INTRODUCTION

A l'instar des deux grandes révolutions qui ont eu lieu dans le passé, le 21ème siècle se caractérise par une profonde mutation des pratiques et la révolution du savoir et du savoir partagé. Ces mutations axées sur l'information ont profondément affectées les mœurs, les usages, les façons d'être et d'agir des populations du monde entier. Les outils d'accès et de partage de l'information se sont développés à tel point qu'on entrevoit que d'ici les dix prochaines années, le web offrira à ses utilisateurs tous les services usuels.

En effet, la tendance technologique met les réseaux Internet et intranet au cœur de tout développement fiable car leur adoption crée au sein de nos sociétés une révolution des pratiques, une meilleure gestion du temps et des ressources. Administrations, Organismes, Société Privée, Vie sociale et personnelle, aucun domaine ne peut se tenir à l'écart et demeurer performant.

C'est dans cette optique que nous avons décidé de placer l'Administration Générale du Gouvernement au sein des administrations modernes de notre époque.

L'analyse des besoins exprimés par les utilisateurs révèle bien un besoin de travail collaboratif et une gestion efficace des tâches quotidiennes. C'est dans cette optique que nous avons décidé de mettre en place un système de messagerie pour faciliter les échanges de données entre les utilisateurs.

Il existe bien des solutions payantes comme Exchange Server de Microsoft qui comportent toutes les fonctionnalités mais également des solutions libres comme Postfix qui est le système de messagerie le plus puissant, sécurisé et largement utilisé de nos jours.

L'étude de notre choix se portera sur Postfix non seulement à cause des nombreux avantages qu'il offre mais parce qu'il fonctionne sous Linux qui est un système d'exploitation robuste et libre.

GENERALITE

A- Les Composants d’un système de Messagerie

On compte trois composants dans un système de messagerie. Ils sont :

L’UA (User Agent), est le programme utilisé par le client pour composer, envoyer et recevoir les messages. Pour la composition et l'envoi des messages, il existe des programmes comme mail sous Linux. D'autres programmes sont utilisés comme Eudora, Netscape, kmail.... On appelle souvent l'UA un “ mailer local ” si on utilise des outils comme Eudora, Outlook, Mutt, Kmail ou un “ webmail ” si on utilise un navigateur comme Mozilla, Netscape ou Internet explorer pour consulter sa messagerie. Ces outils utilisent des protocoles différents. Les protocoles utilisés sont SMTP ou UUCP pour envoyer, et POP3, IMAP, POP3s, IMAPs pour recevoir.

Le MTA (Message Transfert Agent), est un agent de routage (sendmail, MS eXchange...) et un agent de transport (SMTP, UUCP). L'agent de routage a pour but d'acheminer le message, en fonction de l'adresse vers son destinataire. Pour nous, avec l'environnement Linux, l'agent de routage est sendmail. L'agent de transport reçoit un message et une direction. Il ne prend aucune décision sur la route à utiliser. Pour nous, le protocole de transport peut être SMTP ou UUCP. Le logiciel Sendmail assure les deux fonctions de transport et de routage.

Le DA (Deliver Agent), est utilisé pour la remise physique du courrier entrant dans la boîte aux lettres de l'utilisateur (BAL). Sous Linux, nous utilisons procmail.

B- Les protocoles

SMTP

Le protocole SMTP (« Simple Mail Transfert Protocol ») est utilisé pour le transfert de Mail entre un UA et un MTA ou entre MTA dans un réseau internet ou intranet.

- **Structure des messages**

Un message est schématiquement composé de deux parties, l'en-tête et le corps du message. Ces deux parties sont séparées par une ligne blanche.

L'en-tête est découpé ainsi :

FROM:	expéditeur
TO:	destinataire(s)
CC:	copie à
BCC:	copie aveugle
REPLY-TO:	adresse de réponse
ERROR-TO:	adresse en cas d 'erreurs
DATE:	date expédition
RECEIVED :	informations de transferts
MESSAGE-ID:	identificateur unique de message
SUBJECT:	sujet

- **Le dialogue entre le client et le serveur**

Le dialogue est défini par le protocole SMTP selon un schéma client/serveur. Sur le client, un démon (programme sendmail ou smtpd par exemple) attend les requêtes TCP sur le port 25 d'un client (le programme mail par exemple). Le dialogue est en ASCII. Pour tester, utilisez la commande **telnet *Serveur_SMTP 25***.

Voici quelques requêtes SMTP

HELO ou EHLO :	présenter le client au serveur
MAIL :	donner l’adresse de l’émetteur
RCPT:	donner l’adresse du destinataire
DATA :	donner le message en ASCII
VRFY :	vérifier si un compte existe
EXPN :	connaître les méthodes d’une liste de diffusion
QUIT :	terminer le processus

Exemple d’une session SMTP

[espera@mail~]$ telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
220 mail.gouv.bj ESMTP Postfix
>>> EHLO mail
250- mail.gouv.bj
250-PIPELINING
250-SIZE 10240000
250-ETRN
250 8BITMIME
>>> MAIL FROM:<espera@gouv.bj>
250 Ok
>>> RCPT TO:<alexandre@gouv.bj>
250 Ok

>>>DATA

354 End data with <CR><LF>.<CR><LF>

Bonjour Mr Alexandre

.

250 Ok: queued as C21B15769B

>>> QUIT

221 Bye

Connection closed by foreign host.

ESMTP

Le protocole ESMTP (« Extended SMTP » est une modernisation du protocole SMTP. La représentation des données utilise 8 bits au lieu de 7 bits dans SMTP. Cela simplifie la manipulation des caractères accentués et des données binaires.

POP

Le protocole **POP** (« Post Office Protocol ») est utilisé par les logiciels clients (Netscape, Eudora, Outlook...) pour relever le courrier sur les serveurs de messagerie. Le client pop utilise un couple Nom d'utilisateur/mot de passe pour la phase identification/authentification par le serveur.

IMAP (Internet Message Access Protocol)

Le protocole pop a été conçu pour la consultation “ hors ligne ” (*off line*). IMAP permet la consultation hors ligne, mais également “ en ligne ”, selon un processus interactif entre le client et le serveur. Les messages ne sont plus rapatriés sur le client. Ils restent en dépôt sur le serveur jusqu'à ce que l'utilisateur demande explicitement la suppression ou le transfert.

Ce procédé est particulièrement intéressant pour les utilisateurs mobiles. Ils peuvent consulter leurs messages à partir de machines ou de lieux non définis à l'avance.

Comme la connexion au serveur est permanente pendant la durée du traitement, il présente l'inconvénient d'un surcoût financier dû à la liaison téléphonique.

Ces services utilisent des protocoles/ports différents. Ils peuvent cohabiter simultanément sur le même serveur. Un utilisateur peut utiliser, selon ses besoins, l'un ou l'autre des services POP ou IMAP.

Vous devrez installer et configurer sur les postes clients un client IMAP (Outlook, Kmail...).

Des logiciels d'interface sur le serveur, comme Squirremail ou IMP, permettent de transformer le serveur IMAP en serveur “ webmail ”. Les clients pourront alors utiliser n'importe quel navigateur pour consulter leur boîte aux lettres.

MIME (« Multipurpose Internet Mail Extension »)

Conçu à une époque où le courrier électronique se limitait à du texte, le protocole SMTP impose certaines restrictions sur le contenu des messages. Ils ne doivent être constitués que de caractères ASCII et sont limités en taille. L’extension MIME a été conçue pour permettre d’échanger des textes utilisant des ensembles de caractères différents ainsi que des documents de tout type (image, son, vidéo…).

I- Présentation de Postfix

Postfix est un gestionnaire de messagerie électronique développé par **Wietse Venema** et plusieurs contributeurs. Nommé Secure Mailer lors de la première version en 1998, il fut publié comme logiciel libre (IBM public licence) sous le nom de Postfix. C'est un logiciel simple à configurer et conçu pour une sécurité optimale. De plus, il est peu gourmand en ressources système et constitue donc une véritable alternative à Sendmail. Le choix de Postfix est légitime tant pour le traitement de flux importants de messages que pour de petites installations.

A- Objectifs principaux

Le serveur de messagerie standard sur les systèmes Unix est le serveur Sendmail. Sendmail a fait ses preuves. L'inconvénient est son mode de configuration. Toutes les fonctions de messagerie sont réalisées par un seul programme. Sa structure est dite monolithique et la configuration du fichier « sendmail.cf » en est d'autant plus compliquée. Ce phénomène s'accroît avec l'amplification de l'utilisation du service de messagerie (augmentation de fréquence/volume) et avec l'exposition aux tentatives de piratage des serveurs de messagerie. Il existe d'autres serveurs de messagerie sur Unix (QMail, Exim...). Tous présentent des inconvénients au niveau utilisation de la bande passante, inter-opérabilté, respect des RFC, facilité de configuration, sécurité...

L'objectif de Postfix est d'apporter une solution à ces différents problèmes.

- **Large diffusion**

Postfix doit être largement diffusé et utilisé afin d'avoir un impact sensible sur les performances et la sécurité des systèmes de messagerie sur l'Internet. C'est pourquoi Postfix est un logiciel libre sans aucune restriction.

- **Performance**

Postfix est au moins trois fois plus rapide que ses plus proches « rivaux » (Sendmail et Qmail).

Un serveur Postfix sur un PC de bureau peut envoyer et recevoir quotidiennement un million de mails différents.

Postfix utilise les « trucs » utilisés sur les serveurs Web pour réduire la création de processus, et d'autres types de « trucs » permettent de réduire l'utilisation du système de fichiers, tout ça sans compromettre les performances.

- **Compatibilité**

Postfix a été conçu pour être compatible avec Sendmail afin de faciliter la migration. Les fichiers /var/spool/mail, /etc/aliases, NIS, et ~/.forward sont utilisés.

Toutefois, l'administration devant être simple, Postfix n'utilise pas de fichier sendmail.cf :-).

- **Flexibilité**

Postfix est conçu de façon modulaire, une douzaine de petits programmes effectue des tâches bien précises.

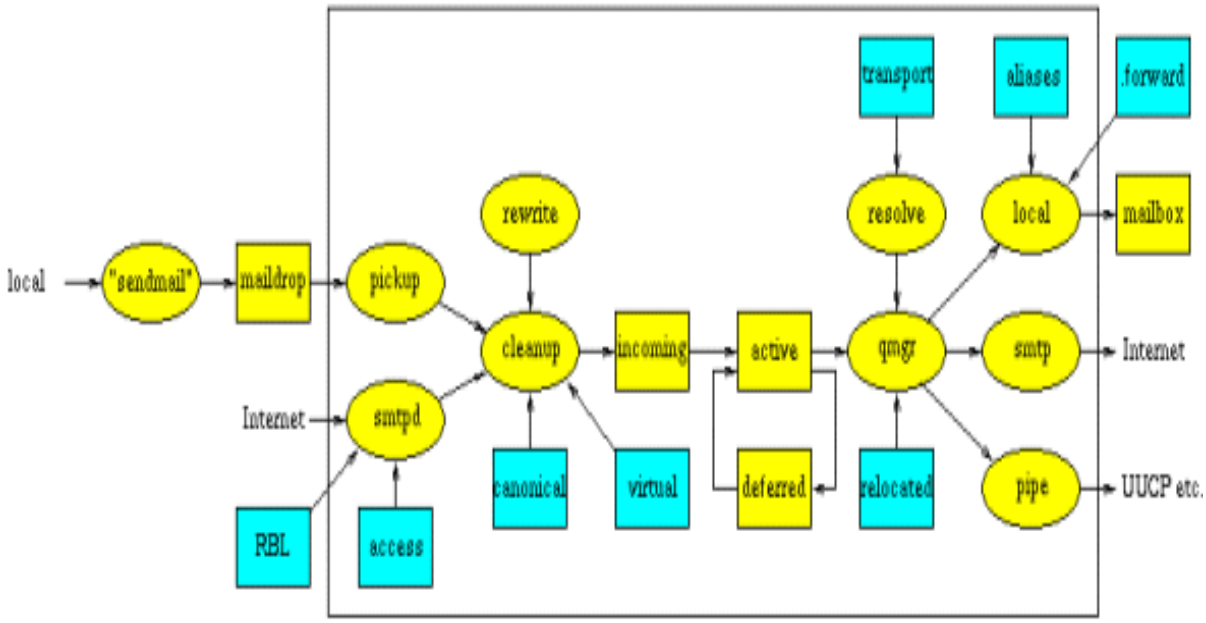
Il est possible de remplacer les programmes par défaut par des produits maison, voire de supprimer certains programmes inutiles dans certains cas (un firewall ou une station de travail n'a pas besoin de livrer localement des mails).

- **Sécurité**

Postfix utilise plusieurs niveaux de défense afin de protéger le système de toute intrusion. Chaque programme est enfermé dans sa cage (chrooté), il n'y a aucun lien direct entre le réseau et les programmes sensibles comme la livraison

du courrier local. Postfix ne fait même pas confiance à ses propres files de courrier.

Architecture globale de Postfix



La figure montre les composants principaux du système Postfix et le cheminement de l'information entre eux.

Les ellipsoïdes jaunes sont des programmes de courrier.

Les boîtes jaunes sont des files d'attente ou des dossiers de courrier.

Les boîtes bleues sont des tables de consultation.

L’ensemble des programmes situés dans le cadre noir fonctionnent sous le contrôle du démon master.

Les données situées dans le cadre noir appartiennent au système de courrier Postfix.

Afin de maintenir une grande image lisible, les éléments suivants ont été omis:

Les utilitaires "ligne de commande" de Postfix.

Le démon master de Postfix.

Les requêtes DNS par les démons de serveur et de client SMTP.

Le démon ***bounce*** ou ***defer*** qui gère le "rebon" des e-mails.

Les requêtes de réécriture et de résolution d'adresse du serveur de SMTP et de l'agent local de la livraison.

Le cheminement du courrier expédié par l'agent local de la livraison.

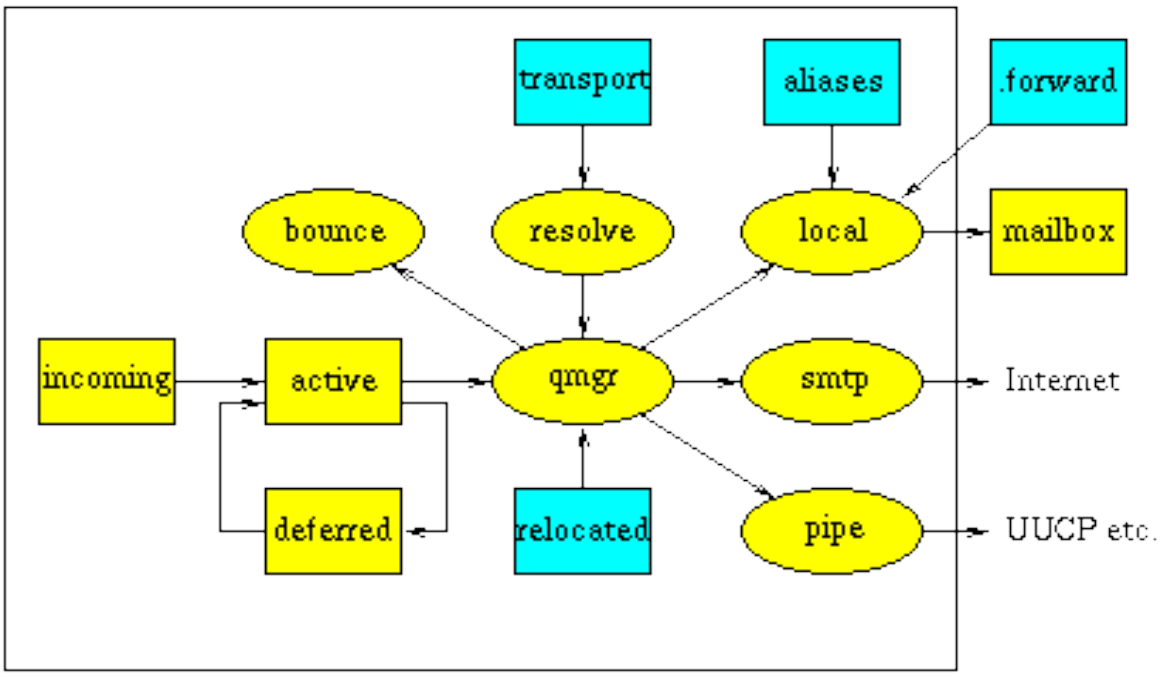
Le cheminement des notifications de postmaster pour des erreurs de protocole, des violations de politique, etc...

Les déclenchements pour alerter le démon de collecte et le gestionnaire de files d'attente que le nouveau courrier est arrivé dans le maildrop et les files d'attente entrantes, respectivement.

Toutes les opérations de Postfix sont bien compartimentées. Cela garantit donc une sécurité optimale.

1. La réception des messages

Lorsqu'un message arrive dans le système de courrier Postfix, quelle que soit son origine, son premier arrêt se fait dans la file d'attente ***Incoming***. La figure ci-dessous montre les composants principaux qui sont impliqués lors de l'arrivée d'un nouveau courrier.



a. Origine du courrier

- **Le courrier est posté localement.**

Si le courrier est posté sur la machine locale par les utilisateurs, le programme Sendmail de Postfix appelle le programme privilégié postdrop qui dépose le message dans le répertoire de la file maildrop où le message est pris par le démon de collecte pickup.
Ce démon fait quelques contrôles "sanitaires", afin d'éviter de polluer le reste du

système de mail avec du courrier invalide.
Pour éviter des accidents, les permissions du répertoire contenant maildrop sont telles que tout le monde peut y écrire, mais aucun utilisateur n'a le droit d'effacer le contenu

- **Le courrier provient du réseau**

Si le message provient d'un réseau, le serveur SMTP Postfix (smtpd) reçoit le message et fait quelques contrôles "sanitaires", afin de protéger le reste du système Postfix.
Le serveur SMTP peut être configuré pour mettre en application des commandes d'ECU (Unsollicited Commercial Mail) sur la base de listes noires locales ou issues du réseau, de requêtes DNS (domaine de l'expéditeur) ou toute autre information concernant l'émetteur.

- **Autres origines possibles.**

Le courrier peut être généré par le système Postfix lui-même, dans le but de renvoyer un message non-délivrable à son expéditeur, c'est le démon bounce ou defer qui se charge de ce travail.

Le courrier peut aussi être généré par l'agent local de remise (local) après interrogation de la base d'alias ou du fichier .forward propre à l'utilisateur.

Enfin, le courrier est généré par le système Postfix pour avertir le postmaster d'un problème (chemin indiqué par la flèche qui n'aboutit pas). Postfix peut être configuré pour alerter le postmaster en cas de problème de protocole SMTP, de violation de règles de sécurité UCE etc.

b. Traitement du courrier

- **Le message est livrable**

Le courrier est expédié par l'agent local de la livraison locale, soit par l'intermédiaire d'une entrée dans la base de données des alias, soit par l'intermédiaire d'une entrée dans le fichier .forward au niveau de l'utilisateur.

Le démon de nettoyage cleanup met en application l'étape de traitement finale pour le nouveau courrier. Il ajoute le champ From: et d'autres en-têtes manquants dans le message, il demande éventuellement au demon trivial-rewrite de réécrire l'adresse de réponse dans le format standard nom_utilisateur@nom_de_domaine, et il extrait optionnellement les adresses des destinataires de l'en-tête.
Le démon cleanup insère le résultat sous la forme d'un seul fichier dans la file d'attente incoming, et informe le gestionnaire de files d'attente queue manager (qmgr) de l'arrivée du nouveau courrier.
Le démon cleanup peut être configuré pour transformer des adresses sur la base des tables de consultations canonical et virtual.

- **Le courrier n'est pas livrable**

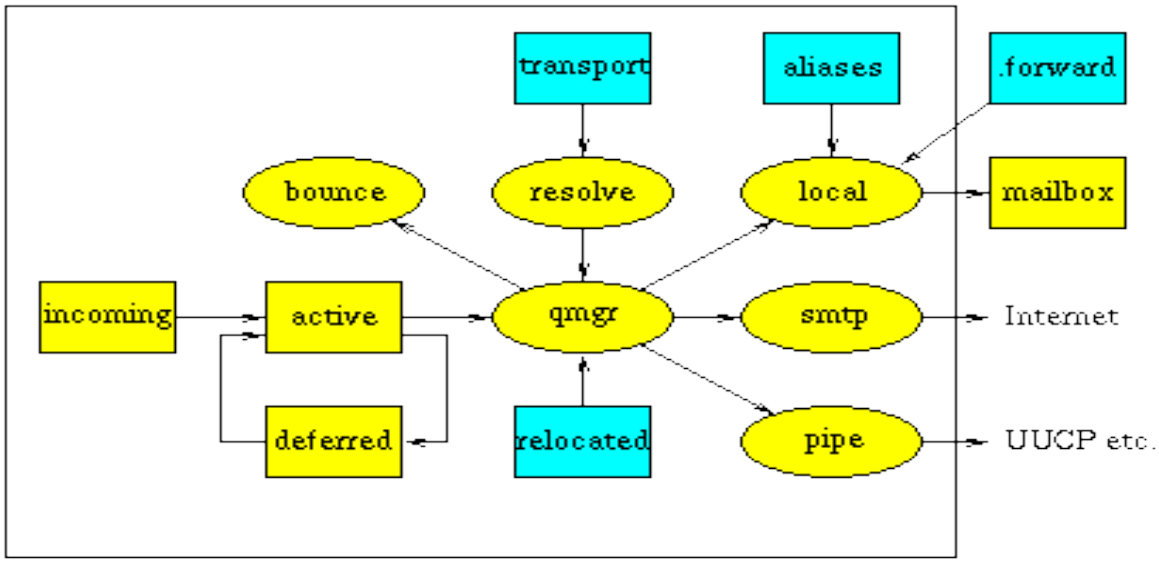
Un e-mail est généré automatiquement par le système Postfix, afin de renvoyer le courrier non livrable à l'expéditeur.
Ce sont les démons bounce ou defer qui annoncent la mauvaise nouvelle.

Un autre e-mail est également généré automatiquement par le système Postfix pour informer le responsable de la messagerie (postmaster) en cas de problème.

Postfix n'implémente pas encore un véritable langage de réécriture des adresses. L'implémentation d'un tel langage demanderait des efforts non-justfiés, la

plupart des sites n'en ayant pas besoin. A la place de cela, Postfix utilise des requêtes sur des tables.

2. Livraison du courrier



Une fois qu'un message a atteint la file d'attente incoming, l'étape suivante consiste à le livrer.
La figure montre les principaux composants du système de distribution du courrier de Postfix.

Le gestionnaire de file d'attente qmgr (queue manager) est le cœur du système de messagerie Postfix.
Il contacte les agents de livraison locale, smtp, lmtp ou pipe et envoie une demande de livraison avec le chemin d'accès au fichier qui contient la file d'attente, l'adresse de l'expéditeur, le nom de l'hôte à qui il faut livrer si la destination n'est pas locale et une ou plusieurs adresses de destinataires.

Le gestionnaire maintient une file d'attente deferred séparée pour chaque message qui n'a pas pu être livré (pour des raisons temporaires), de manière à ce

qu'un compte-rendu de livraison trop volumineux ne vienne pas ralentir l'accès des autres files.

Le gestionnaire maintient une petite file d'attente active avec juste quelques messages prêts pour la livraison.
Active agit comme une petite fenêtre sur les files d'attentes incoming ou deferred.
Cette méthode évite au gestionnaire de faire des débordements de mémoire si le serveur est fortement chargé et évite ainsi de consommer trop de ressources.

Optionnellement, le gestionnaire fait "rebondir" le message pour les destinataires qui sont référencés dans la table relocated.
Cette table contient des informations sur les utilisateurs qui ont changé d'adresse.

Sur la demande du gestionnaire de file d'attente, le daemon trivial-rewrite résout les destinations.
Par défaut, il fait uniquement la distinction entre les destinations locales ou distantes.
Des informations de routage additionnelles peuvent être spécifiées dans la table transport.

Sur la demande du gestionnaire de file d'attente, les daemons bounce et defer génèrent des rapports de non-livraison lorsqu'un message ne peut être acheminé, soit à cause d'une erreur non récupérable, soit parce que le destinataire n'est pas joignable pendant une durée trop longue.

L'agent local de la livraison sait gérer les boîtes aux lettres de type UNIX, les bases de données du type "alias" de sendmail (le MTA concurrent), les fichiers de type .forward de l'utilisateur.
De multiples agents locaux de livraison peuvent être exécutés en parallèle, mais

la livraison en parallèle au même utilisateur est habituellement limitée.
Avec l'agent de livraison sendmail de Postfix qui permet de poster des courriers, l'agent de livraison locale forme l'interface utilisateur familière de sendmail (le MTA concurrent).
L'agent de la livraison locale a la possibilité d'utiliser d'autres moyens de livraison locale : vous pouvez le configurer pour qu'il livre le courrier dans le répertoire home des utilisateurs, et vous pouvez même le configurer pour déléguer la livraison du courrier à une commande externe telle que le programme procmail bien connu.

Le client smtp recherche une liste d'échangeurs de courrier pour l'hôte de destination, trie la liste par préférence, et essaie chaque adresse alternativement jusqu'à ce qu'il trouve un serveur qui répond.
Sur un système postfix chargé, vous verrez plusieurs processus de client de smtp fonctionner en parallèle.
Le démon pipe est l'interface unique de sortie vers d'autres modes de transport de courrier (le programme sendmail est l'interface d'entrée).
Le système de courrier Postfix peut par exemple livrer du courrier par l'intermédiaire du protocole UUCP.
Ce protocole vénérable est encore largement répandu.
Par défaut, Postfix comprend des adresses de type "bang path" (Rassurez-vous, ici on parle de SMTP, pas de UUCP qui n'est plus de mise sur Internet, mais seulement dans des réseaux privés).

3. Postfix côté coulisses

Les sections précédentes ont donné une vue d'ensemble simplifiée de la façon dont le système Postfix envoie et reçoit le courrier.
Plusieurs autres choses se produisent dans les coulisses.
Le démon master est le processus de surveillance qui garde un œil sur le bien-être du système de courrier.
Il est typiquement lancé au démarrage du système par la commande postfix, et continue à fonctionner jusqu'à ce que le système s'arrête.
Le démon master lance tous les autres processus de Postfix sur demande, il peut même relancer un démon qui s'est terminé prématurément en raison d'un problème.
Il peut également imposer des limites sur le nombre de processus lancés par les démons comme indiqué dans le fichier de configuration master. cf.
Le démon bounce ou defer est sollicité par n'importe quel autre démon afin de loger les messages non livrés (non-delevery).
De même, le démon trivial-rewrite est appelé pour réécrire une adresse sous la forme nom_utilisateur@nom_de_domaine ou pour résoudre des noms de domaines.
Le démon showq donne l'état de la file d'attente de Postfix. Ce programme se cache derrière la commande mailq.
Le démon flush améliore l'exécution de la demande de smtp ETRN et de son équivalent en ligne de commande : sendmail -qRdestination, pour les destinations choisies.
Pour d'autres destinations, Postfix utilise l'équivalent du sendmail - q.
Le démon spawn écoute sur un port de TCP, un socket UNIX-domaine ou une connexion FIFO, et lance une commande non Postfix avec le socket ou la connexion FIFO reliée aux flux d'entrée, de sortie et d’erreurs standards. Il est

actuellement employé seulement pour utiliser un système de filtrage externe à Postfix.

4. Gestion des files d’attentes

Postfix utilise quatre files d'attentes :

Maildrop : contient les messages locaux.

Incoming : contient les messages qui ont été prélevés dans maildrop par le démon pickup, puis qui ont été traités par le démon cleanup.

Cette file contient aussi les messages venant de l'extérieur. En bref, elle contient les messages qui n'ont pas encore été traités par le gestionnaire de file d'attente.

qmgr : Active est une file contenant les messages en cours de délivrance par qmgr.

Deferred : contient les messages qui n'ont pas pu être délivrés (il y en a 10 dans notre exemple ci-dessous).

De plus, le répertoire /var/spool/postfix/defer contient les mails en attente plus longue et des répertoires qui sont « hachés » afin de ne pas avoir des répertoires contenant trop de fichiers : ainsi, le fichier 7B345AC0B1, par exemple, sera dans defer/7/B/7B345AC0B1.

Le contenu de la file d'attente peut être consulté avec la commande mailq (les habitués de Sendmail ne seront pas dépaysés...). Normalement celle-ci ne doit produire que les messages dont la délivrance n'a pas encore eu lieu.

Le gestionnaire de files ne garde en mémoire que les informations concernant la file Active.

La taille de cette file est limitée car le gestionnaire de files ne devrait jamais se trouver à cours de mémoire à cause d'un pic du trafic de courrier.

Dès qu'il y a de la place dans la file active, le gestionnaire de files y laisse entrer un message de la file incoming, puis un message de la file deferred.

Cette méthode garantit le passage des nouveaux, même lorsque la file deferred est particulièrement longue.

5. Les commandes

Nous parlerons ici des utilitaires "ligne de commandes" livrées avec postfix qui nous serviront à maintenir le système.
Sans compter les commandes sendmail, mailq, et newaliases qui ont déjà été présentées, le système Postfix possède une collection de commandes très utiles. Pour des raisons d'homogénéité, elles seront toutes nommées postquelquechose.

La commande **postfix** contrôle le système de courrier.
C'est l'interface pour démarrer et arrêter le système, et pour quelques autres opérations administratives.
Cette commande est réservée au super utilisateur.
Exemples :
#/**etc/init.d/postfix reload** force postfix à relire ses fichiers de configuration (après modification du /etc/postfix/main.cf).
#/**etc/inid.d/postfix check** vérifie la configuration du système de courrier.
#/**etc/inid.d/postfix flush** force postfix à tenter de vider la file deferred, donc à envoyer les messages en attente.
La commande **postalias** sert à convertir le fichier aliases en format bases de données (*.db).
Ce programme se cache derrière la commande newaliases.
La commande **postcat** montre le contenu de la file d'attente de Postfix.
C'est un programme limité, il peut être remplacé par un autre plus puissant qui permettrait d'éditer les fichiers de file d'attente de Postfix.

La commande **postconf** montre les paramètres donnés dans le fichier main.cf de Postfix : les valeurs réelles, les valeurs par défaut, ou les paramètres qui n'ont pas de valeur par défaut. C'est un programme limité et primaire. Ce programme peut être remplacé par un autre plus puissant qui pourrait non seulement énumérer mais également éditer le fichier main.cf.

Exemples :

#**postconf -n** affiche les paramètres modifiés par notre configuration.

#**postconf -d** affiche les paramètres par défaut.

La commande **postdrop** est appelée par le programme sendmail afin de déposer le courrier dans la file d'attente maildrop.

La commande **postkick** permet de lancer des commandes internes.

La commande **postlock** assure le mécanisme de verrouillage des boîtes aux lettres utilisateurs qui peuvent être utilisées par exemple par des shell scripts.

La commande **postlog** rend la journalisation de Postfix accessible aux shell scripts.

La commande **postmap** sert à convertir en format base de données des tables de consultation de Postfix telles que canonical, virtual et d'autres.

C'est un cousin de la commande de makemap d'UNIX.

La commande **postqueue** est l'utilitaire lancé par la commande de sendmail pour vider ou lister la file d'attente du courrier.

La commande **postsuper** sert à la maintenance de la file d'attente de Postfix. Cette commande est lancée lors du démarrage du système de courrier.

6. Apports en termes de sécurité

Par définition, les programmes de courrier traitent des informations provenant de sources potentiellement dangereuses.

Un système de courrier doit donc être écrit avec une grande attention quand il utilise les droits d'un utilisateur, cela même s'il n'est pas directement connecté à un réseau.

Postfix est un système complexe. La première version comprenait 30000 lignes de code, sans compter les commentaires. Avec un programme aussi complexe, la sécurité du système ne doit pas dépendre d'un seul mécanisme. Sinon, une seule suffirait à rendre vulnérable l'ensemble du logiciel.

Postfix utilise donc plusieurs couches de défense contre des erreurs logicielles ou autres.

a- Moindre privilège

La plupart des démons de Postfix peuvent être lancés avec de moindres privilèges et dans un environnement fermé (chroot).
Cela est plus particulièrement vrai pour les programmes directement exposés au réseau, comme les serveurs et clients smtp.
Bien que l'enfermement et les privilèges les plus bas ne soient pas suffisants pour assurer une sécurité absolument parfaite, cela y contribue fortement.

b- Isolation

Postfix utilise des processus différents afin d'isoler les activités de chacun. En particulier, il n'y a aucun lien entre le réseau et les programmes de livraison locale particulièrement sensibles en terme de sécurité. Un intrus devra passer au travers de plusieurs programmes pour arriver à ce niveau.
Certaines parties du système Postfix sont multi-threadées. Toutefois, aucune des parties en contact direct avec le réseau ne l'est.
La séparation des processus fournit une bien meilleure isolation que le multi-thread utilisant un espace de nom commun.

c- Environnement contrôlé

Aucun des programmes de livraison de Postfix ne nécessite de droits utilisateur. Au lieu de cela, la majorité des programmes Postfix fonctionne sous le contrôle du démon-maître (master) résident qui, lui-même, est dans un environnement controlé, sans aucune relation père-fils avec un quelconque processus utilisateur. Cette méthodologie permet d'exclure tout exploit utilisant

les fichiers ouverts, les signaux, les variables d'environnement que les systèmes Unix passent de pères éventuellement malintentionnés à leurs processus fils.

d- **Programme SUID**

Aucun programme postfix n'est SUID.

L'introduction de ce concept a été la plus grosse erreur de l'histoire d'Unix. Le positionnement du bit UID pose bien plus de problèmes qu'il n'en résout. Chaque fois qu'une nouvelle fonctionnalité a été ajoutée au système Unix, set-uid a entraîné un problème de sécurité : librairies partagées, système de fichiers /proc, support multi-langage, pour n'en mentionner que quelques-unes. De plus, set-uid rend impossible l'utilisation de fonctionnalités qui ont rendus les successeurs d'Unix si attractifs, comme plan9 et les espaces de noms du système de fichiers par processus.

Par défaut, le répertoire de la file maildrop est accessible en écriture au monde entier, afin que les différents processus locaux puissent poster leurs courriers sans requérir l'assistance d'une commande set-uid ou du démon serveur de courrier. Ce répertoire n'est pas utilisé pour les messages venant du réseau et les fichiers de files ne peuvent pas être lus par les autres utilisateurs.

Un répertoire accessible en écriture offre des possibilités en terme de vulnérabilité : un utilisateur local peut faire des liens durs vers les fichiers de file d'un autre utilisateur afin que cette file ne soit jamais libérée et/ou que ses messages soient livrés plusieurs fois ; un utilisateur local peut remplir le répertoire de la file maildrop de cochonneries et essayer de faire planter le système ; un utilisateur local peut aussi faire des liens durs vers les fichiers de quelqu'un d'autre pour se les faire délivrer par mail. Toutefois, les fichiers de files Postfix ont un format particulier ; la probabilité qu'un fichier non-Postfix soit reconnu comme tel est de moins d'un sur 10 puissance 12.

Si le fait que le répertoire de la file maildrop soit accessible en écriture au monde entier vous semble inacceptable, vous pouvez ne pas utiliser cette

solution, révoquez les droits sur le répertoire et préférez l'activation des privilèges set-gid à un petit programme fourni (postdrop) pour permettre aux processus locaux d'envoyer leurs messages.

e- Confiance

Les fichiers de files ne sont pas écrits sur le disque lorsque la destination est sensible, comme pour des fichiers ou des commandes.
Au lieu de cela, les programmes tel que l'agent de livraison locale essayent de prendre leurs décisions avec le souci de la sécurité sur la base des informations reçues initialement.
Bien sûr, les programmes Postfix ne font pas confiance aux données reçues du réseau. En particulier, Postfix filtre les données fournies par l'utilisateur avant de les exporter via des variables d'environnement. S'il y a une leçon à tirer de ce que les administrateurs ont appris des désastres de la sécurité des sites web, c'est bien ceci : ne laissez jamais des données reçues du réseau approcher de l'interpréteur de commandes.
Le filtrage est la meilleure des possibilités.

f- Données volumineuses

La mémoire pour les chaînes de caractères et les tampons est affectée dynamiquement afin d'éviter tous problèmes de dépassement de tampon.
Les lignes longues dans les messages sont fractionnées en morceaux de taille raisonnable et rassemblées à la livraison.
Les diagnostics sont également fractionnés (en un seul endroit !) avant d'être passés au démon syslog afin d'éviter des dépassements de tampons sur les plateformes les plus anciennes. Toutefois, le tronçonnement des données passées aux appels système ou aux librairies n'est pas généralisé. Sur certaines plateformes, le programme peut entraîner des problèmes de dépassements de tampon, à cause du logiciel utilisé dans les couches inférieures.

Aucun dispositif de défense contre les lignes de commande anormalement longues n'est réalisé, les noyaux Unix imposant leur propre limite, suffisante pour bloquer les programmes ou les utilisateurs malintentionnés.

g- Autres défenses

Le nombre d'instances d'un objet donné en mémoire est limité, afin d'éviter au système de devenir instable en cas de charge importante.
En cas de problème, le programme se mettra en veille avant d'envoyer un message d'erreur au client, avant de se planter sur une erreur fatale,
ou avant d'essayer de redémarrer un logiciel défaillant. L'objectif est d'éviter de détériorer davantage une éventuelle situation de problème.

II- Configuration de Postfix

Le fichier de configuration de Postfix (/etc/postfix/main.cf) contient plusieurs centaines de paramètres.
Heureusement, ils ont des valeurs par défaut convenables et appropriées.
Dans la plupart des cas, pour pouvoir utiliser le système de courrier Postfix, il vous suffira de renseigner deux ou trois paramètres :

- Le nom de domaine utilisé pour le courrier sortant
- Les domaines terminaux pour l'acheminement du courrier
- Les clients autorisés à utiliser Postfix

Ces valeurs seront utilisées pour définir les valeurs par défaut de nombreux autres paramètres.

Le paramètre suivant déterminera le niveau et donc le nombre d'alertes envoyées au postmaster local :

- Les erreurs que nous rapportons au postmaster

D'ailleurs, si vous changez des paramètres d'un système Postfix, n'oubliez pas de lancer la commande :
/etc/init.d/postfix reload pour que Postfix prenne en compte les nouvelles valeurs.

Si vous lancez Postfix sur une interface virtuelle du réseau, ou si votre machine lance d'autres systèmes de courrier sur des interfaces virtuelles, vous devrez renseigner les paramètres suivants :

- Le nom du serveur Postfix
- Le domaine de Postfix
- Les Réseaux de confiance

- Les adresses réseau de Postfix

A- Le nom de domaine utilisé pour le courrier sortant

Le paramètre ***myorigin*** indique le "vrai" nom du serveur qui apparaîtra dans tout courrier posté sur cette machine.
La valeur par défaut est le nom local de machine, **$myhostname,** qui a pour valeur par défaut le nom de la machine.
A moins de ne travailler que sur un très petit domaine, la valeur du paramètre **$mydomain,** qui a pour valeur par défaut le nom du domaine de la machine, peut être préférable.

Ce paramètre permet de renseigner postfix sur la machine qui a posté.
Exemples:

myorigin = **$myhostname** (défaut)
myorigin = **$mydomain** (probablement souhaitable)

B- Les domaines terminaux pour l'acheminement du courrier

Le paramètre ***mydestination*** indique quels sont les domaines que cette machine desservira localement, au lieu de le transmettre à une autre machine.
La valeur par défaut est de recevoir le courrier à destination de la machine elle-même.

Vous pouvez indiquer zéro ou plusieurs noms de domaine, /des/fichiers et/ou des tables de correspondance type:name (telles hash:, btree:, nis:, ldap:, ou mysql:), séparées par des espaces et/ou des virgules. /un/fichier est remplacé par son contenu; type:name demande qu'une consultation de table soit faite et détermine simplement l'existence : le résultat de la consultation est ignoré.

Si votre machine est un serveur de mails pour son domaine tout entier, vous pouvez utiliser la variable **$mydomain**.

Exemples:

Par défaut:

***mydestination* = $myhostname localhost.$mydomain**

Serveur de messagerie pour tout un domaine

***mydestination* = $myhostname localhost.$mydomain $mydomain**

Machine avec multiples enregistrements A :

***mydestination* = $myhostname localhost.$mydomain www.$mydomain ftp.$mydomain**

Attention: afin d'éviter des boucles de routage du courrier, vous devez énumérer tous les noms (hostnames) de la machine, y compris $myhostname, et localhost.$mydomain

C- Les clients autorisés à utiliser Postfix

Par défaut, Postfix relaie le courrier des clients des réseaux autorisés et des domaines autorisés. Les réseaux autorisés sont définis par le paramètre mynetworks. La valeur par défaut autorise tous les clients des sous-réseaux IP auxquels la machine est reliée.

Les domaines autorisés de client sont définis par le paramètre de configuration de ***relay_domains***.

Par défaut les clients de confiance sont les noms (hostnames) du (des) domaine(s) énuméré(s) dans mydestination.

D- Les erreurs que nous rapportons au postmaster

Il est d'abord nécessaire de mettre en place un alias associant le postmaster à une personne réelle.
Cet alias doit être défini, de sorte que les gens puissent signaler des problèmes de distribution du courrier.
Le système Postfix lui-même signale également des problèmes au postmaster.
Vous ne serez peut être pas intéressé par tous les types de rapports d'erreurs, ainsi ce mécanisme de reportage est configurable.
Par défaut, seuls les problèmes sérieux sont signalés au postmaster (ressource, logiciel) :

Par défaut:
***notify_classes* = resource, software**
La signification des différentes classes de rapport sont les suivantes :
bounce
Une copie du courrier non livrable est envoyée au postmaster.
Si le courrier est non livrable, un prétendu avis de non-livraison simple est envoyé, avec une copie du message qui n'a pas été fourni.
Pour des raisons d'intimité, la copie de postmaster d'un avis de non-livraison simple est tronquée après les en-têtes de messages originaux.
Si un avis de non-livraison simple est non livrable, le postmaster reçoit un double avis de non-livraison avec une copie de l'avis de non-livraison simple entier.

Le message d'alerte qui accompagne la copie du message original est appelé bounce.

2bounce
Deux messages de bounce sont envoyés au postmaster.

delay

Le postmaster est informé de tout courrier qui a été retardé. Dans ce cas, le postmaster reçoit les en-têtes du message seulement.

policy

Le postmaster est informé des demandes de client qui ont été rejetées en raison des restrictions de la politique (ECU).
Le postmaster reçoit une transcription entière de la session smtp.

protocol

Le postmaster est informé des erreurs de protocole (côté de client ou de serveur) ou les tentatives d'un client d'exécuter des commandes non implémentées. Le postmaster reçoit une transcription entière de la session de smtp.

resource

Le postmaster est informé des raisons de non livraison du courrier liées à des problèmes de ressource (par exemple, une erreur lors de l'écriture dans le répertoire de la file d'attente).

software

Le postmaster est informé des raisons de non livraison de courrier suite à des problèmes logiciels.

E- Le nom du serveur Postfix

Le paramètre ***myhostname*** décrit le nom complet et conforme (fqdn) de la machine utilisant le système Postfix.
$myhostname est la valeur par défaut ainsi que dans beaucoup d'autres paramètres de configuration de Postfix.

Par défaut, ***myhostname*** est le nom local de la machine.
Si votre nom de machine n'est pas complet et conforme, ou si vous lancez

Postfix sur une interface virtuelle, il est nécessaire de préciser le nom à utiliser. C'est sous ce nom que la machine s'annonce lors du HELO.

Exemples:

myhostname = **host.local.domain** (le hostname local n'est pas FQDN)

myhostname = **host.virtual.domain** (interface virtuelle)

myhostname = **virtual.domain** (interface virtuelle)

F- Le domaine de Postfix

Le paramètre ***mydomain*** indique le domaine parent de **$myhostname.** Par défaut, il vaut **$myhostname** sans la première partie du nom (Sauf si on est un "top-level-domain cad : .fr, .com, ...).

Exemples:

mydomain = **local.domain**

mydomain = **virtual.domain** (interface virtuelle)

G- Les Réseaux de confiance

Le paramètre ***mynetworks*** prend comme valeur la liste des réseaux de confiance de Postfix.
Cette information peut être utilisée par les dispositifs anti-UCE pour identifier les clients smtp de confiance qui sont autorisés à utiliser le relais de messagerie Postfix.

Vous pouvez indiquer la liste de réseaux de confiance dans le fichier main.cf, ou vous pouvez laisser Postfix déduire la liste pour vous.
Par défaut, Postfix effectue le travail pour vous.
Ces réseaux seront considérés comme des réseaux locaux.

Défaut:

mynetworks_style = **subnet**

La signification des valeurs est la suivante :

class

Clients smtp de confiance dans les réseaux de la classe A/B/C pour lesquels Postfix accepte le relais0.

Ne faites pas ceci avec un emplacement de dialup - Postfix ferait alors confiance au réseau de votre fournisseur tout entier.

Au lieu de cela, indiquez "à la main" les réseaux explicites, comme décrit ci-dessous.

subnet (défaut)

Fait confiance aux clients smtp dans les sous-réseaux d'IP de Postfix.

host

Fait confiance seulement à la machine locale.

Alternativement, vous pouvez indiquer les réseaux "à la main". Dans ce cas, Postfix ignore le paramètre ***mynetworks_style***.

Pour indiquer la liste de réseaux de confiance, indiquez les plages d'adresses réseau dans la notation de CIDR (network/mask), par exemple:

***mynetworks* = 168.100.189.0/28, 127.0.0.0/8**

Vous pouvez également indiquer le nom absolu d'un fichier de valeurs au lieu d'énumérer les valeurs dans le fichier main.cf.

H- Les adresses du réseau de Postfix

Le paramètre ***inet_interfaces*** indique toutes les adresses d'interface réseau sur lesquelles le système Postfix doit écouter.

Le courrier adressé à l'*utilisateur @* [adresse *réseau]* sera fourni localement, comme s’il était adressé à un domaine énuméré dans **$mydestination.**

Par défaut Postfix écoute sur toutes les interfaces actives.
Si vous voulez recevoir des mails sur des interfaces virtuelles, vous devrez indiquer sur quelles interfaces vous écouter.

Vous devez indiquer les interfaces explicites de la machine pour les réceptions non virtuelles de courrier de la machine elle-même : les attentes de mails non virtuelles ne doivent jamais écouter sur les interfaces virtuelles où vous auriez une boucle de mails.

Exemples:

Par défaut:
inet_interfaces **= all**

Centre serveur virtuel:
inet_interfaces **= virtual.host.name** (domaine virtuel)
inet_interfaces **= $myhostname localhost.$mydomain** (écoute non virtuelle)
inet_interfaces **= 10.0.0.1** (avant, faire #ifconfig add eth0:1 10.0.0.1 ; route add 10.0.0.1 dev eth0:1)

I- MISE EN PLACE DE POSTFIX

Le but de notre projet est de configurer un serveur SMTP Postfix, installer les serveurs IMAP et POP, mettre en place un Web mail SquirrelMail pour la consultation des mails et enfin tester le fonctionnement de l'ensemble.

Configuration requise

Le serveur sur lequel sera installé Postfix aura les caractéristiques suivantes :

Nom du produit	Processeurs	Mémoire en standard	Contrôleur de stockage	Disques durs
Serveur spécial HP ProLiant ML330 G6 format tour	Processeur Intel® Xeon® E5506	2 Go (1 x 2 Go)	Smart Array B110i SATA RAID ; Smart Array P410/Zero Memory	2

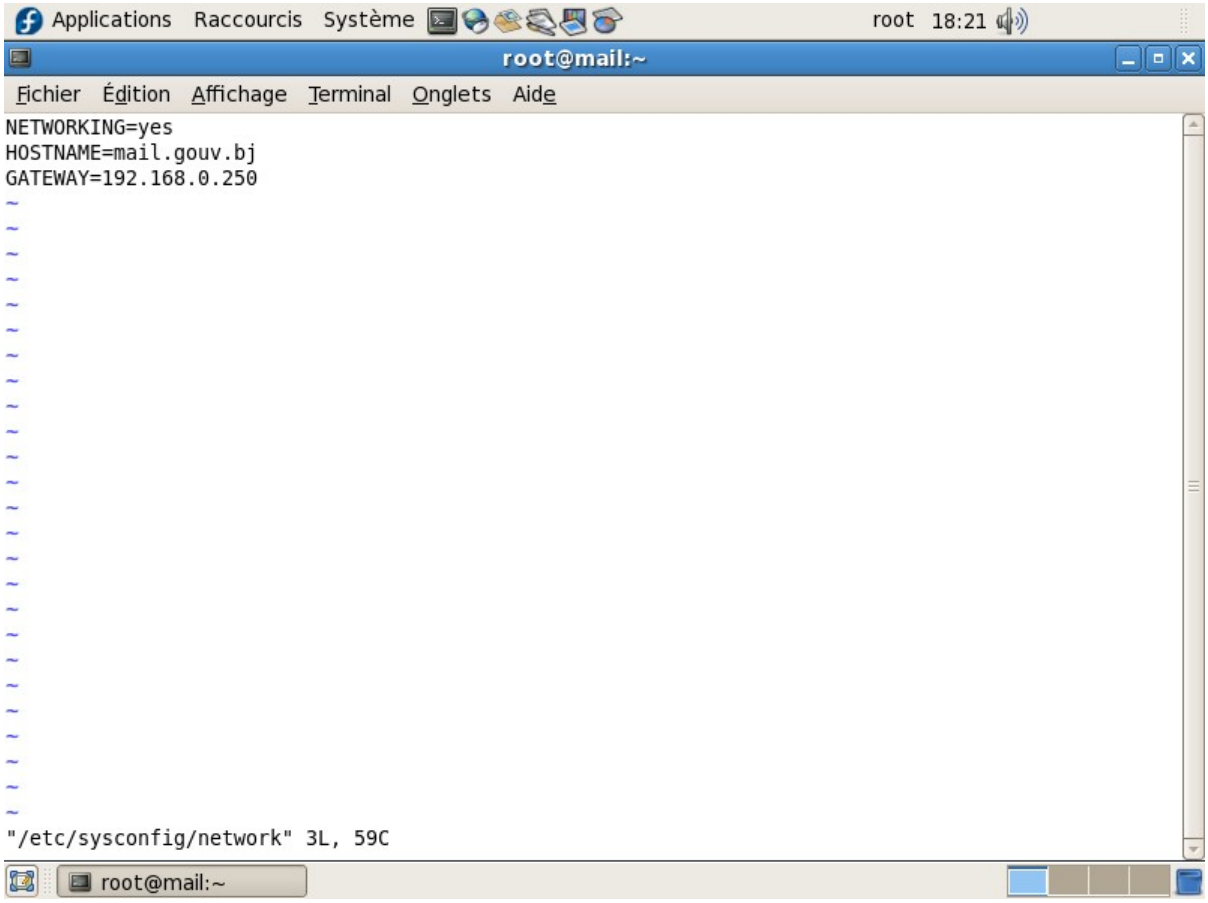
Par défaut tous les paquets nécessaires pour la mise en place du serveur de messagerie avec Postfix ont été installés lors l'installation de Fedora Core7

Bind-9.4.0-6.fc7 pour la mise en place du serveur DNS
Postfix-2.3.6-1 configuration du serveur de messagerie
Dovecot-1.0.0-11.fc7 pour la configuration de POP et IMAP
Procmail-3.22-19.fc7 pour la configuration du DA
Httpd-2.2.4-4 pour la mise en place du serveur web
squirrelmail-1.4.10a.1fc7.noarch pour la mise en place du web mail

A. Nom de machine

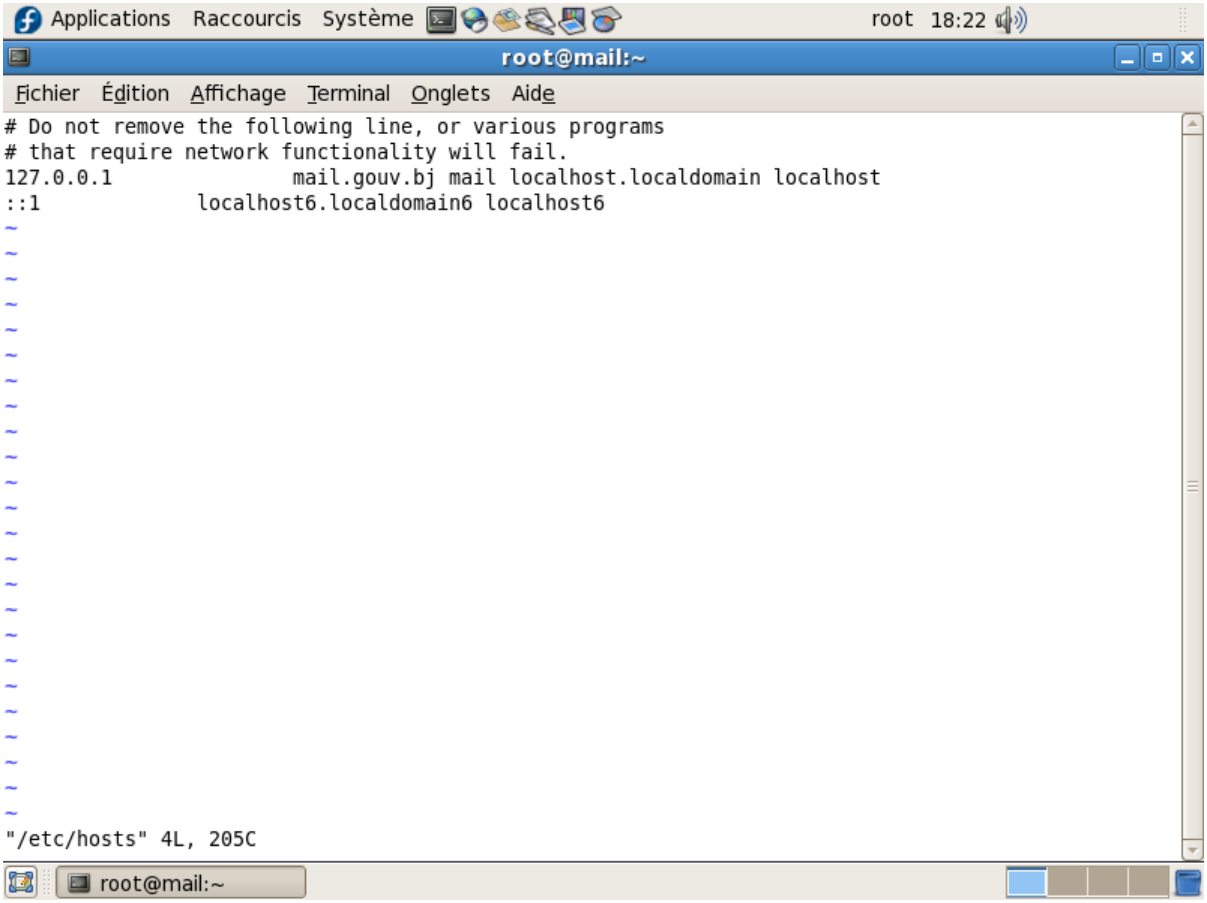
Editons le fichier /etc/sysconfig/network et modifions la ligne suivante :

HOSTNAME=mail.gouv.bj



Editons ensuite le fichier /etc/hosts

127.0.0.1 Localhost mail localhost.localdomain mail.gouv.bj



B. Configuration de la carte réseau

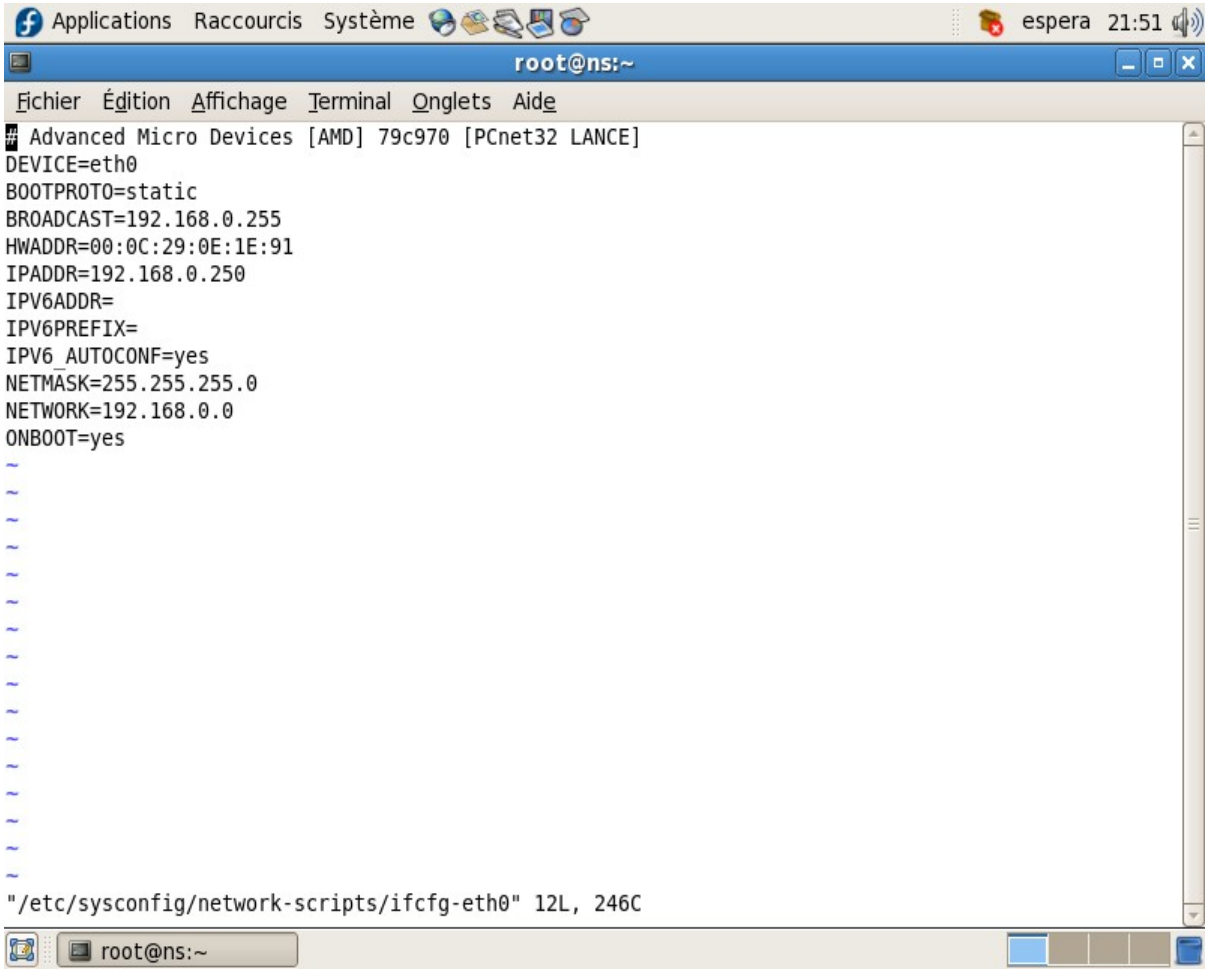
Editons le fichier /etc/sysconfig/network-scripts/ifcfg-eth0 et modifions les lignes suivantes :

IPADDR=192.168.0.250

NETMASK=255.255.255.0

NETWORK=192.168.0.0

BROADCAST=192.168.0.255



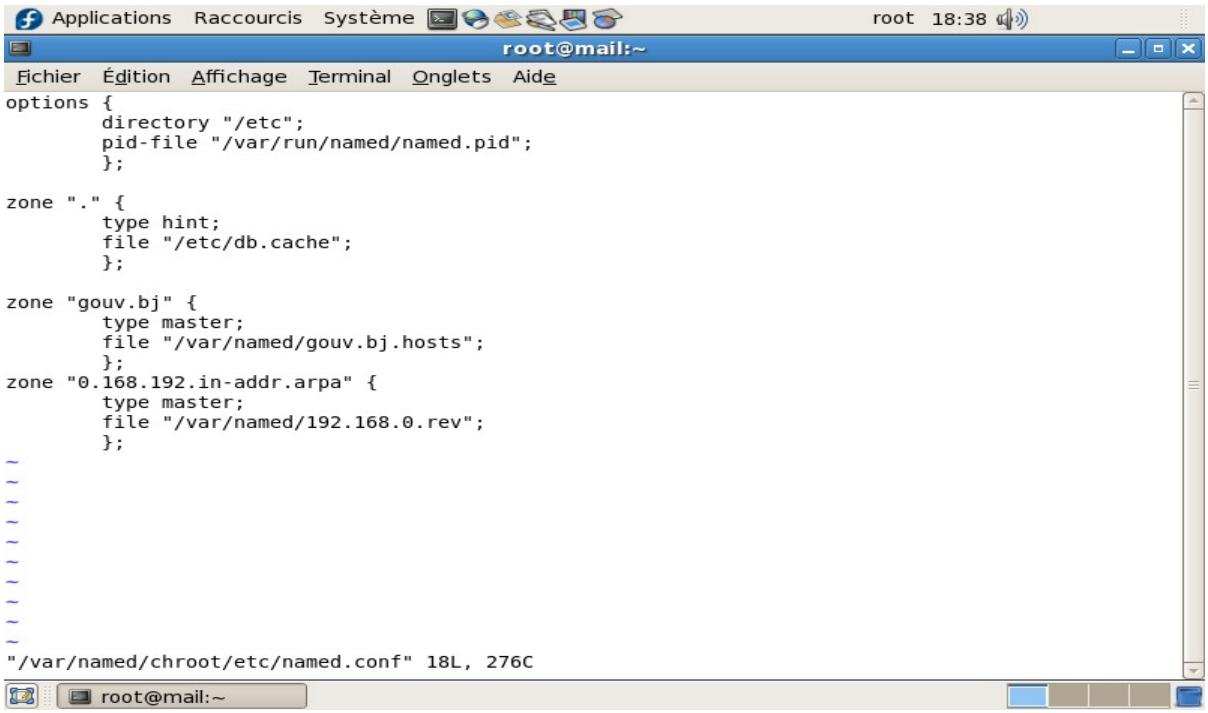
C. Configuration du serveur DNS

Editons le fichier named.conf dans /etc/named.conf et créons les zones (pour Fedora core7 allez dans /var/named/chroot/etc/named.conf) suivantes :

Zone direct : gouv.bj

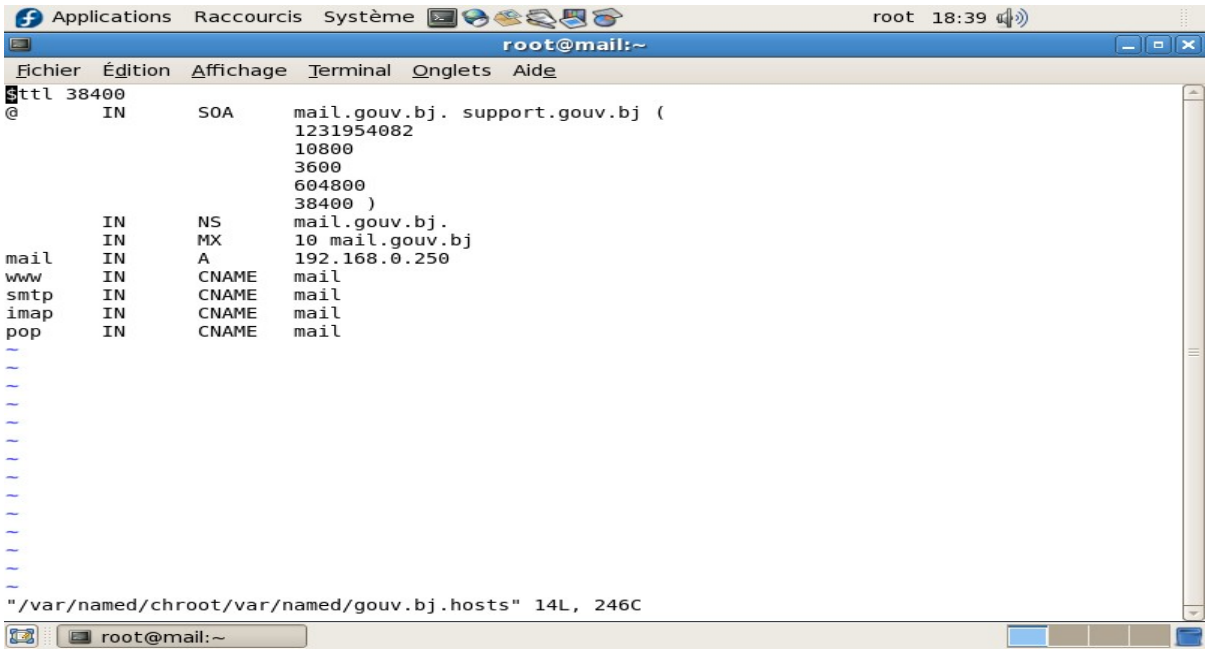
Zone inverse : 0.168.192.in-addr.arpa

```
zone "gouv.bj" {
        type master;
        file "/var/named/gouv.bj.hosts";
        };
zone "0.168.192.in-addr.arpa" {
        type master;
        file "/var/named/0.168.192.rev";
        };
```



Créons ensuite le fichier de zone direct gouv.bj.hosts dans /var/named/chroot/var/named/ gouv.bj.hosts. Dans Fedora core7 allez dans /var/named/chroot/var/named/

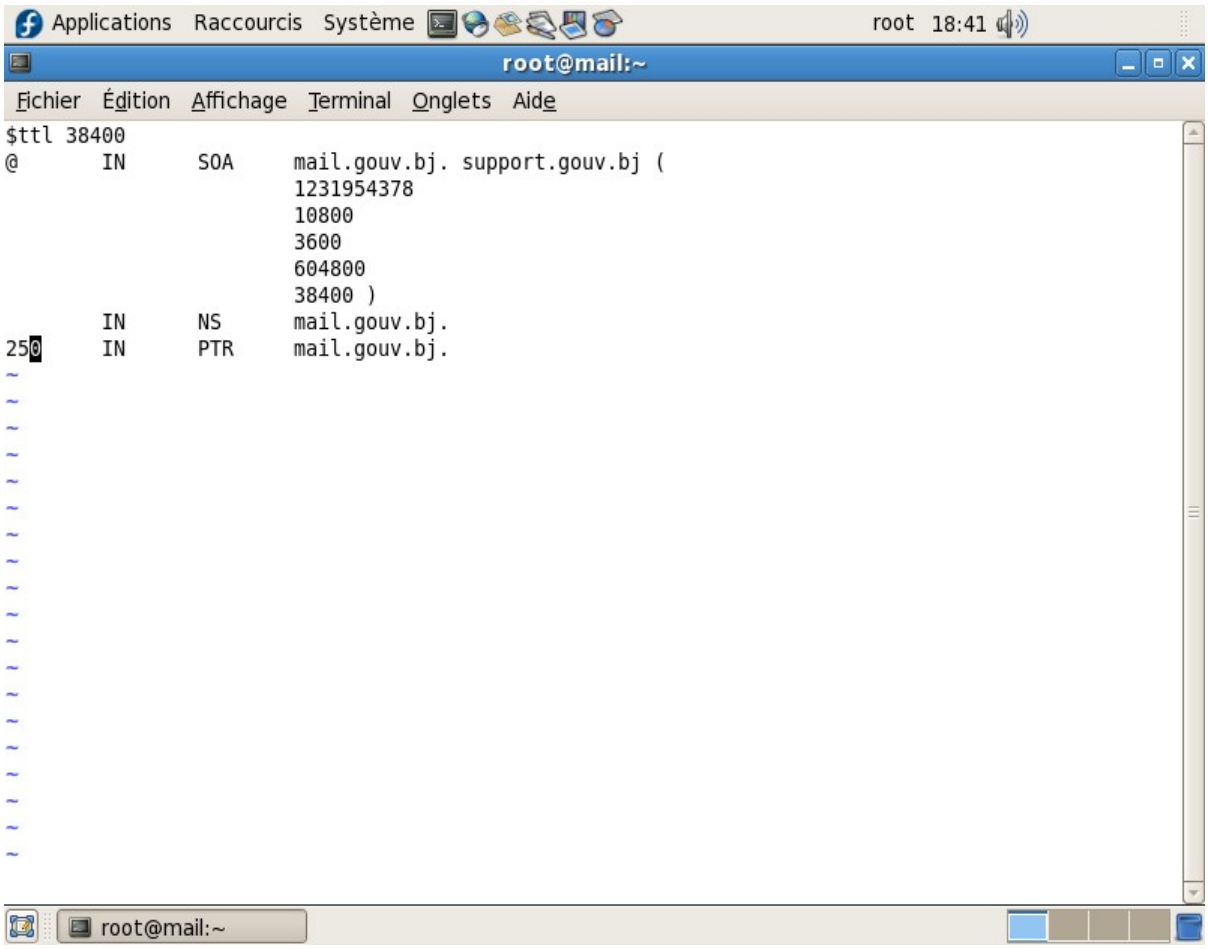
```
$ttl 38400
@       IN      SOA     mail.gouv.bj  support.gouv.bj (
                        1202720398
                        10800
                        3600
                        604800
                        38400)
        IN      NS      mail.gouv.bj.
        IN      MX      10 mail.gouv.bj.
mail    IN      A       192.168.0.250
smtp    IN      CNAME   mail
pop     IN      CNAME   mail
imap    IN      CNAME   mail
```



Créons enfin le fichier de zone inversé 0.168.192.rev dans

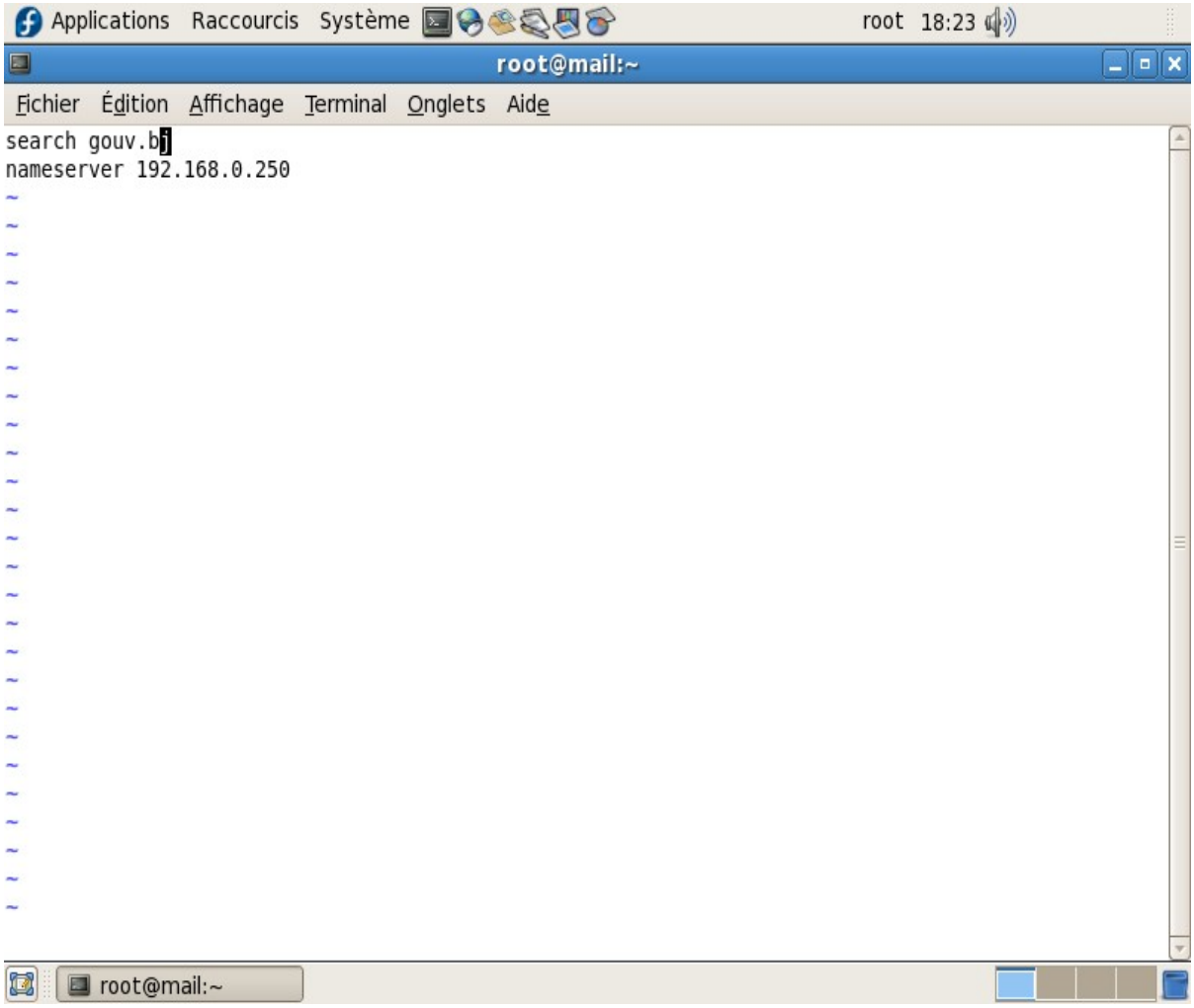
/var/named/chroot/var/named/0.168.192.rev

```
$ttl 38400
@       IN      SOA     mail.gouv.bj. support.gouv.bj. (
                        1202720398
                        10800
                        3600
                        604800
                        38400)
        IN      NS      mail.gouv.bj.
250     IN      PTR     mail.gouv.bj.
```



Editons le fichier /etc/resolv.vonf

Nameserver 192.168.0.250



D. Configuration de Postfix

Editons le fichier main.cf dans /etc/postfix/main.cf et modifions les lignes suivantes :

#

myhostname = mail.gouv.bj

#

Comme son intitulé l'indique, c'est le nom canonique du serveur de mail.

Son nom complet en fait.

Penser à renseigner ce nom en concordance avec son adresse ip dans le

fichier /etc/hosts, sinon postfix peut se comporter bizarrement.

#

mydomain = gouv.bj

#

Le nom de domaine que va gérer postfix

#

#myorigin = $myhostname

myorigin = $mydomain

#

Quand le serveur envoie un email, il complète le message avec le nom du

domaine émetteur.

#

inet_interfaces = all

#inet_interfaces = $myhostname

#inet_interfaces = $myhostname, localhost

#inet_interfaces = localhost

#

Sur quelles interfaces écoute postfix ; par défaut postfix écoute sur

localhost uniquement ; on peut choisir de mettre inet_interfaces = all pour

qu'il écoute sur toutes les interfaces ou spécifier chaque interface comme

ici. Attention, l'adresse correspondant à la variable myhostname est lue
dans le fichier /etc/hosts.

#
#mydestination = $myhostname, localhost.$mydomain, localhost
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
#mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain,
#mail.$mydomain, www.$mydomain, ftp.$mydomain
#
Pour quelles entités postfix va recevoir les emails, par défaut uniquement
pour localhost, il faut définir en supplément $mydomain pour avoir un
serveur de messagerie pour tout un domaine, on peut également gérer des
alias rattachés au serveur comme ici www.mondomaine.fr
#
#local_recipient_maps = unix:passwd.byname $alias_maps
#local_recipient_maps = proxy:unix:passwd.byname $alias_maps
#local_recipient_maps =
#
unknown_local_recipient_reject_code =450
#
#mynetworks_style = class
#mynetworks_style = subnet
#mynetworks_style = host
#
#mynetworks = 192.168.0.0/24, 127.0.0.0/8
Variable à modifier quand on a plusieurs sous réseaux, mais postfix par
défaut accepte le relais pour les réseaux représentés par ses interfaces.
Cette variable permet de bloquer les spams venant de réseaux inconnus.

```
#
#mynetworks = $config_directory/mynetworks
#mynetworks = hash:/etc/postfix/network_table
#
#relay_domains = $mydestination
#
#relayhost = $mydomain
#relayhost = [gateway.my.domain]
#relayhost = [mailserver.isp.tld]
#relayhost = uucphost
#relayhost = [an.ip.add.ress]
#
# Cette variable est très utile dans le cas où vous avez un serveur interne de
# messagerie inconnu d'Internet. Entrez entre crochets le nom du serveur
# sortant SMTP de votre Fournisseur d'accès, par exemple [smtp.wanadoo.fr].
# Les messages sortant sur Internet seront expédiés à ce serveur au lieu
# d'être émis en direct par votre serveur. Cela contourne les filtres antispam
# de certains serveurs de messagerie.
#
#relay_recipient_maps = hash: /etc/postfix/relay_recipients
#
#in_flow_delay = 1s
#
#alias_maps = dbm:/etc/aliases
alias_maps = hash:/etc/aliases
#alias_maps = hash:/etc/aliases, nis:mail.aliases
#alias_maps = netinfo:/aliases
#
#alias_database = dbm:/etc/aliases
```

#alias_database = dbm:/etc/mail/aliases

alias_database = hash:/etc/aliases

#alias_database = hash:/etc/aliases, hash:/opt/majordomo/aliases

#

Valeurs par défaut du fichier aliases.

Pour avoir plus d'informations, jeter un oeil au "man aliases"

Ce fichier sert à créer des comptes virtuels et à indiquer au système qui

est l'administrateur de messagerie qui recevra les messages d'erreur du

serveur.

#

recipient_delimiter = +

#

#home_mailbox = Mailbox

home_mailbox = .Maildir/

#

#mail_spool_directory = /var/mail

mail_spool_directory = /var/spool/mail

#

mailbox_command = /usr/bin/procmail

#mailbox_command = /some/where/procmail -a "$EXTENSION"

#

smtpd_banner = $myhostname ESMTP $mail_name

#smtpd_banner = $myhostname ESMTP $mail_name ($mail_version)

#

local_destination_concurrency_limit = 2

default_destination_concurrency_limit = 20

E. Configuration du serveur POP, IMAP

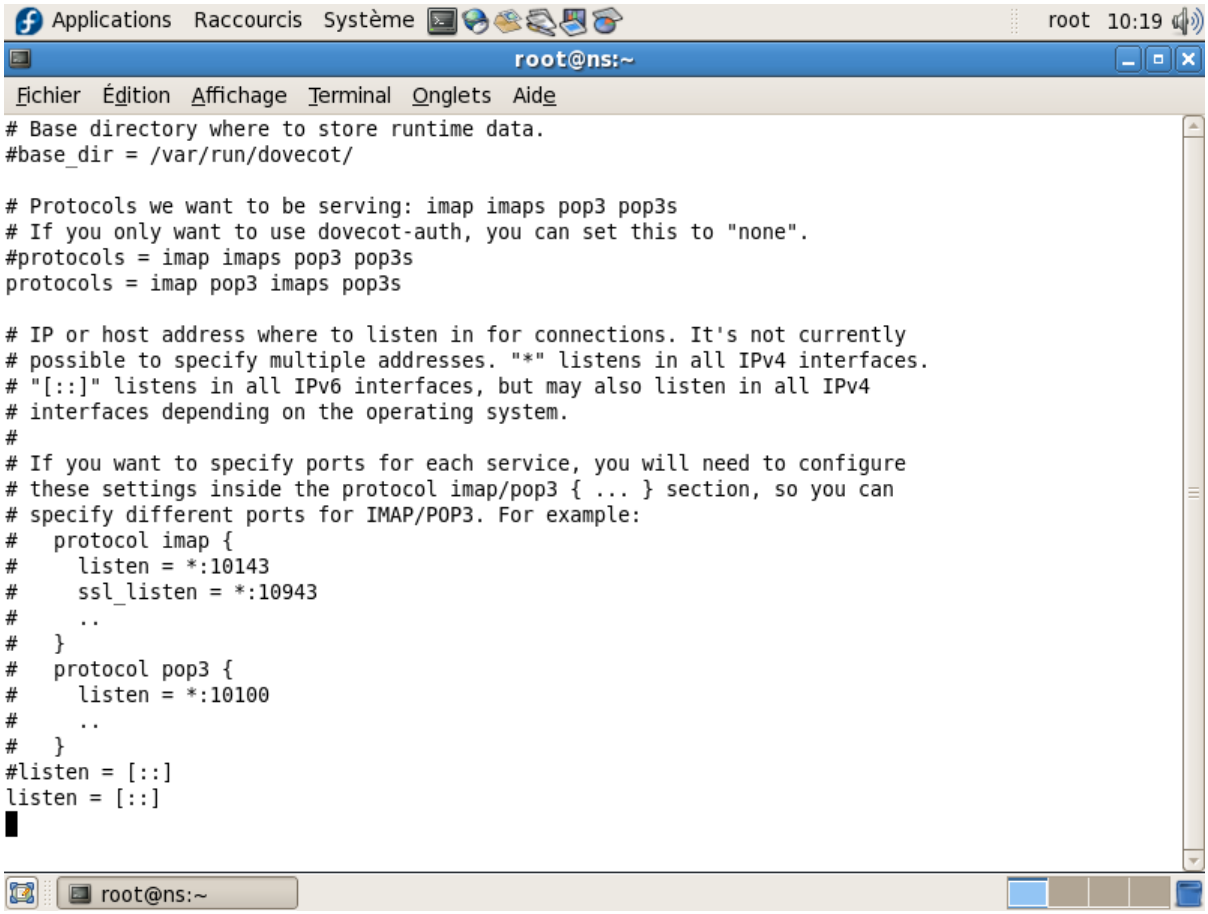
Editons le fichier dovecot.conf dans /etc/dovecot.conf et modifions les lignes suivantes :

Les Protocoles autorisés

protocols = imap pop3 imaps pop3s

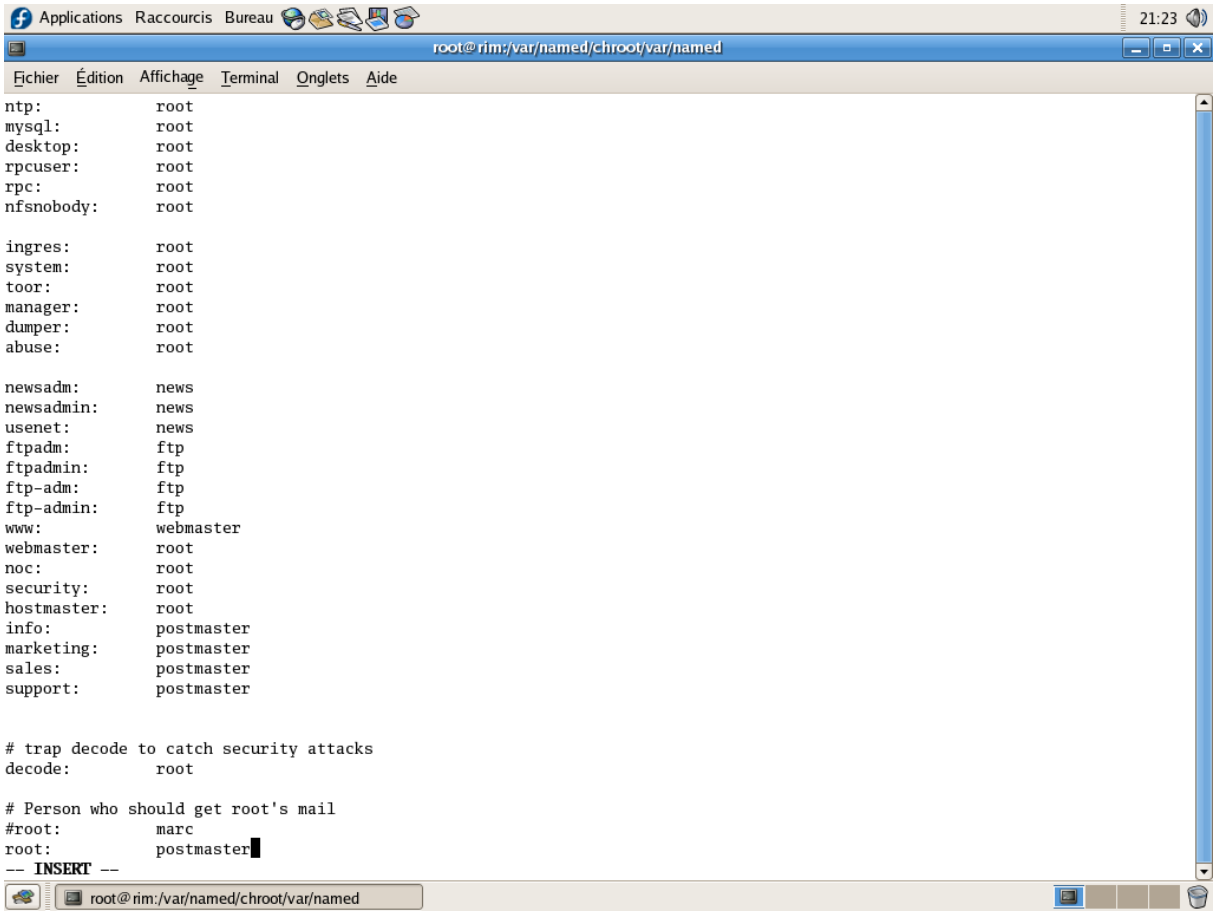
Autoriser toutes les adresses IPV4 et IPV6

Listen = [::]



Modification du fichier /etc/aliases

Root: postmaster



Démarrage des services

/etc/init.d/network start

/etc/init.d/bind start

/etc/init.d/postfix start

/etc/init.d/dovecot start

/etc/init.d/httpd start

/newalises

Notre serveur de messagerie est enfin prêt pour être exploité.

Il ne nous reste qu'a créer des utilisateurs

/useradd espera –s /usr/bin/nologin

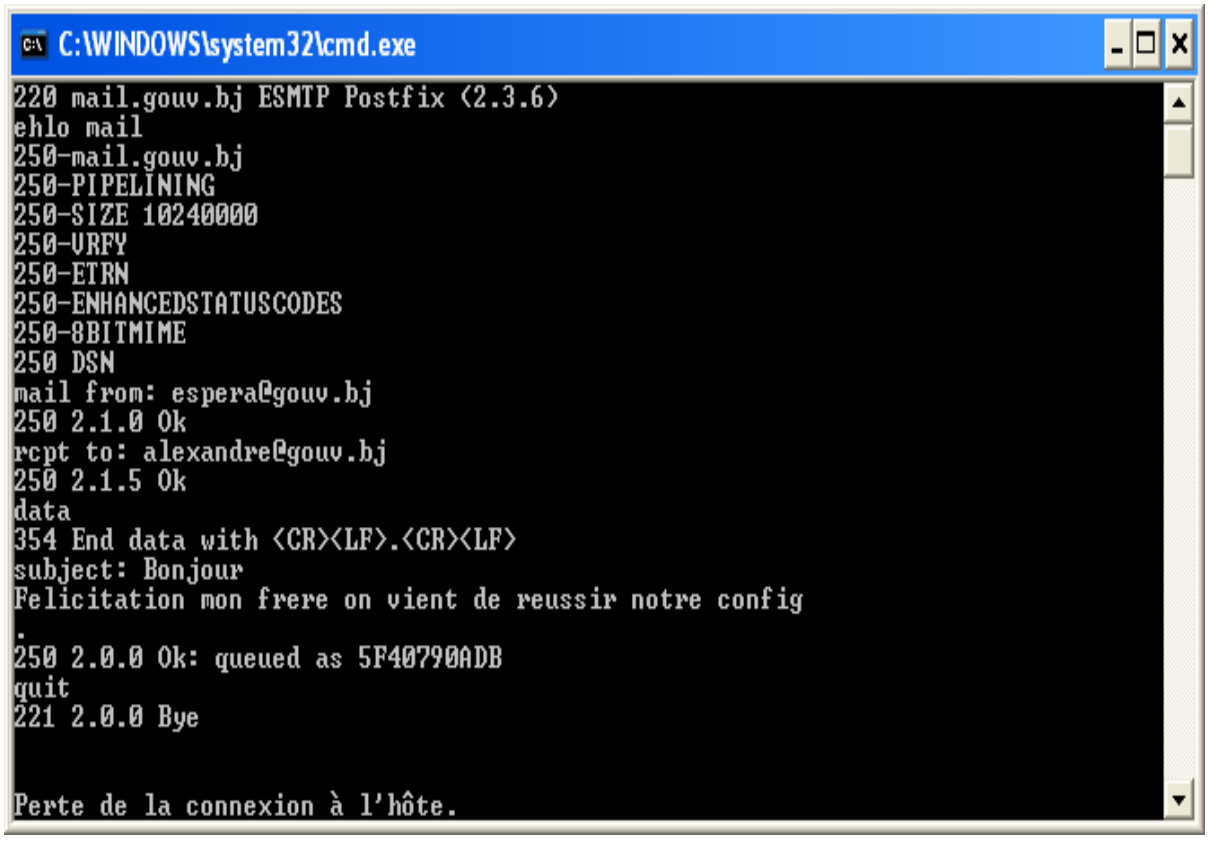
/Passwd @menne2006

/useradd alexandre –s /usr/bin/nologin

/Passwd @menne2006

Test du serveur SMTP

C:\Documents and settings\Admin> telnet mail.gouv.bj 25



II- CONFIGURATION DES CLIENTS (SquirrelMail et Outlook)

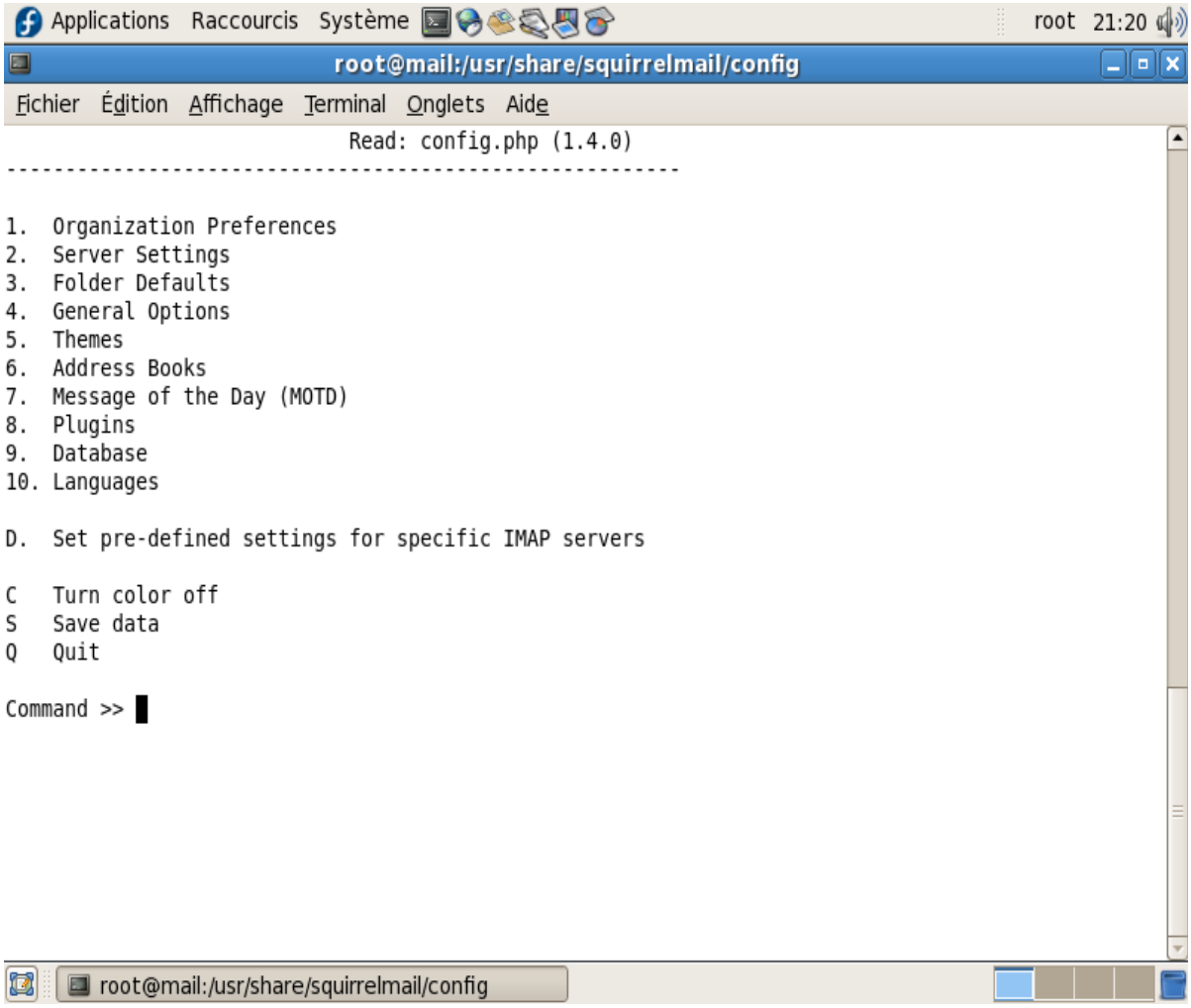
A. Mise en place d’un webmail avec SquirrelMail

SquirrelMail est un webmail (c'est-à-dire une interface web pour consulter son courrier électronique), initié par Nathan et Luke Ehresman, écrit en PHP4. Il supporte les protocoles IMAP et SMTP, et toutes les pages sont générées en HTML pur (sans aucun JavaScript), ceci afin d'être compatible avec le maximum de navigateurs.

Son objectif est de fournir une compatibilité optimale pour se rendre aussi accessible que possible. Parce que c'est un logiciel libre sous licence GPL, il est adaptable à toute sorte d'architecture.

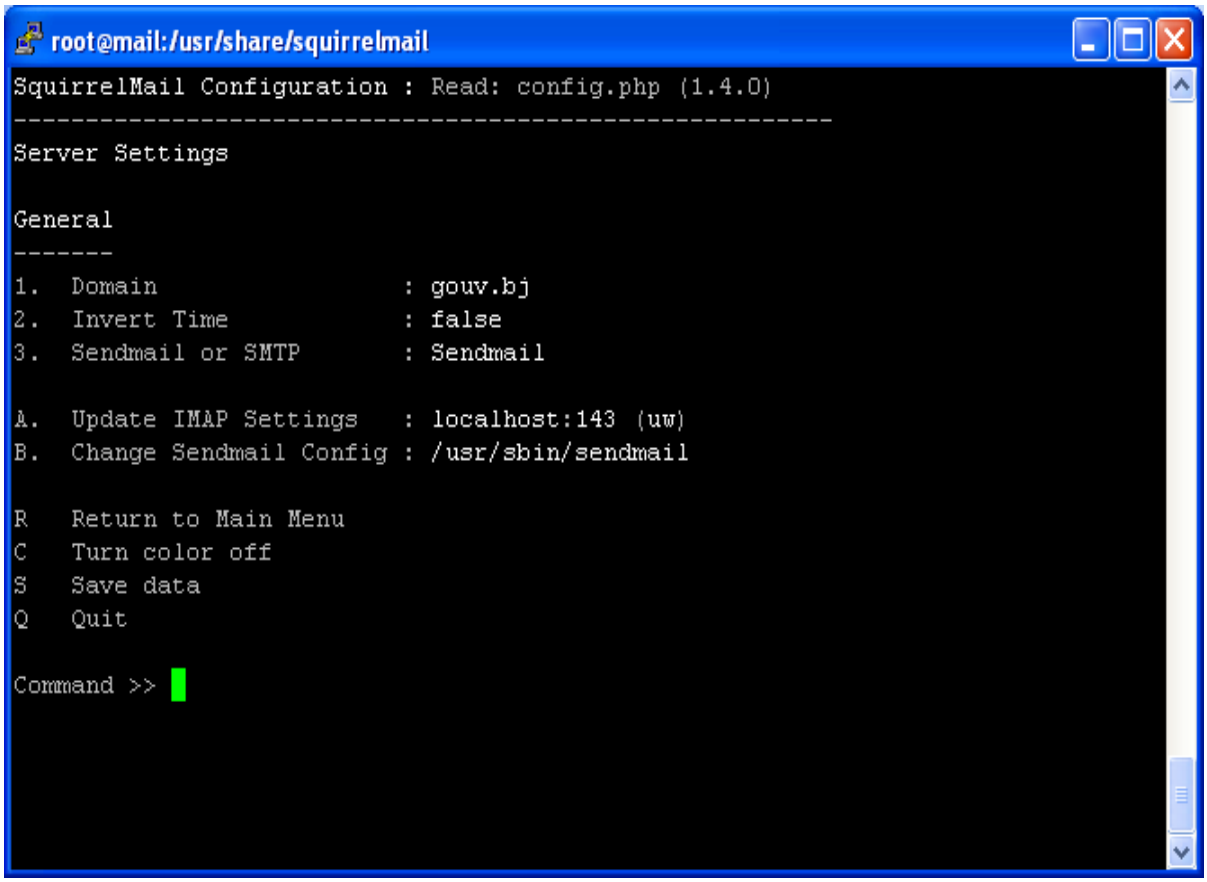
Configuration

La configuration squirrelmail peut se faire soit manuellement en éditant le fichier config.php (répertoire /usr/share/squirrelmail/config) pour modifier ses paramètres, soit, beaucoup plus convivial, en utilisant le petit script perl conf.pl situé dans ce même répertoire. Pour le lancer : ./conf.pl (point slash conf.pl). Un menu comportant dix (10) options apparaît, qui permet de configurer complètement SquirrelMail.



Quelques modifications à effectuer :

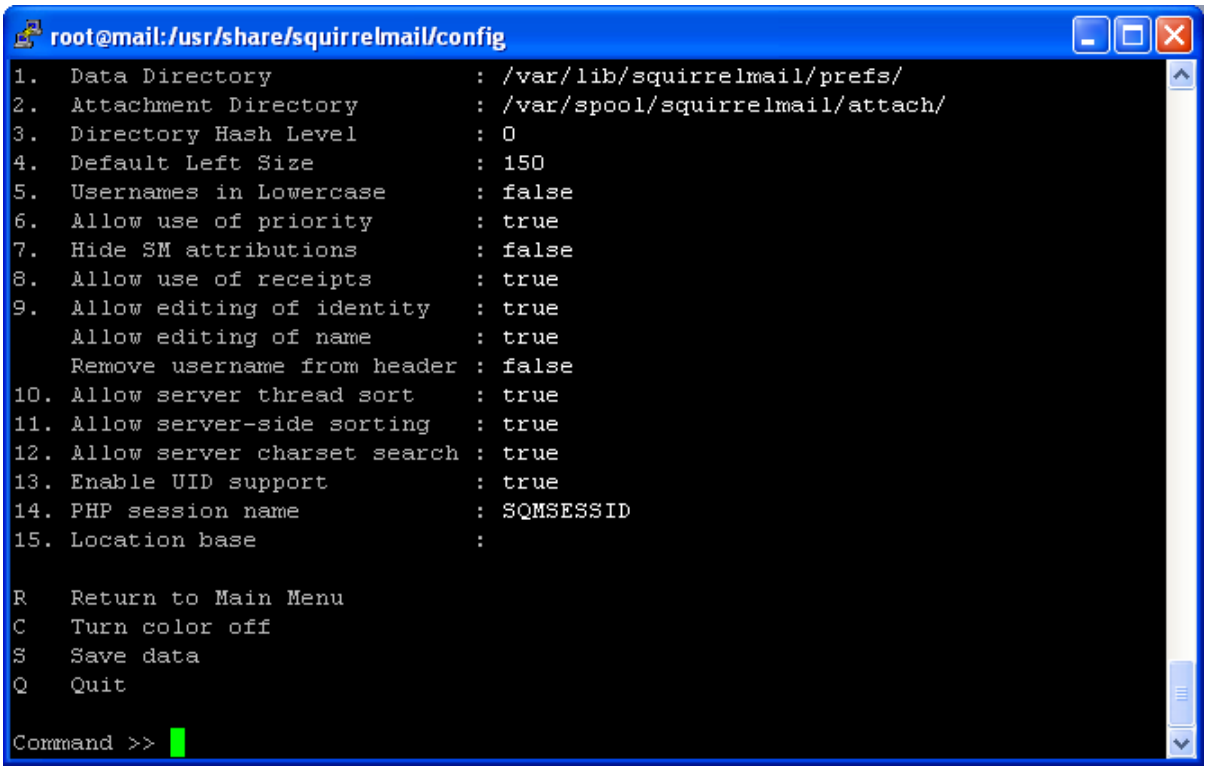
- Server Settings / Domain : gouv.bj



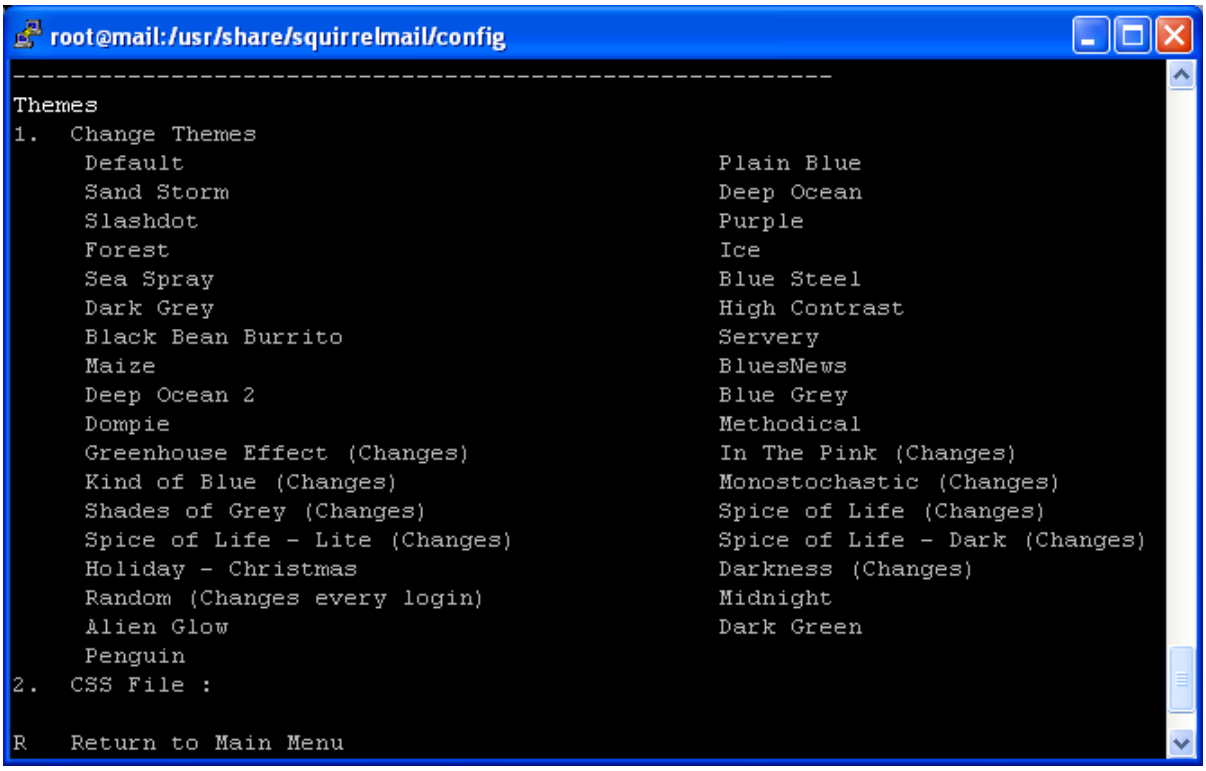
General Options

/ Data Directory : /var/lib/squirrelmail/prefs

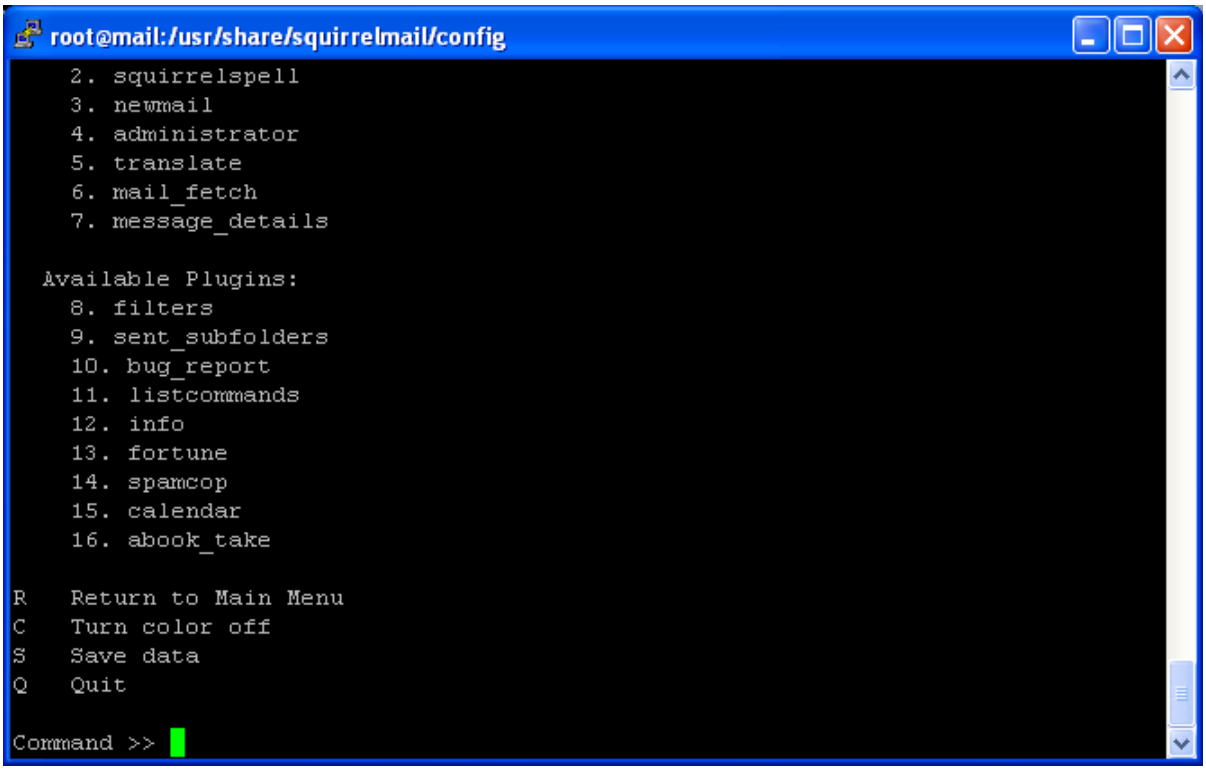
/var/spool/squirrelmail/attach



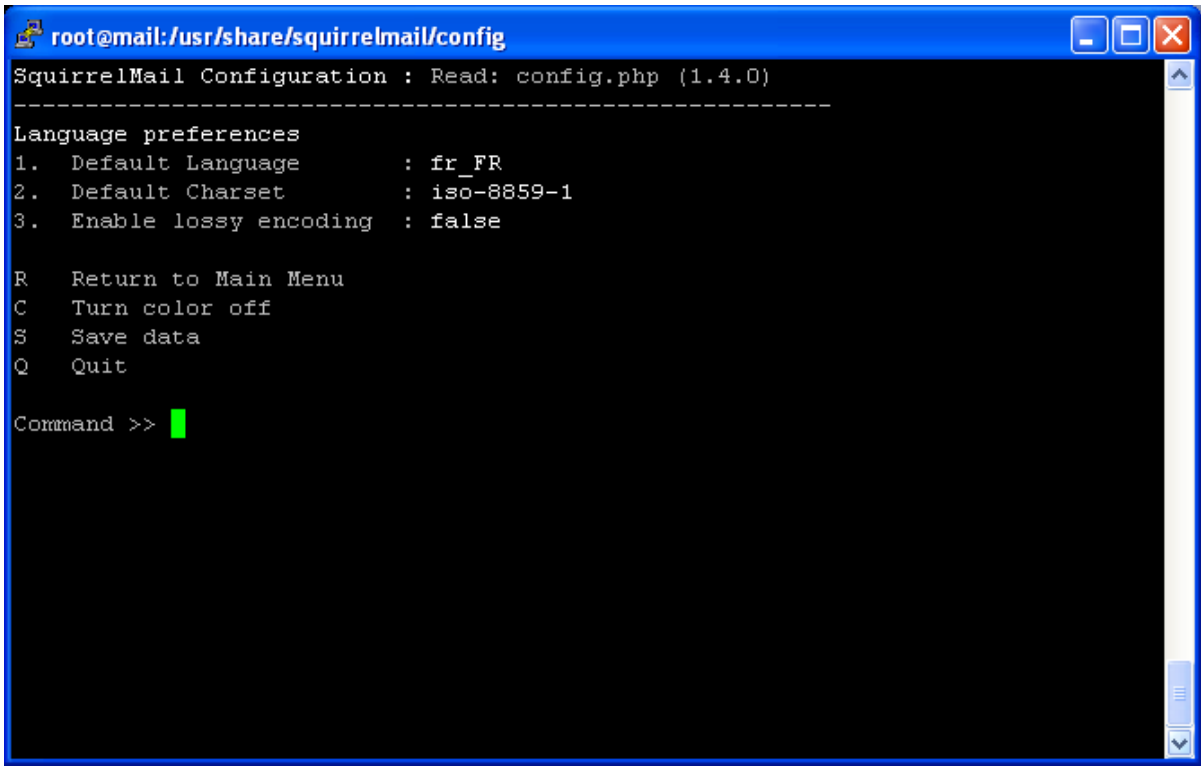
- Themes: pour choisir celui qui vous plaît!



- Plugins : pour installer un plugin, parmi ceux disponibles (Available Plugins)

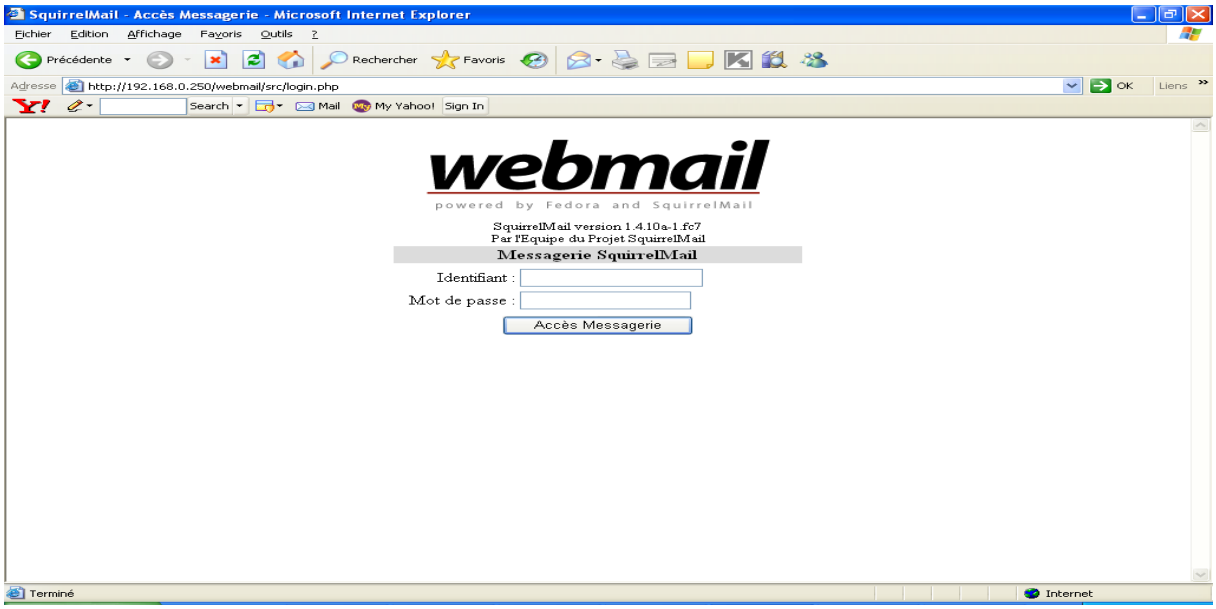


- Langage : Default Langage : remplacer en_US par fr_FR

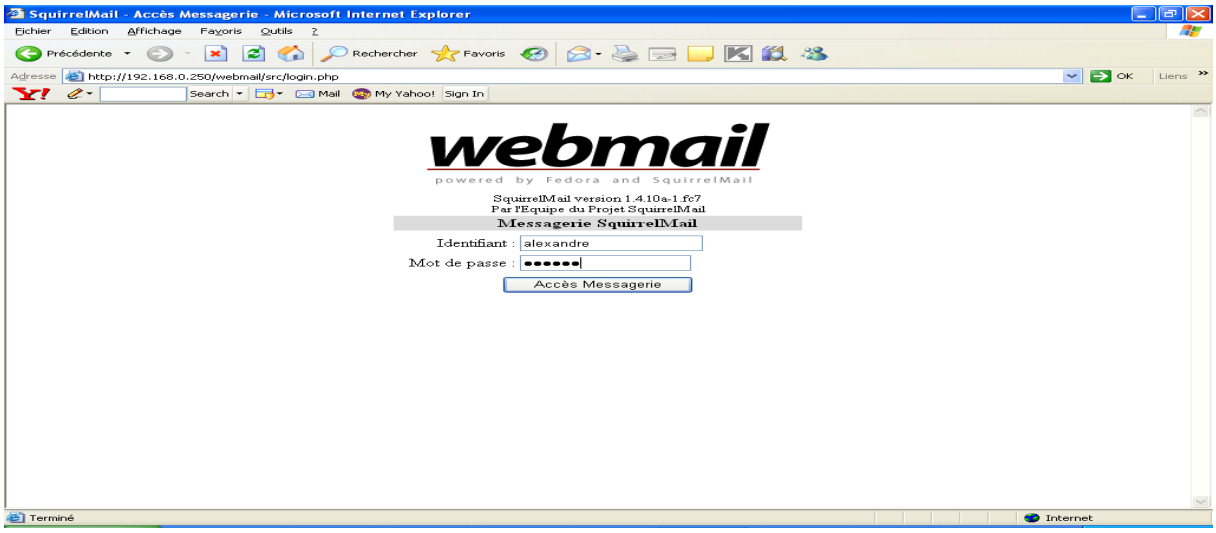


- S sauve ces modifications, Q quitte l'application de configuration.

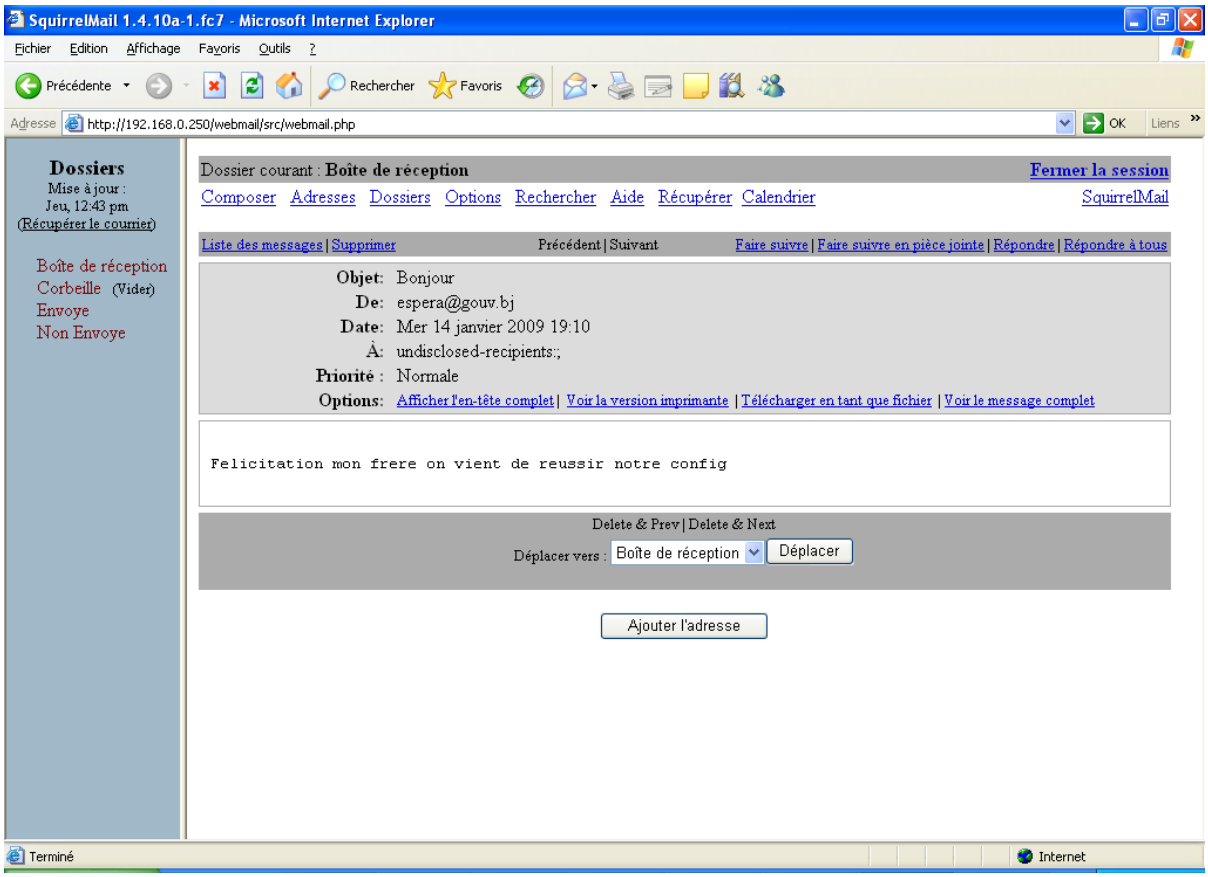
Puis, à partir d'un navigateur sur un poste distant, se rendre à l'url http:// mail.gouv.bj /webmail


SquirrelMail - Accès Messagerie - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Précédente
Rechercher
Favoris
Adresse
http://192.168.0.250/webmail/src/login.php
OK
Liens
Search
Mail
My Yahoo!
Sign In
webmail
powered by Fedora and SquirrelMail
SquirrelMail version 1.4.10a-1.fc7
Par l'Equipe du Projet SquirrelMail
Messagerie SquirrelMail
Identifiant :
Mot de passe :
Accès Messagerie
Terminé
Internet

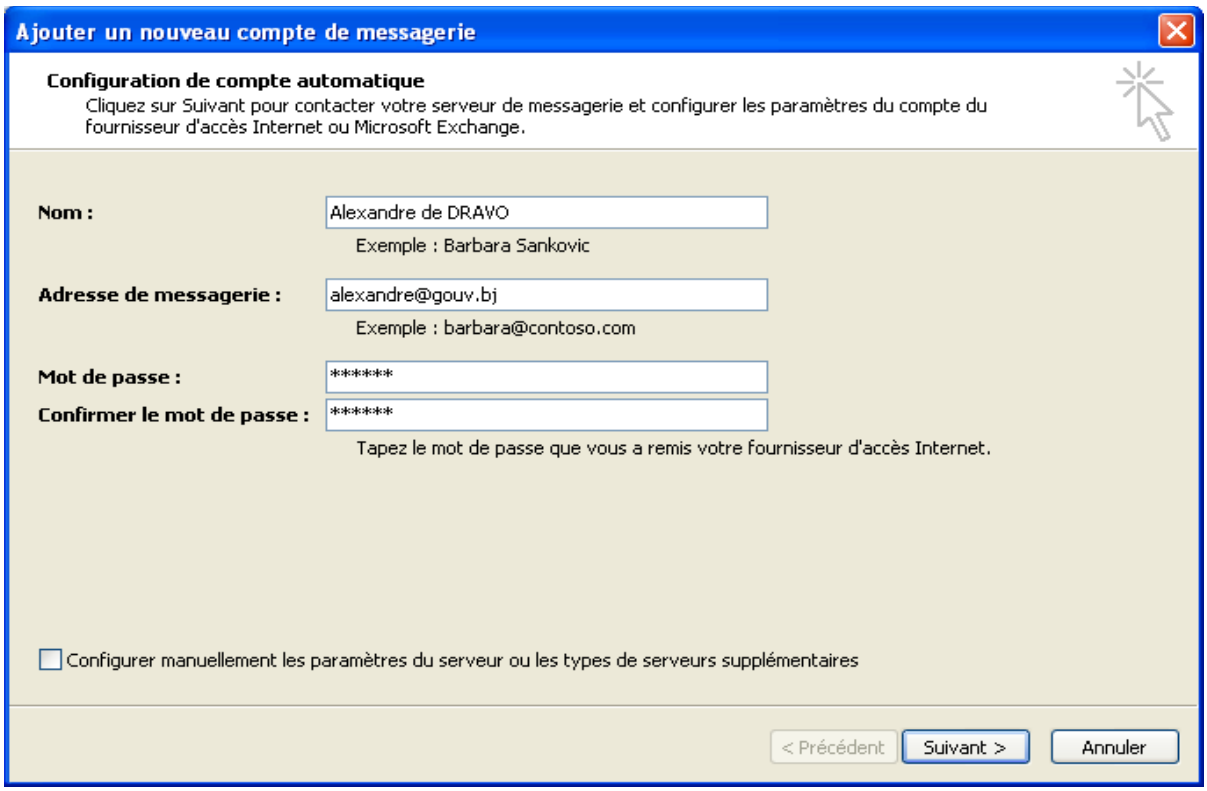
Connectons-nous à présent avec le compte alexandre sur notre webmail

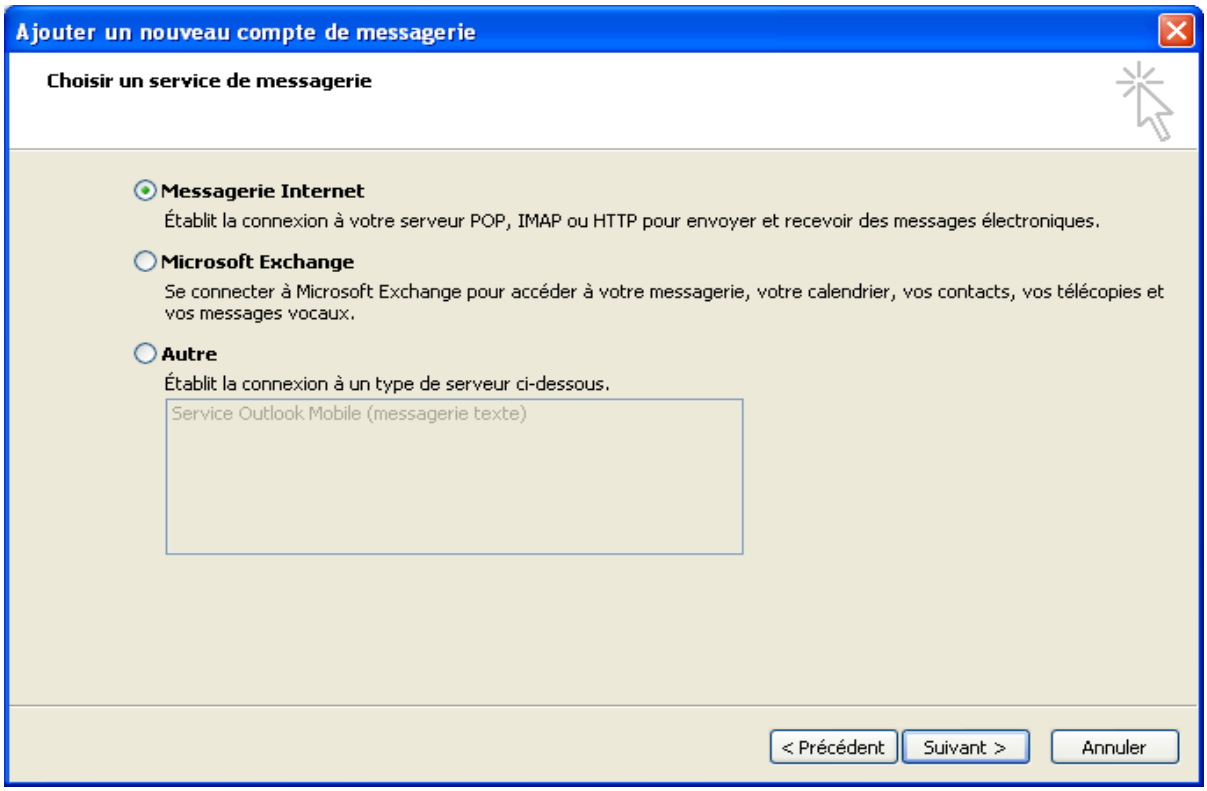


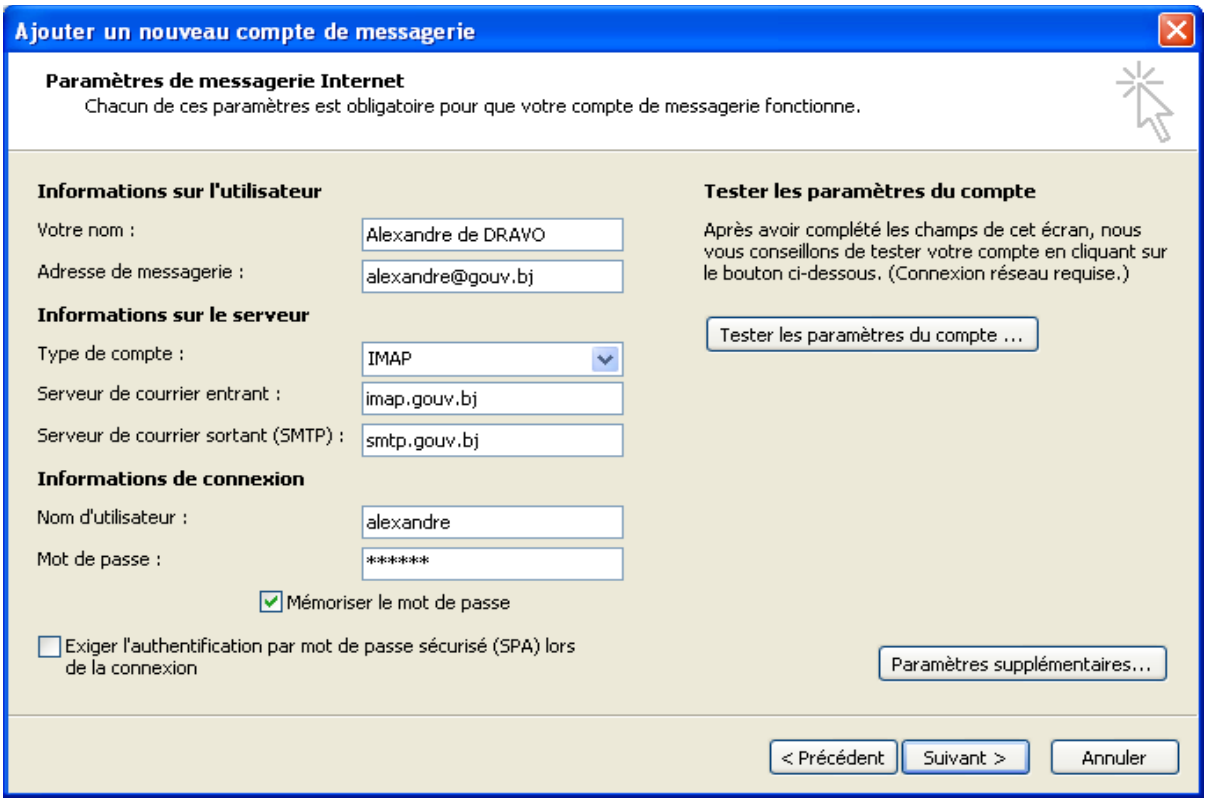
Nous constatons que le message envoyé par espera@gouv.bj à alexandre@gouv.bj en ligne de commande, apparaît bien dans la boîte aux lettres d'Alexandre sur Squirrelmail.

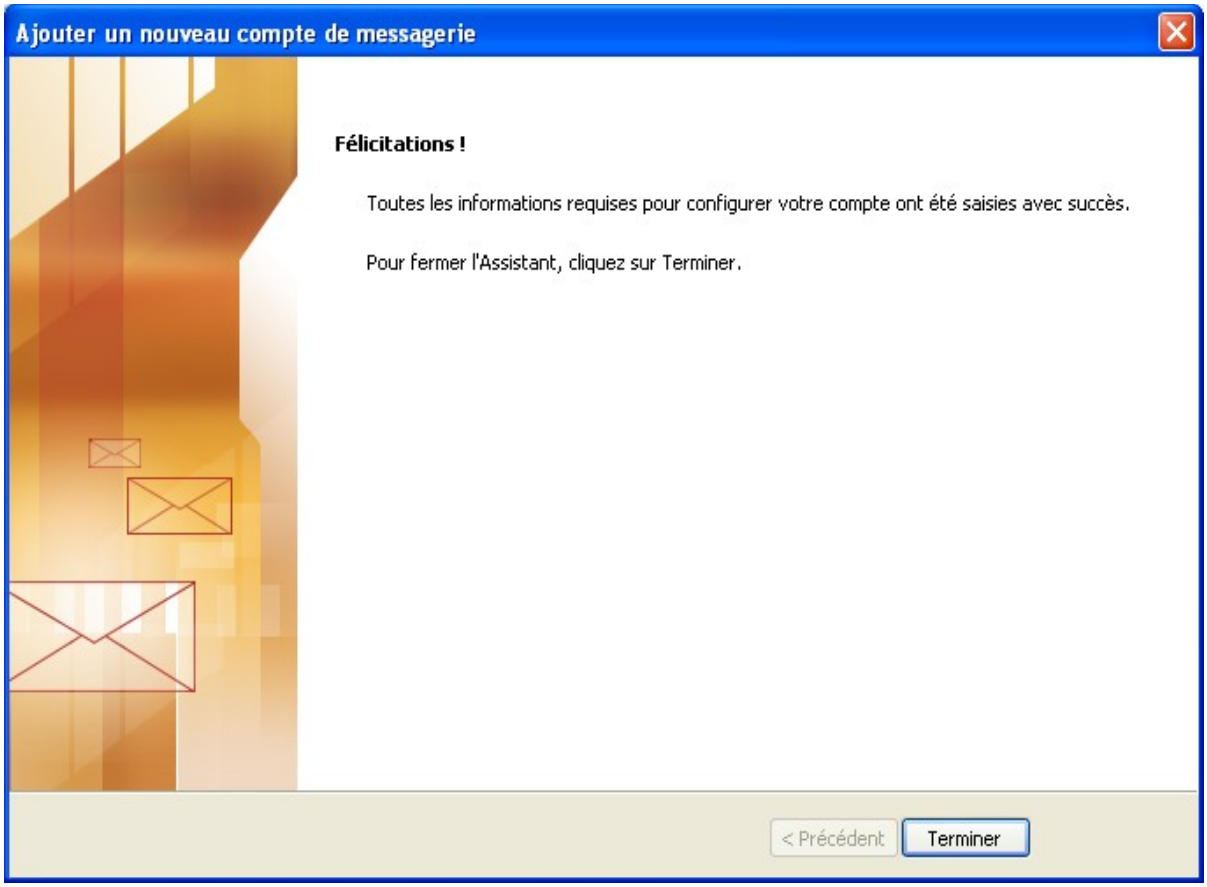


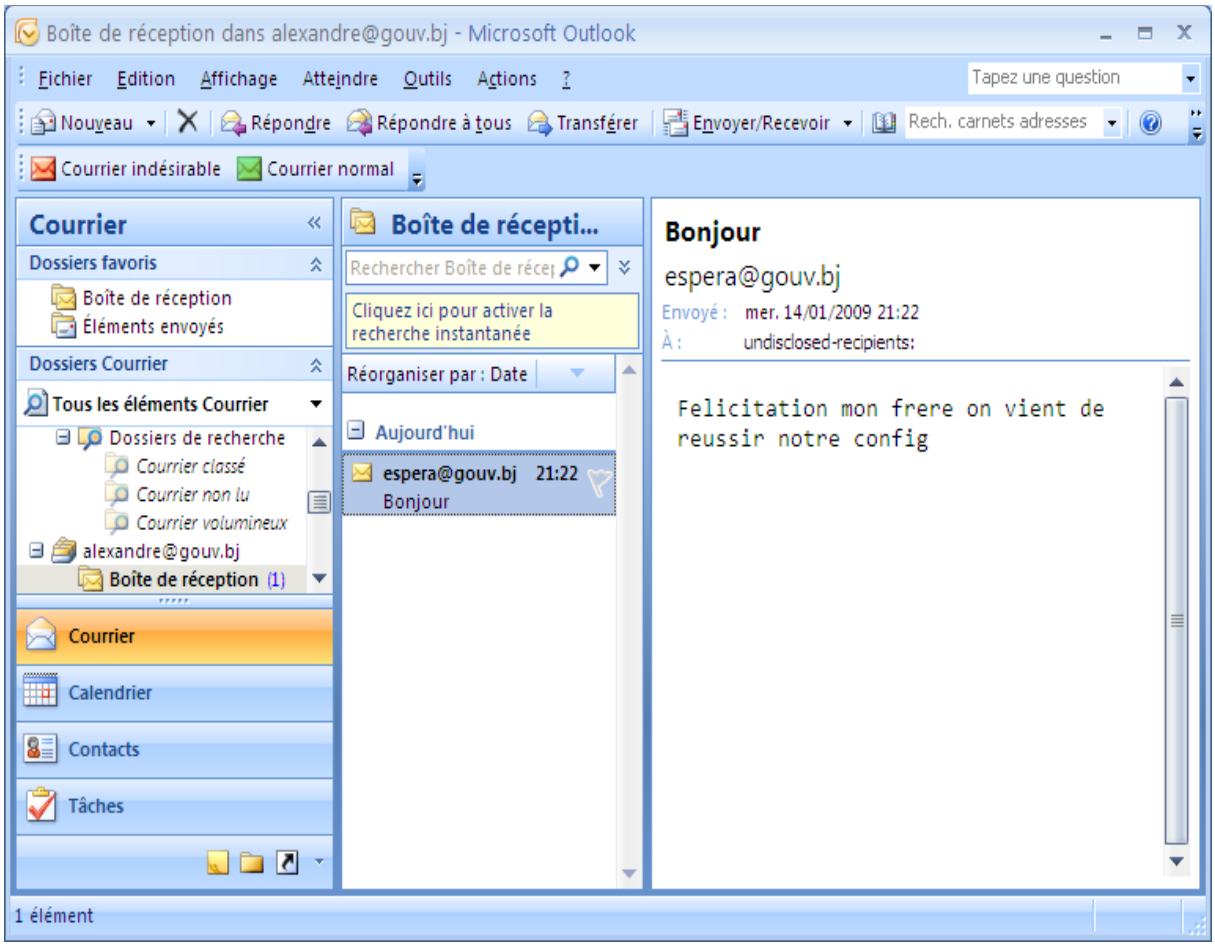
B. Configuration du client de Messagerie Outlook






Ajouter un nouveau compte de messagerie
Paramètres de messagerie Internet
Chacun de ces paramètres est obligatoire pour que votre compte de messagerie fonctionne.
Informations sur l'utilisateur
Votre nom :
Alexandre de DRAVO
Adresse de messagerie :
alexandre@gouv.bj
Informations sur le serveur
Type de compte :
IMAP
Serveur de courrier entrant :
imap.gouv.bj
Serveur de courrier sortant (SMTP) :
smtp.gouv.bj
Informations de connexion
Nom d'utilisateur :
alexandre
Mot de passe :
****
Mémoriser le mot de passe
Exiger l'authentification par mot de passe sécurisé (SPA) lors de la connexion
Tester les paramètres du compte
Après avoir complété les champs de cet écran, nous vous conseillons de tester votre compte en cliquant sur le bouton ci-dessous. (Connexion réseau requise.)
Tester les paramètres du compte ...
Paramètres supplémentaires...
< Précédent
Suivant >
Annuler


Ajouter un nouveau compte de messagerie
Félicitations !
Toutes les informations requises pour configurer votre compte ont été saisies avec succès.
Pour fermer l'Assistant, cliquez sur Terminer.
< Précédent
Terminer


Boîte de réception dans alexandre@gouv.bj - Microsoft Outlook
Fichier Edition Affichage Atteindre Outils Actions ?
Tapez une question
Nouveau Répondre Répondre à tous Transférer Envoyer/Recevoir Rech. carnets adresses
Courrier indésirable Courrier normal
Courrier
Dossiers favoris
Boîte de réception
Éléments envoyés
Dossiers Courrier
Tous les éléments Courrier
Dossiers de recherche
Courrier classé
Courrier non lu
Courrier volumineux
alexandre@gouv.bj
Boîte de réception (1)
Courrier
Calendrier
Contacts
Tâches
Boîte de récepti...
Rechercher Boîte de réce
Cliquez ici pour activer la recherche instantanée
Réorganiser par : Date
Aujourd'hui
espera@gouv.bj 21:22
Bonjour
Bonjour
espera@gouv.bj
Envoyé : mer. 14/01/2009 21:22
À : undisclosed-recipients:
Felicitation mon frere on vient de reussir notre config
1 élément

CONCLUSION

La messagerie électronique reste le moyen le plus efficace pour l'envoi et la réception des messages. Postfix permet une bonne compatibilité avec les fichiers de conf de sendmail et une excellente portabilité sur plusieurs plateformes.

La mise en place du serveur de messagerie à l'Administration Générale du Gouvernement facilitera l'échange des données en toute sécurité et rendra les agents plus productifs

Nous souhaiterions que le serveur de messagerie Postfix qui reste un logiciel libre, résistant bien à la charge et très sécurisé, puisse participer aussi à l'amélioration des prestations et des chiffres d'affaire des entreprises.