



# Livre blanc

## Messagerie unifiée et annuaire d'entreprise avec Linux

Eric Lacroix <Eric.Lacroix@alcove.fr>

29 Septembre 2000

### Résumé

Ce livre blanc décrit une solution complète de messagerie (courrier électronique), munie d'un annuaire d'entreprise. Parmi les technologies utilisées, on trouve Linux, Exim et OpenLDAP.

*Avec les livres blancs d'Alcôve, bénéficiez de l'expérience de la première société européenne d'expertise sur les logiciels libres.*

### Copyright

Alcôve, tous droits réservés.



## Table des matières

<b>1</b>	<b>Les outils informatiques pour la communication en entreprise</b>	<b>1</b>
1.1	La multiplication des outils . . . . .	1
1.2	Vers une unification des systèmes . . . . .	1
<b>2</b>	<b>Les fonctionnalités d'un système unifié</b>	<b>3</b>
2.1	Courrier électronique . . . . .	3
2.1.1	Transport . . . . .	3
2.1.2	Consultation . . . . .	3
2.2	Annuaire d'entreprise . . . . .	4
2.3	Antivirus . . . . .	5
2.4	Fonctionnalités étendues . . . . .	5
2.4.1	Aliasing . . . . .	5
2.4.2	Forwarding . . . . .	5
2.4.3	Listes de diffusion . . . . .	5
2.4.4	Filtres spécifiques et anti-spam . . . . .	7
<b>3</b>	<b>La mise en place du système</b>	<b>8</b>
3.1	Architecture du système . . . . .	8
3.1.1	Réseau . . . . .	8
3.1.2	Matériel . . . . .	8
3.2	Système d'exploitation - Debian GNU/Linux . . . . .	8
3.3	Annuaire - OpenLDAP . . . . .	9
3.4	Transport du courrier - Exim . . . . .	10
3.4.1	Envoi . . . . .	11
3.4.2	Réception . . . . .	11
3.5	Consultation du courrier - Solid-pop3d . . . . .	12
3.6	Gestion des comptes . . . . .	12
3.6.1	Comptes Unix . . . . .	12
3.6.2	Fonctions d'administration . . . . .	12
3.7	Migration de messagerie . . . . .	13
<b>A</b>	<b>Références</b>	<b>14</b>



# 1 Les outils informatiques pour la communication en entreprise

## 1.1 La multiplication des outils

La communication dans l'entreprise par l'intermédiaire du système informatique a bien souvent été considérée et mise en place avant l'émergence de l'Internet, à l'exception du monde universitaire. Les technologies mises en place répondaient alors de manière plutôt satisfaisante aux besoins de l'entreprise.

La généralisation de l'utilisation du courrier électronique («e-mail»), dans le cadre domestique d'une part, et pour les communications inter-entreprises d'autre part, en a fait le moyen évident et universel pour envoyer des messages écrits. Par exemple, le fonctionnement asynchrone de l'*e-mail* est idéal pour les communications internationales, ne subissant pas les contraintes du décalage horaire. Beaucoup plus souple d'emploi et plus économique que le fax, cette solution est devenue aussi commune que le téléphone et bien plus rapide que le courrier postal.

Contrairement aux systèmes de messageries internes propriétaires, le courrier électronique repose sur des protocoles standards de l'Internet : SMTP, MIME, POP3, IMAP. Sous ces noms se cachent des façons d'échanger et délivrer des messages, de vérifier la présence de courrier dans une boîte aux lettres et de le rapatrier sur son poste de travail afin de le consulter.

L'efficacité du courrier électronique a progressivement convaincu les entreprises. Dans un premier temps pour les dirigeants et les cadres, puis son utilisation s'est généralisée à toutes les catégories de salariés dont le poste de travail est équipé d'un micro-ordinateur.

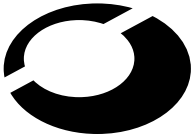
Cependant, l'utilisation du courrier électronique (e-mail) cohabite encore souvent avec le système de messagerie interne pré-existant. On y trouve deux raisons principales : l'entreprise ne souhaite pas que tous ses collaborateurs aient une adresse e-mail sur l'Internet ; les systèmes de messageries internes offrent des services d'annuaire d'entreprise, ce qui n'est pas le cas de l'e-mail, du moins de manière standard.

La cohabitation de ce double service a cependant de lourdes conséquences en termes d'administration des systèmes : plus de demandes de création de comptes, de changements de mots de passe perdus, de pannes à résoudre etc. ...

## 1.2 Vers une unification des systèmes

Alors que la messagerie interne était gérée par le service informatique de l'entreprise, la gestion du courrier électronique (sur Internet) était souvent confiée à une société de services qui possédait la technologie pour offrir cette prestation (principalement l'accès au réseau Internet).

La définition d'un standard Internet d'annuaire électronique et le développement d'outils sur ce standard permettent depuis quelques années à des applications utilisant le standard de l'*e-mail* de fournir les mêmes fonctionnalités que les systèmes spécialisés de messageries internes : une gestion simple (création, modifications d'informations diverses, fermeture de compte), un accès public ou restreint à un annuaire des adresses électroniques.



Ce livre blanc décrit une solution à base de logiciels libres, interfaçables avec des logiciels avec lesquels sont dorénavant familiers les utilisateurs de micro-ordinateurs et stations de travail. Cette solution permet de factoriser l'administration d'une messagerie à la fois pour la communication interne et pour Internet.

Le système dans son ensemble fournit les services SMTP (envoi et réception du courrier), POP3 (consultation du courrier par des logiciels tels que Netscape Communicator ou Outlook), LDAP (annuaire contenant les informations des utilisateurs du courrier électronique). Ce système peut être configuré pour fournir l'*aliasing* (une boîte aux lettres correspond à plusieurs adresses), le *forwarding* (le courrier destiné à une adresse est redirigé vers une ou plusieurs adresses, adresse initiale y compris). Des listes de diffusion (*mailing-lists*) peuvent être également gérées.



## 2 Les fonctionnalités d'un système unifié

Ce chapitre décrit les fonctionnalités qu'un système de messagerie électronique moderne doit fournir et qui peuvent être mises en place avec des outils libres.

### 2.1 Courrier électronique

#### 2.1.1 Transport

Le système repose sur les protocoles standards de courrier électronique de l'Internet. Ceci comprend le transport des messages (émission, réception), la désignation et la localisation des correspondants (adresses *e-mail*).

Les utilisateurs doivent pouvoir échanger du courrier électronique, aussi bien en interne (entre personnes de l'entreprise) qu'avec des correspondants extérieurs.

Le système permet la réception de courriers destinés à l'entreprise que l'on distingue par un ensemble de noms de domaines désignant la société, préalablement définis. Le nom de domaine est la partie de l'adresse électronique à droite du symbole "@". Il peut arriver qu'un message qui est adressé à un autre domaine que ceux de la société arrive sur le système. Dans ce cas le message est retourné à son expéditeur avec une note lui indiquant que le nom de domaine n'est pas accepté sur ce serveur.

Il n'est pas nécessaire de fournir un mot de passe au système pour envoyer un message. Afin que le serveur ne soit pas utilisé de manière abusive par une personne extérieure à l'entreprise, il n'accepte de traiter que les courriers émis à partir d'un poste de travail de la société ou à destination de la société.

Le logiciel chargé de rendre ces services est un *serveur SMTP*<sup>1</sup> ou *MTA*<sup>2</sup>.

#### 2.1.2 Consultation

La majorité des logiciels utilisateurs destinés à lire et envoyer des messages (*MUA*<sup>3</sup>) supportent le protocole *POP3*<sup>4</sup>. L'utilisateur peut consulter sa boîte aux lettres périodiquement. De petits programmes tels que *Netscape Notifier* ou *XBiff* peuvent interroger à intervalles réguliers le serveur *POP3* pour tenir l'utilisateur informé de l'arrivée de nouveaux messages. Le serveur *POP3* permet, après que l'utilisateur se soit identifié par un *login* et un *mot de passe*, de rapatrier et lire les nouveaux messages sur le *MUA* de son choix. En général le *MUA* permet de mémoriser le *login* et le *mot de passe* afin de ne pas les saisir à chaque requête faite au serveur *POP3*.

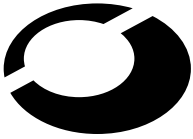
---

<sup>1</sup>**SMTP** (*Simple Mail Transport Protocol*) : protocole utilisé par les *MTA* pour communiquer sur l'Internet.

<sup>2</sup>**MTA** (*Mail Transport Agent*) : terme générique pour désigner un serveur de courrier électronique, chargé du transport, c'est-à-dire l'émission à travers le réseau, la réception, et le stockage dans des boîtes aux lettres. Sur l'Internet, les *MTA* communiquent par le protocole *SMTP*.

<sup>3</sup>**MUA** (*Mail User Agent*) : terme générique pour désigner un logiciel de courrier électronique. C'est le programme utilisateur de gestion du courrier utilisé pour consulter et envoyer des courriers électroniques.

<sup>4</sup>**POP3** (*Post Office Protocol*) : protocole pour le rapatriement du courrier par les utilisateurs.



Une personne de l'entreprise en déplacement, peut par une connexion à l'Internet par l'intermédiaire d'un fournisseur d'accès Internet (FAI) consulter son courrier professionnel, en interrogeant le serveur POP3 de l'entreprise.

## 2.2 Annuaire d'entreprise

Le système doit répondre au besoin de recherche d'une adresse *e-mail* d'un membre de l'entreprise. Un annuaire centralisé, consultable par des outils conviviaux permet d'obtenir un complément d'information, à propos d'un nom, d'un *e-mail*, ou d'une fraction de l'un d'eux. La norme LDAP<sup>5</sup> définit un protocole correspondant à ces besoins. Le composant *Messenger* de *Netscape Communicator* permet par exemple de consulter et d'effectuer des recherches sur ce type d'annuaires (*Outlook* ainsi que des logiciels libres tels que *Mozilla* offrent le même type de fonctionnalités). La figure 2.1 (gauche) donne un exemple de liste d'utilisateurs, obtenue avec le carnet d'adresse de Netscape Communicator. La figure 2.1 (droite) montre le détail d'une fiche renseignant un utilisateur.

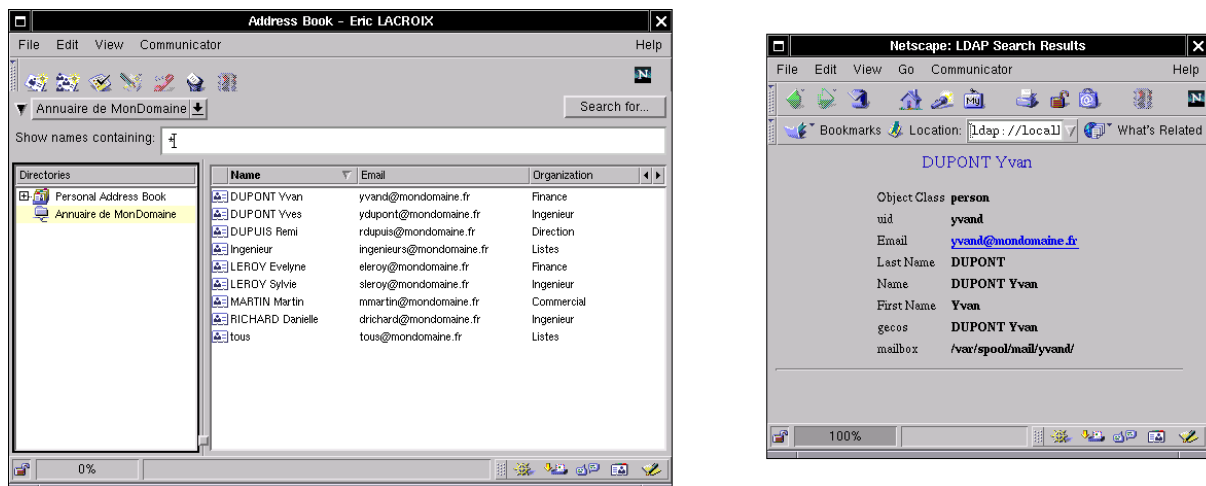


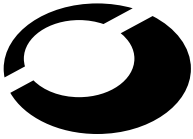
FIG. 2.1 – Détails d'une entrée de l'annuaire sous Netscape 4.7

Cet annuaire électronique n'est en général accessible que depuis le réseau interne de l'entreprise. Il contient toutes les informations concernant la messagerie. Les serveurs SMTP et POP3 l'utilisent pour valider une adresse électronique, pour localiser la boîte aux lettres sur le serveur (*pool*<sup>6</sup> de mails) et pour l'authentification des utilisateurs lors de requêtes POP3. Il est aussi utilisé pour la gestion des *alias* et du *forwarding* (voir la section sur les fonctionnalités étendues).

Une partie des informations contenues dans l'annuaire est sensible, ou n'a en tout cas de sens que pour le système. L'utilisateur ne doit pas avoir accès à de telles informations.

<sup>5</sup>**LDAP** (*Lightweight Directory Access Protocol*) : protocole léger pour accéder à des annuaires. C'est une norme ISO qui est optimisée pour la consultation, à la différence des systèmes de bases de données qui doivent être performants en écriture également.

<sup>6</sup>**Spool** : répertoire ou ensemble de répertoires dans lequel sont stockés les courriers électroniques de manière temporaire. Il existe un *spool* utilisateur, où sont stockés les *e-mails* avant d'être consultés ; et un *spool* système pour les courriers en cours de traitement (transport).



Tout logiciel qui supporte LDAP permet de consulter cet annuaire. Les utilisateurs ont ainsi un choix d'outils de recherche puissants (recherche par nom, ou partie du nom, par adresse électronique, par service, etc. ).

## 2.3 Antivirus

Si les systèmes Unix ou Linux ne sont pas la cible des virus informatiques, il existe néanmoins des outils pour détecter la présence de virus s'attaquant à d'autres systèmes. Ils sont inclus dans les fichiers délivrés par la messagerie.

Le logiciel libre *Amavis* permet d'interfacer un serveur de mails sous Linux avec des antivirus commerciaux, proposés par des sociétés telles que *McAfee* ou *Sophos*, afin de filtrer les messages contenant des scripts (*Visual Basic*, *JavaScript*) ou des programmes attachés pouvant attaquer des environnements *Windows* ou *MacOS* par exemple. L'antivirus *viruswall* de *Trend micro* a la particularité de mettre à jour automatiquement sa base de virus.

Le comportement du système lors de la détection de virus peut être paramétré : effacer le message sans autre opération, délivrer tout de même le message en informant son destinataire et/ou l'administrateur système, mettre le message en attente et avertir l'administrateur.

## 2.4 Fonctionnalités étendues

Au-delà du fonctionnement élémentaire (transport et consultation du courrier), on retrouve les possibilités offertes sur les systèmes de courrier électronique des systèmes Unix : *aliasing*, *forwarding*, listes de diffusion, filtres etc.

### 2.4.1 Aliasing

L'*aliasing* consiste à associer plusieurs adresses électroniques à une même boîte aux lettres, c'est-à-dire à un même compte utilisateur.

L'exemple de la figure 2.2 montre que Rémi DUPUIS a deux adresses *e-mail*. Que l'une ou l'autre soit utilisée (i.e. *rdupuis@mondomaine.fr* ou *pdg@modomaine.fr*) pour lui écrire, il trouvera le message dans son unique boîte aux lettres.

Des outils d'administration permettent de définir ou effacer les *alias* d'un utilisateur.

### 2.4.2 Forwarding

Le *forwarding* consiste à rediriger le courrier vers une ou plusieurs nouvelles adresses. Le cas le plus typique se présente lorsqu'un collaborateur quitte la société ou qu'il dispose d'un autre compte *e-mail* autre part et qu'il préfère utiliser.

Il est également possible, en mettant l'adresse originale dans la liste des nouvelles adresses de garder une copie du courrier sur la messagerie de l'entreprise.

### 2.4.3 Listes de diffusion

On parle ici de listes de diffusion dans le sens où un message que l'on envoie à une unique adresse est distribué à un ensemble de personnes.

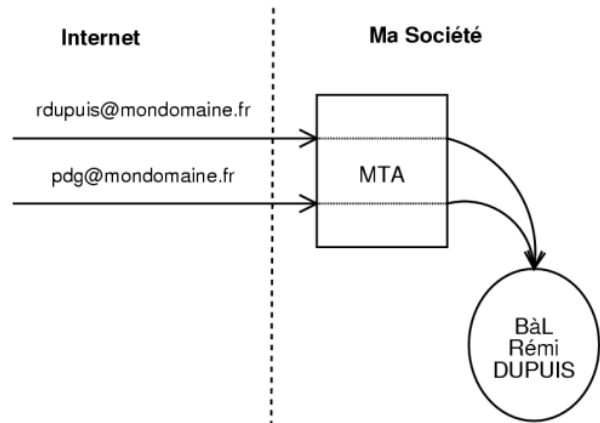
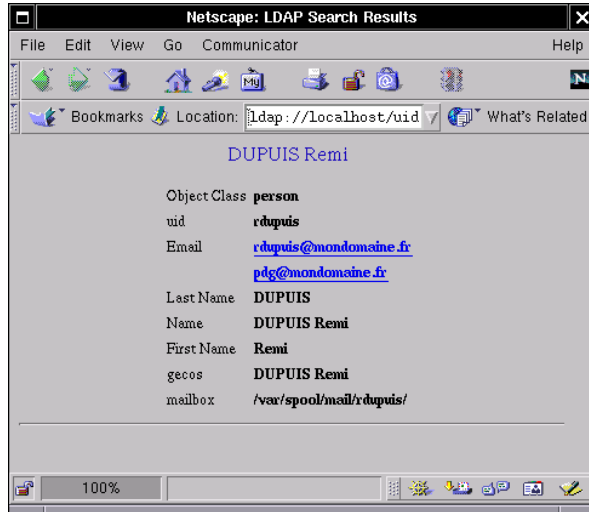


FIG. 2.2 – Adresse «aliasée»

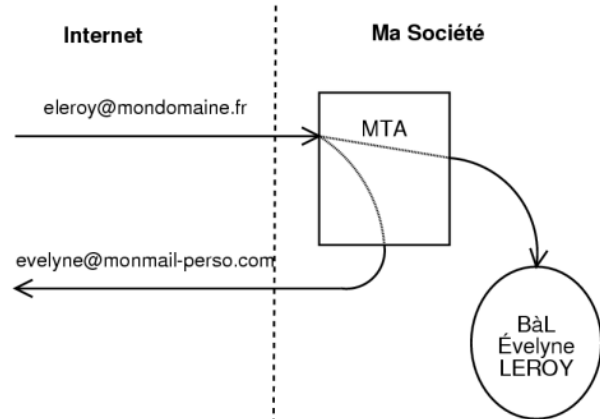
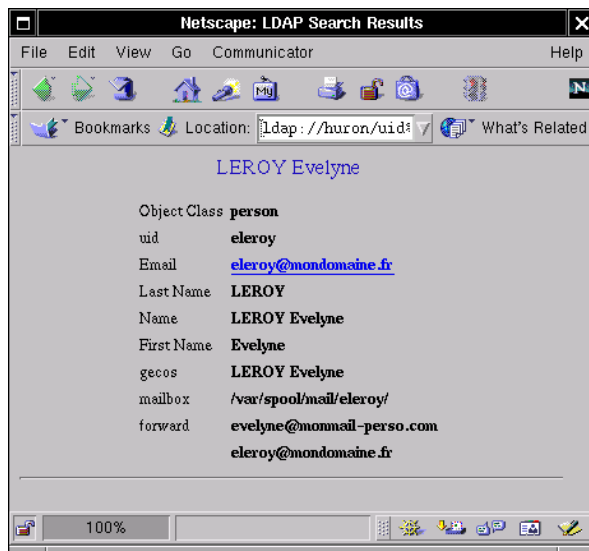


FIG. 2.3 – Message «forwardé»



Des outils d'administration permettent de définir des listes, d'ajouter ou retirer des adresses à ces listes, de connaître les listes définies et leurs membres.

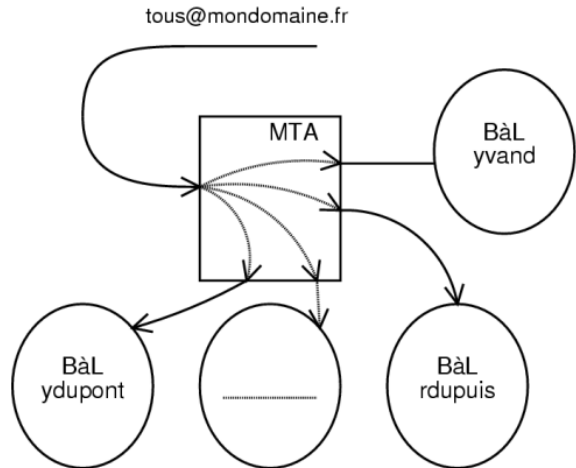
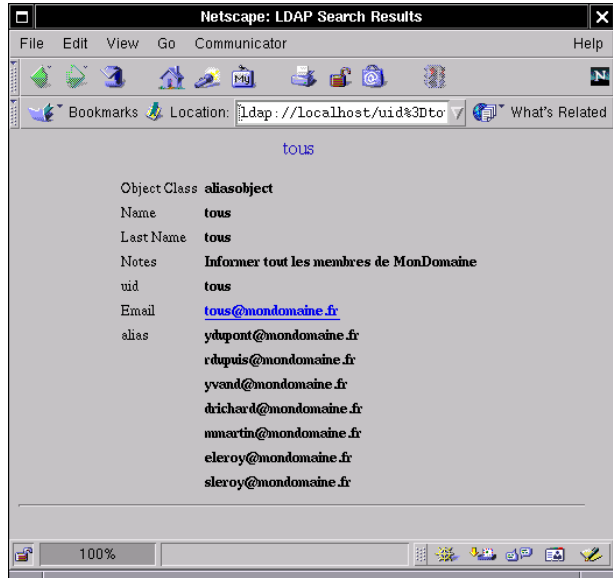


FIG. 2.4 – Envoi à une liste de diffusion

#### 2.4.4 Filtres spécifiques et anti-spam

Il existe de nombreuses possibilités de filtrage du courrier passant par le système de messagerie : filtrage sur l'émetteur du message, le destinataire, sur la taille des messages ou à partir de toute autre information qui se trouve dans l'annuaire.

Le mot *spam* est utilisé couramment dans le sens de message non-sollicité. En effet, certaines personnes utilisent de manière abusive le courrier électronique, à des fins publicitaires ou mal intentionnées.

Un mécanisme de filtrage particulier permet de mettre en place des mesures anti-*spam*, à l'aide de serveurs spécialisés situés sur Internet qui répertorient des adresses IP connues pour être à l'origine de *spams*. Ces serveurs sont aussi connus sous le nom de listes noires ou *RBL* (Realtime Blackhole List).

Un autre filtrage possible pour des raisons de sécurité, consiste à refuser les messages destinés aux listes de diffusion provenant de l'extérieur.



## 3 La mise en place du système

### 3.1 Architecture du système

#### 3.1.1 Réseau

Une architecture possible consiste à utiliser un Firewall<sup>1</sup> à trois pattes, c'est-à-dire avec le réseau local protégé, sans connexion directe avec l'Internet, et disposant d'une DMZ<sup>2</sup> (zone démilitarisée, troisième patte du Firewall) sur laquelle sont placés les services Internet (serveur Web, forum de discussions etc. ).

Concernant la messagerie, un serveur principal, fournissant tous les services de la messagerie, l'annuaire et hébergeant les boîtes à lettres est placé sur le réseau local. Les échanges avec l'extérieur, que se soit la réception ou l'envoi de messages ou bien la consultation de courrier à distance, s'effectuent par l'intermédiaire d'une machine relais placée sur la DMZ. Ainsi, aucune connexion directe n'est possible entre le réseau local et l'Internet, le service de messagerie a le même niveau de protection que le reste des applications internes.

#### 3.1.2 Matériel

Le choix d'une technologie *Intel* est convenable en raison de son bon rapport performances/prix et le très bon support de Linux pour cette plate-forme et ses périphériques. Il faut s'assurer que le matériel choisi est compatible avec le système (ce qui est constaté dans la majorité des cas).

La machine relais peut être une machine assez légère puisqu'elle n'effectue que peu de traitements, le serveur local, quant à lui, doit être correctement dimensionné en fonction des besoins de l'entreprise.

La disponibilité du système est assurée principalement par un système de disques SCSI redondants (RAID 5 et/ou RAID 1), un système de sauvegardes de type DAT pouvant également être mis en place. Des solutions de serveurs redondants peuvent être également envisagées. Pour plus d'informations sur les solutions haute-Disponibilité on peut consulter le livre blanc Alcôve sur la haute-Disponibilité.

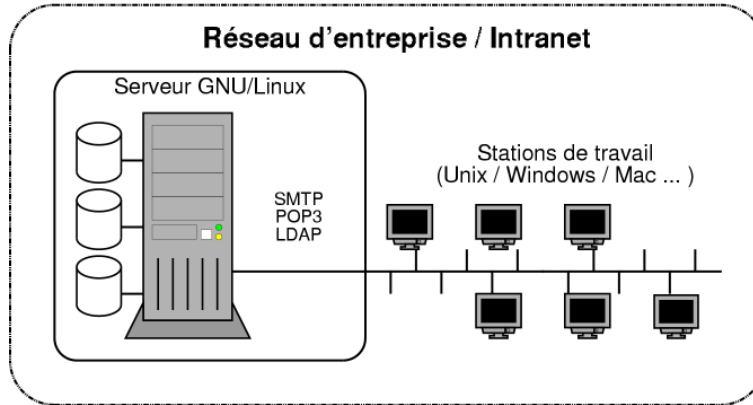
### 3.2 Système d'exploitation - Debian GNU/Linux

La distribution Linux **Debian GNU** <sup>3</sup> /**Linux** version 2.2 (aussi appelée Potato) à été choisie. Elle est en effet une des mieux adaptées pour la mise en place de serveurs d'entreprise. Son utilisation se justifie par sa fiabilité, la puissance du système de gestion de paquets. Le système de packaging Debian (deb) est très performant. Il gère efficacement les dépendances entre les paquets : à l'installation d'un paquet, un logiciel (*apt-get*) propose d'installer automatiquement les paquets nécessaires dont dépend celui-ci.

<sup>1</sup>**Firewall** : passerelle entre deux ou plusieurs réseaux qui filtre les flux de données.

<sup>2</sup>**DMZ** : réseau local où les flux entrant et sortant sont moins filtrés. Typiquement, une DMZ possède des adresses IP visibles depuis l'Internet.

<sup>3</sup>**GNU** (*GNU's Not Unix* (GNU N'est pas Unix)) : nom du projet initié par Richard Stallman en 1984 qui consiste à reprogrammer un système compatible Unix sous une licence qui en permet la libre distribution. Cette licence est la **GPL** (*GNU General Public License*) : elle permet la libre utilisation, libre modification, et la libre redistribution des logiciels, et impose de fournir le code source des binaires rendus publics.



Il faut recompiler le noyau Linux spécialement pour cette solution, avec le support natif du contrôleur RAID utilisé et entre autre, le système de fichiers journalisé *ReiserFS*. Afin d'accroître la sécurité et la stabilité du système, les fonctionnalités qui ne sont pas nécessaires sont aussi désactivées.

Le système de fichiers *ReiserFS* a été retenu car il s'avère bien plus performant que le classique *ext2* (système de fichiers standard de Linux) quand un grand nombre de fichiers sont manipulés. De plus, la fonctionnalité de journalisation<sup>4</sup> permet un redémarrage beaucoup plus rapide du système en cas d'arrêt impromptu (panne de courant par exemple). Le format de boîtes aux lettres utilisé est MailDir qui, à la différence du plus courant MBox qui stocke les *e-mails* d'un compte dans un seul fichier, utilise un fichier par message. Le format MailDir permet un accès concurrent à plusieurs courriers d'un même utilisateur. Lors de la consultation d'un courrier (impliquant l'ouverture du fichier contenant ce courrier), un verrou est posé et interdit un autre accès au fichier. Avec MBox l'incorporation d'un nouveau message suite à sa réception ne peut pas se faire si le destinataire est en train de demander la consultation de son courrier. Le courrier en cours de réception est alors mis en attente par le MTA jusqu'à la levée du verrou. Ceci a pour effet d'augmenter le nombre de traitements lors de la réception du courrier et augmente la charge de la machine.

### 3.3 Annuaire - OpenLDAP

Depuis quelques années, la norme LDAP (*Lightweight Directory Access Protocol*) se voit de plus en plus utilisée et implémentée. Les annuaires LDAP permettent par exemple de remplacer NIS ou NIS+ utilisés couramment sous Unix, ou bien encore NDS de Novell, ou l'annuaire NT, implémentations propriétaires de LDAP. Les annuaires basés sur LDAP permettent l'authentification des utilisateurs, mais leur champ d'application est bien plus vaste.

De nombreuses applications savent interroger les annuaires LDAP, que ce soit *Netscape Communicator* en passant par le serveur de courriers électroniques *Exim*. De plus, une bibliothèque Unix/Linux (*libpam.so*) permet à des applications qui utilisent un système d'authentification PAM (Pluggable Authentication Modules) d'interroger un annuaire LDAP sans modification de l'application. Il suffit de configurer PAM pour qu'il ait une correspondance entre le couple *login/password* demandé par l'application et deux attributs de l'annuaire. Il peut être intéressant de modifier une application qui utilise PAM pour qu'elle fasse ses requêtes

<sup>4</sup>**Journalisation** : elle assure que toute mise à jour des données est stockée dans un journal de transactions avant d'être écrite sur le disque. Un système de fichiers journalisé permet de retrouver les données intactes, après un crash, et réduit le temps de redémarrage des serveurs.



directement à la base LDAP et gagner ainsi en performance. La complexité d'une telle modification dépend du logiciel considéré.

On retiendra le serveur OpenLDAP version 2 qui est une implémentation libre de la norme LDAP v3, développée à partir du code original de l'*Université du Michigan*. Il offre de bonnes performances, est évidemment libre d'utilisation et de modification puisque sous licence OPL (OpenLDAP Public Licence). Il est de plus un des seuls serveurs LDAP à respecter totalement la norme.

Les données d'un annuaire LDAP sont organisées en arbre qui, par exemple, peut représenter la structure de l'entreprise.

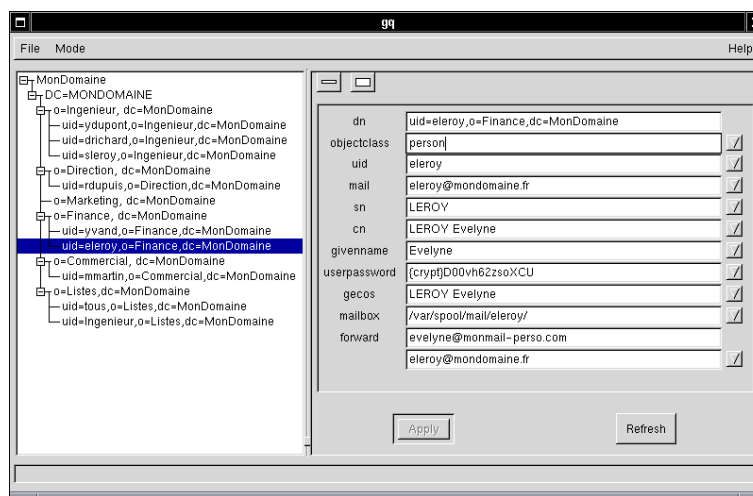


FIG. 3.1 – Exemple de représentation d'annuaire

Les informations que nous devons trouver dans l'annuaire pour le service de courrier électronique sont :

- les *login* et mot de passe pour l'authentification d'un utilisateur,
- le *login* servant à désigner la boîte aux lettres,
- le chemin d'accès au *pool* de *mail*,
- une adresse *e-mail* associée au compte *e-mail*.

En plus de ces informations minimales, on peut ajouter des adresses *e-mails* supplémentaires, une listes d'*alias* et/ou d'adresses vers lesquelles faire suivre le courrier (*forward*).

Les informations énumérées précédemment sont celles utiles ou nécessaires au système. Les utilisateurs, eux, ont besoin d'un complément d'information. Dans cette optique le choix est infini, mais de manière classique, il est fait figurer dans l'annuaire nom, prénoms, service. À ces informations peuvent être facilement ajoutés, la fonction, le numéro de téléphone, de fax, bureau de la personne etc.

## 3.4 Transport du courrier - Exim

Le MTA *Exim* (Mail Transport Agent ou agent de transport de courrier) est un serveur SMTP (Simple Mail Transport Protocol, protocole de courrier électronique de l'Internet) compatible au niveau de la ligne de commande avec *Sendmail*, certainement le MTA le plus utilisé du monde Unix. Exim sait interroger un



certain nombre de sources d'information, dont les annuaires LDAP. De plus, il sait délivrer le courrier dans des *spools* au format MBox ou MailDir.

Une grande qualité d'Exim est son fichier de configuration : il est clair et structuré, sa lecture n'est pas une tâche ardue, contrairement à la difficulté légendaire de la configuration de Sendmail. Ceci facilite la maintenance et l'ajout de fonctionnalités au service de courrier électronique.

De plus, Exim offre de bonnes performances (meilleures que Sendmail en nombre d'*e-mails* traités et en charge de la machine).

### 3.4.1 Envoi

L'envoi de courrier se fait à partir d'un client SMTP (MS Outlook, Netscape Communicator, ou des logiciels libres tels que Mutt, KMail et Evolution) configuré pour utiliser la machine serveur mise en place. Il suffit d'indiquer à son logiciel le nom du serveur SMTP.

Le serveur Exim est généralement configuré pour n'accepter de relayer que les *e-mails* provenant de l'intranet (le réseau étant isolé du reste par le FireWall, le cas contraire ne se présente pas) et le traite de deux manières différentes, qu'ils soient adressés à une adresse locale ou distante.

Dans le cas d'une adresse locale, voir le paragraphe concernant la réception du courrier.

Si l'adresse du ou des destinataires est distante, le message est envoyé (par SMTP) au relais de *mail* sur la DMZ faisant également tourner Exim. Le relais se charge alors de délivrer le courrier à bon port.

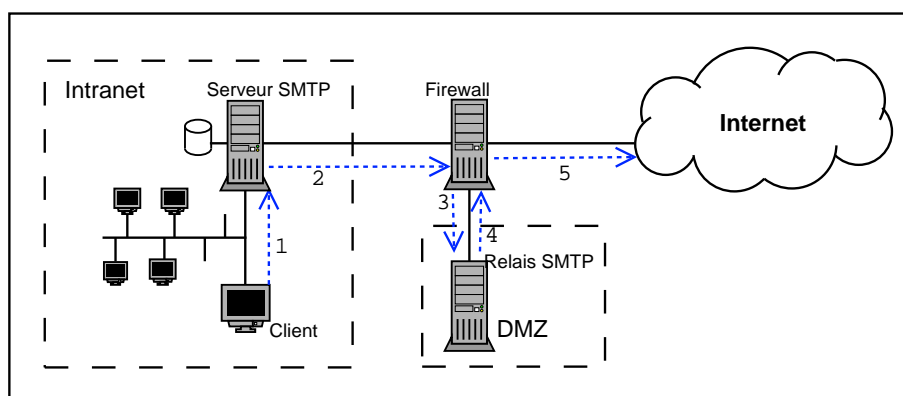


FIG. 3.2 – Envoi d'un e-mail à l'extérieur

Le relais Exim est configuré pour ne traiter que le courrier qui lui est envoyé par le serveur local, ou pour envoyer au serveur local le courrier à destination de l'entreprise provenant de l'Internet. En aucun cas, le relais ne peut être utilisé par un client Netscape ou Outlook directement (par exemple pour éviter qu'un individu connecté à l'Internet, utilise le relais de l'entreprise pour envoyer son courrier).

### 3.4.2 Réception

Il existe deux cas de réception de courrier :

- Le premier cas est celui où l'*e-mail* provient de l'entreprise. Dans ce cas, Exim délivre directement le courrier dans le *pool* local du destinataire, s'il existe, ou bien retourne un message d'erreur à l'expéditeur.



- Le second cas concerne la réception de messages provenant de l'Internet. Le relais de courrier électronique ayant été configuré dans le DNS <sup>5</sup> comme MX <sup>6</sup> pour le ou les domaine(s) de la société. Il reçoit donc le courrier à destination de l'entreprise, et le redirige vers le serveur du réseau local, qui se charge ensuite de vérifier l'existence de l'utilisateur et de livrer le courrier dans le *spool* correspondant.

### 3.5 Consultation du courrier - Solid-pop3d

La consultation du courrier se fait en interrogeant un serveur POP3. Un serveur POP3 utilisable dans le contexte décrit est **Solid-pop3d** car il répond à deux contraintes : le support du format MailDir et la possibilité d'interroger un annuaire LDAP grâce à son support PAM.

Alcôve a modifié Solid-pop3d pour lui permettre de prendre une identité générique. Cette identité générique est celle utilisée pour l'accès aux fichiers dans lesquels sont stockés les *e-mails* (voir section suivante à propos du compte générique).

## 3.6 Gestion des comptes

### 3.6.1 Comptes Unix

Le serveur de courrier électronique étant dédié à cette application, il n'est pas nécessaire que les abonnés à la messagerie aient un compte utilisateur sur la machine.

Un compte générique verrouillé est utilisé pour l'accès aux boîtes aux lettres afin de faciliter l'administration et renforcer la sécurité en réduisant au strict minimum le nombre d'utilisateurs pouvant se connecter (utilisation standard du système). Les serveurs POP3 et SMTP prennent cette identité pour consulter ou déposer un message.

### 3.6.2 Fonctions d'administration

Toutes les opérations d'administration peuvent se faire par des scripts écrits en langage Python ou Perl, et pouvant s'exécuter sur toute machine Unix de l'intranet disposant d'un interpréteur Python (ou Perl) et du module LDAP correspondant au langage utilisé.

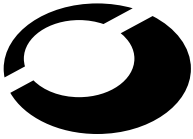
Ces scripts peuvent être adaptés ou étendus en vue d'une utilisation sous forme de scripts CGI <sup>7</sup>, pour le développement d'une interface d'administration par le Web. Ceci implique également de disposer d'un serveur web *Apache* pour exécuter ces scripts.

De manière similaire, une interface d'administration et de consultation par le web, reposant sur des scripts PHP par exemple, peut être développée.

<sup>5</sup>**DNS** (*Domain Name System*) : service réparti sur l'Internet qui permet d'associer un nom de machine (ex : www.mondomaine.fr) à une adresse du protocole internet, IP (ex : 192.16.2.19), et vice-versa.

<sup>6</sup>**MX** (*Mail Exchanger*) : c'est une entrée dans la base DNS d'un domaine. Elle désigne la machine qui traite le courrier destiné à ce domaine (ex : le MX de mondomaine.com est mail.mondomaine.com, et le MX de mondomaine.fr est aussi mail.mondomaine.com). On dissocie ainsi les noms des serveurs des noms de domaines pour le courrier électronique.

<sup>7</sup>**CGI** (*Common Gateway Interface*) : protocole d'exécution de programmes sur un serveur Web selon l'URL demandée par le client, laquelle est souvent provoquée par la validation d'un formulaire HTML.

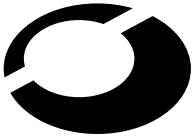


### 3.7 Migration de messagerie

Des méthodes pour récupérer les courriers d'un système de messagerie rendu obsolète peuvent être étudiées. De manière générale, il faut que l'on puisse disposer de la liste des *logins* et *mots de passe* de comptes concernés, ou bien pouvoir accéder directement aux répertoires contenant les boîtes aux lettres.

La migration peut se faire de manière pratiquement transparente pour les utilisateurs, sans interruption du service de plus de 5 ou 10 minutes.

Enfin, certains MUA permettent de ne pas effacer les *e-mails* sur le serveur après leur récupération, les utilisateurs peuvent ainsi retrouver d'anciens messages.



## A Références

- OpenLDAP - <http://www.openldap.org/>
- Exim - <http://www.exim.org/>
- Solid-Pop3d - <http://solidpop3d.pld.org.pl/>
- The Internet Engineering Task Force - <http://www.ietf.org/>
- Debian - <http://www.debian.org/>
- Python - <http://www.python.org/>
- Perl - <http://www.perl.org/>
- Apache - <http://www.apache.org/>
- RealTime BlackHole List - <http://mail-abuse.org/rbl/>
- GNU - <http://www.gnu.org/>
- AMaVIS - <http://www.amavis.org/>
- Sophos - <http://www.sophos.com/>
- McAfee - <http://www.mcafee.com/anti-virus/>
- Trend micro - <http://www.antivirus.com/>