de pouvoir utiliser `ssh` vers chaque client (vous pouvez utiliser `ssh-add` sur le serveur pour éviter d'enter votre mot de passe chaque fois).
2. Installez urpmi-parallel-ssh ou urpmi-parallel-ka-run sur le serveur. Le premier *plugin* utilise simplement `ssh` pour distribuer des commandes aux clients, alors que le second utilise `ka-run`, une méthode de parallélisation efficace que vous pouvez utiliser avec `rsh` ou `ssh`, qui est bien adaptée au grappe de serveurs.
3. Éditez `/etc/urpmi/parallel.cfg` afin d'obtenir quelque chose de similaire à :

   ```
   mynetwork:ssh:host1:host2:host3
   ```

   Sur cette ligne, `mynetwork` est le nom de l'alias que vous allez utiliser pour spécifier le réseau à urpmi; `ssh` est la méthode d'installation (pour utiliser ka-run, vérifier l'entrée pour `/etc/urpmi/parallel.cfg` dans urpmi.files(5)), et `hostN` sont les noms des clients sur votre réseau. Vous pouvez mettre `localhost` dans cette liste.
4. Lancez la commande urpmi: par exemple, pour installer « package_name »:

   ```
   urpmi --parallel mynetwork package_name
   ```

5.1.2.5. urpmi restreint

urpmi possède un équivalent plus sûr : `rurpmi`. Il est très similaire à urpmi, et possède une gamme de fonctionnalités limitées. Il a été conçu pour être utilisé par des usagers n'ayant pas les droits d'administration `root`, mais plutôt les privilèges `sudo` seulement. Ceci prévient les abus pouvant compromettre le système.

La syntaxe de `rurpmi` est similaire à urpmi, mais prévient l'installation arbitraire de RPM. Ils doivent provenir d'une source média enregistrée. Aussi, certaines options dangereuses sont également interdites. Consultez le *man page* de `rurpmi(8)` pour en avoir la liste.

5.1.2.6. Supprimer des RPM avec urpme

L'outil pour désinstaller des RPM se nomme urpme. Par exemple :

```
urpme <liste des paquetages>
```

Cette commande tentera de supprimer tous les paquetages listés ainsi que leurs dépendances. Il refusera de désinstaller les paquetages « importants » (faisant partie du système de base, par exemple).

Voir la *man page* de `urpme(8)` pour connaître toutes les options prises en charge par urpme.

Notez que urpme n'est pas en mesure de détecter des paquetages inutiles. Par exemple, une bibliothèque qui n'est pas utilisée. Pour faire du nettoyage, `rpm-find-leaves` est un outil pratique. Il affichera tous les RPM présents sur votre système qui ne sont requis par aucun autre paquetage.

5.1.3. Rechercher des paquetages avec urpmf and urpmq

5.1.3.1. urpmf

`urpmf` est une sorte de `grep` pour la base de données de urpmi (la BD de tous les RPM d'un média). Par défaut, il cherchera dans les noms de fichiers contenus sur un média, mais une variété d'options permettent des recherches avancées.

Par exemple, pour trouver tous les paquetages commençant par `apache-` :

```
urpmf --name '^apache-'
```

Le `^` est l'indicateur de début de ligne standard utilisé dans les expressions régulières.

Pour trouver tous les paquetages contenant des fichiers dont le nom contient `/etc/httpd.conf.d` :

```
urpmf /etc/httpd.conf.d
```

Pour trouver tous les paquetages qui fournissent `mail-server` avec leur version et leur numéro (**-f**) :

```
urpmf --provides -f mail-server
```

Consultez la *man page* de `urpmf(8)` pour plus d'exemples et la liste de toutes les options.

5.1.3.2. urpmq

L'outil `urpmq` permet de rechercher dans la base de données de urpmi. Il permet plusieurs modes d'opération, en voici quelques-uns particulièrement intéressants :

```
urpmq -i package
```

Affiche les informations de ce paquetage (comme `rpm -qi` pour un paquetage installé). L'option `--summary` est similaire, mais retourne l'information résumée en une ligne.

```
urpmq --source package
```

Retourne l'URL d'origine du paquetage.

```
urpmq -d package
```

Affiche la liste de tous les RPM requis par le paquetage spécifié (récursivement).

Inversement, `urpmq -R package` donne la liste des RPM qui requiert le paquetage sélectionné.

Référez-vous à la *man page* de `urpmq(8)` pour en connaître toutes les options.

5.1.4. Gestion des logiciels avec Rpmdrake

La gamme d'outils urpmi est conçue pour le mode texte. Vous pouvez également utiliser l'outil en mode graphique Rpmdrake. Il se compose de plusieurs parties accessibles en choisissant une des entrées du menu principal Système+Configuration+Paquetages ou directement en cliquant sur Gestionnaire de logiciels dans le Mandriva Linux Control Center.

Figure 5-4. Gestion d'applications dans le Centre de contrôle Mandriva Linux

Nous vous recommandons d'accéder à Rpmdrake via le Mandriva Linux Control Center.

5.1.4.1. Installer des logiciels

Au démarrage, Rpmdrake effectue une recherche dans la base de données de paquetages disponibles. Puis, l'interface Installation de paquetages logiciel s'affiche.

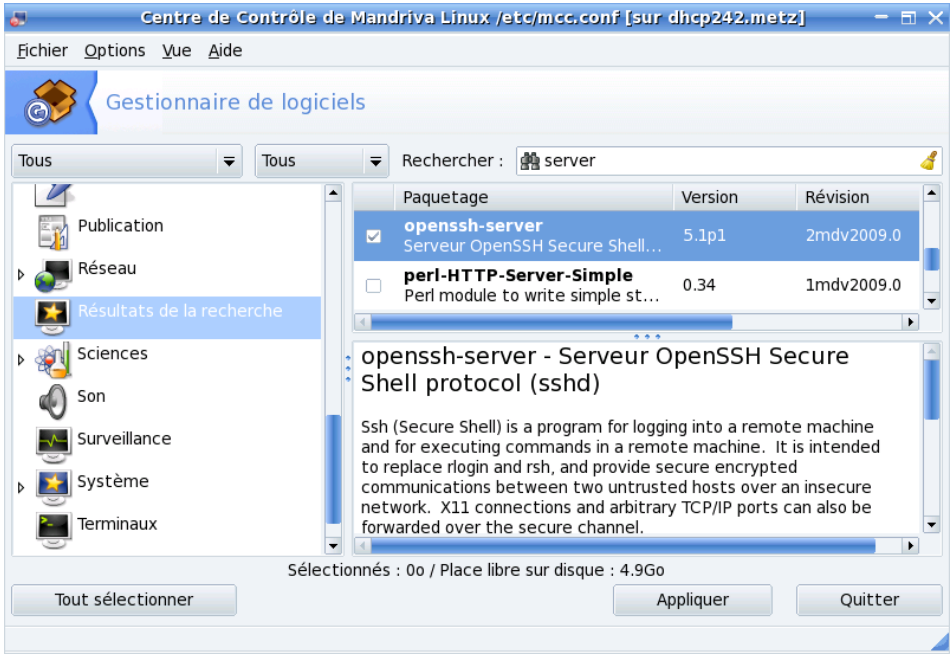


Figure 5-5. Installation des paquetages logiciels

La fenêtre se divise en quatre zones : la partie supérieure offre plusieurs options pour afficher la liste des paquetages disponibles. Cette liste se trouve au milieu à gauche. À sa droite s'affiche la description du paquetage sélectionné. Enfin, le bas de la fenêtre comprend la barre d'état avec deux boutons et des informations sur la taille des paquetages sélectionnés par rapport à la place disponible sur votre système.

De plus, une barre d'état située dans la partie inférieure de la fenêtre affiche des messages concernant les actions en cours ou complétées.

5.1.4.1.1. Sélection des paquetages à installer

Dans, Figure 5-5, le paquetage nommé `samba-3.2.7-0.3mdv2009.0` est sélectionné dans la vue arborescente. Dans la zone de description, on retrouve l'espace disque nécessaire, un intitulé (« Samba (SMB) server programs »), suivi d'une description détaillée. Remarquez que la description peut être en anglais.

Si vos médias de sources de paquetages sont configurés pour utiliser les listes complètes de paquetages (et non pas les fichiers de résumé `synthesis` : le format complet `hdlist` est cependant utilisé par défaut), vous pouvez obtenir plus d'informations sur un paquetage en cochant Informations maximales. De plus, les fichiers contenus dans ce paquetage ainsi que l'historique des modifications (*changelog*).

La barre d'état vous informe de l'espace disque requis pour l'installation des paquetages que vous avez sélectionnés ainsi que l'espace disponible. Remarquez que l'espace requis peut être supérieur à la taille du paquetage en lui-même. Ceci est dû à la nécessité d'installer ses dépendances.

Rpmdrake affichera un avertissement si vous tentez d'installer plus de paquetages que l'espace disque ne le permet. Vous pouvez néanmoins continuer après avoir effacé du disque des fichiers dont vous n'avez plus besoin.

Lancez l'installation en cliquant sur Installer. Une nouvelle fenêtre apparaît montrant la progression du processus d'installation. Si vous préférez quitter en n'installant aucun logiciel, utilisez Quitter.

Pendant la sélection, il se peut que vous choisissiez un paquetage qui a lui même besoin d'autres paquetages (bibliothèques ou autres nécessaires à son bon fonctionnement). Dans ce cas, Rpmdrake affiche un avertissement présentant la liste des paquetages nécessaires (dépendances). Vous pouvez soit accepter, soit Annuler l'installation (Figure 5-6).

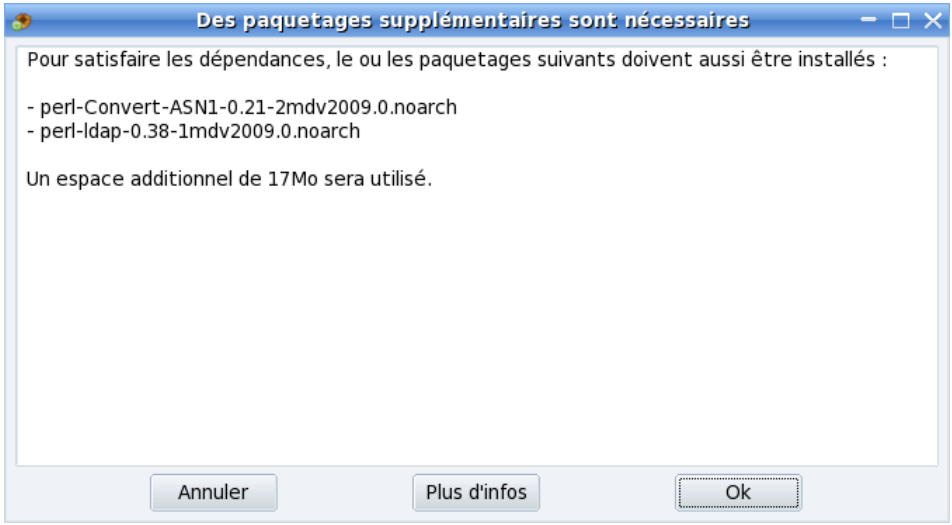


Figure 5-6. Rpmdrake — alerte de dépendances

Il peut aussi arriver que plusieurs paquetages différents soient en mesure de fournir une même dépendance. La liste de tous les choix susceptibles de convenir vous sera alors proposée. Lisez les descriptions des options en cliquant sur les boutons Info et choisissez celui qui vous semble convenir le mieux.

Nous allons maintenant voir les fonctionnalités de recherche et de tri facilitant votre tâche d'administrateur :

5.1.4.1.2. Recherche d'un paquetage

Pour trouver un logiciel, entrez le nom (entier ou partiel), ou un mot en rapport avec ce paquetage dans le champ à côté du bouton Chercher. Puis choisissez où vous pensez que ce mot peut se trouver (dans le nom du paquetage, sa description, ou parmi les noms des fichiers contenus dans le paquetage). Cliquez sur Chercher et une nouvelle liste (Résultats de la recherche) apparaît, vous affichant les résultats que Rpmdrake a trouvés en interrogeant la base de données de paquetages.

Les différents choix de recherche sont :

Choix Mandriva Linux

> Cette présentation reprend celle utilisée lors de l'installation de Mandriva Linux. C'est la plus facile, car seulement les paquetages jugés les plus utiles de la distribution seront affichés.

Tous les paquetages, classement alphabétique

Au lieu d'une vue arborescente, une liste de tous les paquetages disponibles est présentée.

Tous les paquetages, par groupe

Arborescence de tous les paquetages triés par groupe fonctionnel (jeux, système, vidéo, etc).

Tous les paquetages, par taille

Vous obtenez une liste des paquetages triés par taille.

Tous les paquetages, sélectionnés ou non

Cette présentation est une liste plate où tous les paquetages sélectionnés pour l'installation apparaissent en premier, puis viennent les autres paquetages.

Tous les paquetages, par média

Une arborescence dans laquelle les paquetages sont classés selon le média auquel ils appartiennent (voir Section 5.1.4.4).

Tous les paquetages, nouveaux ou mis à jour

Dans ce mode, vous obtenez deux branches (si des mises à jour sont disponibles) : la première donne la liste des paquetages disponibles à l'installation, la deuxième affiche les paquetages installés pour lesquels une mise à jour est disponible.

5.1.4.2. Suppression de logiciels

Cette interface est identique à celle que nous venons de voir pour l'installation des paquetages (Section 5.1.4.1), donc nous ne répéterons pas ici ses fonctions de bases.

5.1.4.3. Mise à jour Mandriva Linux

Lorsque vous lancez Mandriva Linux Update, il vous demande en premier lieu de choisir un « dépôt » sur Internet pour aller chercher les mises à jour. Choisissez-en un situé dans un pays près du vôtre.

Une légère différence par rapport à l'interface d'« installation de paquetages » est que vous pouvez choisir quelle sorte de mise à jour vous souhaitez installer en les groupant de certaines façons. Vous pouvez sélectionner :

Mises à jour de sécurité

Elles règlent des problèmes de sécurité et doivent être installées en priorité.

Corrections de bogues

Elles abordent des problèmes de comportement des applications.

Mises à jour normales

Elles n'apportent que des améliorations mineures.

L'autre différence est la zone de texte supplémentaire (Raison de la mise à jour) sous la description du paquetage. Elle fournit des informations sur la raison de cette mise à jour. Cela peut vous aider à décider si telle ou telle mise à jour est utile ou non. C'est particulièrement utile si vous avez une connexion Internet lente ou si vous payez au volume transféré.

5.1.4.4. Le gestionnaire des médias

Cette partie de Rpmdrake est dédiée à la définition des médias de paquetages disponibles. Comme vous pouvez le voir dans Figure 5-7, certains médias sont déjà disponibles : « Main », « Contrib », etc. Avec cet outil, vous pouvez ajouter d'autres médias logiciel : un CD que vous avez récupéré contenant des RPM, un média réseau sur Internet, etc.

Figure 5-7. Le gestionnaire de médias

Les cases à cocher sur la gauche vous permettent de désactiver temporairement un média : lorsque la case n'est plus cochée, les paquetages de ce média n'apparaîtront plus dans l'interface d'installation ou de mise à jour des paquetages logiciel.

Activé?

> Décochez cette boîte pour désactiver temporairement le média correspondant. Les paquetages que ce média contient ne pourront pas être installés à moins que vous ne réactiviez ce média.

M.à.J.?

> Cette boîte doit être cochée à côté du média de mise à jour, c'est-à-dire celui qui contient les paquetages de mise à jour. Ainsi, seuls les médias de mise à jour seront pris en compte lorsque vous chercherez des mises à jour.

Différentes actions peuvent être réalisées sur les médias via plusieurs boutons.

Supprimer

Permet de supprimer un média que vous ne souhaitez plus utiliser. Sélectionnez le média à enlever de la liste, puis cliquez sur ce bouton.

Éditer

Permet de changer les paramètres du média sélectionné, comme l'URL ou le chemin relatif vers le fichier `synthesis/hdlist`.

Vous pouvez paramétrer un média afin qu'il soit accessible par l'intermédiaire d'un mandataire spécifique en cliquant sur Mandataire. Vous pouvez aussi définir un mandataire global pour tous les médias distants en cliquant sur Mandataire depuis l'interface principale.

Cette option permet aussi de passer des fichiers `hdlist` aux fichiers `synthesis`.

Les fichiers de synthèse ne contiennent que le nom du paquetage, ses dépendances et un court résumé : vous ne pourrez pas, par exemple, faire de recherches sur les fichiers fournis par un paquetage non installé, ou consulter sa description complète.

Ajouter

Ce bouton permet d'ajouter toutes les sources officielles de paquetage à partir de dépôts Internet. Cette option est pratique si vous avez une connexion Internet rapide ou si vous avez seulement le premier CD d'installation sous la main. Choisissez un miroir situé à proximité près de chez vous.

Une fois que vous avez choisi votre miroir et cliquez sur OK, l'information relative aux paquetages de la source choisie est téléchargée et vous pouvez installer ou mettre à jour tous les paquetages abrités par cette source média.

Ajouter la source personnalisée

Permet d'accéder à une nouvelle fenêtre pour ajouter un nouveau média.

Mettre à jour

Vous obtiendrez une liste de tous les médias configurés. Vous pourrez ainsi choisir ceux que vous souhaitez mettre à jour : cliquez sur le bouton Mettre à jour pour lancer la mise à jour. Ceci est notamment utile pour les médias distants auxquels sont ajoutés de nouveaux paquetages.

Gérer les clés

Il est important que les nouveaux paquetages logiciel que vous installez soient authentifiés. Pour cela, chaque paquetage peut être signé électroniquement avec une « clé », et vous pouvez autoriser/interdire des clés pour chaque média. Sur Figure 5-8, vous pouvez voir que la clé de Mandriva Linux est autorisée pour le média « Installation CD ». Cliquez sur Ajouter une clé pour autoriser une autre clé pour ce média (attention, procédez avec précaution, comme pour toutes les questions relatives à la sécurité de votre système), et sur Supprimer une clé pour enlever la clé du média sélectionné.

Comme avec toutes les questions reliées à la sécurité, assurez-vous de bien savoir de quoi il en retourne avant d'enlever des clés.

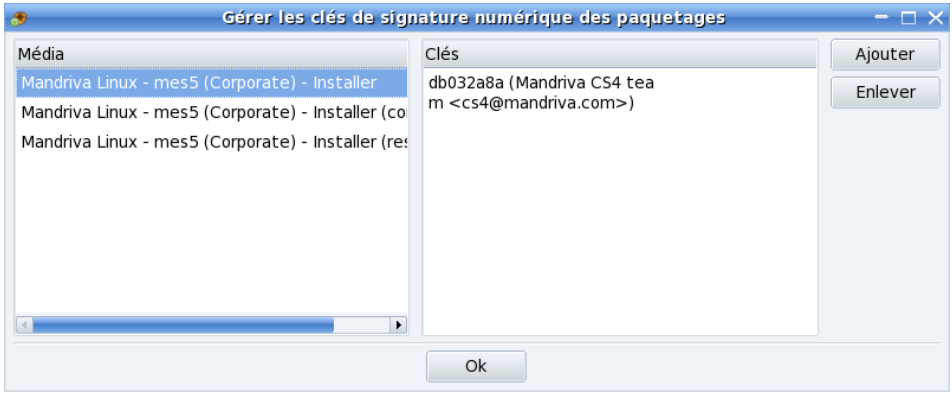


Figure 5-8. Rpmdrake — gestion des clés

Mandataire

Si votre ordinateur est placé derrière un pare-feu, mais que vous souhaitez néanmoins utiliser les possibilités qu'offre Rpmdrake d'accéder à des médias sur Internet (pour les mises à jour notamment), il peut être nécessaire de passer par un serveur mandataire (ne serait-ce que pour l'accès à certains serveurs de paquetages). Remplissez le champ Nom du serveur mandataire et éventuellement les Nom d'utilisateur et mot de passe pour se connecter au mandataire. Confirmez alors votre configuration en cliquant sur OK.

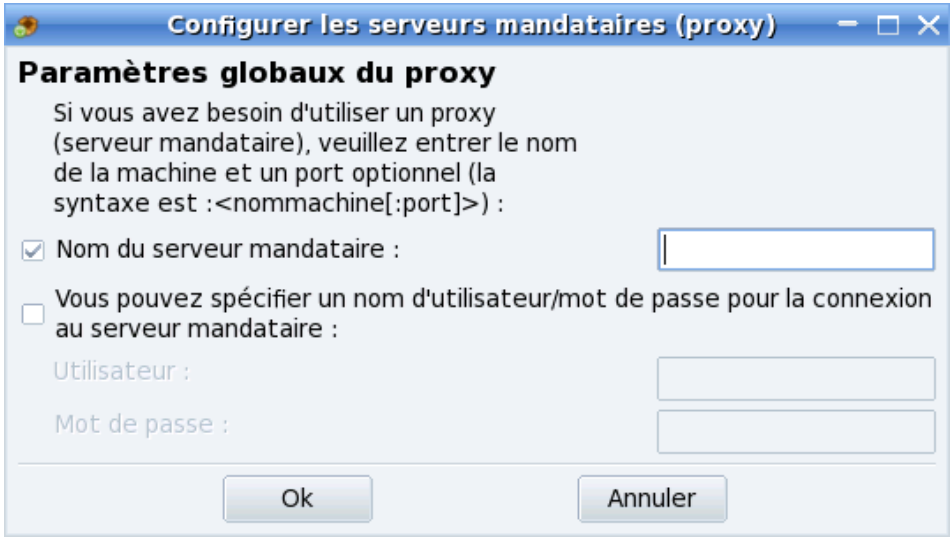


Figure 5-9. Rpmdrake — configurer un mandataire

Parallèle

Si vous utilisez un grand réseau d'ordinateurs, vous pouvez souhaiter installer un paquetage logiciel sur tous les ordinateurs, en parallèle ; ce bouton ouvrira une fenêtre vous permettant de configurer le mode « Parallèle ». Consultez la *man page* pour plus d'informations à propos du mode parallèle.

Options générales

Cette boîte de dialogue permet de changer d'utilitaire de téléchargement des nouveaux paquetages, et de désactiver la vérification des paquetages par rapport aux clés de chiffrement. Ces choix sont utilisés pour toutes les sources.

Flèches haut et bas

Ces boutons permettent de changer l'ordre dans lequel les sources sont prises en compte lorsque le système essaye d'installer un paquetage.

Pour les utilisateurs avancés

Rpmdrake traite le fichier de configuration de urpmi (`/etc/urpmi/urpmi.cfg`) de haut en bas pour obtenir la liste de sources média et les paquetages que chaque source abrite.

Si un fichier donné apparaît dans plus d'un média et que les versions diffèrent, le paquetage le plus récent sera installé, ignorant les autres.

Si un paquetage se retrouve dans deux médias et que la version du paquetage est la même, seulement le paquetage apparaissant dans la première source listée dans `urpmi.cfg` sera utilisé, ignorant les autres.

Quoi qu'il en soit, vous ne manquerez pas les paquetages disponibles.

Rpmdrake traite le fichier de configuration de urpmi (`/etc/urpmi/urpmi.cfg`) de haut en bas pour obtenir la liste de sources média et les paquetages que chaque source abrite.

Si un fichier donné apparaît dans plus d'un média et que les versions diffèrent, le paquetage le plus récent sera installé, ignorant les autres.

Si un paquetage se retrouve dans deux médias et que la version du paquetage est la même, seulement le paquetage apparaissant dans la première source listée dans `urpmi.cfg` sera utilisé, ignorant les autres.

Quoi qu'il en soit, vous ne manquerez pas les paquetages disponibles.

5.1.4.5. Gestion des groupes d'ordinateurs

5.1.4.5.1. Définition des groupes

Le mode parallèle de Rpmdrake permet de gérer les paquetages de manière globale sur tout un groupe de machines. Cela simplifie sensiblement l'administration d'un grand nombre de machines comme un réseau local. Assurez-vous que les paquetages `park-rpmdrake`, `urpmi-parallel-ssh` et `urpmi-parallel-ka-run` sont installés.

Cet outil n'est disponible qu'en mode expert. Choisissez le menu Options→Mode expert puis rendez-vous dans la section Gestionnaire de logiciels du Centre de contrôle Mandriva Linux.

Une fois l'application ouverte, utilisez le bouton Nouveau groupe pour créer un nouveau groupe de machines : choisissez lui un Nom, sélectionnez le Protocole à utiliser (`ssh` dans notre exemple), puis cochez les réseaux à scanner (pour détecter les machines) ou ajoutez de nouveaux réseaux (par défaut, seul le réseau local est listé). Cliquez enfin sur Scan.

Les hôtes à gérer doivent présenter un serveur `ssh`, et le port correspondant (`tcp/22` par défaut) doit être ouvert sur le pare-feu éventuel. Le paquetage `rsync` devra aussi y être installé. Enfin, l'utilisateur `root` doit être autorisé à se connecter en utilisant `ssh` (`PermitRootLogin yes` dans `/etc/ssh/sshd_config`, sur chaque hôte).

Attendez la fin du scan réseau, puis cochez les hôtes à incorporer au groupe.

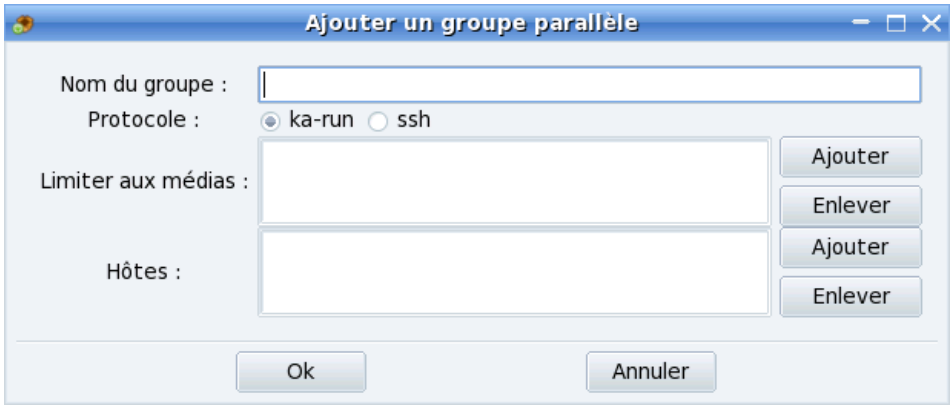


Figure 5-10. Ajouter des machines à un groupe

Le mot de passe `root` vous est alors demandé pour chacun des hôtes sélectionnés.

5.1.4.5.2. Gestion des paquetages du groupe de machines

Afin que le mode parallèle fonctionne, il est nécessaire que tous les hôtes du groupe soient disponibles.

Il suffit de sélectionner le groupe à gérer puis presser le bouton Utiliser le groupe. Vous pouvez alors installer des paquetages sur tous les hôtes du groupe comme vous le feriez pour une seule machine.

Il est aussi possible d'utiliser la ligne de commande :

```
urpmi --parallel <group_name> <package_name>
```

En utilisant `urpmi --parallel Conception gimp`, vous installerez GIMP sur tous les ordinateurs faisant partie du groupe `Conception`.

Pour supprimer un paquetage d'un groupe de machines, utilisez :

```
urpme --parallel <group_name> <package_name>
```

Par exemple, lancez `urpme --parallel Conception gcc` pour enlever le compilateur `C` des machines du même groupe.

5.2. Équilibrage de charge

Ce chapitre présente la mise en place d'une solution d'équilibrage de charge (*load balancing*) et de distribution des services afin de disposer d'un service dit de « haute disponibilité ». Il décrit la méthode d'installation, les éléments spécifiques aux besoins du service ainsi que la configuration requise pour la mise en œuvre.

5.2.1. Information requise

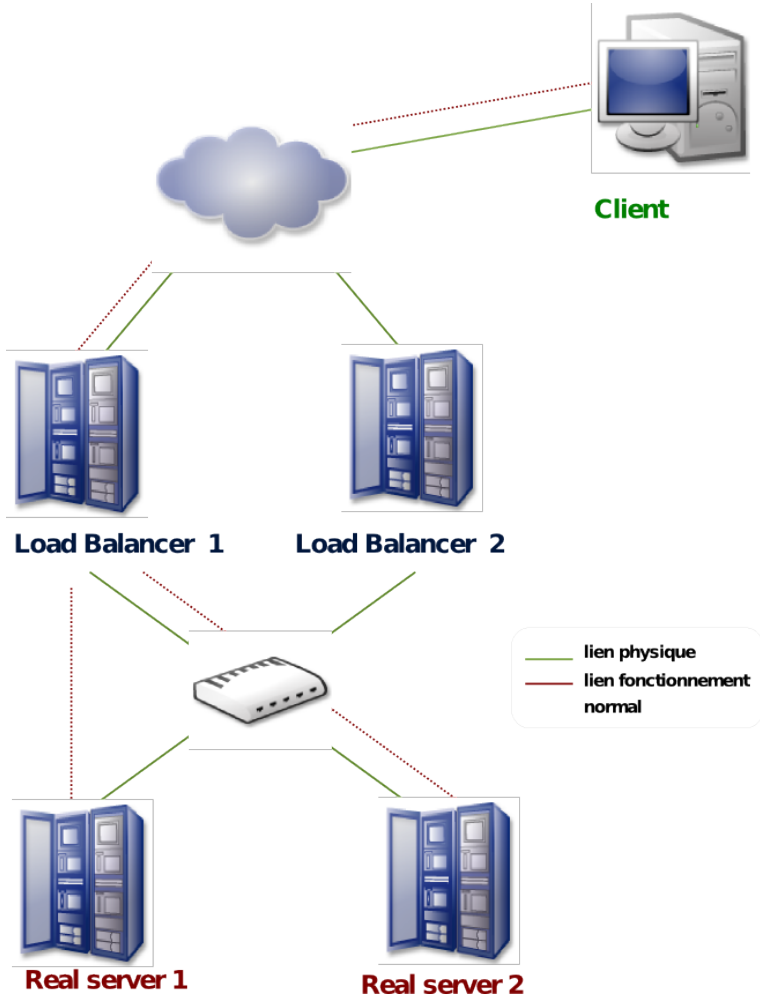


Figure 5-11. Schéma type d'équilibrage de charge

La problématique que nous étudierons est simple : un administrateur souhaite établir une redondance transparente pour son serveur Web afin de garantir la disponibilité de son Intranet. Nous disposons dans ce cas de quatre machines, qui seront réparties de la façon suivante :

- deux équilibreurs de charge ou *load balancers* en anglais (identifiés par `lb1` et `lb2`),

- deux vrais serveurs, soit *real servers* en anglais, (également appelés nœuds, identifiés par `rs1` et `rs2`) sur lesquels tourne le service en question.

Les équilibreurs de charge ont pour fonction de répartir la « charge » sur les machines en fonction de critères définis au préalable. Les vrais serveurs sont les serveurs physiques sur lesquels tournent les services. Dans notre cas, il s'agit d'un serveur Web. Dans le cas où la charge viendrait à augmenter, il est possible de gagner de la puissance de façon transparente en ajoutant simplement une machine supplémentaire.

L'équilibrage des adresses IP sera la suivante :

```
10.0.0.3 - adresse IP de lb1
   10.0.0.4 - adresse IP de lb2
   10.0.0.5 - adresse IP du service Web de l'Intranet

192.168.0.1 - adresse IP local de la passerelle
   192.168.0.12 - adresse IP de rs1
   192.168.0.13 - adresse IP de rs2
```

5.2.2. Concepts généraux et références Web

Le fonctionnement de l'équilibrage de charge s'effectue au niveau IP et est traité directement par le noyau Linux. L'équilibreur de charge agit donc en quelque sorte comme un routeur puisqu'il redirige les requêtes, et donc les paquets, vers une cible particulière en fonction de différentes règles.

Principales références Web :

- Site officiel de Linux Virtual Server (LVS) (`http://www.linuxvirtualserver.org/`)
- HOWTO le plus complet autour de LVS, remplace par la pratique la documentation officielle (`http://www.austintek.com/LVS/LVS-HOWTO/`)
- Site officiel de Keepalived (`http://www.keepalived.org/`)
- Section concernant iproute2 du Linux Advanced Routing HOWTO (`http://lartc.org/howto/lartc.iproute2.html`)

5.2.3. Installation et configuration de LVS

5.2.3.1. Les paquets nécessaires

Sur les équilibreurs de charge :

ipvsadm

Contient l'exécutable contrôlant le module `ip_vs` du noyau Linux destiné a répartir la charge entre les machines.

keepalived

Abrite le logiciel Keepalived qui sera utilisé pour contrôler `ipvsadm`. Keepalived contient également un démon `vrrp` destiné à assurer la continuité du service.

Sur les serveurs Web :

iproute2

Permet d'utiliser les fonctionnalités avancées de routage IP du noyau Linux.

5.2.3.2. Installation

1. Sur les équilibreurs de charge

   En tant que root, installez le paquet `keepalived` qui satisfera aux dépendances requises :

   ```
   [root@lb1 ~]#urpmi keepalived
   Pour satisfaire les dépendances, les paquetages suivants vont être
   installés:
   ipvsadm-1.24-6mdv2009.0
   keepalived-1.1.17-1mdvmes5
   Procéder à l'installation des 2 paquetages ? (0 Mo) (O/n)
   ```

   Attention, vous devez impérativement installer ces paquets sur les deux équilibreurs de charge !

2. Sur les serveurs Web

   Normalement, le paquet `iproute2` devrait déjà déjà être installé. Si ce n'est pas le cas, installez-le :

   ```
   [root@lb1 ~]#urpmi iproute2
   ```

La configuration générale s'effectue uniquement dans le fichier `/etc/keepalived/keepalived.conf`. Tous les éléments de configuration donnés ci-dessous sont à placer dans ce fichier (par défaut, celui-ci contient une configuration d'exemple).

5.2.3.3. Configuration des équilibreurs de charge

Tout d'abord, il faut charger le module `ip_vs` au démarrage de la machine. Pensez à ajouter ce module à `/etc/modprobe.preload`. Normalement, Keepalived chargera automatiquement le module.

```
#modprobe ip_vs
```

Keepalived sera utilisé pour gérer `ipvsadm` ainsi que le *failover* entre les équilibreurs de charge. En effet, nous avons établi la redondance entre les équilibreurs de charge, par sécurité, pour s'assurer de ne pas avoir à se préoccuper de cet aspect. Le paquet `keepalived` installe également `ipvsadm` qui est l'outil d'administration de `ip_vs` (le module noyau permettant ceci).

Premièrement, vérifiez que celui-ci propose bien l'`ip_forward`, sinon cela ne fonctionnera pas :

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Ensuite, éditez le fichier `/etc/keepalived/keepalived.conf`. La section `global_defs` s'applique à la configuration de Keepalived en général. Elle permet de définir les options de notification, et surtout le `lvs_id` (identifiant unique d'une machine).

```
global_defs {
    notification_email {
    mon@mail.com
    }
    notification_email_from keepalived@domaine.tld
    smtp_server 127.0.0.1
    smtp_connect_timeout 30
    lvs_id LVS_MAIN
    }
```

La section `vrrp\_instance` permet de définir les modalités d'utilisation du démon `VRRP` inclus dans Keepalived. Ce protocole permet une attribution à la volée des adresses IP entre plusieurs machines. Cette solution permet la redondance des équilibreurs de charge. Au cas où l'un de ceux-ci ne serait plus disponible, le second prendrait le relais, en reprenant à son compte l'adresse IP indiquée en `virtual\_ipaddresse{}`. Pour le second équilibreur de charge, la directive `state` contiendra la valeur `SLAVE`. `virtual_ipaddress` définit toutes les adresses IP que l'équilibreur de charge doit s'attribuer lorsqu'il est défini en maître. Attention, la directive `virtual_ipaddress` prend uniquement une adresse IP par ligne et possède une limite de 32 IP.

```
vrrp_instance VI_1 {
    state MASTER
    interface eth0
    virtual_router_id 51
```

```
    priority 100
    advert_int 1
    authentication {
    auth_type PASS
    auth_pass 1111
    }
    virtual_ipaddress {
    10.0.0.5
    }
    }
```

La section suivante concerne la définition des serveurs virtuels à mettre en redondance, et les protocoles en question.

```
# Virtual Servers definitions

    virtual_server 192.168.0.1 80 {
    delay_loop 30
    lb_algo wlc
    lb_kind NAT
    persistence_timeout 50
    protocol TCP
```

Si aucun vrai serveur n'est accessible, `keepalived` renverra la requête sur celui-ci. Il permet d'afficher une page d'information statique en cas de problème.

```
sorry_server 192.168.0.1 80
```

On ajoute tous les *realservers* :

```
real_server 192.168.0.12 80 {
    weight 20
    }

    real_server 192.168.0.13 80 {
    weight 8
    }

    }
```

5.2.3.4. Configuration des vrais serveurs

Les machines étant sur un réseau local avec les équilibreurs de charge, nous devons les forcer à utiliser ces derniers comme passerelle pour tout le trafic. Nous allons donc créer une route statique forçant ce trajet. `iproute2` permet cela.

Ensuite, nous allons créer les règles :

```
#!/bin/sh -e
    echo 200 LVS >> /etc/iproute2/rt_tables
    /sbin/ip rule add from 192.168.0.12 table LVS
    /sbin/ip route add default via 192.168.0.1 dev eth0 table LVS
    /sbin/ip route flush cache
```

Testons maintenant la configuration. On relance keepalived :

```
# service keepalived restart
```

Il ne vous reste plus qu'à lancer votre navigateur favori, et à vous rendre à l'adresse http://10.0.0.5 (`http://10.0.0.5`). Si la page s'affiche correctement, c'est que votre configuration est fonctionnelle. Bien entendu, il s'agit ici d'une configuration de base, à laquelle il peut être intéressant d'ajouter certaines fonctionnalités : pare-feu sur les équilibreurs de charge, surveillance réseau précise, etc.

Une fois le serveur installé, vous pouvez utiliser la commande `ipvsadm -L` afin de connaître l'état de votre équilibrage de charge :

```
# ipvsadm
    IP Virtual Server version 1.2.0 (size=4096)
    Prot LocalAddress:Port Scheduler Flags
    -> RemoteAddress:Port           Forward Weight ActiveConn
    InActConn TCP  10.0.0.5:www wlc persistent 20
    -> 10.0.0.3:www                  Route   25     294        916
    -> 10.0.0.4:www                 Route   8      243        754
```

5.2.3.5. Configuration avancée

Keepalived dispose d'un moteur de vérification, capable de s'assurer que les serveurs Web ajoutés dans votre cluster LVS haute disponibilité sont bien atteignables. Pour cela, il suffit d'ajouter une section dans la configuration du serveur Web dans le fichier `/etc/keepalived/keepalived.conf`. La vérification peut consister en un simple `ping` :

```
TCP_CHECK { connect_port 80 connect_timeout 3
    }
```

Elle peut aussi aller jusqu'à vérifier que la page servie correspond bien à la page attendue.

```
HTTP_GET {
    url {
    path /
    digest 69c520033af926d40e7d5d832e3933f6
    }
    connect_timeout 5
    nb_get_retry 3
    delay_before_retry 2
    }
```

Pour générer le hash, utilisez l'exécutable `genhash` avec la commande suivante :

```
[root@lb1 ~]# genhash -s 193.188.255.4 -p 80 -u /
    MD5SUM = 5b5af20a92f1dbe92328005329d1753f
```

Il est également possible de déclencher des actions si un événement se produit (typiquement, basculer sur le second équilibreur de charge suite à la non-disponibilité du premier), via les directives suivantes situées dans la section `vrrp` :

```
notify_master /path_to_script/script_master.sh
    (or notify_master "/path_to_script/script_master.sh <arg_list>")
    notify_backup /path_to_script/script_backup.sh
    (or notify_backup "/path_to_script/script_backup.sh <arg_list>")
    notify_fault /path_to_script/script_fault.sh
    (or notify_fault "/path_to_script/script_fault.sh <arg_list>")
```

5.3. Virtualisation

Dans ce chapitre, nous exposons les concepts et les procédures nécessaires à l'implémentation de machines virtuelles sur votre Mandriva Enterprise Server 5 en utilisant Xen, KVM ou l'outil graphique Virt-manager. Vous pourrez ainsi utiliser plusieurs systèmes d'exploitation sur votre machine.

5.3.1. Xen

5.3.1.1. Concepts généraux et références Web principales

Xen est un moniteur de machine virtuelle pour les processeurs X86 (fonctionnant sur CPU de classe i686 et x86-64) et permet l'exécution de multiples systèmes d'exploitation invités (*guest*) sur un seul serveur. Les serveurs invités (aussi appelés *domains*) ont besoin dfchargement'un noyau modifié supportant les hyperappels (*hypercall*) Xen qui remplace les accès physiques au matériel. Au démarrage, le noyau Xen est chargé (par GRUB) ainsi que les noyaux invités pour le premier serveur invité. *domain0* possède les privilèges pour accéder au matériel physique (périphériques PCI et ISA), pour gérer les autres serveurs invités ainsi que pour fournir des périphériques virtuels (disque et réseau) pour les autres serveurs invités.

Voici les principales ressources Web concernant la configuration de Xen (en anglais) :

- Site officiel (`http://www.cl.cam.ac.uk/Research/SRG/netos/xen/`)
- Principal vendeur de Xen (`http://citrix.com/`)
- Xen Wiki (`http://wiki.xensource.com/`)

5.3.1.2. Installation et configuration des serveurs invités

5.3.1.2.1. Avant de commencer

Nous avons installé un Mandriva Enterprise Server 5 sur un disque dur de 12 Go. Durant l'installation, nous avons créé une partition de 5 Go. Son système de fichiers est monté sur / pour l'installation du `domain0`. Nous avons également préparé une partition de 256 Mo de swap sur `/dev/sda5`.

Nous avons donc 7 Go de disponible. Nous avons créé 2 partitions de 3,2 Go, pas encore montées, pour 2 installations de systèmes d'exploitation invités ainsi que deux espaces swap de 256 Mo.

Voici la table de partition :

```
root domain0 -> sda1
swap domain0 -> sda5

root guest1 -> sda6
swap guest1 -> sda7

root guest2 -> sda8
swap guest2 -> sda9
```

5.3.1.2.2. Installation des RPM

Votre Mandriva Enterprise Server 5 fournit les modifications nécessaires au noyau afin que les fonctionnalités de Xen soient implémentées correctement. Vous aurez donc besoin du noyau modifié ainsi que des outils de gestion de virtualisation.

```
# urpmi kernel-xen xen
```

5.3.1.2.3. Configuration du domain0

L'installation du rpm `xen` a effectué pour vous la configuration du chargeur de démarrage et la création de l'initrd. Ce qui suit est un rappel pour configurer le `domain0`. Il vous reste à mettre en place le lancement automatique des services xen au démarrage de la machine.

1. Configuration de GRUB

   Vous devez ajouter une entrée dans le fichier de configuration de GRUB (`/boot/grub/menu.lst`) afin que Xen/Xenolinux puisse démarrer. Votre entrée devrait ressembler à :

   ```
   title XEN 3 / Mandriva Enterprise Server 5
   kernel (hd0,0)/boot/xen.gz dom0_mem=131072
   module (hd0,0)/boot/vmlinuz-2.6.18.8-xen-3.3.0-7mdv root=/dev/sda1 ro
   module (hd0,0)/boot/initrd-2.6.18-8-xen-3.3.0-7mdv.img
   ```

   Révision des paramètres principaux :

   kernel

   indique à GRUB l'adresse physique de Xen et les paramètres requis par le noyau (dans ce cas-ci, définir la taille de l'allocation de mémoire du `domain0` en kilo-octet).

   module

   La première ligne définit le noyau Xenolinux que Xen doit démarrer ainsi que ses paramètres et sont des paramètres standards de Linux, l'identification du root et les partitions initiales à monter en lectures seules.

module

La deuxième ligne indique le chemin d'accès à `initrd`. Cela doit être le module et non le `initrd` de la configuration de GRUB, si non Xen ne démarrera pas.

2. Création de initrd

   Nous allons maintenant créer un fichier `initrd` afin que les serveurs invités de Xen soient gérés au démarrage :

   ```
   # mkinitrd -v -f /boot/initrd-2.6.18.8-xen-3.3.0-7mdv.img
   2.6.18.8-xen-3.3.0-7mdv
   ```

En ajoutant le nouveau noyau dans `menu.lst`, il est recommandé de garder vos entrées existantes. Vous pourriez avoir à redémarrer votre ancien noyau Linux en cas de problèmes.

3. Démarrer les services Xen

   À la fin du processus d'installation et de configuration, redémarrez votre système et choisissez l'entrée Xen dans le menu GRUB.

   Durant le démarrage, la première partie affiche de l'information concernant Xen (niveau matériel). La dernière partie affiche sur Xenolinux.

   Pour créer des serveurs invités supplémentaires, démarrez le démon `xend`. Vous pouvez également démarrer le démon `xendomains`, qui lance les *domains* additionnels sur `domain0` au démarrage.

   ```
   # chkconfig --add xend
   # chkconfig --add xendomains
   # service xend start
   # service xendomains start
   ```

À partir de maintenant, vous pouvez utiliser la commande `xm` pour surveiller ou gérer les domains sur votre système.

5.3.1.2.4. L'installation de serveurs invités

La première étape de création d'un nouveau serveur invité consiste à **préparer un système de fichiers root** afin qu'il démarre. Typiquement, on pourrait l'inscrire sur une partition normale, une partition LVM, un fichier sur disque ou sur un serveur NFS. La solution la plus simple consiste à démarrer avec un disque d'installation et d'installer la distribution sur une nouvelle partition de votre disque dur.

Dans les sections suivantes, nous vous proposons une autre option pour créer des serveurs invités supplémentaires. Elle s'appuie sur une copie de la partition root de `domain0`, installée avec urpmi dans une partition locale ou dans un fichier.

```
# mkdir -p /mnt/xen
```

Copie de partition. L'avantage principal de cette méthode est que le disque d'installation ne sera pas nécessaire. On copie la partition `root` du `domain0` sur une autre partition du disque dur afin d'obtenir un second système de fichiers qui sera utilisé par les serveurs invités.

```
# mount /dev/sda6 /mnt/xen
# rsync -avDx / /mnt/xen
# cp -ar /dev/* /mnt/xen/dev/
# umount /mnt/xen
```

La commande `rsync` synchronisera la partition root seulement, sans suivre les liens vers les autres systèmes de fichiers.

Si vos répertoires `/usr` et `/var` sont sur des partitions séparées, vous devrez refaire la commande précédente pour chaque point de montage, sauf les réseaux et les entrées spéciales.

Si vous avez différents schémas de partition entre `domain0` et les autres serveurs invités, n'oubliez pas d'adapter votre fichier `/etc/fstab` au système de fichiers du serveur invité.

Installation de Mandriva Enterprise Server 5 avec urpmi. Avec une installation basée sur `urpmi`, vous aurez une nouvelle installation de Mandriva Enterprise Server 5.

1. D'abord, montez votre nouvelle partition :

   ```
   # mount /dev/sda6 /mnt/xen
   ```

2. Définissez votre média pour urpmi :

   ```
   # urpmi.addmedia --distrib --urpmi-root /mnt/xen url
   ```

Vous devez configurer correctement `url` afin qu'ils pointent vers le répertoire contenant les médias d'installation.

3. Installez le système de base du Mandriva Enterprise Server 5 sur votre serveur invité et utilisez `urpmi` pour installer les mises à jour et les nouveaux logiciels.

```
# urpmi --urpmi-root /mnt/xen basesystem urpmi
```

Le système vous posera plusieurs questions. Répondez comme vous le feriez pour une installation classique (choisissez le `kernel-xen`).

4. Les étapes suivantes configurent les dernières fonctionnalités :

   Copiez les fichiers de configuration pour le `domain0`.

   ```
   # cp /etc/resolv.conf /mnt/xen/etc
   # cp /etc/fstab /mnt/xen/etc
   ```

5. Il vous faut Configurer correctement le fichier `/etc/fstab` du *domain* invité. Par exemple, la partition `/dev/sda6` devenant `/dev/sda1` :

   ```
   /dev/sda1 / ext3 relatime,user_xattr,acl 1 1
   /dev/sda5 swap swap defaults 0 0
   none /proc proc defaults 0 0
   ```

   a. Copiez les configurations réseau de `domain0`.

      ```
      # cp /etc/sysconfig/network-scripts/ifcfg-eth0 \
      /mnt/xen/etc/sysconfig/network-scripts
      ```

   b. Installez le client DHCP, si nécessaire.

      ```
      # urpmi --urpmi-root /mnt/xen dhcp-client
      ```

   c. Entrez en mode chroot pour la configuration finale.

      ```
      # chroot /mnt/xen
      ```

   d. Créez les fichiers vides de configuration nécessaires.

      ```
      # touch /etc/mtab /etc/urpmi/urpmi.cfg /var/lib/urpmi/MD5SUM
      ```

   e. Créez `shadow` à partir de `passwd`.

      ```
      # pwconv
      ```

   f. Activez le réseau en créant un fichier `/etc/sysconfig/network` abritant le contenu suivant :

      ```
      NETWORKING=yes
      ```

   g. Définissez le mot de passe root.

      ```
      # passwd root
      ```

   h. Sortir de la console chroot.

      ```
      # exit
      ```

   i. Démontez les partitions invitées.

      ```
      # umount /mnt/xen
      ```

Installez un Mandriva Enterprise Server 5 dans un fichier. Cette méthode offre l'avantage de ne pas modifier la structure de partition de votre disque dur. Nous expliquerons comment créer et monter une image d'un disque.

Vous pouvez choisir une des deux méthodes d'installation proposées plus bas (urpmi ou une copie de partition `root`).

1. D'abord, créez un fichier image du serveur invité de votre Mandriva Enterprise Server 5. Cette commande crée une image de 1 Go, remplie de zéro, dans un ficher nommé `mandriva.img` situé dans le répertoire courant.

   ```
   # dd if=/dev/zero of=mandriva.img bs=1M count=1 seek=1024
   ```

2. Créez maintenant un système de fichiers dans le fichier image. L'option

   `-j`

   précise le type `ext3`.

   ```
   # mke2fs -F -j mandriva.img
   ```

3. Enfin, vous pouvez monter votre image sur un point de montage.

   ```
   # mount -o loop mandriva.img /mnt/xen
   ```

Utilisez maintenant ce point de montage comme une partition physique et installez Mandriva Enterprise Server 5.

Dans le fichier de configuration du serveur invité, l'option du disque doit être modifiée afin que `phy:sdaX` soit remplacé par `file:path/of/file`. Les autres options restent identiques.

5.3.1.2.5. Configuration des serveurs invités supplémentaires

Avant de pouvoir démarrer un *domain* supplémentaire, vous devriez créer un fichier de configuration pour les *domains* invités. Les sections suivantes décrivent ces étapes. Elle ne sont pas essentielles, mais contribuent grandement au démarrage sans problème des serveurs invités.

Créez un fichier de configuration pour un domain invité. Le fichier de configuration suivant (disons « mandriva ») devrait être situé dans le répertoire `/etc/xen` du `domain0` pour un démarrage manuel, ou dans le répertoire `/etc/xen/auto` pour un démarrage automatique par xendomains au démarrage.

```
kernel = "/boot/vmlinuz-2.6.18.8-xen-3.3.0-7mdv"
ramdisk = "/boot/initrd-xen-2.6.18.8-xen-3.3.0-7mdv.img"
memory = 128
name = "Mandriva"
dhcp = "dhcp"
disk = [ 'phy:sda6,sda1,w', 'phy:sda7,sda5,w' ]
root = "/dev/sda1 ro"
extra = "xencons=tty"
hostname = "mandriva2009"
vif = [ '' ]
```

Ce fichier décrit les options les plus couramment utilisées pour la définition d'un serveur invité. Voici une courte description pour chaque option :

kernel

Établit le lien vers le noyau que vous avez compilé pour Xen.

memory

Définit la taille de la mémoire allouée au serveur invité en méga-octets.

name

Le nom du serveur invité.

dhcp

Retirez le commentaire de la variable DHCP afin que ce serveur invité reçoive une adresse IP du serveur DHCP.

disk

Liste des unités par blocs (*block devices*) exportées au serveur invité. Dans cet exemple, la partition physique `sda6` prend le nom `sda1` dans les serveurs invités et devient la partition `root`. La partition `sda7` devient pour sa part le swap. Si votre disque est un fichier image, vous devriez remplacer `phy:sdaX` par `file:path/of/file`. L'option `w` détermine les accès lecture/écriture sur cette partition. Utilisez l'option `r` pour définir des partitions en lecture seule.

root

Spécifie l'unité root sur la ligne de commande du noyau. On doit prendre le schéma de partition de l'option disque.

extra

Des « extras » à ajouter à la ligne de commande du noyau.

hostname

Le nom du serveur invité.

vif

La configuration de l'interface réseau de l'invité.

Toutes les modifications de configuration détaillées dans la section suivante doivent être réalisées dans le fichier de configuration du serveur invité, et non dans le `domain0`. Il existe deux possibilités :

- Lancer le serveur invité avec xm avec la commande `xm create -c /etc/xen/auto/mandriva`. Ensuite, on modifiera le serveur invité directement dans celui-ci.
- Tapez une commande chroot tel que :

  ```
  chroot /mnt/xen
  ```

  Pour sortir de la console chroot, tapez `exit` et n'oubliez pas de libérer le système de fichiers `/mnt/xen` en tapant `umount /mnt/xen`.

Allons-y maintenant avec la dernière étape de configuration.

1. **Modifiez `/etc/inittab`.** Si vous voulez évitez de voir apparaître des messages comme :

   ```
   INIT: Id "2" respawning too fast: disabled for 5 minutes
   INIT: Id "3" respawning too fast: disabled for 5 minutes
   INIT: Id "4" respawning too fast: disabled for 5 minutes
   INIT: Id "5" respawning too fast: disabled for 5 minutes
   INIT: Id "6" respawning too fast: disabled for 5 minutes
   ```

   Dans votre console invitée, vous devez commenter les terminaux inutilisés dans `/etc/inittab` en faisant :

   ```
   1:2345:respawn:/sbin/mingetty tty1
   #2:2345:respawn:/sbin/mingetty tty2
   #3:2345:respawn:/sbin/mingetty tty3
   #4:2345:respawn:/sbin/mingetty tty4
   #5:2345:respawn:/sbin/mingetty tty5
   #6:2345:respawn:/sbin/mingetty tty6
   ```

2. **Les services xend et xendomains.** Si vous avez installé votre système en copiant le `root` d'un système de fichiers, tel que décrit précédemment, les services xend et xendomains sont probablement configurés pour être lancés au démarrage. Ils sont inutiles pour les serveurs invités supplémentaires. Nous allons les désactiver comme suit :

   ```
   # /etc/init.d/xend stop
   # /etc/init.d/xendomains stop
   # chkconfig xend off
   # chkconfig xendomains off
   ```

3. **Le service Keytable.** Afin d'éviter des messages d'erreur au moment du chargement du fichier keymap lors du démarrage des serveurs invités, désactivez le service :

   ```
   # chkconfig keytable off
   # /etc/init.d/keytable stop
   ```

   Mais la dernière commande ne suffit pas, ce service étant appelé directement dans le fichier `/etc/rc.d/rc.sysinit`. Nous allons commenter les 3 lignes suivantes (905,906,907) :

   ```
   #if [ -x /etc/init.d/keytable -a -d /usr/lib/kbd/keymaps ]; then
   #    /etc/init.d/keytable start
   ```

```
#fi
```

Comme le domain0 initialise le même clavier que tous les autres serveurs invités, vous constaterez que le service keytable et numlock ne sont pas nécessaires dans les serveurs invités.

4. **Service Numlock.** Finalement, en mode serveur invité, le message suivant apparaît lorsque le service numlock est démarré ou au moment de la connexion (*login*) :

```
KDGETLED: Argument invalide Error reading current led setting.
Maybe stdin is not a VT?
```

Pour éviter ce problème, désactivez le service comme suit :

```
# /etc/init.d/numlock stop
# chkconfig numlock off
```

À cette étape, nous avons maintenant un système Xen qui contient un domain0 et un ou plusieurs serveurs invités additionnels prêts à utiliser.

5.3.1.3. Gestion des serveurs invités

5.3.1.3.1. Configuration réseau

Cette section présente les bases de la réseautique sur Xen et leur configuration.

Réseautique

Le schéma réseau est fort simple. Le domain0 a le contrôle réel des interface Ethernet. Chaque serveur invité a une interface réseau virtuelle. Ces dernières sont normales, sauf qu'elles sont nommées vifY.X, « X » étant le numéro de l'interface (0 pour eth0) et « Y » le numéro du serveur invité. Toutes les interfaces vif et eth sont branchées sur la passerelle peth0 pour l'accès au réseau.

Consultez XenNetworking (http://wiki.xensource.com/xenwiki/XenNetworking) obtenir de l'information détaillée sur la réseautique avec Xen.

Vous y trouverez une documentation et des explications précises sur les interfaces Ethernet, les adresses MAC, les passerelles, les redirections, les noms, les réseaux élargis, etc.

5.3.1.3.2. L'outil xm

xm fournit plusieurs options pour la gestion des serveurs invités. En voici un survol :

- Démarrer les *domains* invités : avant de démarrer un *domain* invité, vous devriez lui créer un fichier de configuration.

  Pour lancer un *domain* additionnel :

  ```
  # xm create -c /etc/xen/auto/mandriva
  ```

  La commande `create` lance une nouvelle instance de *domain*. L'option `-c` configure la console afin qu'elle retourne immédiatement et `mandriva` est le chemin du fichier contenant la configuration du serveur invité que vous démarrez. Vous devriez maintenant voir une liste de serveurs invités additionnels :

  ```
  # xm list
  ```

  Vous trouverez plus de détails sur la configuration et la syntaxe en utilisant `xm help`.

- Utilisation de la console Xen : si vous ne spécifiez pas l'option `-c` au démarrage, vous pouvez toujours utiliser la console.

  ```
  # xm console Mandriva
  ```

  `Mandriva` est le nom du serveur invité. Vous pouvez également utiliser le numéro d'identification affiché dans la sortie standard de `xm list`.

  Pour quitter une console invitée, tapez `Ctrl+]` (`Ctrl+$` dans une console virtuelle locale ou tty).

- Sauvegarde et récupération des *domains* invités : l'administrateur d'un système Xen peut suspendre une machine virtuelle dans son état courant vers un fichier dans `domain0` et reprendre l'exécution plus tard.

  Par exemple, vous pouvez suspendre un domain appelé « mandriva » sur disque :

  ```
  # xm save Mandriva mandriva.chk
  ```

  Cette commande arrête le serveur invité « mandriva » et sauve son état courant dans un fichier `mandriva.chk`.

  Pour repartir ce *domain*, utilisez la commande `xm restore` :

  ```
  # xm restore mandriva.chk
  ```

  Cette commande récupère l'état du *domain* et en redémarre l'exécution. Le *domain* repartira dans le même état et la console pourra se reconnecter en utilisant la commande `xm console Mandriva`.

5.3.1.4. Dépannage

- Si vous obtenez l'erreur suivante :

  ```
  Error: Error creating domain (12, 'Cannot allocate memory')
  ```

  ajoutez l'option `dom0_mem` sur la ligne de commande de Xen dans `grub.conf` :

- Si vous obtenez l'erreur suivante :

  ```
  Error: Error creating domain: Kernel image does not exist :
  /boot/vmlinuz-2.6.18.8-xen-3.3.0-7mdv
  ```

  installez le paquetage `kernel-xen` sur l'invité.

5.3.2. KVM

5.3.2.1. Concepts généraux et références Web principales

KVM (Kernel-based Virtual Machine) est une solution de virtualisation pour les architectures x86 disposant des technologies Intel VT (vmx) ou AMD-V (svm). Pour savoir si vous disposez de ces instructions de virtualisation dans votre processeur:

```
# grep '(vmx|svm)' /proc/cpuinfo
```

Si vous savez que le processeur inclut une extension de virtualisation mais que celle-ci n'apparaît pas, vérifiez que l'option est bien activée dans le BIOS. Si ce n'est pas le cas, activez-là. Afin que la modification soit prise en compte, un reboot ne suffit pas, il faut éteindre complètement le serveur.

Avec KVM, vous pouvez déployer des machines virtuelles Linux ou Windows®.

Le site du projet KVM est linux-kvm.org (`http://www.linux-kvm.org/page/Main_Page`)

5.3.2.2. Installation

Vous aurez besoin des paquets qemu-img et kvm

```
# urpmi qemu-img kvm
```

Pour utiliser KVM, le module noyau doit être chargé. Cela est fait automatiquement. Néanmoins, vous pouvez le vérifier par la commande :

```
# lsmod |grep kvm
```

- Dans le cas où vous avez la technologie AMD-V, si le module n'est pas chargé, chargez le à l'aide de la commande:

  ```
  # modprobe kvm-amd
  ```

- Dans le cas où vous avez la technologie Intel VT, si le module n'est pas chargé, chargez le à l'aide de la commande:

  ```
  # modprobe kvm-intel
  ```

L'utilisateur avec lequel vous allez créer vos machines virtuelles doit appartenir au groupe kvm (ici l'utilisateur se nomme test).

```
#usermod -G kvm test
```

Vérifiez avec la commande id par exemple que votre utilisateur appartient bien au groupe kvm :

```
$id
uid=500(test) gid=500(test) groupes=422(kvm),500(test)
```

5.3.2.3. Installation des machines invitées

Prévoyez un espace suffisamment grand pour stocker vos machines virtuelles. Vous pouvez également créer une partition séparée pour cet espace.

Vous devez commencer par créer une image qui contiendra la machine invitée. La commande suivante crée une image dont la taille maximale sera de 3G.

```
$ qemu-img create mes5dvd 3G
Formatting 'mes5dvd', fmt=raw, size=3145728 kB
```

Différents formats d'image existent, se référer à man qemu-img pour connaître les différents formats possibles.

Nous allons installer à partir du DVD d'installation une Mandriva Enterprise Server 5 dans l'image précédemment créee et nommée `mes5dvd`.

```
kvm -k fr -m 512 -cdrom /dev/cdrom -drive file=mes5dvd
```

Les options correspondent à :

- -k fr : clavier français.
- -m 512 : la machine virtuelle aura 512 de mémoire.
- -cdrom /dev/cdrom : le périphérique cdrom de la machine virtuelle sera `/dev/cdrom` c'est à dire le périphérique cdrom de la machine physique.
- -drive file=mes5dvd : le disque dur de la machine virtuelle sera le fichier `mes5dvd`.

Le CD ou DVD d'installation présent dans votre lecteur CD est un CD/DVD bootable. Après le lancement de la commande, une fenêtre apparaît et l'installation de votre machine virtuelle commence. Procédez à l'installation complète.

Pour démarrer ensuite votre machine virtuelle :

```
kvm -k fr -m 512 -cdrom /dev/cdrom -drive file=mes5dvd,boot=on
```

De nombreuses options peuvent être passées à KVM (vous pouvez vous référer à man kvm).

Avec la méthode décrite ci-dessus, votre machine virtuelle aura du réseau (accès au même réseau que la machine physique). C'est KVM qui se charge de la configuration du réseau. Si vous souhaitez installer plusieurs machines virtuelles, vous devrez configurer un bridge et natter vos machines virtuelles. Pour savoir configurer un bridge et l'utiliser avec KVM, vous pouvez vous référer à la documentation disponible sur linux-kvm.org (`http://www.linux-kvm.org/page/Networking`)

5.3.3. Virt-manager

Virt-manager est un outil graphique d'aide à la configuration de vos outils de virtualisation. Grâce à Virt-manager, vous pouvez utiliser Xen, KVM ou encore QEMU. Cet outil vous permettra de créer et gérer vos machines virtuelles, de configurer vos sous-réseaux et vos espaces de stockage.

5.3.3.1. Démarrer Virt-manager

Virt-manager utilise libvirtd qu'il faut donc démarrer:

```
#/etc/init.d/libvirtd start
```

Pour le rajouter en démarrage automatique:

```
#chkconfig libvirtd on
```

En fonction de l'outil de virtualisation que vous utilisez, pensez à le rendre opérationnel : démarrez le démon xend si vous utilisez Xen, chargez les modules noyau nécessaires au fonctionnement de KVM si vous utilisez KVM.

Vous pouvez ensuite lancer Virt-manager, dans le menu Applications > Outils > Emulateurs > Gestionnaire de machine virtuelle:

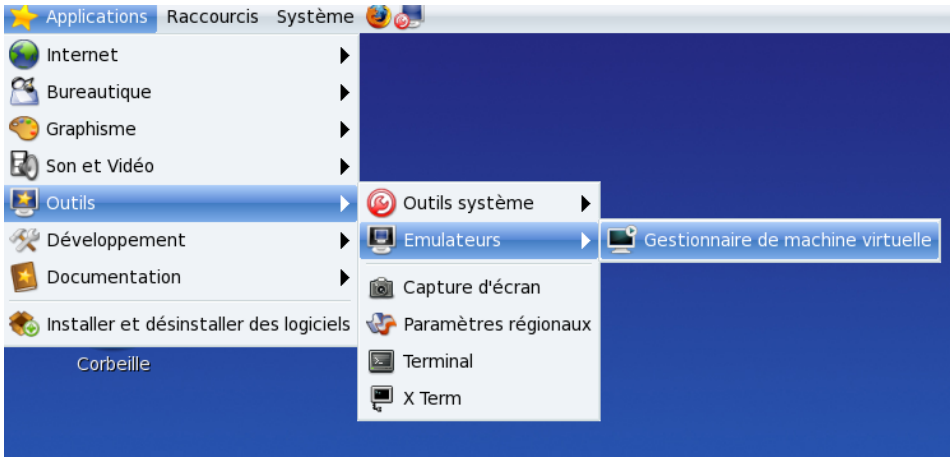


Figure 5-12. Lancement de Virt-manager

ou en ligne de commande :

```
#virt-manager
```

5.3.3.2. Utilisation de Virt-manager

5.3.3.2.1. Création de machine virtuelle

Une fois Virt-manager connecté à votre outil de virtualisation, vous pouvez cliquer sur Nouveau pour installer les machines virtuelles.

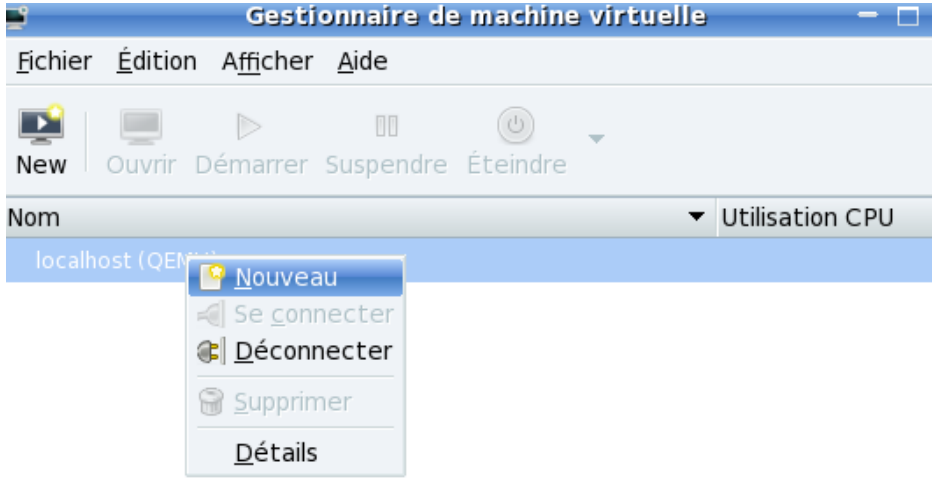


Figure 5-13. Création de machine virtuelle

5.3.3.2.2. Configuration des réseaux virtuels et du stockage

Pour configurer vos réseaux virtuels et vos espaces de stockage, vous devez effectuer un clic droit sur Votre domaine > Détails

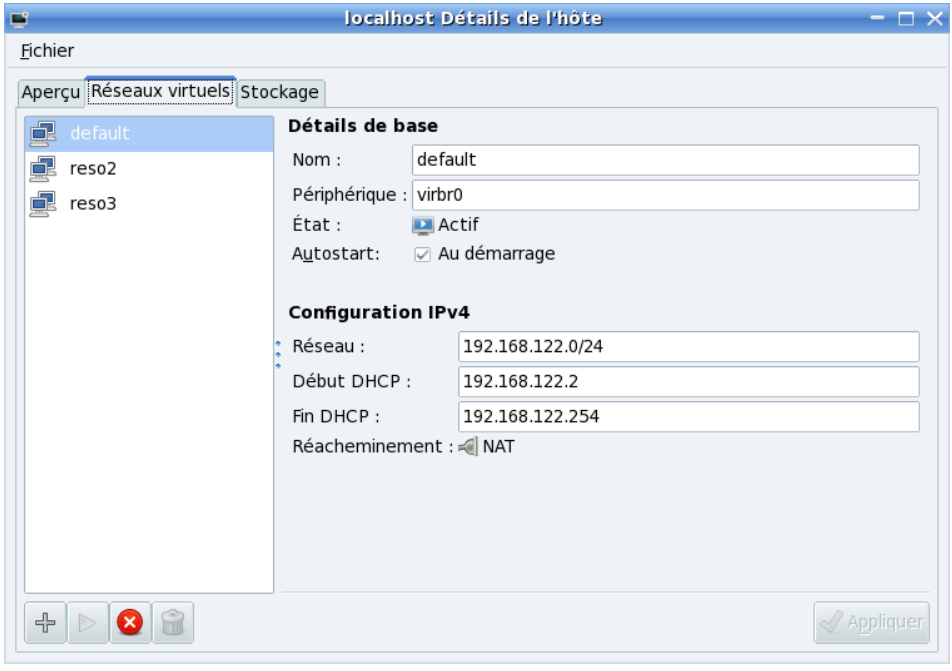


Figure 5-14. Configuration des réseaux virtuels

Pour plus d'informations,vous pouvez consulter le site officiel (`http://virt-manager.et.redhat.com/`) de Virt-manager.

Chapitre 6. Mandriva Directory Server

6.1. Présentation de Mandriva Directory Server

Mandriva Directory Server est un annuaire d'entreprise basé sur OpenLDAP permettant de gérer les comptes et profils des utilisateurs d'un parc informatique.

Grâce à l'ajout de modules additionnels, le Mandriva Directory Server peut aussi faire office de serveur de fichiers multi-protocoles (NFS, NETBIOS et WEBDAV) avec authentification des utilisateurs grâce à l'annuaire Mandriva Directory Server.

L'interface de Mandriva Directory Server est appelée Mandriva Management Console (MMC).

Mandriva Management Console est l'interface commune avec l'outil de gestion de parc hétérogène Pulse 2. Pour plus d'informations, voir (`http://pulse2.mandriva.org/`)

Selon votre installation, les modules de gestion suivants seront disponibles dans l'interface :

- module Base : utilisateurs et groupes
- module Samba : ressources d'un domaine Windows® (PDC NT4)
- module Messagerie : système de messagerie
- module Réseau : DNS et DHCP
- module Audit : contrôle et rapports des modifications
- module Politique de Mot de passe : règles de mot de passe utilisateur

Pour se connecter à la Mandriva Management Console, pointez un navigateur web sur l'URL suivante : http://server_ip/mmc

6.1.1. Connection à Mandriva Directory Server

Figure 6-1. Page de login de Mandriva Directory Server

Pour se connecter à la Mandriva Management Console , il est nécessaire de posséder un compte.

Il y a deux types de comptes :

- Le compte root est le compte d'administration de la Mandriva Management Console. C'est un compte spécial qui donne accès à toutes les fonctions de la Mandriva Management Console. Il s'agit d'un compte fictif, dont le mot de passe correspond à celui du gestionnaire du LDAP. Ce n'est pas le compte root système.

Ce compte a toujours accès à toutes les fonctionnalités de l'interface

- Tous les autres comptes sont des comptes utilisateurs qui ont été créés à partir de la Mandriva Management Console. Par défaut, ces comptes n'ont pas le droit de se connecter à la Mandriva Management Console. Il est nécessaire pour cela de leur positionner des droits particuliers dans l'interface (ACLs).

Figure 6-2. Page d'accueil de Mandriva Directory Server

Il est possible pour un utilisateur de choisir son niveau d'utilisation de l'interface. Par défaut, il est en mode Normal. Il suffit de cliquer sur Mode Normal pour basculer en mode Expert. Le mode expert permet d'accéder à des options particulières.

L'option Mode Normal permet de bénéficier d'une interface simplifiée de façon à augmenter la rapidité d'utilisation. Par la suite, ce document ne détaillera pas les fonctionnalités disponibles en mode expert.

6.2. Gestion des comptes utilisateurs

La base des comptes utilisateurs est contenue dans l'annuaire LDAP de Mandriva Directory Server. Cet annuaire contient toutes les propriétés (ou champs) associées aux comptes utilisateurs.

6.2.1. Liste des comptes utilisateurs

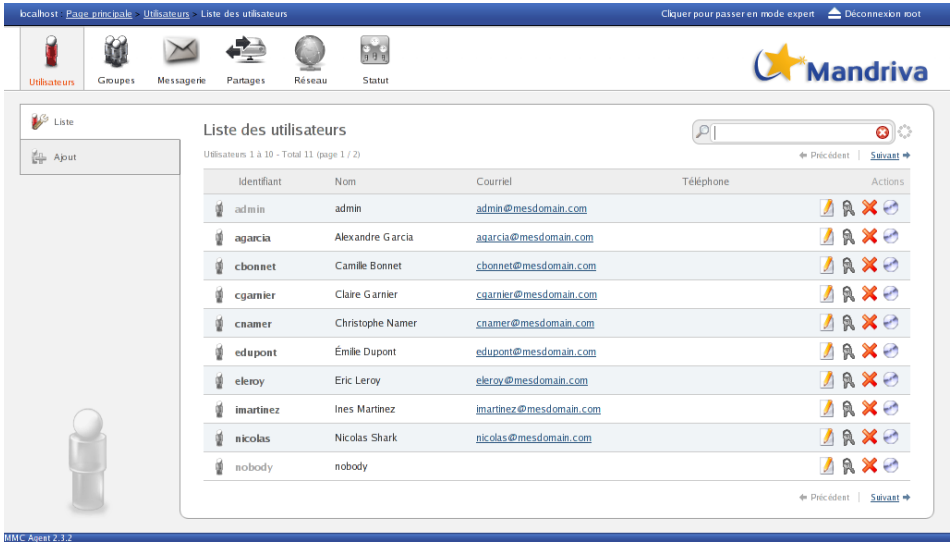


Figure 6-3. Liste des comptes utilisateurs

Cette liste est composée de quatre colonnes :

- Identifiant : le nom utilisé pour que l'utilisateur se connecte
- Nom d'utilisateur : le prénom et le nom de l'utilisateur
- Répertoire utilisateur : l'emplacement sur le disque dur du serveur du répertoire de stockage personnel de l'utilisateur
- Actions : il s'agit des actions disponibles sur ce compte utilisateur. Dans l'ordre, elles correspondent à Modifier le compte, Modifier les droits d'accès , Supprimer le compte et Faire une sauvegarde du répertoire personnel.

6.2.2. Ajouter un compte utilisateur

Pour ajouter un compte utilisateur, cliquez sur l'onglet Ajout. La page correspondante s'affiche alors.

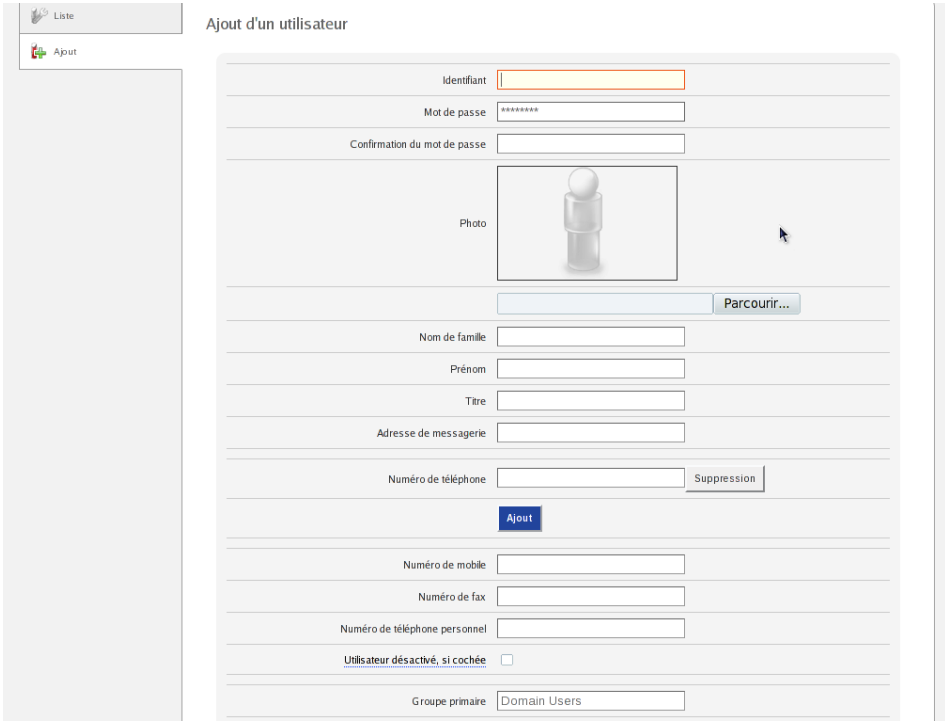


Figure 6-4. Ajout d'un compte utilisateur

Cette page permet de renseigner les propriétés de compte de base, suivi éventuellement d'autres propriétés selon les modules Mandriva Management Console installés et activés.

Les propriétés de compte de base doivent toujours être renseignées. Ensuite, selon les ressources que l'on souhaite mettre à disposition de l'utilisateur, les autres propriétés devront être renseignées. Veuillez vous référer aux chapitres correspondant aux modules gérant ces propriétés. Les autres propriétés pourront être renseignées à tout moment après l'ajout du compte.

Les propriétés de comptes de base sont les suivantes :

- Identifiant : nom utilisé par l'utilisateur pour se connecter
- Nom : nom de famille de l'utilisateur
- Prénom : prénom de l'utilisateur
- Mot de passe, Confirmer le mot de passe : ces deux champs doivent contenir le mot de passe de l'utilisateur. Lorsque les mots de passe sont tapés, les caractères sont remplacés par des étoiles

- Adresse de messagerie : adresse email de l'utilisateur. Si l'annuaire est couplé à un webmail (tel roundcube), l'adresse renseignée est l'adresse email principale de réception d'emails de l'utilisateur
- Numéro de téléphone : numéro de téléphone de l'utilisateur
- Utilisateur désactivé, si cochée : permet de désactiver le compte UNIX de l'utilisateur, afin qu'il ne puisse plus ouvrir de session UNIX. Dans les faits, l'interpréteur de commande (voir plus bas) de l'utilisateur est positionnée automatiquement à `/bin/false`. La désactivation de compte UNIX n'affecte en rien l'état d'activation des autres types de propriétés du compte.

Pour les identifiants d'utilisateurs, il est recommandé d'utiliser uniquement des minuscules, et de suivre un schéma de nommage cohérent pour tous les utilisateurs. Par exemple, un site peut décider que les identifiants seront le nom des utilisateurs, ou le nom précédé ou suivi de la première lettre de leur prénom.

Une fois un compte créé, l'identifiant n'est pas modifiable. La seule façon de le faire est de détruire le compte et de le recréer.

Lorsque l'interface Mandriva Management Console est en mode expert, d'autres champs suivants sont aussi disponibles: Répertoire de l'utilisateur, Interpréteur de commande, UID, GID.

Le champ Groupe primaire permet la sélection du groupe principal de l'utilisateur. Un groupe par défaut est toujours proposé. Pour utiliser un autre groupe, effacez le nom proposé et commencez à taper le nom du groupe auquel vous désirez joindre l'utilisateur afin de bénéficier de l'auto-complétion.

6.2.3. Supprimer un compte utilisateur

Pour supprimer un compte utilisateur, cliquez sur la croix rouge dans la zone d'actions d'un compte utilisateur. Un popup s'affiche, et il vous est alors demandé si vous voulez supprimer définitivement les fichiers de l'utilisateur.

Si vous cochez la case Supprimer tous les fichiers de l'utilisateur lors de la suppression d'un compte, le contenu du répertoire personnel de l'utilisateur sera alors effacé définitivement.

6.3. Gestion des groupes d'utilisateurs

Un utilisateur peut appartenir à un ou plusieurs groupes. Les groupes servent à regrouper des utilisateurs afin de leur attribuer des droits communs.

6.3.1. Ajouter un groupe

Pour ajouter un groupe, cliquez sur l'onglet Ajout.

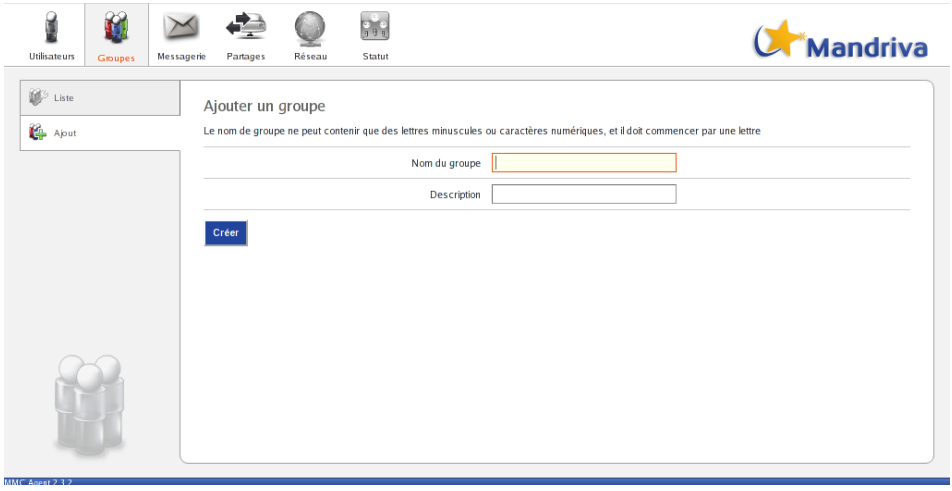


Figure 6-5. Liste des groupes d'utilisateurs

Il suffit alors d'entrer le nom d'un groupe dans l'entrée de texte proposée, puis de cliquer sur le bouton Créer.

6.3.2. Éditer les membres d'un groupe

Dans la liste des groupes, cliquez sur l'icône d'édition d'un groupe.

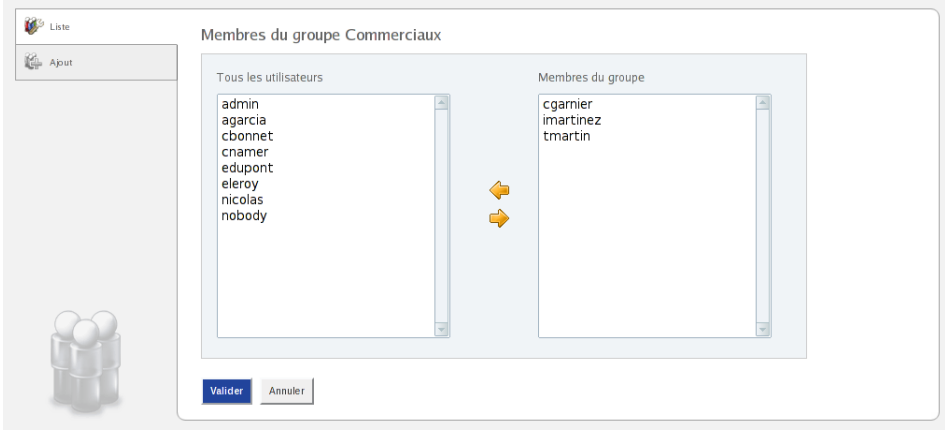


Figure 6-6. Édition des membres d'un groupe

La page d'édition des membres du groupe s'affiche alors. Elle est divisé en deux colonnes :

- La colonne de gauche est la liste de tous les utilisateurs enregistrés dans l'annuaire LDAP
- la colonne de droite est la liste courante des membres du groupe.

Grâce aux deux flèches rouges situées entre les deux listes, les utilisateurs sont ajoutés ou retirés du groupe. Il est possible de sélectionner plusieurs utilisateurs simultanément en faisant un clic droit avec la souris et en passant sur les utilisateurs simultanément. Une sélection discontinue est possible en cliquant sur les utilisateurs et en appuyant en même temps sur la touche « Ctrl» (Control) de votre clavier.

Il n'est pas possible d'enlever un utilisateur de son groupe primaire. Pour effectuer cette opération, il faut utiliser la page d'édition de l'utilisateur et changer son groupe primaire.

6.3.3. Supprimer un groupe

Dans la liste des groupes, cliquez sur l'icône de suppression d'un groupe, en forme de croix rouge.

La suppression du groupe ne supprime pas les utilisateurs de ce groupe. Ces utilisateurs ne font juste plus partie de ce groupe, puisqu'il n'existe plus.

6.4. Module Partages (Samba)

Samba met à disposition de postes Windows® des services de partages de ressources (fichiers, imprimantes, etc.) et d'authentification. La version de Samba disponible sur Mandriva Directory Server possède toutes les fonctionnalités d'un Contrôleur de Domaine Primaire Windows® NT4. Le module Samba est disponible en cliquant sur l'onglet Partages.

La Mandriva Management Console permet de configurer les principaux aspects du serveur Samba de Mandriva Directory Server :

- Contrôleur de domaine : Mandriva Directory Server peut faire office de contrôleur de domaine et ainsi gérer des comptes utilisateurs et machines d'un domaine Windows®, à la place d'un serveur Windows® NT4.
- Serveur de fichiers : la Mandriva Management Console permet de créer des dossiers partagés sur Mandriva Directory Server, accessibles ensuite via des postes Windows®.

6.4.1. Gestion de comptes utilisateurs Samba

Les comptes utilisateurs Samba sont équivalents à des comptes utilisateurs Windows®. Si le Mandriva Directory Server est utilisé en tant que contrôleur de domaine (PDC) Windows®, il est possible d'ajouter aux comptes utilisateurs des propriétés de compte Samba pour les transformer en comptes utilisateurs Windows®. Ainsi, les utilisateurs pourront se connecter sur le domaine Windows® et accéder aux ressources disponibles sur le domaine.

6.4.1.1. Ajout d'un utilisateur Samba

Aller dans le module Utilisateurs, et cliquer sur Ajout. Renseigner les propriétés de base de l'utilisateur comme expliqué dans le chapitre de gestion des utilisateurs, puis cocher la case Accès SAMBA.

Il est aussi possible d'ajouter les propriétés Samba à un utilisateur déjà existant.

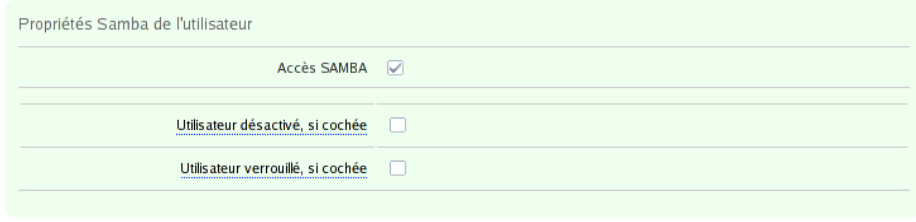


Figure 6-7. Propriétés Samba

Si on ajoute les propriétés SAMBA à un utilisateur déjà existant, le mot de passe de l'utilisateur est demandé une nouvelle fois. Ceci est du au fait que le mot de passe utilisateur au sens LDAP du terme et le mot de passe SAMBA ne correspondent pas au même attribut LDAP. De plus, comme le mot de passe de l'utilisateur est stocké de manière chiffrée dans l'annuaire (champ userPasswod), il n'est pas possible de le retrouver afin de calculer le mot de passe SAMBA (champ sambaNTPassword).

Pour un grand nombre d'utilisateur, il est possible d'utiliser un script faisant appel à l'API de programmation Mandriva Management Console afin d'automatiser cet ajout des propriétés SAMBA.

Les deux cases à cocher s'affichent :

- Utilisateur désactivé : si elle est cochée, l'utilisateur ne peut alors plus se connecter sur le domaine Windows® et utiliser les ressources mises à disposition par Samba.
- Utilisateur verrouillé : selon la configuration de Samba, il est possible que dans certains cas le compte Samba d'un utilisateur soit verrouillé. Par exemple, s'il s'est trompé plusieurs fois en tapant son mot de passe. Dans ce cas, son compte est verrouillé temporairement et il ne peut plus se connecter. Décochez alors cette case pour qu'il puisse se connecter à nouveau.

En mode expert, les champs supplémentaires suivants sont disponibles : Chemin du profil de l'utilisateur, Script d'ouverture de session, Chemin du répertoire de base et Connecter le répertoire de base au lecteur réseau .

Ces champs sont généralement configurés une fois pour toute pour le domaine, dans les options générales de Samba. S'ils sont laissés vides, les options générales seront utilisées. Il y a donc rarement besoin de les remplir.

6.4.1.2. Suppression d'un utilisateur Samba

Dans la page d'édition de l'utilisateur, il suffit de décocher la case Accès SAMBA et valider. L'utilisateur ne pourra alors plus accéder aux ressources disponibles sur le domaine.

6.4.2. Gestion des partages Samba

6.4.2.1. Ajouter un partage

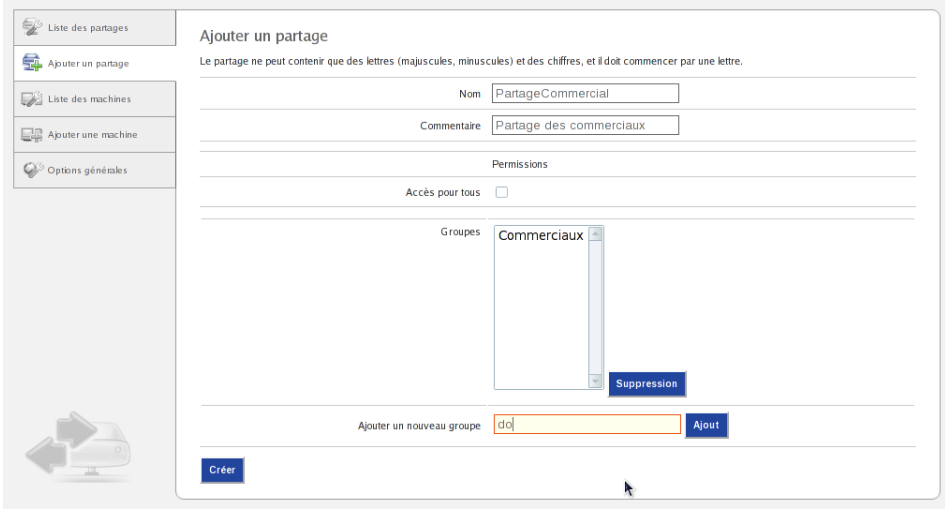


Figure 6-8. Ajouter un partage

Pour ajouter un partage sur le réseau, allez sur l'onglet Ajouter un partage.

Les champs suivants doivent alors être renseignés :

- Nom : nom du partage tel qu'il est disponible sur le réseau Windows®.
- Commentaires : ce texte sera visible depuis les clients Windows® lorsqu'ils consulteront les partages disponibles sur le serveur Mandriva Directory Server.
- Antivirus sur ce partage : active ou non l'analyse antivirus des fichiers ouverts sur ce partage. Les fichiers vérolés seront alors placés dans une zone de quarantaine.
- Permissions : droit d'accès au partage. Il faut choisir les groupes d'utilisateurs qui auront accès en lecture et en écriture sur le partage. Si la case Tout le monde est cochée, les utilisateurs ne faisant pas parti des groupes d'utilisateurs sélectionnés pourront aussi accéder au partage. Dans le cas contraire, seuls les membres des groupes sélectionnés pourront l'utiliser.

En mode expert, deux autres champs sont disponibles : Le partage est visible sur le domaine et Groupes administrateurs de ce partage.

La case Tout le monde cochée permet de créer rapidement une zone de partage public accessible à tous les utilisateurs.

Les groupes UNIX et Samba étant identiques, les utilisateurs UNIX ont les mêmes droits et restrictions d'accès sur le partage que les utilisateurs Windows®. La seule différence est la façon d'accéder au partage : les utilisateurs UNIX accèdent au partage directement via le système de fichiers du Mandriva Directory Server.

6.4.2.2. Éditer un partage

Pour éditer un partage, il faut cliquer sur l'icône d'édition dans la liste des partages dans la zone d'actions d'un partage.

Une page similaire à la création de partage s'affiche. Une fois les modifications faites, cliquez sur Modifier pour les appliquer.

Si les groupes sélectionnés dans les permissions sont changés, les utilisateurs des anciens groupes ne faisant pas partie des nouveaux groupes ne pourront alors plus accéder leurs fichiers, bien que ceux-ci leur appartiennent toujours.

6.4.3. Gestion des machines

Si SAMBA est configuré en tant que PDC (Contrôleur Primaire de Domaine), il est possible de gérer les machines inscrites dans le domaine Windows® dont il est le maître.

Les comptes machines sont similaires aux comptes utilisateurs, et sont enregistrés dans l'annuaire LDAP du Mandriva Directory Server.

Pour que les onglets Gestion des machines et Ajout d'une machine s'affichent, la case Ce serveur est un PDC doit être cochée dans l'onglet Options générales.

6.4.3.1. Ajouter une machine sur le domaine

Quand une machine est inscrite dans le domaine, les utilisateurs peuvent alors l'utiliser pour se connecter au domaine Windows®. Ainsi, ils auront accès à toutes les ressources partagées disponibles dans le domaine.

La méthode d'inscription proposée par l'interface ne fonctionne pas avec certaines versions de Windows®. Il est plutôt recommandé dans ce cas, de joindre la machine directement depuis l'interface de sélection de domaine de cette machine, dans ses paramètres de configuration Windows®.

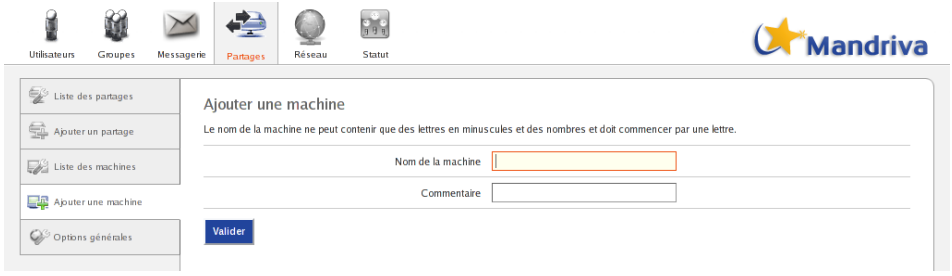


Figure 6-9. Ajouter une machine

Pour inscrire une machine sur le domaine depuis l'interface Mandriva Management Console, cliquez sur Ajouter une machine.

Renseignez alors les champs suivants :

- Nom de machine : nom NETBIOS de la machine sur le domaine Windows
- Commentaires : commentaires associés à la machine.

Enfin, cliquez sur Ajouter pour inscrire la machine sur le domaine.

6.4.4. Options générales de Samba

L'onglet Options générales permet de modifier les options principales du serveur Samba.

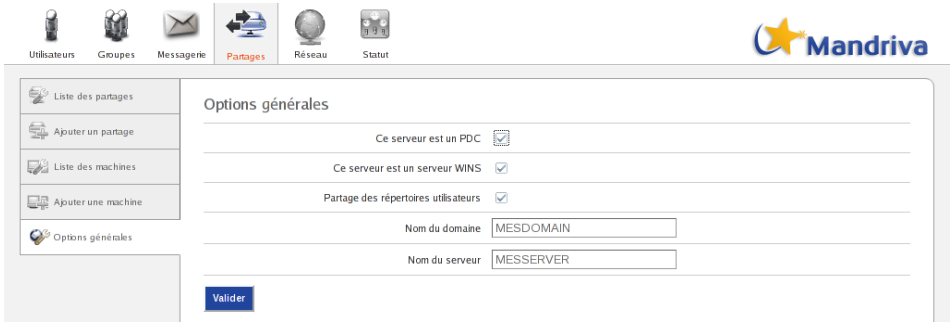


Figure 6-10. configuration de Samba

Les éléments de configuration suivants sont disponibles :

- Ce serveur est un PDC : si cette case est cochée, Samba simule le fonctionnement d'un contrôleur de domaine Windows® NT4 (PDC). Il s'annonce alors sur le réseau en tant que PDC, et fournit à tous les membres du domaine les services associés à cette responsabilité.
- Partager les répertoires utilisateurs : si cette case est cochée, lorsqu'un utilisateur Samba visualise les partages disponibles sur le serveur, il verra un partage dont le nom est identique à son identifiant, et dont le contenu est son répertoire personnel.
- Nom du domaine : domaine sur lequel est situé le serveur Samba. Si le serveur est un PDC, il s'agit du domaine que contrôle le PDC.

  Nom du serveur : nom NETBIOS du serveur Samba. Le serveur sera visible avec ce nom dans le domaine.

En mode expert, les mêmes champs que pour le mode expert des propriétés Samba d'un utilisateur sont disponibles : Chemin du profil de l'utilisateur, Script d'ouverture de session, Chemin du répertoire de base et Connecter le répertoire de base au lecteur réseau.

6.5. Module Messagerie

Mandriva Directory Server peut être couplé à un service de messagerie.

Ce service se connecte à l'annuaire afin :

- d'obtenir les informations nécessaires à la livraison des emails.
- d'identifier les utilisateurs lorsqu'ils se connectent à leur boîte avec leur client de messagerie.

La Mandriva Management Console permet de configurer :

- l'adresse de messagerie des utilisateurs, avec éventuellement des alias de messagerie.
- l'adresse de messagerie de groupe d'utilisateurs.
- de nouveaux domaines de messagerie, si le support de domaines de messagerie multiples est activé.

6.5.1. Mode de fonctionnement de la messagerie

L'administrateur ayant installé Mandriva Directory Server a choisi le mode de fonctionnement de la messagerie :

- domaine de messagerie unique : le service de messagerie ne délivre des mails que pour un seul domaine. Le domaine de messagerie de tous les utilisateurs de l'annuaire sera donc le même.
- domaines de messagerie multiples (aussi appelés domaines virtuels) : le service de messagerie délivre plusieurs domaines, et ces domaines pourront être gérés par l'intermédiaire de l'interface. Mandriva Directory Server est dans ce mode si l'onglet Messagerie est présent dans la barre de navigation de la Mandriva Management Console.

Selon le mode choisi, les champs de gestion du service de messagerie pour les utilisateurs sont différents.

6.5.2. Ajout et modification d'un utilisateur de la messagerie

Pour qu'un utilisateur puisse utiliser la messagerie, il faut, soit à la création de son profil soit en le modifiant, cocher la case Accès au service de messagerie. L'utilisateur doit avoir le champ Adresse de messagerie renseigné pour que cet accès soit possible.

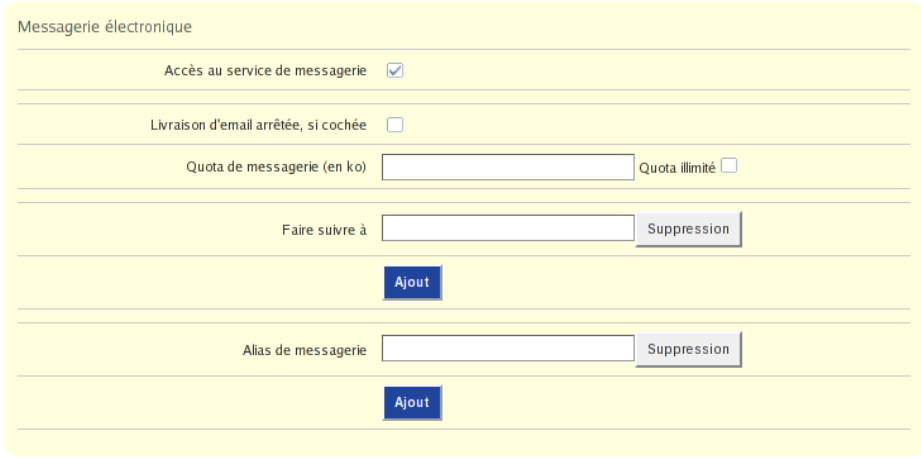


Figure 6-11. Ajout d'un compte de messagerie

Dans les deux modes de gestion du service de messagerie, les champs suivants sont disponibles :

- Livraison d'email arrêtée, si cochée : ce champ permet d'arrêter temporairement la livraison de messages à l'utilisateur.
- Alias de messagerie : il s'agit des adresses de messageries supplémentaires de l'utilisateur. Plusieurs utilisateurs peuvent avoir le même alias de messagerie afin d'envoyer des messages à un ensemble d'utilisateurs très simplement.

Dans le mode domaine de messagerie unique, le champ suivant est disponible :

- Utilisateur interne destinataire (maildrop) : il permet d'indiquer l'identifiant de l'utilisateur au sein de l'annuaire qui reçoit les mails pour l'adresse indiquée dans le champ Adresse de messagerie de l'utilisateur. Par défaut, c'est l'identifiant de l'utilisateur, car c'est dans la majorité des cas le comportement voulu. Il est possible de faire suivre les messages vers une autre adresse en renseignant tout simplement cette autre adresse dans le champ.

Dans le mode domaines de messagerie multiples, les champs suivants sont disponibles :

- Faire suivre à : tous les messages à destination de l'utilisateur seront renvoyés aux autres adresses de messagerie spécifiées dans ces champs
- Répertoire de livraison des emails : uniquement disponible en mode expert, ce champ permet de spécifier où seront stockées physiquement par le systè-

me de messagerie les messages de l'utilisateur. S'il n'est pas renseigné, ce champ est rempli automatiquement lors de la création du compte de messagerie.

6.5.3. Suppression d'un utilisateur de la messagerie

Dans la page d'édition d'un utilisateur, décochez la case Accès au service de messagerie. L'utilisateur ne recevra alors plus de mail.

6.5.4. Ajout et suppression d'un groupe d'utilisateurs dans la messagerie

Cette fonctionnalité permet d'envoyer simplement à un groupe d'utilisateur des messages, en utilisant le nom du groupe. Par exemple, si un groupe s'appelle `direction`, on pourra envoyer un message à tous les membres de ce groupe en utilisant l'adresse `direction@votre-domaine.org` .

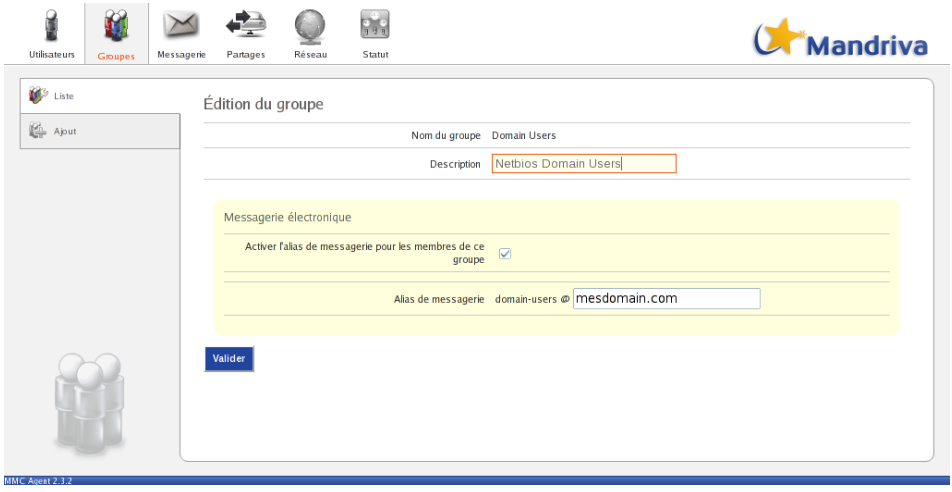


Figure 6-12. Alias de messagerie pour un groupe d'utilisateurs

Allez dans le module Groupes, et cliquez sur l'icône d'édition d'un groupe. Cliquez ensuite sur la case à cocher Activer l'alias de messagerie pour les membres de ce groupe. L'adresse de messagerie qui sera utilisé pour ce groupe s'affiche alors. Dans le cas de domaines multiples, vous aurez besoin de compléter le domaine de messagerie.

Cliquez sur Valider pour enregistrer les modifications. À ce moment là, les utilisateurs membres du groupe auront automatiquement un nouvel alias de

messagerie positionné sur l'adresse de messagerie de groupe que vous venez de créer. Quand un utilisateur sera ajouté ou supprimé de ce groupe, l'alias de messagerie du groupe sera respectivement ajouté ou supprimé.

Pour supprimer un groupe d'utilisateurs de la messagerie, il suffit de décocher la case.

6.5.5. Gestion des domaines de messagerie

Cette fonctionnalité n'est disponible qu'en mode multi-domaines.

Allez dans le module Messagerie. La liste des domaines de messagerie et leur description s'affiche. Le nombre d'utilisateurs dans chaque domaine est indiqué entre parenthèses. Il vous est possible de filtrer les domaines affichés grâce au champ de recherche.

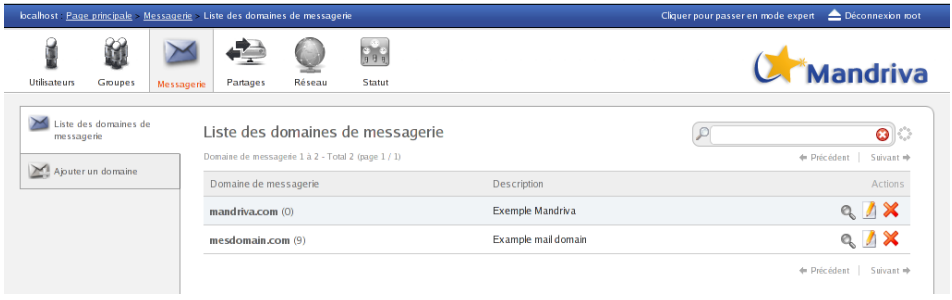


Figure 6-13. Liste des domaines de messagerie

Pour chaque domaine de la liste, les actions suivantes sont disponibles :

- Voir les membres du domaine : permet d'afficher et d'éditer les comptes utilisateurs ayant une adresse de messagerie dans ce domaine.
- Éditer le domaine : permet d'éditer la description du domaine de messagerie.
- Supprimer le domaine : permet de supprimer un domaine de messagerie. Attention, tous les utilisateurs ayant leur adresse dans ce domaine ne recevront plus de messages.

Pour ajouter un domaine de messagerie, cliquer sur Ajouter un domaine.

Il faut alors renseigner :

- Domaine de messagerie : nom DNS du domaine de messagerie (par exemple : « mandriva.com »).
- Description : texte libre pour décrire le domaine.

6.6. Module Réseau

Le module DNS/DHCP du Mandriva Directory Server permet de créer et de gérer pour un LAN :

- des zones DNS : enregistrement de type NS, A et CNAME, avec gestion automatique des zones inverses.
- des sous-réseaux DHCP : configuration, d'hôtes à IP statique, et intervalle d'IP dynamique.

Il est aussi possible de lier une zone DNS et un sous-réseaux DHCP ensemble. Ainsi, la création d'un hôte statique dans un sous-réseau DHCP déclenchera automatiquement la création d'un enregistrement de type A dans la zone DNS associée.

Les zones DNS et les configurations DHCP sont stockées dans l'annuaire.

6.6.1. Interface du module

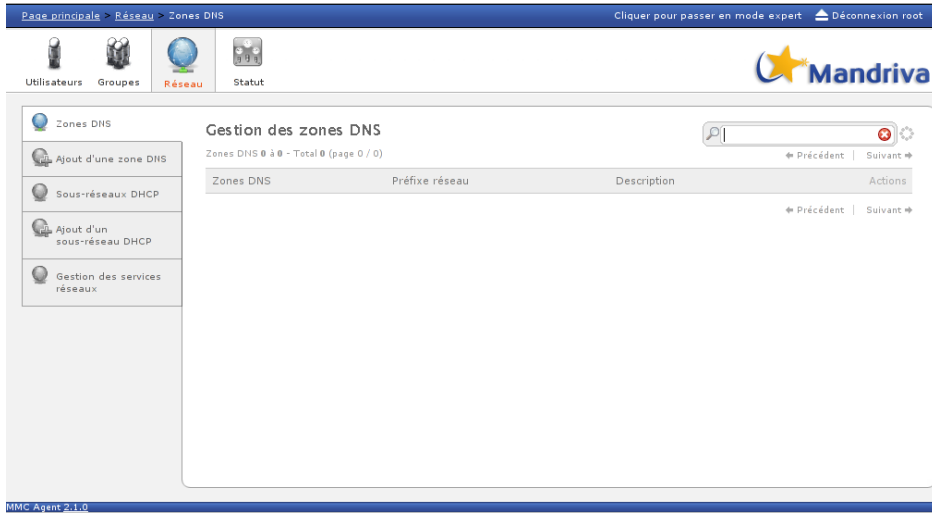


Figure 6-14. Module DNS/DHCP

Le module réseau du Mandriva Directory Server présente cinq onglets dans la partie gauche de l'interface :

- Les deux premiers sont dédies à la gestion du module DNS
- Les deux suivants sont dédies à la gestion du module DHCP
- Le dernier permet de gérer l'état des différents services gérés par ce module.

Comme dans toutes les pages du Mandriva Directory Server contenant des listes, il sera possible de faire une recherche dynamique à l'aide du champ situé en haut à droite.

Notons également que certains éléments de l'interface ne sont disponibles qu'en mode expert.

6.6.2. Gestion du DNS

6.6.2.1. Ajout d'une zone

Pour ajouter la gestion d'une zone sur le serveur DNS, cliquez sur l'onglet Ajout d'une zone DNS sur la gauche.

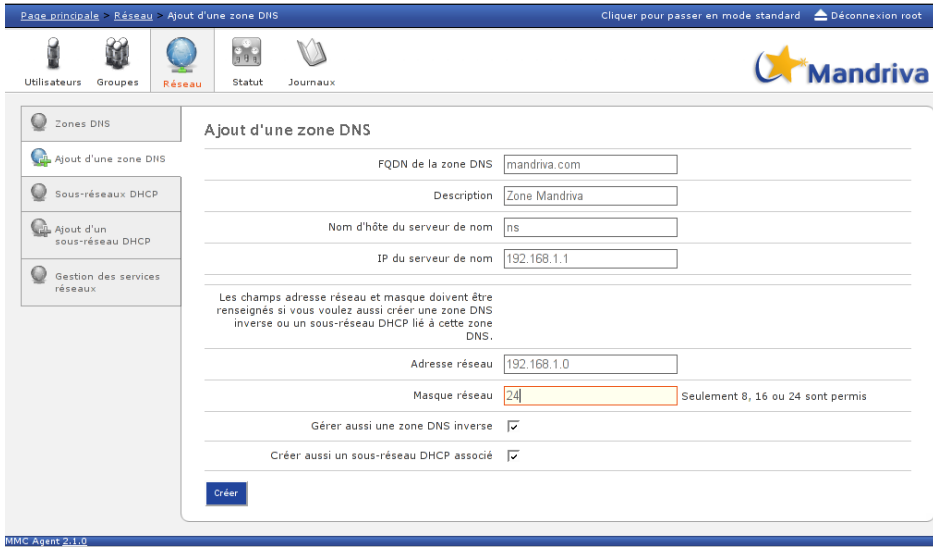


Figure 6-15. Ajout d'une zone DNS

La page présentée permet de renseigner les informations de base nécessaires à la création de la zone :

- FQDN de la zone DNS : il s'agit du nom de la zone proprement dit.
- Description : c'est un champ texte qui permet d'associer une description à la zone.
- Nom d'hôte du serveur de nom : nom DNS du serveur qui sera enregistré dans l'entrée NS de la zone.

- IP du serveur de nom : saisir ici l'adresse IP du serveur DNS. Cette IP sera associée au nom renseigné dans le champ précédent.

Cette page offre également la possibilité de créer un sous-réseau DHCP associé à cette zone DNS.

Si vous désirez gérer les services conjointement, vous pouvez alors renseigner les champs suivants :

- Adresse réseau : Adresse du réseau servi par le DHCP associé à la zone.
- Masque réseau : Masque de sous-réseau.
- Gérer aussi une zone DNS inverse : En sélectionnant cette option, la zone inverse associée au réseau sera gérée de manière transparente parallèlement à la zone standard.
- Créer aussi un sous-réseau DHCP associé : En sélectionnant cette option, la zone DNS et le sous-réseau seront liés et pourront être gérés conjointement.

Après validation, la zone qui vient d'être créée est visible directement en cliquant sur le bouton Zones DNS sur la gauche de l'écran.

La liste affichée présente alors l'ensemble des zones enregistrées dans le Mandriva Directory Server :

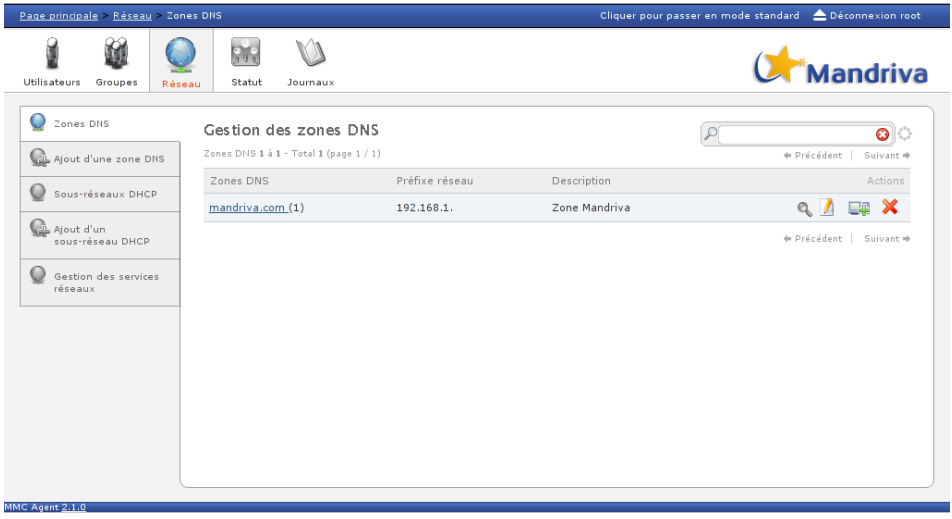


Figure 6-16. Liste des zones DNS gérées par Mandriva Directory Server

On retrouve dans cette liste le nom de la zone, sa description et éventuellement l'adresse du réseau associé. À droite de chaque ligne on retrouve quelques boutons permettant de gérer cette zone. Les actions associées à ces boutons sont détaillées dans les paragraphes suivants.

Le sous-réseau DHCP qui vient d'être créé avec la zone DNS est minimal. Pour compléter ce sous-réseau, voir le chapitre suivant qui détaille la gestion du service DHCP.

6.6.2.2. Ajout d'un enregistrement de type A

Lorsque la zone est créée, il est possible d'ajouter des enregistrements de type A. C'est à dire, d'associer directement un nom DNS à une adresse IP.

Pour cela, suivez la procédure suivante :

- Cliquez sur l'onglet Zones DNS à gauche.
- Cliquez sur le nom de la zone à éditer.
- Cliquez sur le bouton Ajouter un hôte.

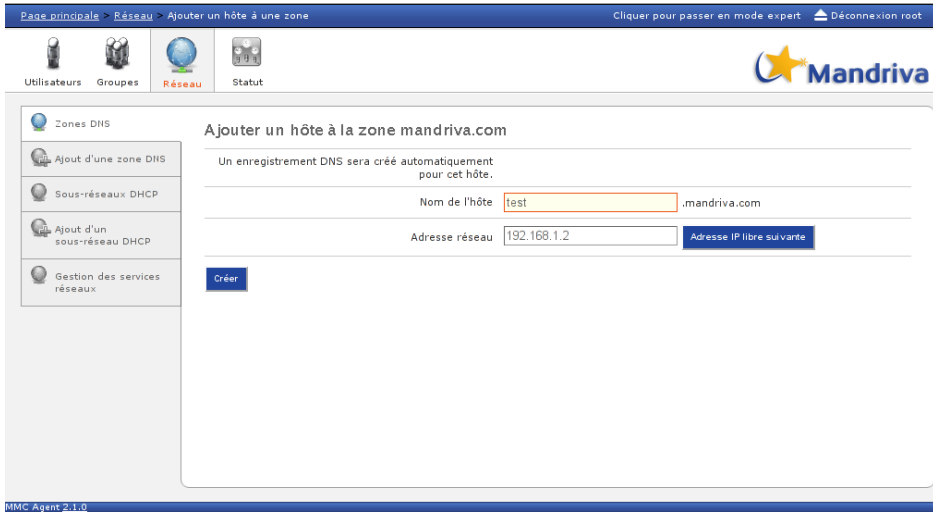


Figure 6-17. Ajout d'une entrée de type A

Un écran semblable à celui présenté ci-dessus apparaît.

- Saisissez d'abord le nom de la machine dans le champ Nom de l'hôte.
- Saisissez ensuite l'adresse que vous désirez associer à ce nom d'hôte.

Le bouton Adresse IP suivante recherche automatiquement l'adresse IP libre suivante.

La machine sera effectivement ajoutée dans la zone DNS lorsque vous aurez cliqué sur le bouton Créer.

6.6.2.3. Suppression d'un enregistrement de type A

Pour supprimer un enregistrement de type A, suivez simplement la procédure suivante :

- Cliquez sur l'onglet Zones DNS à gauche.
- Cliquez sur le nom de la zone à éditer.
- Cliquez sur le bouton de suppression correspondant à l'enregistrement que vous désirez supprimer.

Si un ou plusieurs CNAME étaient associés à cet enregistrement, ils seront également supprimés.

6.6.2.4. Gestion des enregistrements de type CNAME (ALIAS)

Les enregistrements CNAME permettent d'associer un ou plusieurs noms DNS à un autre nom DNS. Il est ainsi possible d'accéder à une même machine en utilisant plusieurs noms DNS différents au sein de la même zone.

Dans l'interface de Mandriva Directory Server, un enregistrement CNAME est forcement relatif à un enregistrement de type A.

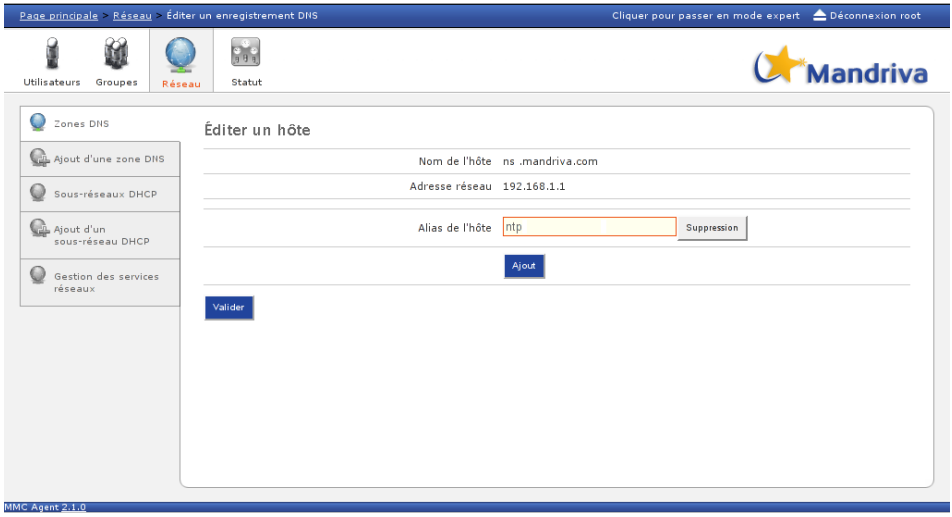


Figure 6-18. Ajout d'une entrée de type CNAME

Pour ajouter un CNAME sur un hôte, suivez la procédure suivante :

- Cliquez sur l'onglet Zones DNS à gauche.
- Cliquez sur le nom de la zone à éditer.
- Cliquez sur le bouton d'édition correspondant à l'enregistrement sur lequel vous désirez ajouter un CNAME.

Il est maintenant possible d'ajouter ou de supprimer autant de CNAME que vous le désirez à l'aide des boutons Ajout et Suppression.

6.6.2.5. Gestion des enregistrements de type MX

Les enregistrements MX (Mail eXchange) permettent de connaître les serveurs SMTP du domaine concerné. Chaque enregistrement MX doit contenir un nom d'hôte (qui doit de son côté disposer d'un enregistrement A) et une priorité.

Pour configurer votre enregistrement MX, suivez la procédure suivante:

- Cliquez sur l'onglet Zone DNS sur la partie gauche.
- Cliquez sur Éditer la zone.

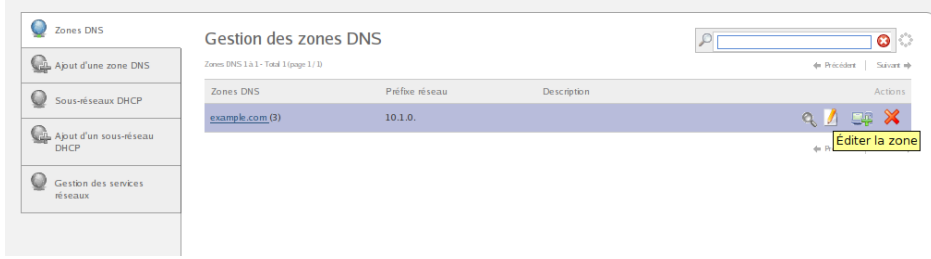


Figure 6-19. Éditer une zone DNS

- Dans le champ Enregistrements MX (serveurs SMTP), indiquez la priorité et le nom d'hôte de votre serveur SMTP. Par exemple: 10 smtp.example.com.

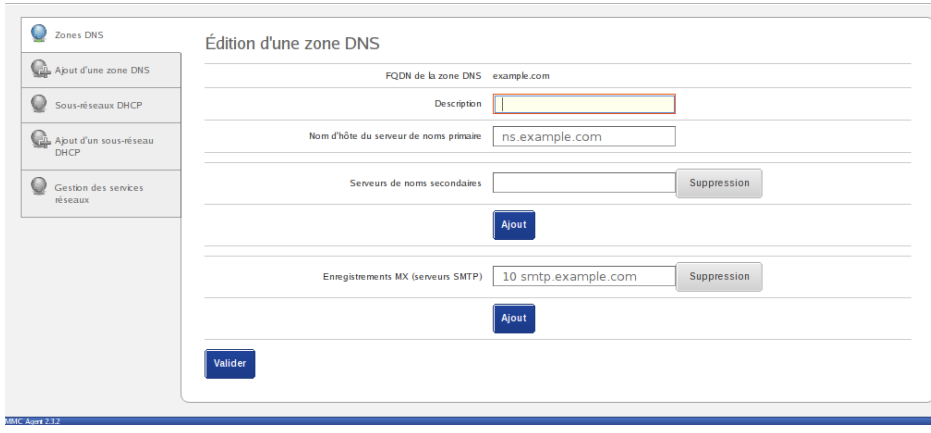


Figure 6-20. Enregistrements MX

6.6.2.6. Suppression d'une zone

La suppression d'une zone se fait simplement en cliquant sur le bouton se suppression disponible sur la droite dans la liste des zones.

La suppression d'une zone engendre automatiquement la suppression de tous les enregistrements précédemment créés dans cette zone, y compris dans l'annuaire LDAP.

6.6.3. Gestion du DHCP

6.6.3.1. Ajouter/Éditer un sous-réseau DHCP

Pour ajouter la gestion d'un sous-réseau DHCP, cliquez sur l'onglet Ajout d'un sous-réseau DHCP sur la gauche.

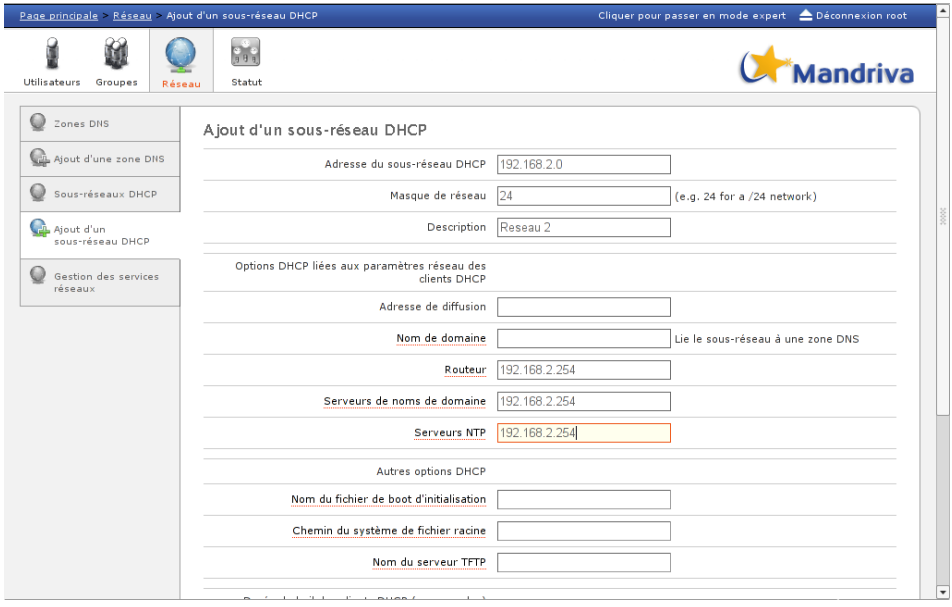


Figure 6-21. Ajout d'un sous-réseau DHCP

La page présentée permet de renseigner les informations de base nécessaires à la création du sous-réseau :

- Adresse du sous-réseau DHCP : Il s'agit de l'adresse du réseau à créer.
- Masque de réseau : Saisir le masque de réseau au format entier (8, 16 ou 24).
- Description : C'est un champ texte qui permet d'associer une description au réseau.

Les champs listés ensuite permettent de définir les options qui seront fournies aux clients DHCP :

- Adresse de diffusion : il s'agit de l'adresse de broadcast que l'on souhaite fournir aux clients.
- Nom de domaine : le domaine indiqué dans ce champ sera utilisé par les clients pour suffixer leurs requêtes DNS. Les clients pourront alors utiliser

le nom « ntp » au lieu de « ntp.mandriva.com ». Notons qui si le domaine renseigné ici est un domaine défini dans les Zones DNS de Mandriva Directory Server, le sous-réseau DHCP sera automatiquement lié à la cette zone.

- Routeur : C'est la passerelle par défaut qui sera fournie aux clients.
- Serveurs de noms de domaine : Saisir dans ce champ une liste d'adresses IP séparées par des virgules pour indiquer les serveurs de noms disponibles sur le réseau.
- Serveurs NTP : Saisir dans ce champ une liste d'adresses IP séparées par des virgules pour indiquer les serveurs de temps disponibles sur le réseau.

Il est également possible de définir des options avancées pour le serveur DHCP. Par exemple pour permettre aux machines du réseau de démarrer sur un serveur PXE ou pour modifier les durées des baux DHCP.

L'édition d'un sous-réseau DHCP se fait à l'aide de la même interface. Pour éditer un sous-réseau existant, cliquez simplement sur l'onglet Sous-réseau DHCP puis cliquez sur le bouton d'édition correspondant au sous-réseau à modifier.

6.6.3.2. Configuration d'un intervalle d'IP dynamique

Pour les machines qui ne sont pas encore enregistrées dans votre Mandriva Directory Server, vous pouvez définir une plage d'adresses dynamiques qui seront servies aux machines dont l'adresse physique (MAC) est inconnue.

Pour cela, cochez simplement la case Plage d'adresses dynamiques pour les clients DHCP non enregistrés et indiquez l'adresse de début et de fin de cette plage.

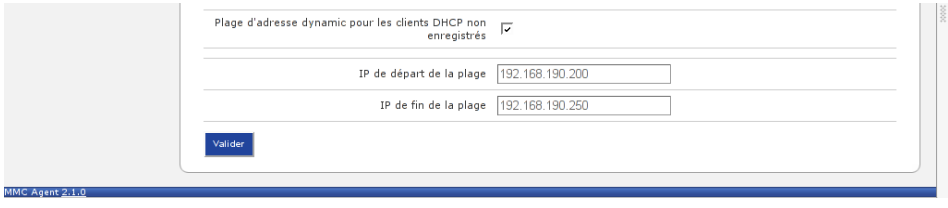


Figure 6-22. Plage d'adresses dynamiques

Après validation et re-démarrage du service DHCP, les clients recevront une adresse aléatoire appartenant à cette plage dynamique.

6.6.3.3. Ajouter/Modifier une configuration d'hôte statique

Mandriva Directory Server permet également de réserver une adresse IP à une machine particulière en se basant sur son adresse MAC. En utilisant cette méthode, le client dispose des avantages d'une IP attribuée par DHCP (facilité de configuration, distribution de paramètres, ...) et conserve toujours la même adresse IP.

Pour enregistrer cette réservation d'adresse, suivez la procédure ci-dessous :

- Cliquez sur l'onglet Sous-Réseaux DHCP à gauche.
- Cliquez sur le nom du réseau à éditer.
- Cliquez sur le bouton Ajouter un hôte statique.

Vous pouvez alors enregistrer un couple adresse MAC/adresse IP ainsi que certaines options spécifiques à cette machine (facultatif) comme indiqué sur l'écran ci-dessous :

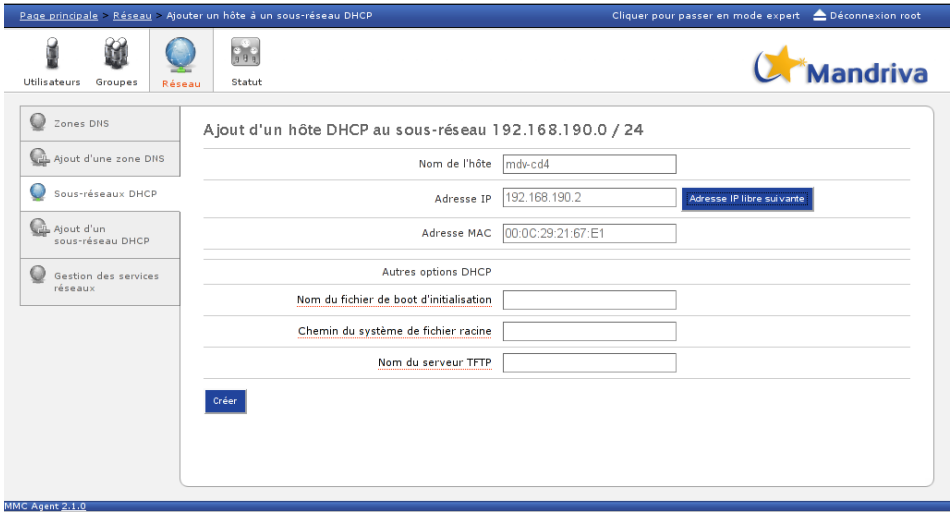


Figure 6-23. Ajout d'un hôte statique (réservation d'adresse)

Dans l'exemple présenté, la machine « mdv-cd4 » d'adresse MAC 00:0C:29:21:67:E1 recevra toujours l'adresse IP 192.168.190.2 par DHCP.

6.6.3.4. Transformer une configuration dynamique en configuration statique

L'inconvénient de la méthode présentée dans le paragraphe précédent est qu'il faut connaître l'adresse physique (MAC) de la machine. Pour contour-

ner ce problème, Mandriva Directory Server offre la possibilité de transformer un bail provenant de la plage dynamique en bail statique. Ainsi vous pouvez enregistrer une machine dans le DHCP, sans même saisir son adresse MAC.

Pour effectuer cette transformation, suivez la procédure suivante :

- Cliquez sur l'onglet Sous-Réseaux DHCP à gauche.
- Cliquez sur le nom du réseau à éditer.

L'écran présenté affiche alors la liste des hôtes statiques et la liste des machines ayant reçu une adresse de la plage dynamique.

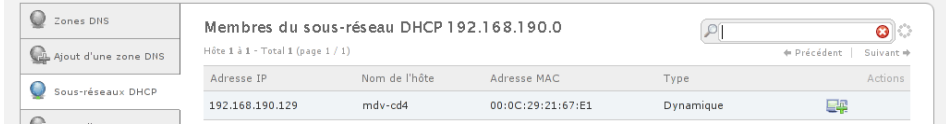


Figure 6-24. Transformation d'un hôte dynamique en hôte statique

6.6.3.5. Supprimer une configuration statique

Pour supprimer un réservation d'adresse et que la machine obtiennent une adresse IP appartenant à la plage d'adresses dynamiques, il suffit de cliquer sur le bouton de suppression disponible en face de la machine dans la liste des hôtes du sous-réseau.

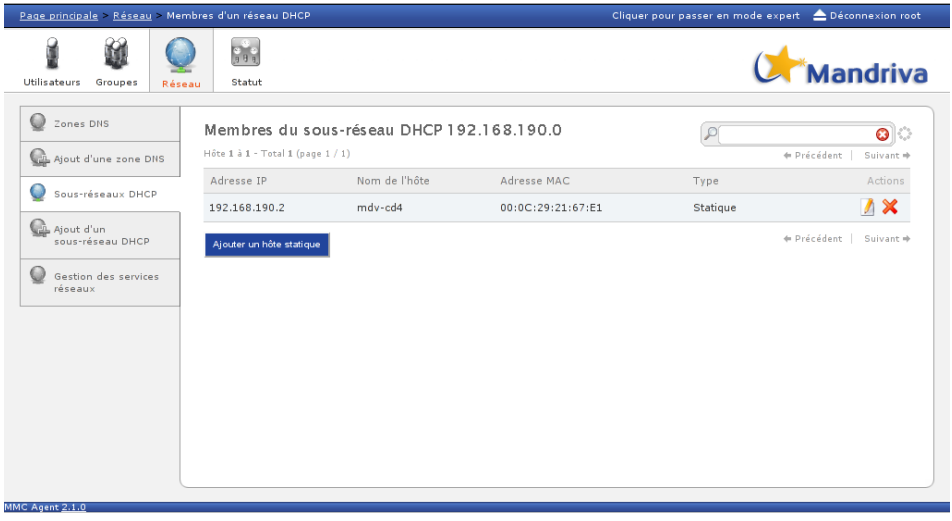


Figure 6-25. Suppression d'un hôte statique

6.6.3.6. Supprimer un sous-réseau DHCP

La suppression d'un sous-réseau DHCP se fait simplement en cliquant sur le bouton disponible sur la droite dans la liste des sous-réseaux.

Lors de la suppression d'un sous-réseau DHCP, tous les hôtes statiques appartenant à ce sous-réseau seront supprimés.

6.6.4. Gestion des services

6.6.4.1. Arrêt et démarrage

Le module fournit une interface permettant de gérer l'état des différents services gérés.

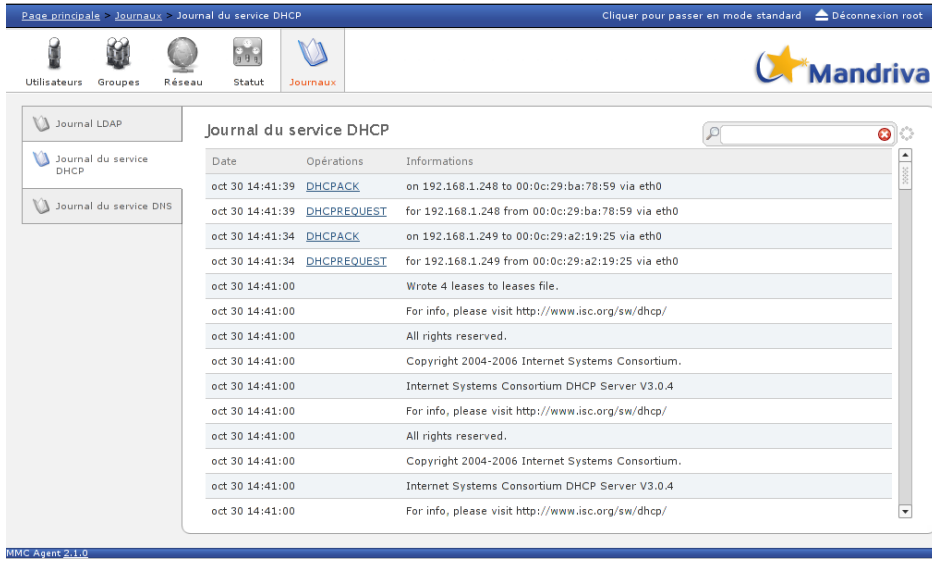


Figure 6-26. Gestion des services DNS et DHCP

Il est possible de stopper et de démarrer chaque service à l'aide des boutons stop et play. Pour recharger le service, cliquer simplement sur le bouton de rechargement.

Si des serveurs DNS sont configurés pour être esclave de cette zone, il faut impérativement recharger le service pour que les modifications soient automatiquement envoyées sur les serveurs esclaves.

6.6.4.2. Visualisation des journaux

En mode expert, le module offre une interface de visualisation des journaux de chaque service. Cette interface est accessible via le bouton loupe dans la page de gestion des services ou a travers l'onglet Journaux dans la menu supérieur. Notons que l'affichage des journaux est automatiquement actualisé.

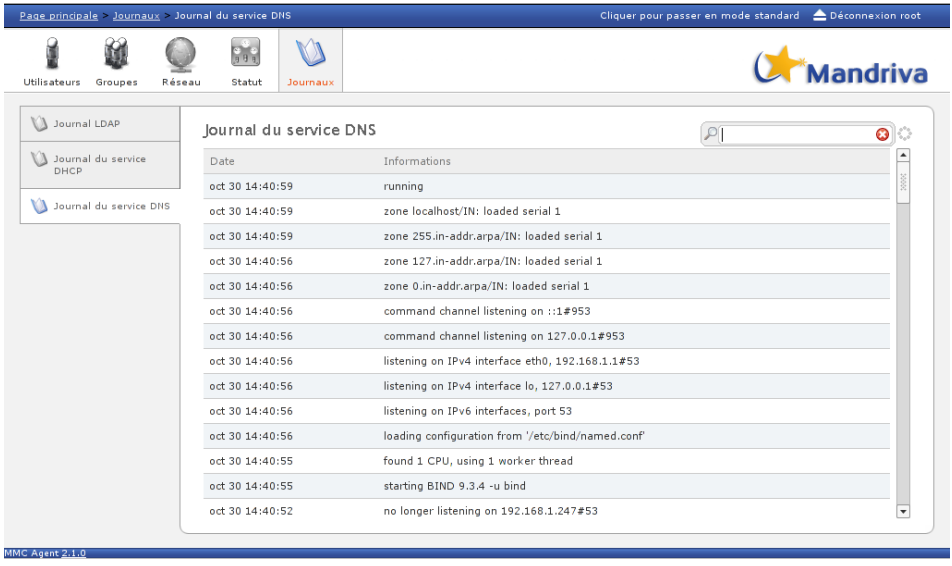


Figure 6-27. Visualisation des journaux DNS

6.7. Module d'audit

Le module d'audit permet de tracer toutes les opérations faites par les utilisateurs de l'interface web Mandriva Management Console. Des pages web de rapport permettent ensuite à l'administrateur de savoir qui a fait quoi, et quand.

Les opérations tracées sont les suivantes :

- modifications dans l'annuaire LDAP : Par exemple: création, modification, ou suppression d'un utilisateur.
- modifications sur le système de fichiers : Par exemple: création d'un partage Samba.
- démarrage et arrêt de service. Par exemple: arrêt du service DHCP.

D'une manière générale, toutes les opérations considérées comme sensibles sont enregistrées.

6.7.1. Onglet Audit

Pour visualiser les actions effectuées sur tous les modules, cliquez sur l'onglet Audit.

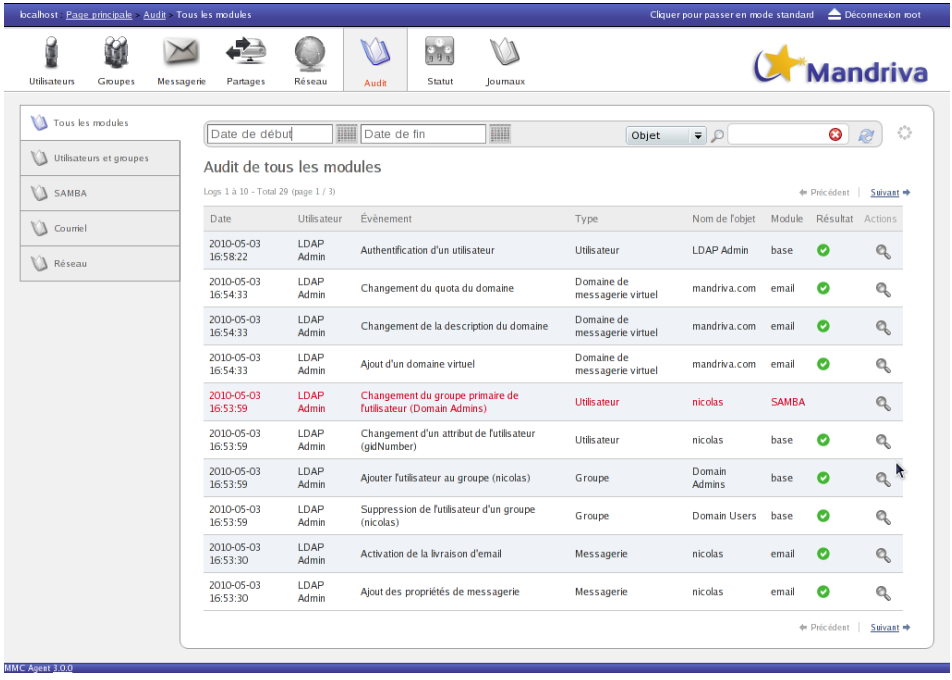


Figure 6-28. Liste des modifications dans tous les modules

Les évènements sont affichés par ordre chronologique inverse, afin d'accéder tout de suite aux derniers évènements. Les colonnes du rapport sont les suivantes:

- date : la date de l'évènement ;

- utilisateur : l'identifiant de l'utilisateur ayant déclenché l'évènement ;
- évènement : le nom de l'évènement ;
- type : le type de l'objet sur lequel porte l'évènement ;
- nom de l'objet : le nom de l'objet sur lequel porte l'évènement ;
- résultat : indique si l'évènement a été réalisé avec succès. Si oui, une icône verte est affichée dans la colonne. Dans le cas contraire, la colonne est vide, et la ligne est affichée en rouge ;
- actions : il est possible d'avoir plus de détails sur un évènement en cliquant sur l'icône en forme de loupe.

Plusieurs filtres sont disponibles:

- la période des évènements à afficher ;
- le nom de l'objet sur lequel on veut afficher tous les évènements associés. Par exemple, pour afficher toutes les opérations liées à l'utilisateur "jdoe", choisissez objet dans la liste déroulante, et renseignez "jdoe" dans la boîte de recherche ;
- le type des objets sur lesquels on veut afficher tous les évènements associés. Par exemple, pour afficher toutes les opérations liées aux zones DNS, choisissez Type dans la liste déroulante, puis Zone DNS ;
- le type d'opération. Par exemple, pour afficher toutes les opérations de suppression d'utilisateur, choisissez Action dans la liste déroulante, puis Suppression de l'utilisateur ;
- l'utilisateur déclenchant une opération. Pour afficher toutes les opérations effectuées par "jdoe", choisissez Utilisateur dans la liste déroulante, puis renseignez "jdoe" dans la boîte de recherche ;
- les onglets de gauche permettent de filtrer les opérations selon les modules disponible dans la Mandriva Management Console. Par exemple, pour afficher toutes les opérations du module Samba, cliquez sur l'onglet de gauche SAMBA.

6.7.2. Audit d'un utilisateur

Sur la page d'édition d'un utilisateur, le champ Dernière action affiche l'horodatage de la dernière opération qui a été effectuée sur le compte utilisateur.Quand on clique sur l'horodatage, le journal des évènements du compte utilisateur s'affiche.

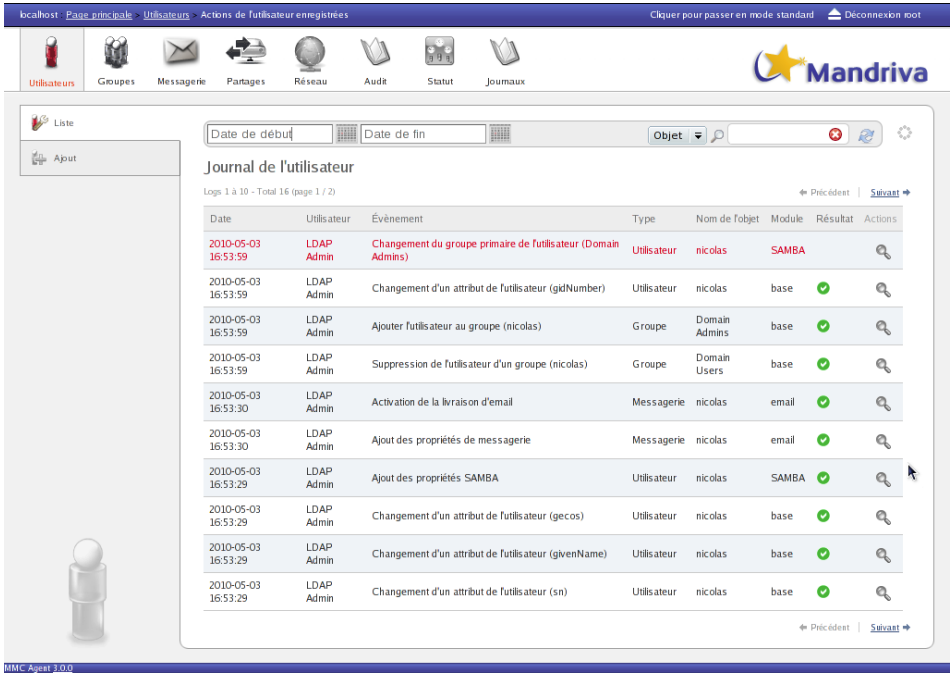


Figure 6-29. Audit d'un utilisateur

Ce rapport a la même forme que le rapport de l'onglet Audit, et comporte aussi certains filtres.

6.8. Module politique des mots de passe LDAP

Ce module est composé de deux parties:

- Par défaut, un serveur LDAP ne vérifie pas la qualité des mots de passe des comptes utilisateurs, et ne permet pas d'avoir des règles telles qu'une période de validité par exemple. La première partie de ce module consiste donc en une configuration particulière du serveur LDAP afin que celui-ci applique des politiques de mot de passe ;
- Ces politiques étant des objets LDAP, le module de politique des mots de passe de la Mandriva Management Console permet d'en régler les paramètres.

La Mandriva Management Console permet de gérer deux types de politique:

- la politique de mots de passe par défaut : elle est appliquée à l'ensemble des utilisateurs de l'annuaire LDAP, et donc de l'ensemble des utilisateurs déclarés via l'interface web Mandriva Management Console ;

- la politique de mots de passe par utilisateur . Si une politique est activée sur un compte utilisateur, la politique par défaut pour ce compte est ignorée.

6.8.1. Paramètres disponibles

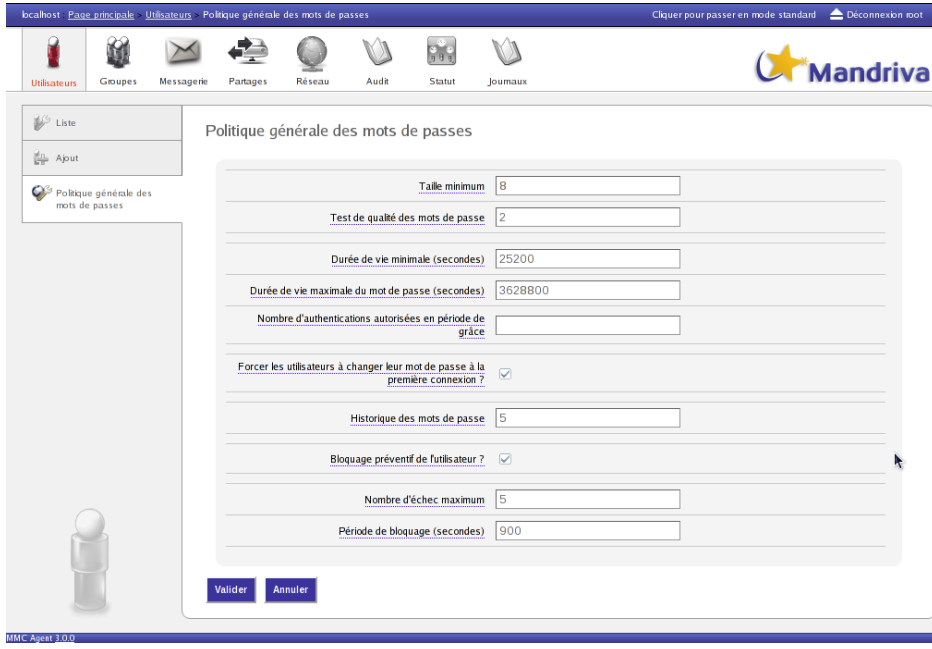


Figure 6-30. Paramètres de mot de passe globaux

Une politique de mots passe dispose des paramètres suivants:

- Taille minimum : cet attribut contient le nombre minimum de caractères pour un mot de passe ;
- Test de qualité des mots de passe : cet attribut indique comment la qualité du mot de passe est testée lors qu'il est ajouté ou modifié. Si cet attribut n'est pas présent, ou sa valeur est 0, le test de qualité n'est pas réalisé. Une valeur de 1 signifie que le serveur LDAP vérifiera sa qualité, et si le serveur ne peut pas le vérifier il sera tout de même accepté. Une valeur de 2 signifie que le serveur vérifiera sa qualité, et si le serveur ne peut pas le vérifier, il renverra une erreur et refusera le mot de passe ;
- durée de vie minimale (en secondes) : cet attribut contient le nombre de secondes qui doit s'écouler avant de pouvoir changer le mot de passe. Si cet

attribut n'est pas présent, le temps est fixé à 0 secondes. (i.e. le mot de passe peut être modifié aussi souvent que désiré) ;

- durée de vie maximale (en secondes) : cet attribut contient le nombre de secondes au bout duquel le mot de passe modifié expirera. Si cet attribut n'est pas présent ou est égal à 0, le mot de passe n'expire pas ;
- nombre d'authentification autorisées en période de grâce : cet attribut contient le nombre d'authentifications possible avec un mot de passe expiré. Si cet attribut n'est pas présent ou est égal à 0, les utilisateurs dont le mot de passe est expiré ne pourront pas s'authentifier ;
- forcer les utilisateurs à changer leur mot de passe à la première connexion : cette option défini si les utilisateurs doivent changer leur mot de passe quand il se connectent à l'annuaire après que le mot de passe ait été modifié par l'administrateur ;
- historique des mots de passe : cet attribut permet de définir le nombre maximum de mots de passe utilisés. Si cet attribut n'est pas présent ou est égal à 0, les mots de passe utilisés ne seront pas stockés, et donc des mots de passe précédemment utilisés pourront être re-utilisés ;
- blocage préventif de l'utilisateur : lorsque activé, cette option indique que le mot de passe ne peut plus être utilisé après un nombre donné d'échecs consécutifs lors de l'authentification. Le nombre maximum d'échec consécutifs est spécifié dans le champ Nombre d'échec maximum ;
- nombre d'échec maximum : cet attribut définie le nombre maximum d'échec à l'authentification consécutifs après lequel le mot de passe ne pourra plus être utilisé pour s'authentifier. Si cet attribut n'est pas présent ou est égal à 0, cette politique n'est pas appliquée. La valeur de Blocage préventif de l'utilisateur sera ignorée ;
- période de blocage (en secondes) : cet attribut contient le nombre de secondes pendant lequel un mot de passe ne peut pas être utilisé à cause d'un trop grand nombre d'échecs d'authentification consécutifs. Si cet attribut n'est pas présent ou est égal à 0, le mot de passe ne peut plus être utilisé jusqu'à ce qu'un administrateur remette à zéro le mot de passe.

6.8.2. Test de qualité des mots de passe

Si le test de qualité des mots de passe est activé, le mot de passe doit répondre à tous les critères suivants:

- il contient au moins un chiffre ;
- il contient au moins une lettre minuscule ;
- il contient au moins une lettre majuscule ;

- il contient au moins un caractère spécial (exemple: #, $, %, ...) ;
- tous les caractères sont différents.

6.8.3. Connexion des utilisateurs à la Mandriva Management Console

Si le module de politique de mots de passe est actif, un utilisateur qui se connecte à la Mandriva Management Console recevra un message d'avertissement si:

- le mot de passe de l'utilisateur a été ré-initialisé par un administrateur. Le compte LDAP de l'utilisateur est alors restreint, et celui-ci doit le changer dès que possible via la page de changement de mot de passe ;
- le compte utilisateur est en période de grâce. L'utilisateur doit alors changer son mot de passe dès que possible, sinon il sera bientôt bloqué.

6.8.4. Ré-initialisation d'un mot de passe utilisateur

Figure 6-31. Paramètres de mot de passe d'un utilisateur

Un drapeau de ré-initialisation du mot de passe est disponible sur la page d'édition du compte utilisateur. S'il est positionné, et si la politique de mot passe appliquée sur l'utilisateur le force à changer son mot de passe à la première connexion, un message d'avertissement le préviendra et lui demandera de changer son mot de passe (voir paragraphe précédent).

6.9. Authentification sur postes clients

Lorsque Samba est installé sur Mandriva Enterprise Server 5, il est alors possible de se connecter sur un poste client en s'authentifiant sur le domaine à l'aide de l'annuaire LDAP, que ce soit sur des postes Windows® ou Linux.

Pour cela, il est nécessaire que:

- le poste de travail soit joint au domaine;
- les comptes utilisateurs aient les droits d'accès Samba (pour les clients Windows® uniquement).

6.9.1. Clients Windows®

Pour un client Windows® 7 (Seven), il est nécessaire d'effectuer des actions préalables. Il faut en effet modifier la Base de registre Windows® - cf. (`http://wiki.samba.org/index.php/Windows7`):

```
HKLM\System\CCS\Services\LanmanWorkstation\Parameters
DWORD  DomainCompatibilityMode = 1
DWORD  DNSNameResolutionRequired = 0
```

Pour joindre un poste de travail Windows® à un domaine Samba, il faut accéder aux Propriétés Systèmes. Par exemple, en effectuant un clic droit sur Poste de travail puis Propriétés.

Figure 6-32. Joindre Windows® à un domaine: 1

Allez ensuite sur l'onglet Nom de l'ordinateur et cliquez sur le bouton Modifier.

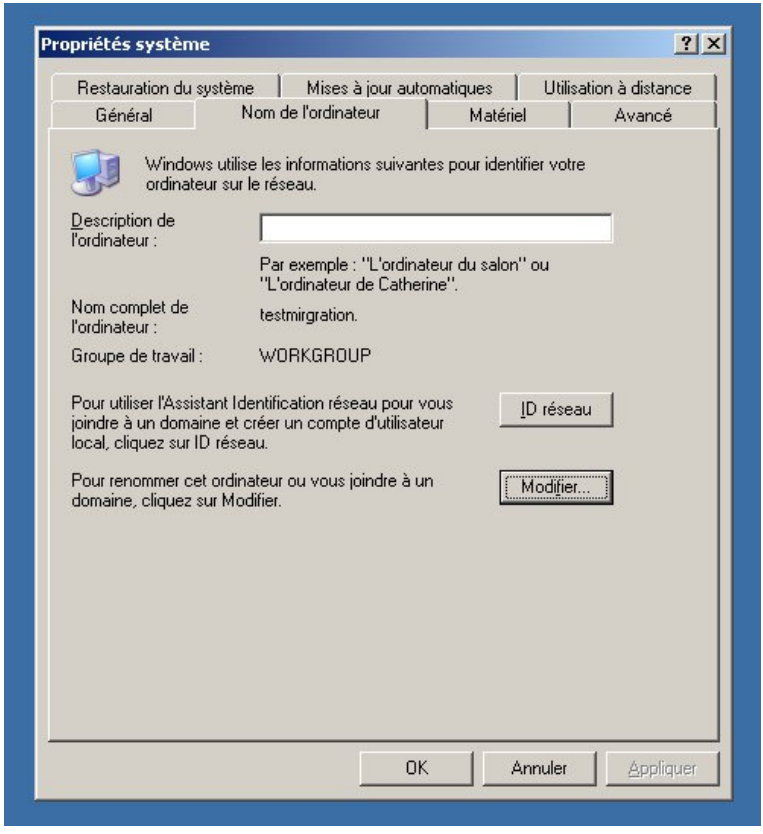


Figure 6-33. Joindre Windows® à un domaine: 2

Renseignez ensuite le nom de domaine et validez en cliquant sur le bouton OK.

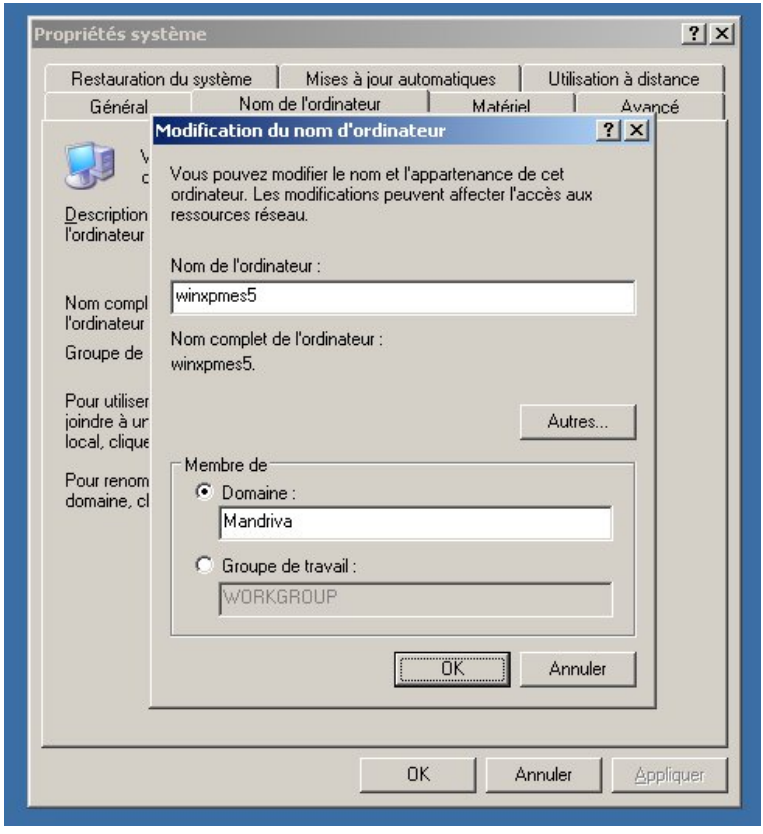


Figure 6-34. Joindre Windows® à un domaine: 3

Une fenêtre d'authentification apparaît. Renseignez alors le compte administrateur qui est autorisé à joindre le domaine Samba et validez ensuite à l'aide du bouton OK.

Ce compte correspond à un compte Administrateur du domaine créé dans la Mandriva Management Console.

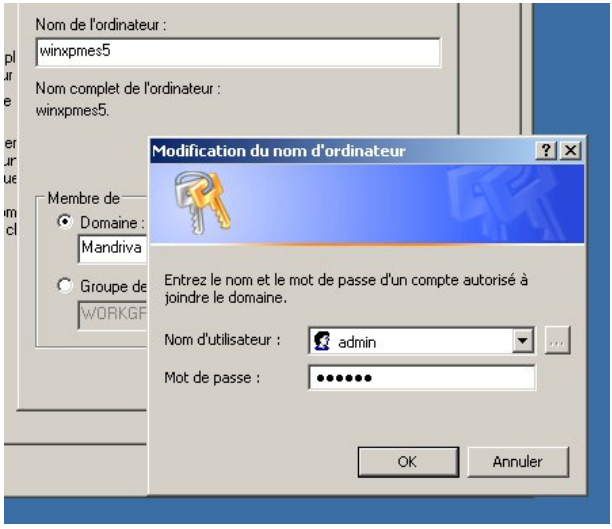


Figure 6-35. Joindre Windows® à un domaine: 4

L'opération peut prendre un peu de temps. Une nouvelle fenêtre doit apparaître vous indiquant que vous avez bien rejoint le domaine (Mandriva dans cet exemple).

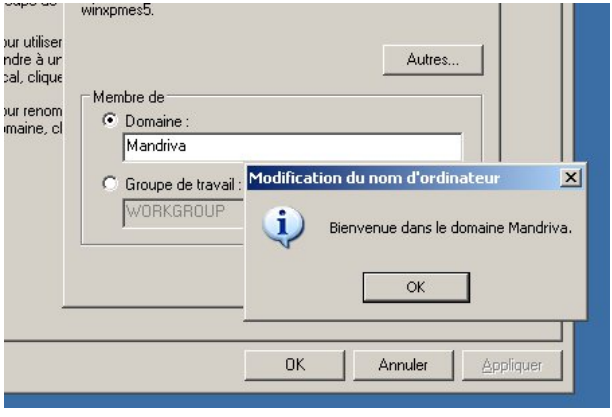


Figure 6-36. Joindre Windows® à un domaine: 5

Vous pouvez maintenant redémarrer le poste client. La fenêtre d'authentification de Windows® doit vous proposer le domaine (Mandriva dans cet exemple). Connectez vous alors avec un compte Utilisateur du domaine (user1 dans cet exemple).

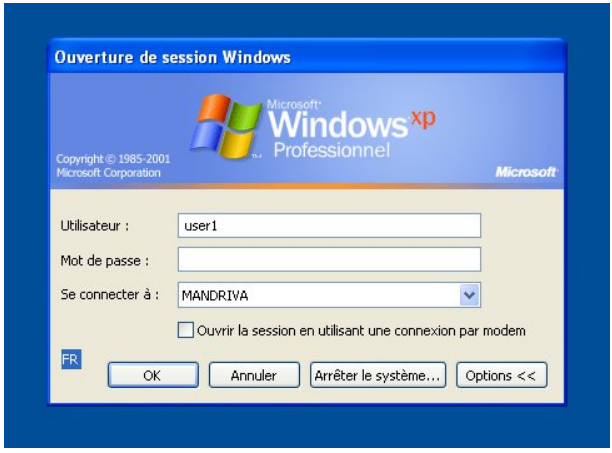


Figure 6-37. Connexion à un domaine sous Windows®

6.9.2. Clients Mandriva

La méthode d'authentification utilisée sous Linux sera directement LDAP.

Pour ce type d'authentification, il est nécessaire d'ouvrir le port 389 en tcp sur le serveur Mandriva Directory Server.

Pour configurer le client Mandriva Linux, utilisez l'outil Configurer votre Ordinateur à partir du menu. Une fois dans l'outil, allez dans l'onglet Système puis cliquer sur Authentification, comme indiqué sur la copie d'écran ci-dessous.

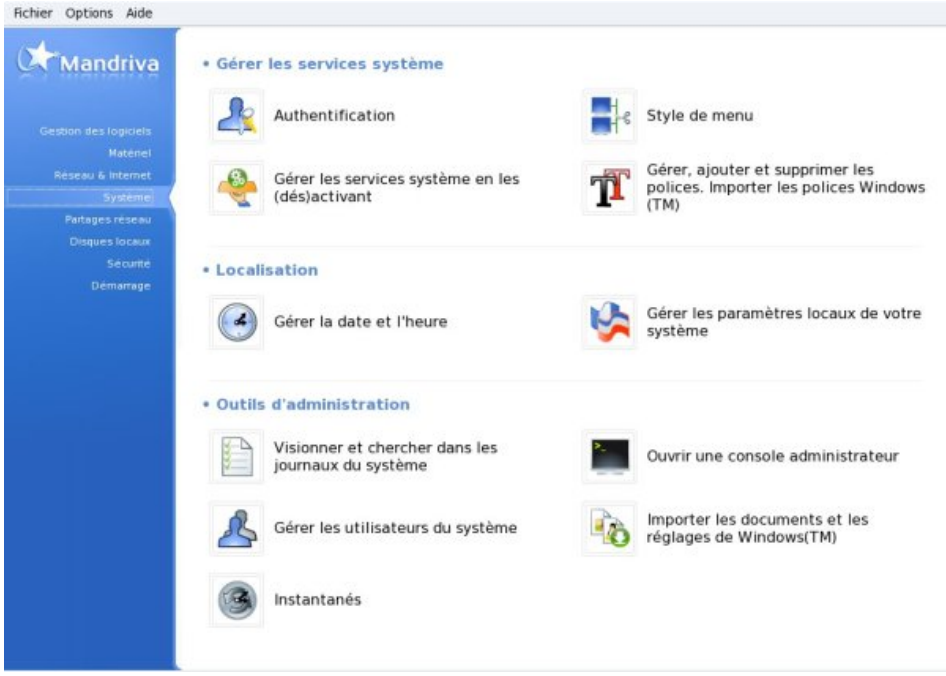


Figure 6-38. Authentification LDAP sous Mandriva: 1

Choisissez alors le type d'authentification, c'est à dire LDAP.

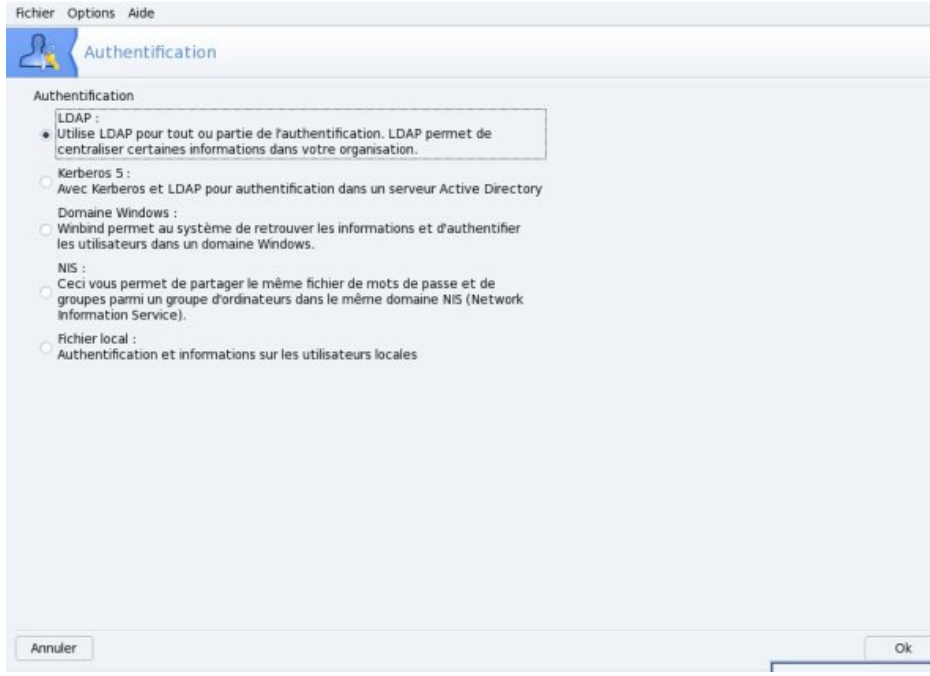


Figure 6-39. Authentification LDAP sous Mandriva: 2

Sur la fenêtre suivante, renseignez le nom de votre serveur LDAP dans le champ prévu a cet effet, c'est à dire le nom FQDN (de préférence) ou l'adresse IP du serveur Mandriva Directory Server.

Cliquez alors sur Récupérer le DN Racine, le champ Racine DN doit se renseigner automatiquement avec le suffixe de votre racine LDAP. Enfin, cliquez sur OK.

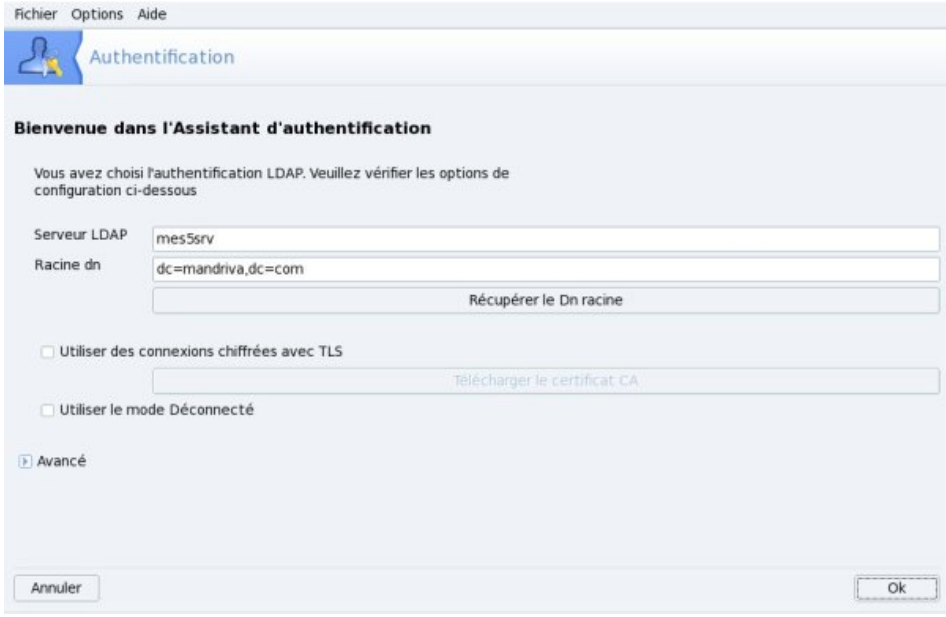


Figure 6-40. Authentification LDAP sous Mandriva: 3

Pour visualiser les comptes du domaine, vous pouvez exécuter la commande suivante dans une console :

```
# getent passwd
```

Chapitre 7. Stack Middleware

Gestion des intergiciels de Mandriva Enterprise Server 5

Tel que présenté dans le schéma des piles, Mandriva Enterprise Server 5 propose un certain nombre de composantes constituant les intergiciels parmi les plus courants pour des serveurs d'entreprises :

- serveur d'identité : le serveur d'annuaire OpenLDAP et le serveur d'authentification réseau Kerberos ;
- serveur de bases de données : MySQL et PostgreSQL, les deux principales bases de données libres.

7.1. Gestion des services Web : LAMP et Proxy

7.1.1. Gérer un serveur LAMP

Ce chapitre a pour but de présenter la mise en place d'une plate-forme LAMP (Linux, Apache, MySQL, PHP). Il décrit la méthode d'installation, les éléments spécifiques aux besoins du service, ainsi que la configuration mise en œuvre.

Voici quelques sources de renseignements supplémentaires :

- le site officiel d'Apache (`http://httpd.apache.org`) ;
- la documentation officielle d'Apache (`http://httpd.apache.org/docs/2.2`).

7.1.1.1. Installation et arborescence d'Apache

Mandriva Enterprise Server 5 fournit un certain nombre de paquets pour installer un serveur Apache, comprenant respectivement le serveur lui-même, des utilitaires, et des modules.

- `apache-mpm-prefork` : contient le démon serveur, dit MPM (*Multi-Processing Module*). Si vous avez choisi d'installer Mandriva Server Setup, `apache-mpm-prefork` a été automatiquement installé ;

- `apache-base` : contient les utilitaires Apache comme Apache Bench (ab) qui permet des tests de charge, des outils et les journaux (*logs*) ;
- `apache-modules` : contient les modules de base d'Apache ;
- `apache-conf` : contient l'ensemble des fichiers de configuration d'Apache ;
- `apache-doc` : abrite la documentation officielle d'Apache.

Vous pouvez compléter cette liste en fonction de vos besoins en installant des modules supplémentaires pour gérer des scripts PHP, le mode SSL sécurisé, l'authentification, etc. Tous ces paquets se nomment `apache-mod_*`.

L'arborescence d'Apache se présente de la manière suivante :

Les données : `/var/www` :

- `/var/www/` : racine des données servies par Apache (DocumentRoot) ;
- `/var/www/cgi-bin` : positionnement des scripts CGI ;
- `/var/www/error` : ensemble des pages d'erreur `http` ;
- `/var/www/html` : racine ;
- `/var/www/admin` : installation des applications Web d'administration ;
- `/var/www/icons` : icônes passées dans le domaine public proposées pour vos applications Web ;
- `/var/www/perl` : positionnement des scripts perl.

Les fichiers journaux Apache : `/var/log/httpd/` :

- `/var/log/httpd/access_log` : fichier journal des pages accédées ;
- `/var/log/httpd/error_log` : fichier journal des erreurs du serveur.

Les exécutables Apache :

- `/usr/sbin` : ensemble des exécutables du serveur et utilitaires associés ;
- `/etc/init.d/httpd` : initscript d'Apache.

Les fichiers de configuration d'Apache : `/etc/httpd` :

- `/etc/httpd` : racine de la configuration d'Apache (ServerRoot) ;
- `/etc/httpd/conf` : contient l'ensemble des fichiers de configuration de base du serveur ;
- `/etc/httpd/conf/fileprotector.conf` : directives de protection de certains fichiers sensibles (ex. : php) ;
- `/etc/httpd/conf/httpd.conf` : fichier de configuration principal du serveur ;
- `/etc/httpd/conf/mime.types` : configuration des types MIME ;
- `/etc/httpd/conf/vhosts.d` : répertoire contenant les fichiers de configuration des `virtualhosts` ;
- `/etc/httpd/conf/webapps.d` : fichiers de configuration des applications Web ;
- `/etc/httpd/conf.d` : contient un lien vers les modules Apache, les bibliothèques, les fichiers journaux Apache, et les fichiers de configuration des modules.

7.1.1.2. Configurer un serveur Apache

7.1.1.2.1. Configuration de base du serveur Apache

La configuration fournie en standard est souvent fonctionnelle sans aucune modification. Une des fonctionnalités les plus souvent utilisée est le recours aux serveurs virtuels (ou *virtualhosts*).Le terme de `virtualhost` fait référence à la possibilité d'héberger plusieurs sites sur un même serveur Apache.

Pour les activer, vérifiez que vous disposez de ces deux lignes dans `/etc/httpd/conf/httpd.conf` :

```
NameVirtualHost *:80
     Include conf/vhosts.d/*.conf
```

Il vous reste alors à les déclarer dans un fichier en indiquant le `DocumenRoot` (emplacement des fichiers) et le `ServerName` (nom identifiant le serveur virtuel). Au vu de la configuration fournie par défaut sous Mandriva Linux, vous devez fournir un fichier nommé `*.conf` positionné dans le répertoire `/etc/httpd/conf/vhosts.d`.

Si vous utilisez des serveurs virtuels combinés à du `https`, vous ne pourrez disposer que d'un serveur virtuel par adresse IP disponible.

Illustrons notre propos par un exemple :

```
<VirtualHost *:80>
     DocumentRoot /var/www/html/test1
     ServerName www.test1.com
     </VirtualHost>

     <VirtualHost *:80>
     DocumentRoot /var/www/html/test2
     ServerName www.test2.org
     </VirtualHost>
```

Redémarrez Apache et testez.

Pour des raisons de facilitation d'administration, il est recommandé de prévoir un fichier de configuration et un fichier journal par serveur virtuel.

7.1.1.2.2. Boîte à outils pour la gestion du serveur Apache

L'`initscript /etc/init.d/httpd` dispose d'options qui permettent de gérer le lancement, l'arrêt et la demande d'informations :

- Arrêter le serveur :

```
# service httpd stop
       Shutting down httpd:   [  OK  ]
```

- Démarrer le serveur :

```
# service httpd start
       Starting httpd:     [  OK  ]
```

- Redémarrer le serveur :

```
# service httpd restart
       Shutting down httpd:   [  OK  ]
       Starting httpd:     [  OK  ]
```

- Recharger la configuration du serveur :

```
# service httpd reload
       Reloading httpd:     [  OK  ]
```

- Consulter l'état du serveur :

```
# service httpd status
Apache is running.
httpd: 12137 12136 12135 12134 12133 12132 12131 12130 12122
```

- Consulter l'état détaillé du serveur :

```
# service httpd extendedstatus
                       Apache Server Status for localhost

   Server Version: Apache/2.2.9 (Mandriva Linux/PREFORK-12mdv2009.0)
          mod_ssl/2.2.9 OpenSSL/0.9.8h PHP/5.2.6 with Suhosin-Patch

   Server Built: Sep 20 2008 03:50:58
   ____________________________________________________________________

   Current Time: Wednesday, 06-May-2009 11:42:39 CEST
   Restart Time: Wednesday, 06-May-2009 11:42:37 CEST
   Parent Server Generation: 0
   Server uptime: 1 second
   Total accesses: 0 - Total Traffic: 0 kB
   CPU Usage: u0 s0 cu0 cs0
   0 requests/sec - 0 B/second -
   1 requests currently being processed, 7 idle workers

W_______.....................................................
.............................................................
.............................................................
.............................................................

   Scoreboard Key:
   "_" Waiting for Connection, "S" Starting up, "R" Reading Request,
   "W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
   "C" Closing connection, "L" Logging, "G" Gracefully finishing,
   "I" Idle cleanup of worker, "." Open slot with no current process

########################################
########################################
```

- Vérifier la configuration d'Apache (`httpd.conf`) :

```
# service httpd configtest
Vérification de l'intégrité de la configuration d'apache :      [  OK  ]
```

- Vérifier la configuration des *virtualhosts* :

```
# service httpd configtest_vhosts
Vérification de l'intégrité de la configuration d'apache :      [  OK  ]
```

- Démarrer le serveur en mode « debug » lors de tests avant mise en production :

```
# service httpd debug
Starting httpd (debug mode and in the foreground):
[Fri Sep 01 05:51:53 2008] [notice] core dump file size limit raised
 to 4294967295 bytes
[Fri Sep 01 05:51:53 2008] [info] mod_unique_id: using ip addr
 192.168.40.140
[Fri Sep 01 05:51:54 2008] [notice] Digest: generating secret for
 digest authentication ...
[Fri Sep 01 05:51:54 2008] [notice] Digest: done
[Fri Sep 01 05:51:54 2008] [info] mod_unique_id: using ip addr
 192.168.40.140
```

  Tous les messages apparaissent alors de manière détaillée sur la console.

Outre les commandes proposées ci-dessus, la commande `telnet` sur le port 80 ou 443 permet de valider le bon fonctionnement du serveur :

- Cas d'un serveur fonctionnel :

```
# telnet example.com 80
Trying 192.168.40.140...
Connected to example.com (192.168.40.140).
Escape character is '^]'.
```

- Cas d'un serveur non fonctionnel :

```
# telnet example.com 80
Trying 192.168.40.140...
telnet: connect to address 192.168.40.140: Connection refused
telnet: Unable to connect to remote host: Connection refused
```

7.1.1.3. Configuration avancée d'Apache

7.1.1.3.1. Configurer https

Vous devez au préalable installer le RPM `apache-mod_ssl`.

Par défaut, une clé privée et un certificat sont générés lors de l'installation du RPM. La génération nécessite le RPM `openssl`. Les clés et certificats sont stockés par défaut dans `/etc/pki/tls/private/localhost.key` et `/etc/pki/tls/certs/localhost.crt`.

Voici comment générer votre propre clé:

Les opérations sont à réaliser dans `/etc/pki/tls/private/` :

```
# openssl genrsa -des3  -out server.key 1024
```

Retirez le mot de passe de la clé privée :

```
# openssl rsa -in server.key -out server.pem
```

Vous devez ensuite générer le certificat qui sera affiché lors de la connexion sécurisée. Pour ce faire, tapez la commande qui suit. Vous pouvez entrer les valeurs du certificat par défaut en éditant le fichier `/usr/lib/ssl/openssl.cnf`.

```
# openssl req -new -key server.key -out server.csr
```

Vous pouvez alors le signer vous-même comme suit si vous n'avez pas d'autorité de certification :

```
# openssl x509 -req -days 60 -in server.csr

-signkey server.key -out server.crt
```

Les fichiers de configuration de `apache-mod_ssl` sont :

- `/etc/cron.daily/certwatch`
- `/etc/httpd/modules.d/40_mod_ssl.conf`
- `/etc/httpd/modules.d/41_mod_ssl.default-vhost.conf`

Il faut éditer une section dans le fichier `/etc/httpd/modules.d/41_mod_ssl.default-vhost.conf` afin de pouvoir mettre en place le certificat sur une partie du serveur.

```
<IfDefine HAVE_SSL> <IfModule !mod_ssl.c>
     LoadModule ssl_module modules/mod_ssl.so </IfModule>
     </IfDefine>

     <IfModule mod_ssl.c>
     NameVirtualHost 192.168.40.119:443
     <VirtualHost toto:443>
     ServerName toto
     SSLEngine on
     SSLCertificateFile /etc/pki/tls/certs/localhost.crt
     SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
     DocumentRoot /var/www/html/vhost4
     ErrorLog logs/ssl_error_log
     <IfModule mod_log_config.c>
     TransferLog logs/ssl_access_log
```

```
</IfModule>
</VirtualHost>
</IfModule>
```

Après avoir relancé le serveur, on doit pouvoir accéder à l'URL `https://192.168.40.119` et ainsi accepter le certificat proposé par la machine.

7.1.1.4. Sécuriser Apache

7.1.1.4.1. Sécuriser la configuration de base

Sécuriser Apache consiste essentiellement à modifier la configuration de base fournie à l'installation, en grande partie dans le fichier `/etc/httpd/conf/httpd.conf`.

Supprimons d'abord la bannière de présentation du service, elle fournit des informations fort utiles pour orienter une attaque sur Apache. Dans `/etc/httpd/conf/httpd.conf` :

```
ServerSignature Off
     ServerTokens Prod
```

Pour vérifier, utilisez la commande HEAD :

- avec bannière :

```
$ HEAD http://dhcp140
200 OK
Connection: close
Date: Wed, 06 May 2009 09:43:52 GMT
Accept-Ranges: bytes
ETag: "1bdd3-d7-452ee8885b240"
Server: Apache/2.2.9 (Mandriva Linux/PREFORK-12mdv2009.0)
Content-Length: 215
Content-Type: text/html
Last-Modified: Sat, 26 Jul 2008 14:59:13 GMT
Client-Date: Wed, 06 May 2009 09:43:52 GMT
Client-Peer: 192.168.40.140:80
Client-Response-Num: 1
```

- sans bannière :

```
$ HEAD http://dhcp140
200 OK
Connection: close
Date: Wed, 06 May 2009 09:50:04 GMT
Accept-Ranges: bytes
ETag: "1bdd3-d7-452ee8885b240"
Server: Apache
```

```
  Content-Length: 215
  Content-Type: text/html
  Last-Modified: Sat, 26 Jul 2008 14:59:13 GMT
  Client-Date: Wed, 06 May 2009 09:50:04 GMT
  Client-Peer: 192.168.40.140:80
  Client-Response-Num: 1
```

On recommande également de supprimer la résolution de nom : elle encombre inutilement le réseau. Dans `/etc/httpd/conf/httpd.conf` :

```
HostnameLookups Off
```

Supprimons également la possibilité de publier des pages Web dans le répertoire `/home` des utilisateurs (module `Apache mod_userdir`). Celui-ci n'est maintenant plus installé par défaut. Vous pouvez vérifier la présence du paquetage :

```
# rpm -qa | grep apache-mod_userdir
```

La ligne suivante doit être mise en commentaire dans `/etc/httpd/conf/httpd.conf` :

```
# LoadModule userdir_module modules/mod_userdir.so
```

Interdire l'affichage des index de pages : dans les définitions des directives `<Directory>`, désactivez le plus possible les `Indexes`. Vérifiez la présence de la directive `<Directory />` dans `/etc/httpd/conf/httpd.conf`. Elle doit comprendre au moins les éléments suivants :

```
<Directory />
    Options -Indexes
    AllowOverride None
     </Directory>
```

7.1.1.4.2. Sécuriser les virtualhosts

En cas d'utilisation de virtualhosts sur la machine, créez un « virtualhost catch-all ». Ainsi, si un visiteur lance une requête sur l'adresse IP plutôt que le nom du « virtualhost », vous contrôlerez la page affichée.

```
<VirtualHost _default_:*>
     DocumentRoot /var/www/html/defaut
     </VirtualHost
```

Pensez à créer le répertoire correspondant au `DocumentRoot` spécifié et positionnez un fichier `index.html` à l'intérieur, par exemple.

Il est également utile de disposer de fichiers journaux spécifiques à chacun des virtualhosts définis, de manière à être capable d'identifier d'éventuels problèmes rapidement. On obtient alors l'arborescence de fichiers journaux suivante (à créer) :

```
/var/log/httpd/
 |-virtualhost1
 | |-access_log
 | `-error_log
 |-virtualhost2
 | |-access_log
 | `-error_log
 ...
```

Ci-dessous un exemple de fichier de configuration d'un virtualhost utilisant cette séparation de fichiers journaux :

```
# cat /etc/httpd/conf/vhosts.d/virtualhost1
     <VirtualHost 172.20.30.40>
     DocumentRoot /var/www/html/virtualhost1
     ServerName virtualhost1.domaine.com

     ErrorLog logs/virtualhost1/error_log
     CustomLog logs/virtualhost1/access_log combined
     </VirtualHost>
```

Il faut également penser à mettre à jour le système de rotation des fichiers journaux d'Apache pour prendre en compte les nouveaux fichiers créés :

```
# cat /etc/logrotate.d/httpd
/var/log/httpd/*_log /var/log/httpd/virtualhost1/*_log
 /var/log/httpd/apache_runtime_status /var/log/httpd/ssl_mutex {
    rotate 5
    monthly
    missingok
    notifempty
    nocompress
    prerotate
        /etc/rc.d/init.d/httpd closelogs > /dev/null 2><1
    endscript
    postrotate
        /etc/rc.d/init.d/httpd closelogs > /dev/null 2><1
    endscript
}
```

7.1.1.5. Mettre à disposition PHP

7.1.1.5.1. Installation et configuration de PHP

Seul PHP5 est fourni sur Mandriva Enterprise Server 5. Par défaut, PHP5 est compilé avec un correctif spécifique « Suhosin-Patch », permettant d'apporter des éléments supplémentaires de sécurité. Pour en savoir plus , visitez le site de hardened-php (`http://www.hardened-php.net/suhosin/`).

On installera principalement le paquetage `apache-mod_php` qui modifiera également la configuration d'Apache pour prendre en compte l'interprétation de PHP et redémarrer Apache. Son installation entraîne des dépendances consistant en modules de base PHP jugés nécessaires dans la majeure partie des configurations.

Dans le cas de la mise en place d'une plate-forme « LAMP », il faudra également installer le module Apache permettant de réaliser des requêtes SQL en PHP : `php-mysql`

La configuration de PHP se fait essentiellement dans `/etc/php.ini`. Chaque fonctionnalité est introduite sous forme de [bloc]. Chaque variable est écrite de la manière suivante :

```
variable = valeur
```

Le fichier fourni par défaut est suffisant pour disposer de PHP de manière fonctionnelle. On verra comment le sécuriser dans le chapitre suivant (Section 7.2).

Mandriva Enterprise Server 5 propose une particularité : `/etc/php.d`. Pour éviter d'alourdir le fichier `php.ini`, tous les modules dynamiques font l'objet d'un fichier dédié dans `/etc/php.d` et sont inclus dans la configuration globale. Ainsi, de base, on trouve les fichiers suivants :

```
# ls /etc/php.d
12_ctype.ini      22_ftp.ini        37_mysqli.ini     57_sysvsem.ini
13_curl.ini       23_gd.ini         42_pgsql.ini      58_sysvshm.ini
18_dom.ini        24_gettext.ini    43_posix.ini      60_tokenizer.ini
21_openssl.ini    26_iconv.ini      47_session.ini    62_xml.ini
21_zlib.ini       28_ldap.ini       54_hash.ini       62_xmlrpc.ini
63_xmlreader.ini  64_xmlwriter.ini  70_pdo.ini        78_sqlite.ini
81_filter.ini     82_json.ini       98_suhosin.ini
```

7.1.1.5.2. Sécuriser PHP : améliorer la configuration de base

Nous vous proposons un certain nombre de points à améliorer dans la configuration fournie par défaut. Les modifications proposées ci-dessous sont toutes à réaliser dans le fichier `/etc/php.ini`.

- Désactiver dans un premier temps les variables globales si les applications le supportent :

```
register_globals = Off
```

- Supprimer PHP de la bannière : la mise à disposition de PHP sur le serveur n'apparaît plus dans les en-têtes du serveur :

```
expose_php = Off
```

- Supprimer également l'affichage des messages d'erreur lors de l'exécution de scripts PHP, qui peuvent donner des informations sur d'éventuelles vulnérabilités :

```
display_errors = Off
```

- Activer les logs PHP, ceci afin de permettre de déboguer rapidement un script en consultant les logs gérés par le démon `syslogd` :

```
log_errors = Off
       error_log = syslog
```

- Désactiver le téléchargement vers le serveur (*upload*) de fichiers :

```
file_uploads = Off
```

- Désactiver l'utilisation des « magic quotes » :

```
magic_quotes_gpc = Off
       magic_quotes_runtime = Off
       magic_quotes_sybase = Off
```

- Interdire le chargement de modules externes :

```
enable_dl = Off
```

- Ne pas autoriser le traitement d'URL comme des fichiers : le paramètre permet alors d'aller télécharger sur un autre serveur :

```
allow_url_fopen = Off
```

- Supprimer **.** du chemin des librairies : à utiliser avec précaution car certains scripts peuvent ne plus fonctionner :

```
include_path = "/usr/lib/php/:/usr/share/pear/"
```

- Enfermer l'exécution des scripts PHP : permet de limiter les répertoires dans lesquels les scripts pourront être appelés. Vous pouvez en spécifier plusieurs, séparés par des virgules :

  ```
  open_basedir = /var/www/html/appli
  ```

  En cas d'utilisation de virtualhosts, l'option est plus significative lorsqu'elle est spécifiée dans la configuration même du virtualhost, ce qui permet d'affiner le comportement de PHP :

  ```
  <VirtualHost 127.0.0.1>
   DocumentRoot /var/www/html/virtualhost1/html
   ServerName virtualhost1.domaine.com
   php_admin_value open_basedir /var/www/html/virtualhost1
         </VirtualHost>
  ```

- Spécifiez des fonctions non autorisées dans les scripts qui peuvent mettre en danger le système. Vous pouvez en spécifier plusieurs, séparés par des virgules :

```
disable_functions = exec,system
```

Pour déterminer la liste des fonctions :

```
$ lynx -dump http://fr.php.net/manual/fr/ref.filesystem.php |
grep 'function\.' | awk -F'.' '{ print $5 }'
```

7.1.2. Mise en place d'un mandataire

L'objectif de cette section est d'installer un système de proxy-cache, principalement pour les clients utilisant le protocole HTTP (ou FTP). Le service propose principalement les fonctionnalités suivantes :

- optimisation de la bande passante, lorsque beaucoup de clients consultent les mêmes ressources ;
- contrôle et filtrage de l'accès (en terme de contenu, d'authentification au service ou d'horaires).

Squid est un serveur mandataire Internet qui assure ces fonctions.

7.1.2.1. Principe de fonctionnement

Un proxy est aussi appelé serveur mandataire ou serveur intermédiaire de proximité. Il sert d'intermédiaire entre le client et la ressource à atteindre. Son but est en général d'optimiser la requête initiale et d'en contrôler la validité. Ici, l'optimisation de la requête passe par l'utilisation d'une copie locale des ressources Internet les plus fréquemment accédées par les clients : le cache.

Le mandataire possède sur ses disques un cache, une copie locale des ressources Internet les plus fréquemment consultées. Lorsqu'un client demande l'accès à une ressource, le proxy vérifie s'il détient une copie récente ou non de cette ressource. Si c'est le cas, il renvoie la copie locale, plutôt que de laisser le client accéder à la ressource distante. Cela réduit le trafic sur le lien extérieur de manière conséquente.

Squid est un service/démon qui attend les requêtes HTTP/HTTPS/FTP sur un port déterminé (3128 par défaut, 8080 plus habituellement pour un proxy).

Lorsqu'une requête lui parvient, le proxy vérifie éventuellement les autorisations suivantes :

La machine qui fait la requête est dans une plage d'IP autorisées à utiliser le service ; l'utilisateur spécifié (dans le cas de l'utilisation d'une authentification) est autorisé à utiliser le service ; et la tranche horaire permet l'accès au service.

Si l'une de ces conditions n'est pas remplie, le proxy renvoie une erreur significative. Sinon, la procédure continue avec une vérification du contenu du cache (dans le cas d'un proxy-cache). On a alors divers comportements possibles :

- la ressource demandée n'est pas dans le cache, et Squid relaie la requête via Internet (et stocke cette ressource) ;
- la ressource demandée est dans le cache. Si cette ressource n'est pas trop ancienne, c'est cette copie locale qui est retournée au client. Sinon, Squid relaie la requête via Internet, et stocke cette nouvelle version.

7.1.2.2. Installation et arborescence

L'installation ne représente pas de difficultés particulières, il vous suffit d'installer le paquet `squid`.

Voici les principaux points de l'arborescence à connaître :

- `/etc/squid` : contient les fichiers de configuration de squid et principalement `squid.conf` ;

- `/usr/lib/squid` : outils supplémentaires comme `cachemgr.cgi` et `squid_ldap_auth` ;
- `/var/log/squid` : contient les journaux du serveur Squid ;
- `/var/spool/squid` : contient les caches du serveur.

7.1.2.3. Configuration du serveur Squid

La configuration de Squid est basée sur la création de listes de contrôle d'accès (ou ACL pour *Access Control List*) aux ressources HTTP. Ce contrôle repose sur des filtres qui concernent : la provenance, la destination, les horaires de connexion, les protocoles (HTTP/HTTPS/FTP) et méthodes utilisées (GET/POST).

7.1.2.3.1. Positionnement des ACL

Ces ACL peuvent aussi bien déterminer les autorisations d'accès que la mise en cache des ressources accédées. Toute la configuration est positionnée dans le fichier `/etc/squid/squid.conf`.

Configurer la provenance

- Authentification par mot de passe :

```
acl aclname proxy_auth username ...  acl aclname
   proxy_auth_regex [-i] pattern ...
```

- IP de la machine source :

```
acl aclname src ip-address/netmask
  ... (clients IP address) acl aclname src addr1-addr2/netmask
  ... (range of addresses)
```

- Domaine de la machine source :

```
acl aclname srcdomain .foo.com ...
# reverse lookup, client IP
```

- Nombre de connexions simultanées pour une machine donnée :

```
acl aclname maxconn
  number acl aclname max_user_ip [-s]
  number
```

- Le navigateur employé :

```
  acl aclname browser [-i] regexp ...
# pattern match on
  User-Agent header
```

Configurer la destination

- Domaine de destination :

```
acl aclname dst ip-address/netmask ... (URL
  host's IP address) acl aclname dstdomain .foo.com ...
# Destination server from URL
```

- Portion d'URL :

```
acl aclname dstdom_regex [-i] xxx ...
#  regex matching server acl aclname url_regex [-i] ^http://
   ...
# regex matching on whole URL acl aclname urlpath_regex
   [-i] \.gif$ ...
# regex matching on URL path
```

- Horaires de connexion :

```
acl aclname time [day-abbrevs]
   [h1:m1-h2:m2]
```

- Les protocoles (HTTP/HTTPS/FTP) et méthodes utilisées (GET/POST/) :

```
acl aclname proto HTTP FTP ...  acl aclname
   method GET POST ...
```

Cette liste n'est pas exhaustive mais elle reprend les ACL principalement utilisées.

7.1.2.3.2. Configuration des accès

Par défaut, la configuration fait que le service écoute sur le port 3128, et qu'aucun client/réseau n'est autorisé à traverser le proxy.

```
http_port 3128

#Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl localhost src 127.0.0.1/255.255.255.255

http_access allow localhost

http_access deny all
```

Seul le proxy lui-même (`acl localhost src 127.0.0.1/255.255.255.255`) est autorisé à utiliser le proxy (`http_access allow localhost`). Toutes les autres machines, quelle que soit leur IP (`acl all src 0.0.0.0/0.0.0.0`) se verront refuser l'accès (`http_access deny all`).

Pour autoriser le réseau interne à utiliser le proxy, il faut déclarer une ACL où l'on spécifie le où les réseaux concernés :

```
acl MyNetworks src 10.0.0.0/24 192.168.0.0/24
```

Il faut ensuite donner l'autorisation à cette ACL :

```
http_access allow MyNetworks
```

Ce qui donne la configuration complète suivante :

```
acl all src 0.0.0.0/0.0.0.0
acl localhost src 127.0.0.1/255.255.255.255
acl MyNetworks src 10.0.0.0/24 192.168.0.0/24
...
http_access allow localhost
http_access allow MyNetworks
http_access deny all
```

On peut envisager de modifier l'ACL « all » plutôt qu'en ajouter une nouvelle, mais cela peut engendrer une faille, en ne spécifiant pas de politique de sécurité par défaut.

Voici une combinaison d'ACL sur l'IP et les horaires :

1. Il faut d'abord définir le ou les réseaux concernés :

   ```
   acl MyNetworks src 10.0.0.0/24
          192.168.0.0/24
   ```

2. Ensuite les jours et horaires de connexion (du lundi au vendredi, de 8 h 30 à 18 h 30) :

```
acl WORKING time MTWHF
 08:30-18:30
```

3. Reste à coupler les deux afin de n'autoriser les machines du ou des réseaux spécifiés à utiliser le proxy que pendant les horaires définis :

```
http_access allow MyNetwork
 WORKING
```

Ce qui donne la configuration complète suivante :

```
acl all src 0.0.0.0/0.0.0.0
acl localhost src 127.0.0.1/255.255.255.255
acl MyNetworks src 10.0.0.0/24 192.168.0.0/24
acl WORKING time MTWHF 08:30-18:30
...
http_access allow localhost
http_access allow MyNetworks WORKING
http_access deny all
```

7.1.2.3.3. Configuration du cache

Le cache est la mémoire de Squid. Comme les accès, il est possible d'utiliser les ACL pour autoriser ou interdire la mise en cache de certains objets. En général, on ne mettra pas en cache les pages issues d'un traitement dynamique, à savoir les `cgi`, et plus généralement les requêtes comportant un « ? » dans l'URL.

```
acl QUERY urlpath_regex cgi-bin \?
     no_cache deny QUERY
```

Le cache fonctionne avec un système de swap disque. Les objets les plus récents sont stockés en mémoire, alors que les plus anciens sont stockés sur disque. Il faut donc adapter la taille du cache en mémoire (directive `cache_mem`, défaut 8 Mo) et sur le disque (`directive cache_dir`, défaut 100 Mo) en fonction du trafic Internet pour réduire le swap.

De même, on veillera à paramétrer les tailles minimum et maximum des objets à mettre en cache (`directives minimum_object_size` – défaut 0 Ko, `maximum_object_size` - défaut 4096 Ko, `maximum_object_size_in_memory` – défaut 8 Ko). Pour mettre en place un cache performant, on veillera à avoir suffisamment de RAM, et des disques possédant des accès rapides (SCSI).

La règle énoncée dans la FAQ est la suivante : il faut compter 10 Mo de RAM par Go de cache disque. Il est recommandé d'avoir 2 fois plus de RAM sur la machine que ce qui est prévu pour Squid.

7.1.2.4. Authentifier les accès sur un annuaire LDAP

Il est possible de mettre en place une authentification pour vérifier qu'un utilisateur, identifié par son identifiant et son mot de passe, a le droit (ou non) de naviguer sur le Web. Cette authentification peut être basée sur plusieurs types de base d'utilisateurs : LDAP, NCSA (`.htpasswd`), MSNT/SMB/winbind/NTLM, PAM, getpwam (basé sur `/etc/passwd`), sasl, Digest. Nous aborderons ici LDAP.

L'authentification est vérifiée par un programme externe (`squid_ldap_auth`) qui retourne vrai ou faux sur la correspondance de l'identifiant et du mot de passe.

Il faut donc créer une ACL qui fait appel à l'authentification (`acl ACLName proxy_auth REQUIRED`), puis l'associer à l'ACL qui définit les sources de requêtes (dans le cas présent, les réseaux internes, `acl ACLName src 10.0.0.0/24`).

```
auth_param basic children 5
auth_param basic program /usr/lib/squid/squid_ldap_auth -v 3 -b
 ou=Users,dc=example,dc=com localhost
auth_param basic realm Example.com Squid Server
auth_param basic credentialsttl 2 hours
...
acl password proxy_auth REQUIRED
...
acl all src 0.0.0.0/0.0.0.0
acl localhost src 127.0.0.1/255.255.255.255
acl MyNetworks src 10.0.0.0/24 192.168.0.0/24
...
http_access allow localhost
http_access allow MyNetworks password
http_access deny all
```

Le paquet `squid` fournit la commande `squidclient`. Elle vous permet de tester rapidement le bon fonctionnement de votre serveur et retourne sur la console l'ensemble du dialogue entre le client et le serveur.

```
squidclient http://localhost
 HTTP/1.0 200 OK
 Date: Fri, 01 Sep 2008 10:11:24 GMT
 Server: Apache
```

```
Last-Modified: Fri, 28 Jul 2008 10:57:38 GMT
ETag: "4355-2c-2e3d2c80"
Accept-Ranges: bytes
Content-Length: 44
Content-Type: text/html
X-Cache: MISS from unconfigured
Via: 1.0 unconfigured:3128 (squid/2.6.STABLE1)
Proxy-Connection: close
<html><body><h1>It works!</h1></body></html>
```

7.2. Service d'identité

Le service d'identité permet de fournir des services d'authentification et d'autorisation aux utilisateurs et aux services dans un réseau. Ceci peut être implémenté à travers plusieurs protocoles tous dépendants du type de client. Voici les protocoles disponibles :

- authentification UNIX standard en local ;
- LDAP ;
- Kerberos ;
- Samba.

L'utilisation LDAP avec Mandriva Enterprise Server 5 est fortement recommandée puisqu'il tente de l'utiliser pour le plus grand nombre de services possibles. Pour ce faire, utilisez le paquetage `openldap-mandriva-dit`. Ce paquetage installe un arbre LDAP de base prêt à héberger les services suivants :

- authentification : UNIX®, Samba et Kerberos (en utilisant l'implémentation Heimdal) ;
- autorisation : UNIX®, Samba, Kerberos et le nouveau module *Password Policy overlay* de OpenLDAP ;
- DNS ;
- Sudo ;
- DHCP.

Dans ce chapitre, nous nous concentrons sur l'authentification et l'autorisation en utilisant OpenLDAP puis, plus tard, Kerberos. Pour des renseignements

supplémentaires sur comment utiliser DNS, DHCP ou `sudo` avec LDAP, veuillez consulter le chapitre correspondant.

Après avoir lu ce chapitre, vous serez en mesure d'exécuter les opérations suivantes :

- intégrer l'authentification UNIX®, Samba et Kerberos dans LDAP ;
- utiliser des politiques de mots de passe ;
- déléguer des privilèges d'administration aux utilisateurs et aux groupes pour les services LDAP ;
- régler les problèmes communs de LDAP.

7.2.1. Concepts généraux

Comptes, groupes administratifs et arborescence.

7.2.1.1. Annuaires

Nous présenterons ici quelques concepts généraux à propos de LDAP, la gestion des utilisateurs et des groupes.

Les serveurs d'annuaires peuvent être vus comme des bases de données stockant des renseignements. LDAP est le protocole utilisé pour accéder à ces services :

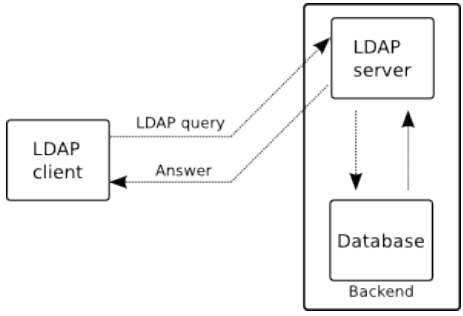


Figure 7-1. Protocole LDAP

Le type de bases de données varie beaucoup entre les implémentations. Ce pourrait être une base de données relationnelle standard, une base de données plus spécialisées comme Berkeley DB, un script dynamique qui génère la sortie, etc.

Toutefois, LDAP tend à être comparé aux bases de données relationnelles (SQL). Il existe des différences importantes :

- hiérarchie : au lieu d'utiliser des tables avec des entrées et des champs, il utilise des arbres et des noeuds, un peu comme un système de fichiers ;
- optimisation pour la lecture : d'habitude, les annuaires sont plus sollicités en lecture qu'en écriture
- distribué : l'arborescence permet aux branches d'être stockées ailleurs sans compromettre la vue d'ensemble ;
- une forte standardisation : le type de donnée stocké dans un annuaire relève d'une forte standardisation, autant dans le nom des données que dans son type. Ceci s'appuie habituellement sur des RFC.

Voici un court exemple d'un arbre qui s'étend sur plus d'un serveur :

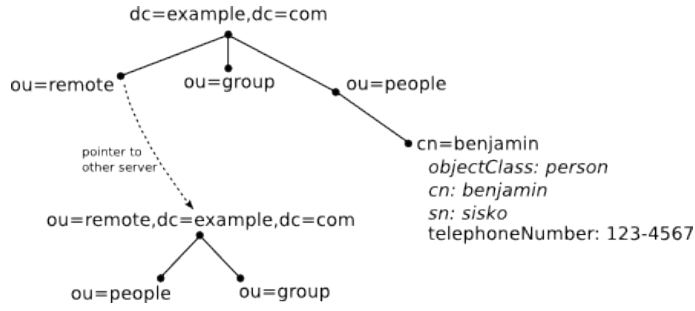


Figure 7-2. Arbre LDAP

Les services d'authentification et d'autorisation sont de bons candidats pour l'utilisation d'un annuaire. Vu qu'ils ont besoin de performance de lecture maximale, ils subissent moins d'opérations d'écriture et peuvent être distribués dans un Système d'Information, tout en restant connectés.

L'ensemble de règles concernant les données stockées dans un annuaire s'appelle un schéma. Le schéma d'annuaire définit plusieurs éléments :

- classes d'object : elles définissent la nature d'une entrée et le type d'information qu'elle contient ;
- attributs : les données elles-mêmes, similaires à un champ dans une base de données standard ;
- indexation et règles d'ordonnancement : spécifie comment doit fonctionner la recherche sur un attribut spécifique, et comment il doit être trié ;

- type de valeur : définit le type de donnée que l'attribut devrait contenir (numérique, chaîne, objet binaire, etc).

Le schéma est avantageux pour la standardisation, mais il est parfois difficile d'ajouter des données à un annuaire. Alors que dans une base de données, c'est aussi simple que d'ajouter un nouveau champ, dans un annuaire, vous devez obéir au schéma. Vous ne pouvez pas simplement ajouter n'importe quel type d'attribut à une entrée : seulement ceux alloués par les classes d'objet.

Par exemple, voici la définition d'une classe d'objet `person` :

```
objectclass ( 2.5.6.6 NAME 'person'
    DESC 'RFC2256: a person'
    SUP top STRUCTURAL
    MUST ( sn $ cn )
    MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )
```

Ceci nous dit :

- cet objet est défini dans le RFC 2256 ;
- c'est un objet structurel ;
- les attributs sn et cn sont obligatoires ;
- les attributs optionnels `userPassword`, `telephoneNumber`, `seeAlso` et `description` sont admissibles dans une entrée utilisant cette classe d'objet.

Figure 7-2 illustre aussi les attributs obligatoires et certains attributs optionnels de la classe d'objet `person`.

7.2.1.2. Arborescence, groupes et privilèges

Le paquetage `openldap-mandriva-dit` offre une arborescence qui peut héberger les services décrits, ainsi que l'authentification et l'autorisation. Voici l'arborescence :

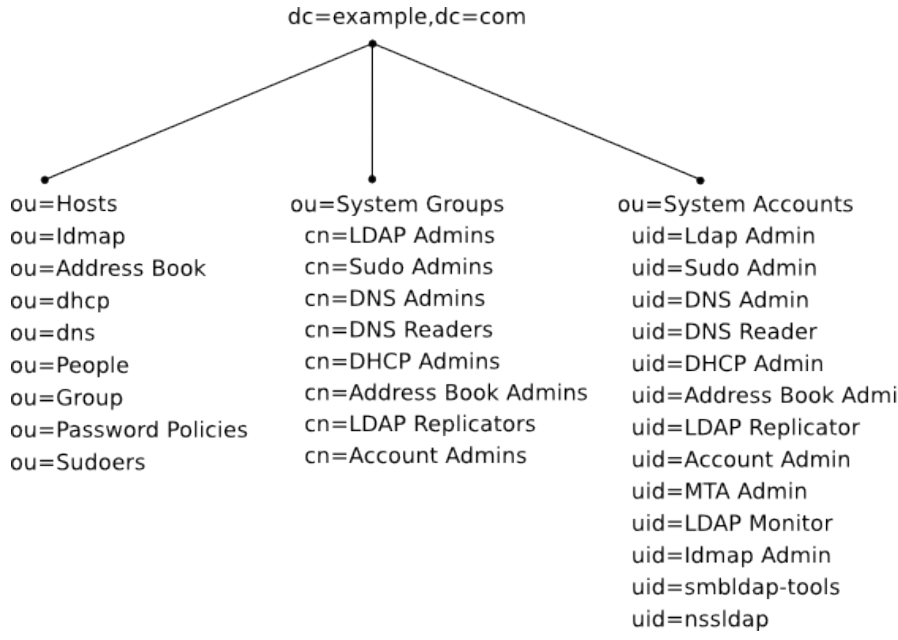


Figure 7-3. Arborescence

La première entrée de l'annuaire, `dc=example,dc=com`, est substituée lors de l'installation par le domaine DNS détecté.

Chaque groupe possède un ensemble de privilèges assignés à ses membres, et ce par défaut. Le membre initial est l'administrateur du groupe dans la branche `SystemAccounts`. Les privilèges sont tels que chaque membre peut administrer la branche de service respective. Donc, les membres du groupe `SudoAdmins` peuvent lire et écrire sur la branche `ou=Sudoers`.

Les autres groupes qui ne sont pas directement associés à un service sont décrits plus bas :

- LDAP Admins : peuvent lire et écrire sur n'importe quelle partie de l'arbre. Ils sont aussi exempts de limite de taille ou de temps.
- DNS Readers : seul les membres de ce groupe peuvent lire la branche `ou=DNS`.
- LDAP Replicators : les membres peuvent lire toutes les parties de l'annuaire et ne sont pas sujets à des limites de taille ou de temps.
- Account Admins : les membres peuvent créer de nouveaux comptes (unix, samba ou kerberos) sous les branches `ou=People`, `ou=Group` et `ou=Hosts`.
- MTA Admins : les membres peuvent écrire sur certains attributs spécifiques reliés au courriel :

  - tous les attributs utilisés par la classe d'objet `inetLocalMailRecipient` ;
  - l'attribut `mail`.

- LDAP Monitors : les membres peuvent lire l'arbre spécial `cn=Monitor`, qui héberge des données statistiques en direct au sujet du serveur OpenLDAP.

Par défaut, deux comptes supplémentaires sont fournis avec cet arbre : `smbldap-tools` et `nssldap`. Le premier est utilisé par la suite d'outils `smbldap-tools` et est membre du groupe `AccountAdmins`. Le deuxième, `nssldap`, est un compte de lecture générique et n'est pas utilisé par défaut par un quelconque service. Il est fourni par commodité pour l'administrateur. Aucun ACL spécial n'est en place pour ce compte.

7.2.1.3. Installation

Le paquetage `openldap-mandriva-dit` contient aussi un script d'installation qui peut être exécuté depuis une console. Le script est installé dans `/usr/share/openldap/scripts/mandriva-dit-setup.sh` :

- parle au domaine DNS (en suggérant ce qui a été détecté automatiquement) ;
- construit l'entrée de l'annuaire de premier niveau depuis ce domaine en utilisant des attributs de style `dc` ;
- crée et importe un fichier `LDIF` contenant les comptes et groupes décrits ici ;
- installe de nouveaux fichiers `slapd.conf` et `mandriva-dit-access.conf` (faisant des sauvegardes des fichiers précédents) avec les ACL par défaut et d'autres configurations utiles (comme le cache) ;
- charge le fichier `ldif`, faisant une sauvegarde de l'annuaire de base de données précédent.

Même si le script fait plusieurs tests et sauvegarde plusieurs fichiers avant de les écraser, nous avisons les administrateurs de faire une copie de sauvegarde de leurs données avant de l'exécuter.

Voici un exemple utilisant le domaine `dc=example,dc=com` :

```
# /usr/share/openldap/scripts/mandriva-dit-setup.sh
Please enter your DNS domain name [mycompany.com]:
example.com


Administrator account

The administrator account for this directory is
uid=LDAP Admin,ou=System Accounts,dc=example,dc=com
```

```
Please choose a password for this account:
New password: secretpass
Re-enter new password: secretpass


Summary
=======

Domain:      example.com
LDAP suffix: dc=example,dc=com

Confirm? (Y/n)            Y
config file testing succeeded
Stopping ldap service
Finished, starting ldap service
Running /usr/bin/db_recover on /var/lib/ldap
removing /var/lib/ldap/alock
Starting slapd (ldap + ldaps):                [  OK  ]

Your previous database directory has been backed up as
/var/lib/ldap.1145397294
```

Maintenant le service `ldap` est fonctionnel. Vous pouvez utiliser le compte administrateur avec le mot de passe que nous venons de régler pour peupler l'arbre. C'est le seul compte activé dans l'arbre jusqu'à présent : tous les autres sont désactivés. Pour activer le compte d'administration, il doit posséder un mot de passe. Par exemple, activons le compte `DNSAdmin` :

```
$ ldappasswd -x -D "uid=LDAP Admin,ou=System Accounts,dc=example,dc=com"
 -W -S "uid=DNS Admin,ou=System Accounts,dc=example,dc=com"
New password: newsecret
Re-enter new password: newsecret
Enter LDAP Password: here is the password for the bind (-D) user:
 LDAP Admin
Result: Success (0)
```

Maintenant, le compte `DNSAdmin` possède un mot de passe et peut être utilisé pour administrer la branche `ou=dns` de l'arbre.

7.2.2. Authentification des utilisateurs UNIX

Cet arbre n'a rien de spécial en regard des comptes POSIX (comptes UNIX traditionnels) :

- `ou=People` : branche qui contient les comptes de personnes (sauf `kerberos`). Donc, un compte utilisateur pourrait être quelque chose comme `uid=john, ou=People,dc=example,dc=com`. Ces entrées doivent posséder au moins la classe d'objet `posixAccount`.
- `ou=Group` : les comptes de groupe vont dans cette branche. Par exemple, on pourrait avoir `cn=marketing,ou=Group,dc=example,dc=com`. Ces entrées doivent posséder au moins une classe d'objet `posixGroup`.

Le groupe qui peut écrire sur ces branches est `cn=AccountAdmins,ou=SystemGroups,dc=example,dc=com`. Le propriétaire et membre initial de ce groupe est `uid=AccountAdmin,ou=SystemAccounts,dc=example,dc=com`.

Par défaut, tous les comptes système sauf `LDAPAdmin` sont bloqués. Pour en utiliser un, vous devez lui régler un mot de passe. L'exemple ci-dessous active le compte `AccountAdmin` en lui assignant un mot de passe :

```
$ ldappasswd -x -D "uid=LDAP Admin,ou=System Accounts,dc=example,dc=com"
 -W -S "uid=Account Admin,ou=System Accounts,dc=example,dc=com"
New password: password for account admin
Re-enter new password: retype it
Enter LDAP Password:
Result: Success (0)
```

Ceci utilise le compte `LDAPAdmin` pour régler un mot de passe pour `AccountAdmin`, qui est maintenant activé et peut être utilisé pour ajouter, supprimer ou modifier des utilisateurs et des groupes.

7.2.2.1. Créer un compte

Plusieurs frontaux (*front-end*) existent pour LDAP et ils peuvent créer des comptes POSIX. Voici un exemple rapide en utilisant le programme Luma. Il possède plusieurs greffons (*plugins*) et un de ceux-ci permet de gérer les utilisateurs :

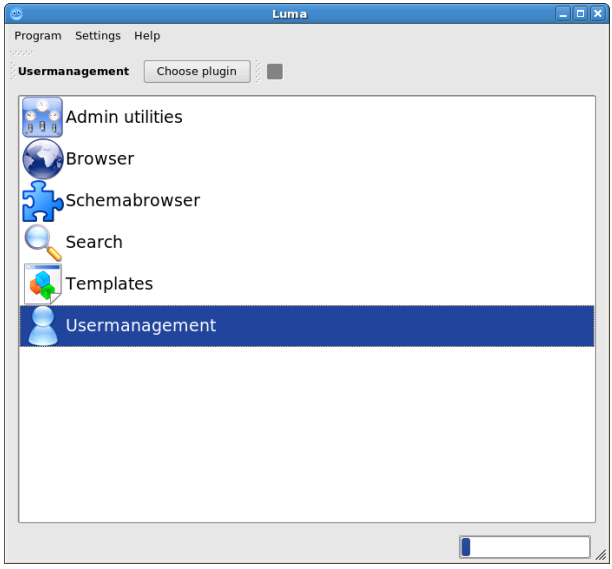


Figure 7-4. Greffon Luma

Voici le greffon de gestion des utilisateurs :

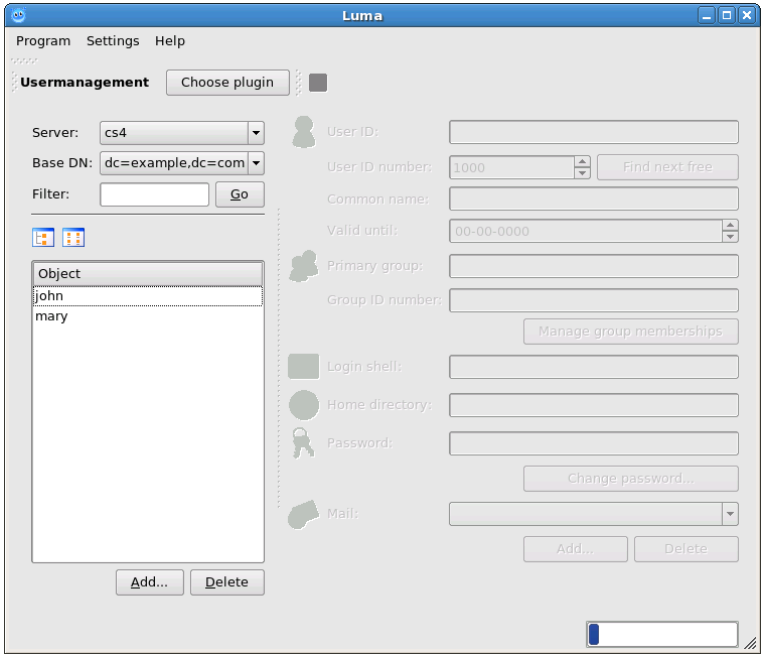


Figure 7-5. Greffon de gestion des utilisateurs

Premièrement, il faut indiquer sur quel serveur et quelle branche vous voulez ajouter un utilisateur. Dans cet exemple, nous nous plaçons sur la branche `ou=People` :

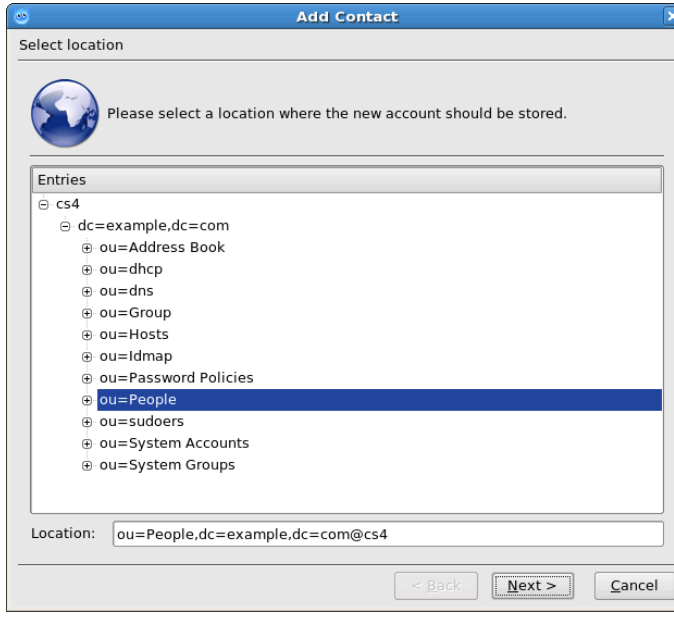


Figure 7-6. Où ajouter un utilisateur

Ensuite, nous entrons l'information nécessaire pour cet utilisateur :

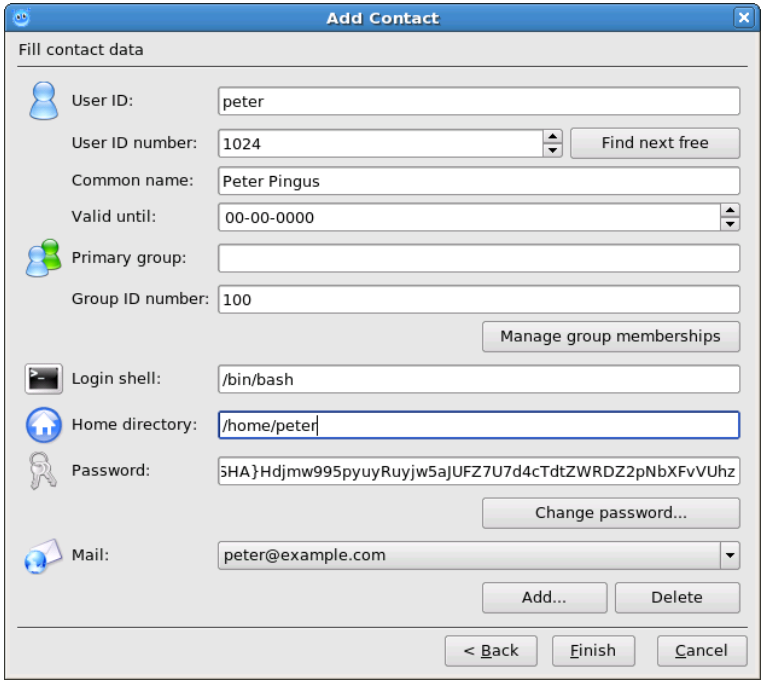


Figure 7-7. Ajouter un utilisateur

Il est nécessaire de spécifier au moins un groupe primaire pour cet utilisateur. Les groupes POSIX LDAP seront automatiquement affichés, mais si vous n'en avez pas, alors la liste sera vide. Maintenant, nous sélectionnons `gidNumber=100`, qui appartient au groupe local `users` :

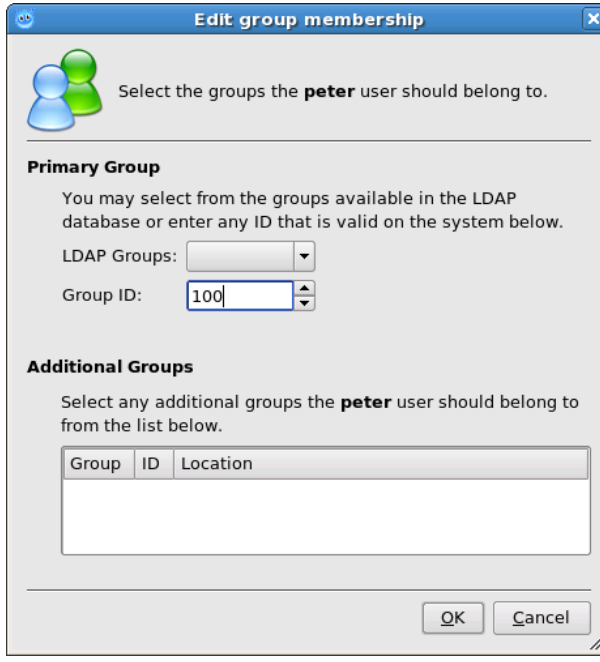


Figure 7-8. Groupes

Voici à quoi ressemble notre nouvel utilisateur dans LDAP :

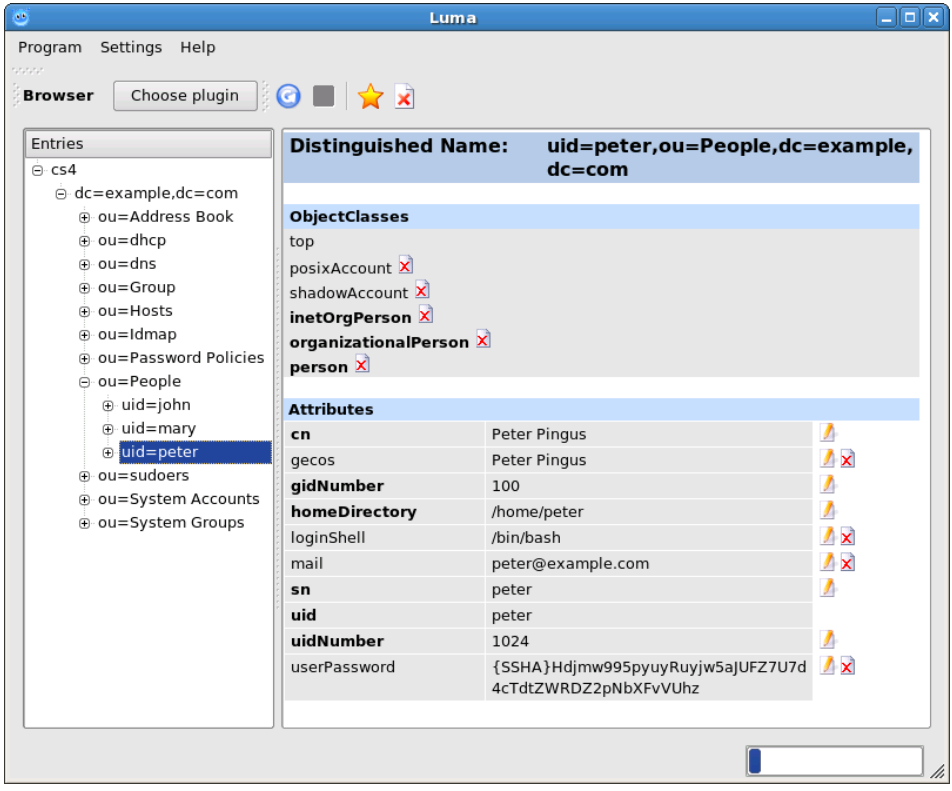


Figure 7-9. Peter dans LDAP

Luma tentera de trouver un `uidNumber` libre pour l'allouer à cet utilisateur. Vous devriez toujours être prudent, toutefois, parce qu'il est incorrect que deux utilisateurs possèdent le même `uidNumber`.

7.2.2.2. Créer des groupes

Les groupes UNIX sont représentés dans LDAP en utilisant la classe `posixGroup`. Une entrée typique pour un groupe ressemble à :

```
dn: cn=ldapusers,ou=Group,dc=example,dc=com
    objectClass: posixGroup
    gidNumber: 1024
    cn: ldapusers
    memberUid: peter
    memberUid: queen
```

Cette entrée définit un groupe appelé `ldapusers` avec un numéro d'identification de 1024 et, jusqu'à présent, deux membres appelés `peter` et `queen`.

Cette structure est assez simple pour être créée manuellement. Il faut simplement être prudent de ne pas donner le même numéro d'identification à plus d'un groupe.

Les groupes système utilisent une classe d'objet différente : `groupOfNames`. La différence principale est que l'adhésion est définie par un DN complet au lieu de seulement un nom, comme c'est le cas pour `posixGroup`. Malheureusement, `posixGroup` et `groupOfUniqueNames` ne peuvent pas être utilisés en même temps parce qu'ils tous les deux des classes structurelles. Nous nous attendons à ce que la révision du RFC2307 redéfinisse `posixGroup` en tant que classe auxiliaire.

7.2.2.3. Déléguer des privilèges d'administration

Tous les membres du groupe `cn=AccountAdmins,ou=SystemGroups,dc=example,dc=com` peuvent gérer des comptes utilisateur dans `ou=People`, `ou=Group` et `ou=Hosts` (pour Samba, qui est expliqué plus loin). Tout administrateur LDAP (*LDAP Admin*) ou l'utilisateur `AccountAdmin` lui-même peut ajouter des membres à ce groupe.

Les groupes système ont des propriétaires, et par défaut, le propriétaire peut toujours éditer l'adhésion du groupe qu'il possède. Pour voir qui est le propriétaire, vérifiez l'attribut `owner` du groupe système en question.

Par exemple, ajoutons l'utilisateur `PeterPingus`, que nous venons de créer, à ce groupe privilégié pour qu'il puisse gérer des comptes :

```
$ ldapmodify -x -D 'uid=Account Admin,ou=System Accounts,
 dc=example,dc=com' -W
Enter LDAP Password: secretpassword
dn: cn=Account Admins,ou=System Groups,dc=example,dc=com
changetype: modify
add: member
member: uid=peter,ou=People,dc=example,dc=com

^D
modifying entry "cn=Account Admins,ou=System Groups,dc=example,dc=com"
```

La même opération peut être faite avec un client graphique. Ajoutez simplement l'attribut `member` en pointant vers le `dn` de l'utilisateur que vous voulez ajouter à ce groupe.

7.2.3. Authentification Samba

Pour utiliser ce DIT avec Samba, suivez cet exemple :

- Disposition en LDAP

  Voici la disposition qui doit être configurée dans `/etc/samba/smb.conf` et `/etc/smbldap-tools/smbldap.conf` :

  - comptes machine : sous `ou=Hosts` ;
  - comptes utilisateur : sous `ou=People` ;
  - comptes groupe : sous `ou=Group` ;
  - branche idmap : sous `ou=Idmap`.

- `ldapadmindn`

  Pour le paramètre de configuration `ldapadmindn` dans `/etc/samba/smb.conf`, utilisez un membre du groupe `AccountAdmins`. Par exemple :

  ```
  ldap admin dn = uid=Account Admin,ou=System Accounts,dc=example,dc=com
  ```

- `smbldap-tools`

  Dans `/etc/smbldap-tools/smbldap_bind.conf`, utilisez l'utilisateur `smbldap-tools` au lieu du `rootdn` de l'annuaire :

  ```
  masterDN="uid=smbldap-tools,ou=System Accounts,dc=example,dc=com"
  ```

  Cet utilisateur est membre du groupe `AccountAdmins`. Si vous voulez utiliser un autre compte, assurez-vous qu'il est membre du même groupe. Sinon, les ACL OpenLDAP par défaut ne fonctionneront pas.

- `smbldap-populate`

  Dans la version 0.9.2, le comportement par défaut de `smbldap-populate` est de créer un compte administrateur avec les attributs suivants :

  - uidNumber = 0
  - gidNumber = 0
  - name: root

- membre de Domain Admins

Ceci signifie que l'utilisateur root est créé dans LDAP. Nous ne vous recommandons pas d'utiliser cette commande avec `smbldap-populate` :

```
# smbldap-populate -a Administrator -k 1000 -m 512
```

Ceci crée un utilisateur dont le nom est Administrator, uidNumber 1000 et gidNumber 512. Vous pouvez aussi utiliser uidNumber 500 si vous voulez qu'il concorde avec le RID de Windows® pour ce type d'utilisateur.

Plus tard, on pourrait donner des privilèges au groupe `DomainAdmins` (voir la commande `netrpc rights grant`), ou vos répertoires partagés pourraient utiliser le paramètre `admin users`.

- IDMAP

Si vous utilisez le *backend* LDAP de IDMAP sur un serveur membre, réglez le paramètre de configuration `ldap admin dn configuration` dans `/etc/samba/smb.conf` au dn d'un membre du groupe `IdmapAdmins`. Par exemple :

```
ldap admin dn = uid=Idmap Admin,ou=System Accounts,dc=example,dc=com
```

Sur les serveurs membres, il n'est pas nécessaire d'utiliser le compte `AccountAdmin` : le groupe `IdmapAdmins` est celui à utiliser puisqu'il ne peut écrire que dans le conteneur `ou=Idmap`.

7.2.3.1. Créer des comptes Samba

La manière recommandée de créer des comptes Samba sur LDAP est d'utiliser le paquetage `smbldap-tools`. Ce paquetage possède plusieurs outils pour ajouter, supprimer ou modifier des utilisateurs et des groupes dans un arbre LDAP avec les attributs de Samba.

7.2.4. Authentification Kerberos

OpenLDAP peut être utilisé en tant que *backend* pour la base de données Heimdal, ce qui signifie que les comptes principaux peuvent être stockés dans un LDAP. Dans cette section, nous présentons les étapes nécessaires pour intégrer le *backend* LDAP de Heimdal avec OpenLDAP et `openldap-mandriva-dit`. Si vous n'avez pas besoin de cette caractéristique, vous pouvez utiliser le serveur Kerberos par défaut, qui utilise les paquetages MIT, et sauter le texte qui suit.

Nous commencerons avec un nouvel univers que nous appellerons EXAMPLE.COM. Nous assumons que openldap-mandriva-dit est installé et que le script fourni a été exécuté, soit manuellement ou via Mandriva Server Setup.

Lorsque vous utilisez le *backend* LDAP, nous vous recommandons d'avoir un script pour créer les utilisateurs, puisque Heimdal, par défaut, utilise la classe d'objet structurel account. Comme il est plus courant d'utiliser inetOrgPerson (ou une classe dérivée), l'entrée principale devrait être supprimée et ajoutée à nouveau plus tard avec inetOrgPerson.

Une autre approche est de créer en premier lieu l'utilisateur avec les outils standards (smbldap-tools, un script manuel, un modèle dans gq ou luma, etc.) et ensuite d'ajouter les attributs kerberos plus tard. Nous documentons les deux approches.

7.2.4.1. Paquetages

En raison de conflits avec le paquetage Kerberos de MIT, Heimdal est packagé comme suit dans Mandriva Enterprise Server 5 :

- heimdal-libs
- heimdal-server
- heimdal-workstation
- heimdal-devel

Les conflits ont été résolus. Seulement heimdal-libs peut être installé concurremment avec les bibliothèques de MIT.

7.2.4.2. Survol des changements

Voici un survol rapide des changements nécessaires pour que Heimdal puisse utiliser OpenLDAP en tant que *backend* de base de données, et utiliser le DIT openldap-mandriva-dit :

- configurez Heimdal pour qu'il utilise LDAP en tant que *backend* ;
- configurez OpenLDAP pour qu'il accepte les connexions depuis Heimdal via ldapi:// ;
- testez cette table de correspondance ;
- initialisez la base de données ;
- gérez les comptes utilisateur.

7.2.4.3. Heimdal avec OpenLDAP

Afin d'obtenir une base de données sur LDAP, la section `[kdc]` suivante doit être utilisée dans le fichier `/etc/krb5.conf` de Heimdal :

```
[kdc]
database = {
    dbname = ldap:ou=People,dc=example,dc=com
    mkey_file = /var/heimdal/mkey
    acl_file = /var/heimdal/kadmind.acl
    }
```

Ceci donnera comme directive à Heimdal d'utiliser le serveur OpenLDAP installé sur le même hôte et d'utiliser la branche `ou=People` pour ces principaux. La méthode d'accès Heimdal utilise ldapi:// , qui est une interface de connexion (*socket*) UNIX sur le système de fichiers local. L'authentification est gérée par SASL EXTERNAL, que nous configurerons plus tard.

7.2.4.4. Utilisation de ldapi

OpenLDAP doit être configuré pour accepter les connexions via ldapi://. Il faut éditer le fichier `/etc/sysconfig/ldap`. Changez la liste SLAPD URL pour celle-ci :

```
    # SLAPD URL list
    SLAPDURLLIST="ldap:/// ldaps:/// ldapi:///"
```

OpenLDAP doit ensuite être redémarré.

7.2.4.5. Utilisation de SASL EXTERNAL

Heimdal utilise SASL EXTERNAL pour s'authentifier au serveur OpenLDAP lorsqu'il se connecte via une interface de connexion ldapi://. Ce faisant, le lien dn devient :

```
# ldapwhoami -Y EXTERNAL -H ldapi:///var/run/ldap/ldapi
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn:gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
Result: Success (0)
```

Nous allons lier ce dn à un binddn plus significatif via `authz-regexp`. Le fichier `slapd.conf` fourni avec `openldap-mandriva-dit` fait déjà cela, mais dans un souci d'exhaustivité, le voici de toute manière :

```
(...)
ppolicy_default "cn=default,ou=Password Policies,dc=example,dc=com"

authz-regexp "gidNumber=0\\\+uidNumber=0,cn=peercred,cn=external,cn=auth"
"uid=Account Admin,ou=System Accounts,dc=example,dc=com"
authz-regexp ^uid=([^,]+),cn=[^,]+,cn=auth$ uid=$1,ou=People,dc=example,dc=com
```

Avec cette modification et après avoir redémarré OpenLDAP, `ldapwhoami` sait maintenant que nous sommes le `AccountAdmin` :

```
# ldapwhoami -Y EXTERNAL -H ldapi:///var/run/ldap/ldapi
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn:uid=account admin,ou=system accounts,dc=example,dc=com
Result: Success (0)
```

Notez que tout processus se connectant à l'interface de connexion ldapi:// en tant que root (uid=0, gid=0) sera traité comme un `AccountAdministrator` après ce changement!

7.2.4.6. Initialisation du référenciel Kerberos

Nous pouvons maintenant initialiser Kerberos. Après le redémarrage d'OpenLDAP, exécutez la commande suivante :

```
# kadmin -l
    kadmin> init EXAMPLE.COM
    Realm max ticket life [unlimited]:7d
    Realm max renewable ticket life [unlimited]:7d
    kadmin
```

Ceci créera quelques principaux par défaut sous `ou=People` :

```
ou=People
krb5PrincipalName=krbtgt/EXAMPLE.COM@EXAMPLE.COM,ou=People,dc=example,dc=com
krb5PrincipalName=kadmin/changepw@EXAMPLE.COM,ou=People,dc=example,dc=com
krb5PrincipalName=kadmin/admin@EXAMPLE.COM,ou=People,dc=example,dc=com
krb5PrincipalName=changepw/kerberos@EXAMPLE.COM,ou=People,dc=example,dc=co
krb5PrincipalName=kadmin/hprop@EXAMPLE.COM,ou=People,dc=example,dc=com
krb5PrincipalName=default@EXAMPLE.COM,ou=People,dc=example,dc=com
```

7.2.4.7. Gestion des comptes utilisateur et principal

Le schéma Heimdal permet aux comptes principaux d'être stockés sur une branche différente de celles des comptes utilisateurs. Par exemple, vous pourriez placer les comptes principaux sous `ou=KerberosPrincipals` et les comptes utilisateurs sous `ou=People`.

Cette façon de faire possède un désavantage évident, soit de créer un problème dans la gestion des utilisateurs : lorsqu'un utilisateur est supprimé, par exemple, le compte principal correspondant est aussi supprimé. En d'autres mots, nous aurions besoin d'un pointeur dans l'entrée utilisateur pour le compte principal (l'attribut `seeAlso` est couramment utilisé pour des manœuvres de ce genre). Et un script devrait suivre cet attribut et supprimer le compte principal.

L'avantage serait qu'un utilisateur peut être associé avec plusieurs principaux kerberos en utilisant l'attribut `seeAlso`, comme john@UNIVERS et john/admin@UNIVERS.

Le plus gros désavantage des schémas où les principaux sont séparés des utilisateurs est l'intégration avec Samba et LDAP. Heimdal ne mettra à jour que le hash du mot de passe de Samba s'il est stocké dans la même entrée. La même chose se produit avec `userPassword` : vu qu'OpenLDAP utilise le module `smbk5pwdi` (compilé en prenant en charge Kerberos), les liens simples ne pourront qu'utiliser le mot de passe de Kerberos si tout est dans la même entrée.

Une autre option serait de stocker les clés principales et les attributs qui y sont relatifs juste sous l'entrée utilisateur. Nous pouvons faire cela car les classes d'objet Kerberos sont auxiliaires. Donc, l'utilisateur John serait, par exemple : `uid=john,ou=people,dc=example,dc=com`, et les clés Kerberos seraient stockées dans cette même entrée. Lorsque cet utilisateur est supprimé, le compte principal l'est aussi. Le désavantage est qu'un utilisateur ne peut avoir qu'un principal, et non plusieurs comme dans le cas précédent (où john pouvait avoir `john@UNIVERS` et `john/admin@UNIVERS` associés à la même entrée `uid=john,ou=people,dc=example,dc=com`).

Mais un problème apparaît : qu'utilisons-nous pour créer cet utilisateur en premier lieu? Si nous utilisons kadmin, cela créera une entrée de la forme suivante :

```
krb5PrincipalName=john@EXAMPLE.COM,ou=People,dc=example,dc=com
```

le compte étant la classe d'objet structurel. Comme nous tendons à utiliser une classe dérivée de `person` en tant que classe structurelle (comme `inetOrgPerson`), il y a conflit. Si nous utilisons kadmin, nous aurions à supprimer l'entrée et à l'ajouter de nouveau avec `inetOrgPerson` (et ses attributs obligatoires).

Le mieux serait de créer en premier lieu l'utilisateur avec d'autres outils tels que smbldap et Luma, puis d'ajouter les attributs Kerberos plus tard. Les avantages principaux sont :

- le nommage RDN demeurera constant avec le reste des entrées (aucun krb5PrincipalName dans le RDN si nous n'en voulons pas) ;
- le paramétrage de la classe d'objet structurel peut se faire comme bon nous semble (par exemple, `inetOrgPerson`) ;
- les comptes utilisateur et principal sont ensemble sous `ou=People`.

Le plus gros désavantage est que la table de correspondance entre les utilisateurs et les principaux serait de 1:1, ce qui signifie qu'un utilisateur pourrait avoir au plus un principal Kerberos associé avec son entrée.

Toutefois, les deux schémas peuvent être utilisés ensemble. La question qui nous préoccupe est plutôt comment allons nous gérer les comptes. Donc, les utilisateurs réguliers pourraient stockés leur clé Kerberos dans l'entrée utilisateur, tandis que les clés d'administration et de service pourraient être stockés sous la même branche, qu'aucun utilisateur n'y soit associé. Ce n'est pas très constant en regard de l'arbre (après tout, `ou=People` était censé hébergé des personnes), mais ça marche.

Nous continuons avec deux exemples : l'utilisation de kadmin directement, et l'utilisation d'un autre script pour créer en premier lieu le compte utilisateur et ensuite, ajouter les attributs Kerberos.

7.2.4.8. Utilisation de kadmin directement

Nous allons créer un compte Kerberos pour l'utilisateur « john » en utilisant kadmin directement. Nous n'avons pas à démarrer Heimdal à ce stade puisque nous allons utiliser kadmin en mode local :

```
# kadmin -l
    kadmin> add john
    Max ticket life [1 day]:10h
    Max renewable life [1 week]:1w
    Principal expiration time [never]:
    Password expiration time [never]:
    Attributes []:
    john@EXAMPLE.COM's Password: somesecretpassword
    Verifying - john@EXAMPLE.COM's Password: somesecretpassword
    kadmin>
```

Cela crée l'entrée suivante :

```
    dn: krb5PrincipalName=john@EXAMPLE.COM,ou=People,dc=example,dc=com
    objectClass: top
```

```
objectClass: account
objectClass: krb5Principal
objectClass: krb5KDCEntry
krb5PrincipalName: john@EXAMPLE.COM
uid: john
krb5KeyVersionNumber: 0
krb5MaxLife: 36000
krb5MaxRenew: 604800
krb5KDCFlags: 126
(...)
```

On peut obtenir un billet pour cet utilisateur :

```
# service heimdal start
Starting kdc:                                          [  OK  ]
# kinit john
john@EXAMPLE.COM's Password: somesecretpassword
# klist
Credentials cache: FILE:/tmp/krb5cc_0
Principal: john@EXAMPLE.COM

Issued           Expires          Principal
Jun 20 15:43:23  Jun 20 22:23:23  krbtgt/EXAMPLE.COM@EXAMPLE.COM
#
```

Cependant, remarquez que l'utilisateur `john` n'a pas les attributs POSIX nécessaires pour devenir un utilisateur système. De toute façon, nous avons besoin d'autre chose pour créer cet utilisateur POSIX : ici, le rôle de Heimdal est terminé.

7.2.4.9. Ajouter des attributs Kerberos à une entrée existante

Si le compte utilisateur existe déjà dans l'annuaire, nous n'avons qu'à ajouter les classes d'objet Heimdal nécessaires pour ce compte.

Donc, pour cet exemple, nous utiliserons un paquetage `smbldap-tools` préconfiguré pour créer un utilisateur modèle et ensuite, nous lui ajouterons les classes Kerberos et les attributs.

Remarquez que nous n'ajoutons pas les attributs Samba tout de suite :

```
# smbldap-useradd mary
# getent passwd mary
mary:x:1001:513:System User:/home/mary:/bin/bash
```

L'utilisateur ressemble à ceci dans l'annuaire :

```
dn: uid=mary,ou=People,dc=example,dc=com
objectClass: top
```

```
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: mary
sn: mary
givenName: mary
uid: mary
uidNumber: 1001
gidNumber: 513
homeDirectory: /home/mary
loginShell: /bin/bash
gecos: System User
userPassword: {crypt}x
```

Nous utiliserons la modification LDAP suivante pour ajouter les attributs et classes Kerberos à cet utilisateur :

```
$ ldapmodify -x -D 'uid=Account Admin,ou=System Accounts,dc=example,dc=com'
    -W
Enter LDAP Password: somepassword
     dn: uid=mary,ou=people,dc=example,dc=com
     changetype: modify
     add: objectClass
     objectClass: krb5Principal
     objectClass: krb5KDCEntry
     -
     add: krb5PrincipalName
     krb5PrincipalName: mary@EXAMPLE.COM
     -
     add: krb5KDCFlags
     krb5KDCFlags: 126
     -
     add: krb5KeyVersionNumber
     krb5KeyVersionNumber: 0

    modifying entry "uid=mary,ou=people,dc=example,dc=com"
```

Maintenant, `mary` est reconnue en tant que principal Kerberos. Heimdal peut ajouter les clés et autres attributs manquants en tapant la commande de changement de mot de passe en tant qu'administrateur ou en mode admin local :

```
# kadmin -l
kadmin> passwd mary
mary@EXAMPLE.COM's Password: somesecretpass
Verifying - mary@EXAMPLE.COM's Password:
somesecretpass  kadmin>
```

Ceci ajoute les attributs manquants et maintenant, `mary` est un principal Kerberos complet :

```
$ kinit mary
mary@EXAMPLE.COM's Password: somesecretpass
$ klist
Credentials cache: FILE:/tmp/krb5cc_500
Principal: mary@EXAMPLE.COM

Issued           Expires          Principal
Jun 20 16:14:48  Jun 20 22:54:48  krbtgt/EXAMPLE.COM@EXAMPLE.COM $
```

`mary` est également un compte POSIX. À titre de rappel : dans une seule entrée LDAP, nous avons POSIX, Samba et Kerberos. Mais il existe toujours trois sources de mot de passe.

7.2.4.10. Intégration des mots de passe

La fonction la plus recherchée dans un réglage où Heimdal utilise OpenLDAP en tant que *backend* de base de données est l'intégration de mot de passe.

Sur un réseau, il existe trois sources d'authentification très communes, soit les mots de passe Samba, les mots de passe POSIX et les mots de passe Kerberos. L'utilisation de LDAP ne rend pas magique l'intégration des trois mots de passe : LDAP n'est qu'un espace de stockage et, en effet, chaque application l'utilise pour elle-même. Par exemple, voici les attributs utilisés pour le stockage des mots de passe par Samba, Heimdal et POSIX :

- Samba : `sambaNTPassword`, `sambaLMPassword` ;
- Heimdal : `krb5Key` ;
- posix : `userPassword`.

Donc, `pam_ldap` peut changer le `userPassword` lorsque l'utilisateur exécute la commande `password` depuis la console, mais la clé Heimdal et les hashs Samba ne seront pas changés. Nous avons un problème de synchronisation.

Certains administrateurs exécutent des scripts pour régler ce problème, ou n'alloue à l'utilisateur que le droit de changer son mot de passe via un frontal quelconque qui prendra en charge les détails concernant la mise à jour de tous les hashs. Une autre option consiste à utiliser le module `smbk5pwd`.

Le module `smbk5pwd` est disponible dans le répertoire `contribs` du *tarball* OpenLDAP et, lorsque compilé avec le support Samba et Kerberos, il permet cette intégration de mot de passe automatiquement. Ce module est disponible par défaut dans le paquetage `openldap-servers`.

L'intégration se déroule en trois temps :

- Modifications des mots de passe EXOP

Ce module intercepte les modifications de mot de passe OpenLDAP EXOP et met à jour la clé Kerberos et les hashs Samba pour la même entrée, s'ils sont présents. Ceci signifie qu'une commande `ldappasswd`, par exemple, changera les mots de passe Samba et Kerberos. Lorsque Samba utilise l'option `ldappasswdsync` dans `smb.conf`, il réalise également une modification de mot de passe EXOP et met à jour la clé Kerberos.

- `kpasswd`

  Lorsque Heimdal reçoit une requête de changement de mot de passe à travers kadmin ou kpasswd, il vérifie si la l'entrée cible contient les hashs d'un mot de passe Samba. Si c'est le cas, ces entrées hash sont également mises à jour. L'attribut `userPassword`, utilisés pour les authentifications simples, n'est pas touché, mais voyez la prochaine entrée.

- authentifications simples (userPassword)

  Les liens simples (*simple binds*) utilisent l'attribut `userPassword` pour la vérification du mot de passe. Si cet attribut contient le hash spécial `{K5KEY}`, la vérification du mot de passe sera faite contre la clé Kerberos de la même entrée. Donc, afin que les liens simples utilisent le mot de passe Kerberos, nous n'avons qu'à remplacer l'attribut `userPassword` avec `{K5KEY}`.

Les modifications de configuration suivantes sont nécessaires afin d'utiliser le module `smbk5pwd` :

```
(...)
modulepath      /usr/lib/openldap
moduleload      back_monitor.la
moduleload      syncprov.la
moduleload      ppolicy.la
moduleload      smbk5pwd.so
password-hash   {K5KEY}
(...)
database bdb
(...)
overlay ppolicy
ppolicy_default "cn=default,ou=Password Policies,dc=example,dc=com"

overlay smbk5pwd
(...)
```

Si nous ne changeons pas le mécanisme de hash du mot de passe serveur à {K5KEY}, alors les changements de mot de passe via EXOP écraseront l'attribut `userPassword` avec le nouvel hash au lieu de laisser `{K5KEY}`.

Le module `smbk5pwd` accepte certaines instructions de configuration comme `smbk5pwd-enable` et `smbk5pwd-must-change`. Veuillez lire le fichier README dans le répertoire de documentation `openldap-servers` pour plus de détails.

Si Samba est utilisé, alors l'option `ldappasswdsync` devrait être réglée à `Only`. Avec cette option, Samba ne fera que la modification de mot de passe EXOP, et attendez-vous à ce que le serveur OpenLDAP mette à jour les hashs de Samba, soit exactement ce que fait `smbk5pwd`.

Dans la section `[global]` de `/etc/samba/smb.conf`, ajoutez:

```
ldap passwd sync = Only
```

Mainteneant, testez `ldappasswd`, `smbpasswd` et `kpasswd` : un changement de mot de passe réalisé par une ou l'autre de ces applications devrait changer les trois sources d'authentification.

7.2.5. Ajustements

Nous verrons ici des ajustements à réaliser sur OpenLDAP. Il vous aideront à obtenir le meilleur de votre serveur d'annuaire.

7.2.5.1. DB_CONFIG

La base de données par défaut d'OpenLDAP se nomme BDB (Berkeley DataBase). C'est une base de donnée robuste utilisée par de nombreux projets hautement paramétrables avec le fichier `DB_CONFIG`.

OpenLDAP (la version packagée par Mandriva Linux) est livré par défaut avec un fichier `DB_CONFIG`, mais celui-ci devrait être ajusté pour chaque environnement spécifique. Une configuration incorrecte peut causer de sérieux problèmes de performances ainsi que des problèmes d'intégrité de données.

Nous présentons ici les options clés de `DB_CONFIG` que tout administrateur OpenLDAP devrait connaître.

`set_cachesize<gbytes><bytes><ncache>`

Ce paramètre établit la mémoire cache à utiliser :

- `<gigabytes>` : taille du cache en gigaoctets.
- `<bytes>` : taille du cache en octets. Par exemple, si la valeur précédente est établie à `1` et celle-ci à `536870912`, la taille totale de la cache, constituée de la somme des deux valeure, serait de `1610612736` octets. La taille maximale d'une cache par segment (voir l'option suivante) est de 4 gigaoctets.

- <ncache> : le nombre de cache. Chaque cache est alloué dans une région de mémoire continue. La valeur 0 ou 1 indique seulement 1 segment.

set_lg_bsize<octets>

La base de données BDB est transactionnelle. Ce qui signifie que chaque écriture est d'abord notée dans un log, puis exécutée par la suite. Le paramètre set_lg_bsize indique la taille de la mémoire tampon (en octet) pour ce fichier journal. Chaque fois que cette taille de mémoire est atteinte, le log est écrit sur le disque.

set_lg_dir<path>

Par défaut, le fichier journal des transactions est écrit dans le même répertoire que la base de données. Ce répertoire peut varier afin d'utiliser un autre disque pour améliorer les performances globales.

La plupart des configurations de DB_CONFIG prennent effet au chargement de la base de données, ce qui peut être accompli avec la commande db_recover. Par exemple, pour rebâtir l'environnement dans /var/lib/ldap, la commande serait db_recover -v -h /var/lib/ldap (-v pour voir plus de détails).

Il faut toujours exécuter db_recover lorsque le démon slapd est arrêté.

Après avoir ajusté DB_CONFIG, particulièrement le paramètre relié à la cache, vous devriez utiliser la commande db_stat -m -h /var/lib/ldap pour en vérifier l'efficacité. Vous verrez alors un rapport du pourcentage de requêtes en cache. Vous voulez une valeur suppérieur à 90 %. Si votre serveur a assez de RAM, ceci peut-être gonflé jusqu'à 99 % ou même 100 %.

7.2.5.2. Cache OpenLDAP

En plus du cache de BDB, OpenLDAP possède aussi son propre cache. La paramètre de configuration cachesize prend une valeur comme argument qui détermine le nombre d'entrées qui doivent être conservées en cache. La valeur par défaut est 1000 (mille). Ce paramètre a un impact moindre sur les performances.

7.2.5.3. Index

Les index constituent la pierre angulaire de tous les types de bases de données. Sans index, les recherches peuvent être longues à compléter, et avoir un impact important sur le CPU.

Le paramètre `index` dans la section `database` de `slapd.conf` est utilisé pour spécifier quel attribut doit être indexé et avec quel type d'index. La syntaxe habituelle est :

```
index <attr1[,attr2,...]> <[pres,eq,approx,sub]>
```

Le type d'index varie selon le type de recherche prévu pour cet attribut. Par exemple, les recherches de type (`uid=*john*`) auront besoin d'un index `sub` pour la rapidité. Voici les types d'index les plus communs :

`pres`

: L'index de présence, utilisé par les tests pour vérifier la présence d'un attribut.

`eq`

: L'index d'égalité (equality) pour tester l'égalité. Par exemple, (`uid=john`).

`approx`

: L'index approximatif utilisé dans les recherches qui utilisent les tests approximatifs. Par exemple, (`uid~=sisko`).

`sub`

: Cet index est utilisé pour des recherches utilisant des sous-chaînes comme (`uid=*john*`). Notez que par défaut, OpenLDAP n'appliquera pas d'index de sous-chaînes pour les attributs avec moins de 2 caractères (voir `slapd.conf(5)` pour plus de détails permettant de changer ceci).

Le prochain exemple utilise différents types d'index pour certains attributs :

```
index   objectClass,uid,uidNumber,gidNumber,memberUid   eq
index   ou                                             eq
index   cn,mail,surname,givenname                      eq,sub
index   entryCSN,contextCSN,entryUUID                  eq
```

Dès qu'une recherche est lancée sur les attributs qui n'ont pas d'index appropriés, un mise en garde sera écrite dans les journaux du service :

```
Jul 31 14:12:36 pandora slapd[15130]: conn=8 op=1 SRCH
```

```
    base="dc=example,dc=com" scope=2 deref=0 filter="(ou=remotes)"
Jul 31 14:12:36 pandora slapd[15130]: <= bdb_equality_candidates: (ou)
    index_param failed (18)
```

Dès que ceci arrive, cela indique que la recherche a été particulièrement lente. Soit l'attribut doit être indexé, soit la recherche doit être modifiée pour inclure cet attribut.

Lorsqu'un index est ajouté après que la base de données ait été peuplé, celle-ci doit être réindexée. Cette tâche est accomplie en arrêtant le service et en exécutant la commande `slapindex`. Ce processus réindexera tous les attributs, ce qui peut être long pour certaines bases de données volumineuses.

7.2.5.4. RAM

OpenLDAP peut bénéficier d'un serveur avec beaucoup de RAM. Lorsque c'est possible, ou si vous constatez que le cache n'est pas très performant, ajoutez de la RAM à votre serveur. L'annuaire s'en portera mieux et vos utilisateurs également...

7.2.6. Utilisation avancée

OpenLDAP propose plusieurs options de superposition qui peuvent vous aider à exploiter un serveur d'identité. En voici quelques-unes, notamment :

- Password policies : contrôle l'expiration, la qualité des mots de passe, les comptes gelés, etc.
- Unique overlay : s'assure que certain attributs sont uniques.
- Dynamic groups and lists : création de groupe et de liste à la volée.
- Referential integrity : maintient la correspondance entre les entrées qui référencent d'autres entrées.
- Replication with syncrepl : crée des copies de vos données sur un autre serveur OpenLDAP.

Le paquetage du serveur Mandriva OpenLDAP propose la plupart des superpositions et des fondations en tant que modules séparés dans le répertoire `/usr/lib/openldap`. Pour charger une superposition, vous devez éditer `/etc/openldap/slapd.conf` comme ceci :

```
(...)
modulepath      /usr/lib/openldap
moduleload      overlay-filename
```

```
(...)
database bdb
(...)
overlay overlay-name
 overlay-specific-options
(...)
```

Donc, chargez d'abord le module `moduleload` puis, à l'intérieur de la section `database` activez-la par la directive `overlay`. N'importe quelle option de configuration de superposition spécifique peut maintenant être utilisée.

7.2.6.1. Politique de mot de passe

La superposition politique de mot de passe (`ppolicy.la`) intercepte les changements de mots de passe LDAP et y applique plusieurs politiques telles que :

- l'historique des mots de passe ;
- la longueur de mot de passe ;
- l'expiration des mots de passe ;
- les comptes bloqués ;
- le changement de mot de passe forcé.

Plusieurs politiques peuvent être définies sur le serveur et tous les usagers peuvent être assignés à n'importe quelle politique, ou recevoir celle par défaut.

Les versions récentes de `pam_ldap` (182 ou plus) supporte ce module OpenLDAP. Pour l'activer, ajoutez `pam_lookup_policyyes` dans `/etc/ldap.conf`.

À titre d'exemple, nous allons configurer un compte avec un changement de mot de passe forcé, une longueur minimum avec un historique de mot de passe. La liste complète des politiques et leur usage sont documentés dans la page de man `slapo-ppolicy(5)`.

1. Le fichier `/etc/openldap/slapd.conf` créé par défaut par `openldap-mandriva-dit` a déjà le support des politiques de mot de passe. Afin d'être complet, nous avons mis l'emphase sur les changements nécessaires :

```
(...)
include /usr/share/openldap/schema/dyngroup.schema
include /usr/share/openldap/schema/ppolicy.schema
(...)
modulepath      /usr/lib/openldap
moduleload      back_monitor.la
```

```
moduleload      syncprov.la
moduleload      ppolicy.la
# loads the module
(...)
database        bdb
suffix          "dc=example,dc=com"
(...)
overlay ppolicy # activates the overlay
ppolicy_default "cn=default,ou=Password Policies,dc=example,dc=com"
(...)
```

Après avoir redémarré le serveur, il va charger la politique de mot de passe et commencer à la diffuser dans la liste des capacités du serveur.

2. Maintenant, vous devez définir une politique. Notez que dans le fichier de configuration, une politique par défaut est déjà définie. Son contenu est rudimentaire et aucune règle n'y est encore définie :

```
dn: cn=default,ou=Password Policies,dc=example,dc=com
cn: default
objectClass: pwdPolicy
objectClass: namedObject
pwdAttribute: userPassword
```

La classe d'objet `namedObject` est définie dans le fichier de schéma `kolab.schema`. Si vous décidez de ne pas charger de schéma, une politique de mot de passe cassera les `namedObject` inutiles et les définiront ailleurs.

Si nous voulons appliquer les politiques listées plus tôt, nous devons changer cette entrée ou en créer une nouvelle. Nous allons changer cette entrée, la politique par défaut de notre base de données. Nous pourrons par la suite la clôner vers d'autres politiques, si nous le désirons.

Ci-dessous, la commande pour ajouter la politique désirée. Les membres du groupe système `AccountAdmins` peuvent changer les politiques :

```
$ ldapmodify -x -D 'uid=Account Admin,ou=System Accounts,
      dc=example,dc=com' -W
Enter LDAP Password: secretpassword
dn: cn=default,ou=Password Policies,dc=example,dc=com
changetype: modify
add: pwdMustChange
pwdMustChange: TRUE
-
add: pwdCheckQuality
pwdCheckQuality: 2
-
add: pwdInHistory
pwdInhistory: 2
-
add: pwdMinLength
```

```
pwdMinLength: 5

modifying entry "cn=default,ou=Password Policies,dc=example,dc=com"

^D
```

Explications :

- `pwdMustChange:TRUE`

  Force les usagers dont le mot de passe est réinitialisé à changer leur mot de passe. Leurs opérations LDAP seront restreintes tant que celui-ci n'est pas changé.

- `pwdCheckQuality:2`

  Active la validation de la qualité du mot de passe. Cette fonction va également activer `pwdMinLength` que nous établissons plus bas. La valeur 2 signifie que si pour une raison ou une autre la qualité du mot de passe ne peut être vérifiée (parce que le client l'assigne dans un hash, par exemple), la validation échouera.

- `pwdInHistory:2`

  Active l'historique de mot de passe et mémorise jusqu'aux 2 précédents mots de passe.

- `pwdMinLength:5`

  Définit la taille minimum d'un mot de passe à 4 caractères. Si c'est moins, le nouveau mot de passe sera rejeté.

Maintenant, toutes les entités qui n'ont pas d'instruction spécifique pour utiliser une autre politique seront asujetties à cette politique par défaut, y compris les comptes système .

3. Nous allons débuter nos tests avec l'usager `peter` en le forçant à changer son mot de passe. En tant qu'admin, nous marquons son mot de passe comme réinitialisé.

```
$ ldapmodify -x -D 'uid=Account Admin,ou=System Accounts,dc=example,
 dc=com' -W
Enter LDAP Password: secretpassword
dn: uid=peter,ou=People,dc=example,dc=com
changetype: modify
add: pwdReset
pwdReset: TRUE

modifying entry "uid=peter,ou=People,dc=example,dc=com"

^D
```

Voyons ce qui arive lorsque `peter` essaie, par exemple, de faire une recherche :

```
$ ldapsearch -x -LLL -D uid=peter,ou=People,dc=example,dc=com
 -W uid=peter uid
Enter LDAP Password: peter's password
Insufficient access (50)
Additional information: Operations are restricted to
 bind/unbind/abandon/StartTLS/modify password
```

Donc, `peter` est maintenant obliger de changer son mot de passe. Si nous activons le support `ppolicy` dans le client, nous avons un indice de ce qui s'est passé :

```
$ ldapsearch -x -LLL -D uid=peter,ou=People,dc=example,dc=com
 -W -e ppolicy uid=peter uid
Enter LDAP Password: peter's password
ldap_bind: Success (0); Password must be changed
Insufficient access (50)
```

Allez-y et changez le mot de passe pour `1234` :

```
$ ldappasswd -x -D uid=peter,ou=People,dc=example,dc=com -W -s
 1234 uid=peter,ou=People,dc=example,dc=com
Enter LDAP Password: peter's password
Result: Constraint violation (19)
Additional info: Password fails quality checking policy
```

Nous constatons que la politique `pwdMinLength` entre en fonction : nous avons utilisé un mot de passe de 4 caractères ou moins. Essayons avec 5 caractères :

```
$ ldappasswd -x -D uid=peter,ou=People,dc=example,dc=com -W
 -s 12345 uid=peter,ou=People,dc=example,dc=com Enter LDAP
Password: Result: Success (0)
```

Ça fonctionne. Finalement, pour démontrer la politique d'historique de mot de passe, essayons de changer le mot de passe en utilisant la valeur précédente :

```
$ ldappasswd -x -D uid=peter,ou=People,dc=example,dc=com
 -W -s peteroldpass uid=peter,ou=People,dc=example,dc=com
Enter LDAP Password: 12345
Result: Constraint violation (19)
Additional info: Password is in history of old passwords
```

Pour assigner une politique différente selon l'usager, utilisez l'attribut `pwdPolicySubentry` et pointez le vers le dn de la politique à utiliser. Par exemple, pour appliquer la politique `cn=marketing` à l'usager `peter`, faites :

```
$ ldapmodify -x -D 'uid=Account Admin,ou=System Accounts,dc=example,
 dc=com' -W
Enter LDAP Password: secretpassword
dn: uid=peter,ou=People,dc=example,dc=com
```

```
changetype: modify
add: pwdPolicySubentry
pwdPolicySubentry: cn=marketing,ou=Password Policies,dc=example,dc=com

modifying entry "uid=peter,ou=People,dc=example,dc=com"

^D
```

De cette façon, nous pouvons avoir différentes politiques appliquées à différents usagers. À l'heure actuelle, il n'est pas possible d'appliquer une politique à un groupe d'usagers, le changement doit être appliqué à chaque usager avec l'attribut `pwdPolicySubentry`.

Soyez prudent lorsque vous utilisez les politiques de mots de passe de OpenLDAP avec des applications qui ont leur propre politique ou le propre hash de mots de passe. Samba est un bon exemple. L'utilisation des politiques de Samba et de OpenLDAP en même temps serait problématique, compte tenu que Samba utilise ses propres attributs de mot de passe, tandis que OpenLDAP surveille `userPassword`. Il est possible que Samba permette un changement de mot de passe pendant que OpenLDAP le refuse en raison de politiques divergentes.

7.2.6.2. Superposition unique

La superposition unique (*unique overlay*) est utilisée en prévention qu'une partie de l'arborescence ne répète une paire attribut-valeur. Par exemple, la branche `ou=People` pourrait surveiller les changements dans l'attribut `uidNumber`. Si un changement devait survenir demandant d'utiliser un numéro pour cet attribut qui est déjà utilisé ailleurs, le changement serait refusé. Donc, chaque écriture vers un attribut surveillé déclenche une recherche LDAP pour cet attribut et vérifie si cette valeur est assignée quelque part dans la branche surveillée.

Il est très important que l'attribut surveillé ait l'index approprié !

À titre d'exemple, configurons le serveur pour prévenir la duplication de `uidNumber` et `cn` sous `ou=People`. Toutes les options sont décrites dans la page de man `slapo-unique(5)`.

1. Les changements à la configuration de `slapd.conf` :

```
(...)
```

```
modulepath      /usr/lib/openldap
moduleload      back_monitor.la
moduleload      syncprov.la
moduleload      unique.la # loads the module
(...)
database        bdb
suffix          "dc=example,dc=com"
(...)
overlay unique # activates the overlay
 unique_base  ou=People,dc=example,dc=com
 unique_attributes uidNumber cn

(...)
```

Après le rédémarrage du service OpenLDAP, le module sera chargé et nous pourrons faire des tests.

2. Test :

   Voyons ce qui arrive lorsqu'on essaie de changer le `uidNumber` d'un usager pour une valeur déjà assignée à un usager :

```
$ ldapmodify -x -D 'uid=Account Admin,ou=System Accounts,dc=example,
 dc=com' -W Enter LDAP Password:
secretpassword dn: uid=queen,ou=People,dc=example,dc=com
changetype: modify replace: uidNumber uidNumber: 1024

modifying entry "uid=queen,ou=People,dc=example,dc=com"
ldap_modify: Constraint violation (19)
additional info: some attributes not unique
```

   Le changement a été refusé tel que prévu parce que le `uidNumber` qui a été choisi était déjà utilisé par un autre usager.

Prenez soin de ne pas lister d'attributs qui pourraient avoir des valeurs doublées. `gidNumber`, par exemple, pendant qu'il est unique pour identifier un groupe POSIX, peut être utilisé plusieurs fois avec la même valeur sous `ou=People` : pensez aux usagers qui partagent le même groupe principal.

7.2.6.3. Groupes et listes dynamiques

Les groupes et les listes dynamiques sont très similaires et peuvent être utilisés pour peupler automatiquement une entrée avec des éléments.

Par exemple, nous pourrions avoir une liste dynamique qui s'étendrait automatiquement pour inclure toutes les addresses email que nous avons assignées à des utilisateurs. Ce serait notre alias email `all@example.com`.

De la même manière, nous pourrions avoir un groupe nommé `allusers` qui serait toujours à jour concernant les usagers de notre annuaire. Si un usager est supprimé ou ajouté, le groupe refléterait ce changement dynamiquement.

Dès qu'une entrée avec une classe surveillée est retournée suite à une requête, une recherche est lancée pour assembler les attributs qui doivent être retournés avec la requête. C'est cette recherche qui rend l'entrée dynamique. Les paramètres de recherche sont encodés dans un attribut de cette même entrée.

L'exemple suivant illustre comment configurer l'alias email automatique présenté plus haut, qui s'étendra toujours pour inclure tous les usagers de l'annuaire :

1. Changements dans `slapd.conf` :

```
(...)
modulepath      /usr/lib/openldap
moduleload      back_monitor.la
moduleload      syncprov.la
moduleload      dynlist.la # loads the module
(...)
database        bdb
suffix          "dc=example,dc=com"
(...)
overlay dynlist # activates the overlay
# dynlist-attrset <group-oc> <URL-ad> [<member-ad>]
dynlist-attrset nisMailAlias labeledURI

(...)
```

   Le paramètre `nisMailAlias` est le nom de la classe qui lancera la recherche et `labeledURI` est le nom de l'attribut qui contient les spécifications de la recherche. C'est plus facile à comprendre en voyant l'entrée à la prochaine étape.

2. Voici une entrée de notre alias email `allusers` :

```
dn: cn=allusers,ou=Aliases,dc=example,dc=com
cn: allusers
objectClass: nisMailAlias
objectClass: labeledURIObject
labeledURI: ldap:///ou=People,dc=example,dc=com?mail?one?
 (objectClass=inetOrgPerson)
```

L'arborescence par défaut n'offre pas la branche `ou=Alias`. Afin d'ajouter l'entrée `cn=allusers`, vous devez d'abord ajouter `ou=Alias` :

```
dn: ou=Aliases,dc=example,dc=com
objectClass: organizationalUnit
ou: Aliases
```

Souvenez-vous que `nisMailAlias` est l'initiateur. Dès qu'une entrée avec cette classe est retournée, la recherche spécifiée dans `labeledURI` est lancée. Dans notre cas, la recherche signifie :

- base: `ou=People,dc=example,dc=com`
- scope: `one`
- filter: `(objectClass=inetOrgPerson)`
- returned attribute: `mail`

Cette recherche retournera l'attribut `mail` pour chaque entrée sous `ou=People` qui possède la classe `inetOrgPerson`.

Voici son fonctionnement :

```
$ ldapsearch -x -LLL cn=allusers
dn: cn=allusers,ou=Aliases,dc=example,dc=com
cn: allusers
objectClass: nisMailAlias
objectClass: labeledURIObject
labeledURI: ldap:///ou=People,dc=example,dc=com?mail?one?
 (objectClass=inetOrgPerson)
mail: peter@example.com
mail: queen@example.com
```

Comparez ce résultat avec celui obtenu précédemment : voyez-vous la différence ?

Il y a deux nouveaux attributs qui n'étaient pas dans l'entrée originale : l'adresse email pour `peter` et `queen`. Ces entrées ont été ajoutées dynamiquement grâce à la recherche réalisée lorsque cette entrée a été retournée. Si nous retirons l'attribut mail de `queen`, ou toute l'entrée, la prochaine recherche sous `allusers` n'affichera plus cette adresse.

Nous allons faire une configurations similaire, mais pour le groupe dynamique.

1. Changements à `slapd.conf` :

```
(...)
modulepath      /usr/lib/openldap
moduleload      back_monitor.la
```

```
moduleload      syncprov.la
moduleload      dynlist.la # loads the module
(...)
database        bdb
suffix          "dc=example,dc=com"
(...)
overlay dynlist # activates the overlay
# dynlist-attrset <group-oc> <URL-ad> [<member-ad>]
dynlist-attrset groupOfNames labeledURI member

(...)
```

Surveillons maintenant une différente classe d'object : `groupOfNames`. Dès qu'une entrée l'incluant est retournée, la recherche spécifiée dans l'attribut `labeledURI` est lancée et toutes les entrées qui correspondent sont listées avec l'attribut `member`.

2. L'entrée de groupe dynamique :

```
dn: cn=allusers,ou=Group,dc=example,dc=com
cn: allusers
objectClass: groupOfNames
objectClass: labeledURIObject
member: uid=LDAP Admin,ou=System Accounts,dc=example,dc=com
labeledURI: ldap:///ou=People,dc=example,dc=com??one?
 (objectClass=inetOrgPerson)
```

Le filtre de recherche est très similaire au précédent. Mais maintenant nous ne sommes plus intéressés par le contenu de l'attribut mail. Nous voulons simplement lister toutes les personnes présentes dans la branche `ou=People`.

3. Pour le tester, voyons le contenu de notre groupe dynamique :

```
$ ldapsearch -x -LLL -b ou=Group,dc=example,dc=com cn=allusers
dn: cn=allusers,ou=Group,dc=example,dc=com
cn: allusers
objectClass: groupOfNames
objectClass: labeledURIObject
member: uid=LDAP Admin,ou=System Accounts,dc=example,dc=com
member: uid=john,ou=People,dc=example,dc=com
member: uid=mary,ou=People,dc=example,dc=com
member: uid=peter,ou=People,dc=example,dc=com
member: uid=queen,ou=People,dc=example,dc=com
labeledURI: ldap:///ou=People,dc=example,dc=com??one?
 (objectClass=inetOrgPerson)
```

Aussi, lorsque nous comparons ceci avec le fichier original, le résultat inclut désormais ces nouveaux attributs `member`. Il ont été créés dynamiquement selon les résultats de la recherche. Si nous supprimons l'un d'eux de la base de données et que nous effectuons une recherche sur le groupe à nouveau, celui-ci sera à jour et n'affichera pas les usagers supprimés.

Notez cependant qu'une recherche comme celle présentée plus bas ne fonctionnerait pas sur un groupe dynamique.

```
$ ldapsearch -x -LLL -b ou=Group,dc=example,dc=com
 "(&(objectClass=groupOfNames)
 (member=uid=queen,ou=People,dc=example,dc=com))"
```

Pour que cela fonctionne, le serveur devrait effectuer la recherche spécifiée dans `labeledURI` pour chaque groupe, ce qui n'est pas supporté pour le moment. Mais une comparaison fonctionne :

```
$ ldapcompare -x cn=allusers,ou=group,dc=example,dc=com
 member:uid=queen,ou=People,dc=example,dc=com
TRUE
```

7.2.6.4. Intégrité référentielle

L'intégrité référentielle est une fonctionnalité commune dans les bases de données relationnelles. Ce concept signifie que lorsqu'une entrée qui est requise par une autre est supprimée, l'opération est refusée. Un scénario commun dans le monde LDAP serait de supprimer un compte utilisateur sans supprimer l'usager du groupe. Ce qui occasionnerait des usagers fantômes à l'intérieur de groupes, c'est-à-dire, des groups avec des usagers qui n'existent plus.

Pour gérer ce scénario, les administrateurs ont typiquement recours à des scripts ou des outils qui mettront les groupes à jour, ou n'importe quelle entité dépendante de l'entrée suprimée. Ceci n'est pas difficile, seulement quelques recherches et une mise à jour sont nécessaires.

La couche de superposition `refint` permet de réaliser une partie de ceci automatiquement. Poursuivons avec notre exemple de groupe. Cette superposition peut être configurée pour garder l'intégrité de l'attribut `member`, qui liste le membre du groupe. Dès qu'une entrée est supprimée de l'annuaire, une recherche est lancée sur tous les attributs `member` pointant vers cette entrée supprimée. Les entrées qui correspondent se verront l'attribut `member` retiré, maintenant ainsi l'intégrité.

Ceci démontre que la couche de superposition `refint`, plutôt que de refuser une opération qui briserait l'intégrité, va plutôt retirer ou renommer les attributs pour composer avec la suppression.

L'exemple suivant supprime un usager et montre comment le groupe est mis à jour automatiquement.

1. Changements à `slapd.conf` :

```
(...)
modulepath      /usr/lib/openldap
moduleload      back_monitor.la
moduleload      syncprov.la
moduleload      refint.la # loads the module
(...)
database        bdb
suffix          "dc=example,dc=com"
(...)
overlay refint # activates the overlay
refint_attributes member
refint_nothing "uid=LDAP Admin,ou=System Accounts,dc=example,dc=com"

(...)
```

La couche de superposition a seulement deux paramètres de configuration

- `refint_attributes` : l'attribut d'intégrité. Si, par exemple, une entrée nommée `uid=John,ou=People,dc=example,dc=com` est retirée, une recherche est lancée pour `member="uid=John,ou=People,dc=example, dc=com"` et cet attribut est retiré pour les entrées correspondantes.
- `refint_nothing` : il est possible que le dernier attribut d'une entrée soit supprimé par contrainte d'intégrité. Certaines classes d'objets, par contre, requièrent au moins un attribut. Si cette situation devait se présenter, la couche de superposition peuplera le dernier attribut avec le dn configuré ici. Donc, par exemple, si le dernier membre d'un groupe est `uid=John,ou=People,dc=example,dc=com` et que cet usager a été retiré de la base de données, afin de ne pas laisser le groupe sans membre (ce qui est interdit par la classe d'objet `groupOfNames`), la superposition va ajouter `member=uid=LDAPAdmin,ou=SystemAccounts,dc=example, dc=com` au groupe.

La couche de superposition d'integrité référentielle fonctionne avec le DN complet. Ce qui signifie qu'il n'est pas possible de l'utiliser pour maintenir l'intégrité des classes de groupe qui utilisent l'attribut `memberUid`, par exemple, parce que cet attribut tient juste un nom d'usager et non un DN.

2. Test :

   Imaginons que nous avons le groupe suivant avec 2 utilisateurs :

```
$ ldapsearch -x -LLL cn=mkt member
dn: cn=mkt,ou=Group,dc=example,dc=com
member: uid=peter,ou=People,dc=example,dc=com
member: uid=queen,ou=People,dc=example,dc=com
```

Si nous supprimons peter de la base de données, le groupe est automatiquement mis à jour pour refléter que cet usager est supprimé :

```
$ ldapdelete -x -D 'uid=Account Admin,ou=System Accounts,dc=example,
 dc=com' -W uid=peter,ou=People,dc=example,dc=com
Enter LDAP Password: secretpassword
$ ldapsearch -x -LLL cn=mkt member
dn: cn=mkt,ou=Group,dc=example,dc=com
member: uid=queen,ou=People,dc=example,dc=com
```

Si nous supprimons le dernier usager du groupe, (queen), nous verrons alors la configuration refint_nothing s'activer :

```
$ ldapdelete -x -D 'uid=Account Admin,ou=System Accounts,dc=example,
 dc=com' -W uid=queen,ou=People,dc=example,dc=com
Enter LDAP Password: secretpassword
$ ldapsearch -x -LLL cn=mkt member
dn: cn=mkt,ou=Group,dc=example,dc=com
member: uid=LDAP Admin,ou=System Accounts,dc=example,dc=com
```

Au lieu de laisser le groupe sans membres, ce qui est proscrit par la classe d'objet groupOfNames, le recouvrement est ajouté au DN refint_nothing en tant que son seul membre.

7.2.7. Réplication avec syncrepl

Afin d'assurer la disponibilité en cas de panne ou de problème majeur, il est particulièrement utile d'avoir plusieurs serveurs LDAP offrant les mêmes donnés. La réplication permet cette fonctionalité. syncrepl est la solution de choix.

La réplication est assez flexible pour nous permettre de répliquer un annuaire en entier ou en partie. Par exemple, imaginons qu'un serveur de courriel dans une zone DMZ a besoin d'accéder au serveur LDAP de l'entreprise pour valider un email. Une approche pourrait être de le laisser faire sa requête dans le serveur LDAP interne :

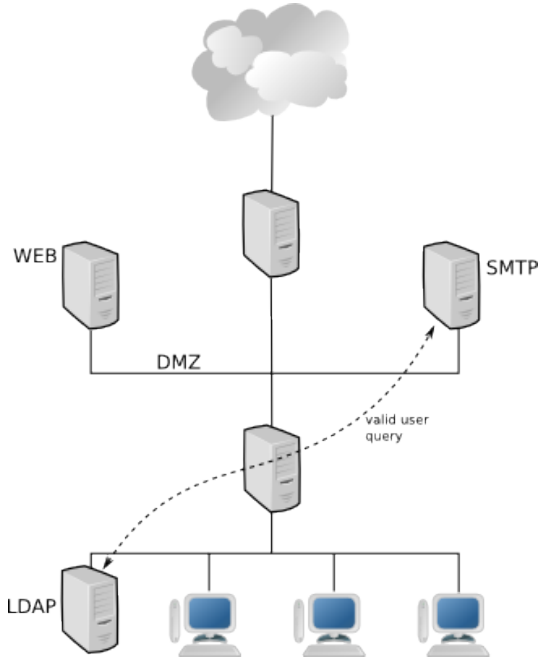


Figure 7-10. En utilisant un serveur LDAP interne

Une autre approche serait de placer un serveur consommateur LDAP dans la DMZ. Ce serveur n'a pas besoin de l'ensemble de l'annuaire, seulement des informations pertinentes pour le serveur de courriel (et potentiellement d'autres serveurs DMZ). Cette réplication filtrerait les autres attributs. En plus, un serveur mail peut continuer à livrer des messages même si le serveur interne principal est en panne .

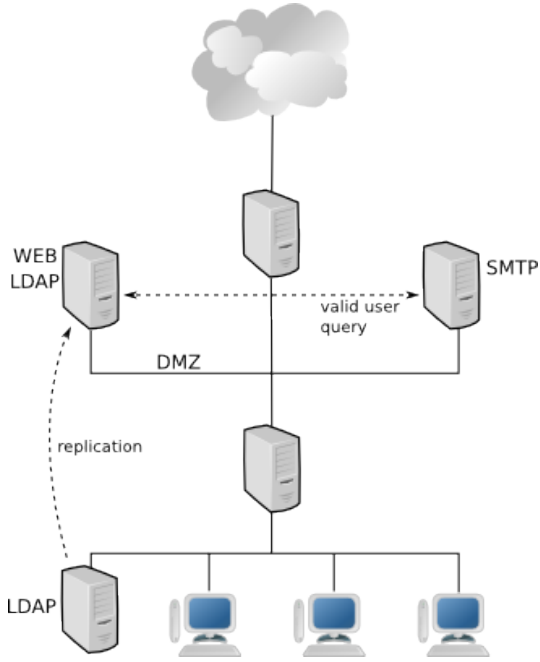


Figure 7-11. En utilisant une réplique

7.2.7.1. Configuration du producteur

Le rôle du producteur est assigné par la couche de superposition `syncprov`. La configuration du paquetage `openldap-mandriva-dit` et ses scripts de démarrage ont déjà tous les détails nécessaires.

Voici ce dont nous aurons besoin dans `slapd.conf` :

```
(...)
modulepath      /usr/lib/openldap
moduleload      back_monitor.la
moduleload      syncprov.la
(...)

database        bdb
suffix          "dc=example,dc=com"
(...)
overlay syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100
```

Selon le fonctionnement de syncrepl (consultez `OpenLDAPAdminGuide` et le `RFC4533` pour plus de détails), les opérations d'écriture sont mieux suivies

avec l'utilisation d'un log de session. Ce sont des valeurs suggérées qui varient selon le nombre d'écritures reçues par l'annuaire dans une période donnée.

- `syncprov-checkpointopsminutes` : met `contextCSN` à jour dans l'annuaire après que l'opération d'écriture de `ops` ou plus de `minutes` minutes se sont écoulées depuis le dernier checkpoint. Notez que ces numéros ne sont pas vérifiés après une opération d'écriture.
- `syncprov-sessionlogops` : taille du log qui va enregistrer l'information à propos des opérations d'écriture.

Il nous reste un changement à faire : configurer les limites.

`syncrepl` fonctionne via une opération de recherche hiérarchique. Le consommateur lancera cette recherche sur le producteur et la réponse contient les données devant être répliquées. Donc, si le consommateur commence vide, la réponse contiendra toutes les données à répliquer. Une fois synchronisée, la réponse ne contiendra que les entrées changées, ajoutées ou supprimées. Ce qui signifie :

- Le consommateur doit pouvoir lire les données : donc les ACL appropriées doivent être en place pour permettre cette lecture des données à être répliquées.
- Les bonnes limites doivent être en place pour le consommateur sur le producteur : nous ne voulons pas que le consommateur atteigne une limite de taille durant la réplication et ainsi empêcher la réplication de toutes les entrées.

Afin d'aborder tous ces enjeux, la solution habituelle est de créer un compte spécifique à la réplication et d'ajuster les ACL et les limites pour ce compte. `openldap-mandriva-dit` accomplit ceci à travers le groupe `LDAPReplicators` et ses membres :

```
limits group="cn=LDAP Replicators,ou=System Groups,dc=example,dc=com"
    limit size=unlimited
    limit time=unlimited

access to dn.subtree="dc=example,dc=com"
by group.exact="cn=LDAP Admins,ou=System Groups,dc=example,dc=com" write
by group.exact="cn=LDAP Replicators,ou=System Groups,dc=example,dc=com"
 read
by * break
```

Cette configuration vérifie que les membres du groupe `LDAPReplicators` peuvent lire toutes les entrées et attributs, et n'a pas de limite de taille ou de temps appliquée, ce qui correspond exactement à ce dont nous avons besoin pour le

support de la réplication avec syncrepl. Notez que les ACLs peuvent être ajustées si vous préférez limiter les accès de lecture aux données qui n'ont pas besoin d'être répliquées.

Après avoir fait ces modifications et redémarré le service, ce serveur est prêt a recevoir des consommateurs avec des données répliquées. Aucun autre changement n'est nécessaire (mise à part de l'optimisation) pour ajouter un autre consommateur.

7.2.7.2. Configurer le consommateur

La configuration au niveau consommateur est plus complexe et ressemble au processus de slurpd. Il y a deux types de réplications :

- `refreshOnly` : le consommateur initie la réplication en contactant le producteur et en demandant des données. Une fois les données reçues, cela arrête la connexion et le consommateur se met en mode veille pour une durée spécifiée. Une fois ce délai expiré, il se réveille, contacte le serveur et répète l'opération.
- `refreshAndPersist` : encore une fois, le consommateur initie la réplication en contactant le producteur. La différence, c'est qu'une fois les données reçues, la connexion reste ouverte. Le producteur utilisera désormais cette connexion pour avertir le consommateur des changements. Donc, au lieu d'un appel comparable à `cron`, les consommateurs qui utilisent `refreshAndPersist` obtiennent des nouvelles données dès qu'elles sont disponibles sur le producteur.

pour la réplication `refresh`, voici ce dont on a besoin :

```
syncrepl    rid=001
provider=ldap://provider.example.com
starttls=critical
type=refreshOnly
interval=00:01:00:00
searchbase="dc=example,dc=com"
scope=sub
filter="(objectClass=*)"
attrs="*,+"
bindmethod=simple
binddn="uid=LDAP Replicator,ou=System Accounts,ou=global,dc=example,dc=com"
credentials="ldapreplicator"
```

Pour `refreshAndPersist`, la configuration est comme ceci :

```
syncrepl rid=001 provider=ldap://provider.example.com
starttls=critical type=refreshAndPersist retry="60 +"
searchbase="dc=example,dc=com" scope=sub
```

```
filter="(objectClass=*)" attrs="*,+" bindmethod=simple
binddn="uid=LDAP Replicator,ou=System Accounts,ou=global,dc=example,dc=com"
credentials="ldapreplicator"

    updateref   ldap://provider.example.com
```

Les paramètres plus importants sont décrits plus bas. Vous trouverez plus de détails dans la page de man de `slapd.conf(5)`.

`rid`

Spécifie un identifiant unique pour cet instance consommateur.

`producteur`

URI du producteur.

`starttls`

Lorsque les opérations START TLS doivent être utilisées, (`yes`) et si c'est critique ou non (`critical`).

`type`

Le type de cette réplication : soit `refreshOnly` ou `refreshAndPersist`.

`interval`

Dans le mode `refreshOnly`, ce paramètre spécifie l'intervalle entre les tentatives de réplication. Le format est `dd:hh:mm:ss`.

`retry`

Dans le mode `refreshAndPersist`, ce paramètre spécifie comment gérer la situation lorsque le producteur est non-disponible. La syntaxe est une liste d'intervalle `retryinterval` et `numberofretries` en paire. Si le symbole + est utilisé à la place de `numberofretries`, cela signifie « indéfiniment ».

`searchbase,scope,filter,attrs`

Ces paramètres ont le même comportement que les opérations régulières de recherche LDAP, et peuvent être utilisés pour choisir en détail les données à répliquer. Les valeurs par défaut sont suffisantes pour toute la `searchbase`, avec tous les attributs disponibles.

`bindmethod`

Quelle méthode de connexion utiliser : `simple` ou `sasl`.

`binddn`

Dans le cas de la connexion `simple`, cette option spécifie le dn de connexion qui doit être utilisé.

`credentials`

Spécifie le secret associé avec la connexion `simple` et `sasl`.

N'utilisez pas un hash de mot de passe (*hashed password*) pour le paramètre `credentials`, ce doit être du texte clair ! Souvenez-vous que dans ce cas, le consommateur est un client LDAP comme tous les autres.

7.2.7.3. Test de réplication

Pour tester la réplication, la façon la plus simple est de vider la base de données et de la redémarrer en étant vide. Les fichiers journaux de producteur *producer logs* (au `loglevel256`) devraient afficher les connexions des consommateurs (nous avons supprimé quelques colonnes pour que ce soit plus clair) :

```
conn=1 fd=27 ACCEPT from IP=10.0.4.29:4479 (IP=0.0.0.0:389)
conn=1 op=0 BIND
 dn="uid=LDAP Replicator,ou=System Accounts,dc=example,dc=com"
 method=128
conn=1 op=0 BIND
 dn="uid=LDAP Replicator,ou=System Accounts,dc=example,dc=com"
 mech=SIMPLE ssf=0
conn=1 op=0 RESULT tag=97 err=0 text=
conn=1 op=1
 SRCH base="dc=example,dc=com" scope=2 deref=0 filter="(objectClass=*)"
conn=1 op=1 SRCH attr=* +
conn=1 op=2 UNBIND
conn=1 fd=27 closed
```

Après un court instant, et fonction de la taille de l'annuaire, le consommateur devrait être synchro avec le producteur.

7.2.8. Tâches d'entretien

Nous listons quelques tâches d'entretien qui devraient être faites périodiquement pour assurer que votre service d'identité fonctionne correctement.

7.2.8.1. Efficacité du cache

Pour surveiller l'efficacité du cache BDB, vous devez lancer la commande `db_stat`. Voici un exemple :

```
# db_stat -m -h /var/lib/ldap/ | head -n 6
40MB 1KB 604B   Total cache size.
1       Number of caches.
40MB 8KB        Pool individual cache size.
0       Requested pages mapped into the process' address space.
975     Requested pages found in the cache (98%).
19      Requested pages not found in the cache.
(...)
```

L'écran précédent montre la taille actuelle du cache (`40MB`) et le pourcentage de réponse pertinente (*hit percentage*) de la base de données principale (`98%`). Une façon rapide de faire un survol des réponses de la base de données est d'utiliser la commande `db_stat -m -h /var/lib/ldap | grep %`.

Si le pourcentage de réponse pertinente est peu élevé (disons sous les 90 %), vous devriez accroître le cache. Souvenez-vous d'exécuter `db_recover` après pendant que le service est arrêté afin que ces changements deviennent effectifs.

Notez que vous devriez toujours prendre en considération le nombre de requêtes qu'un fichier de base de données a reçu. S'il y a peu de requêtes, le pourcentage de réponse pertinente pourrait être déformé.

7.2.8.2. Gestion des transactions dans les fichiers journaux

OpenLDAP utilise le support pour les transactions qu'utilise BDB. Cela veut dire qu'en temps voulu, le répertoire de base de données se remplira de fichiers journaux :

```
# l /var/lib/ldap/log.*
-rw-------  1 ldap ldap 170K Ago 18 17:40 /var/lib/ldap/log.0000000001
```

Par défaut, chaque fichier journal grossira jusqu'à une taille de 10 Mo et sera pivoté, ce qui signifie qu'un nouveau fichier commencera. Chaque fichier journal contient toutes les opérations d'écriture faites sur la base de données. Il serait donc possible de la reconstruire depuis zéro si tous les fichiers journaux sont disponibles. C'est ce qu'on appelle une « restauration » (*catastrophic recovery*).

Un fichier journal peut contenir des transactions ouvertes, c'est-à-dire des changements qui n'ont pas encore été envoyés à la base de données. La commande `db_archive` peut être utilisée pour lister les fichiers journaux qui

ne sont plus en utilisation et qui pourraient être supprimés (ou sauvegardés ailleurs si vous voulez pouvoir exécuter une restauration extraordinaire dans le futur) :

```
# db_archive -h /var/lib/ldap
#
```

Dans cet exemple, aucun fichier journal n'a été imprimé par `db_archive`, ce qui signifie que tous les fichiers journaux sont en fonction. Voici une sortie différente possible :

```
# db_archive -h /var/lib/ldap
log.0000000001
log.0000000002
log.0000000003
#
```

Ceci signifie que les fichiers journau affichés ne sont plus en usage et peuvent être supprimés ou sauvegardés. L'outil peut supprimer ces fichiers journaux automatiquement à travers l'option `-d`.

En option, les fichiers journaux peuvent être supprimés automatiquement par la bibliothèque elle-même, lorsqu'ils sont pivotés. Pour que cela arrive, vous devez spécifier au drapeau `DB_LOG_AUTOREMOVE` dans le fichier `DB_CONFIG` :

```
(... other DB_CONFIG options ...)
set_flags DB_LOG_AUTOREMOVE
```

7.2.8.3. Vérification des index

Les index sont importants pour toutes les bases de données, et donc aussi les annuaires. Lorsque OpenLDAP reçoit une requête de recherche sur des attributs non indexés, une mise en garde est inscrite dans le fichier journal. Particulièrement dans les premiers jours de mise en production, il est important de regarder les fichiers journaux périodiquement et de repérer ces mises en garde, de réindexer les attributs ou de changer les paramètres de recherche :

```
# grep index_param /var/log/ldap/ldap.log
Aug 24 10:04:43 mes5 slapd[27399]: <= bdb_equality_candidates:
 (ou) index_param failed (18)
Aug 24 10:04:45 mes5 slapd[27399]: <= bdb_equality_candidates:
 (ou) index_param failed (18)
(...)
Jul 21 15:43:59 mes5 slapd[29666]: <= bdb_equality_candidates:
 (sambaSIDList) index_param failed (18)
Jul 21 15:43:59 mes5 slapd[29666]: <= bdb_equality_candidates:
```

```
 (sambaSIDList) index_param failed (18)
(...)
```

Ceci montre qu'au moins deux recherches étaient faites sur des attributs non indexés. Dans les deux cas, l'index manquant était de type égalité *equality type* (donc, `bdb_equality_candidates`). Pour remédier à la situation, ces index doivent être ajoutés et la base de données doit être réindexée.

7.2.9. Dépannage

Voici quelques astuces pour vous dépanner lorsque des problèmes connus dans OpenLDAP surviendront.

7.2.9.1. Reconnaître les utilisateurs dans LDAP

Le symptôme classique est d'exécuter `getent passwd john` et que l'utilisateur `john` n'existe pas, mais il est dans l'annuaires LDAP. Plusieurs éléments sont impliqués dans cette vérification pourtant simple, ce qui veut dire que plusieurs éléments peuvent en être la cause.

Le chemin à travers lequel cette commande passe est plus ou moins celui-ci : glibc, nss, nss_files, nss_ldap, ldap, user entry (classe d'objet `posixAccount`). Jetons-y un œil :

- Fichiers journaux du serveur : premièrement, vérifiez les fichiers journaux du serveur OpenLDAP pour voir si une requête de recherche est journalisée. Si tel est le cas, alors le problème se trouve probablement dans les données (non présentes ou incorrectes).
- `/etc/nsswitch.conf` : vérifiez si `ldap` est correctement ajouté à la table de correspondance `passwd` et toute autre table que vous interrogez.
- `nss_ldap` : vérifiez que le paquetage `nss_ldap` est installé.
- `/etc/ldap.conf` : vérifiez la recherche de base sur le serveur et si SSL est utilisé, ou non. S'il fonctionne, vérifiez l'information relative au certificat sur le serveur et le client.
- Données utilisateur : vérifiez si l'utilisateur existe sur le serveur LDAP et que les données sont correctes (classe d'objet `posixAccount`). Vérifiez les ACL. Essayez de faire manuellement la commande de recherche que `nss_ldap` fait.

7.2.9.2. Fichiers journaux du serveur

OpenLDAP vous donne un niveau exhaustif de détails en ce qui concerne les fichiers journaux du serveur. Celui qui est le plus utilisé, et celui que nous recommandons pour commencer à déboguer, est le 256. Donc, lorsque vous déboguez, assurez-vous de commencer avec `loglevel256` dans `slapd.conf`. D'autres niveaux sont disponibles, lisez la page de man de `slapd.conf(5)` pour une liste complète.

7.2.9.3. Cas divers

Pour qu'un serveur d'identité fonctionne correctement, plusieurs services sont nécessaires. Voici une liste non exhaustive :

- Protocole de temps réseau (NTP) : obligatoirement requis par le serveur Kerberos, c'est toutefois une bonne idée d'exécuter ce service sur tous les serveurs afin qu'ils soient tous à la même heure.
- Service de nom de domaine (DNS) : il est aussi obligatoire d'avoir un service DNS bien configuré et disponible sur le réseau. Plusieurs services échoueront probablement de façon bizarre si le DNS n'est pas disponible ou mal configuré.
- Permission de système de fichiers : le démon `slapd` est exécuté en tant qu'utilisateur non privilégié. Parfois, on exécute la commande `db_recover` en tant que root et on oublie de changer le propriétaire des fichiers qui ont été touchés par `ldap`. L'initscript s'occupe de ceci automatiquement, mais parfois on exécute des choses en mode de débogage sans l'initscript, et cela échouera si le démon ne peut pas lire les fichiers de la base de données. La même logique s'applique au fichier de configuration principal et aux certificats SSL : ils doivent être lisibles par l'utilisateur `ldap`.
- Si `slapd` échoue soudainement au démarrage lorsque le recouvrement (*overlay*) smbk5pwd vient d'être ajouté, la cause probable est que `/var/heimdal` a des permissions strictes et que l'utilisateur `ldap` ne peut pas entrer dans le répertoire. Donnez simplement au groupe `ldap` les permissions `r-x` pour ce répertoire et tout devrait fonctionner.

7.3. Serveurs de base de données

7.3.1. Serveur de bases de données MySQL

Ce document vise à fournir les informations nécessaires à une administration sommaire d'un serveur de base de données MySQL.

Ce document n'a pas pour but d'apprendre le SQL, et l'ensemble des commandes SQL disponibles dans MySQL est disponible dans la documentation en ligne sur le site officiel de MySQL : (`http://dev.mysql.com/doc/#manual`).

7.3.1.1. Concepts de base et références

MySQL est un système de gestion de bases de données relationnelles (SGBDR) libre développé par la société MySQL AB. La société a été fondée par les développeurs de MySQL et offre du service autour de cet outil.

Ce SGBD(R) dispose de différents moteurs de stockage développés par MySQL AB, comme MyISAM (non relationnel), ou par des sociétés tiers comme innoDB (relationnel), de Innobase Oy.

Liste d'URL à connaître :

- Le site de la société MySQL AB (`http://www.mysql.com/`) : ses produits et ses services ;
- le site du SGBDR MySQL (`http://dev.mysql.com/`) : forums, documentation, téléchargements... ;
- le site pour télécharger MySQL ; (`http://dev.mysql.com/downloads/`)
- La documentation officielle. (`http://dev.mysql.com/doc/`)

Voici la liste des RPM disponibles sous Mandriva Enterprise Server 5 :

- `mysql` : le moteur du système de gestion de bases de données.
- `mysql-client` : l'ensemble des clients en ligne de commande pour le serveur MySQL (outils d'administration, de sauvegarde et de restauration).
- `mysql-common` : l'ensemble des fichiers communs aux précédents paquetages.
- `mysql-Max` : cette version inclut des fonctionnalités supplémentaires qui n'ont pas été complètement testées, ou qui ne sont pas requises dans un ca-

dre standard d'utilisation. Quand ces fonctionnalités sont suffisamment stables, elles sont incluses dans la version standard. Le principal atout de cette version est l'inclusion de MySQL Cluster et des services l'accompagnant.

- `mysql-bench` : l'ensemble des programmes et scripts fournis par MySQL pour réaliser des tests de performance (*benchmarks*).

7.3.1.2. Installation et configuration du serveur

7.3.1.2.1. Administration de base

S'il existe des outils Web ou graphiques pour se connecter à un serveur MySQL, comme phpMyAdmin (`http://www.phpmyadmin.net`), le paquetage fournit aussi tout le nécessaire pour administrer le serveur et les bases de données.

Immédiatement après l'installation, il n'existe que les bases indispensables au fonctionnement de MySQL. La base « mysql » contient la liste des bases et des utilisateurs MySQL.

```
# mysql -u root
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1
Server version: 5.0.81 Mandriva Linux - MySQL Standard Edition (GPL)

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.

mysql> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| test               |
+--------------------+
3 rows in set (0.00 sec)

mysql> \r mysql
Connection id:    10
Current database: mysql

mysql> SHOW TABLES;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| columns_priv              |
| db                        |
| func                      |
| help_category             |
| help_keyword              |
```

```
| help_relation             |
| help_topic                |
| host                      |
| proc                      |
| procs_priv                |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| user                      |
+---------------------------+
17 rows in set (0.00 sec)

mysql> SELECT user FROM user;
+------+
| user |
+------+
| root |
|      |
| root |
|      |
| root |
+------+
5 rows in set (0.00 sec)
```

S'il n'existe pas de bases de données (autre que les bases système), deux utilisateurs sont déjà définis : root et un utilisateur anonyme. Le premier est l'administrateur de la base de données, le second un utilisateur lambda qui a accès à la base `test`. Il existe 2 lignes pour chacun de ces utilisateurs : l'une permet à l'utilisateur concerné de se connecter via le nom d'hôte `localhost`, l'autre par le véritable nom de la machine ou son adresse IP.

7.3.1.2.2. Mot de passe de l'administrateur

Le premier travail consiste à spécifier un mot de passe pour ces comptes, ou tout au moins pour l'administrateur. Pour cela, il existe plusieurs méthodes en ligne de commande shell ou SQL. Il faut évidemment penser à le faire pour les 2 entrées qui existent dans la base des utilisateurs.

```
# mysqladmin -u root password 'nouveaumotdepasse'
# mysqladmin -u root -h MES5 password 'nouveaumotdepasse'
```

La seconde commande ne peut fonctionner que si MySQL autorise les connexions réseau.

En SQL, il existe différentes alternatives :

```
# mysql -u root mysql
mysql> SET PASSWORD FOR 'root'@'localhost' = PASSWORD('nouveau_mot');
mysql> SET PASSWORD FOR 'root'@'MES5' = PASSWORD('nouveau_mot');
```

ou

```
# mysql -u root mysql
mysql> UPDATE mysql.user SET Password = PASSWORD('nouveau_mot')
    ->     WHERE User = 'root';
mysql> FLUSH PRIVILEGES;
```

Ici, la commande ne prend pas en compte la notion de nom d'hôte (*hostname*), ce qui explique qu'il n'est pas nécessaire de la taper 2 fois. Concernant l'utilisateur anonyme, on pourra réaliser les mêmes opérations.

Une fois qu'un mot de passe est spécifié, il est nécessaire de le saisir lors de chaque connexion à la base :

```
# mysql -u root
ERROR 1045 (28000): Access denied for user 'root'@'localhost'
 (using password: NO)
# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1
Server version: 5.0.81 Mandriva Linux - MySQL Standard Edition (GPL)

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.

mysql>
```

7.3.1.2.3. Suppression des comptes anonymes

Le compte anonyme, s'il est utile pour réaliser les premiers tests, n'a aucun intérêt sur un serveur en production. Il est donc préférable de le supprimer :

```
# mysql -u root -p mysql
Enter password:
Reading TABLE information FOR completion of TABLE AND COLUMN names
You can turn off this feature TO get a quicker startup WITH -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1
Server version: 5.0.81 Mandriva Linux - MySQL Standard Edition (GPL)

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.

mysql> DELETE FROM user WHERE user="";
Query OK, 2 rows affected (0.00 sec)
```

7.3.1.3. Gestion des bases et des utilisateurs

7.3.1.3.1. Création/Suppression d'une base

L'administrateur du serveur doit créer des bases de données pour séparer les données de travail des différentes applications nécessitant une base de données :

```
# mysql -u root -p mysql
Enter password:
Reading TABLE information FOR completion of TABLE AND COLUMN names
You can turn off this feature TO get a quicker startup WITH -A

Welcome TO the MySQL monitor.  Commands end WITH ; OR \g.
Your MySQL connection id IS 822 TO server version: 5.0.23-log

Type 'help;' OR '\h' FOR help. Type '\c' TO clear the buffer.

mysql> CREATE DATABASE MaBase;
Query OK, 1 row affected (0.00 sec)
mysql> SHOW DATABASES;
+----------+
| DATABASE |
+----------+
| MaBase   |
| mysql    |
| test     |
| tmp      |
+----------+
4 rows IN SET (0.00 sec)
```

Cette base sera détruite par la commande suivante :

```
mysql> DROP DATABASE MaBase;
Query OK, 0 rows affected (0.00 sec)

mysql> SHOW DATABASES;
+----------+
| DATABASE |
+----------+
| mysql    |
| test     |
| tmp      |
+----------+
3 rows IN SET (0.00 sec)
```

7.3.1.3.2. Ajout et suppression d'utilisateurs

Comme il est utile de séparer les données dans des bases, il est important de séparer les droits d'accès à ces données. Il suffit de créer des utilisateurs avec les droits nécessaires (administrateur de la base en question, utilisateur avec accès en lecture, ou autre) :

```
mysql> GRANT ALL ON MaBase.* TO 'MonAdmin'@'localhost' IDENTIFIED BY
 'motdepasse' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SELECT,INSERT,UPDATE,DELETE ON MaBase.* TO
 'MonUser'@'localhost' IDENTIFIED BY 'motdepasse';
Query OK, 0 rows affected (0.00 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
mysql> SELECT host,user,password FROM user;
+-----------+----------+-------------------+
| host      | user     | password          |
+-----------+----------+-------------------+
| localhost | root     | 4b9d71ac52feb410 |
| MES5      | root     | 4b9d71ac52feb410 |
| localhost | MonAdmin | 614e5cb70bb87e92 |
| localhost | MonUser  | 614e5cb70bb87e92 |
+-----------+----------+-------------------+
4 rows IN SET (0.00 sec)
mysql> SELECT * FROM db;
+-----------+---------+----------+-------------+-------------+-------------+-------
| Host      | Db      | User     | Select_priv | Insert_priv | Update_priv | Delete
+-----------+---------+----------+-------------+-------------+-------------+-------
| %         | test    |          | Y           | Y           | Y           | Y
| %         | test\_% |          | Y           | Y           | Y           | Y
| localhost | MaBase  | MonAdmin | Y           | Y           | Y           | Y
| localhost | MaBase  | MonUser  | Y           | Y           | Y           | Y
+-----------+---------+----------+-------------+-------------+-------------+-------
4 rows IN SET (0.00 sec)
```

On retrouve les utilisateurs créés et les droits qui leur sont associés sur la ou les bases concernées.

La suppression d'un utilisateur se fait à travers les commandes suivantes :

```
mysql> REVOKE ALL ON MaBase.* FROM MonUser@localhost;
Query OK, 0 rows affected (0.00 sec)

mysql> DROP user MonUser@localhost;
Query OK, 0 rows affected (0.00 sec)
```

Il faut d'abord annuler (*revoke*) les privilèges d'un utilisateur avant de le supprimer (*drop*).

7.3.1.3.3. Insertion de données dans les bases

La plupart des logiciels incluent un fichier qui contient le schéma de la base de données et les quelques données nécessaires à la mise en route du logiciel en question. Ce fichier est en fait une succession des commandes SQL que l'administrateur devrait passer pour créer le contenu de la base. L'administrateur passera une commande proche de celle-ci, après avoir créé la base et l'utilisateur correspondants :

```
# mysql -u MonAdmin -p MaBase < monFichier.sql
Enter password:
```

7.3.1.4. Arborescence du serveur MySQL

7.3.1.4.1. Stockage des données MySQL

L'ensemble des bases de données et des fichiers journaux sont stockés dans un répertoire spécifié par la variable `datadir` :

```
mysql> SHOW VARIABLES LIKE 'datadir';
+---------------+-----------------+
| Variable_name | Value           |
+---------------+-----------------+
| datadir       | /var/lib/mysql/ |
+---------------+-----------------+
1 row IN SET (0.00 sec)
```

7.3.1.4.2. Configuration du server ou des clients locaux

Le serveur, comme les clients, peut se passer d'un fichier de configuration, et peut démarrer avec des valeurs par défaut. Néanmoins, au cours de la vie du serveur, l'administrateur de la base de données pourra adapter certaines variables pour optimiser les performances. Plutôt que d'avoir à modifier ces variables lors d'un éventuel redémarrage du serveur, le fichier de configuration permet de stocker ces valeurs, et les reprendre au lancement du serveur. De même, on pourra stocker des informations nécessaires aux clients locaux.

Ce fichier s'appelle `my.cnf`.

MySQL cherche les fichiers suivants lors de son démarrage :

- `/etc/my.cnf` : abrite les options globales ;
- `datadir/my.cnf` : contient les options spécifiques au serveur ;

- `defaults-extra-file` : c'est le fichier spécifié par –defaults-extra-file=# ;
- `~/.my.cnf` : contient les options spécifiques à l'utilisateur.

7.3.1.4.3. Journaux et bases de données

Dans le répertoire `datadir`, on retrouve les fichiers journaux, les sockets MySQL, ainsi que les répertoires contenant les bases de données MySQL/MyISAM elles-mêmes :

```
# ll /var/lib/mysql
total 21068
-rw-rw----  1 mysql mysql 10485760 aoû 28 10:18 ibdata1
-rw-rw----  1 mysql mysql  5242880 aoû 28 10:18 ib_logfile0
-rw-rw----  1 mysql mysql  5242880 aoû 28 10:16 ib_logfile1
drwx--x--x  2 mysql mysql     4096 aoû 28 10:16 mysql/
-rw-rw----  1 mysql mysql    15151 aoû 28 10:16 mysql-bin.000001
-rw-rw----  1 mysql mysql   493595 aoû 28 10:16 mysql-bin.000002
-rw-rw----  1 mysql mysql    11925 aoû 28 10:16 mysql-bin.000003
-rw-rw----  1 mysql mysql      117 aoû 28 10:18 mysql-bin.000004
-rw-rw----  1 mysql mysql      422 aoû 28 10:18 mysql-bin.000005
-rw-rw----  1 mysql mysql       98 aoû 28 10:18 mysql-bin.000006
-rw-rw----  1 mysql mysql      114 aoû 28 10:18 mysql-bin.index
srwxrwxrwx  1 mysql mysql        0 aoû 28 10:18 mysqlmanager.sock=
srwxrwxrwx  1 mysql mysql        0 aoû 28 10:18 mysql.sock=
drwx--x--x  2 mysql mysql     4096 aoû  5 12:45 test/
drwx------  2 mysql mysql     4096 aoû 28 10:16 tmp/
```

En effet, on retrouve les bases `mysql`, `test` et `tmp`, ainsi qu'un fichier `ibdata1`, qui contient les tables utilisant un moteur de stockage InnoDB.

Les fichiers `mysql-bin.XXXXXX` contiennent les journaux (binaires) du serveur, permettant de rejouer toutes les opérations réalisées à partir d'un instant donné (après restauration d'une sauvegarde, par exemple).

7.3.1.5. Gestion du serveur

7.3.1.5.1. Sauvegarde ou restauration d'une base de données

La restauration d'une base de données correspond à très peu de choses à l'insertion de données dans une base de données. Il reste donc à savoir créer la sauvegarde. Une commande livrée avec MySQL réalise le travail : `mysqldump`.

```
# mysqldump --add-drop-table -u MonAdmin -p MaBase > monFichier.sql
Enter password:
# cat monFichier.sql
```

```
-- MySQL dump 10.9
--
-- Host: localhost    Database: MaBase
-- ------------------------------------------------------
-- Server version       4.1.12

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS,
 FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE,
 SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `test`
--

DROP TABLE IF EXISTS `test`;
CREATE TABLE `test` (
  `test` char(255) DEFAULT NULL
) ENGINE=MyISAM DEFAULT CHARSET=latin1;

--
-- Dumping data for table `test`
--


/*!40000 ALTER TABLE `test` DISABLE KEYS */;
LOCK TABLES `test` WRITE;
UNLOCK TABLES;
/*!40000 ALTER TABLE `test` ENABLE KEYS */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;
```

Afin de ne pas avoir besoin de purger complètement la base à restaurer, il faut faire une sauvegarde avec l'option `-add-drop-table`, ce qui ajoute l'ordre de détruire la table avant de la recréer (si elle existe), et ce **avant de réaliser la restauration**. Il suffit d'utiliser la commande vue plus haut (Section 7.3.1.3.3) de données dans une base de données pour restaurer la sauvegarde contenue dans le fichier `monFichier.sql`.

```
# mysql -u MonAdmin -p MaBase < monFichier.sql
Enter password:
```

La documentation MySQL fournit de plus amples renseignements sur la mise en place d'une sauvegarde, et son usage lors d'une restauration. L'utilisation des journaux binaires y est décrite.

7.3.1.5.2. Accéder aux informations du serveur

Pour activer, modifier et supprimer des fichiers journaux (pour déboguer), ou optimiser les performances du serveur en fonction de son utilisation actuelle, ou modifier le type de tables créé par défaut, il est nécessaire de connaître l'état et la configuration du serveur, et modifier cette dernière sans redémarrer le serveur.

Configuration du serveur

La configuration du serveur est accessible via la commande SQL suivante :

```
mysql> SHOW VARIABLES;
+---------------------------------+-------------------------------+
| Variable_name                   | Value                         |
+---------------------------------+-------------------------------+
| back_log                        | 50                            |
| basedir                         | /                             |
| bdb_cache_size                  | 8388600                       |
| bdb_home                        | /var/lib/mysql/               |
| bdb_log_buffer_size             | 32768                         |
| bdb_logdir                      |                               |
| bdb_max_lock                    | 10000                         |
| bdb_shared_data                 | OFF                           |
| bdb_tmpdir                      | /var/lib/mysql/.tmp/          |
| binlog_cache_size               | 32768                         |
...
```

La plupart de ces variables peuvent être configurées dans le fichier `/etc/my.cnf`, et seront donc prises en compte au démarrage du service. Néanmoins, il peut être nécessaire de modifier certaines d'entre elles durant la vie du serveur, sans forcément qu'un redémarrage du serveur soit nécessaire pour être prises en compte.

De plus, certaines valeurs peuvent être modifiées pour la session courante, ou pour l'ensemble des sessions (liste des variables).

Il est nécessaire d'avoir le privilèges `SUPER` pour modifier des variables `GLOBAL`. Par défaut, si `SESSION` ou `GLOBAL` ne sont pas spécifiées, il s'agit d'une modification de variable pour la session en cours.

```
mysql> SET sort_buffer_size=10000;
mysql> SET SESSION sort_buffer_size=10000;
mysql> SET GLOBAL sort_buffer_size=10000;
```

Pour pérenniser une modification, il est important de la reporter dans le fichier `/etc/my.cnf` afin que la valeur spécifiée à la volée soit de nouveau prise en compte.

État du serveur

Afin d'adapter les variables au cours de la vie du serveur, il est nécessaire de voir l'état d'un certain nombre d'indicateurs :

```
mysql> SHOW STATUS;
+--------------------------------+------------+
| Variable_name                  | Value      |
+--------------------------------+------------+
| Aborted_clients                | 436        |
| Aborted_connects               | 3          |
| Binlog_cache_disk_use          | 0          |
| Binlog_cache_use               | 0          |
| Bytes_received                 | 481501964  |
| Bytes_sent                     | 3913113658 |
| Com_admin_commands             | 877        |
...
```

L'étude de ces variables d'état impacte les variables à modifier dans le paragraphe précédent.

7.3.1.6. Dépannage

7.3.1.6.1. Perte du mot de passe de l'administrateur

Lorsque l'administrateur perd son mot de passe, il existe un moyen d'accéder au serveur après avoir désactiver la notion de privilèges afin de réinitialiser ce mot de passe.

Il s'agit de redémarrer le serveur avec l'option –skip-grant-tables, et de réaffecter un mot de passe.

```
# service mysqld stop
Shutting down MySQL: .                                     [  OK  ]
# mysqld --skip-grant-tables
mysqld: Can't create/write to file '/root/tmp/ibi2gyFL' (Errcode: 13)
090605 12:08:05  InnoDB: Error: unable to create temporary file; errno: 13
090605 12:08:05 [Warning] Can't open and lock time zone table:
Table 'mysql.time_zone_leap_second' doesn't exist trying to live without them
090605 12:08:05 [Note] mysqld: ready for connections.
Version: '5.0.81'  socket: '/var/lib/mysql/mysql.sock'  port: 0
Mandriva Linux - MySQL Standard Edition (GPL)
# mysql -u root mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1 to server version: 5.0.24-log

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
```

```
mysql> UPDATE user SET Password=PASSWORD('testor') WHERE User='root';
Query OK, 0 rows affected (0.01 sec)
Rows matched: 2  Changed: 0  Warnings: 0

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
# killall mysqld
# service mysqld start
Starting MySQL:                                                [  OK  ]
```

Les tests vérifient qu'il est bien nécessaire de s'authentifier, qu'un mot de passe quelconque n'est pas correct, et que finalement, le client se connecte correctement si le bon mot de passe est employé.

```
# mysql -u root mysql
ERROR 1045 (28000): Access denied for user 'root'@'localhost'
 (using password: NO)
# mysql -u root -p mysql
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost'
 (using password: YES)
# mysql -u root -p mysql
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4 to server version: 5.0.24-log

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

7.3.1.6.2. Autres

La documentation officielle MySQL (`http://dev.mysql.com/doc/refman/5.0/fr/problems.html`) reprend les principaux incidents qu'on peut identifier sur un tel service.

7.3.1.7. Modifier le mot de passe d'un compte

L'administrateur peut modifier le mot de passe d'un utilisateur par la commande suivante :

```
mysql> SET PASSWORD FOR 'myUser'@'localhost' = PASSWORD('motdepasse');
```

Un utilisateur peut modifier son propre mot de passe en omettant la clause `FOR` :

```
mysql> SET PASSWORD = PASSWORD('motdepasse');
```

7.3.1.8. Accéder à MySQL via le réseau

Par défaut, les serveurs MySQL sont installés sans permettre l'accès au serveur via le réseau (TCP). C'est un dispositif de sécurité lors de l'installation, le temps de mettre en place un mot de passe pour l'administrateur du serveur. Lorsqu'il est nécessaire de permettre l'accès à MySQL via le réseau, commentez la ligne `skip-networking` dans le fichier `/etc/my.cnf` et redémarrez le serveur.

7.3.1.9. Optimisation des tables

Pendant la vie d'une base de données, il arrive fréquemment qu'on supprime des données dans les tables. Si les données n'apparaissent plus à la lecture du contenu de la table concernée, l'espace disque utilisé par ces données n'en est pas pour autant libéré.

Pour cela, il est nécessaire de réorganiser l'espace occupé par la table. De même, cette opération de maintenance reconstruit les index pour faciliter l'accès aux informations.

En ligne de commande, la commande `myisamchk` réalise ce travail sur les tables de type MyISAM (`isamchk` pour les tables ISAM). Ce même outil sert aussi à analyser ou réparer les tables d'une base de données.

```
# myisamchk  --silent -a -r -S /var/lib/mysql/*/*.MYI
```

Il est possible de faire la même manipulation avec une commande SQL. Notez que la table est verrouillée durant l'exécution de la commande :

```
mysql> \r test
Connection id:    488
Current DATABASE: test

mysql> CREATE TABLE `test` (   `test` char(255) DEFAULT NULL )
 ENGINE=MyISAM DEFAULT CHARSET=latin1;
Query OK, 0 rows affected (0.00 sec)

mysql> OPTIMIZE TABLE test;
+-----------+----------+----------+----------------------------+
| TABLE     | Op       | Msg_type | Msg_text                   |
+-----------+----------+----------+----------------------------+
| test.test | OPTIMIZE | STATUS   | TABLE IS already up TO date |
+-----------+----------+----------+----------------------------+
1 row IN SET (0.00 sec)
```

Si la commande `myisamchk` prend tout son sens dans un script qui réalise cette intervention à intervalle régulier, la commande SQL possède l'avantage de laisser le serveur gérer les accès aux tables pour les optimisations. Avec `myisamchk`, vous devez vous en assurer vous-même.

7.3.2. Gérer un server de bases de données PostgreSQL

7.3.2.1. Concepts généraux et références Web

PostgreSQL est un système de gestion de bases de données relationnelles objet (ORDBMS) fondé sur POSTGRES, Version 4.2. Ce dernier a été développé à l'université de Californie au département des sciences informatiques de Berkeley. POSTGRES est à l'origine de nombreux concepts qui ne seront rendus disponibles au sein de systèmes de gestion de bases de données commerciales que bien plus tard.

PostgreSQL est un descendant libre du code original de Berkeley. Il supporte une grande partie du standard SQL tout en offrant de nombreuses fonctionnalités modernes :

- requêtes complexes ;
- clés étrangères ;
- déclencheurs (*triggers*) ;
- vues ;
- intégrité des transactions ;
- contrôle des accès concurrents (MVCC ou *MultiVersion Concurrency Control*).

De plus, PostgreSQL est extensible par l'utilisateur de plusieurs façons, en y ajoutant :

- de nouveaux types de données ;
- de nouvelles fonctions ;
- de nouveaux opérateurs ;
- de nouvelles fonctions d'agrégat ;
- de nouvelles méthodes d'indexage ;
- de nouveaux langages de procédure.

Et grâce à sa licence libre, PostgreSQL peut être utilisé, modifié et distribué librement, quelque soit le but visé, qu'il soit privé, commercial ou académique.

Principaux liens Web :

- site officiel PostgreSQL (`http://www.postgresql.org/`)
- documentation officielle (`http://www.postgresql.org/docs/manuals/`)
- documentation francophone (`http://docs.postgresql.fr/`)

7.3.2.2. Installation des paquets PostgreSQL

Mandriva Enterprise Server 5 fournit essentiellement 3 paquets :

- `postgresql8.3` : partie cliente de PostgreSQL ainsi que les commandes nécessaires pour manipuler les bases de données ;
- `postgresql8.3-contrib` : ensemble de contributions fournies dans les sources officielles PostgreSQL ;
- `postgresql8.3-server` : partie cliente de PostgreSQL ;

L'installation minimale consiste à installer les parties cliente et serveur de PostgreSQL.

7.3.2.3. Administration de base

7.3.2.3.1. 1er tour du propriétaire

S'il existe des outils Web ou graphiques pour se connecter à un serveur PostgreSQL, le paquetage fournit aussi tout le nécessaire pour administrer le serveur et les bases de données.

Immédiatement après l'installation, il n'existe que les bases indispensables au fonctionnement du serveur et l'administrateur du système.

```
# psql -U postgres
Mot de passe pour l'utilisateur postgres :
Bienvenue dans psql 8.1.4, l'interface interactive de PostgreSQL.

Tapez:  \copyright pour les termes de distribution
        \h pour l'aide-mémoire sur les commandes SQL
        \? pour l'aide-mémoire sur les commandes psql
        \g ou terminez avec un point-virgule pour exécuter une requête
        \q pour quitter

postgres=#postgres=# \l
     Liste des bases de données
    Nom    | Propriétaire | Encodage
-----------+--------------+----------
 postgres  | postgres     | LATIN9
 template0 | postgres     | LATIN9
 template1 | postgres     | LATIN9
(3 lignes)
postgres=# \c postgres
Vous êtes maintenant connecté à la base de données «postgres».
postgres=# \dt
Pas de relations trouvées.
postgres=# select * from pg_user;
 usename  | usesysid | usecreatedb | usesuper | usecatupd |  passwd  | valuntil | u
----------+----------+-------------+----------+-----------+----------+----------+--
```

```
 postgres |       10 | t           | t        | t         | ******** |          |
(1 ligne)

postgres=# select * from pg_shadow;
 usename  | usesysid | usecreatedb | usesuper | usecatupd |  passwd  | valuntil | u
----------+----------+-------------+----------+-----------+----------+----------+--
 postgres |       10 | t           | t        | t         |          |          |
(1 ligne)

postgres=# select * from pg_roles;
 rolname  | rolsuper | rolinherit | rolcreaterole | rolcreatedb | rolcatupdate | ro
----------+----------+------------+---------------+-------------+--------------+---
 postgres | t        | t          | t             | t           | t            | t
(1 ligne)
```

Les commandes `template1` et `template0` n'ont pas de caractère particulier en dehors du fait que `template1` est la base de données source par défaut pour la commande `CREATE DATABASE`. Par exemple, on pourrait supprimer `template1` et la recréer à partir de `template0` sans effet secondaire gênant. Ce procédé peut être utile lorsqu'on a encombré `template1` d'objets inutiles.

La base de données PostgreSQL est aussi créée quand le groupe est initialisé. Cette base de données est destinée à devenir celle par défaut pour la connexion des utilisateurs et applications. C'est une simple copie de `template1` et elle peut être supprimée et recréée, si nécessaire.

7.3.2.3.2. Mot de passe de l'administrateur

Le premier travail à réaliser est de spécifier un mot de passe pour le compte de l'administrateur.

```
# psql -U postgres
Mot de passe pour l'utilisateur postgres :
Bienvenue dans psql 8.1.4, l'interface interactive de PostgreSQL.

Tapez:  \copyright pour les termes de distribution
        \h pour l'aide-mémoire sur les commandes SQL
        \? pour l'aide-mémoire sur les commandes psql
        \g ou terminez avec un point-virgule pour exécuter une requête
        \q pour quitter

postgres=# ALTER ROLE postgres PASSWORD 'dfgdfg';
ALTER ROLE
postgres=# select * from pg_shadow;
 usename  | usesysid | usecreatedb | usesuper | usecatupd |               passwd
----------+----------+-------------+----------+-----------+-------------------------
 postgres |       10 | t           | t        | t         | md52bfd7fb3f9637b310a01
(1 ligne)
```

La documentation officielle de PostgreSQL préconise la création d'un rôle (*user*) qui dispose des droits `CREATEDB` et `CREATEROLE` mais qui n'est pas

un super-utilisateur, et d'utiliser ce rôle pour toute la gestion des bases de données et des rôles. Cette approche évite les dangers encourus en travaillant en tant que super-utilisateur pour des tâches qui ne nécessitent pas vraiment ces privilèges.

```
postgres=# CREATE ROLE admin CREATEDB CREATEROLE LOGIN PASSWORD 'admin';
CREATE ROLE
postgres=# select * from pg_shadow;
 usename  | usesysid | usecreatedb | usesuper | usecatupd |              passwd
----------+----------+-------------+----------+-----------+-------------------------
 postgres |       10 | t           | t        | t         | md52bfd7fb3f9637b310a01
 admin    |    16384 | t           | f        | f         | md5f6fdffe48c908deb0f4c
(2 lignes)

postgres=# select * from pg_roles;
 rolname  | rolsuper | rolinherit | rolcreaterole | rolcreatedb | rolcatupdate | ro
----------+----------+------------+---------------+-------------+--------------+---
 postgres | t        | t          | t             | t           | t            | t
 admin    | f        | t          | t             | t           | f            | t
(2 lignes)
```

Par défaut, PostgreSQL ne met en place aucun mécanisme d'authentification. Vous pouvez configurer cette authentification dans le fichier `PGDATA/pg_hba.conf` (ou `PGDATA` est égal à `/var/lib/pgsql/data` par défaut sous Mandriva Linux) :

```
# psql -U admin postgres
Bienvenue dans psql 8.1.4, l'interface interactive de PostgreSQL.

Tapez:  \copyright pour les termes de distribution
        \h pour l'aide-mémoire sur les commandes SQL
        \? pour l'aide-mémoire sur les commandes psql
        \g ou terminez avec un point-virgule pour exécuter une requête
        \q pour quitter

postgres=>

# cat /var/lib/pgsql/data/pg_hba.conf
# PostgreSQL Client Authentication Configuration File
# ===================================================
...
# TYPE  DATABASE    USER        CIDR-ADDRESS          METHOD

# "local" is for Unix domain socket connections only
local   all         all                               md5
# IPv4 local connections:
host    all         all         127.0.0.1/32          md5
# IPv6 local connections:
host    all         all         ::1/128               md5
# service postgresql restart
Stopping postgresql service:                                   [  OK  ]
Starting postgresql service:                                   [  OK  ]
# psql -U admin postgres
Mot de passe pour l'utilisateur admin :
```

```
Bienvenue dans psql 8.1.4, l'interface interactive de PostgreSQL.

Tapez:  \copyright pour les termes de distribution
        \h pour l'aide-mémoire sur les commandes SQL
        \? pour l'aide-mémoire sur les commandes psql
        \g ou terminez avec un point-virgule pour exécuter une requête
        \q pour quitter

postgres=>
```

7.3.2.4. Gestion des bases et des utilisateurs

7.3.2.4.1. Création et suppression d'une base

L'administrateur du serveur doit créer des bases de données pour séparer les données de travail des différentes applications nécessitant une base de données.

```
]# psql -U admin postgres
Mot de passe pour l'utilisateur admin :
Bienvenue dans psql 8.1.4, l'interface interactive de PostgreSQL.

Tapez:  \copyright pour les termes de distribution
        \h pour l'aide-mémoire sur les commandes SQL
        \? pour l'aide-mémoire sur les commandes psql
        \g ou terminez avec un point-virgule pour exécuter une requête
        \q pour quitter

postgres=> CREATE DATABASE test;
CREATE DATABASE
postgres=> \l
     Liste des bases de données
    Nom    | Propriétaire | Encodage
-----------+--------------+----------
 postgres  | postgres     | LATIN9
 template0 | postgres     | LATIN9
 template1 | postgres     | LATIN9
 test      | admin        | LATIN9
(4 lignes)
```

Cette base sera détruite par la commande suivante :

```
postgres=> DROP DATABASE test;
DROP DATABASE
postgres=> \l
     Liste des bases de données
    Nom    | Propriétaire | Encodage
-----------+--------------+----------
 postgres  | postgres     | LATIN9
 template0 | postgres     | LATIN9
```

```
 template1 | postgres     | LATIN9
(3 lignes)
```

7.3.2.4.2. Ajout et suppression d'utilisateurs

Comme il est utile de séparer les données dans des bases, il est important de séparer les droits d'accès à ces données. Il suffit de créer des utilisateurs avec les droits nécessaires (administrateur de la base en question, utilisateur avec accès en lecture, autre) :

```
# psql -U admin postgres
Mot de passe pour l'utilisateur admin :
Bienvenue dans psql 8.3.7, l'interface interactive de PostgreSQL.

Tapez:  \copyright pour les termes de distribution
        \h pour l'aide-mémoire sur les commandes SQL
        \? pour l'aide-mémoire sur les commandes psql
        \g ou terminez avec un point-virgule pour exécuter une requête
        \q pour quitter

postgres=> CREATE DATABASE test;
CREATE DATABASE
postgres=> \l
     Liste des bases de données
    Nom    | Propriétaire | Encodage
-----------+--------------+----------
 postgres  | postgres     | LATIN9
 template0 | postgres     | LATIN9
 template1 | postgres     | LATIN9
 test      | admin        | LATIN9
(4 lignes)
postgres=# CREATE USER monadmin PASSWORD 'motdepasse';
CREATE ROLE
postgres=# CREATE USER monuser PASSWORD 'motdepasse';
CREATE ROLE
postgres=# GRANT ALL ON DATABASE test TO monadmin WITH GRANT OPTION;
GRANT
postgres=# \c test monadmin
Mot de passe pour l'utilisateur monadmin :
Vous êtes maintenant connecté à la base de données «test» en tant
 qu'utilisateur «monadmin».
test=> GRANT ALL ON DATABASE test TO monuser;
GRANT
test=> \c test monuser
Mot de passe pour l'utilisateur monuser :
Vous êtes maintenant connecté à la base de données «test» en tant
 qu'utilisateur «monuser».
test=> CREATE TABLE matable ( test varchar(255) DEFAULT NULL );
CREATE TABLE
test=> \c postgres admin
Mot de passe pour l'utilisateur admin :
Vous êtes maintenant connecté à la base de données «postgres» en tant
 qu'utilisateur «admin».
```

```
postgres=> SELECT * FROM pg_user;
 usename  | usesysid | usecreatedb | usesuper | usecatupd |  passwd  | valuntil | u
----------+----------+-------------+----------+-----------+----------+----------+--
 postgres |       10 | t           | t        | t         | ******** |          |
 admin    |    16384 | t           | f        | f         | ******** |          |
 monadmin |    16416 | f           | f        | f         | ******** |          |
 monuser  |    16417 | f           | f        | f         | ******** |          |
(4 lignes)
```

On retrouve les utilisateurs créés et les droits qui leur sont associés sur la ou les bases concernées.

La suppression d'un utilisateur se fait via les commandes suivantes :

```
postgres=> REVOKE ALL ON DATABASE test FROM monuser;
REVOKE
postgres=> DROP ROLE monuser;
DROP ROLE
```

Il faut d'abord annuler (*revoke*) les privilèges d'un utilisateur et supprimer tous les objets dont il est propriétaire avant de le supprimer (*drop*).

7.3.2.4.3. Insertion de données dans les bases

La plupart des logiciels inclut un fichier qui contient le schéma de la base de données et les quelques données nécessaires à la mise en route du logiciel en question. Ce fichier est en fait une succession des commandes SQL que l'administrateur devrait passer pour créer le contenu de la base. L'administrateur passe une commande proche de celle-ci, après avoir créé la base appelée « test », et l'utilisateur correspondant `monuser` :

```
# psql -U monuser test < MyFile.sql
Mot de passe pour l'utilisateur monuser :
```

7.3.2.5. Administration au quotidien

7.3.2.5.1. Sauvegarde ou restauration d'une base de données

Une restauration de base de données correspond à très peu de choses à l'insertion de données dans une base de données. Il reste donc à savoir créer la sauvegarde. Une commande livrée avec PostgreSQL réalise le travail : `pg_dump`.

```
# pg_dump --clean -U postgres test
Mot de passe :
--
-- PostgreSQL database dump
```

```
--

SET client_encoding = 'LATIN9';
SET check_function_bodies = false;
SET client_min_messages = warning;

SET search_path = public, pg_catalog;

DROP TABLE public.products;
DROP SCHEMA public;
--
-- Name: public; Type: SCHEMA; Schema: -; Owner: postgres
--

CREATE SCHEMA public;


ALTER SCHEMA public OWNER TO postgres;

--
-- Name: SCHEMA public; Type: COMMENT; Schema: -; Owner: postgres
--

COMMENT ON SCHEMA public IS 'Standard public schema';


SET default_tablespace = '';

SET default_with_oids = false;

--
-- Name: products; Type: TABLE; Schema: public; Owner: postgres; Tablespace:
--

CREATE TABLE products (
    product_no integer,
    name text,
    price numeric
);


ALTER TABLE public.products OWNER TO postgres;

--
-- Data for Name: products; Type: TABLE DATA; Schema: public; Owner: postgres
--

COPY products (product_no, name, price) FROM stdin;
\.


--
-- Name: public; Type: ACL; Schema: -; Owner: postgres
--

REVOKE ALL ON SCHEMA public FROM PUBLIC;
```

```
REVOKE ALL ON SCHEMA public FROM postgres;
GRANT ALL ON SCHEMA public TO postgres;
GRANT ALL ON SCHEMA public TO PUBLIC;


--
-- PostgreSQL database dump complete
--
```

Lorsque votre base de données dépend des OID (par exemple en tant que clés étrangères), vous devez indiquer à `pg_dump` de sauvegarder aussi les OID. Pour cela, utilisez l'option `-o` sur la ligne de commande.

Il suffit d'utiliser la commande vue plus haut (Section 7.3.2.4.3) dans une base de données pour restaurer la sauvegarde contenue dans le fichier `monFichier.sql`.

```
# psql -U monuser test < MaSauvegarde.sql
Mot de passe pour l'utilisateur monuser :
```

La documentation de PostgreSQL fournit de plus amples renseignements sur la mise en place d'une sauvegarde, et son usage lors d'une restauration.

7.3.2.5.2. Accéder aux informations du serveur : configuration du serveur

Contenue dans le fichier `/var/lib/pgsql/data/postgresql.conf`, l'ensemble de la configuration du serveur est accessible via la commande SQL suivante :

```
postgres=> SHOW ALL;
              name       | setting |                  description
-------------------------+---------+-----------------------------------------------
 add_missing_from        | off     | Automatically adds missing TABLE REFERENCES TO
 archive_command         | unset   | WAL archiving command.
 australian_timezones    | off     | Interprets ACST, CST, EST, AND SAT AS Australia
 authentication_timeout | 60      | Sets the maximum time IN seconds TO complete cl
...

postgres=> SET timezone TO 'Europe/Paris';
SET
```

7.3.2.6. Description de l'arborescence de PostgreSQL

7.3.2.6.1. Stockage des données

Toutes les bases de données et les fichiers journaux sont stockés dans un répertoire spécifié par la variable `datadir` :

```
postgres=# SHOW data_directory;
   data_directory
---------------------
 /var/lib/pgsql/data
(1 ligne)
```

7.3.2.6.2. Configuration du server

Il existe deux fichiers de configuration principaux pour PostgreSQL :

- `postgresql.conf` : permet de définir l'ensemble des variables d'exécution du serveurs ;
- `pg_hba.conf` : permet de gérer les droits d'accès au serveur PostgreSQL.

PostgreSQL applique les valeurs données dans ces deux fichiers lors de son démarrage. Toute modification de ces fichiers nécessitent donc un redémarrage du serveur.

7.3.2.7. Configuration avancée

7.3.2.7.1. Modifier le mot de passe d'un compte

L'administrateur peut modifier le mot de passe d'un utilisateur par la commande suivante :

```
postgres=# ALTER ROLE monuser PASSWORD 'motdepasse';
ALTER ROLE
```

Un utilisateur peut modifier son propre mot de passe en omettant la clause `FOR` :

```
postgres=# \c test monuser
Mot de passe pour l'utilisateur monuser :
Vous êtes maintenant connecté à la base de données «test» en tant
 qu'utilisateur «monuser».
test=> ALTER role monuser password 'motdepasse';
ALTER ROLE
```

7.3.2.7.2. Optimisation

Pendant la vie d'une base de données, il arrive fréquemment qu'on supprime des données dans les tables. Si les données n'apparaissent plus à la lecture du contenu de la table concernée, l'espace disque utilisé par ces données n'en est pas pour autant libéré. Pour cela, il est nécessaire de réorganiser l'espace occupé par la table.

L'outil étant complexe, et l'optimisation des données étant un point clé des performances d'un système de gestion de bases de données, il est recommandé de lire la documentation au sujet de cet outil (`vacuum` (sql)/ `vacuumdb`).

La commande `vacuumdb` réalise ce travail en ligne de commande. Ce même outil sert aussi à analyser ou réparer les tables d'une base de données.

```
# vacuumdb -f -U postgres test
Mot de passe :
VACUUM
```

Il est possible de faire la même manipulation avec une commande SQL.

```
# psql -U postgres test
Mot de passe pour l'utilisateur postgres :
Bienvenue dans psql 8.1.4, l'interface interactive de PostgreSQL.

Tapez:  \copyright pour les termes de distribution
        \h pour l'aide-mémoire sur les commandes SQL
        \? pour l'aide-mémoire sur les commandes psql
        \g ou terminez avec un point-virgule pour exécuter une requête
        \q pour quitter

test=# VACUUM FULL products;
VACUUM
```

Chapitre 8. Stack Services

Gestion des services fournis dans Mandriva Enterprise Server 5

Tel que présenté dans le schéma des piles, Mandriva Enterprise Server 5 propose un certain nombre de services parmi les plus courants pour un serveur d'entreprise :

- services réseau standards : incluant un serveur de nom Bind, un serveur d'adresses IP dynamiques DHCP, et un serveur PXE (PXELinux) pour le déploiement de machines.
- services de partage de fichiers et d'imprimantes : un serveur d'impression (CUPS), un serveur de fichier et de domaine (Samba), et d'autres serveurs de fichiers (NFS, ProFTPD).
- services de messagerie : serveur SMTP (Postfix), serveur POP/IMAP (Cyrus-IMAP), et gestion du courrier indésirable et des virus.

Cette documentation présente un tour d'horizon de ces services et de leur gestion au quotidien dans un environnement Mandriva Enterprise Server 5.

8.1. Gestion des principaux services réseau

8.1.1. Gestion du serveur de noms avec BIND

Dans ce chapitre, nous allons présenter brièvement comment configurer les options générales du serveur de noms BIND, comment déclarer une nouvelle zone (nom de domaine) gérée par votre serveur DNS. Ce qui signifie que d'autres ordinateurs sur votre réseau, et peut-être d'Internet, pourront accéder aux services et aux ordinateurs sous vos noms de domaine.

8.1.1.1. Comment fonctionne un serveur DNS ?

Un serveur DNS permet d'associer une adresse IP a un nom et vice versa. Par exemple : `www.mandriva.com` (« nom ») est actuellement associé à `212.85.147.118` (« adresse »). Pour faire une analogie, un serveur de noms agit comme un répertoire téléphonique : vous fournissez un nom et il retourne un numéro vous permettant de rejoindre votre correspondant. Par contre, ce

mécanisme est transparent pour l'usager : il ne verra jamais l'adresse IP grâce au serveur DNS.

BIND (Berkeley Internet Name Domain) est l'implémentation du système DNS basé sur le RFC 1034/1035 (nom de domaine). BIND est composé de 3 parties principales :

- un espace hiérarchique de nom ;
- un serveur de nom contenant de l'information à propos de la hiérarchie du nom et de la configuration du domaine. Ce serveur est `named`.
- un résolveur, c'est-à-dire une gamme de routines de la bibliothèque C dont le but est de traduire des noms en adresse IP. Ces routines sont appelées par les services Internet comme ftp. Les résolveurs reçoivent de l'information de BIND directement. Mais vous pouvez aussi définir l'ordre de résolution. Cet ordre est défini dans le fichier `/etc/nsswitch.conf`. Les sources habituelles pour la résolution de noms sont le fichier `/etc/hosts` et le serveur DNS :

```
# cat
      /etc/nsswitch.conf ...  hosts: files nisplus nis dns
      ...
```

`files` est utilisé par `/etc/hosts`, et `dns` par BIND.

Il existe 3 types de serveur de nom :

Primary server (serveur primaire)

> Il s'agit de l'autorité concernant l'information qu'il fournit. Ce type de serveur peut déléguer son autorité pour des sous-domaines. Les serveurs primaires retournent l'information la plus à jour.

Secondary server (serveur secondaire)

> Il agit comme serveur de secours pour les résolveurs. Il contient la même information que le serveur primaire et il demande ces mises à jour au serveur primaire. Ce processus se nomme transfert de zone (*zone transfer*) et il utilise le protocole DNS NOTIFY, un mécanisme permettant au serveur maître d'informer ses subordonnés de changements aux zones.

Serveur cache

> Celui-ci ne conserve pas l'information localement. Il n'est pas autoritaire. Il demande au serveur primaire ou secondaire de résoudre ses requêtes et garde l'information en cache (antémémoire). Il est principalement utilisé pour réduire le trafic externe dans un réseau et ainsi réduire les besoins de bande passante Internet.

Pour en savoir plus sur BIND, nous vous recommandons fortement de lire BIND 9 Administrator Reference Manual (`http://www.bind9.net/manuals`) (en anglais), disponible localement dans le répertoire `/usr/share/doc/bind-doc` après avoir installé `bind-doc`. N'hésitez pas à consulter le site officiel de BIND (`http://www.bind9.net/`).

8.1.1.2. Installation de BIND et l'arborescence de BIND

L'installation de BIND est relativement simple, la configuration de base l'est aussi. Par contre, les configurations avancées peuvent devenir très complexe, c'est pourquoi nous en proposons seulement un survol.

8.1.1.2.1. Paquetages à installer et l'arborescence de BIND

Vous avez simplement besoin d'un paquetage : BIND. Il contient le serveur de noms et les outils pour établir la bonne configuration :

```
# urpmi bind
```

Par défaut, Mandriva Enterprise Server 5 fournit le serveur BIND en mode `chroot`. Cela signifie que les programmes de BIND sont redirigés vers un autre répertoire que celui d'origine. Il ne peut appeler de fichier à l'extérieur de ce répertoire. Il s'agit d'une façon pratique d'isoler une application en laquelle vous n'avez pas confiance et qui peut être dangereuse pour la sécurité du serveur.

Finalement, voici l'arborescence principale d'un serveur BIND. `/var/lib/named` est la racine pour le serveur de noms :

```
    /etc/init.d/named
    /var/lib/named/
|-- dev
|-- etc
|-- proc
     |-- xxx
`-- var
     |-- log
     |-- named
     |-- run
     `-- tmp
```

`/var/lib/named/etc` contient les fichiers de configuration principaux :

- `named.conf`: ce fichier est lu par le démon `named` au démarrage. Il contient le chemin pour obtenir tous les fichiers de données pour chaque domaines gérés, le type de serveur de noms pour chacun et la configuration générale du serveur de nom.

- `rndc.conf` et `rndc.key` : ces fichiers configurent le comportement de `rndc`, qui contrôle l'opération du serveur de nom. Il communique avec le serveur de noms sur une connexion TCP, envoyant des commandes signées numériquement.
- `named` : est le démon pour le serveur de nom BIND, qui écoute pour recevoir les requêtes.

Vous trouverez des fichiers de journalisation dans `/var/lib/named/var/log`. Par défaut, BIND offre une façon de conserver des informations dans des fichiers différents, selon les requêtes :

- `default.log` : information générale qui n'est pas classifiée dans d'autres fichiers journaux, comme les informations de démarrage et d'arrêt ;
- `notify.log` : protocole de notification concernant les changements dans les fichiers de données sur les serveurs maîtres. ;
- `query.log` : toutes les requêtes pour un serveur de noms ;
- `security.log` : approbation et rejet de requêtes ;
- `update.log` : journal des mises à jour dynamiques ;
- `xfer-in.log` : garde les requêtes de transfer de zone qu'un serveur de noms reçoit une fois activé ;
- `xfer-out.log` : requêtes de transfert de zone envoyées par le serveur de nom lorsqu'il est activé.

Vous pouvez ajouter différents fichiers en utilisant d'autres catégories, mais les principales ont été définies plus haut.

8.1.1.2.2. Gestion du service BIND

Vous pouvez utiliser la ligne de commande `service` qui fournit diverses options :

```
service named {start|stop|status|restart|reload}
```

start

: Lance le démon `named` en lisant la configuration générale et les informations de zone.

stop

: Arrête le démon `named`.

status

Cette commande offre de l'information intéressante concernant le serveur de nom : nombre de zone gérées, le niveau des fichiers de journalisation, de l'information sur les zones transférées, statut général de démon `named`.

```
# service named status
       number of zones: 4
       debug level: 0
       xfers running: 0
       xfers deferred: 0
       soa queries in progress: 0
       query logging is ON
       recursive clients: 0/1000
       tcp clients: 0/100
       server is up and running
```

reload

Ce paramètre ne redémarre pas BIND complètement. Il force la relecture des fichiers de zone. Utilisez cette commande lorsque vous appliquez des changements aux fichiers de zone.

8.1.1.3. Configuration avancée et dépannage

8.1.1.3.1. Comment résoudre les problèmes?

Si le service n'a pas démarré, consultez le fichier `/var/log/messages` pour lire le message de *debug* de BIND. Si vous ne trouvez pas l'erreur, utilisez `named-checkconf` et `named-checkzone` pour vérifier votre configuration :

`named-checkconf`

Cette commande permet de vérifier `named.conf` pour y trouver les erreurs de syntaxe :

```
# named-checkconf -t /var/lib/named /etc/named.conf
/etc/named.conf:101: zone '0.0.127.in-addr.arpa': type not
present
```

Vous devez utilisez l'option `-t` pour spécifier le répertoire chroot.

`named-checkzone`

Cette commande vous permet de vérifier les fichiers de zone et y identifier des erreurs de syntaxe :

```
# named-checkzone
       local /var/lib/named/var/named/reverse/named.local zone
       local/IN: loaded serial 1997022700 OK
```

Le premier paramètre identifie la zone vérifiée dans `named.conf`. Le second est le fichier de zone.

Avec le paquetage `bind-utils`, vous pouvez utiliser plusieurs outils et particulièrement, la commande `dig` pour effectuer des requêtes sur le serveur DNS. Par exemple, pour interroger votre serveur concernant `machine2.mydomain.test` passez la commande suivante :

```
$ dig machine2.mydomain.test @127.0.0.1
; <<>> DiG 9.2.3 <section<>> machine2.mydomain.test @127.0.0.1
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3287
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;machine2.mydomain.test.        IN    A

;; ANSWER SECTION:
machine2.mydomain.test. 38400   IN    A    192.168.1.12

;; AUTHORITY SECTION:
mydomain.test.          38400   IN    NS   mycomputer.mydomain.test.

;; Query time: 14 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Jan 23 14:11:10 2004
;; MSG SIZE  rcvd: 81>
```

8.1.1.3.2. Entrées SOA

Les entrées SOA (*Start Of Authority*) définissent les paramètres globaux pour une zone. Il peut être essentiel de l'optimiser, particulièrement si vous gérer des serveurs secondaires (*slaves*). En voici un exemple :

```
$TTL 3360
$ORIGIN domain.test.
@       IN      SOA             ns1.domain.test.  admin.domain.test.       (
 2005072801; serial number
 6H;  refresh
 2H;  update retry
```

```
     1W;  expiry
     24H;  minimum
    )

 TXT                    "My test domain"


 IN      NS             ns1.linuxeries.org.
 IN      NS             ns6.gandi.net.
```

La syntaxe générale est :

```
name ttl class
   rr name-server email-addr (sn ref ret ex min)
```

Expliquons les paramètres principaux et comment les optimiser :

`$TTL`

La valeur TTL (*Time To Live*) détermine la durée en seconde qu'une entrée peut rester en mémoire cache. Elle est utilisée principalement pour gérer des serveurs secondaires.

`$ORIGIN`

ORIGIN définit une valeur de base de laquelle les substitutions pour des domaines non qualifiés sont réalisées au moment de traiter les fichiers de zone. Si cette valeur n'est pas définie, elle sera remplacée par la valeur de `named.conf`. `@` doit être remplacé par la dernière valeur de $ORIGIN dans un fichier de zone.

`class`

Établit la classe d'une entrée. Il prend maintenant la valeur IN (Internet).

`name-server`

C'est un serveur de nom qui répondra en tant qu'autorité pour le domaine. Il est spécifié avec son nom de domaine complet (*Fully Qualified Domain Name ou FQDN*) et se termine par un **point**.

`mail-addr`

L'adresse électronique de l'administrateur de la zone. Celui qui devrait être contacté en cas de problème. La syntaxe est :

`mailbox-name@domain.com. .`

`serial number`

Ce numéro de série doit être augmenté lors de chaque modification du fichier de zone. C'est une façon pour les serveurs secondaires d'identifier les changements et de recharger leur configuration. Il n'y a pas de règles établies pour le composer, mais la convention suggère une valeur de date ce qui en simplifie la lecture : `aaaammjjss`, aaaa = année, mm = mois et jj = jour, alors que ss = seconde. Grâce à la variable `seconde`, vous pouvez le changer plusieurs fois par jour.

`refresh`

Détermine la durée d'attente avant qu'un serveur secondaire recharge la configuration du serveur principal. Le RFC recommande entre 1200 et 43200 secondes.

`update retry`

Constitue la durée entre les tentatives de mise à jour lorsqu'un serveur secondaire tente de contacter le serveur principal, suite à l'expiration de REFRESS. Habituellement les valeurs sont entre 180 secondes à 900 secondes.

`expiry`

Les serveurs secondaires arrêterons de répondre aux requêtes pour cette zone lorsque cette valeur sera expirée et qu'ils n'aurons pas réussi à rejoindre le serveur principal. Le RFC suggère entre 1209600 et 2419200 secondes (2-4 semaines).

`minimum`

Il s'agit d'une durée négative de cache, ce qui signifie que la durée `ERREUR DE NOM = NXDOMAIN` sera conservée dans la mémoire cache.

Par défaut, les valeurs sont en secondes, mais vous pouvez utilisez : s ou S (secondes), m ou M (minutes), h ou H (heures), d ou D (journée), w ou W (semaines).

Le site Web dnsreport (`http://member.dnsstuff.com/pages/dnsreport.php`) propose de vérifier votre configuration DNS, surtout si vous avez un nom de domaine public. Entrez votre zone ou votre nom de domaine et consultez le rapport complet qui en résultera.

8.1.1.4. Gestion des informations de Bind dans un répertoire OpenLDAP

Mandriva Enterprise Server 5 a basé tous les services inclus sur des répertoires LDAP, dans la mesure du possible. BIND fait partie du lot. Vous devez par contre suivre les étapes suivantes pour conserver les données de BIND dans un répertoire LDAP :

1. Importez vos zones dans la branche `ou=dns` de LDAP, où les ACL (*Access Control List*) s'attendent à trouver les informations DNS.
2. Configurez `named.conf` pour l'utilisation de LDAP pour chaque zone importée.
3. Configurez les paramètres d'authentification LDAP dans `named.conf` (`ou=dns` est exclusivement lisible par un administrateur DNS ou de membres du groupe DNS READERS).

Afin de présenter ces étapes, nous allons utiliser l'exemple de zone suivant, basé sur le fichier `example.com.zone` :

```
$TTL
   86400 $ORIGIN example.com.  @ IN SOA
   aurelio.example.com. hostmaster.example.com. ( 1 ; serial number
   10800 ; refresh 3600 ; retry 604800 ; expires 86400 ) ; TTL @ IN NS
   aurelio.example.com.  @ IN MX 10 mail.example.com.

   gateway         IN      A       10.0.1.1
   dogs            IN      A       10.0.1.7
   mail            IN      A       10.0.1.8
   aurelio         IN      A       10.0.1.9

   dhcp010         IN      A       10.0.1.10
   dhcp011         IN      A       10.0.1.11

   ns1             IN      CNAME   aurelio
   kdc             IN      CNAME   dogs

   localhost       IN      A       127.0.0.1
```

8.1.1.4.1. Configuration de named.conf

Nous devons configurer `named.conf` pour qu'il consulte LDAP pour ces deux zones. Le fichier présenté plus bas est un exemple.

Souvenez-vous que named opère en mode chroot et qu'il n'utilise pas le fichier/`etc/hosts`, mais le sien à l'intérieur du chroot. Évitez également de faire des boucles : par exemple, n'utilisez pas un serveur de noms qui est dans la zone LDAP pour spécifier un serveur LDAP. En général, il est préférable d'utiliser des adresses IP plutôt que des noms dans `named.conf`.

```
options {
        directory "/var/named";
        allow-transfer { none; };
        notify no;
        allow-query { any; };
};

zone "." {
        type hint;
        file "named.ca";
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "named.local";
};

zone "example.com" {
        type master;
        database "ldap ldap://127.0.0.1/ou=dns,dc=example,dc=com??sub??
          !bindname=uid=DNS%20Reader%2c
ou=System%20Accounts%2cdc=example%2cdc=com,!x-bindpw=dnsreader 86400";
};

zone "1.0.10.in-addr.arpa" {
        type master;
        database "ldap ldap://127.0.0.1/ou=dns,dc=example,dc=com??sub??!
          bindname=uid=DNS%20Reader%2c
ou=System%20Accounts%2cdc=example%2cdc=com,!x-bindpw=dnsreader 86400";
};
...
```

Le paramètre `database` établit la base de données à utiliser pour le fichier de zone. Dans notre cas, c'est LDAP. L'URL paraît complexe, il suit le format générique du RFC 2255 :

```
ldap://server/basedn?attributes?scope?filter?extensions
```

Donc, si on veut spécifier une recherche dans un sous-répertoire de `ou=dns` sur `localhost`, sans filtre par défaut, attributs ou extensions, ce serait :

```
ldap://localhost?ou=dns,dc=example,dc=com??sub?
```

Notre DIT, par contre, requiert des recherches authentifiées sur `ou=dns`, on doit donc ajouter une extension. Les extensions se définissent par une liste de noms séparés par des virgules, possiblement précédés par « ! » ce qui indique un usage critique. Nous utiliserons bindname et x-bindpw (ce dernier, n'étant pas standard, doit être précédé par « x- »). L'URL se compose maintenant comme suit :

```
ldap://localhost?ou=dns,dc=example,dc=com??sub??!bindname=uid=DNS
    Reader, ou=System
    Accounts,dc=example,dc=com,!x-bindpw=dnsreader
```

Comme les extensions sont séparées par des virgules, nous devons séparer les virgules dans binddn. Nous devons également annoncer les espaces. Nous accomplissons ceci en utilisant la syntaxe d'encodage standard des URL. Dans notre cas, l'URL devient finalement :

```
ldap://localhost/ou=dns,dc=example,dc=com??sub??!bindname=uid=DNS%20Reader%2c
    ou=System%20Accounts%2cdc=example%2cdc=com,!x-bindpw=dnsreader
```

Soyez prudent car `/etc/named.conf` doit être en mode `0640`, usager `root:named` car il contient maintenant 2 secrets : la clé rndc et les crédits LDAP utilisés pour lier le répertoire (grâce à la clé rndc, il devrait déjà avoir ces permissions, mais vérifiez quand même).

8.1.1.4.2. Ajout d'information dans le répertoire LDAP

Après avoir préparé votre arborescence avec le script `mandriva-setup.sh`, vous pouvez insérer ces fichiers de zone dans LDAP à `ou=dns` (en utilisant les droits DNS Admin).

Vous pouvez utiliser l'outil `zonetoldap` fourni par le paquetage `bind`. Il analyse les fichiers de zone DNS en format `BIND 9`, et charge le contenu dans un répertoire LDAP. Si la zone existe déjà, `zonetoldap` sortira avec succès. Si la zone n'existe pas ou partiellement, `zonetoldap` tente d'ajouter ou de compléter l'information de zone.

L'entrée SRV doit être placée en commentaire car `zonetoldap` ne peut la gérer pour l'instant. Nous l'ajouterons manuellement plus tard.

```
$ zonetoldap -D 'uid=DNS
   Admin,ou=System Accounts,dc=example,dc=com' -W \ -b
   ou=dns,dc=example,dc=com -z example.com -f example.com.zone -h
   localhost -c Enter LDAP Password: secretpass
```

Cette opération produit les entrées suivantes sous `ou=dns,dc=example,dc=com` :

```
dc=com
    dc=example
    relativeDomainName=ns1+zoneName=example.com
    relativeDomainName=mail+zoneName=example.com
    relativeDomainName=localhost+zoneName=example.com
    relativeDomainName=kdc+zoneName=example.com
    relativeDomainName=gateway+zoneName=example.com
    relativeDomainName=dogs+zoneName=example.com
    relativeDomainName=dhcp011+zoneName=example.com
    relativeDomainName=dhcp010+zoneName=example.com
    relativeDomainName=aurelio+zoneName=example.com
    relativeDomainName=@+zoneName=example.com
```

Nous devons encore ajouter l'entrée SRV que nous avons précédemment mise en commentaire. Utilisez la commande LDIF suivante :

```
dn: relativeDomainName=_kerberos._udp+zoneName=example.com,dc=example,
     dc=com,ou=dns,dc=example,dc=com
    objectClass: dNSZone
    relativeDomainName: _kerberos._udp
    zoneName: example.com
    SRVRecord: 0 0 88 dogs
```

Ajoutons-la :

```
$ ldapadd -x -D 'uid=DNS Admin,ou=System Accounts,dc=example,dc=com' \
    -W -f srv.ldif
    Enter LDAP Password: secretpass
    adding new entry "relativeDomainName=_kerberos._udp
      +zoneName=example.com,dc=example,dc=com,
    ou=dns,dc=example,dc=com"
```

Vous devriez toujours réviser les entrées produites par `zonetoldap`, car il pourrait y avoir d'autres conflits avec d'autres entrées.

8.1.1.5. Gestion d'un serveur DHCP

DHCP (*Dynamic Host Configuration Protocol*) est un protocole réseau permettant d'assigner dynamiquement des adresses IP ainsi que les configurations globales du réseau.

8.1.1.5.1. Fonctionnement d'un serveur DHCP

Le diagramme ci-dessous explique le premier dialogue entre un client demandant une adresse IP et un serveur DHCP. Il est important de bien le saisir car puisque tous ces types de paquet apparaîtront dans les fichiers de journalisation. En comprenant leur contenu, vous pourrez mieux identifier une configuration problématique.

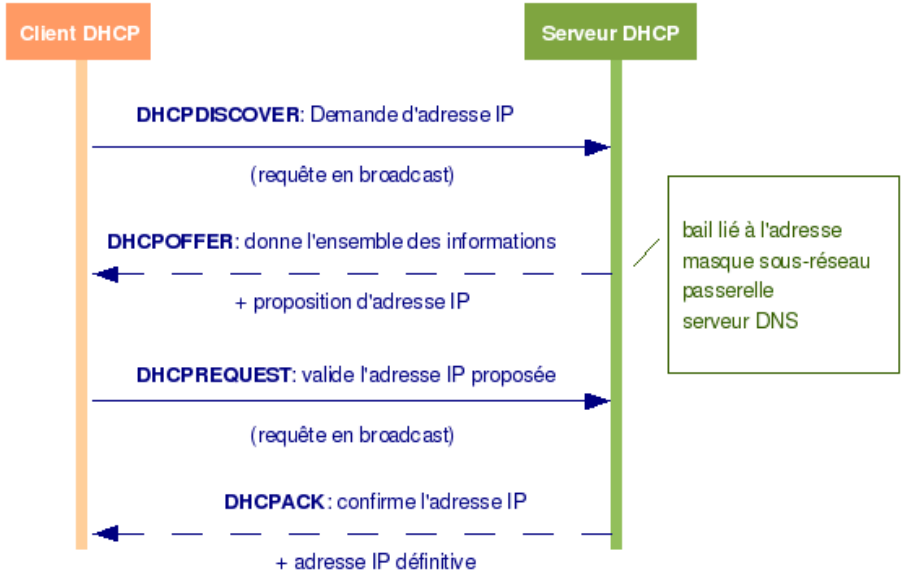


Figure 8-1. Fonctionnement d'un serveur DHCP

Il s'agit d'un dialogue de base et il pourrait être beaucoup plus long (lorsqu'une adresse IP est refusée, par exemple).

Un autre raison pour générer un dialogue entre un client et un serveur DHCP est la gestion de la réservation. Un serveur DHCP utilise des adresses IP selon des réservations : les adresses IP sont réservées pour une période déterminée pour optimiser les ressources du réseau. Vous trouverez donc des dialogues pour la gestion des réservations. Dès qu'une réservation est presque terminée, le client peut demander au serveur de la renouveler. Les clients utiliseront DHCPRESQUEST. Aussi, lorsque la réservation est presque terminée, le serveur peut envoyer une requête DHCPNAK indiquant l'expiration de la réservation et proposant le renouvellement. Si le serveur ne reçoit pas de réponse, l'adresse deviendra à nouveau disponible pour d'autres requêtes. La gestion des réservations est un des points clés pour optimiser la gestion des requêtes DHCP.

8.1.1.5.2. Installation et configuration du serveur DHCP

8.1.1.5.2.1. Installation des paquetages et arborescence DHCP

L'installation d'un serveur DHCP est relativement facile. Vous devez installer le paquetage `dhcp-server`. Vous devrez également installer `dhcp-common`. Ce dernier contient principalement de la documentation et des répertoires pour les fichiers de réservation.

```
# urpmi dhcp-server
```

L'arborescence DHCP est également simple :

- `/etc/dhcpd.conf.sample` : exemple de configuration d'un serveur DHCP. Vous pouvez l'utiliser comme modèle également. Si c'est votre choix, le fichier final devra se nommer `/etc/dhcp.conf`.
- `/etc/rc.d/init.d/dhcpd` : script pour gérer le démon DHCP.
- `/etc/sysconfig/dhcpd` : contient les paramètres qui doivent être ajoutés au serveur DHCP au démarrage.
- `/usr/sbin/dhcpd` : démon du serveur DHCP.
- `/usr/sbin/dhcpd-chroot.sh` : script permettant de faire tourner le serveur DHCP en mode chroot.
- `/usr/sbin/dhcpd-conf-to-ldap.pl` : script permettant d'inclure les informations de DHCP dans un répertoire LDAP
- `/usr/sbin/dhcpreport.pl` : script permettant d'afficher de l'information à propos des données du serveur DHCP.
- `/var/lib/dhcp/dhcpd.leases`: base de données qui entrepose les données de réservation.

8.1.1.5.2.2. Configuration du serveur DHCP

La configuration d'un serveur DHCP consiste principalement à écrire le fichier `/etc/dhcpd.conf`.

8.1.1.5.2.2.1. Paramètres généraux

Voici les paramètres les plus communs :

`ddns-update-style`

C'est un paramètre requis concernant le mise à jour automatique du DNS. Le serveur ne sera pas fonctionnel sans ce paramètre. Vous pouvez l'utilisez avec la valeur au minimum `none`.

`authoritative`

Ce paramètre est très important puisqu'il détermine si le serveur DHCP devrait envoyé des messages DHCP-NAK aux clients mal configurés. Si ce n'est pas fait, les clients seront incapables d'obtenir une adresse IP s'il change de sous-réseau jusqu'à ce que leur réservation précédente expire, ce qui peut être long dans certains cas. Aussi, si quelqu'un installe un serveur DHCP dans le même segment de réseau, il ne dérangera pas les dialogues avec les clients en envoyant des messages de DHCPNAK.

Vous pouvez aussi considérer comme des paramètres généraux toutes les options de réseau qui seront les mêmes pour tous les clients et réseau. Les déclarations d'option d'un serveur DHCP commencent toujours par le mot-clé `option`, suivi du nom de l'option et de ses données :

```
option <option_name> <data>
```

8.1.1.5.2.2.2. Déclaration de réseau et de client

Vous devez maintenant définir des clients ou des réseaux pour vos politiques DHCP. En voici un exemple :

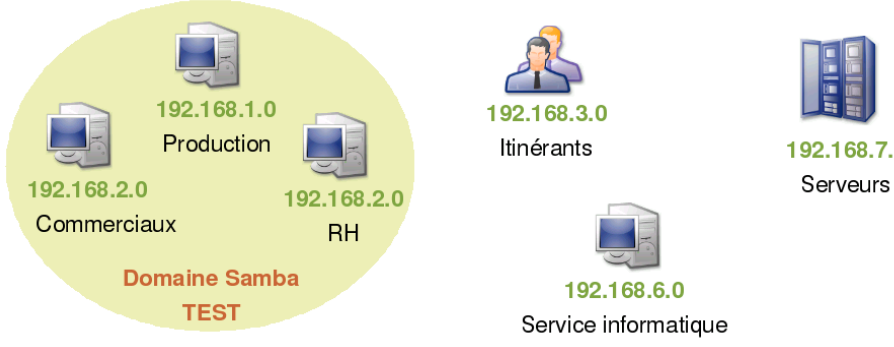


Figure 8-2. Application des déclarations pour une configuration DHCP pratique.

Nous avons 4 différents types de réseau :

- Samba domain : `commercial`, `HR` et `Production` appartiennent à ce domaine. La plupart des postes devraient avoir des IP réservées afin qu'elles conservent toujours la même. L'accès à Internet est réservé à `commercial` et `HR` en utilisant la même passerelle.
- Temporary users : ces usagers ont des droits minimum sur les ressources réseau. Ces postes auront des réservations très courtes et utilisent leur propre passerelle pour accéder à Internet.
- IT services: ces usagers ne font pas partie du domaine samba mais auront des adresses IP réservées. Ils utilisent leur propre passerelle.
- Servers : même description que IT services.

Le serveur DHCP permet de simplifier la configuration en utilisant des déclarations d'hôte et de réseau. Voici les principaux types de définition :

`host`

La déclaration `host` vous permet de fournir un adresse IP fixe pour un ordinateur, basée sur l'adresse MAC de sa carte réseau. Vous pouvez lui fournir une adresse et un nom.

```
host
  <non_fqdn> { option host-name "<fqdn>"; hardware
  ethernet <MAC_address>; fixed-address <IP_address>;
  }
```

`group`

La déclaration `group` permet de regrouper des déclarations d'hôtes et d'assigner des paramètres communs tels que le serveur DNS ou le serveur Netbios.

```
group <name> {
  <option_name> <data>;
  <option_name> <data>;
  ...

  host <non_fqdn> { ... }
  host <non_fqdn> { ... }
  ...
  }
```

`subnet`

La déclaration `subnet` permet de fournir une configuration spécifique pour l'adressage dynamique d'un réseau précis. Vous aurez à établir la plage d'IP fournies et les options réseau.

```
subnet <network_address> netmask <netmask_address> {
  <option_name> <data>;
  <option_name> <data>;
  ...
 range <ip_address_min> <ip_address_max>
  }
```

`pool`

La déclaration `pool` permet de fournir des paramètres spécifiques pour un sous-réseau dans une déclaration `subnet`.

```
subnet <network_address>
       netmask <netmask_address> { <option_name> <data>; ...
       pool { <option_name> <data>; range <ip_address_min>
       <ip_address_max> } ...  }
```

Utilisons les déclarations et les paramètres disponibles pour configurer le fichier du serveur DHCP de notre exemple :

```
# cat /etc/dhcpd.conf
ddns-update-style none;
authoritative;

# common network options
# common domain name server
option domain-name              "domain.tst";
# common domain name server IP address
option domain-name-servers      192.168.7.1;
# common ntp server
option ntp-servers  192.168.7.2;

# Define Samba Domain computers

group sambanet {
# gateway IP address
option routers   192.168.2.254;
# netbios server IP address
option  netbios-name-servers 192.168.2.253;
# do not allow clients that have no host declaration
# to get an IP address
deny unknown-clients;

host com1 {
# fully qualified hostname
option host-name "com1.domain.tst";
```

```
# MAC address
hardware ethernet 00:A0:78:8E:9E:AA;
# provided fix IP address
fixed-address 192.168.2.1;
}
...
host hr1 {
option host-name "hr1.domain.tst";
hardware ethernet 00:A0:78:8E:9E:AA;
fixed-address 192.168.2.10;
}
...
}

group sambalone {
option  netbios-name-servers 192.168.2.253;
deny unknown-clients;

host prod1 {
option host-name "prod1.domain.tst";
hardware ethernet 00:A0:78:8E:9E:AA;
fixed-address 192.168.1.1;
}
...
}

subnet 192.168.3.0 netmask 255.255.255.0 {
range 192.168.3.1 192.168.3.200;
allow unknown-clients;
option routers 192.168.3.254;
}

group IT {
option routers  192.168.6.254;
deny unknown-clients;

host it1 {
option host-name "it1.domain.tst";
hardware ethernet 00:A0:78:8E:9E:AA;
fixed-address 192.168.6.1;
}
...
}

group servers {
option routers  192.168.7.254;
deny unknown-clients;

host dns {
option host-name "dns.domain.tst";
hardware ethernet 00:A0:78:8E:9E:AA;
fixed-address 192.168.7.1;
}
...
}
```

La configuration du serveur DHCP vous permet d'utiliser plusieurs paramètres. Les pages de man de dhcpd.conf, dhcp-options et dhcpd.leases vous propose ces options avec des exemples.

8.1.1.5.2.3. Gestion du serveur DHCP

Vous pouvez gérer votre service DHCP avec le `dhcp initscript` afin de démarrer, arrêter ou redémarrer le démon. Utilisez la commande suivante :

```
service
    {start|stop|restart|status} dhcpd
```

Vous pouvez aussi spécifier la manière de démarrer le démon en utilisant le fichier `/etc/sysconfig/dhcpd`, celui-ci étant lu au démarrage du serveur. En voici les paramètres :

`INTERFACES`

Il peut déterminer sur quelle interface réseau écoute le `dhcpd`. Par défaut, `dhcpd` écoute sur toutes les interfaces.

`OPTIONS`

Vous pouvez ajouter plus d'options pour configurer votre démon :

- `-q` : évite l'affichage des informations de licence au démarrage (utilisé par défaut) ;
- `-p` : dicte le port sur lequel le serveur doit écouter pour recevoir les requêtes (par défaut 67). Cette option peut être utilisée pour configurer le serveur de relais DHCP ;
- `-d` : redirige tous les logs sur la sortie d'erreur standard,.

8.1.1.5.3. Gestion des données DHCP dans un répertoire OpenLDAP

Suivez ces étapes pour conserver vos données DHCP dans un répertoire OpenLDAP :

1. Importez les données de `/etc/dhcpd.conf` dans `ou=dhcp`.
2. Configurez `/etc/dhcpd.conf` pour qu'il utilise LDAP (avec ou sans authentification).

Veuillez également consulter le fichier `README.ldap` dans le répertoire de documentation de `dhcp-common` (`/usr/share/doc/dhcp-common/README.ldap`).

8.1.1.5.3.1. Configuration de `dhcpd.conf`

Vous pouvez maintenant retirer la majorité de la configuration de `/etc/dhcpd.conf`, laissant seulement la partie LDAP. En voici le résultat :

```
ldap-server "mes5.mandriva";
ldap-port 389;
ldap-username "uid=DHCP Reader,ou=System Accounts,dc=example,dc=com";
ldap-password "dhcpreader";
ldap-base-dn "ou=dhcp,dc=example,dc=com";
ldap-method dynamic;
```

Dans cet exemple, nous avons choisi d'utiliser des liens authentifiés, mais des recherches anonymes peuvent également être utilisées : retirez simplement `ldap-username` et `ldap-password`. Après ce changement, le serveur DHCP peut être démarré et il va consulter l'arborescence LDAP.

8.1.1.5.3.2. Importation des données dans le répertoire LDAP

Le paquetage `dhcp-common` inclut un script `contrib` pouvant servir à importer un `/etc/dhcpd.conf` existant dans LDAP : `/usr/sbin/dhcpd-conf-to-ldap.pl`.

Dans cet exemple, nous allons importer les configurations élémentaires suivantes :

```
ddns-update-style none;

     subnet 172.16.10.0 netmask 255.255.255.0 {
     option routers 172.16.10.1;
     option subnet-mask 255.255.255.0;

     option domain-name "example.com";

     option domain-name-servers 10.0.0.5;
     default-lease-time 21600;
     max-lease-time 43200;

     deny unknown-clients;

     host test009.example.com {
     hardware ethernet 00:C0:DF:02:93:71;
     fixed-address 172.16.10.5;
     }
     }
```

La commande ci-dessous crée le fichier LDIF correspondant au `dhcpd.conf` actuel. Notez également que ce script n'a pas encore été testé avec toutes les configurations possibles de DHCP. Consultez toujours le fichier LDIF.

```
$ perl /usr/sbin/dhcp-common-3.0.3/contrib/dhcpd-conf-to-ldap.pl \
     --basedn "ou=dhcp,dc=example,dc=com" \
     --dhcpdn "cn=DHCP Config,ou=dhcp,dc=example,dc=com" \
     --conf /etc/dhcpd.conf --server mes5.example.com --ldif dhcpd.ldif
     Creating LDAP Configuration with the following options:
     Base DN: ou=dhcp,dc=example,dc=com
     DHCP DN: cn=DHCP Config,ou=dhcp,dc=example,dc=com
     Server DN: cn=mes5.example.com, ou=dhcp,dc=example,dc=com

     Done.
```

Voici les options utilisées :

- basedn : la branche où seront conservés les informations DHCP ;
- dhcpdn : l'entrée contenant la configuration du serveur ;
- conf : le fichier `dhcpd.conf` qui sera migré vers LDAP ;
- server : le nom du serveur DHCP (devrait correspondre à la valeur de la commande `hostname`) ;
- ldif : le fichier `ldif`.

`dhcpd.ldif` contient maintenant les données que l'on veut importées. Vérifions :

```
dn: cn=mes5.example.com, ou=dhcp,dc=example,dc=com
cn: mes5.example.com
objectClass: top
objectClass: dhcpServer
dhcpServiceDN: cn=DHCP Config,ou=dhcp,dc=example,dc=com

dn: cn=DHCP Config,ou=dhcp,dc=example,dc=com
cn: DHCP Config
objectClass: top
objectClass: dhcpService
dhcpPrimaryDN: cn=mes5.example.com, ou=dhcp,dc=example,dc=com
dhcpStatements: ddns-update-style none
dn: cn=172.16.10.0, cn=DHCP Config,ou=dhcp,dc=example,dc=com
cn: 172.16.10.0
objectClass: top
objectClass: dhcpSubnet
objectClass: dhcpOptions
dhcpNetMask: 24
dhcpStatements: default-lease-time 21600
dhcpStatements: max-lease-time 43200
dhcpStatements: deny unknown-clients
```

```
dhcpOption: routers 172.16.10.1
dhcpOption: subnet-mask 255.255.255.0
dhcpOption: domain-name "example.com"
dhcpOption: domain-name-servers 10.0.0.5

dn: cn=test009.example.com, cn=172.16.10.0, cn=DHCP Config,ou=dhcp,
 dc=example,dc=com
cn: test009.example.com
objectClass: top
objectClass: dhcpHost
dhcpHWAddress: ethernet 00:c0:df:02:93:71
dhcpStatements: fixed-address 172.16.10.5
```

Ces données peuvent maintenant être importées. Nous allons utiliser le compte DHCP Admin pour cela :

```
$ ldapadd -x -D "uid=DHCP Admin,ou=System Accounts,dc=example,dc=com"
 -W -f dhcpd.ldif
Enter LDAP Password: secretpass
adding new entry "cn=mes5.example.com, ou=dhcp,dc=example,dc=com"

adding new entry "cn=DHCP Config,ou=dhcp,dc=example,dc=com"

adding new entry "cn=172.16.10.0, cn=DHCP Config,ou=dhcp,dc=example,
 dc=com"

adding new entry "cn=test009.example.com, cn=172.16.10.0, cn=DHCP
 Config,ou=dhcp,dc=example,dc=com"
```

8.2. Partage de fichiers et d'imprimantes

8.2.1. Partage d'imprimantes avec CUPS

Ce chapitre est basé sur la documentation officielle de CUPS.

CUPS (Common UNIX Printing System) est un système d'impression pour les systèmes UNIX®. Il fut développé par Easy Software Products pour faire la promotion d'une solution d'impression standard pour tous les fournisseurs et pour tous les utilisateurs de systèmes UNIX®.

8.2.1.1. Fonctionnement de CUPS

Lors de la première impression vers une file d'impression, CUPS crée une file d'attente pour suivre l'état de l'imprimante (OK, manque de papier, etc.) et des travaux d'impression. La plupart du temps, la file d'impression est associée à une imprimante branchée directement sur votre ordinateur par port USB ou port parallèle, mais CUPS peut aussi se connecter à une imprimante réseau. Quelque soit le type des imprimantes, les files d'impression CUPS associées s'afficheront comme les autres files d'impression déjà configurées (files LPD par exemple) dans les applications.

À chaque impression, CUPS crée un travail d'impression et le dirige vers la file d'impression demandée. Ce fichier contient le nom du document et les pages à imprimer. Les travaux sont numérotées (file-1, file-2, etc.) afin de permettre le suivi des travaux en cours d'impression, et éventuellement de les annuler. Lorsque CUPS reçoit un travail d'impression, il détermine le meilleur programme (filtres, pilotes d'imprimantes, moniteur de port, etc.) pour convertir les pages en format imprimable et les exécute ensuite pour imprimer le document.

Lorsque le travail d'impression est complètement imprimée, CUPS le retire de la file d'attente, et entame le travail suivant. Vous pouvez également être averti lorsqu'un travail est terminé ou en cas de problème.

CUPS utilise le protocole d'impression Internet Printing Protocol (IPP) pour gérer les travaux et les files d'impression. Les protocoles Line Printer Deamon (LPD), Server Message Block (SMB) et AppSocket (aussi appelé JetDirect) sont aussi supportés avec des fonctionnalités limitées.

Mandriva Enterprise Server 5 fournit CUPS 1.3.

Pour en savoir plus, consultez le site officiel de CUPS : http://cups.org/ (`http://cups.org/`)

8.2.1.2. Installation et arborescence de CUPS

Voici les paquetages dont vous aurez besoin pour profiter du serveur CUPS ainsi que les principaux fichiers `PPD` requis par la plupart des imprimantes.

- `cups` : fournit tous les fichiers serveur
- `cups-drivers` : contient les pilotes d'imprimantes à utiliser avec CUPS et les fichiers PPD appropriés.
- `hplip-hpijs-ppds` : fichiers PPD pour le pilote dimpression HPIJS
- `postscript-ppds` : contient les fichiers PPD pour les imprimantes PostScript

- `hplip`: un paquetage de pilotes HP pour fournir du support GNU/Linux pour la plupart des imprimantes Hewlett-Packard DeskJet, LaserJet, PSC, OfficeJet, et PhotoSmart, ainsi que les périphériques tout-en-un.

Décrivons l'arborescence de CUPS :

- `/etc/cups` : fichiers de configuration tels que `printers.conf`, annulés par la directive `ServerRoot` dans `cupsd.conf`.
- `/usr/include` : fichiers d'include pour le développement de nouveaux composants CUPS.
- `/usr/lib` : fichiers bibliothèques de CUPS.
- `/usr/lib/cups` : programmes serveur tels que `backends` et `filters`, annulés par la directive `ServerBin` dans `cupsd.conf`.
- `/usr/share/cups` : fichiers de données tels que des polices, annulés par la directive `DataDir` dans `cupsd.conf`.
- `/usr/share/cups/doc` : fichiers de documentation, annulés par la directive `DocumentRoot` dans `cupsd.conf`.
- `/usr/share/locale` : fichiers de traduction.
- `/var/cache/cups` : cache de données tels que `ppds.dat` et `remote.cache`, annulés par la directive `CacheDir` dans `cupsd.conf`.
- `/var/log/cups` : `access_log`, `error_log`, et `page_log`, annulés par les directives `AccessLog`, `ErrorLog`, `PageLog` dans `cupsd.conf`.
- `/var/run/cups` : Données d'état telles que les certificats d'authentification.
- `/var/spool/cups` : travaux d'impression mis dans la file d'attente, annulées par la directive `RequestRoot` dans `cupsd.conf`.

8.2.1.3. Configurer votre serveur CUPS

Vous pouvez configurer CUPS avec les fichiers de configuration ou l'interface Web. Nous recommandons l'interface Web pour les configurations de base et la gestion des files d'impression (ajout, modification, suppression) et l'édition des fichiers de configuration pour les tâches avancées, principalement pour la sécurité.

8.2.1.3.1. Utiliser l'interface Web de CUPS

Vous pouvez accéder à l'interface Web par HTTPS sur le port 631 : https://cups_server:631 (`https://cups_server:631`).

L'onglet Tâches permet de gérer les travaux d'impression. L'onglet Administration vous offrira une interface Web pour ajouter, modifier et supprimer des

imprimantes. Cliquez simplement sur Ajouter une imprimante ou Administrer les imprimantes.

CUPS est configuré par défaut pour afficher les imprimantes partagées par d'autres serveurs CUPS, et limiter l'accès au système et ses imprimantes. Les opérations d'administration demandent une authentification de base pour un membre du groupe `sys`. Les connexions sont acceptées via (`/var/run/cups/cups.sock`) ou "localhost" (127.0.0.1). Les utilisateurs n'ont pas les droits pour annuler des travaux qui ne leur appartiennent pas.

Vous pouvez changer ces paramètres dans l'onglet Administration dans la section Paramètres de base du serveur : cochez les options que vous voulez.

La section Serveur vous donne également accès aux fichiers journaux :

- Liste des accès et Liste des erreurs : les données d'accès et d'erreur de CUPS sont inscrites dans ces journaux.
- Liste des pages : ce fichier contient tous les accès à l'interface web de CUPS.

Ajoutons une nouvelle imprimante. CUPS permet la détection automatique. Si les imprimantes sont activées et branchées sur le réseau, CUPS devrait les détecter, et la liste New Printers Found apparaîtra. Cliquez sur Ajouter l'imprimante et remplissez les champs avec les informations relative à cette imprimante.

Votre imprimante n'est peut-être pas détectée par CUPS parce que vous n'avez pas le fichier PPD adéquat pour cette imprimante.

1. Dans l'onglet Administration cliquez sur Ajouter une imprimante.
2. Dans le premier écran, remplissez le champ Nom pour cette imprimante, et dans Lieu sa localisation physique.
3. Dans le second écran, choisissez dans la liste le périphérique pour accéder à votre imprimante.
4. Dans le troisième écran, remplissez l'URI pour accéder à votre imprimante.
5. Dans le dernier écran, l'interface vous demande de choisir une imprimante dans la liste. Comme vous ne pouvez la trouver, fournissons un fichier PPD pour l'imprimante. Vous le trouverez sur le CD de votre fabricant. Cliquez sur le bouton Parcourir et choisissez ce fichier dans l'arborescence.

Cette procédure n'est pas infaillible puisque certain fichiers PPD ne sont pas complétés adéquatement. Consultez http://linuxprinting.org (`http://linuxprinting.org`) pour vérifier la compatibilité de votre équipement.

Une fois que vos imprimantes sont ajoutées, vous pouvez modifier leur configuration. Cliquez sur Imprimantes. Choisissez l'imprimante en cliquant sur celle que vous désirez modifier. Vous verrez alors ce qui suit :

- Imprimer la page de test CUPS : Imprimer une page test pour l'imprimante configurée.
- Arrêter l'imprimante : arrêter complètement une imprimante.
- Rejeter les tâches : l'imprimante ne sera pas arrêtée, mais elle n'acceptera pas de nouvelles tâches.
- Transférer toutes les tâches : déplacer toutes les tâches vers une autre imprimante.
- Annuler toutes les tâches : annuler toutes les tâches pour cette imprimante.
- Cacher l'imprimante : cacher cette imprimante des utilisateurs.
- Modifier l'imprimante : modifier la configuration de l'imprimante, accès URI, pilotes, etc.
- Définir les options de l'imprimante : modifier les options d'impression tels que la résolution, taille de la page, bannière, etc.
- Supprimer l'imprimante : supprimer une imprimante complètement.
- Choisir par défault : définir en tant qu'imprimante par défaut pour les utilisateurs.
- Définir les autorisations : afficher les utilisateurs qui peuvent utiliser ou non cette imprimante.

8.2.1.3.2. Configuration avancée par l'édition des fichiers de configuration

Vous trouverez les fichiers de configuration dans `/etc/cups`. Le fichier `/etc/cups/client.conf` permet de définir la configuration du client CUPS. `/etc/cups/cupsd.conf` permet de définir la configuration du serveur CUPS.

Le `/etc/cups/cupsd.conf` contient les directives de configuration contrôlant le fonctionnement du serveur. Chaque directive est affichée sur une ligne et est suivie de sa valeur. Les commentaires sont introduit avec le dièse (« # ») au début de la ligne.

La syntaxe générale de `cupsd.conf` est comparable à celle de Apache. Vous pouvez spécifier des paramètres généraux en utilisant `<directive> <parametre>`.

Voyons les principales options de configuration :

`AuthType`

La directive AuthType définie le type d'authentification à utiliser :

- `None` : aucune authentification ne sera utilisée (default)
- `Basic` : l'authentification de base (Basic) sera appliquée en utilisant le mot de passe et les fichiers de groupe de UNIX®
- `Digest` : Le mode d'authentification Digest sera utilisé avec le fichier `/etc/cups/passwd.md5`
- `BasicDigest` : L'authentification de base sera appliquée en utilisant `/etc/cups/passwd.md5`

Lors de l'utilisation de mode d'authentification Basic, Digest, or BasicDigest, les clients se branchant par l'interface localhost peuvent également s'authentifier avec un certificat. La directive `AuthType` doit apparaître dans la section `Location` ou `Limit`.

`BrowseAddress`

La directive `BrowseAddress` spécifie une adresse où envoyer les informations nécessaires à la déclaration des imprimantes. Les clients CUPS peuvent alors recevoir automatiquement la liste des imprimantes disponibles sur le serveur. Plusieurs directives `BrowseAddress` peuvent être spécifiées pour l'envoi des informations sur plusieurs réseaux et systèmes.

La valeur `@LOCAL` permet envoyer les informations d'impression à toutes les interfaces locales. La valeur `@IF(name)` va envoyer les informations seulement à l'interface identifiée.

Par défaut, aucune information n'est envoyé.

`BrowseAllow`

La directive `BrowseAllow` spécifie un système ou un réseau en provenance desquels les informations de déclaration d'imprimante sont acceptées par le serveur CUPS. Par défaut toutes les informations reçues sont acceptées. La directive `HostNameLookups` doit être activée si vous utilisez des noms DNS en tant que valeur du paramètre `BrowseAllow`.

La validation des adresses IP supporte des concordances exactes, partielles qui correspondent à des réseaux en utilisant le masque réseau de 255.0.0.0, 255.255.0.0 et 255.255.255.0, ou des adresses réseau utilisant le masque réseau spécifié, ou encore des adresses au format CIDR (IP/MASK). `@LOCAL name` permet la consultation à partir de toutes les interfaces locales. `@IF(name)` ne permettra la consultation qu'à partir des interfaces identifiées.

Vous pouvez également avoir recours à la directive `BrowseDeny` pour refuser des informations. Sa syntaxe est identique à `BrowseAllow`.

`Browsing`

Cette directive détermine si la réception des données à propos de imprimantes disponibles sur le réseau est activé. Le valeur par défaut est `On` (activé). Cette directive n'active pas le partage des imprimantes locales à ce serveur CUPS. Pour cela vous devez également utiliser la directive `BrowseAddress` ou `BrowseProtocols` pour annoncer les imprimantes locales aux autres systèmes.

`DefaultShared`

Cette directive spécifie si les imprimantes sont partagées (publiées) par défaut. La valeur par défaut est `yes` (oui).

`JobRetryInterval`

`JobRetryInterval` indique le nombre de secondes à attendre entre les tentatives pour réessayer une tâche. Habituellement utilisée pour les fax, elle peut également être utilisée avec les imprimantes normales dont la politique d'erreur est `retry-job`. La valeur par défaut est 30 secondes.

CUPS vous permet d'établir les droits d'accès au serveur :

```
<Location />
Order Deny,Allow
Deny From All
Allow From 127.0.0.1
Allow From @LOCAL
</Location>
```

Dans cet exemple, nous permettons aux utilisateurs d'accéder à l'interface Web de CUPS à partir de localhost et lorsqu'ils sont dans le même réseau local. Avec cette méthode, vous pouvez configurer les droits d'administration.

`Location`

La directive `Location` spécifie le contrôle d'accès et les options d'authentification pour les ressources HTTP spécifiées. Les directives `Allow`, `AuthType`, `Deny`, `Encryption`, `Limit`, `LimitExcept`, `Order`, `Require`, et `Satisfy` peuvent toutes apparaître dans cette directive.

Voici les chemins des ressources HTTP les plus communes pour le serveur CUPS :

- `/` : le chemin pour toutes les opérations de type `get` (`get-printers`, `get-jobs`, etc.)

- `/admin`: le chemin pour toutes les opérations d'administration (`add-printer`, `delete-printer`, `start-printer`, etc.)
- `/admin/conf` : le chemin pour accéder aux fichiers de configuration de CUPS (`cupsd.conf`, `client.conf`, etc.)
- `/admin/log` : le chemin pour accéder aux journaux (`access_log`, `error_log`, `page_log`)
- `/classes` : le chemin pour toutes les classes d'imprimantes
- `/classes/nom` : la ressource pour la classe d'imprimantes s'appelant « nom »
- `/jobs` : le chemin pour toutes les opérations sur les tâches (`hold-job`, `release-job`, etc.)
- `/printers` : le chemin pour toutes les imprimantes
- `/printers/nom` : le chemin pour l'imprimante « nom »

Les ressources les plus spécifiques et précises sont prioritaires sur les moins spécifiques. Donc les directives placées dans `/printers/nom` sont prioritaires sur celles dans `/printers`. Les directives dans `/printers` seront prises en considération avant celles dans `/`. Aucune directive n'est héritée.

```
Allow
    <Location /path>
 ...
 Allow from All
 Allow from None
 Allow from *.domain.com
 Allow from .domain.com
 Allow from host.domain.com
 Allow from nnn.*
 Allow from nnn.nnn.*
 Allow from nnn.nnn.nnn.*
 Allow from nnn.nnn.nnn.nnn
 Allow from nnn.nnn.nnn.nnn/mm
 Allow from nnn.nnn.nnn.nnn/mmm.mmm.mmm.mmm
 Allow from xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
 Allow from @LOCAL
 Allow from @IF(name)
 </Location>
```

La directive `Allow` spécifie un nom d'hôte, une adresse IP, ou un réseau qui peut accéder au serveur. Les directives `Allow` sont cumulatives, donc plusieurs `Allow` peuvent être utilisées pour permettre l'accès à plusieurs hôtes ou réseaux. La notation `/mm` précise un masque de sous-réseau CIDR.

Le nom `@LOCAL` permettra l'accès à toutes les interfaces locales. Le nom `@IF(name)` limitera l'accès à l'interface nommée.

8.2.1.4. Sécuriser votre serveur CUPS

Dans la configuration autonome par défaut, il y a peu de risques de sécurité - le serveur CUPS n'accepte pas les connexions distantes, et accepte seulement les informations partagées à partir de son sous-réseau local. Lorsque vous partagez une imprimante ou activez l'administration distante, vous exposez potentiellement votre système à des accès non autorisés. Cette page fournit une analyse des problèmes potentiels de sécurité avec CUPS et décrit des stratégies pour améliorer la sécurité de votre serveur.

Enjeux de l'authentification

Lorsque vous activez l'administration distante, le serveur utilisera l'authentification de base pour les tâches d'administration. Le serveur CUPS supporte l'authentification en mode Basic, Digest et Local Certificate :

- L'authentification en mode de base (Basic) envoie les noms d'utilisateurs et mots de passe de manière lisible sur le réseau. Comme CUPS a recours au nom d'utilisateur et mot de passe du système, ces informations peuvent donc être lues, puis utilisées pour accéder au serveur et possiblement accéder à des comptes privilégiés.

  Il est donc recommandé d'activer le chiffrement pour cacher le nom d'utilisateur et le mot de passe - c'est l'option par défaut sur MacOS X et sur les systèmes GNU lorsque TLS ou OpenSSL sont installés.

- L'authentification Digest utilise le MD5 checksum du nom d'utilisateur, mot de passe et du domaine de CUPS, afin que le nom d'utilisateur et mot de passe original ne soient pas envoyés sur le réseau en texte clair.

  Vous devriez activer le chiffrement pour cacher l'information nom d'utilisateur et mot de passe.

- L'authentification par certificat local (local certificate authentication) envoie un certificat 128-bit permettant d'identifier un utilisateur authentifié. Les certificats sont créés à la volée au hasard et conservés dans des fichiers sous `/var/run/cups/certs`. Ils ont des permissions

de lecture : `root + lpadmin` pour les certificats root et `lp + lp` pour les certificats CGI. Comme les certificats ne sont disponibles que sur le système local, le serveur CUPS n'accepte pas d'authentification locale si le client n'est pas connecté à l'interface loopback (127.0.0.1) ou à la socket UNIX du serveur CUPS (*Unix domain socket*).

Assurez-vous que seuls les utilisateurs autorisés font parti du groupe lpadmin.

Attaque par déni de service

Lorsque le partage d'imprimante ou l'administration distante est activée, le serveur CUPS, comme tous les services Internet, est vulnérable face aux multiples attaques par déni de service possibles :

- Établir de multiples connexions au serveur jusqu'à ce que le serveur ne puisse plus répondre.

  Aucun logiciel ne permet de protéger votre serveur contre ce genre d'attaque. La directive `MaxClientsPerHost` peut être utilisée pour configurer CUPS afin qu'il limite le nombre de connexions permises à un même client, ce qui ne prévient pas une attaque distribuée.

  Vous devriez limiter l'accès aux clients et réseaux de confiance.

- Répéter des ouvertures et des fermetures de connexion au serveur le plus vite possible.

  Il n'y a pas de façon facile de se protéger contre ceci dans CUPS. Si l'attaque origine de l'extérieur du réseau, vous pourriez filtrer ce genre d'attaque. Cela dit, dès que le serveur reçoit une requête, il doit au moins l'ouvrir pour identifier son origine.

- Submerger le réseau avec des paquets de diffusion sur le port 631.

  Il est possible de désactiver la réception des données d'imprimante diffusées si CUPS détecte cette attaque. Par contre, si vous avez plusieurs imprimantes sur votre réseau, CUPS peut conclure qu'une attaque est en cours alors que des données valides sont reçues.

  Vous devriez bloquer les paquets de diffusion en provence de réseaux distants ou non autorisés avec à un routeur ou un pare-feu.

- Envoyer des requêtes IPP partielles, plus précisément, envoyer une partie de la valeur d'un attribut puis arrêter la transmission.

  La code actuel va attendre une seconde avant de faire expirer la valeur partielle reçue et fermer la connexion. Ceci va ralentir le temps de réponse du serveur pour les requêtes valides et peut même engendrer

des pertes de paquets de diffusion, mais n'aura pas d'autre impact significatif sur les opérations du serveur.

Vous devriez bloquer les paquets IPP en provence de réseaux distants ou non autorisés avec à un routeur ou un pare-feu.

- Envoyer de gros travaux d'impression aux imprimantes, empêchant les autres utilisateurs d'imprimer.

  Il y a peu de moyen de contrôler la taille des fichiers envoyés à l'impression, seulement l'attribut `MaxRequestSize`. Cependant, celui-ci ne vous protégera pas contre les utilisateurs abusifs et l'impression de centaines, voir de milliers de pages.

  Vous devriez restreindre l'accès aux hôtes ou réseaux connus, et ajouter un contrôle d'accès au niveau utilisateur pour les imprimantes haut de gamme.

Enjeux du chiffrement

CUPS supporte le chiffrement SSL 3.0 128-bit et TLS 1.0 des connexions réseau avec OpenSSL, GNU TLS et la bibliothèque de chiffrement CDSA. En plus des problèmes de sécurité potentiels posés par les protocoles TLS ou SSL, CUPS a les problèmes suivants :

Validation/révocation de certificat : actuellement, CUPS ne valide pas et ne révoque pas les certificats client ou serveur lors de l'établissement d'une connexion sécurisée. Cette situation peut permettre une attaque *man in the middle* ou des attaques basées sur le vol d'identité sur des réseaux non sécurisés. Les prochaines versions de CUPS supporteront la validation et la révocation de certificats.

Ne vous fiez pas au chiffrement lorsque vous vous connectez sur un serveur depuis Internet ou depuis un réseau non sécurisé.

8.2.1.5. Publication des imprimantes dans un annuaire LDAP.

CUPS permet de publier les imprimantes dans un annuaire LDAP afin de les ajouter en tant que nouvelles imprimantes. Comme plusieurs autres services, vous devrez indiquer à CUPS comment accéder à l'annuaire LDAP, dans `/etc/cups/cupsd.conf` :

BrowseLDAPBindDN

La directive `BrowseLDAPBindDN` spécifie le DN de l'utilisateur LDAP à utiliser pour se connecter à l'annuaire. La valeur par défaut n'est pas définie (*undefined*).

BrowseLDAPDN

La directive `BrowseLDAPDN` spécifie le DN du conteneur LDAP où sont enregistré les imprimantes partagées. La valeur par défaut n'est pas définie.

BrowseLDAPPassword

Cette directive spécifie le mot de passe pour accéder au serveur LDAP avec le compte défini par le paramètre BrowseLDAPBindDN. Par défaut, elle n'est pas définie.

BrowseLDAPServer

Cette directive indique le nom du serveur LDAP sur lequel se connecter. Par défaut, elle n'est pas définie.

Voici un exemple :

```
BrowseLocalProtocols ldap
BrowseRemoteProtocols ldap

BrowseLDAPServer localhost
BrowseLDAPDN ou=printers,dc=example,dc=com
BrowseLDAPBindDN uid=Manager,dc=example,dc=com
BrowseLDAPPassword password
```

8.2.2. Partager ses fichiers avec NFS

NFS permet d'exporter des répertoires complets, voire un système de fichiers, à travers le réseau, permettant ainsi le partage de fichiers entre utilisateurs. Ce type de partage est simple à mettre en place et est utilisé essentiellement avec les systèmes GNU/Linux et UNIX®. NFS n'est pas recommandé si vous avez de fortes contraintes de sécurité. L'utilisation de NFS est de toute façon à limiter à un réseau local.

8.2.2.1. Installer un serveur NFS

L'installation est simple et ne requiert que le paquetage `nfs-utils`.

8.2.2.2. Configurer un serveur NFS

La configuration des exportations de systèmes de fichiers NFS se fait dans le fichier `/etc/exports`. Il vous permet d'établir le mode d'accès aux données, les droits accordés aux utilisateurs et aux machines. Il est impératif de veiller à l'assignation de ces droits pour sécuriser l'accès aux données.

8.2.2.3. Utiliser NFS v4

Mandriva Enterprise Server 5 propose un serveur de type NFS v4. Cette nouvelle version apporte de fortes améliorations concernant la sécurité et les fonctionnalités :

- Ajout des états sur les fichiers concernant les verrouillages, la lecture et l'écriture, entre le client et le serveur.
- Base de baux pour le verrouillage des fichiers, permettant au client de récupérer la propriété du fichier pendant le temps du bail. Le client doit contacter le serveur pour éventuellement en étendre la durée.
- Ajout de composants de sécurité tels que Kerberos 5 et SPKM3.
- Extension du support des ACL fichiers, ajoutant notamment les noms de groupes et utilisateurs permettant ce type d'accès direct.
- Combinaison de plusieurs protocoles NFS permettant une meilleure gestion par les pare-feux.
- Support de la réplication.
- La capacité pour les clients de maintenir des sessions ou de les récupérer malgré un crash serveur ou une panne du réseau.
- Gestion d'un pseudo système de fichiers permettant de gérer tous les exports NFS à partir d'une même racine.

Voici une procédure vous permettant de mettre en oeuvre l'arborescence des exports NFS, avec la mise en place de Kerberos 5. Les pré-requis à cette configuration sont de disposer des paquetages NFS installés et d'un serveur Kerberos opérationnel.

1. Déclarer le pseudo système de fichiers dans `/etc/fstab`

   Il vous suffit d'ajouter les deux lignes suivantes :

   ```
   rpc_pipefs /var/lib/nfs/rpc_pipefs rpc_pipefs
         defaults 0 0 nfsd /proc/fs/nfsd nfsd defaults 0
         0
   ```

   Puis, comme pour un système de fichiers classique, montez-le :

   ```
   # mount rpc_pipesfs
   ```

2. Créer la racine de l'arborescence d'exports

   NFSv4 mettant à votre disposition un nouveau pseudo système de fichiers, tous les exports sont positionnés à partir d'une arborescence racine :

   ```
   /exports/
         |-- test1
         |-- ...
         `-- testn
   ```

   Pour la créer, il suffit de spécifier le paramètre `fsid=0` :

   ```
   # cat /etc/exports
    /export  *(rw,fsid=0,insecure,no_subtree_check,5)
   ```

3. Créer l'arborescence d'exports

   La suite de l'arborescence est alors plus classique :

   ```
   # cat /etc/exports
    /export  *(rw,fsid=0,insecure,no_subtree_check)
    /export/test1  *(rw,nohide,insecure,no_subtree_check)
    ...
   ```

   Le montage de la ressource se fait en relation à la racine NFS :

   ```
   # mount nfs4srv:/test1 /mnt/nfs
   ```

4. Utilisation de Kerberos

   Créez, dans un premier temps, un principal pour NFS. Créez également une clé pour le serveur et le client en utilisant le shell `kadmin` :

   ```
   kadmin.local:  addprinc -randkey nfs/nfs4srv.edge-it.subnet
   WARNING: no policy specified for nfs/nfs4srv.example.com@EXAMPLE.COM;
    defaulting to no policy
   Principal "nfs/nfs4srv.example.com@EXAMPLE.COM" created.

   kadmin.local:  ktadd  -e des-cbc-crc:normal nfs/nfs4srv.example.com
   Entry for principal nfs/nfs4srv.example.com with kvno 3, encryption
    type Triple DES cbc mode with HMAC/sha1 added to keytab
    WRFILE:/etc/krb5.keytab.
   Entry for principal nfsnfs4srv.example.com with kvno 3, encryption
    type DES cbc mode with CRC-32 added to keytab
    WRFILE:/etc/krb5.keytab.
   ```

   Copier le fichier `krb5.keytab` sur le serveur NFS et les clients utilisant NFSv4.

   Il reste alors à créer les exports utilisant `krb5`, au moyen d'un client spécifique, `gss/krb5`.

   ```
   # cat /etc/exports
   /export gss/krb5(rw,fsid=0,insecure,no_subtree_check,sync,5)
   ```

   Utilisez la commande mount avec l'option `sec=kbr5` :

   ```
   # mount -t nfs4 -o sec=krb5 nfs4srv:/ /nnt/nfs
   ```

8.2.3. Serveur de fichiers FTP

ProFTPD vous permet de créer et configurer un serveur FTP.

8.2.3.1. Installation et arborescence de ProFTPD

`proftpd` est le paquetage fournissant l'ensemble du serveur

L'arborescence fournie par `proftpd` est relativement simple :

- `/etc/proftpd.conf` : fichier de configuration de proFTPD
- `/etc/xinetd.d/proftpd-xinetd` : configuration du démon `proftpd` lancé via `xinetd` (à déconseiller)
- `/etc/rc.d/init.d/proftpd` : initscript de proFTPD configuré en mode autonome
- `/var/log/proftpd` : répertoire des fichiers de journalisation de proFTPD

8.2.3.2. La boîte à outils ProFTPD

Pour vérifier la syntaxe du fichier de configuration :

```
# proftpd -t
    Checking syntax of configuration file
    Syntax check complete.
```

Pour vérifier le bon fonctionnement du serveur :

```
# service proftpd status
    proftpd (pid 32445) est en cours d'exécution ...
    # telnet 192.168.40.52 21
    Trying 192.168.40.52...
    Connected to tellure.edge-it.subnet (192.168.40.52).
    Escape character is '^]'.
    220 ProFTPD 1.2.10 Server (ProFTPD Default Installation)
    [192.168.40.52]
```

On testera également une session complète en se connectant au serveur.

Le paquet `proftpd` installe, outre le démon serveur, un certain nombre de commandes qui peuvent s'avérer utiles pour suivre l'état du serveur.

ftpcount

Permet de compter le nombre de connexions au serveur ftp à un moment donné

```
$ ftpcount
Master proftpd process 32445:
Service class                      -   1 user
```

ftptop

Permet de visualiser en temps réel l'activité du serveur ftp et de ses connexions

```
ftptop/0.9: Thu Jan  5 11:54:49 2009, up for 1 min
1 Total FTP Sessions: 0 downloading, 0 uploading, 1 idle

PID   S USER     CLIENT               SERVER          TIME COMMAND
32455 I anne     test.domain.subne 0.0.0.0:21      0m47s  idle
```

ftpwho

Permet de visualiser à un moment donné les connexions actives au serveur et des informations concernant les sessions en cours.

```
$ ftpwho -v
standalone FTP daemon [32445], up for  2 hrs 18 min
  542 anne     [ 0m11s]  0m11s idle
        client: workstation.edge-it.subnet [192.168.40.140]
        server: 0.0.0.0:21 (ProFTPD Default Installation)
        location: /
Service class                      -   1 user
```

8.2.3.3. Sécuriser un serveur Proftpd

La sécurisation d'un serveur FTP passe en amont par la mise en place d'un coupe feu efficace. Hormis ce point, la sécurisation passe avant tout par la gestion des utilisateurs et la personnalisation de la configuration.

Ci-dessous un fichier de configuration type, que nous allons détailler par la suite :

```
# cat /etc/proftpd.conf
    ServerName                      "FTP SERVER"
ServerType                      standalone
DeferWelcome                    off
TransferLog                     /var/log/proftpd.xferlog
DefaultRoot                     ~
RequireValidShell               off
```

```
ServerIdent                     off
RootLogin       off

ShowSymlinks                    off
DefaultServer                   on
AllowOverwrite                  off

TimeoutNoTransfer               600
TimeoutStalled                  600
TimeoutIdle                     1200

DisplayLogin                    /etc/welcome.msg
DisplayFirstChdir               .message

DenyFilter                      \*.*/
Bind                            192.168.10.55
```

8.2.3.3.1. Gestion des utilisateurs

Une grande partie de la sécurisation d'un serveur FTP est liée à la gestion des utilisateurs, d'où des étapes indispensables.

Utilisateurs sans shell

Il est préférable de dédier les accès ftp à des utilisateurs sans shell qui seront créés de la manière suivante :

```
# useradd -s /bin/false user
```

ou en modification

```
# usermod -s /bin/false user
```

Pour autoriser l'accès au ftp pour des utilisateurs sans shell, on ajoute dans `/etc/proftpd.conf` :

```
RequireValidShell  on
```

Sessions utilisateurs en mode chroot

On emprisonne les utilisateurs dans un répertoire fixé, l'empêchant ainsi de remonter dans l'arborescence. Pour ce faire, on ajoute la ligne suivante dans `/etc/proftpd.conf` :

```
 DefaultRoot                    ~
```

Interdire l'accès du serveur ftp à root

Comme les mots de passe circulent en texte, on court le risque de voir le mot de passe de root récupéré. Pour ce faire, on ajoute la ligne suivante dans `/etc/proftpd.conf` :

```
RootLogin off
```

Interdire les connexions anonymes

C'est chose faite par défaut car la mise en place de cette fonctionnalité demande l'installation d'un paquetage supplémentaire (proftpd-anonymous).

Limiter les connexions à une liste donnée d'utilisateurs

La directive `Limit` permet de spécifier des utilisateurs et/ou des groupes autorisés ou non à se connecter.

```
<Limit LOGIN>
 AllowUser admin
 AllowGroups devels
 DenyAll
</Limit>
```

8.2.3.3.2. Sécuriser la configuration du serveur

Tous les points mentionnés ci-dessous sont relatifs à des modifications du fichier `/etc/proftpd.conf`.

proftpd n'utilise les privilèges root que lorsque cela s'avère nécessaire. Dans le cas contraire, il utilise l'identité définie dans la configuration. Les étapes nécessitant les privilèges root sont :

- accès aux ports inférieurs ou égaux à 1024
- détermination des limitations sur les ressources
- lecture des informations de configuration
- exécution de portions de code liées au réseau

Masquer la bannière

Il s'agit de ne pas afficher les informations concernant le type de serveur ftp et sa version.

```
ServerIdent                     off
```

Pour vérifier :

```
# telnet 192.168.40.52 21
 Trying 192.168.40.52...
 Connected to tellure.edge-it.subnet (192.168.40.52).
 Escape character is '^]'.
 220 192.168.40.52 FTP server ready
```

Modifier le port d'accès par défaut

Définir un port au-dessus du port 1024 (accessible à un utilisateur non root). On peut éventuellement prévoir une règle `iptables` pour rendre transparente la manipulation.

Modifier les messages par défaut

Le serveur proftpd renvoie un certain nombre de messages lors des différentes étapes d'une session ftp. Certains d'entre eux peuvent être modifiés pour communiquer avec l'utilisateur (rappel de règles de sécurité, droits et devoirs...) ou pour masquer des messages qui pourraient mettre en évidence un type de serveur et une version.

Voici la liste des directives correspondant à ces messages :

- `DisplayConnect <fichier>` : message affiché avant la procédure d'authentification
- `DisplayFirstChdir <fichier>` : message affiché lors du premier changement de répertoire
- `DisplayLogin <filename>` : message affiché lors du login
- `DisplayGoAway <filename>` : message affiché lors d'une connexion rejetée
- `DisplayQuit <filename>` : message affiché en fin de session ftp
- `ServerName <texte>` : chaîne affichée lors des messages de login

À ces directives, on peut ajouter `DeferWelcome` qui, lorsqu'il est activé, n'affiche le message de bienvenue que lorsque l'utilisateur est authentifié avec succès.

Établir des *timeouts*

Ils permettent d'éviter de maintenir ouvertes des connexions non utilisées. Il existe un certain nombre de niveaux sur lesquels on peut fixer des *timeouts* :

- `TimeoutNoTransfer <seconds>` : nombre maximum de secondes pendant lesquelles un client authentifié peut rester connecté inactif, (par défaut : 300)
- `TimeoutStalled <seconds>` : nombre maximum de secondes pendant lesquelles une connexion ftp peut rester dans l'état *stalled* (par défaut : 3600)
- `TimeoutIdle <seconds>` : nombre maximum de secondes pendant lesquelles une connexion FTP peut rester dans l'état inactif (*idle*) (par défaut : 600).

Contrôle des commandes passées par l'utilisateur

La directive `Limit` permet de lister précisément les commandes autorisées pour les utilisateurs du serveur ftp. Ces commandes peuvent être spécifiées une par une ou par une désignation de groupe de commandes.

Commandes individuelles

- `CWD` (Change Working Directory) : changement de répertoire
- `MKD` / `XMKD` (MaKe Directory) : création d'un répertoire
- `RNFR` (ReName FRom), `RNTO` (ReName TO) : renommage d'un répertoire
- `DELE` (DELEte) : destruction d'un fichier
- `RMD` / `XRMD` (ReMove Directory) : destruction d'un répertoire
- `RETR` (RETRieve) : transfert d'un fichier du serveur vers le client
- `STOR` (STORe) : transfert d'un fichier du client vers le serveur

Groupes de commandes

- `READ All FTP` : commandes concernant la lecture de fichiers (ne concerne pas le listage d'un répertoire) : `RETR`, `SITE`, `SIZE`, `STAT`
- `WRITE All FTP` : commandes concernant l'écriture, la création et la suppression d'un répertoire `APPE`, `DELE`, `MKD`, `RMD`, `RNTO`, `STOR`, `XMKD`, `XRMD`
- `DIRS All FTP` : commandes concernant l'affichage des fichiers des répertoires `CDUP`, `CWD`, `LIST`, `MDTM`, `NLST`, `PWD`, `RNFR`, `XCUP`, `XCWD`, `XPWD`

- `ALL ALL FTP` commande identiques à `READ WRITE DIRS`.

Exemple

Limiter les utilisateurs dans leurs commandes en leur retirant tous les droits de suppression de fichiers et de répertoires dans le dépôt ftp

```
<Limit RNFR DELE RMD>
 DenyAll
 </Limit>
```

Gestion des interfaces réseau

Dans le cas où la machine dispose de plusieurs interfaces et/ou de plusieurs adresses IP, il est conseillé de lier le serveur à une adresse unique.

```
Bind  192.168.10.55
```

Correction d'une faille de sécurité de ftp

La ligne ci-dessous permet de contrer une faille provoquée par la commande :

```
NLST /../*/../*/../*/../*/../*/../*/../*/../*/../*/../
DenyFilter  \*.*/
```

8.2.3.3.3. Personnaliser les règles d'accès aux fichiers en fonction des besoins

Proftpd donne la possibilité de préciser la configuration du serveur en fonction de contextes bien définis :

- des répertoires
- des virtualhosts (la notion dans proftpd est très semblable à celle que l'on retrouve dans Apache)

Prenons le cas de répertoires. Le dépôt ftp est situé dans `/var/lib/ftp` :

- `/var/lib/ftp/datas` : données de l'application accessibles en écriture pour les développeurs et en lecture pour les visiteurs
- `/var/lib/ftp/pub` : dépôt accessible pour tous les utilisateurs pour déposer des fichiers mais sans pouvoir effectuer de suppression

La configuration correspondante serait :

```
<Directory /var/lib/ftp/datas>
```

```
<Limit WRITE DIRS>
DenyGroup visiteurs
AllowGroup devels
</Limit>
</Directory>
<Directory /var/lib/ftp/pub>
<Limit ALL>
AllowGroup visiteurs devels
</Limit>
</Directory>
```

8.2.3.4. Utiliser l'authentification LDAP sur ProFTPD

Proftpd dispose, par défaut, d'un module permettant d'authentifier les utilisateurs du serveur ftp à partir d'un annuaire OpenLDAP.

La configuration est relativement simple. Nous partirons de la configuration suivante :

```
LDAPServer <adresse_ip_serveur_ldap> LDAPDNInfo
    "cn=Manager,dc=example,dc=com" "<password>" LDAPQueryTimeout 5
    LDAPDoAuth on "dc=example,dc=com" LDAPDoUIDLookups on
    "ou=Personnes,dc=example,dc=com" LDAPDoGIDLookups on
    "ou=Groupes,dc=example,dc=com" LDAPNegativeCache off
    LDAPHomedirOnDemand off LDAPDefaultAuthScheme MD5
```

La configuration s'appuie sur les paramètres spécifiant les données essentielles pour accéder au serveur LDAP et l'interroger :

LDAPDNInfo

Contient les informations de DN pour le contact initial à l'annuaire

LDAPQueryTimeout

Fixe le timeout sur les requêtes LDAP

LDAPDoAuth

Autorise l'authentification LDAP

LDAPDoUIDLookups

Fixe le GID par défaut à assigner aux utilisateurs quand l'attribut uidNumber n'est pas trouvé.

LDAPDoGIDLookups

Autorise la résolution LDAP pour les droits de groupe et GID pour la lecture des répertoires.

LDAPHomedirOnDemand

Force tous les utilisateurs authentifiés par LDAP à utiliser par défaut HomeDironDemand.

LDAPDefaultAuthScheme

Fixe le hash d'authentification à utiliser lorsque {hashname} n'est pas spécifié.

8.2.4. Serveur de fichiers et d'impression : Samba

Ce document a pour but de présenter l'installation d'un serveur Samba (contrôleur principal de domaine, authentification et autorisations, serveur de fichiers et d'impression) basé sur un annuaire LDAP pour la gestion des utilisateurs. Il décrit la méthode d'installation, les éléments spécifiques aux besoins du service ainsi que la configuration mise en oeuvre. On trouvera aussi une notice explicative des outils de base pour tester le service et ajouter les premiers utilisateurs.

8.2.4.1. Concepts généraux et références web

Annoncé en janvier 1992, par Andrew Tridgell, étudiant au laboratoire d'informatique à l'Université nationale d'Australie, nbserver ne devait uniquement permettre que de monter des partages Microsoft Windows® sur une machine Unix. Devenu un ensemble complet d'outils pour assurer la gestion des ressources réseau en milieu hétérogène, nbserver prend le nom de Samba (1.6.05) en avril 1994 pour évoquer le protocole implémenté. Au fil des versions, il se rapproche du comportement d'un serveur Microsoft NT4 (Contrôle du domaine, gestion de l'authentification aux ressources, partage des ressources, parcours du réseau SMB...). Samba 2.0 sort en janvier 1999, et Samba 3.0, qui permet enfin la gestion des groupes d'utilisateurs Microsoft Windows, en septembre 2003.

Samba est une suite logicielle permettant l'interconnexion de différents systèmes autour d'un protocole commun baptisé NetBIOS (*Network Basic Input Output System*), sur lequel s'appuient SMB (*Server Message Block*) ou CIFS (*Common Internet File System*) pour assurer le partage de ressources (fichiers, imprimantes, ports séries et parallèles).

Si le protocole de Microsoft SMB a pour but principal le partage de fichiers, les fonctionnalités sont étendues par :

- détermination de la présence d'autres serveurs utilisant ce protocole sur le réseau (*Network Browsing*) ;

- impression par le réseau ;
- authentification pour l'accès aux partages, répertoires et fichiers ;
- verrouillage (*lock*) des fichiers en cours d'utilisation ;
- notification des changements effectués sur les fichiers et répertoires ;
- notation de la version du protocole à employer (*Dialect*) ;
- gestion des attributs de fichier étendus ;
- support de l'Unicode ;
- gestion des verrouillages de fichiers.

L'authentification permet notamment la mise en place de domaines de type Microsoft NT4.

Principales références Web :

- Site Web officiel de Samba (anglais) (`http://www.samba.org/`)
- Documentation (`http://samba.org/samba/docs/`)
- Collection de Howto sur Samba (`http://samba.org/samba/docs/man/Samba-HOWTO-Collection/`)
- Projet de traduction de la documentation de Samba 3 (`http://home.gna.org/sambadoc/`)
- Samba By Example (`http://samba.org/samba/docs/man/Samba-Guide/`)
- smb.conf (`http://samba.org/samba/docs/man/manpages-3/smb.conf.5.html`)
- Samba Wiki (`http://wiki.samba.org/index.php/Main_Page`)

8.2.4.2. Installation et configuration

À la fin de cette partie, un serveur PDC (Primary Domain Controler, ou Contrôleur Primaire de Domaine) aura été mis en place. Les utilisateurs, groupes et machines seront conservés dans un annuaire LDAP. On considère qu'un annuaire est déjà fonctionnel, et permettra l'ajout des données nécessaires. Mais avant de se lancer dans cette partie, il est impératif d'installer les paquetages Samba et de tester une configuration simple.

8.2.4.2.1. Les paquetages nécessaires

- samba-server : contient les démons smbd (authentification et gestion de l'accès aux partages) et nmbd (dialogue)
- samba-client : contient les clients qui permettent d'accéder à des ressources SMB/CIFS distantes (nécessite mount-cifs, pour monter un système de fichiers distant de type CIFS).
- samba-winbind : permet à des logiciels tiers (PAM, serveur Samba membre du domaine, Squid, apache,...) de s'authentifier sur un serveur de domaine (Samba ou Microsoft Windows). Une telle architecture peut nécessiter nss_wins (pour PAM).
- samba-doc : l'ensemble de la documentation Samba.
- smbldap-tools: ce paquetage contient l'ensemble des scripts `smbldap-tools`, qui facilitent la manipulation des données (utilisateurs, groupes, machines) dans le cadre d'un serveur Samba authentifié sur un annuaire LDAP.

Passons en revue l'arborescence Samba :

`/etc/samba`

: contient l'ensemble des fichiers de configuration du serveur, essentiellement `samba.conf` pour la configuration générale et la configuration des partages, et `smb-winbind.conf` pour la configuration de Winbind.

`/usr/lib/samba/vfs`

Ce répertoire liste l'ensemble des modules VFS (*Virtual File System*) disponibles sur votre serveur. Dans la version actuelle, vous disposez de :

- `audit` : outil d'audit permettant une vérification exhaustive des accès au système de fichiers via les partages de données définies.
- `default_quota` : permet d'établir des quotas par défaut pour des utilisateurs et/ou des groupes
- `extd_audit` : identique à `audit` mais avec une conservation différente des logs
- `recycle` : permet de mettre en place des corbeilles réseau.
- `netatalk` : permet de gérer une compatibilité Apple sur les partages de ressources.

Vous trouverez plus d'information dans la documentation officielle : les VFS modules dans un serveur Samba (`http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/VFS.html`).

`/var/cache/samba`

Ce répertoire contient l'ensemble des mémoires caches dans des fichiers au format `*.tdb`. Ils contiennent des informations telles que le parcours des ressources, les noms Netbios, les logins... Ces fichiers peuvent être à l'origine de dysfonctionnements lorsque, par exemple, la mémoire cache demeure inchangée alors que des modifications sont intervenues.

`/var/log/samba`

Vous trouverez ici l'ensemble des logs du serveur Samba. Attention ce répertoire peut rapidement atteindre une taille gigantesque, particulièrement si vous travaillez sur un réseau comportant un nombre important de machines.

8.2.4.2.2. Configuration du serveur Samba en mode autonome

Il est à préciser que dans la phase de test, il est préférable de redémarrer Samba complètement après chaque modification du fichier `/etc/samba/smb.conf`.

8.2.4.2.2.1. Pré-requis

Voici la liste des éléments à définir pour démarrer :

Nom du groupe de travail

En mode autonome, il est nécessaire de définir le nom du groupe de travail auquel appartient le serveur. Il s'agit juste d'une information arbitraire mais obligatoire pour regrouper différentes machines dans un même groupe virtuel.

Cette information est donnée par l'attribut workgroup. C'est aussi cette option qui nous permettra de spécifier le nom du domaine à contrôler lorsque notre serveur deviendra un PDC. Pour cette documentation, le groupe de travail aura pour nom example.

```
# cat /etc/samba/smb.conf
[global]
...
        workgroup = example
...
```

Il est impératif de spécifier cet attribut.

Nom NetBIOS de la machine

Il est possible de donner un nom NetBIOS à la machine qui sera différent du nom affecté dans le DNS, cela se gère via l'attribut netbios name :

```
# cat /etc/samba/smb.conf
[global]
...
        netbios name = MES5
...
```

Cet attribut est optionnel. S'il est omis, par défaut, l'attribut prendra le nom de la machine tel que défini au DNS.

Commentaire sur la machine

De même, on pourra associer un commentaire afin d'identifier plus clairement la machine :

```
# cat /etc/samba/smb.conf
  [global]
  ...
  server string = Samba Server %v
  ...
```

Là encore, cet attribut est facultatif. S'il est omis, il restera vide.

8.2.4.2.2.2. Configuration du service

C'est le moyen le plus simple et le plus rapide de tester les paquetages installés. Pas de notion de domaine, juste un serveur avec quelques utilisateurs qui peuvent se connecter sur un partage personnel (`[homes]`), et un partage public, ouvert à tous (même les anonymes). Ce simple test nous permet de valider que les paquetages sont opérationnels et que l'authentification fonctionne.

Utilisons le fichier `/etc/samba/smb.conf` suivant :

```
# cat /etc/samba/smb.conf
[global]
        workgroup = example
        server string = Samba Server %v
        map to guest = Bad User
        log file = /var/log/samba/%m.log
        max log size = 50
```

```
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

[homes]
      # l'utilisation du bloc [homes] correspond à une définition par
      # défaut des répertoires personnels des utilisateurs
      ; le path par défaut sera donc ///home/nomDuUser//
        # on pourrait rajouter les attributs suivants pour agrémenter
        # la définition du partage
        ; comment = Home Directories
        ; browseable = no
        # et les utilisateurs peuvent y créer/modifier/supprimer des
        # fichiers/répertoires
        read only = no

[public]
        # ce partage définit un répertoire publique
        path = /home/public
        comment = Public Directory
        # il n'est pas nécessaire de s'authentifier pour y accéder
        guest ok = yes
      # et les utilisateurs peuvent y créer/modifier/supprimer des
      # fichiers/répertoires
        read only = no
        ; browseable = no
```

À compter de la version 3.4.x, Samba stocke par défaut les détails de compte Samba dans le backend **tdbsam** au lieu du backend **smbpasswd** qui était le backend par défaut des versions depuis au moins Samba 2.0.x . En prévision de l'arrivée de Samba 3.4.x, il est conseillé d'utiliser le backend **tdbsam**.

En effet, le processus de mise à niveau ne migre pas les comptes. Il est donc conseillé de migrer dès maintenant les détails de compte Samba du backend **smbpasswd** au backend **tdbsam** à l'aide de la commande (en tant que root):

```
#pdbedit -i smbpasswd -e tdbsam
```

Dans le cas, déconseillé, où vous désirez garder le backend **smbpasswd**, n'oubliez pas d'ajouter l'option suivante dans le fichier `smb.conf`:

```
passdb backend = smbpasswd
```

Vérifions qu'il ne comporte pas d'erreurs :

```
# testparm
      Load smb config files from /etc/samba/smb.conf
      Processing section "[homes]"
      Processing section "[public]"
      Loaded services file OK.
```

```
WARNING: passdb expand explicit = yes is deprecated
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions

[global]
workgroup = example
server string = Samba Server %v
map to guest = Bad User
log file = /var/log/samba/%m.log
max log size = 50
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

[homes]
read only = No

[public]
comment = Public Directory
path = /home/public
read only = No
guest ok = Yes
```

Pas d'erreurs notables, seul un warning concerne un attribut obsolète qui est défini par défaut.

8.2.4.2.2.3. Démarrage du service

Le service peut donc être démarré :

```
# service smb start
Lancement du service Samba :                                [  OK  ]
Lancement du service NMB :                                      [  OK  ]
# ps aux
...
root     27843  0.0  0.7  10724  4028 ?        Ss   12:43   0:00 smbd -D
root     27844  0.0  0.7  10724  4020 ?        S    12:43   0:00 smbd -D
root     27854  0.0  0.4   6568  2068 ?        Ss   12:43   0:00 nmbd -D
...
```

Le service est démarré, il s'agit maintenant de voir s'il répond aux requêtes :

```
# smbclient -L localhost
Password:
Domain=[MES5] OS=[Unix] Server=[Samba 3.2.7]

        Sharename       Type      Comment
        ---------       ----      -------
        homes           Disk
        public          Disk      Public Directory
        IPC$            IPC       IPC Service (Samba Server 3.2.7)
        ADMIN$          IPC       IPC Service (Samba Server 3.2.7)
Domain=[MES5] OS=[Unix] Server=[Samba 3.2.7]

        Server               Comment
```

```
        ---------            -------

        Workgroup            Master
        ---------            -------
        example
```

Le service répond lorsqu'on lui demande de lister les ressources visibles. On pourra jouer avec l'attribut `browseable` dans les partages pour vérifier qu'ils apparaissent ou non. Pour la suite des tests, le partage `[homes]` aura l'attribut `browseable = no`.

8.2.4.2.2.4. Première connexion : mode anonyme

Nous avons défini un partage public, accessible à tous, même sans authentification, il faut donc vérifier qu'il est utilisable dans ce cas :

```
# mkdir -m 777 /home/public
      #  ll /home
total 28
...
drwxrwxrwx  2 root   root   4096 jui 26 13:03 public/
# smbclient //localhost/public
Password:
Domain=[MES5] OS=[Unix] Server=[Samba 3.2.7]
smb: \> dir
  .                           D        0  Wed Jul 26 13:03:24 2008
  ..                          D        0  Wed Jul 26 13:03:24 2008

                48377 blocks of size 16384. 47347 blocks available
smb: \> mkdir test
smb: \> dir
  .                           D        0  Wed Jul 26 13:03:56 2008
  ..                          D        0  Wed Jul 26 13:03:24 2008
  test                        D        0  Wed Jul 26 13:03:56 2008

                48377 blocks of size 16384. 47347 blocks available
# ll /home/public/
total 4
drwxr-xr-x  2 nobody nogroup 4096 jui 26 13:03 test/
```

Tout semble opérationnel pour le moment.

8.2.4.2.2.5. Création et utilisation d'un utilisateur

Créons maintenant un utilisateur sur le système et sur samba :

```
# useradd -g users -m qatest
# getent passwd qatest
qatest:x:1001:100::/home/qatest:/bin/bash
# ll /home/qatest/ -d
drwxr-xr-x  3 qatest users 4096 jui 26 12:34 /home/qatest//
# passwd qatest
Changing password for user qatest.
      New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
# smbpasswd -a qatest
New SMB password:
Retype new SMB password:
# cat /etc/samba/smbpasswd
qatest:1001:8B28C7EF8A97362BAAD3B435B51404EE
 :EB407C0BA4F661A80BCF6B8231A0F6F7:[U          ]:LCT-44C74D6A:
```

Vérifions notre utilisateur :

```
# ssh qatest@localhost
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
qatest@localhost's password:
[qatest@mes5] $ smbclient -L localhost -U qatest
Password:
Domain=[MES5] OS=[Unix] Server=[Samba 3.2.7]

        Sharename       Type      Comment
        ---------       ----      -------
        public          Disk      Public Directory
        IPC$            IPC       IPC Service (Samba Server 3.2.7)
        ADMIN$          IPC       IPC Service (Samba Server 3.2.7)
        qatest          Disk      Home directory of qatest
Domain=[MES5] OS=[Unix] Server=[Samba 3.2.7]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        example            MES5
```

On voit ici que le partage `[homes]` a disparu de la liste (attribut `browseable = no` en place), mais qu'un partage du nom de l'utilisateur est apparu. En effet, un utilisateur a le droit de voir son propre répertoire, si on utilise la définition standard de `[homes]`.

Connectons-nous à ce partage :

```
$ smbclient //localhost/qatest -U qatest
Password:
```

```
Domain=[MES5] OS=[Unix] Server=[Samba 3.2.7]
smb: \> dir
  .                                   D        0  Wed Jul 26 13:14:33 2008
  ..                                  D        0  Wed Jul 26 13:03:24 2008
  tmp                                 D        0  Wed Jul 26 12:34:36 2008
  .screenrc                           H     3793  Wed Jul 26 12:34:37 2008
  .bash_logout                        H       24  Wed Jul 26 12:34:37 2008
  .bash_profile                       H      191  Wed Jul 26 12:34:37 2008
  .bashrc                             H      124  Wed Jul 26 12:34:37 2008
  .bash_completion                    H      145  Wed Jul 26 12:34:37 2008
  .bash_history                       H       33  Wed Jul 26 13:14:33 2008

                48377 blocks of size 16384. 47346 blocks available
smb: \> mkdir test
smb: \> dir
  .                                   D        0  Wed Jul 26 13:26:04 2008
  ..                                  D        0  Wed Jul 26 13:03:24 2008
  tmp                                 D        0  Wed Jul 26 12:34:36 2008
  .screenrc                           H     3793  Wed Jul 26 12:34:37 2008
  .bash_logout                        H       24  Wed Jul 26 12:34:37 2008
  .bash_profile                       H      191  Wed Jul 26 12:34:37 2008
  .bashrc                             H      124  Wed Jul 26 12:34:37 2008
  .bash_completion                    H      145  Wed Jul 26 12:34:37 2008
  .bash_history                       H       72  Wed Jul 26 13:24:36 2008
  test                                D        0  Wed Jul 26 13:26:04 2008

                48377 blocks of size 16384. 47346 blocks available
$ ll -a
total 40
drwxr-xr-x  4 qatest users 4096 jui 26 13:26 ./
drwxr-xr-x  6 root   root  4096 jui 26 13:03 ../
-rw-r--r--  1 qatest users  145 jui 26 12:34 .bash_completion
-rw-------  1 qatest users   72 jui 26 13:24 .bash_history
-rw-r--r--  1 qatest users   24 jui 26 12:34 .bash_logout
-rw-r--r--  1 qatest users  191 jui 26 12:34 .bash_profile
-rw-r--r--  1 qatest users  124 jui 26 12:34 .bashrc
-rw-r--r--  1 qatest users 3793 jui 26 12:34 .screenrc
drwxr-xr-x  2 qatest users 4096 jui 26 13:26 test/
drwx------  2 qatest users 4096 jui 26 12:34 tmp/
```

Voyons maintenant le partage public :

```
$ smbclient //localhost/public -U qatest
Password:
Domain=[MES5] OS=[Unix] Server=[Samba 3.2.7]
smb: \> dir
  .                                   D        0  Wed Jul 26 13:03:56 2008
  ..                                  D        0  Wed Jul 26 13:03:24 2008
  test                                D        0  Wed Jul 26 13:03:56 2008

                48377 blocks of size 16384. 47346 blocks available
smb: \> mkdir qatest
smb: \> dir
  .                                   D        0  Wed Jul 26 13:30:35 2008
  ..                                  D        0  Wed Jul 26 13:03:24 2008
```

```
  test                            D        0  Wed Jul 26 13:03:56 2008
  qatest                          D        0  Wed Jul 26 13:30:35 2008
                48377 blocks of size 16384. 47346 blocks available
$ ll /home/public/
total 8
drwxr-xr-x  2 qatest users   4096 jui 26 13:30 qatest/
drwxr-xr-x  2 nobody nogroup 4096 jui 26 13:03 test/
```

Notre serveur Samba autonome est pleinement opérationnel.

8.2.4.2.3. Samba avec authentification LDAP

La configuration que nous avons utilisée jusqu'à maintenant va nous servir de base. Nous n'allons que modifier l'authentification. Celle-ci sera désormais basée sur un annuaire LDAP.

8.2.4.2.3.1. Une installation de Samba fonctionnelle

Il suffit de se reporter au paragraphe précédent (Section 8.2.4.2.2). On conservera les mêmes pré-requis qu'au paragraphe précédent concernant le nom de domaine, le nom NetBIOS de la machine et le commentaire associé.

```
# vi /etc/samba/smb.conf
[global]
        ...
        workgroup = example
        netbios name = MES5
        server string = Samba Server %v
        ...
```

8.2.4.2.3.2. SID du Domaine

Tant que le service n'a pas été démarré au moins une fois, aucun SID n'a été attribué au serveur/domaine. C'est pour cette raison que la récupération de cette information n'est réalisée qu'après le test en mode autonome.

L'information est conservée dans `/etc/samba/secrets.tdb`, mais elle n'est pas lisible directement. On le récupérera avec la commande `net getlocalsid`:

```
# net getlocalsid
SID for domain dhcp110 is: S-1-5-21-1518519320-3136826138-1578965553
```

8.2.4.2.3.3. Utilisateurs et groupes du domaine

Rappelons dans un premier temps la liste des SID particuliers reconnus par Windows®. Lors de son installation, Windows® NT4/200x/XP est configuré avec certaines entités (utilisateur, groupe ou alias). Chaque entité a un RID identifié. Ces RID spécifiques doivent être respectés afin de préserver l'intégrité des opérations. Samba doit être alimenté avec ces entités essentielles du domaine.

Si Samba est configuré pour utiliser tdbsam, les entités essentielles sont automatiquement créées. Si LDAP est utilisé, l'administrateur de l'annuaire est responsable de leur création : on pourra utiliser les `smbldap-tools` pour cela, et notamment le script `smbldap-populate`.

Entité déclarée	RID	Type	Essentiel
Domain Administrator	500	User	Non
Domain Guest	501	User	Non
Domain KRBTGT	502	User	Non
Domain Admins	512	Group	Oui
Domain Users	513	Group	Oui
Domain Guests	514	Group	Oui
Domain Computers	515	Group	Non
Domain Controller	516	Group	Non
Domain Certificate Admins	517	Group	Non
Domain Schema Admins	518	Group	Non
Domain Enterprise Admins	519	Group	Non
Domain Policy Admins	520	Group	Non
Builtin Admins	544	Alias	Non

Entité déclarée	RID	Type	Essentiel
Builtin users	545	Alias	Non
Builtin Guests	546	Alias	Non
Builtin Power Users	547	Alias	Non
Builtin Account Operators	548	Alias	Non
Builtin System Operators	549	Alias	Non
Builtin Print Operators	550	Alias	Non
Builtin Backup Operators	551	Alias	Non
Builtin Replicator	552	Alias	Non
Builtin RAS Servers	553	Alias	Non

Tableau 8-1. Entités d'un domaine Windows

D'après ces spécifications, nous déduisons des entités obligatoires et des entités facultatives :

- entrées obligatoires : s'il n'est pas obligatoire au bon fonctionnement du PDC, l'administrateur du domaine (Domain Administrator/500 - par défaut, seul compte à avoir le contrôle intégral du système) est néanmoins important pour la gestion du domaine. Un utilisateur *nobody* doit être créé si on souhaite utiliser la directive `ldapsam:trusted` (pour diminuer le dialogue entre Samba et le sous-système posix).

  Concernant les groupes, on créera **impérativement** : le groupe des Administrateurs du Domaine, le groupe des Utilisateurs du Domaine, le groupe des Invités du Domaine.

- entités facultatives : à la vue du tableau, on ajoutera les entités correspondantes, et en particulier le groupe des Machines du Domaine afin d'y rattacher les machines qu'on intégrera dans ce domaine.

8.2.4.2.3.4. Annuaire LDAP

Le but de ce chapitre n'est pas d'installer un annuaire. Si certaines manipulations sont décrites ici, elles ne peuvent en aucun cas être considérées comme une recette de mise en oeuvre d'un annuaire LDAP de production. Sur un

serveur utilisé pour l'authentification de services tels que ssh/PAM, la messagerie, apache, on trouvera déjà une arborescence.

Pour ce chapitre :

- Le `basedn` considéré sera `dc=example,dc=com`.
- Les utilisateurs sont dans l'OU `ou=people,dc=example,dc=com`
- Les groupes sont dans l'OU `ou=group,dc=example,dc=com`
- Il faut créer une `OU` pour conserver les comptes de machines, si on ne souhaite pas les mélanger avec les utilisateurs (`ou=hosts,dc=example,dc=com`).
- Il faut aussi disposer d'un (ou plusieurs) compte(s) qui aura (auront) le droit d'écrire dans ces `OU`s, ainsi que dans le `basedn` pour ajouter/modifier/supprimer les informations propres à Samba, et les outils complémentaires.

Il est possible de mettre rapidement en place un serveur LDAP avec un script fourni avec la distribution. Il faut installer le paquetage `openldap-example-dit`. Puis exécuter le script qui génère la configuration avec les données qui seront spécifiées. Ce script crée l'arborescence et les comptes nécessaires à Samba+LDAP, mais aussi à d'autres applications :

```
# /usr/share/openldap/scripts/example-dit-setup.sh
Please enter your DNS domain name [example.com]:
exmaple.com


Administrator account

The administrator account for this directory is
uid=LDAP Admin,ou=System Accounts,dc=example,dc=com

Please choose a password for this account:
New password:
Re-enter new password:


Summary
=======

Domain:        example.com
LDAP suffix:   dc=example,dc=com
Administrator: uid=LDAP Admin,ou=System Accounts,dc=example,dc=com

Confirm? (Y/n)

config file testing succeeded
Stopping ldap service
Finished, starting ldap service
Lancement de /usr/bin/db_recover sous /var/lib/ldap
removing /var/lib/ldap/alock
```

```
Lancement de slapd (ldap + ldaps) :                    [  OK  ]

Your previous database directory has been backed up as /var/lib/
ldap.1155740637
All files that were backed up got the suffix "1155740637".

# ldapsearch -x
# extended LDIF
#
# LDAPv3
# base <> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# example.com
dn: dc=example,dc=com
dc: example
objectClass: domain
objectClass: domainRelatedObject
associatedDomain: example.com

# People, example.com
dn: ou=People,dc=example,dc=com
ou: People
objectClass: organizationalUnit

# Group, example.com
dn: ou=Group,dc=example,dc=com
ou: Group
objectClass: organizationalUnit
description: Container for user accounts

# System Accounts, example.com
dn: ou=System Accounts,dc=example,dc=com
ou: System Accounts
objectClass: organizationalUnit
description: Container for System and Services privileged accounts

# System Goups, example.com
dn: ou=System Groups,dc=example,dc=com
ou: System Groups
objectClass: organizationalUnit
description: Container for System and Services privileged groups

# Hosts, example.com
dn: ou=Hosts,dc=example,dc=com
ou: Hosts
objectClass: organizationalUnit
description: Container for Samba machine accounts
...
# Account Admin, System Accounts, example.com
dn: uid=Account Admin,ou=System Accounts,dc=example,dc=com
uid: Account Admin
objectClass: account
objectClass: simpleSecurityObject
```

```
description: Account used to administer all users, groups, machines
 and general accounts

# nssldap, System Accounts, example.com
dn: uid=nssldap,ou=System Accounts,dc=example,dc=com
uid: nssldap
objectClass: account
objectClass: simpleSecurityObject
description: Unprivileged account which can be used by nss_ldap for
 when anonymous searches are disabled
...
```

On retrouve les OUs dont il est question pour Samba (`People/Group/Hosts`) ainsi qu'une OU (`System Accounts`) contenant les comptes de connexion pour les différents outils de gestion des comptes (Account Admin, nssldap).

8.2.4.2.3.5. NSS + LDAP

Nous avons vu dans la partie concernant le mode autonome (Section 8.2.4.2.2.5) qu'il fallait d'abord créer un utilisateur système puis le faire reconnaître par Samba (Création et utilisation d'un utilisateur). Il en va de même pour un PDC dont les utilisateurs sont enregistrés dans un annuaire LDAP.

Pour cela, il faut créer un utilisateur Posix dans l'annuaire LDAP puis ajouter les informations spécifiques à Samba (utilisation des smbldap-tools, par ex), et il faut aussi que le système puisse accéder à cet utilisateur. Il faut donc configurer NSS (Name Service Switch).

Installons nssldap.

```
# urpmi nss_ldap
```

Pour que NSS sache qu'il doit consulter un annuaire LDAP pour trouver des utilisateurs et des groupes, il faut modifier `/etc/nsswitch.conf` :

```
# /etc/nsswitch.conf
# An example Name Service Switch config file. This file should be
# sorted with the most-used services at the beginning.
#
...
passwd:         files ldap
shadow:         files
group:          files ldap
...
```

Il est important de conserver l'ordre spécifié entre `files` et ldap afin que les comptes d'administration propres à la machine soient trouvés sans avoir besoin d'interroger l'annuaire LDAP.

Il ne suffit pas d'indiquer à NSS d'interroger un annuaire LDAP, encore faut-il préciser lequel, et comment. Pour cela, il faut renseigner `/etc/ldap.conf`. Dans ce fichier, on pourra spécifier un utilisateur (ici `uid=nssldap,ou=System Accounts,dc=example,dc=com`) qui se branchera à l'annuaire LDAP pour lire les informations : ça n'est pas indispensable, mais peut être utile à des fins de traçage des requêtes et/ou de mise en place d'ACL complexes.

```
# vi /etc/ldap.conf
host 127.0.0.1
base dc=example,dc=com
# On décommentera les 2 lignes suivantes à des fins de traçage/ACL
#binddn uid=nssldap,ou=System Accounts,dc=example,dc=com
#bindpw nssldap
nss_base_passwd         ou=People,dc=example,dc=com?one
nss_base_passwd         ou=Hosts,dc=example,dc=com?one
nss_base_shadow         ou=People,dc=example,dc=com?one
nss_base_group          ou=Group,dc=example,dc=com?one
```

Afin que Samba fonctionne correctement, il est nécessaire de permettre à NSS de lire le contenu de l'OU Hosts : Samba pourra ainsi identifier les machines qui souhaiteront se connecter au domaine.

Il faut maintenant vérifier que le mécanisme fonctionne. Il faut pour cela disposer d'utilisateurs et de groupes dans l'annuaire LDAP. Si ce n'est pas déjà le cas, voici un fichier `ldif` qu'on peut ajouter le temps des tests :

```
# vi /root/test.ldif
# Groupe test
dn: cn=test,ou=Group,dc=example,dc=com
objectClass: top
objectClass: posixGroup
gidNumber: 200
cn: test

# Utilisateur test
dn: uid=test,ou=People,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: test
sn: test
givenName: test
uid: test
uidNumber: 1000
gidNumber: 200
homeDirectory: /home/test
loginShell: /bin/bash
gecos: System User
userPassword: test
```

```
# ldapadd -x -D "uid=LDAP Admin,ou=System Accounts,dc=example,dc=com"
 -w <passwd> -f test.ldif
adding new entry "cn=test,ou=Group,dc=example,dc=com"

adding new entry "uid=test,ou=People,dc=example,dc=com"
```

Vérifions maintenant que le fonctionnement est adéquat avec les commandes suivantes :

```
# getent passwd test
test:x:1000:200:System User:/home/test:/bin/bash
# getent group test
test:x:200:
# id test
uid=1000(test) gid=200(test) groupes=200(test)
```

8.2.4.2.3.6. Fonctionnement de Pam et LDAP

Il est possible de permettre aux utilisateurs définis dans l'annuaire LDAP de se connecter physiquement à la machine via SSH ou via une mire de login. Pour cela, il faut aussi configurer PAM, et les services en question, cela se fait via le paquetage pam_ldap.

Installons le paquetage pam_ldap.

```
# urpmi pam_ldap
```

Il faut ensuite modifier le fichier `/etc/pam.d/system-auth`, l'ensemble des services utilisant PAM pointe dessus.

```
# vi /etc/pam.d/system-auth
#%PAM-1.0

auth        required      pam_env.so
auth        sufficient    pam_unix.so likeauth nullok
auth        sufficient    pam_ldap.so use_first_pass
auth        required      pam_deny.so

account     sufficient    pam_unix.so
account     sufficient    pam_ldap.so
account     required      pam_deny.so

password    required      pam_cracklib.so retry=3 minlen=2  dcredit=0
 ucredit=0
password    sufficient    pam_unix.so nullok use_authtok md5 shadow
password    sufficient    pam_ldap.so
password    required      pam_deny.so

session     required      pam_limits.so
session     required      pam_unix.so
```

Pour vérifier le bon fonctionnement de pam-ldap, il suffit d'essayer de se connecter avec l'utilisateur créé pour vérifier si la configuration est correcte ou non.

```
# su - test
su: AVERTISSEMENT: ne peut changer de répertoire vers /home/test: Aucun
 fichier ou répertoire de ce type
-bash-3.00$ id test
uid=1000(test) gid=200(test) groupes=200(test)
```

L'avertissement apparaît car le répertoire de l'utilisateur (`/home/test`) n'existe pas.

Pour le même test avec SSH, il est nécessaire de modifier la configuration de SSH et de le redémarrer.

```
# vi /etc/ssh/sshd_config
...
# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication mechanism.
# Depending on your PAM configuration, this may bypass the setting of
# PasswordAuthentication, PermitEmptyPasswords, and
# "PermitRootLogin without-password". If you just want the PAM account
# and session checks to run without PAM authentication, then enable
# this but set
# ChallengeResponseAuthentication=no
UsePAM yes
...
# service sshd restart
Arrêt de sshd :                                            [  OK  ]
Lancement de sshd :                                        [  OK  ]
# ssh test@localhost
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
Password:
Could not chdir to home directory /home/test: No such file or directory
/usr/X11R6/bin/xauth:  error in locking authority file
 /home/test/.Xauthority
-bash-3.00$ id
uid=1000(test) gid=200(test) groupes=200(test)
```

8.2.4.2.3.7. Utilisation des smbldap-tools

Le paquetage `smbldap-tools` fournit un ensemble d'outils pour manipuler les comptes utilisateurs Samba dans l'annuaire LDAP.

```
# ll /usr/sbin/smbldap-*
-rwxr-xr-x  1 root root  5987 mar 21 14:41 /usr/sbin/smbldap-groupadd*
-rwxr-xr-x  1 root root  2473 mar 21 14:41 /usr/sbin/smbldap-groupdel*
-rwxr-xr-x  1 root root  8881 mar 21 14:41 /usr/sbin/smbldap-groupmod*
-rwxr-xr-x  1 root root  2005 mar 21 14:41 /usr/sbin/smbldap-groupshow*
-rwxr-xr-x  1 root root 10294 mar 21 14:41 /usr/sbin/smbldap-passwd*
-rwxr-xr-x  1 root root 14995 mar 21 14:41 /usr/sbin/smbldap-populate*
-rwxr-xr-x  1 root root 20969 mar 21 14:41 /usr/sbin/smbldap-useradd*
-rwxr-xr-x  1 root root  3244 mar 21 14:41 /usr/sbin/smbldap-userdel*
-rwxr-xr-x  1 root root  7633 mar 21 14:41 /usr/sbin/smbldap-userinfo*
-rwxr-xr-x  1 root root 18992 mar 21 14:41 /usr/sbin/smbldap-usermod*
-rwxr-xr-x  1 root root  1958 mar 21 14:41 /usr/sbin/smbldap-usershow*
```

Pour utiliser ces outils, il faut les configurer afin qu'ils respectent l'organisation que nous avons choisi pour notre structure. On doit aussi récupérer le `SID` du domaine.

Installons le paquetage smbdap-tools

```
# urpmi smbldap-tools
```

Pour utiliser ces outils, il faut préciser le `SID`, le nom du domaine, le nom des différentes OU de l'annuaire LDAP, le ou les annuaires LDAP à utiliser, ainsi que les attributs `posix` et `samba` par défaut. On pourra utiliser le fichier minimal suivant (ou reporter l'équivalent dans le fichier fourni par défaut) :

```
# vi /etc/smbldap-tools/smbldap.conf
      SID="S-1-5-21-2433760973-660784831-1051970529"
      sambaDomain="example

slaveLDAP="127.0.0.1"
slavePort="389"
masterLDAP="127.0.0.1"
masterPort="389"

ldapTLS="0"
verify="require"
cafile="/etc/ssl/cacert.pem"
clientcert=""
clientkey=""

suffix="dc=example,dc=com"
usersdn="ou=People,${suffix}"
computersdn="ou=Hosts,${suffix}"
groupsdn="ou=Group,${suffix}"
idmapdn="ou=Idmap,${suffix}"

sambaUnixIdPooldn="sambaDomainName=${sambaDomain},${suffix}"
```

```
scope="sub"

hash_encrypt="SSHA"
crypt_salt_format="%s"

userLoginShell="/bin/false"
userHome="/home/%U"
userHomeDirectoryMode="700"
userGecos="smbldap System User"
defaultUserGid="513"
defaultComputerGid="515"
skeletonDir="/etc/skel"
defaultMaxPasswordAge="45"

userSmbHome="\\MES5\%U"
userProfile="\\MES5\profiles\%U"
userHomeDrive="U:"
userScript=""

mailDomain="example.com"

with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
with_slappasswd="0"
slappasswd="/usr/sbin/slappasswd"
```

Il faut aussi renseigner le fichier `/etc/smbldap-tools/smbldap_bind.conf` : ce fichier spécifie les comptes qui permettront de se connecter à l'annuaire LDAP pour effectuer les différentes manipulations.

```
# cat /etc/smbldap-tools/smbldap_bind.conf
slaveDN="uid=Account Admin,ou=System Accounts,dc=example,dc=com"
slavePw="passwd"
masterDN="uid=Account Admin,ou=System Accounts,dc=example,dc=com"
masterPw="passwd"
```

Vérifions maintenant le bon fonctionnement des outils :

```
# smbldap-usershow test
dn: uid=test,ou=People,dc=example,dc=com
objectClass: top,person,organizationalPerson,inetOrgPerson,
 posixAccount,shadowAccount
cn: test
sn: test
givenName: test
uid: test
uidNumber: 1000
gidNumber: 200
homeDirectory: /home/test
loginShell: /bin/bash
gecos: System User
userPassword: test
# smbldap-groupshow test
dn: cn=test,ou=Group,dc=example,dc=com
```

```
objectClass: top,posixGroup
gidNumber: 200
cn: test
```

Créons maintenant les utilisateurs et groupes du domaine. Les smbldap-tools fournissent un outil (`smbldap-populate`) qui crée la base de l'annuaire LDAP avec les utilisateurs et groupes nécessaires au bon fonctionnement de la solution.

Ajoutons les comptes nécessaires à la solution :

```
# smbldap-populate -a Administrator -k 500 -m 512
Populating LDAP directory for domain example (S-1-5-21-2433760973-
 660784831-1051970529)
(using builtin directory structure)

entry dc=example,dc=com already exist.
entry ou=People,dc=example,dc=com already exist.
entry ou=Group,dc=example,dc=com already exist.
entry ou=Hosts,dc=example,dc=com already exist.
entry ou=Idmap,dc=example,dc=com already exist.
adding new entry: uid=Administrator,ou=People,dc=example,dc=com
adding new entry: uid=nobody,ou=People,dc=example,dc=com
adding new entry: cn=Domain Admins,ou=Group,dc=example,dc=com
adding new entry: cn=Domain Users,ou=Group,dc=example,dc=com
adding new entry: cn=Domain Guests,ou=Group,dc=example,dc=com
adding new entry: cn=Domain Computers,ou=Group,dc=example,dc=com
adding new entry: cn=Administrators,ou=Group,dc=example,dc=com
adding new entry: cn=Account Operators,ou=Group,dc=example,dc=com
adding new entry: cn=Print Operators,ou=Group,dc=example,dc=com
adding new entry: cn=Backup Operators,ou=Group,dc=example,dc=com
adding new entry: cn=Replicators,ou=Group,dc=example,dc=com
adding new entry: sambaDomainName=example,dc=example,dc=com

Please provide a password for the domain Administrator:
Changing UNIX and samba passwords for Administrator
New password:
Retype new password:
```

8.2.4.2.3.8. Configuration du serveur Samba

La section `[global]` du fichier `/etc/samba/smb.conf` devra contenir les informations suivantes :

```
[global]
...
# on peut définir plusieurs types de sources
;passdb backend = ldapsam, smbpasswd, guest
;passdb backend = ldapsam:ldap://myfirstldap.edge-it.fr,
 ldapsam:ldap://mysecondldap.edge-it.fr, guest
# ici, on travaille avec un annuaire LDAP local
passdb backend = ldapsam:ldap://127.0.0.1
```

```
# on se connecte à l'annuaire avec le compte LDAP suivant
ldap admin dn = uid=Account Admin,ou=System Accounts,dc=example.dc=com
# en TLS ou SSL
; ldap ssl = start_tls
ldap ssl = off

# le basedn et les OU où sont conservés les informations
ldap suffix = dc=example.com
ldap machine suffix = ou=hosts
ldap user suffix = ou=people
ldap group suffix = ou=group

# cette option permet de ne pas avoir besoin de configurer PAM
# ce n'est valable que si les utilisateurs Samba n'ont pas a accéder
 directement à un compte sur la machine.
ldapsam:trusted = yes
```

La vérification permet de constater qu'il n'y a pas d'erreurs détectées.

```
# testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[public]"
Loaded services file OK.
WARNING: passdb expand explicit = yes is deprecated
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions

[global]
        workgroup = EXAMPLE
        server string = Samba Server %v
        map to guest = Bad User
        passdb backend = ldapsam:ldap://127.0.0.1
        log file = /var/log/samba/%m.log
        max log size = 50
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        ldap admin dn = uid=Account Admin,ou=System Accounts,
          dc=example,dc=com
        ldap group suffix = ou=group
        ldap machine suffix = ou=hosts
        ldap suffix = dc=example,dc=com
        ldap ssl = no
        ldap user suffix = ou=people
        ldapsam:trusted = yes

[homes]
        read only = No
        browseable = No

[public]
        comment = Public Directory
        path = /home/public
        read only = No
```

```
        guest ok = Yes
```

Testons la connexion en mode anonyme :

```
# smbclient -L localhost
Password:
Domain=[MES5] OS=[Unix] Server=[Samba 3.2.7]

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          IPC       IPC Service (Samba Server 3.2.7)
        IPC$            IPC       IPC Service (Samba Server 3.2.7)
        public          Disk      Public Directory
Domain=[MES5] OS=[Unix] Server=[Samba 3.2.7]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        example             MES5
```

On doit ensuite faire connaître le mot de passe du compte de connexion à l'annuaire à Samba :

```
# smbpasswd -W
Setting stored password for "uid=Samba Admin,ou=System Accounts,
 dc=example,dc=com" in secrets.tdb
New SMB password:
Retype new SMB password:
```

On peut déjà vérifier que le lien avec l'annuaire LDAP est en place (en saisissant un mauvais mot de passe puis le bon).

```
# smbclient -L localhost -U administrator
Password:
session setup failed: NT_STATUS_LOGON_FAILURE
#  smbclient -L localhost -U administrator
Password:
Domain=[MES5] OS=[Unix] Server=[Samba 3.2.7]

        Sharename       Type      Comment
        ---------       ----      -------
        public          Disk      Public Directory
        IPC$            IPC       IPC Service (Samba Server 3.2.7)
        ADMIN$          IPC       IPC Service (Samba Server 3.2.7)
Domain=[MES5] OS=[Unix] Server=[Samba 3.2.7]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        example
```

Définissons maintenant notre serveur comme PDC, car jusqu'à présent, nous l'utilisions en autonome :

```
#  vi /etc/samba/smb.conf
[global]
...
        # PDC
        security = user
        # OS level > 32 pour être élu
        os level = 128
        # permet le déclenchement des élections
        # définition d'un PDC
        local master = yes
        # dmain master browser
        domain master = yes
        # force les élections pour devenir PDC
        preferred master = yes
        # le serveur fait de l'authentification
        domain logons = yes
...
#  testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[public]"
Loaded services file OK.
WARNING: passdb expand explicit = yes is deprecated
Server role: ROLE_DOMAIN_PDC
Press enter to see a dump of your service definitions

[global]
        workgroup = example
        server string = Samba Server %v
        map to guest = Bad User
        passdb backend = ldapsam:ldap://127.0.0.1
        log file = /var/log/samba/%m.log
        max log size = 50
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        domain logons = Yes
        os level = 128
        preferred master = Yes
        domain master = Yes
        ldap admin dn = uid=Samba Admin,ou=System Accounts,dc=edge-it,
          dc=subnet
        ldap group suffix = ou=group
        ldap machine suffix = ou=hosts
        ldap suffix = dc=edge-it,dc=subnet
        ldap ssl = no
        ldap user suffix = ou=people
        ldapsam:trusted = yes

[homes]
        read only = No
        browseable = No

[public]
```

```
comment = Public Directory
path = /home/public
read only = No
guest ok = Yes
```

8.2.4.2.3.9. Gérer les partages de fichiers Samba

Nous avons vu jusqu'à présent la configuration générale d'un serveur Samba et la mise en place de son rôle sur le réseau. Passons maintenant en revue les types de partages de ressources que vous pouvez mettre en place.

La syntaxe d'un partage est relativement simple et s'inscrit à la suite des paramètres génériques du serveur :

```
[<nom_partage>]
 comment = "<votre commentaire>"
 path = <chemin_ressource>
 browseable = <yes|no>
 writable = <yes|no>
```

Tout comme pour la section générale, un partage est introduit par son nom entre crochets. Ci-dessous les paramètres les plus courants :

- `comment` : entrez ici un commentaire suffisamment significatif, il apparaît lors du parcours des ressources et vous permet d'en identifier rapidement le contenu
- `path` : spécifie le chemin local vers la ressource partagée
- `browseable` : détermine si la ressource doit apparaître lors du parcours des ressources
- `writable` : indique les droits en écriture ou en lecture sur la ressource partagée

partage de type `logon`

Ce partage spécifique concerne les scripts de netlogon ou scripts de connexion des utilisateurs du domaine. Il permet le partage des scripts de netlogon générés à la volée grâce à la directive `root preexec`.

```
[netlogon] comment = Network Logon Service
  path = /data/samba/netlogon guest ok = yes writable = no
  write list = @administrateurs browseable = no root preexec =
  /data/samba/netlogon/logon_script '%m' '%U' '%a' '%g'
  '%L'
```

partage de type `profile`

Dans le cas où vous avez recours au profils itinérants, ceux-ci feront donc également l'objet d'un partage Samba spécifique utilisant le mot clé `profiles`.

```
[profiles] path = /data/samba/profiles
       browseable = no guest ok = yes writable = yes
```

partage de type `homes`

Vous pouvez mettre à disposition les répertoires personnel (*homes*) des utilisateurs. On utilisera pour cela le mot clé réservé `homes`. `%u` est une variable prédéfinie contenant le nom d'utilisateur de l'utilisateur.

```
[homes] comment = Home
  Directories browseable = no writable = yes path =
  /data/samba/prives/%u
```

partage de type `group`

Ce type de partage vous permet de définir des ressources accessibles pour un ou plusieurs groupes donnés. Il évite de définir un partage par groupe. Le principe est simple : il repose sur la détermination de droits dans l'arborescence des données. Le paramètre `hide unreadable` permet de cacher aux utilisateurs les répertoires pour lesquels il n'a aucun droit. Par exemple :

```
# ll /data/samba/groupes/ total
       24 drwxrws--- 111 root commercial 4096 avr 28 17:45 clients/
       drwxrws--- 23 root utilisateurs 4096 sep 9 2008 commercial/
       drwxrws--- 6 root support 104 jui 19 14:24 support/
```

Le partage peut alors être écrit de la manière suivante :

```
[groupes] comment =
  Stockage Groupes path = /data/samba/groupes writable = yes
  browseable = yes hide unreadable = yes
```

8.2.4.2.3.10. Gérer les partages d'imprimantes Samba

Nous avons vu les partages de fichiers, abordons maintenant les partages d'imprimantes. Samba vous permet de faire du partage d'accès mais aussi du partage de drivers, vous évitant ainsi d'avoir à installer ces drivers sur chacune des machines clientes.

Le partage spécifique `[printers]` permet le partage de toutes les imprimantes disponibles grâce à CUPS. Le partage spécifique `[print$]` permet lui le partage des drivers.

```
# partage des imprimantes déclarées
 [printers]
 comment = All Printers
 path = /var/spool/samba
 browseable = no
 guest ok = yes
 writable = no
 printable = yes
 create mode = 0700

 # partage de distribution des pilotes d'impression
 [print$]
 path = /var/lib/samba/printers
 browseable = yes
 read only = yes
 write list = @administrateurs
      guest ok = yes
```

Vous devrez au préalable disposer d'un serveur CUPS fonctionnel et déclaré dans la section [global] :

```
[global]
 ...
 # on se sert des imprimantes définies dans CUPS
 # on charge la liste
 printcap name = cups
 load printers = yes

 # ajout des imprimantes autorisé pour le groupe administrateurs
 printer admin = @administrateurs
```

Si le serveur CUPS n'est pas sur la même machine, vous pouvez ajouter la directive `cups server` suivie de l'adresse du serveur.

Une fois que vos partages sont définis, ainsi que le serveur CUPS utilisé, il reste à faire prendre en compte les imprimantes définies dans CUPS par Samba. On utilise pour cela la commande `cupsaddsmb` :

```
cupsaddsmb
      -a -u <nom_administrateur>
```

Dans le cas d'un ajout d'imprimantes à votre serveur CUPS, il sera nécessaire de relancer le serveur Samba avant d'exécuter la commande `cupsaddsmb`.

8.2.4.2.4. Dépannage

Régler un problème de Samba n'est pas toujours une tâche facile. Voici une liste de vérifications à réaliser pour les dysfonctionnements les plus courants :

- Vérifier l'espace disque disponible dans les systèmes de fichiers contenant les partages
- Vérifier l'espace disque disponible pour les fichiers de journalisation (attention, si le niveau est élevé, vérifier également l'espace dans /tmp. Un niveau élevé peut également affecter considérablement les performances du serveur.
- Vérifier l'inactivité éventuelle de processus Samba afin de régler au mieux le timeout
- Vérifier l'espace mémoire utilisé par les processus Samba.

La documentation officielle de Samba propose un guide complet vous permettant d'identifier de manière exhaustive les sources de problèmes et les outils à mettre en place pour les diagnostiquer : section *Troubleshooting* de la documentation Samba (`http://samba.org/samba/docs/man/Samba-HOWTO-Collection/troubleshooting.html`).

8.2.4.2.5. ACLs étendues

Microsoft Windows® utilise un jeu d'ACLs (*Access Control Lists*) et d'attributs étendus par rapport au triplé standard accessible sur un système GNU/Linux (`Read/Write/Execute` pour un utilisateur, son groupe, ou tout le monde). Il est possible de simuler une partie de ces informations sous GNU/Linux en utilisant un système de fichiers qui supporte un tel format, et en ajoutant les paquetages qui facilitent la gestion de ces ACLs.

Vous devrez alors installer les paquetages suivants :

- acl : ce paquetage contient les commandes `getfacl` et `setfacl` qui permettent de voir, ajouter/modifier/supprimer des ACLs étendues sur un fichier ou répertoire.

- attr : ce paquetage contient les commandes `getfattr` et `setfattr` qui permettent de voir, ajouter/modifier/supprimer des attributs étendus sur un fichier ou répertoire.

Les système de fichiers supportant ces ACLs :

- XFS supporte en mode natif ces 2 jeux d'informations étendues, comme reiserFS et jFS.
- ext2/3 supportent ces informations moyennant une modification (*patch*) sur le système de fichier, et l'activation de l'attribut `acl` lors du montage du système de fichiers concerné.

Par défaut, Mandriva Enterprise Server 5 ajoute le support des Listes de contrôle d'accès avancées (ACL) pour gérer les droits des utilisateurs sur les partitions ext3.

On pourra lire `POSIX Access Control Lists on Linux` pour plus d'informations.

On veillera à utiliser du XFS-512 à la place du XFS-256 (défaut sous la plupart des systèmes linux), car ainsi, les informations étendues seront stockées dans l'inode du fichier ou répertoire concerné, plutôt que dans les métadonnées du système de fichiers. Il y a ainsi un gain sur le temps d'accès à l'information.

8.3. Gestion des services de messagerie

Dans ce chapitre, nous allons discuter d'une configuration comprenant un serveur SMTP local, un serveur POP/IMAP authentifié sur un annuaire LDAP. La protection contre les virus et les spams est assurée par `amavisd-new` et les briques nécessaires. Nous présupposons que l'annuaire LDAP est opérationnel.

8.3.1. Le serveur POP/IMAP Cyrus-IMAPD

Cyrus-IMAP fonctionne aujourd'hui avec une couche de sécurisation de l'authentification SASL (*Simple Authentification and Security Layer*) par défaut. L'authentification sécurisée par SASL utilise par défaut un mode d'authentification basé sur PAM.

Vous trouverez plus d'informations sur le site officiel du projet:

(`http://cyrusimap.web.cmu.edu/`)

8.3.1.1. Installation et arborescence de Cyrus-IMAPD

Trois paquets sont nécessaires :

- `cyrus-sasl` : fournit le client/serveur SASL
- `cyrus-imapd` : fournit le serveur POP/IMAP Cyrus-IMAP
- `cyrus-imapd-utils` : fournit les utilitaires de Cyrus-IMAP et notamment cyradm, l'interface d'administration du serveur.

Les versions évoluent assez peu. Toutefois, la plus grande rigueur est de mise concernant les éventuelles mises à jour de sécurité et notamment pour SASL.

Installons les paquetages requis :

```
# urpmi cyrus-sasl cyrus-imapd cyrus-imapd-utils
```

L'arborescence de Cyrus-IMAP est assez simple :

- `/etc/imapd.conf` : fichier de configuration pour l'accès aux ressources du serveur IMAP
- `/etc/cyrus.conf` : fichier de configuration de Cyrus
- `/var/spool/imap/` : répertoire de conservation des boîtes aux lettres
- `/var/log/mail` : répertoire de fichiers de journalisation

8.3.1.2. Configurer Cyrus-IMAP

Vérifions tout d'abord la liste de tous les modes d'authentification disponibles avec la version de SASL installée :

```
# saslauthd -v
saslauthd 2.1.22
authentication mechanisms: getpwent kerberos5 pam rimap shadow ldap
```

ldap apparaît bien dans cette liste. Le mécanisme utilisé pour l'authentification est spécifié dans le fichier `/etc/sysconfig/saslauthd` :

```
# cat /etc/sysconfig/saslauthd
# $Id: CS-service-messaging.xml,v 1.9 2008-09-12 14:19:36 ennael Exp $
# Authentications mechanism (for list see saslauthd -v)
```

```
SASL_AUTHMECH=pam
...
```

Par défaut, PAM est le mécanisme d'authentification activé. Remplaçons le dans ce fichier par LDAP :

```
# cat /etc/sysconfig/saslauthd
# $Id: CS-service-messaging.xml,v 1.9 2008-09-12 14:19:36 ennael Exp $
# Authentications mechanism (for list see saslauthd -v)
SASL_AUTHMECH=ldap
...
```

Il nous faut maintenant définir les éléments nécessaires pour indiquer le mode de contact de l'annuaire LDAP :

```
# cat /etc/saslauthd.conf
ldap_servers: ldap://<ip_ldap_server>
ldap_version: 3
ldap_auth_method: bind
ldap_bind_dn: cn=Manager,dc=example,dc=com
ldap_bind_pw: <password>
ldap_search_base: ou=Users,dc=example,dc=com
ldap_scope: one
ldap_filter: uid=%u
ldap_verbose: on
```

On vérifie enfin que le service est actif au démarrage. Dans le cas contraire, on le configure dans cet objectif en activant saslauthd pour les niveaux 3 et 5 :

```
# chkconfig --level 35 saslauthd on
# chkconfig --list saslauthd
saslauthd  0:Arrêt  1:Arrêt  2:Marche  3:Marche  4:Marche  5:Marche  6:Arrêt
```

Configurons maintenant Cyrus-IMAP. Il suffit de spécifier le ou les administrateurs du serveur grâce au paramètre `admins` :

```
# cat /etc/imapd.conf
configdirectory: /var/lib/imap
partition-default: /var/spool/imap
admins: imapadmin cyrus
allowanonymouslogin: no
sieveusehomedir: no
sievedir: /var/lib/imap/sieve
sendmail: /usr/sbin/sendmail
hashimapspool: true
sasl_pwcheck_method: saslauthd
sasl_mech_list: PLAIN
tls_cert_file: /etc/ssl/cyrus-imapd/cyrus-imapd.pem
tls_key_file: /etc/ssl/cyrus-imapd/cyrus-imapd.pem
```

Redémarrez le serveur :

```
# service cyrus-imapd restart
```

8.3.1.3. Tester le bon fonctionnement du serveur

Il nous faut tester dans un premier temps saslauthd et le contact de l'annuaire LDAP avec la commande `testsaslauthd` :

Vérifions le bon fonctionnement du serveur Cyrus-IMAP pour POP3 (port 110) et IMAP (port 143) :

```
# telnet 192.168.1.2 143
Trying 192.168.1.2...
Connected to imap.example.com (192.168.1.2).
Escape character is '^]'.
* OK tellure Cyrus IMAP4 v2.3.12-0.p2.4mdv2009.0 server ready
# telnet 192.168.1.2 110
Trying 192.168.1.2...
Connected to imap.example.com (192.168.1.2).
Escape character is '^]'.
+OK tellure Cyrus POP3 v2.3.12-0.p2.4mdv2009.0 server ready
<2428069223.1136796638@imap>
```

8.3.1.4. Administrer Cyrus-IMAPD

L'administration de Cyrus se fait au moyen de l'utilitaire cyradm. Dans un premier temps, on se connecte en tant qu'admistrateur du service :

```
# cyradm --user imapadmin localhost
IMAP Password:
tellure> help
authenticate, login, auth         authenticate to server
chdir, cd                         change current directory
createmailbox, create, cm         create mailbox
deleteaclmailbox, deleteacl, dam  remove ACLs from mailbox
deletemailbox, delete, dm         delete mailbox
disconnect, disc                  disconnect from current server
exit, quit                        exit cyradm
help, ?                           show commands
info                              display mailbox/server metadata
listacl, lam, listaclmailbox      list ACLs on mailbox
listmailbox, lm                   list mailboxes
listquota, lq                     list quotas on specified root
listquotaroot, lqr, lqm           show quota roots and quotas for mailbox
mboxcfg, mboxconfig               configure mailbox
reconstruct                       reconstruct mailbox (if supported)
renamemailbox, rename, renm       rename (and optionally relocate) mailbox
server, servername, connect       show current server or connect to server
setaclmailbox, sam, setacl        set ACLs on mailbox
```

```
setinfo                          set server metadata
setquota, sq                     set quota on mailbox or resource
version, ver                     display version info of current server
```

Ci-dessous les principales opérations de gestion des utilisateurs :

- ajouter un utilisateur et créer ses boites aux lettres : `cm`

```
localhost> cm user.toto
localhost> cm user.toto.sent
localhost> cm user.toto.trash
```

- détruire une boîte aux lettres :`dm`

```
localhost> dm user.toto
```

- lister les boîtes créées : `lm`

```
localhost> lm
      user.loic (\HasNoChildren)
      user.anne (\HasNoChildren)
      user.benjamin (\HasNoChildren)
```

- fixer des quotas : `sq`

```
localhost> sq 524288000 user.anne
      user.loic (\HasNoChildren)
      user.anne (\HasNoChildren)
      user.benjamin (\HasNoChildren)
```

- lister les quotas : `lq`

```
localhost> lq user.anne
 STORAGE 0/524288000 (0%)
```

- fixer des ACL : `setacl`. On utilise les ACL listées ci-dessous :

ACL	Contenu
ACL	**Contenu**
l	voir la liste des boîtes aux lettres sans leur contenu
r	lire le contenu des boîtes aux lettres
s	conserver le statut des messages « vu » et « récent » durant les sessions IMAP
w	écrire (modification des indicateurs des messages « récent », « répondu » et « brouillon »)
i	insérer un message dans la mailbox (déplacement ou copie)
c	créer des sous-boîtes dans la boîte principale (la création de boîtes principales n'étant pas accessible aux utilisateurs non administrateurs)
d	détruire un message et/ou la boîte elle-même
a	administrer la boîte aux lettres (modifier les ACL)
none	aucun droit
read	(=lrs) lire le contenu de la boîte aux lettres
append	(=lrsip) lire le contenu de la boîte aux lettres et ajouter un message dans la file
write	(=lrswipcd) lire le contenu, y poster, ajouter un message dans la file, détruire un message ou la boîte elle-même. Tous les droits sauf celui de modifier les ACL
all	(=lrswipcda) tous les droits, habituellement accordés aux propriétaires respectifs des boîtes aux lettres

Tableau 8-2. Gestion des ACL dans Cyrus-IMAP

Pour fixer des ACL, on utilise la commande suivante :

```
localhost> setacl user.mailgroup anne read
```

- lister les ACL : `lam`

```
localhost> lam user.mailgroup
      anne lrswipcda
      loïc lrswipcda
      benjamin lrswipcda
```

Pour générer les boîtes aux lettres à la volée, créez un fichier contenant l'ensemble des opérations de création de boîtes. Puis, envoyez la sortie standard de l'affichage du fichier à la commande `cyradm`.

Exemple : créons des boîtes pour les utilisateurs anne, loïc et benjamin

```
# cat liste_boites
    cm user.anne
    cm user.loic
    cm user.benjamin
# cat liste_boites |cyradm -user admin localhost
```

8.3.1.5. Boîte à outils Cyrus

Cyrus-IMAP est fourni avec un certain nombre d'outils permettant de tester et de vérifier son bon fonctionnement notamment au niveau de l'authentification :

```
# imtest -a anne localhost
S: * OK tellure Cyrus IMAP4 v2.3.12-0.p2.4mdv2009.0 server ready
C: C01 CAPABILITY
S: * CAPABILITY IMAP4 IMAP4rev1 ACL QUOTA LITERAL+ MAILBOX-REFERRALS
NAMESPACE UIDPLUS ID NO_ATOMIC_RENAME UNSELECT CHILDREN MULTIAPPEND
BINARY SORT THREAD=ORDEREDSUBJECT THREAD=REFERENCES ANNOTATEMORE IDLE
STARTTLS LISTEXT LIST-SUBSCRIBED X-NETSCAPE
S: C01 OK Completed
Please enter your password:
C: L01 LOGIN anne {8}
S: + go ahead
C: <omitted>
S: L01 OK User logged in
Authenticated.
Security strength factor: 0
```

8.3.1.6. Utiliser POP3S et IMAPS

Par défaut, `cyrus-imapd` est installé et comporte l'activation de `pop3s` et `imaps`. Il est fortement recommandé d'utiliser le protocole `IMAP` de façon sécurisée, via `SSL` sur le port 443. `IMAPS` peut être une bonne solution pour établir une solution de messagerie sécurisée.

Sous Mandriva Enterprise Server 5, lors de l'installation du démon `cyrus-imap`, IMAPS est activé par défaut. Pour cela, un certificat `SSL` a été généré automatiquement. Si vous souhaitez changer le certificat `SSL`, vous pouvez en générer un nouveau avec la commande suivante :

```
# openssl req -new -x509 -nodes -out /etc/ssl/cyrus-imapd/cyrus-imapd.pem
-keyout cyrus-imapd.pem -days 365
```

8.3.2. Le serveur SMTP Postfix

Dans cette section, nous abordons un seul cas particulier de configuration de Postfix.

8.3.2.1. Concepts de base d'un serveur SMTP

Un serveur SMTP (Simple Mail Transfer Protocol) peut être comparé à un bureau de poste. Le bureau de poste reçoit le courrier pour la zone dans laquelle il se situe et le trie. Si une lettre est destinée à une personne habitant dans la zone desservie par le bureau de poste, il la livrera lui-même dans la boîte aux lettres de cette personne. Dans le cas contraire, la lettre est envoyée au bureau de poste desservant la zone du destinataire.

Les opérations d'un serveur Postfix standard sont similaires. Il reçoit des messages du réseau local et d'autres serveurs de mail qui l'ont identifié comme gestionnaire du courrier pour un domaine donné. Le serveur lit l'adresse du destinataire et :

- si le nom de domaine correspond au domaine géré localement, le message est déposé dans la boîte correspondante.
- dans le cas contraire, le serveur recherche le serveur gestionnaire de la zone concernée et lui envoie le courrier.

Postfix s'est imposé comme le successeur de Sendmail. Postfix est plus récent et son architecture repose sur la notion de modularité.

Principales références Web :

- site officiel de Postfix (`http://postfix.org`)

- documentation officielle de Postfix (`http://www.postfix.org/documentation.html`)
- autres documentations (`http://www.postfix.org/docs.html`)

8.3.2.2. Installation et arborescence de Postfix

L'installation de Postfix est simple et se réduit à l'installation du paquet portant le même nom. Toutefois, Mandriva Enterprise Server 5 fournit un certain nombre de paquetages supplémentaires :

- `postfix-pcre` : support des PCRE (*Perl Compatible Regular Expression*) dans la configuration
- `postfix-ldap` : support des maps LDAP dans Postfix pour la gestion de l'authentification sur un annuaire ldap

L'arborescence de Postfix reflète la modularité de sa conception :

- `/etc/postfix` : répertoire contenant les fichiers de configuration du serveur
- `/var/log/mail` : répertoire contenant les fichiers de journalisation du serveur, répartis en trois fichiers (`info`, `warnings`, `errrors`) en fonction de l'importance des informations
- `/var/spool/postfix` : répertoire contenant l'ensemble des répertoires de spool relatifs au fonctionnement du serveur tel que décrit dans la section précédente.
- `/etc/sysconfig/postfix` : ensemble des options utilisées pour le démarrage des démons du serveur

8.3.2.3. Configurer le serveur Postfix

Le fichier principal de configuration est `/etc/postfix/main.cf`. Nous utiliserons ce fichier pour présenter les paramètres de base assurant le bon fonctionnement du serveur dans le cas présenté en introduction de ce chapitre :

```
# cat /etc/postfix/main.cf
# paramétrage système du serveur
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/lib/postfix
mail_owner = postfix

# nom de machine
myhostname = host.domain.com
```

```
# nom de domaine de la valeur myhostname
mydomain = domain.com
# domaine apparaissant dans le courrier envoyé de cette machine
myorigin = $mydomain

# interfaces sur lesquelles le service va pouvoir écouter (par défaut
# toutes)
inet_interfaces = all
# domaines pour lequels la machine livrera le courrier localement au
# lieu de les transmettre à une autre machine
mydestination = $myhostname, localhost.$mydomain,
 /etc/postfix/destinations
# map contenant les adresses et/ou utilisateurs locaux
local_recipient_maps = $alias_maps

# code spécifiant une réponse du serveur SMTP lorsque le domaine d'un
# destinataire correspond à $mysdestination ou lorsque l'adresse de
# destination ou l'adresse locale n'existe pas. Par défaut, le code
# est utilisé est 450, code qui propose de renouveler l'envoi (550
# pour ne pas le renouveler)
unknown_local_recipient_reject_code = 450
# réseaux autorisés à utiliser le serveur SMTP
mynetworks = 172.16.51.0/24, 127.0.0.0/8

# spécifie les bases qui seront utilisées par la commande newaliases
# pour générer la table des alias
alias_database = hash:/etc/postfix/aliases

mail_spool_directory = /var/spool/mail

# spécifie le mode de transport des mails dans le fichier master.cf
# à utiliser après avoir traité les fichiers aliases et .forward
mailbox_transport = cyrus
# bannière affichée lors de l'accès au serveur SMTP
smtpd_banner = $myhostname ESMTP $mail_name ($mail_version) (Mandrake
 Linux)

debug_peer_level = 2
debugger_command =
PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
xxgdb $daemon_directory/$process_name $process_id & sleep 5
# délai en nombre d'heures au bout duquel un avertissement est envoyé
# quand un courrier n'a pas pu être livré
delay_warning_time = 4

# autres paramétrages système du serveur
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
setgid_group = postdrop
manpage_directory = /usr/share/man
sample_directory = /usr/share/doc/postfix-2.0.6/samples
readme_directory = /usr/share/doc/postfix-2.0.6/README_FILES
```

L'autre fichier de base est `/etc/postfix/master.cf`. Il définit le fonctionnement de chacun des services fonctionnant au sein du serveur :

- `service type` : type de fonctionnement (socket TCP/IP ou UNIX)
- `private` : accès restreint au service Postfix
- `unprivileged` : service exécuté ou non sans les privilèges root
- `chroot` : service qui tourne en mode chroot
- `wakeup time` : temps au-delà duquel le processus est automatiquement réactivé
- `maxproc` : nombre maximum de processus exécutés simultanément
- `command` : commande exécutée

8.3.2.4. La boîte à outils Postfix

Postfix propose un certain nombre d'outils utiles pour l'administration quotidienne du serveur :

Vérifier la configuration

Liste l'ensemble des paramètres utilisés dans le fichier `main.cf`

```
# postconf
```

Liste uniquement les paramètres qui ont été personnalisés

```
# postconf -n
```

Valide la configuration du système de mail Postfix (fichier `main.cf`)

```
# postfix check
postfix: fatal: bad string length 0 < 1: manpage_directory =
```

Configuration du démon postfix

Démarrer | arrêter | relancer | recharger la configuration du service postfix

```
# service postfix start | stop | restart | reload
```

Forcer la livraison des messages gardés en files d'attente

```
# service postfix flush
```

Vérifier l'état du service postfix

```
# service postfix status
       master (pid 6417) est en cours d'exécution...

# ps -ef | grep postfix
```

```
root      6417     1  0 10:18 ? 00:00:00 /usr/lib/postfix/master
postfix   6422  6417  0 10:18 ? 00:00:00 pickup -l -t fifo -u -c -o
 content_filter  -o receive_override_options
postfix   6423  6417  0 10:18 ? 00:00:00 qmgr -l -t fifo -u -c
```

La commande permet de vérifier de manière précise que les différents démons qui constituent Postfix sont en état de marche. On devra voir au moins : `master`, `qmgr` et `pickup`

Gestion des maps Postfix

Recréer la map aliases.db

```
# newaliases
```

Recréer une map spécifiée

```
# postmap <map>
```

Lire le contenu d'une map

```
# postmap -q <map>
```

Gestion des files

Afficher l'ensemble du courrier en attente

```
# postqueue -p
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-------
9D3F67D5F*      338 Fri Jan  6 19:31:43  plop@plop.com
                                         anne@tellure.example.subnet

-- 0 Kbytes in 1 Request.
```

ou

```
# mailq
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-------
9D3F67D5F*      338 Fri Jan  6 19:31:43  plop@plop.com
                                         anne@tellure.example.subnet

-- 0 Kbytes in 1 Request.
```

Supprimer un message inscrit dans une liste d'attente

```
# postsuper -d <queue_ID>
#  postsuper -d  9D3F67D5F
postsuper: 9D3F67D5F: removed
postsuper: Deleted: 1 message
```

`postsuper -d ALL` permet de supprimer l'ensemble des messages en attente dans la file.

8.3.2.5. Sécuriser un serveur de messagerie

Voici quelques informations permettant de sécuriser an minimum votre serveur Postfix.

8.3.2.5.1. Postfix en mode chroot

La sécurisation de Postfix peut commencer par faire en sorte que les démons du serveur soient exécutés dans une "cage". Dans le cas de Postfix, cela signifie que les processus disposent des plus faibles privilèges possibles et d'un accès restreint à l'arborescence, soit `/var/spool/postfix`.

Le paquetage Postfix de Mandriva Enterprise Server 5 est fourni avec un script qui permet facilement d'exécuter Postfix en mode chroot (ainsi que le retour arrière sur la mise en place du chroot) : `postfix-chroot.sh`. Il exécute les points suivants :

- création de l'arborescence pour le chroot, par défaut dans `/var/spool/postfix`
- modification de `/etc/postfix/master.cf` pour spécifier l'exécution des démons en chroot
- rechargement du service

```
# /usr/sbin/postfix-chroot.sh enable
 setting up chroot at: /var/spool/postfix
copy system files into chroot
  /etc/localtime -> /var/spool/postfix/etc/localtime
  /etc/host.conf -> /var/spool/postfix/etc/host.conf
  /etc/resolv.conf -> /var/spool/postfix/etc/resolv.conf
  /etc/nsswitch.conf -> /var/spool/postfix/etc/nsswitch.conf
  /etc/hosts -> /var/spool/postfix/etc/hosts
  /etc/services -> /var/spool/postfix/etc/services
copy additional files into chroot
copy nss libraries into chroot
  /lib64/libnss_dns.so.2 -> /var/spool/postfix/lib64/libnss_dns.so.2
  /lib64/libnss_dns-2.8.so -> /var/spool/postfix/lib64/libnss_dns-2.8.so
  /lib64/libnss_nis.so.2 -> /var/spool/postfix/lib64/libnss_nis.so.2
  /lib64/libnss_nis-2.8.so -> /var/spool/postfix/lib64/libnss_nis-2.8.so
  /lib64/libnss_winbind.so.2 -> /var/spool/postfix/lib64/libnss_winbind.so.2
  /lib64/libnss_winbind.so -> /var/spool/postfix/lib64/libnss_winbind.so
  /etc/ldap.conf -> /var/spool/postfix/etc/ldap.conf
  /lib64/libnss_ldap.so.2 -> /var/spool/postfix/lib64/libnss_ldap.so.2
  /lib64/libnss_ldap-2.8.so -> /var/spool/postfix/lib64/libnss_ldap-2.8.so
  /lib64/libnss_compat.so.2 -> /var/spool/postfix/lib64/libnss_compat.so.2
  /lib64/libnss_compat-2.8.so -> /var/spool/postfix/lib64/libnss_compat-2.8.so
  /lib64/libnss_files.so.2 -> /var/spool/postfix/lib64/libnss_files.so.2
  /lib64/libnss_files-2.8.so -> /var/spool/postfix/lib64/libnss_files-2.8.so
  /lib64/libnss_files.so.2 -> /var/spool/postfix/lib64/libnss_files.so.2
  /lib64/libnss_files-2.8.so -> /var/spool/postfix/lib64/libnss_files-2.8.so
Rechargement du service de courrier Postfix :                  [  OK  ]
```

Par la suite il est important de mettre à jour le chroot lors de modifications pouvant avoir un impact sur l'environnement de messagerie. Pour vérifier la présence de telles modifications, il suffit de taper la commande ci-dessous :

```
# postfix-chroot.sh check
files /var/spool/postfix/etc/hosts and /etc/hosts differ
Rechargement du service de courrier Postfix :             [  OK  ]
```

Pour mettre à jour :

```
# postfix-chroot.sh check_update
Rechargement du service de courrier Postfix :             [  OK  ]
```

8.3.2.5.2. Sécuriser la configuration de Postfix

Dans un premier temps, positionnons un certain nombre d'options dans `/etc/postfix/main.cf`.

```
smtpd_helo_required = yes
     disable_vrfy_command = yes

smtpd_recipient_restrictions =
    reject_invalid_hostname,
    reject_non_fqdn_hostname,
    reject_non_fqdn_sender,
    reject_non_fqdn_recipient,
    reject_unknown_sender_domain,
    reject_unknown_recipient_domain,
    permit_mynetworks,
    reject_unauth_destination,
    check_recipient_access
    check_client_access dbm:/etc/postfix/client_checks,
    reject_rbl_client sbl.spamhaus.org,
    reject_rbl_client cbl.abuseat.org,
    reject_rbl_client dnsbl.sorbs.net,
    permit

smtpd_data_restrictions =
    reject_unauth_pipelining,
    # http://www.postfix.org/postconf.5.html#reject_unauth_pipelining
    permit
```

8.3.2.5.3. Filtrage à l'étape HELO

Une étape importante dans le dialogue avec un serveur SMTP est `HELO`. Un certain nombre de vérifications à ce niveau du dialogue permet d'effectuer un premier filtrage non négligeable. La configuration s'effectue dans `/etc/postfix/main.cf` :

```
smtpd_recipient_restrictions = check_helo_access
dbm:/etc/postfix/helo_checks
```

Cette directive nous permet de spécifier un nouveau fichier dans lequel apparaîtrons les filtres à appliquer. Le fichier ici est `/etc/postfix/helo_checks` :

```
# cat /etc/postfix/helo_checks
# On peut bloquer les machines qui se présentent comme faisant partie
# du domaine alors qu'elles sont à l'extérieur
example.tld REJECT You are not in example.tld

# Idem avec les adresses IP (ici l'IP du serveur de messagerie)
192.168.1.2 REJECT You are not 192.168.1.2

# Idem avec localhost
localhost REJECT You are not me
```

Il est utile de connaître les étapes du dialogue entre un client et un serveur SMTP. Cela vous permettra de détecter des niveaux éventuels de problèmes :

```
$ telnet localhost 25
Trying 127.0.0.1...
Connected to localhost (127.0.0.1).
Escape character is '^]'.
220 dhcp140.example.com ESMTP Postfix (Mandriva MES5)
HELO mandriva.com
250 mes5.example.com
Mail from test@mandriva.com
250 Ok
RCPT To: a@example.com
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
test
.
250 Ok: queued as B4DAE434B
```

L'opération se déroule en 4 étapes :

1. `HELO` : présentation de l'hôte qui contacte, le serveur SMTP répond
2. `Mail From` : adresse de l'expéditeur, le serveur SMTP valide l'adresse
3. `RCPT To:` : adresse du destinataire, le serveur SMTP valide l'adresse

4. DATA : envoi des données, le message est terminé par un ..

8.3.2.5.4. Filtrer l'expéditeur

De la même façon, utilisons la directive adaptée dans /etc/postfix/main.cf

```
smtpd_recipient_restrictions = check_sender_access
dbm:/etc/postfix/sender_checks
```

Dans /etc/postfix/sender_checks :

```
# cat /etc/postfix/sender_checks
# On bannit un domaine
# le code SMTP 554 correspond à : "Transaction failed"
domaine.org 554 Spam not tolerated here

# Un domaine est mis sur la liste noire (RBL) mais on veut quand même
# recevoir des mails de ce domaine domaine.com OK

# Pour un domaine sur la liste noire, on veut recevoir certaines adresses
someuser@example3.tld OK
example3.tld REJECT
```

8.3.2.5.5. Filtrer les destinataires

Si l'on souhaite filtrer les destinataires, par exemple une ancienne boîte aux lettres qui reçoit toujours du spam.

Dans le fichier /etc/postfix/main.cf :

```
smtpd_client_restrictions =
        check_recipient_access regexp:/etc/postfix/rcpt_restrictions
```

Dans /etc/postfix/rcpt_restrictions

```
/sales@domaine\.info/ REJECT
/bob@domaine\.info/ REJECT
```

Si l'on souhaite filtrer sur le format des adresses des destinataires. Dans le main.cf :

```
smtpd_recipient_restrictions = check_client_access
  pcre:/etc/postfix/client_checks.pcre
```

Dans le fichier /etc/postfix/client_checks.pcre :

```
/^\@/ 550 Invalid address format.
/[!%\@].*\@/ 550 This server disallows weird address syntax.
```

8.3.2.6. Utilisation avancée de Postfix

8.3.2.6.1. Support de LDAP dans Postfix

Postfix offre la possibilité d'utiliser un annuaire LDAP pour vérifier le destinataire d'un message et le lui faire parvenir. Vous devrez au préalable installer le paquet `postfix-ldap`.

La technique consiste ensuite à déclarer des maps LDAP, spécifiant le serveur LDAP, la manière d'interroger le serveur et les informations nécessaires à récupérer.

```
# cat /etc/postfix/main.cf
...
# liste d'alias utilisés pour le courrier local
alias_maps = ldap:ldapuser, ldap:ldapgroup

# maps utilisées pour l'authentification LDAP
virtual_alias_maps = ldap:ldapuser, ldap:ldapgroup

# définition des informations nécessaires pour récupérer l'adresse mail d'un
# utilisateur
ldapuser_server_host = 192.168.1.1
ldapuser_server_port = 389
ldapuser_bind = yes
ldapuser_bind_dn = cn=Manager,dc=example,dc=com
ldapuser_bind_pw = secret
ldapuser_search_base = ou=Personnes,dc=example ,dc=com
ldapuser_timeout = 60
ldapuser_query_filter = (&(objectclass=qmailuser)(mailLocalAddress=%s))
ldapuser_result_attribute = mail
ldapuser_lookup_timeout = 60

# définition des informations nécessaires pour récupérer l'adresse mail d'un
# groupe
ldapgroup_server_host = 192.168.1.1
ldapgroup_server_port = 389
ldapgroup_bind = yes
ldapgroup_bind_dn = cn=Manager,dc=example ,dc=com
ldapgroup_bind_pw = secret
ldapgroup_search_base = ou=Groupes,dc=example ,dc=com
ldapgroup_timeout = 60
ldapgroup_query_filter = (&(objectclass=mailalias)(mailAlias=%s))
ldapgroup_result_attribute = rfc822MailMember
ldapgroup_lookup_timeout = 60

# spécifie les bases qui seront utilisées par la commande
# newaliases pour générer la table des alias
alias_database = hash:/etc/postfix/aliases, ldap:ldapuser,
 ldap:ldapgroup
```

Redémarrer le serveur Postfix pour prendre en compte la modification.

8.3.2.6.2. Authentification SMTP sur Postfix

Par défaut, le serveur Postfix configuré n'acceptera que les messages provenant de son réseau. Pour autoriser une autre machine à envoyer un message à travers celui-ci, il existe différentes possibilités. Soit autoriser l'adresse IP de la machine cliente à utiliser le serveur pour envoyer le message, ou bien avoir recours à l'authentification SMTP. C'est cette deuxième possibilité que nous allons voir.

Nous allons devoir installer les paquets suivants :

```
#urpmi libsasl2 libsasl2-devel libsasl2-plug-plain libsasl2-plug-login
```

Tout d'abord, il faut générer un certificat SSL qui servira pour Postfix.

```
# mkdir /etc/postfix/ssl
# cd /etc/postfix/ssl/
# openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 1024
# chmod 600 smtpd.key
# openssl req -new -key smtpd.key -out smtpd.csr
# openssl x509 -req -days 3650 -in smtpd.csr -signkey smtpd.key -out
 smtpd.crt
# openssl rsa -in smtpd.key -out smtpd.key.unencrypted
# mv -f smtpd.key.unencrypted smtpd.key
# openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out
 cacert.pem -days 3650
```

Puis ajouter les options de configuration à Postfix dans `/etc/postfix/main.cf` :

```
# cat /etc/postfix/main.cf
smtpd_sasl_auth_enable = yes
broken_sasl_auth_clients = yes
smtpd_tls_auth_only = no
smtp_use_tls = yes
smtpd_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtpd_tls_key_file = /etc/postfix/ssl/smtpd.key
smtpd_tls_cert_file = /etc/postfix/ssl/smtpd.crt
smtpd_tls_CAfile = /etc/postfix/ssl/cacert.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom
smtpd_recipient_restrictions = permit_mynetworks
 permit_sasl_authenticated
```

Pour tester le bon fonctionnement de l'authentification TLS, vous pouvez simplement vous connecter en telnet :

```
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost (127.0.0.1).
```

```
Escape character is '^]'.
220 localhost ESMTP Postfix (Mandriva MES5)
ehlo localhost
250-localhost
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250 8BITMIME
```

Si vous voyez la ligne `250-STARTTLS` ainsi que `S: 250-AUTH` cela veut dire que l'authentification SMTP est active sur votre serveur. À partir de ce moment, seuls les utilisateurs authentifiés pourront envoyer des messages via ce serveur SMTP. De plus, l'authentification s'effectue de manière cryptée avec SSL. N'oubliez pas de configurer votre client de messagerie dans ce sens.

8.3.3. Solution anti-virus / anti-spam

Éviter les virus et le spam, c'est aussi protéger son serveur de messagerie et l'ensemble du réseau. La solution se présente de cette manière : Postfix transmet avant tout traitement les messages entrant à un service `amavisd-new`. Celui-ci, en fonction de sa configuration, traite lesdits messages au moyen d'un anti-virus ou d'un anti-spam. Une fois ces traitements terminés, les messages sont retournés dans la file entrante de Postfix, qui les traite pour les faire parvenir aux destinataires.

8.3.3.1. Installation des briques logicielles

1. Installer amavisd-new

   Il suffit d'installer le paquet `amavisd-new`. Attention le paquet tire de nombreuses dépendances, essentiellement des modules Perl.

2. Installer SpamAssassin

   Il suffit d'installer le paquetage `spamassassin`.

3. Installer clamav anti-virus

   Vous allez devoir installer les paquetages suivants : `clamav` (librairie commune utilisée pour accéder à l'antivirus), `clamd` (daemon serveur antivirus) et `clam-db` (base antivirus de clamav).

8.3.3.2. Configuration de amavisd-new

La configuration de amavis-d new consiste à spécifier les points suivants dans le fichier `/etc/amavisd/amavisd.conf` :

- domaine de messagerie
- ports d'entrée/sortie des messages
- adresse d'envoi des alertes
- traitement des spams et messages contenant des virus
- spécification de l'antivirus

```
# cat /etc/amavisd/amavisd.conf
 ...
 $mydomain = 'mondomaine.com';
...
$inet_socket_port = 10024;   # listen on this local TCP port(s)
 (see $protocol)
...
# Modifier les adresses mails pour l'envoi des rapports virus / spam
 $virus_admin = "admin\@$mydomain";
 $mailfrom_notify_admin = "admin\@$mydomain";
 $mailfrom_notify_recip = "admin\@$mydomain";
 $mailfrom_notify_spamadmin = "admin\@$mydomain";
...

# Redirection des mails vers Postfix après traitement
$notify_method  = 'smtp:[127.0.0.1]:10025';
$forward_method = 'smtp:[127.0.0.1]:10025'; # set to undef with milter
...

#Traitement des spams et virus détectés
$final_virus_destiny = D_DISCARD;
$final_banned_destiny = D_BOUNCE;
$final_spam_destiny = D_PASS;
$final_bad_header_destiny = D_PASS;
 ...

#Décommenter les lignes correspondant à clamav
['ClamAV-clamd', \&ask_daemon, ["CONTSCAN {}\n",
 "/var/lib/clamav/clamd.socket"],qr/\bOK$/, qr/\bFOUND$/,
 qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],
...

#Décommenter les lignes correspondant à clamav
@av_scanners_backup = (

  ### http://www.clamav.net/   - backs up clamd or Mail::ClamAV
  ['ClamAV-clamscan', 'clamscan',
    "--stdout --disable-summary -r --tempdir=$TEMPBASE {}", [0], [1],
    qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],
...
```

Vérifiez que le démon `clamd` est configuré pour être lancé automatiquement :

```
#chkconfig -list clamd
clamd  0:arrêt  1:arrêt  2:arrêt  3:marche  4:marche  5:marche  6:arrêt
```

8.3.3.3. Configuration de Postfix

Pour prendre en compte amavisd-new dans la configuration de Postfix, il va falloir modifier les fichiers `main.cf` et `master.cf` :

```
# cat /etc/postfix/main.cf
 ...
# traitement des messages entrants
 content_filter=smtp-amavis:[127.0.0.1]:10024
 smtp-amavis_destination_concurrency_limit=2

 # cat /etc/postfix/master.cf
 ...
 127.0.0.1:10025 inet n - y - - smtpd
 -o content_filter=
 -o smtpd_restriction_classes=
 -o smtpd_client_restrictions=
 -o smtpd_helo_restrictions=
 -o smtpd_sender_restrictions=
 -o smtpd_recipient_restrictions=permit_mynetworks,reject
 -o mynetworks=127.0.0.0/8
 -o mynetworks_style=host
 -o strict_rfc821_envelopes=yes
 -o receive_override_options=no_unknown_recipient_checks,
   no_header_body_checks
 -o smtpd_client_connection_limit_exceptions=127.0.0.0/8
 ...
```

Redémarrer Postfix pour prendre en compte la modification. Pour vérifier le bon fonctionnement :

```
 # telnet localhost 10024
 Trying 127.0.0.1...
 Connected to localhost (127.0.0.1).
 Escape character is '^]'.
 220 [127.0.0.1] ESMTP amavisd-new service ready
  # telnet localhost 10025
 Trying 127.0.0.1...
 Connected to localhost (127.0.0.1).
 Escape character is '^]'.
 220 example.com Bienvenue sur le serveur de messagerie de example.com
```

8.3.3.4. Configurer SpamAssassin

Le principal fichier de configuration est `/etc/mail/spamassassin/local.cf` :

```
# cat /etc/mail/spamassassin/local.cf
required_hits 5
rewrite_header Subject [SPAM]
report_safe 0
auto_whitelist_path        /var/spool/spamassassin/auto-whitelist
auto_whitelist_file_mode   0666
dcc_home                   /var/lib/dcc
auto_learn 1
use_razor2 1
use_bayes 1
```

La configuration est à raffiner en fonction de l'utilisation souhaitée : plus les règles de SpamAssassin sont strictes, plus on court le risque de faux positifs.

Afin d'améliorer la détection du SPAM par SpamAssassin, il est intéressant de comprendre le fonctionnement de celui-ci ainsi que les différentes directives de sa configuration. Lors de son analyse, SpamAssassin observe le courriel dans son ensemble, et va lui attribuer un pointage en fonction de différents paramètres. Par exemple, si le courriel contient beaucoup de mots-clés généralement présents dans des courriel de SPAM, le pointage augmentera. En plus de ce système, SpamAssassin utilise un système de règles complexes lui permettant de moduler ce pointage en fonction du type de courrier généralement traité par le serveur. Cela permet, via un apprentissage précis, d'obtenir une détection précise avec peu de faux positifs.

La directive `required_hits` définit le pointage requis pour qu'un courriel soit considéré comme SPAM. Dans ce cas, la directive `rewrite_header` sera prise en compte, et ajoutera la mention `[SPAM]` au sujet du courriel. La directive `use_bayes` indique à SpamAssassin d'utiliser ses différentes règles de calculs internes basées sur l'apprentissage. Tout courriel traité par SpamAssassin contiendra dans son en-tête une trace de ce traitement. Dans votre client de messagerie vous pouvez afficher ces informations.

```
X-Spam-Status: No, score=-2.6 required=5.0 tests=BAYES_00
   autolearn=disabled version=3.0.4
```

N'hésitez pas à regarder le pointage atteint par les courriels étant du spam qui n'auraient pas été détectés comme tels afin de moduler la valeur de `required_hits`. Une autre solution pour améliorer le calcul des pointages est de définir des langues préférées pour les emails. Si vous recevez beaucoup de courriels en français, mettez par exemple les directives suivantes à SpamAssassin :

```
ok_languages fr ok_locales en
```

8.3.3.5. Lancer l'auto-apprentissage de SpamAssassin

Voici un moyen supplémentaire d'affiner les règles de fonctionnement de SpamAssassin en lui envoyant vous-même les messages jugés comme étant du spam.

1. Créer une boîte accessible à tous les utilisateurs :

```
# cyradm --user cyrus localhost
IMAP Password:
localhost> cm user.SPAM
localhost> dam user.SPAM SPAM
localhost> sam user.SPAM anyone all
localhost> lam user.SPAM
anyone lrswipcda
localhost>
```

   Les utilisateurs y déplaceront tous les courriels de spam reçus sur leur compte respectif.

2. Prévoir un script qui lancera l'apprentissage à partir de ces mails, puis les détruira :

```
#Exécution de l'apprentissage
for i in /var/spool/imap/s/user/SPAM/[0-9]*.; do sa-learn
 --showdots --spam $i; done
#Suppression des messages de la boîte
rm -f /var/spool/imap/s/user/SPAM/[0-9]*.
Reconstruire la base Cyrus
su -l cyrus -c "/usr/lib/cyrus-imapd/reconstruct user.SPAM "
```

   Le script est à placer dans une `crontab` et à lancer régulièrement.

Chapitre 9. Supervision

Les logiciels de supervision permettent de surveiller les services et les réseaux en production.

9.1. Cacti

9.1.1. Présentation de Cacti

Cacti est un logiciel de supervision basé sur RRDtool permettant de surveiller l'activité de son architecture informatique à partir de graphiques de mesures. Il est plus utilisé pour la gestion de la capacité (*capacity planning*) et la métrologie (réseau, disques...) que pour la supervision en temps réel dont le rôle est généralement confié à Nagios.

Pour plus d'informations, le site Web officiel de Cacti est http://www.cacti.net/ et la documentation officielle se situe à l'adresse http://docs.cacti.net/wiki:documentation

9.1.2. Configurer le serveur pour le rendre accessible par Cacti

Il faut installer le paquetage net-snmp:

```
#urpmi net-snmp
```

Activez la supervision de tous les disques présents sur l'hôte. Il faut pour cela éditer le fichier `/etc/snmp/snmpd.conf`, rechercher la directive `disk / 10000`, commentez-là et ajoutez la ligne:

```
includeAllDisks 5
```

Terminez en lançant le service SNMP:

```
#service snmpd start
```

9.1.3. Installer et configurer un serveur Cacti

Il y a des pré-requis pour installer Cacti. Un serveur HTTP (Apache est déjà installé par défaut dans Mandriva Enterprise Server 5) et un SGBD sont utilisés. MySQL est pris comme exemple dans la suite de ce document.

Commençons par installer le paquetage Cacti:

```
#urpmi cacti
```

Il faut ensuite créer la base de données MySQL:

```
#mysql –u root
```

ou, si vous avez mis un mot de passe (fortement recommandé):

```
#mysql –u root –p
```

Et lorsque vous êtes connecté à MySQL:

```
create database cacti;
grant all on cacti.* to cactiuser@localhost identified by 'cactiuser';
flush privileges;
quit
```

Il faut enfin créer les tables de la base de données à l'aide du script SQL fourni:

```
mysql –u root cacti < /usr/share/cacti/sql/cacti.sql
```

La configuration Cacti s'effectue avec l'Installation Guide directement dans un navigateur Web à l'adresse http://IP_SERVEUR_MES5/cacti. Les choix proposés par défaut sont corrects pour une configuration classique.

Une fois la configuration effectuée, vous arrivez alors sur l'interface de connexion Cacti. Par défaut, l'identifiant ainsi que le mot de passe est « admin ». Il est demandé de changer celui-ci à la première connexion, faites-le.

Vous êtes enfin connectés à l'interface Cacti et pouvez commencer à préparer la supervision de machines. Commencez par superviser le serveur local.

L'interface de Cacti n'est pas localisée. Autrement dit, elle est uniquement en langue anglaise.

9.1.4. Superviser le serveur local

Il faut préalablement configurer le démon SNMP (cf. Configurer le serveur pour le rendre accessible par Cacti).

Connectez vous sur l'interface Web d'administration de Cacti: http://IP_SERVEUR_MES5/
et suivez ces étapes de base:

1. Ajouter un *device*

   La première étape pour la création de graphiques pour votre réseau est l'ajout d'un *device* pour chaque périphérique réseau que vous souhaitez superviser. Un *device* précise les détails importants tels que le hostname du réseau, les paramètres SNMP, et le type d'hôte.

   Allez dans le menu Devices et cliquez sur Add.

   Le premier champ Description sert à identifier le serveur pour l'utilisateur. Par contre, le Hostname doit correspondre soit au FQDN du serveur soit à son adresse IP. Choisissez ensuite le template à utiliser: dans le cas d'un hôte local, il est possible d'utiliser Local Linux Machine, mais pour vérifier le comportement du démon SNMP, utilisez plutôt ucd/net SNMP Host. La version de SNMP à utiliser est la version 2.

   Récapitulatif des choix de configuration:

   ```
   Description: Serveur Cacti
   Hostname: 127.0.0.1
   Host Template: ucd/net SNMP Host
   SNMP Version: Version 2
   Downed Device Detection: Ping and SNMP
   ```

   Une fois la sélection effectuée, cliquez sur Create. La page suivante affiche les résultats des tests SNMP et Ping.

2. Créer des graphiques pour le nouveau *device*

   Il faut maintenant ajouter les différents types de données que vous voulez superviser sur le *device*. Pour cela, cliquez sur Create Graphs for this Host et cochez les Graph Templates désirés. Vous devriez avoir la disponibilité des graphiques suivants: Traffic (bits/sec) (trafic entrant et sortant des cartes réseaux), CPU usage, Memory usage, et Available Disk Space. Lorsque votre choix est fait, cliquez sur Create.

3. Inclure le *device* dans un Arbre de Graphiques

   Pour pouvoir afficher les graphiques du nouveau *device*, vous devez l'ajouter à un Arbre de Graphiques (*Graph Trees*). Pour cela, cliquez sur le menu Graph Trees et Default Tree. Changez le Name avec un nom plus

parlant: Serveurs par exemple, puis cliquez sur Add pour ajouter un item. La page Tree Items apparaît, sélectionner Host comme Tree Item Type ainsi que Serveur Cacti, que vous avez créé précédemment, comme Host. Terminez en cliquant sur Create.

Vous pouvez maintenant visualisez le résultat en cliquant sur l'onglet du haut nommé Graphs. Sous le menu Serveurs, en cliquant sur host: Serveur Cacti, vous visualisez alors les graphiques attendus.

Attendez tout de même quelques minutes, de manière à ce que quelques données soient remontées pour pouvoir être visibles sur les graphiques.