How-to Integrando o Postfix com Active Directory do Windows

Autoria de Wanderson
20/07/2009
Última Atualização 18/12/2009

Tentarei abordar de forma clara e objetiva como configurar um servidor de e-mail com Postfix integrado com uma base Active Directory do Windows. Iremos utilizar as ferramentas mais comuns em servidores de e-mail: O Antivírus Clamav, Amavisd-new, Anti-Spam SpamAssassin, dovecot/SSL/TLS, dovecot-sieve e Squirrelmail como Webmail.

Iniciando

Assume-se que o servidor FreeBSD esteja instalado e com o Ports atualizado, e o Active Directory funcionado corretamente.

Configuração dos servidores

FreeBSD

Versão: FreeBSD 7.2 RELEASE
Domínio: neonoc.tld
Nome: mx
IP: 192.168.1.200/255.255.255.0

Windows

Versão: Windows 2003 R2 Standard Edition
Domínio: neonoc.tld
Nome: diadora
IP: 192.168.1.100/255.255.255.0

Estrutura do Active Directory

Em nosso exemplo nem todos os usuários da organização terão contas de e-mail, então crie um Grupo Global de Segurança chamado, por exemplo, GGEMAIL e adicione os usuários que receberão uma conta de e-mail como membros do grupo. É necessário criar um usuário não-privilegiado que será usado nas configurações do servidor de e-mail, estou chamando esse usuário de bindmail e a senha será bindmail.

Exemplo:

Usuários criados no Active Directory que terão contas de e-mails.

Wanderson [OU]: Matriz/RH/USUARIOS
Julia [OU]: Matriz/MARKETING/USUARIOS
Josefina [OU]: Matriz/FILIAIS/IPATINGA/USUARIOS

Estrutura do Active Directory

É aconselhável atualizar sua coleção de ports via portsnap. A primeira vez é um pouco demorado, são aproximadamente 50MB de download, nas próximas basta uma portsnap fetch update.

```
#portsnap fetch
#portsnap extract
#portsnap update
```

Antes de prosseguir é necessário criar um usuário que será responsável pela movimentação das caixas de correios.

Também vamos criar o diretório /var/virtual onde ficarão as mensagens dos usuários.

#pw group add vmail –g 1000
#pw user add vmail –u 1000 –g 1000 –d /dev/null –s /sbin/nologin

#mkdir /var/virtual
#chow –R vmail:vmail /var/virtual
#chmod –R 700 /var/virtual

A estrutura de diretório dos usuários ficará da seguinte forma:

/var/virtual/wanderon/Maildir
/var/virtual/julia/Maildir
/var/virtual/josefina/Maildir
...

Dovecot

Instalando o Dovecot

Dovecot será o nosso servidor de IMAP e POP3. Ele oferece um excelente suporte a Quotas, Ldap, dentre outros, também é bastante intuitivo e bem documentado. Seu objetivo é ser um servidor leve e rápido.

Versão utilizada: dovecot-1.1.16

#cd /usr/ports/mail/dovecot
#make config
#make install clean

Selecione as seguintes opções: KQUEUE – SSL – IPV6 – POP3 – LDA - LDAP

Dovecot Sieve

Ele será responsável por filtrar mensagens marcadas com Spam e encaminhar para o diretório apropriado de cada usuário. Ele é um plugin para o Dovecot delivery LDA.

Versão utilizada: dovecot-sieve-1.1.6

#cd /usr/ports/mail/dovecot-sieve
#make install clean

Configurando o Dovecot na inicialização do sistema:

#echo ‘dovecot_enable=”YES”’ >> /etc/rc.conf

Criando certificado SSL/TLS para conexões seguras:
Obs: Estes passos são necessários se pretende usar o SSL, caso contrário pule essa etapa.

#mkdir /etc/ssl/dovecot
#cd /etc/ssl/dovecot
#openssl req -new -x509 -nodes -out cert.pem -keyout key.pem -days 365

Configuração do dovecot.conf

Obs: O arquivo completo de configuração que foi utilizado ficou configurado da seguinte forma:

```
#ee /usr/local/etc/dovecot.conf

#####################
#
protocols = imap imaps pop3 pop3s
disable_plaintext_auth = no
log_path = /var/log/dovecot.log
info_log_path = /var/log/dovecot.log
ssl_disable = no
ssl_cert_file = /etc/ssl/dovecot/cert.pem
ssl_key_file = /etc/ssl/dovecot/key.pem
login_greeting = NEONOC Mailserver Ready.
mail_location = maildir:/var/virtual/%n/Maildir
mail_uid = vmail
mail_gid = vmail
mail_privileged_group = mail
first_valid_uid = 1000
last_valid_uid = 1000
first_valid_gid = 1000
last_valid_gid = 1000
valid_chroot_dirs = /var/virtual
maildir_copy_with_hardlinks = yes
protocol imap {
  mail_plugins = quota imap_quota
  mail_plugin_dir = /usr/local/lib/dovecot/imap
  login_greeting_capability = yes
  imap_client_workarounds = delay-newmail netscape-eoh tb-extra-mailbox-sep
}
protocol pop3 {
  pop3_uidl_format = %08Xu%08Xv
  mail_plugins = quota
  mail_plugin_dir = /usr/local/lib/dovecot/pop3
  pop3_client_workarounds = outlook-no-nuls oe-ns-eoh
}
protocol lda {
  debug = yes
  mail_plugins = cmusieve quota
  mail_plugin_dir = /usr/local/lib/dovecot/lda
  postmaster_address = postmaster@neonoc.tld
  sendmail_path = /usr/sbin/sendmail
  auth_socket_path = /var/run/dovecot/auth-master
  log_path = /var/log/dovecot-lda.log
  info_log_path = /var/log/dovecot-lda.log
  global_script_path = /usr/local/etc/dovecot/dovecot.sieve
  sieve_global_path = /usr/local/etc/dovecot/dovecot.sieve
}
auth_username_format = %Lu
auth default {
  mechanisms = plain login
  passdb ldap {
       args = /usr/local/etc/dovecot-ldap.conf
  }
  userdb ldap {
       args = /usr/local/etc/dovecot-ldap.conf
  }
  user = root
  socket listen {
    master {
      path = /var/run/dovecot/auth-master
      mode = 0600
      user = vmail
      group = vmail
    }
    client {
```

```
    path = /var/run/dovecot/auth-client
    mode = 0660
    user = postfix
    group = postfix
   }
  }
}
dict {
}
plugin {
  quota_rule = *:storage=20480
  quota = maildir
  quota_warning = storage=85%% /usr/local/bin/quota-warning.sh 85%
  sieve  = /usr/local/etc/dovecot/dovecot.sieve
}#
#####################
```

Script Sieve

O Sieve é uma plugin que trabalha em conjunto com Dovecot Delivery LDA. Ele ficará responsável por interceptar mensagens marcadas como Spam pelo SpamAssassin e direciona-la para a pasta Spam dos usuários. O script usado nessa configuração é global e será valido para todos os usuários.

Crie o diretório /usr/local/etc/dovecot e dentro dele o seguinte script:

```
#mkdir /usr/local/etc/dovecot
#ee dovecot.sieve
#chown &ndash;R vmail /usr/local/etc/dovecot

#####################
#
require ["fileinto"];
if header :contains "X-Spam-Level" "**********" {
        discard;
        stop;
}
elsif
header :contains "X-Spam-Status" "Yes" {
        fileinto "INBOX.Spam";
        stop;
}
#
#####################
```

Agora vamos criar os arquivos de logs.

```
#touch /var/log/dovecot-lda.log
#touch /var/log/dovecot.log
#chown vmail /var/log/dovecot*
```

Obs: Mensagens que estiver marcadas como Spam será movida para o diretório “INBOX.Spam” do usuário, o mesmo será criado caso não exista.

Plugin Quota

Todos os usuários terão 20MB(*:storage=20480) de espaço para seus e-mails e uma mensagem de advertência será enviada quando sua Quota atingir 85% de uso. Fique a vontade para definir suas próprias configurações.

Agora vamos criar o script para enviar mensagem de advertência para os usuários.

```
#ee /usr/local/bin/quota-warning.sh
#chown vmail /usr/local/bin/quota-warning.sh
```

```
####################
#!/bin/sh

PERCENT=$1
FROM="postmaster@neonoc.tld"
qwf="/tmp/quota.warning.$$"

echo "From: $FROM
To: $USER
To: postmaster@neonoc.tld
Subject: Sua caixa de e-mail esta com $PERCENT% em uso.
Content-Type: text/plain; charset="UTF-8"

Atenção: Sua caixa de e-mail está com $PERCENT% em uso." >> $qwf

cat $qwf | /usr/sbin/sendmail -f $FROM "$USER"
rm -f $qwf
exit 0
####################
```

Configurando o dovecot-ldap.conf

```
#cd /usr/local/etc
#ee dovecot-ldap.conf

####################
debug_level = 0
hosts = 192.168.1.100
base = dc=neonoc,dc=tld
ldap_version = 3
dn = cn=bindmail,ou=matriz,dc=neonoc,dc=tld
dnpass = bindmail
auth_bind = yes
user_filter =
(&(ObjectClass=person)(sAMAccountName=%u)(memberOf=CN=GGEMAIL,OU=matriz,DC=neonoc,DC=tld))
pass_filter = (&(ObjectClass=person)(sAMAccountName=%u)
(memberOf=CN=GGEMAIL,OU=matriz,DC=neonoc,DC=tld))
####################
```

Iniciando o Dovecot

```
#/usr/local/etc/rc.d/dovecot start
```

Para verificar se o serviço está ativo use o comando ‘sockstat -4l’ e verifique se as portas 110, 143, 993 e 995 estão ativas. Se não estiver consulte os arquivos de logs, verifique os arquivos de configurações e as permissões dos arquivos e diretórios.

Testando autenticação

```
#telnet mx.neonoc.tld 110


#telnet mx.neonoc.tld 143
```

Se tudo ocorreu bem até aqui, verifique se foi criado o caixa de e-mail do usuário em: /var/virtual/

PostfixInstalando o Postfix

O Postfix será o nosso Mail Transfer Agent (MTA) escolhido, que forma o núcleo de qualquer servidor de e-mail.

Dentre outras coisas, o MTA é responsável por mover mensagens entre os vários servidores de e-mail na Internet.

Versão utilizada: postfix-2.4.11

#cd /usr/ports/mail/postfix24
#make config
#make install clean

Selecione as seguintes opções: PCRE – SASL2 – DOVECOT – TLS – OPENLDAP – VDA – TEST

Durante a instalação o sistema lhe fará duas perguntas, reposta ‘y’ em todas.

Configurando o Postfix

Desabilitando o Sendmail

#echo ‘sendmail_enable="NO"’ >> /etc/rc.conf
#echo ‘sendmail_submit_enable="NO"’ >> /etc/rc.conf
#echo ‘sendmail_outbound_enable="NO"’ >> /etc/rc.conf
#echo ‘sendmail_msp_queue_enable="NO"’ >> /etc/rc.conf

Parando o Sendmail

#/etc/rc.d/sendmail forcestop

Iniciando o Postfix no boot do sistema:

#echo ‘postfix_enable=”YES”’ >> /etc/rc.conf

Crie o arquivo ‘/etc/periodic.conf ‘e adicione as seguintes linhas:

#ee /etc/periodic.conf

daily_clean_hoststat_enable="NO"
daily_status_mail_rejects_enable="NO"
daily_status_include_submit_mailq="NO"
daily_submit_queuerun="NO"

Criando certificados SSL/TLS

#mkdir /etc/ssl/postfix
#cd /etc/ssl/postfix
#openssl req -new -x509 -nodes -out smtpd.pem -keyout smtpd.pem -days 3650
#chmod 640 /etc/ssl/postfix/smtpd.pem
#chgrp -R postfix /etc/ssl/postfix

Arquivo Main.cf

Obs: O arquivo completo de configuração que foi utilizado ficou configurado da seguinte forma:

#cd /usr/local/etc/postfix
#ee main.cf

#####################
Configuração Geral
queue_directory = /var/spool/postfix
command_directory = /usr/local/sbin
daemon_directory = /usr/local/libexec/postfix
mail_owner = postfix

```
myhostname = mx.neonoc.tld
mydomain = neonoc.tld
myorigin = $mydomain
mydestination = $myhostname, localhost.$mydomain, localhost
unknown_local_recipient_reject_code = 550
mynetworks_style = host
smtpd_banner = $myhostname ESMTP $mail_name ($mail_version)
debug_peer_level = 2
debugger_command =
    PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
    xxgdb $daemon_directory/$process_name $process_id & sleep 5
sendmail_path = /usr/local/sbin/sendmail
newaliases_path = /usr/local/bin/newaliases
mailq_path = /usr/local/bin/mailq
setgid_group = maildrop
html_directory = no
manpage_directory = /usr/local/man
sample_directory = /usr/local/etc/postfix
readme_directory = no

## Configuração SASL
broken_sasl_auth_clients = yes
smtpd_sender_restrictions = permit_sasl_authenticated, permit_mynetworks
smtpd_recipient_restrictions =
  permit_mynetworks,
  permit_sasl_authenticated,
  reject_non_fqdn_hostname,
  reject_non_fqdn_sender,
  reject_non_fqdn_recipient,
  reject_unauth_destination,
  reject_unauth_pipelining,
  reject_invalid_hostname,
  reject_rbl_client list.dsbl.org,
  reject_rbl_client bl.spamcop.net,
  reject_rbl_client sbl-xbl.spamhaus.org
smtpd_sasl_auth_enable = yes
smtpd_sasl_authenticated_header = yes
smtpd_sasl_local_domain = $myhostname
smtpd_sasl_security_options = noanonymous
smtpd_sasl_type = dovecot
smtpd_sasl_path = /var/run/dovecot/auth-client

## Configuração TLS/SSL
smtp_use_tls = yes
smtpd_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtpd_tls_key_file = /etc/ssl/postfix/smtpd.pem
smtpd_tls_cert_file = /etc/ssl/postfix/smtpd.pem
smtpd_tls_CAfile = /etc/ssl/postfix/smtpd.pem
smtpd_tls_loglevel = 0
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom

## Configuração LDAP/AD
home_mailbox = Maildir/
virtual_mailbox_base = /var/virtual
virtual_uid_maps = static:1000
virtual_gid_maps = static:1000
smtpd_recipient_restrictions = permit_mynetworks, reject_unauth_destination
alias_maps = hash:/etc/aliases
command_directory = /usr/local/sbin
daemon_directory = /usr/local/libexec/postfix
virtual_mailbox_domains =
  NEONOC.TLD
```

```
virtual_mailbox_maps = ldap:ldapvirtual
ldapvirtual_server_host =
  ldap://192.168.1.100
ldapvirtual_search_base = dc=neonoc,dc=tld
ldapvirtual_bind = yes
ldapvirtual_bind_dn = NEONOC\bindmail
ldapvirtual_bind_pw = bindmail
ldapvirtual_query_filter = (sAMAccountName=%u)
ldapvirtual_result_attribute = sAMAccountName
ldapvirtual_version = 3
ldapvirtual_chase_referrals = yes
ldapvirtual_result_format=%s/Maildir/

## Dovecot LDA Agent Delivery
virtual_transport= dovecot
dovecot_destination_recipient_limit=1
#####################
```

Arquivo Master.cf

Descomente a linha “smtps” deixando da seguinte forma:

```
smtps     inet  n       -       n       -       -       smtpd
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
```

Agora insira a seguinte linha no final do arquivo:

```
dovecot   unix  -       n       n       -       -       pipe
   flags=DRhu user=vmail:vmail argv=/usr/local/libexec/dovecot/deliver -d ${user}
```

Iniciando o Postfix

```
#mv /etc/aliases /etc/aliases.OFF
#ln &amp;ndash;s /usr/local/etc/postfix/aliases /etc/aliases
#postaliases /usr/local/etc/postfix/aliases
#/usr/local/etc/rc.d/postfix start
```

Para verificar se o serviço está ativo use o comando ‘sockstat -4l’ e verifique se as portas 25 e 465 estão ativas. Se não estiver consulte o arquivo de log “/var/log/maillog” e verifique os arquivos de configurações.

Testando o envio de mensagem

```
#telnet mx.neonoc.tld 25
```

Para gerar essa senha você pode usar o seguinte commando:

```
#printf '\0Usuario\0Senha' | mmencode
```

O programa mmencode pode ser encontrado em: “/usr/ports/converters/mmencode”.

Terminado os teste, verifique se o usuário recebeu a mensagem corretamente. A mensagem deverá ser entregue na pasta: "/var/virtual/wanderson/Maildir/new" .

ApacheInstalando o Apache

A instalação do servidor Web Apache é necessária para que posteriormente possamos instalar e utilizar o Webmail.

Versão utilizada: httpd-2.2.11

#cd /usr/ports/www/apache22
#make install

As configurações padrões são suficientes para nosso ambiente.

Configurando o Apache para iniciar durante o boot:

#echo ‘apache22_enable=”YES”’ >> /etc/rc.conf

PHP5Instalando o PHP5

A linguagem PHP é necessária já que nosso Webmail é totalmente escrito em PHP.

Versão utilizada: php-5.2.10

#cd /usr/ports/lang/php5
#make config
#make install clean

Selecione a opção: APACHE

Configurando o Apache/PHP

Abra o arquivo ‘/usr/local/etc/apache22/httpd.conf’ e insira as seguintes linhas no final do arquivo:

#ee /usr/local/etc/apache22/httpd.conf

AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps

Localize a linha ‘DirectoryIndex’ e configure da seguinte forma:

#ee /usr/local/etc/apache22/httpd.conf

DirectoryIndex index.php index.html

Verifique se a linha ‘LoadModule php5_module libexec/apache22/libphp5.so’ foi adicionada no arquivo ‘/usr/local/etc/apache22/httpd.conf’.

Instalando PHP5-Extensions

#cd /usr/ports/lang/php5-extensions
#make config
#make install clean

Selecione as seguintes opções: BCMATH – GD – GETTEXT – MBSTRING – CRYPT – PCRE – SESSION - SOCKETS

WebmailInstalando o Webmail

A finalidade do webmail é facilitar a leitura de mensagens partindo de qualquer lugar na internet sem a necessidade de configuração de um cliente de e-mail.

Versão utilizada: squirrelmail-1.4.19

```
#cd /usr/ports/mail/squirrelmail
#make install clean
```

Configurando o Squirrelmail

Crie o arquivo ‘/usr/local/etc/apache22/Includes/squirrelmail.conf’ com o seguinte conteúdo:

```
#ee /usr/local/etc/apache22/Includes/squirrelmail.conf

Alias /squirrelmail/ "/usr/local/www/squirrelmail/"
<Directory "/usr/local/www/squirrelmail">
  AllowOverride None
  Options None
  Order allow,deny
  Allow from all
</Directory>
```

Feito isso dirija-se até o diretório ‘/usr/local/www/squirrelmail’ e execute o script ‘configure’.

```
#cd /usr/local/www/squirrelmail
#./configure
```

1. Escolha a opção “2. Server Settings”.
2. Escolha a opção “1. Domain” e configure com o nome do seu Domínio.
3. Escolha a opção “A. Update IMAP Settings” e a opção “5. IMAP Port” e altere para “993”.
4. Escolha a opção “7. Secure IMAP (TLS)” e altere para “true” pressionando “y”.
5. Escolha a opção “8. Server software” e altere para “dovecot” em seguida pressione “Enter”.
6. Escolha a opção “R Return to Main Menu”.
7. Escolha a opção “10. Languages” e a opção “1. Default Language” e altera para “pt_BR” e pressione “Enter”.
8. Pressione “s” seguido de “Enter” para salvar as configurações em seguida “q” para sair.

Instalando o Plugin para Quota

```
#cd /usr/ports/mail/squirrelmail-check_quota-plugin
#make install
```

Configurando o Plugin

```
#cd /usr/local/www/squirrelmail/plugins/check_quota
#cp config.sample.php config.php
```

Abra o arquivo ‘config.php’ e configure de acordo com o exemplo abaixo:

```
$settings['quota_type'] = 1;
$settings['graph_type'] = 1;
$settings['info_above_folders_list'] = 0;
$settings['show_intro_texts'] = 1;
$settings['details_above_graph'] = 0;
```

Instalando o Plugin autosubscribe

Esse plugin será responsável por criar os diretórios de Spam para todos os usuários. Ele também atualiza o arquivo ‘subscriptions’ dentro dos Maildir dos usuários, tarefa que o ‘/usr/local/etc/dovecot/dovecot.sieve’ não faz.

```
#cd /usr/local/www/squirrelmail/plugins/
```

#fetch http://web.inseto.net/files/postfix/autosubscribe-1.1-1.4.2.tar.gz
#tar xvzf http://web.inseto.net/files/postfix/autosubscribe-1.1-1.4.2.tar.gz
#cd autosubscribe
#cp config_sample.php config.php

Abra o arquivo ‘config.php’ e configure de acordo com o exemplo abaixo:

$autosubscribe_folders='INBOX.Spam';
$autosubscribe_special_folders='INBOX.Spam';

Obs: O nome ‘INBOX.Spam’ deve ser o mesmo nome definido no arquivo ‘/usr/local/etc/dovecot/dovecot.sieve’.

Instalando o Plugin Timeout

#cd /usr/ports/mail/squirrelmail-timeout_user-plugin
#make all install clean

Feito isso dirija-se até o diretório ‘/usr/local/www/squirrelmail’ e execute o script ‘configure’.

#cd /usr/local/www/squirrelmail
#./configure

1. Escolha a opção “8. Plugins” .
2. Para instalar o Plugin basta pressionar seu número. O mesmo procedimento serve para desinstalar.
3. Instale os Plugins: “check_quota”, “autosubscribe”, “timeout_user” e “calendar”.
4. Pressione “s” seguido de “Enter” para salvar as configurações em seguida “q” para sair.

Para finalizar, vamos testar as nossas configurações:

Inicie o servidor Apache

#apachectl start

Verifique se todos os requisitos estão devidamente instalados e configurados, para isso acesso o seguinte endereço:

http://www.neonoc.tld/squirrelmail/src/configtest.php

Se uma mensagem como essa for exibida será preciso configurar o php.ini:

ERROR: You have enabled any one of magic_quotes_runtime, magic_quotes_gpc or magic_quotes_sybase in your PHP configuration. We recommend all those settings to be off. SquirrelMail may work with them on, but when experiencing stray backslashes in your mail or other strange behaviour, it may be advisable to turn them off.

#cd /usr/local/etc/
#cp php.ini-recommended php.ini

Edite o arquivo “php.ini” e altere a linha “short_open_tag = Off” para “short_open_tag = On”

#apachectl graceful

Acesse o endereço novamente para testar a configuração:

http://www.neonoc.tld/squirrelmail/src/configtest.php

Se tudo estiver certo, você já pode acessar seu Webmail. Basta acesso com o nome de usuário sem utilizar “@dominio”.

http://www.neonoc.tld/squirrelmail/

Verifique se a pasta Spam foi criada corretamente. Se ela não estiver disponível pressione “F5” para que seja exibida. Também verifique se a barra de estatus da quota está sendo exibida corretamente.

AntiSpamInstalando o SpamAssassin

O SpamAssassin é uma ferramenta anti-spam de código aberto e bastante popular. Considerados por muitos como uma das melhores ferramentas para combate a Spam e melhor que muitos produtos comerciais.

Versão utilizada: Mail-SpamAssassin-3.2.5

```
#cd /usr/ports/mail/p5-Mail-SpamAssassin
#make config
#make install clean
```

Selecione as opções: AS_ROOT – DKIM – SSL – GNUPG – RAZOR

Iniciando o SpamAssassin no boot do sistema

```
#echo &amp;lsquo;spamd_enable="YES"&amp;rsquo; >> /etc/rc.conf
#echo &amp;lsquo;spamd_flags="-u spamd -H /var/spool/spamd"&amp;rsquo; >> /etc/rc.conf
```

Configurando SpamAssassin

```
#cd /usr/local/etc/mail/spamassassin
#cp local.cf.sample local.cf
```

Configura o aruivo “local.cf” como o exemplo a seguir:

```
#ee local.cf

rewrite_header Subject *****SPAM*****
use_bayes 1
```

Iniciando o SpamAssassin

```
#/usr/local/etc/rc.d/sa-spamd start
```

Configurando o Master.cf

Edite o arquivo “/usr/local/etc/postfix/master.cf” deixando da seguinte forma:

```
dovecot unix - n n - - pipe
  flags=DRhu user=vmail:vmail argv=/usr/local/bin/spamc -u ${user} &amp;ndash;e  /usr/local/libexec/dovecot/deliver -d ${user}


#postfix reload
```

Testando o SpamAssassin

Crie um e-mail e no corpo da mensagem insira a seguinte string:

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

Se a instalação do SpamAssassin estiver correta, o e-mail será classificado como SPAM. Verifique o arquivo de log “/var/log/dovecot-lda.log” durante o envio da mensagem. Por padrão essa mensagem será descarta por seu “score” ser muito alto. Para verificar ser a mensagem marcada como Spam está sendo filtrada e encaminhada para a pasta Spam do usuário, altere a configuração do arquivo “/usr/local/etc/dovecot/dovecot.sieve” para:

```
#ee /usr/local/etc/dovecot/dovecot.sieve

require ["fileinto"];
if header :contains "X-Spam-Status" "Yes" {
	fileinto "INBOX.Spam";
	stop;
}
```

Se tudo estiver correto a mensagem será marcada como Spam e direcionada para a pasta Spam do usuário. O arquivo de log “dovecot-lda.log” irá trazer essa informação: “saved mail to INBOX.Spam”.

AntivírusInstalando o Clamav e Amavis-new

O Clamav e Amavisd-new será responsável pela filtragem de vírus das mensagem de e-mail.

Versão utilizada: clamav-0.95.2

```
#cd /usr/ports/security/clamav
#make config
#make install clean
```

Selecione a opção: MILTER

Instalando o Amavisd-new

Versão utilizada: amavisd-new-2.6.4

```
#cd /usr/ports/security/amavis-new
#make install clean
```

As opções padrões são suficientes.

Configuração do Clamav

```
#ee /usr/local/etc/clamd.conf

LogFile /var/log/clamav/clamd.log
LogFileMaxSize 2M
LogTime yes
PidFile /var/run/clamav/clamd.pid
DatabaseDirectory /var/db/clamav
LocalSocket /var/run/clamav/clamd.sock
FixStaleSocket yes
User clamav
AllowSupplementaryGroups yes
ScanMail yes
```

Configuração do freshclam

#ee /usr/local/etc/freshclam.conf

```
DatabaseDirectory /var/db/clamav
UpdateLogFile /var/log/clamav/freshclam.log
LogFileMaxSize 2M
LogTime yes
PidFile /var/run/clamav/freshclam.pid
DatabaseOwner clamav
AllowSupplementaryGroups yes
DatabaseMirror database.clamav.net
NotifyClamd /usr/local/etc/clamd.conf
```

Configuração do amavisd-new

#ee /usr/local/etc/amavisd.conf

```
use strict;
$max_servers = 2;
$daemon_user  = 'vscan';
$daemon_group = 'vscan';
$mydomain = 'neonoc.tld';
$MYHOME = '/var/amavis';
$TEMPBASE = "$MYHOME/tmp";
$ENV{TMPDIR} = $TEMPBASE;
$QUARANTINEDIR = '/var/virusmails';
$log_level = 0;
$log_recip_templ = undef;
$DO_SYSLOG = 1;
$syslog_facility = 'mail';
$syslog_priority = 'debug';
$enable_db = 1;
$enable_global_cache = 1;
$nanny_details_level = 2;
$enable_dkim_verification = 1;
$enable_dkim_signing = 1;
...

 ['ClamAV-clamd',
   \&ask_daemon, ["CONTSCAN {}\n", "/var/run/clamav/clamd.sock"],
   qr/\bOK$/m, qr/\bFOUND$/m,
   qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],
...

['ClamAV-clamscan', 'clamscan',
    "--stdout --no-summary -r --tempdir=$TEMPBASE {}",
    [0], qr/:.*\sFOUND$/m, qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],

...
```

Ajustando as permissões

#chown –R vscan:clamav /var/amavis/

Configurado os serviços do "Clamav", "Freshclam" e "Amavisd-new" para iniciar no boot do sistema:

```
#echo &amp;lsquo;clamav_clamd_enable="YES"&amp;rsquo; >> /etc/rc.conf
#echo &amp;lsquo;clamav_freshclam_enable="YES"&amp;rsquo; >> /etc/rc.conf
#echo &amp;lsquo;amavisd_enable=&amp;rdquo;YES&amp;rdquo;&amp;rsquo; >> /etc/rc.conf
```

Iniciando os serviços:

```
#/usr/local/etc/rc.d/clamav-clamd start
#/usr/local/etc/rc.d/clamav-freshclam start
#/usr/local/etc/rc.d/amavisd start
```

Configurando o Postfix

Finalizando a integração devemos alterar os arquivos “/usr/local/etc/postfix/main.cf” e “/usr/local/etc/postfix/master.cf”, adicionando os seguintes parâmetros em cada um deles.

```
#ee /usr/local/etc/postfix/main.cf

content_filter=smtp-amavis:[localhost]:10024
```

```
#ee /usr/local/etc/postfix/master.cf

smtp-amavis  unix  -    -    n    -    2  smtp
   -o smtp_data_done_timeout=1200
   -o smtp_send_xforward_command=yes
   -o disable_dns_lookups=yes

127.0.0.1:10025 inet  n  -    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 mynetworks_style=host
   -o mynetworks=127.0.0.0/8
   -o strict_rfc821_envelopes=yes
   -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
```

Com as alterações realizadas é necessário reiniciar o Postfix.

```
#/usr/local/etc/rc.d/postfix restart
```

Testando o filtro de Vírus.

Crie um e-mail e no corpo da mensagem insira a seguinte string:

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

O e-mail deverá ser descarta e marcado como vírus. Para maiores informações consulte o arquivo de log: “/var/log/maillog”.

Isso é tudo, espero que essas informações possam ser úteis
Meus sinceros agradecimentos ao Marco Túlio pela sua contribuição.

Fonte:

http://www.google.com/
http://blog.al-shami.net/

Wanderson Tinti / wanderson (no-spam) bsd.com.br