

Table des matières :

Table des matières :.....	1
Objectif :.....	2
1. Le serveur DNS.....	2
1. Configuration	3
1. Configuration de postfix en serveur pour un domaine	12
1. Installation d'un serveur IMAP.....	13
1. Le webmail	13
1. Installation et paramétrage	14
1. Tests de l'interface	17
1. Personnaliser l'interface	19
1. Administration de Squirrelmail	19
1. Conclusion.....	20
1. Sécurisation du serveur de courriers.....	21

Avant-Propos

Compétences :

- A1.1.1 Analyse du cahier des charges d'un service à produire
- A1.2.4 Déterminer des tests nécessaires à la validation d'un service (3)
- A4.1.9 Rédaction d'une documentation technique

```
GNU nano 2.2.6 Fichier : /etc/hosts
127.0.0.1 localhost
127.0.1.1 dns.rt2a.local dns
192.168.1.144 dns.rt2a.local dns_
```

```
GNU nano 2.2.6 Fichier : /etc/hosts
127.0.0.1 localhost
127.0.1.1 mail.rt2a.local dns
192.168.1.145 mail.rt2a.local dns
```

```
DNS pour serveur de courrier [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Input Périphériques Aide
GNU nano 2.2.6 Fichier : /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
    address 192.168.1.144
    netmask 255.255.255.0
    gateway 192.168.1.254
    dns-nameservers 127.0.0.1 192.168.1.254
    dns-search rt2a.local_
```

```
POSTFIX [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Input Périphériques Aide
GNU nano 2.2.6 Fichier : /etc/network/

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
    address 192.168.1.145
    netmask 255.255.255.0
    gateway 192.168.1.254_
# This is an autoconfigured IPv6 interface
```

Objectif :

Dans cette procédure, nous allons montrer comment installer et configurer un serveur de courrier Postfix sous Debian.

OS	Distribution	Version
Debian	Linux	8.5

1. Le serveur DNS

1. Configuration

```
root@dns:~# nano /etc/bind/named.conf.local
```

```
GNU nano 2.2.6      Fichier : /etc/bind/named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used
// organization
//include "/etc/bind/zones.rfc1918";
//resolution des noms en adresses IP
zone "rt2a.local" IN {
    type master;
    file "/etc/bind/zone.rt2a.local";
};
//resolution inverse des adresses IP
zone "1.168.192.in-addr.arpa" IN {
    type master;
    file "/etc/bind/rev.192.168.1";
};
```

```
root@dns:~# named-checkconf /etc/bind/named.conf.local
```

```
GNU nano 2.2.6      Fichier : /etc/resolv.conf
domain rt2a.local
search rt2a.local
nameserver 192.168.1.144

nameserver 192.168.1.254
```

```
GNU nano 2.2.6      Fichier : /etc/bind/zone.rt2a.local
;
; BIND data file for local loopback interface
;
$TTL      86400
rt2a.local. IN SOA      dns.rt2a.local. mail.rt2a.local. (
2016112110 ; Serial
86400 ; Refresh
21600 ; Retry
3600000 ; Expire
3600 ; Negative Cache TTL
)

rt2a.local. IN NS dns.
dns.rt2a.local. IN A 192.168.1.144
```

```
root@dns:~# named-checkzone rt2a.local /etc/bind/zone.rt2a.local
zone rt2a.local/IN: loaded serial 2016112110
OK
```

```
GNU nano 2.2.6      Fichier : rev.192.168.1
;
; BIND data file for local loopback interface
;
$TTL 86400
1.168.192.in-addr.arpa. IN SOA dns.rt2a.local. root.rt2a.local. (
2016112101 ; Serial
86400 ; Refresh
21600 ; Retry
3600000 ; Expire
3600 ; Negative Cache TTL
)

1.168.192.in-addr.arpa. IN NS dns.

144 PTR dns.
```

```
root@dns:/etc/bind# named-checkzone 1.168.192.in-addr.arpa rev.192.168.1
zone 1.168.192.in-addr.arpa/IN: loaded serial 2016112112
OK
```

```
root@dns:/etc/bind# service bind9 restart
root@dns:/etc/bind# nslookup 192.168.1.144
Server:      192.168.1.144
Address:     192.168.1.144#53

144.1.168.192.in-addr.arpa      name = dns.

root@dns:/etc/bind# nslookup dns.rt2a.local
Server:      192.168.1.144
Address:     192.168.1.144#53

Name:   dns.rt2a.local
Address: 192.168.1.144
```

Ajout de la configuration serveur DNS direct

```
GNU nano 2.2.6      Fichier : zone.rt2a.local
;
; BIND data file for local loopback interface
;
$TTL      86400
rt2a.local. IN SOA      dns.rt2a.local. mail.rt2a.local. (
2016112110 ; Serial
86400 ; Refrech
21600 ; Retry
3600000 ; Expire
3600 ; Negative Cache TTL
)

rt2a.local. IN NS dns.
dns.rt2a.local. IN A 192.168.1.144
mail.rt2a.local. IN A 192.168.1.145
rt2a.local. IN MX 10 mail.rt2a.local._
```

```
root@dns:/etc/bind# named-checkzone rt2a.local /etc/bind/zone.rt2a.local
zone rt2a.local/IN: loaded serial 2016112110
OK
```

Ajout de la configuration serveur DNS indirect

```

GNU nano 2.2.6          Fichier : rev.192.168.1
;
; BIND data file for local loopback interface
;
$TTL 86400
1.168.192.in-addr.arpa. IN SOA dns.rt2a.local. root.rt2a.local. (
2016112101 ; Serial
86400 ; Refresh
21600 ; Retry
3600000 ; Expire
3600 ; Negative Cache TTL
)
1.168.192.in-addr.arpa. IN NS dns.
144 PTR dns.
145 PTR mail._

```

```

root@dns:/etc/bind# named-checkzone 1.168.192.in-addr.arpa rev.192.168.1
zone 1.168.192.in-addr.arpa/IN: loaded serial 2016112101
OK

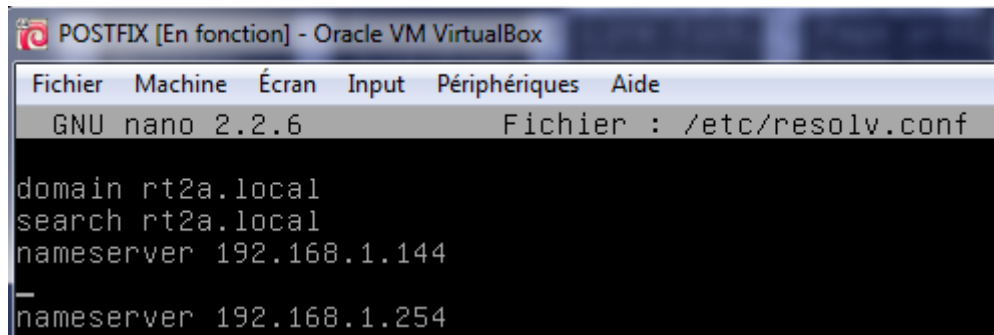
```

```

root@dns:/etc/bind# service bind9 restart

```

LE POSTE MAIL



```

POSTFIX [En fonction] - Oracle VM VirtualBox
Fichier  Machine  Écran  Input  Périphériques  Aide
GNU nano 2.2.6          Fichier : /etc/resolv.conf
domain rt2a.local
search rt2a.local
nameserver 192.168.1.144
_
nameserver 192.168.1.254

```

```

root@mail:~# nslookup 192.168.1.144
Server:          192.168.1.144
Address:         192.168.1.144#53

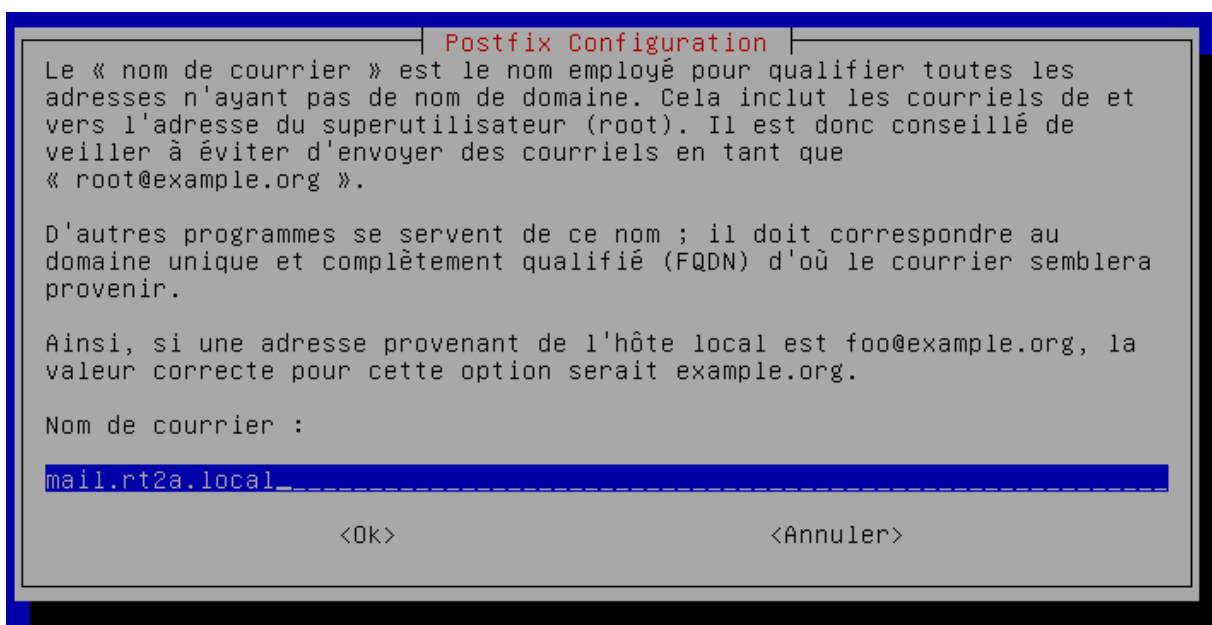
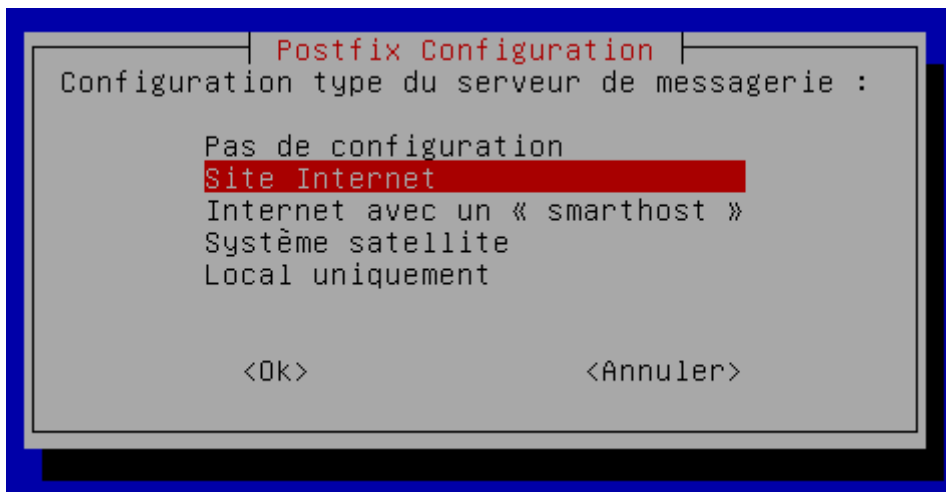
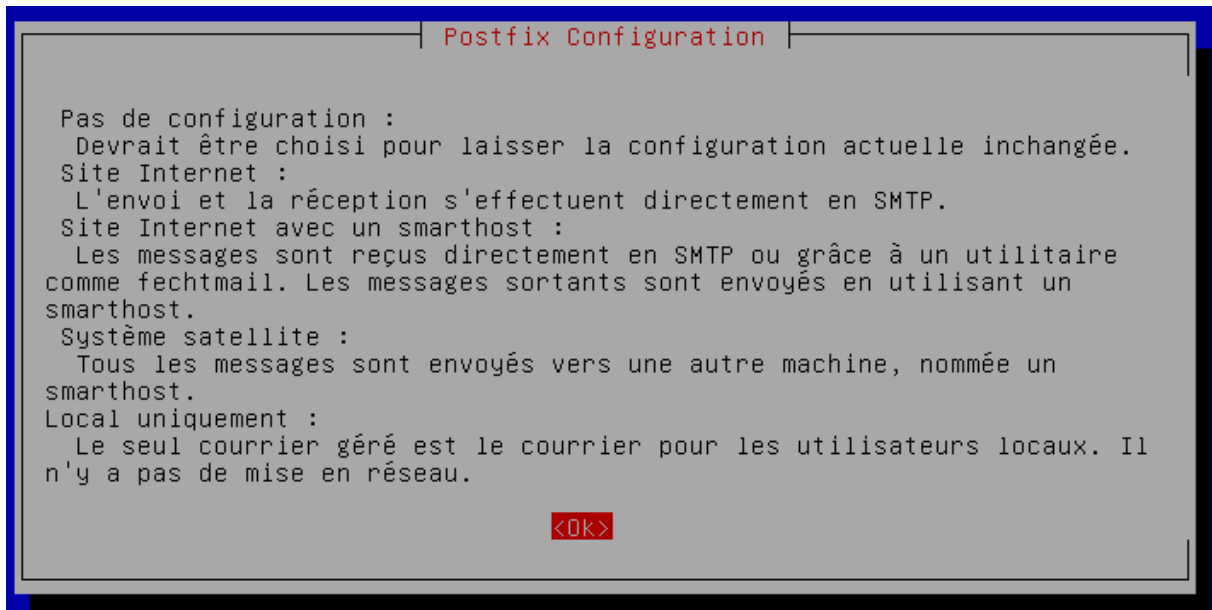
144.1.168.192.in-addr.arpa      name = dns.

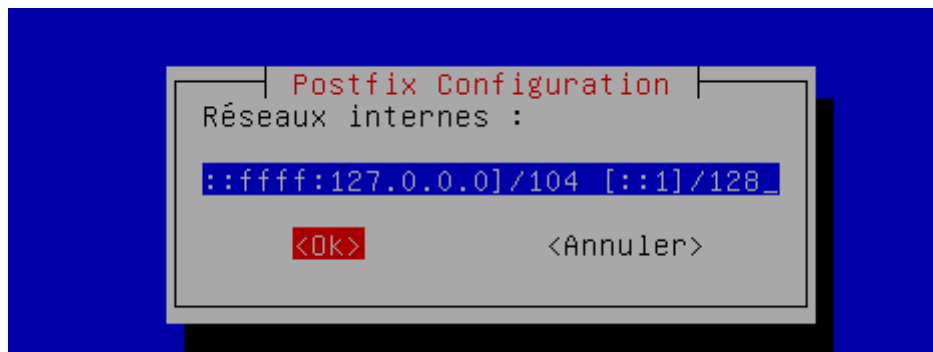
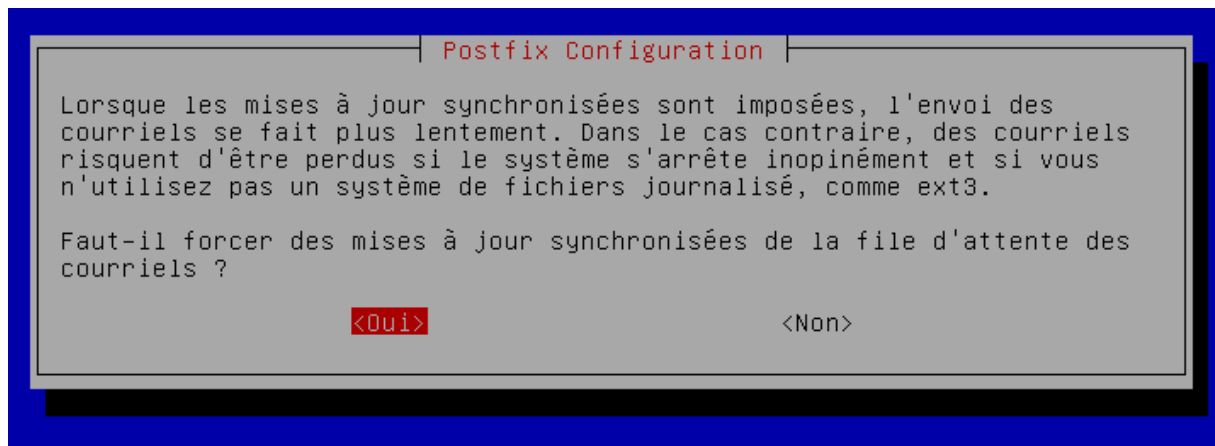
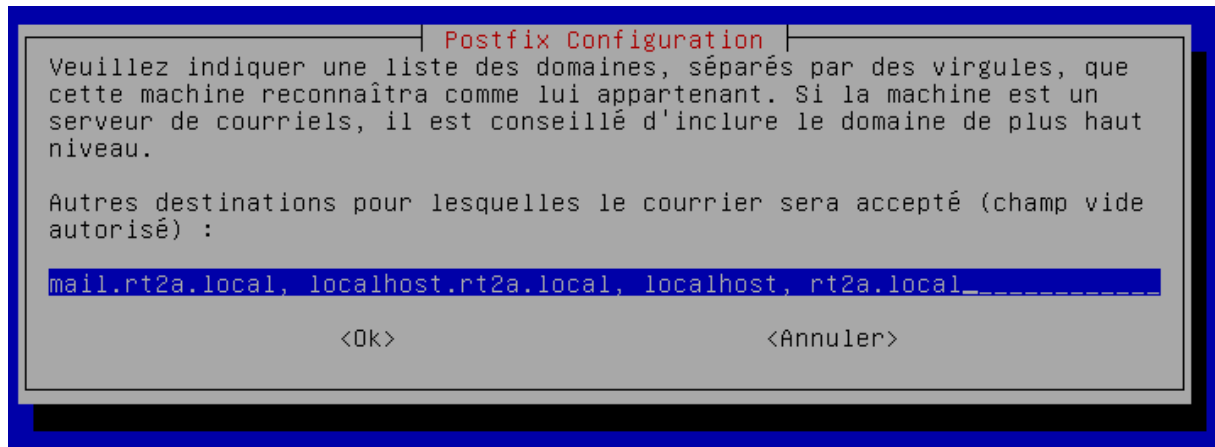
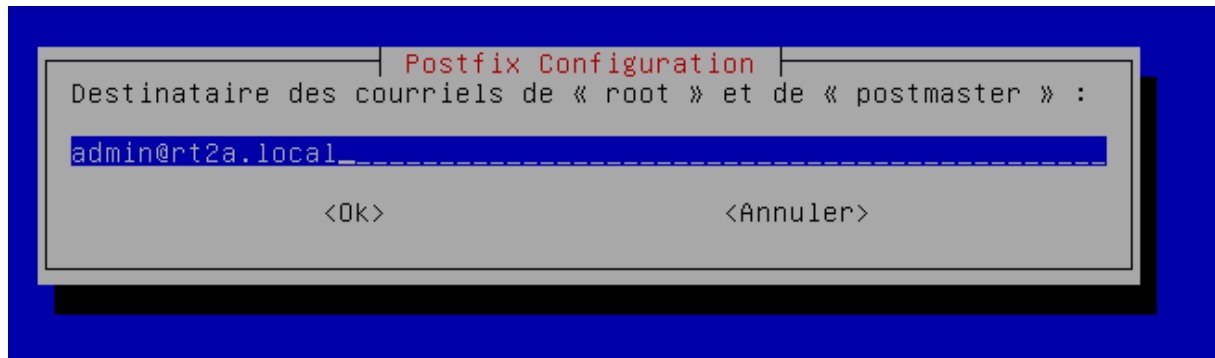
```

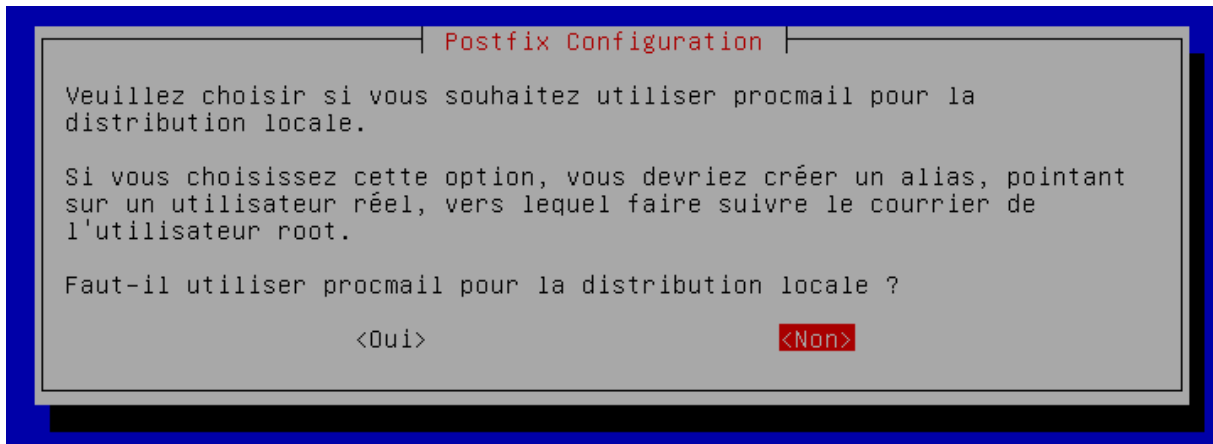
```

root@mail:~# apt-get --purge remove exim4 exim4-base exim4-config exim4-daemon-l
ight

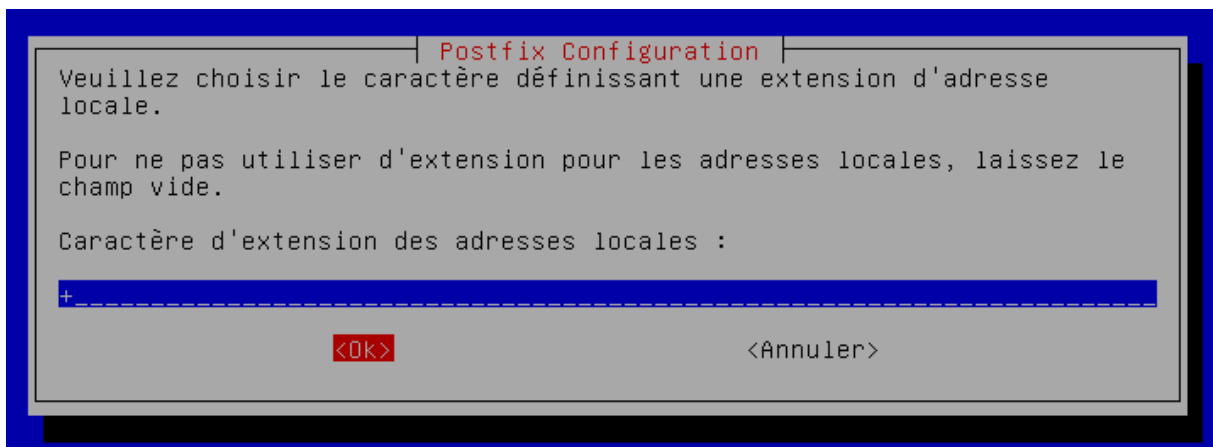
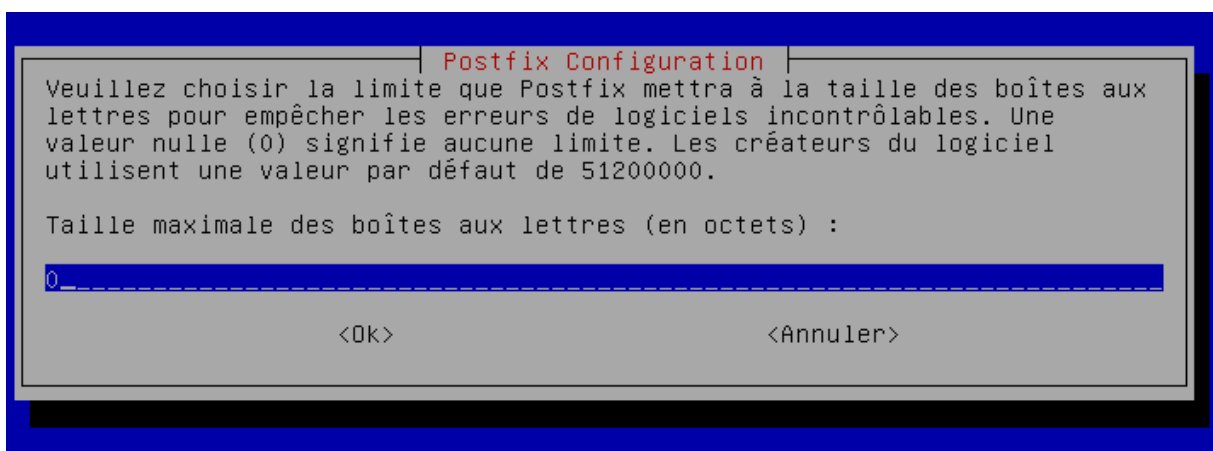
```

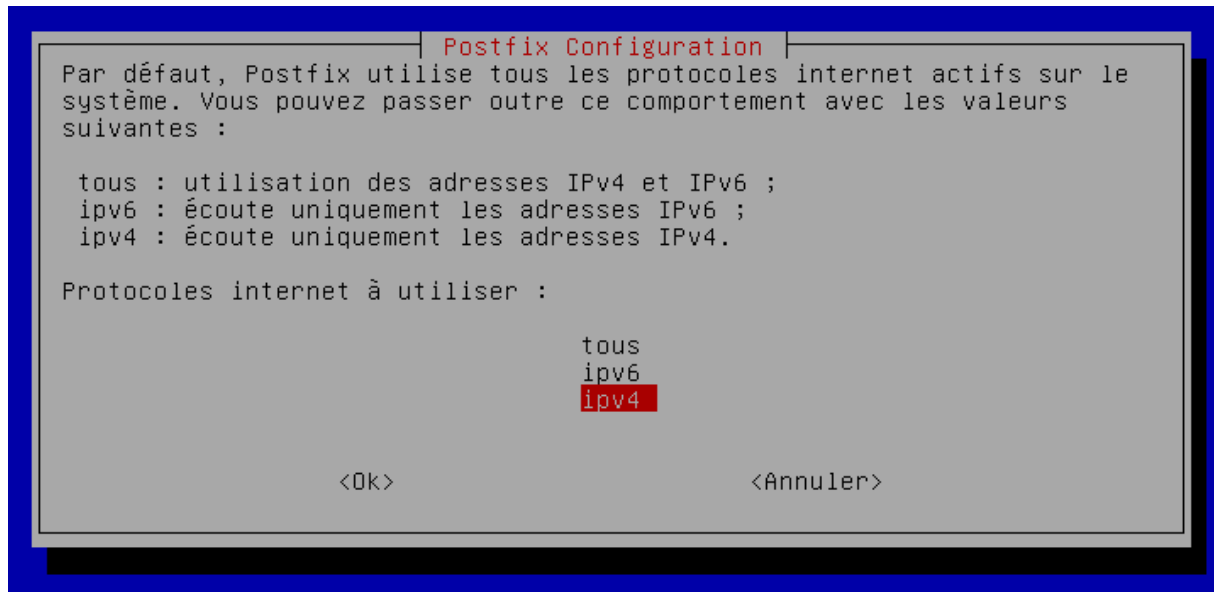






On laisse 0 car par défaut cela correspond a l'infinie.





```
GNU nano 2.2.6      Fichier : /etc/postfix/main.cf      Modifié
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_un$
myhostname = mail.rt2a.local
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = mail, mail.rt2a.local, localhost.rt2a.local, localhost, rt2a.lo$
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_command =
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = localhost
inet_protocols = ipv4_
```

```
GNU nano 2.2.6      Fichier : /etc/postfix/main.cf
myorigin = /etc/mailname
mydestination = mail, mail.rt2a.local, localhost.rt2a.loca
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_command =
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = localhost
inet_protocols = ipv4
home_mailbox = MailDir/_
```

Tester le fichier de configuration

```
root@mail:~# postconf -n
```

```
root@mail:~# service postfix restart
```

Premiers tests :

```
root@mail:~# telnet mail.rt2a.local 25
```

S'il y a une erreur, il faut refaire la configuration avec la commande « dpkg-reconfigure postfix »

Les commandes suivantes pour écrire un mail

```
root@mail:~# telnet mail.rt2a.local 25
Trying 127.0.1.1...
Connected to mail.rt2a.local.
Escape character is '^]'.
220 mail.rt2a.local SMTP Postfix (Debian/GNU)
mail from:root
250 2.1.0 Ok
rcpt to:antoineh
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
yolo000000000000test
.
250 2.0.0 Ok: queued as 5658A548
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Pour aller lire le mail, il suffit d'aller voir dans notre répertoire :

```
root@mail:~# nano /home/antoineh/MailDir/new/1479721015.V808I12M485498.mail
```

```
GNU nano 2.2.6 Fichier : ...ilDir/new/1479721015.V808I12M485498.mail
Return-Path: <root@mail.rt2a.local>
X-Original-To: antoineh
Delivered-To: antoineh@mail.rt2a.local
Received: from localhost (localhost [127.0.0.1])
        by mail.rt2a.local (Postfix) with SMTP id 9E2EE548
        for <antoineh>; Mon, 21 Nov 2016 10:36:15 +0100 (CET)
Message-Id: <20161121093638.9E2EE548@mail.rt2a.local>
Date: Mon, 21 Nov 2016 10:36:15 +0100 (CET)
From: root@mail.rt2a.local

yolo0000
```

Tester la syntaxe du fichier /etc/postfix/main.cf par

```
root@mail:~# /etc/init.d/postfix check
```

1. Configuration de postfix en serveur pour un domaine

Vous allez ajouter à votre serveur MTA la capacité d'un serveur POP. Pour cela il faut le transformer en serveur pour un domaine. Dovecot est un serveur IMAP et POP3 pour les systèmes d'exploitation Unix et dérivés.

```
root@mail:~# apt-get install dovecot-common dovecot-pop3d
```

Vous allez utiliser pour commencer une politique d'authentification simple en « plain text » (sans sécurité). Editer les fichiers /etc/dovecot/conf.d/10-auth.conf puis 20-pop3.conf et 10-mail.conf

```
GNU nano 2.2.6 Fichier : /etc/dovecot/conf.d/10-auth.conf
##
## Authentication processes
##
# Disable LOGIN command and all other plaintext authentications
# SSL/TLS is used (LOGINDISABLED capability). Note that if the r
# matches the local IP (ie. you're connecting from the same comp
# connection is considered secure and plaintext authentication i
# See also ssl=required setting.
disable_plaintext_auth = no_
```

```
GNU nano 2.2.6 Fichier : /etc/dovecot/conf.d/20-pop3.conf
#
# Note that Outlook 2003 seems to have problems with %v.%u format
# Dovecot's default, so if you're building a new server it would
# idea to change this. %08Xu%08Xv should be pretty fail-safe.
#
pop3_uidl_format = %08Xu%08Xv
```

```
# <doc/wiki/MailLocation.txt>
#
mail_location = maildir:/home/%u/MailDir_
```

Relancer le serveur dovecot

```
root@mail:~# service dovecot restart
```

```
root@mail:~# telnet mail.rt2a.local 110
Trying 127.0.1.1...
Connected to mail.rt2a.local.
Escape character is '^]'.
+OK Dovecot ready.
```

1. Installation d'un serveur IMAP

```
root@mail:~# apt-get install dovecot-imapd
```

Fair en sorte que le service Dovecot utilise le protocole IMAP en plus de POP3.

Utiliser l'utilitaire Telnet pour regarder la bonne réactivité de Postfix

```
root@mail:~# telnet mail.rt2a.local 143
Trying 127.0.1.1...
Connected to mail.rt2a.local.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot ready.
```

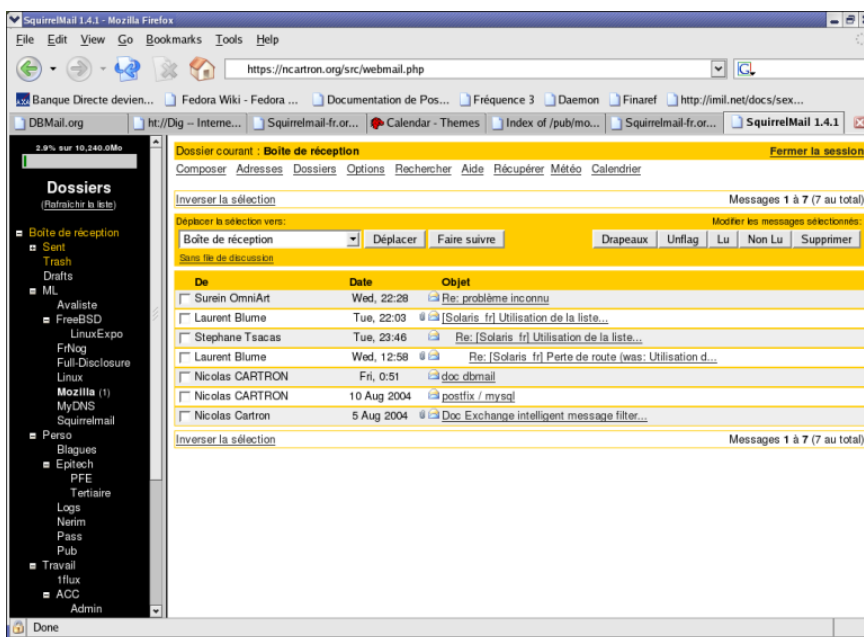
1. Le webmail

Squirrelmail est un webmail sous licence GPL écrit en PHP4. Il supporte les protocoles IMAP et SMTP, et toutes les

pages générées le sont en pur HTML (sans aucun Javascript), ceci afin d'être compatible avec la plupart des

navigateurs. Squirrelmail inclut de base toutes les options de bases d'un logiciel de messagerie : le support MIME, un

carnet d'adresses, et la création de dossiers pour trier vos e-mails.



1. Installation et paramétrage

Sont nécessaires à l'installation de Squirrelmail :

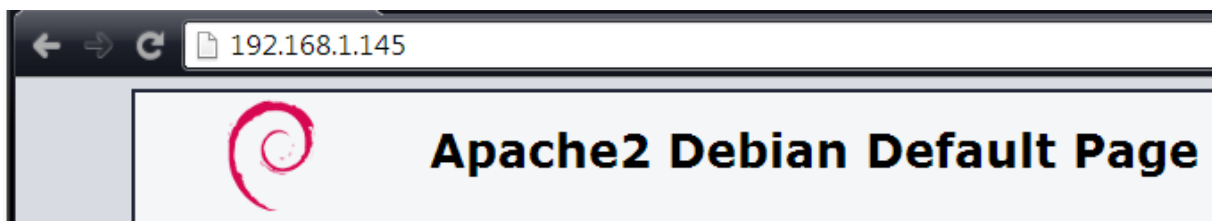
- ☐ Un serveur web (Apache étant le plus utilisé),
- ☐ Le langage PHP 4 ou 5,
- ☐ Un serveur SMTP (Sendmail, Postfix, Qmail, Microsoft Exchange, ...),
- ☐ Un serveur IMAP,
- ☐ Eventuellement Perl (pour la partie configuration).

Vérifier la présence et le bon fonctionnement d'Apache et de Php. Réaliser une page de test en insérant la

commande `phpinfo()`.

On commence par installer apache

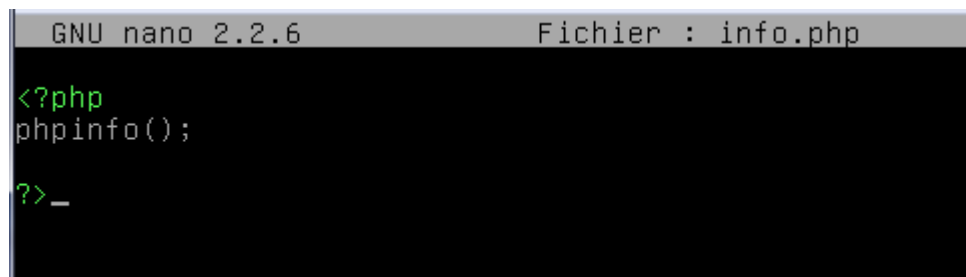
```
root@mail:~# apt install apache2
```



On installe ensuite php5

```
apt install php5_
```

On crée un fichier php dans /var/www/html



On peut apporter quelques modifications si nécessaires au fichier php.ini :

```
$ nano /etc/php5/apache2/php.ini
```

session.use_cookies = 1	
file_uploads = On	autoriser les fichiers attachés
upload_max_filesize = 2M	taille maxi des fichiers attachés
register_globals=off	il est placé par défaut sur On par la distribution Mandrake
expose_php = Off	sécurité : n'expose pas le fait que votre serveur héberge PHP

La dernière version stable est squirrelmail-1.4.22. Procéder à l'installation des paquetages nécessaires :

```
root@mail:~# apt install squirrelmail
```

Installer également dovecot-imapd pour le protocole imap. Il est déjà installer normalement.

Il vous faut procéder à une post configuration de Squirrelmail, ce que vous ferez avant une petite manipulation avec

Dovecot.

Lancer la configuration par squirrelmail-configure.

```
root@mail:~# squirrelmail-configure_
```

```
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Main Menu --
1. Organization Preferences
2. Server Settings
3. Folder Defaults
4. General Options
5. Themes
6. Address Books
7. Message of the Day (MOTD)
8. Plugins
9. Database
10. Languages

D. Set pre-defined settings for specific IMAP servers

C Turn color on
S Save data
Q Quit

Command >> _
```

- 1) Organization Preferences
- 2) Server Settings
- 3) Folder Defaults
- 4) General Options
- 5) Themes
- 6) Address Books (LDAP).
- 7) Message of the Day (MOTD)
- 8) Plugins
- 9) Database
- 10) Languages

Voici les quelques modifications à effectuer :

- Couleur du menu : choix C (Turn color off)
- Francisation de l'interface : remplacer en_US par fr_FR
- Réglage du serveur imap : Dovecot
- Thèmes : pour choisir celui qui vous plaît !
- Message du jour : Bienvenue au Webmail du Campus
- Plugins : pour installer un plugin, parmi ceux disponibles (Available Plugins)
- S sauve ces modifications
- Q quitte l'application de configuration.

Pour régler la couleur :

```
R Return to Main Menu
C Turn color off
S Save data
Q Quit

Command >> c_
```

```
General
-----
1. Domain : trim(implode('', file('/etc/'.(file_exists('/etc/mailname')?'mail':'host').'name')))
2. Invert Time : false
3. Sendmail or SMTP : SMTP

IMAP Settings
-----
4. IMAP Server : localhost
5. IMAP Port : 143
6. Authentication type : login
7. Secure IMAP (TLS) : false
8. Server software : dovecot
9. Delimiter : detect

B. Update SMTP Settings : localhost:25
H. Hide IMAP Server Settings

R Return to Main Menu
C Turn color off
S Save data
Q Quit
```

Ne pas oublier de faire toute les modifications et de sauvegarder

Squirrelmail comporte une mauvaise configuration de la langue française en ISO-8859-1 au lieu d'UTF-8. Il faut procéder à quelques modifications du code source Php.

Editer le fichier `/usr/share/squirrelmail/functions/i18n.php` et changer les lignes suivantes :

```
$languages*'fr_FR'+*'CHARSET'+ = 'UTF-8' ;
```

```
$languages*'fr_FR'+*'LOCALE'+ = array('fr_FR.UTF-8','fr_FR.UTF-8','fr_FR') ;
```

```
$languages['fr_FR']['NAME'] = 'French';
$languages['fr_FR']['CHARSET'] = 'UTF-8';
$languages['fr_FR']['LOCALE'] = array('fr_FR.UTF-8','fr_FR.UTF-8','fr_FR');
$languages['fr']['ALIAS'] = 'fr_FR';
```

Le problème de la langue persiste encore car vous n'avez pas les traductions des messages.

```
root@mail:~# aptitude install squirrelmail-locales
```

Choisissez le langage Fr.

Au niveau d'Apache, ajouter un lien symbolique pointant vers la page d'accueil de Squirrelmail.

```
root@mail:~# cd /var/www/html/
root@mail:/var/www/html# ln -s /usr/share/squirrelmail/
root@mail:/var/www/html# ls
index.html info.php squirrelmail
```

Vérifier la ligne dans le fichier `/etc/dovecot/dovecot.conf` :

```
protocols = imap pop3
```

Tester le serveur IMAP par la commande :

```
root@mail:~# lsof -i:143
COMMAND PID USER  FD  TYPE DEVICE SIZE/OFF NODE NAME
systemd   1 root   33u IPv4  10744    0t0  TCP *:imap2 (LISTEN)
systemd   1 root   34u IPv6  10745    0t0  TCP *:imap2 (LISTEN)
dovecot  487 root    3u IPv4  10744    0t0  TCP *:imap2 (LISTEN)
dovecot  487 root    4u IPv6  10745    0t0  TCP *:imap2 (LISTEN)
```

1. Tests de l'interface

A partir d'un navigateur, saisissez l'URL :

<http://192.168.1.145/squirrelmail> ou <http://mail.rt2a.local/squirrelmail> ou

<http://srt2a.fr/squirrelmail>

Tester aussi la configuration <http://rt2a.local/squirrelmail/src/configtest.php> et visualiser les erreurs éventuelles.

192.168.1.145/squirrelmail/src/configtest.php

SquirrelMail configtest

This script will try to check some aspects of your SquirrelMail configuration and point you to errors wherever it can find them. You need to go run `conf.pl` in the `config/` directory first before you run this script.

SquirrelMail version: 1.4.23 [SVN]
Config file version: 1.4.0
Config file last modified: 22 November 2016 08:30:03

Checking PHP configuration...
PHP version 5.6.27-0+deb8u1 OK.
Running as www-data(33) / www-data(33)
display_errors:
error_reporting: 22527
variables_order OK: GPCS.
PHP extensions OK. Dynamic loading is disabled.

ERROR: You have configured PHP not to allow short tags (`short_open_tag=off`). This shouldn't be a problem with SquirrelMail or any plugin coded according to the SquirrelMail Coding Guidelines, but if you experience problems with PHP code being displayed in some of the pages and changing setting to "on" solves the problem, please file a bug report against the failing plugin. The correct contact information is most likely to be found in the plugin documentation.

Checking paths...
Data dir OK.
Attachment dir OK.
Plugins OK.
Themes OK.
Default language OK.
Base URL detected as: `http://192.168.1.145/squirrelmail/src` (location base autodetected)

Checking outgoing mail service...
SMTP server OK (220 mail.rt2a.local ESMTP Postfix (Debian/GNU))

Checking IMAP service...
IMAP server ready (+ OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot ready.)
Capabilities: * CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN

Checking internationalization (i18n) settings...
gettext - Gettext functions are available. On some systems you must have appropriate system locales compiled.
mbstring - Mbstring functions are available.
recode - Recode functions are unavailable.
iconv - Iconv functions are available.
timezone - Webmail users can change their time zone settings.

Checking database functions...
not using database functionality.

Congratulations, your SquirrelMail setup looks fine to me!

[Login now](#)

192.168.1.145/squirrelmail/src/login.php



SquirrelMail version 1.4.23 [SVN]
Par l'Equipe du Projet SquirrelMail

Messagerie SquirrelMail

Identifiant :

Mot de passe :

On se connecte avec les identifiants de notre utilisateur

Messagerie SquirrelMail

Identifiant :

Mot de passe :

1. Personnaliser l'interface

Vous aurez peut-être envie d'étendre les fonctionnalités de votre interface graphique de messagerie. Pour cela, il faut installer un ou plusieurs plugins, et le choix est vaste... Il en existe plus de 170 différents ! Par défaut, 16 plugins sont déjà installés (mais non activés !) :

- ☐ Abook_take : pour récupérer facilement l'adresse de l'expéditeur d'un mail dans votre carnet d'adresse.

- ☐ Administrator : pour administrer à distance la configuration de SquirrelMail.

- ☐ Bug_report : pour reporter facilement un bug à l'équipe de développement.

- ☐ Calendar : un calendrier simple.

- ☐ Delete_move_next : pour effacer et déplacer facilement vos mails.

- ☐ Filters : pour filtrer vos mails (antispam)

- ☐ Fortune : pour insérer une devise dans vos mails.

La page des plugins en anglais est disponible à l'adresse suivante :
<http://www.squirrelmail.org/plugins.php>

Faites le nécessaire pour faire fonctionner le carnet d'adresses.

1. Administration de Squirrelmail

Gestion des utilisateurs

Seuls les utilisateurs ayant un compte sur votre serveur de mail auront la possibilité d'utiliser SquirrelMail. Pour créer un compte uniquement destiné à la messagerie, sans possibilité de connections sur votre serveur, il faut d'abord créer un groupe d'utilisateur dédié à l'utilisation de SquirrelMail :

```
root@mail:~# groupadd squirrelmail
```

Puis créer chaque utilisateur par l'instruction suivante :

```
$ useradd -c "nom_utilisateur" -s /bin/false -g squirrelmail nom_utilisateur
```

```
root@mail:~# useradd -c "arthur" -s /bin/false -g squirrelmail arthur_
```

Enfin définir le mot de passe pour chaque compte nouvellement créé :

```
$ passwd nom_utilisateur
```

```
root@mail:~# passwd arthur
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd : le mot de passe a été mis à jour avec succès
root@mail:~#
```

Maintenant il faut créer le répertoire personnel de l'utilisateur afin que les mails puissent être stockés dedans.

```
root@mail:/home# mkdir arthur
```

Puis on indique que ce dossier est le répertoire personnel de l'utilisateur.

```
root@mail:/home# chown arthur.squirrelmail /home/arthur
```

Pour tester le fonctionnement, essayer d'envoyer des mails à un autre compte et à vous-même. Utiliser d'abord une adresse mail du type utilisateur@rt2a.org.

To:

Cc:

Bcc:

Subject:

Priorité Accusé de réception : à la lecture à la r

On se connecte avec l'utilisateur arthur

SquirrelMail version 1.4.23 [SVN]
Par l'Equipe du Projet SquirrelMail

Messagerie SquirrelMail

Identifiant :

Mot de passe :

Mail bien reçu

<input type="checkbox"/>	antoineh@mail.rt2a.local	10:22	test
--------------------------	--	-------	----------------------

[Inverser la sélection](#)

1. Conclusion

Vous avez créé un serveur complet avec la suite LAMP, DNS et l'interface Webmail Squirrelmail. Autres interfaces

Webmail :

- RoundCube qui est développé en Ajax,

☐ Rainloop est développé en PHP et se veut complet et simple d'utilisation. Il gère très bien les protocoles

IMAP/SMTP et il dispose d'une interface moderne (HTML5/CSS3) très ergonomique,

1. Sécurisation du serveur de courriers

Amavisd-new est une interface sûre et haute performance entre un MTA et un ou plusieurs filtres de contenu: anti-virus, anti-spam, white/grey/black listings... Il est écrit en Perl et s'interface avec les MTAs à travers les protocoles (E)SMTP ou LMTP 1 .

Il est normalement positionné dans ou près d'un serveur de messagerie électronique, pas nécessairement où les boîtes emails des utilisateurs sont stockées.

SpamAssassin est un logiciel libre mené par l'Apache Software Foundation. SpamAssassin est un filtre anti-spam de type « analyseur de contenu » (ou « content-filter »). Il utilise une grande variété de mécanismes (analyse des headers et du corps d'un message, filtrage Bayésien, blacklist DNS, catalogues collaboratifs d'identification de spams...) pour classer un message en tant que spam (courrier non sollicité) ou ham (courrier légitime). Après chaque test effectué, une note est attribuée. Si la somme de ces notes dépasse le seuil configuré, SpamAssassin identifie le message comme un spam, sinon, comme un ham. SpamAssassin est écrit en Perl.

Quand le filtre anti-spam SpamAssassin (SA) est activé, amavisd-new appelle SA une seule fois par message reçu, quel que soit le nombre de destinataire. Enfin, il décode le message reçu et ses pièces jointes, puis les met à disposition des analyseurs de contenu. Ainsi, le décodage est fait une fois pour toute.

ClamAV (« Clam AntiVirus »), est un logiciel antivirus pour UNIX. Il est généralement utilisé avec les serveurs de courriels pour filtrer les courriers comportant des virus.

Installation

```
# apt-get install amavisd-new spamassassin clamav clamav-daemon zoo unzip bzip2 arj
```

```
nomarch lzop cabextract apt-listchanges libnet-ldap-perl libauthen-sasl-perl clamav-
```

```
docs daemon libio-string-perl libio-socket-ssl-perl libnet-ident-perl zip libnet-dns-
```

```
perl p7zip unrar-free
```

```
root@mail:~# apt-get install amavisd-new spamassassin clamav clamav-daemon zoo unzip bzip2 arj nomarch lzop cabextr  
act apt-listchanges libnet-ldap-perl libauthen-sasl-perl clamav-docs daemon libio-string-perl libio-socket-ssl-perl  
libnet-ident-perl zip libnet-dns-perl p7zip unrar-free
```

Paramétrage de Postfix

Lorsque Postfix reçoit un mail il va le passer à Amavis qui, à son tour, va envoyer le message à travers les filtres

antispam et antivirus. Il repassera ensuite le mail présumé propre à Postfix, pour sa destination finale.

🔗 Editer le fichier `/etc/postfix/master.cf`

Ajouter à la fin les lignes suivantes :

```
amavis unix - - - - 2 smtp
```

```
-o smtp_data_done_timeout=1200
```

```
-o smtp_send_xforward_command=yes
```

```
-o disable_dns_lookups=yes
```

```
-o max_use=20
```

```
127.0.0.1:10025 inet n - - - - smtpd
```

```
-o content_filter=
```

```
-o local_recipient_maps=
```

```
-o relay_recipient_maps=
```

```
-o smtpd_restriction_classes=
```

```
-o smtpd_delay_reject=no
```

```
-o smtpd_client_restrictions=permit_mynetworks,reject
```

```
-o smtpd_helo_restrictions=
```

```
-o smtpd_sender_restrictions=
```

```
-o smtpd_recipient_restrictions=permit_mynetworks,reject
```

```
-o smtpd_data_restrictions=reject_unauth_pipelining
```

```
-o smtpd_end_of_data_restrictions=
```

```
-o mynetworks=127.0.0.0/8
```

```
-o smtpd_error_sleep_time=0
```

```
-o smtpd_soft_error_limit=1001
```

```
-o smtpd_hard_error_limit=1000
```

```
-o smtpd_client_connection_count_limit=0
```

```
-o smtpd_client_connection_rate_limit=0
```

```
-o receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```

```
amavis unix - - - - 2 smtp
-o smtp_data_done_timeout=1200
-o smtp_send_xforward_command=yes
-o disable_dns_lookups=yes
-o max_use=20

127.0.0.1:10025 inet n - - - smtpd
-o content_filter=
-o local_recipient_maps=
-o relay_recipient_maps=
-o smtpd_restriction_classes=
-o smtpd_delay_reject=no
-o smtpd_client_restrictions=permit_mynetworks,reject
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o smtpd_data_restrictions=reject_unauth_pipelining
-o smtpd_end_of_data_restrictions=
-o mynetworks=127.0.0.0/8
-o smtpd_error_sleep_time=0
-o smtpd_soft_error_limit=1001
-o smtpd_hard_error_limit=1000
-o smtpd_client_connection_count_limit=0
-o smtpd_client_connection_rate_limit=0
-o receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```

Ajouter la ligne suivante à la fin du fichier /etc/postfix/main.cf

content_filter = amavis:[127.0.0.1]:10024

```
content_filter = amavis:[127.0.0.1]:10024
```

Activation des filtres Amavis

📄 Editer le fichier /etc/amavis/conf.d/15-content_filter_mode et décommenter les lignes @bypass

```
use strict;

# You can modify this file to re-enable SPAM checking through spamassassin
# and to re-enable antivirus checking.
#
# Default antivirus checking mode
# Please note, that anti-virus checking is DISABLED by
# default.
# If You wish to enable it, please uncomment the following lines:
@bypass_virus_checks_maps = (
    \%bypass_virus_checks, \%bypass_virus_checks_acl, \%bypass_virus_checks_re);
#
# Default SPAM checking mode
# Please note, that anti-spam checking is DISABLED by
# default.
# If You wish to enable it, please uncomment the following lines:
@bypass_spam_checks_maps = (
    \%bypass_spam_checks, \%bypass_spam_checks_acl, \%bypass_spam_checks_re);

1; # ensure a defined return
```

Configuration de la mise en quarantaine

📄 Editer le fichier /etc/amavis/conf.d/50-user et modifier les lignes pour la mise en quarantaine.

```
use strict;

#

# Place your configuration directives here. They will override those in
# earlier files.

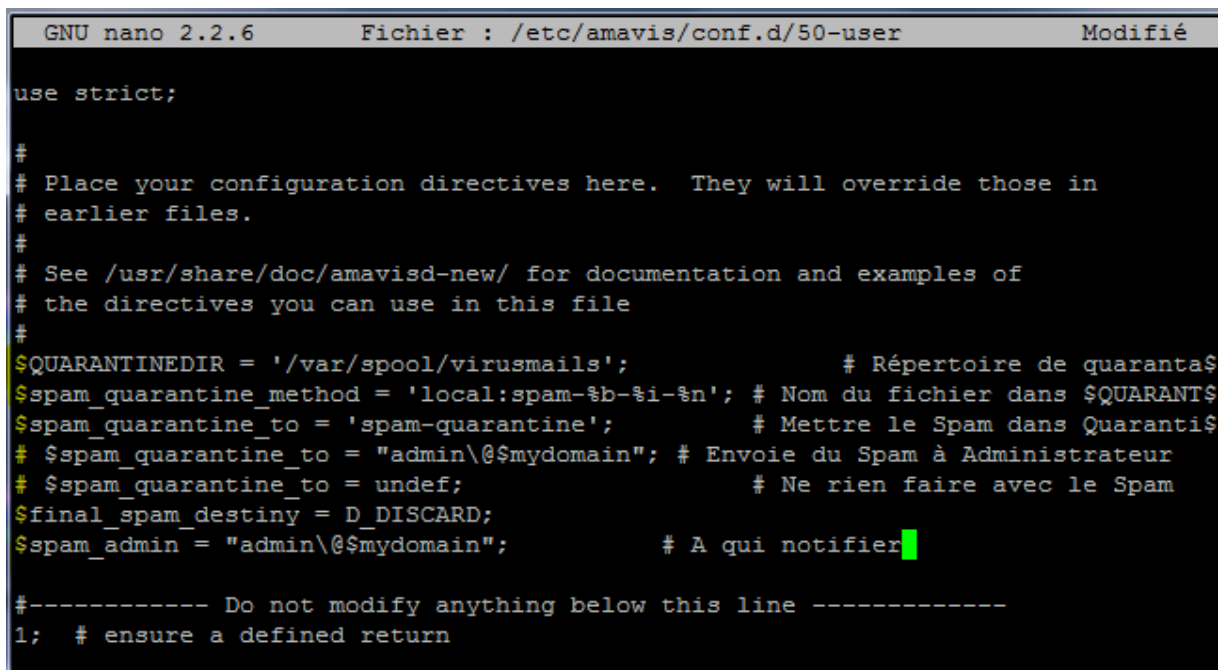
#

# See /usr/share/doc/amavisd-new/ for documentation and examples of
# the directives you can use in this file

#

$QUARANTINEDIR = '/var/spool/virusmails';      # Répertoire de quarantaine
$spam_quarantine_method = 'local:spam-%b-%i-%n'; # Nom du fichier dans $QUARANTINEDIR
$spam_quarantine_to = 'spam-quarantine';      # Mettre le Spam dans Quarantine Directory
# $spam_quarantine_to = "admin\@$mydomain"; # Envoie du Spam à Administrateur
# $spam_quarantine_to = undef;                # Ne rien faire avec le Spam
$final_spam_destiny = D_DISCARD;
$spam_admin = "admin\@$mydomain";            # A qui notifier

#----- Do not modify anything below this line -----
1; # ensure a defined return
```



```
GNU nano 2.2.6      Fichier : /etc/amavis/conf.d/50-user      Modifié
use strict;

#

# Place your configuration directives here. They will override those in
# earlier files.

#

# See /usr/share/doc/amavisd-new/ for documentation and examples of
# the directives you can use in this file

#

$QUARANTINEDIR = '/var/spool/virusmails';      # Répertoire de quaranta$
$spam_quarantine_method = 'local:spam-%b-%i-%n'; # Nom du fichier dans $QUARANT$
$spam_quarantine_to = 'spam-quarantine';      # Mettre le Spam dans Quaranti$
# $spam_quarantine_to = "admin\@$mydomain"; # Envoie du Spam à Administrateur
# $spam_quarantine_to = undef;                # Ne rien faire avec le Spam
$final_spam_destiny = D_DISCARD;
$spam_admin = "admin\@$mydomain";            # A qui notifier
#----- Do not modify anything below this line -----
1; # ensure a defined return
```


☐ Créer le répertoire /var/spool/virusmails et faites-le appartenir à l'utilisateur amavis du groupe du même nom.

```
root@mail:/var/spool# mkdir virusmails
```

```
root@mail:/var/spool# chown -R amavis:amavis /var/spool/virusmails/
```

(a verifier)

Mise à jour des règles SpamAssassin

```
root@mail:~# sa-update -D
```

Activation de SpamAssassin

☐ Editer le fichier /etc/default/spamassassin

Ce fichier d'activer SpamAssassin et de permettre la mise à jour par une tâche cron.

Change to one to enable spamd

ENABLED=1

Options

See man spamd for possible options. The -d option is automatically added.

SpamAssassin uses a preforking model, so be careful! You need to

make sure --max-children is not set to anything higher than 5,

unless you know what you're doing.

OPTIONS="--create-prefs --max-children 5 --helper-home-dir"

Pid file

Where should spamd write its PID to file? If you use the -u or

--username option above, this needs to be writable by that user.

Otherwise, the init script will not be able to shut spamd down.

PIDFILE="/var/run/spamd.pid"

Set nice level of spamd

#NICE="--nicelevel 15"

Cronjob

Set to anything but 0 to enable the cron job to automatically update

spamassassin's rules on a nightly basis

CRON=1

```
ENABLED=1
```

```
CRON=1
```

☐ Ajouter l'utilisateur clamav au groupe amavis

```
root@mail:~# adduser clamav amavis
Ajout de l'utilisateur « clamav » au groupe « amavis »...
Ajout de l'utilisateur clamav au groupe amavis
Fait.
```

Mise en service

☐ Démarrer les services spamassassin, amavis, clamav-daemon.

```
root@mail:~# service spamassassin start
root@mail:~# service amavis start
```

```
root@mail:~# service clamav-daemon start
```

☐ Redémarrer Postfix.

```
root@mail:~# systemctl restart postfix.service
```

Test de SpamAssasin

Vous trouverez dans la doc un exemple de spam: /usr/share/doc/spamassassin/examples/sample-spam.txt.

☐ Copier et coller cette ligne dans un mail et envoyer-le.

X5O!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

To:

Cc:

Bcc:

Subject:

Priorité Accusé de réception : à la lecture à la réception

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

On suffit ensuite d'aller consulter sa boîte mail pour voir que le virus a été détecté :

<input type="checkbox"/> Content-filter at mail.rt2a.local	16:09	+ VIRUS (Eicar-Test-Signature) in mail FROM LOCAL [L...
<input type="checkbox"/> Content filter at	16:07	+ VIRUS (Eicar Test Signature) in mail FROM LOCAL [L...

```
Objet: VIRUS (Eicar-Test-Signature) in mail FROM LOCAL [127.0.0.1]:34770
<antoineh@mail.rt2a.local>
De: "Content-filter at mail.rt2a.local" <postmaster@mail.rt2a.local>
Date: Ven 25 novembre 2016 16:09
À: postmaster@mail.rt2a.local
Priorité: Normale
Options: Afficher l'en-tête complet | Voir la version imprimante | Télécharger en tant que fichier
```

```
A virus was found: Eicar-Test-Signature

Scanner detecting a virus: ClamAV-clamd

Content type: Virus
Internal reference code for the message is 00678-02/aAMv9pq3qh8L

First upstream SMTP client IP address: [127.0.0.1] localhost

Return-Path: <antoineh@mail.rt2a.local>
From: antoineh@mail.rt2a.local
Message-ID: <cb884b6b6d3d91e6c0ad35a62799d.squirrel@192.168.1.145>
Subject: XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
The message has been quarantined as: a/virus-aAMv9pq3qh8L

The message WAS NOT relayed to:
<arthur@mail.rt2a.local>:
  250 2.7.0 Ok, discarded, id=00678-02 - INFECTED: Eicar-Test-Signature

Virus scanner output:
p001: Eicar-Test-Signature FOUND
```

On peut aussi le vérifier dans les fichiers de log

```
root@mail:/var/log# cat mail.info_
Nov 25 16:07:47 mail postfix/qmgr[648]: E3232D89: from=<postmaster@mail.rt2a.local>, size=2580, nrcpt=1 (queue active)
Nov 25 16:07:47 mail amavis[677]: (00677-02) Blocked INFECTED (Eicar-Test-Signature) {DiscardedInternal,Quarantined}, LOCAL [127.0.0.1]:34764 <antoineh@mail.rt2a.local> -> <arthur@mail.rt2a.local>, quarantine: H/virus-HzdpJa0FEYpg, Queue-ID: C0499CF0, Message-ID: <0e5fcff0f056080a16d5a1af76fcb463.squirrel@192.168.1.145>, mail_id: HzdpJa0FEYpg, Hits: -, size: 839, 102 ms
Nov 25 16:07:47 mail postfix/local[641]: E3232D89: to=<antoineh@mail.rt2a.local>
```

15. Pour aller plus loin...

Comment lutter efficacement contre les serveurs émettant des spams ?

16. Quelques commandes utiles pour Postfix

Pour voir l'état des mails mailq

Supprimer tous les mails en queue postsuper -d ALL

Supprimer un mail spécifique postsuper -d DA80E24A0A

Voir le contenu d'un mail dans la queue postcat -q F1F942D236

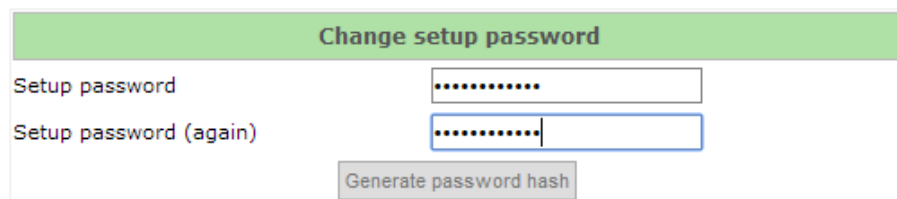
Installation de postfixadmin

```
root@mail:~# apt install php5 mysql-server_  
root@mail:~# apt install postfixadmin_
```

Configuration de postfixadmin :

Il faut aller sur <http://votredomaine/postfixadmin/setup.php>

Le chargement est un peu long car il doit générer la base de données.



**Since version 2.3 there is no requirement to delete setup.php!
Check the config.inc.php file for any other settings that you might need to change!**

Le password utiliser « Password1234 »

Il nous genere un mot de passe

If you want to use the password you entered as setup password, edit config.inc.php and set
`$CONF['setup_password'] = '0fe2ae633acda7ad1d1ae6290e16e521:611f67a9401ce6a78bb1d00dcdd8949f8aed8a6c';`

Après avoir généré le mot de passe de l'admin, on va le copier dans le fichier de
/etc/postfixadmin/config.inc.php

```
GNU nano 2.2.6  Fichier : /etc/postfixadmin/config.inc.php  Modifié  
$CONF['configured'] = true;  
  
// In order to setup Postfixadmin, you MUST specify a hashed password here.  
// To create the hash, visit setup.php in a browser and type a password into th$  
// on submission it will be echoed out to you as a hashed value.  
#$CONF['setup_password'] = 'changeme';  
$CONF['setup_password'] = '0fe2ae633acda7ad1d1ae6290e16e521:611f67a9401ce6a78bb1d00dcdd8949f8aed8a6c';
```

On redémarre les services postfix et apache.

```
root@mail:~# service postfix restart  
root@mail:~# service apache2 restart
```

On remplit les champs pour la création du compte admin

If you want to use the password you entered as setup password, edit config.inc.php and set

```
$CONF['setup_password'] = '0fe2ae633acda7ad1d1ae6290e16e521:611f67a9401ce6a78bb1d00dcd8949f8aed8a6c';
```

Create superadmin account

Setup password: [.....] [Lost password?](#)

Admin: [admin@mail.rt2a.local] [Email address](#)

Password: [.....]

Password (again): [.....]

**Since version 2.3 there is no requirement to delete setup.php!
Check the config.inc.php file for any other settings that you might need to change!**

Mot de passe de l'admin « Password123456 »

Admin has been added!
(admin@mail.rt2a.local)

Create superadmin account

Ensuite on se connecte avec les identifiants à la page : <http://notredomaine/postfixadmin/login.php>

Mail admins login here to administer your domain.

Login (email): [admin@mail.rt2a.local]

Password: [.....]

[Français - French]

Users click here to login to the user section.

On ajoute ensuite notre domaine

Ajouter un nouveau domaine

Domaine: [mail.rt2a.local]

Description: [.....]

Alias: [10] -1 = désactivé | 0 = illimité

Comptes courriels: [10] -1 = désactivé | 0 = illimité

Ajouter les alias par défaut:

Le serveur est un "backup MX":

Le domaine a été ajouté!
(mail.rt2a.local)

Pour les tests, nous laisserons les paramètres de bases.

Ensuite on va dans liste de domaine, dans notre domaine et on fait « ajouter un compte courriel »

Liste Virtuels

Ajouter un nouveau compte courriel à votre domaine.

Nom d'utilisateur: @ ▼

Mot de passe: Mot de passe pour compte POP3/IMAP

Mot de passe (confirmation):

Nom: Nom complet

Actif:

Envoyer le message de bienvenue:

Liste Virtuels

Ajouter un nouveau compte courriel à votre domaine.

Nom d'utilisateur: @ ▼

Mot de passe: Mot de passe pour compte POP3/IMAP

Mot de passe (confirmation):

Nom: Nom complet

Actif:

Envoyer le message de bienvenue: