Postfix + MySQL + Courier + Roudcube Webmail + Postfixadmin + Quota + DKIM + SPF + Debian Jessie

Objetivo desse How To, precisamos instalar e configurar o Postfix trabalhando com a sua autenticação no MySQL, vou abordar também a instalação e a configuração do Dovecot que podemos utilizar como servidor de Imap e Pop, vou abordar a instalação e configuração do servidor Courier que podemos utilizar para Pop e Imap, tanto o Dovecot quanto o Courier vão utilizar a mesma base do Postfix para autenticar os usuários, para o gerenciamento de contas de Emails e domínios vamos utilizar o Postfixadmin, vamos também utilizar o Spamassassin, Clamav e o Amavis para controle de Anti-Spam e Anti-Vírus, depois vou abordar a instalação e configuração do RoundCubeMail para Webmail, vou abordar também a instalação e configuração do AfterLogic Webmail que acho bem melhor que o Roundcubemail em questão de consumo de recursos e alguns geradores de relatórios para os emails e o munin para ficarmos de olho em nosso servidor, vamos tambem fazer a instalação e configuração do knock e do fail2ban para garantirmos mais segurança para o nosso servidor, também vou estar implementando 2 recursos para garantir a autenticidade dos email umas delas é o SPF e a outra o DKIM.

Prepare o seu sistema com o seguinte script Easy-Debian para que não falte nenhum pacote ou configuração.

Download e Instalação do Postfix e Patch para Quota

Eu vou utilizar os seguintes repositórios para a abordagem deste how-to

```
vi /etc/apt/sources.list
# OFFICIAL REPOSITORY
deb http://ftp.br.debian.org/debian jessie main contrib non-free
deb-src http://ftp.br.debian.org/debian jessie main contrib non-free

# SECURITY UPDATE REPOSITORY
deb http://security.debian.org/ jessie/updates main contrib non-free
deb-src http://security.debian.org/ jessie/updates main contrib non-free

# PROPOSE UPDATE REPOSITORY
deb http://ftp.br.debian.org/debian jessie-proposed-updates main contrib
non-free
deb-src http://ftp.br.debian.org/debian jessie-proposed-updates main contrib
non-free

# Nginx Official Repository
deb http://nginx.org/packages/debian/ jessie nginx
deb-src http://nginx.org/packages/debian/ jessie nginx
```

Agora vamos atualizar as informações dos resitórios

```
apt-get update
```

Vamos receber um aviso a respeito do repositório do Nginx não se preocupe já vamos corrigir este problema logo.

Vamos fazer a instalação de alguns pacotes básicos que vamos precisar para a utilização neste how-to

```
apt-get install wget ruby curl vim nmap tcpdump build-essential aptitude vim -y
```

Se quiser uma configuração básica para o seu vimrc pode utulizar a seguinte.

```
vim ~/.vimrc
" .vimrc - Defaults configurations
syntax enable
set tabstop=2
set shiftwidth=2
set softtabstop=2
set expandtab
set laststatus=2
set ruler
set wildmenu
set lazyredraw
set backspace=indent,eol,start
set complete-=i
set smarttab
set nrformats-=octal
set ttimeout
set ttimeoutlen=100
set incsearch
set autoread
```

Agora vamos ajustar o bashrc do usuário root.

```
vim ~/.bashrc
# ~/.bashrc

# TIPS ABOUT PS1:
http://www.cyberciti.biz/tips/howto-linux-unix-bash-shell-setup-prompt.html
PS1='\[\033[01;31m\]\u@\h\[\033[00m\]:\[\033[01;34m\]\w\[\033[00m\]# '

# SET UP SOME ALIAS
alias ls='ls --color=auto'
alias dir='dir --color=auto'
alias vdir='vdir --color=auto'
alias grep='grep --color=auto'
alias fgrep='fgrep --color=auto'
alias egrep='egrep --color=auto'
alias ll='ls -alF'
```

```
alias la='ls -A'
alias l='ls -CF'
alias df='df -Th'

# SET UP THE DEFAULT EDITOR, THE HISTORY FORMAT AND THE TIME ZONE
export EDITOR=vim
export HISTTIMEFORMAT="%h/%d - %H:%M:%S "
TZ='America/Sao_Paulo'; export TZ

# SOURCE GLOBAL DEFINITIONS
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
fi

# ENABLE RECEIVE MSG FROM ANOTHER USER
mesg y
```

Vamos ajustar para os novos usuários que utilizaram o bash como shell padrão

```
vim /etc/skel/.bashrc
# ~/.bashrc

# TIPS ABOUT PS1:
http://www.cyberciti.biz/tips/howto-linux-unix-bash-shell-setup-prompt.html
PS1='\[\033[01;32m\]\u@\h\[\033[00m\]:\[\033[01;34m\]\w\[\033[00m\]$ '

# SET UP SOME ALIAS
alias ls='ls --color=auto'
alias dir='dir --color=auto'
alias vdir='vdir --color=auto'
alias grep='grep --color=auto'
alias fgrep='fgrep --color=auto'
alias egrep='egrep --color=auto'
alias ll='ls -alF'
alias la='ls -A'
alias l='ls -CF'
alias df='df -Th'

# SET UP THE DEFAULT EDITOR, THE HISTORY FORMAT AND THE TIME ZONE
export EDITOR=vim
export HISTTIMEFORMAT="%h/%d - %H:%M:%S "
TZ='America/Sao_Paulo'; export TZ

# SOURCE GLOBAL DEFINITIONS
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
fi

# ENABLE RECEIVE MSG FROM ANOTHER USER
mesg y
```

Agora vamos obter a chave do repositório do Nginx

```
curl -O http://nginx.org/keys/nginx_signing.key
```

Agora vamos importar a chave

```
apt-key add nginx_signing.key
```

Agora já podemos remover a key

```
rm -rf nginx_signing.key
```

Agora já podemos atualizar os repositórios novamente e se certificar que não temos mais o problema com as chaves.

```
apt-get update
```

Para a instalação do sistema em um ambiente estável é necessário que o sistema esteja atualizado. Para isto execute os comandos abaixo:

```
aptitude update && aptitude dist-upgrade -y
```

Agora vamos obter o código fonte do postfix e o patch para cotas

```
cd /usr/src
apt-get source postfix
wget -c
http://wiki.douglasqsantos.com.br/Downloads/mail/postfix-vda-v13-2.11.3.patc
h
```

Vamos mandar instalar o dos2unix por que aonde ta o site a codificação fica meio bagunçada :(

```
aptitude install dos2unix
```

Agora vamos converter o patch

```
dos2unix postfix-vda-v13-2.11.3.patch
```

Agora vamos aplicar o patch

```
cd /usr/src/postfix-2.11.3 && patch -p1 < /usr/src/postfix-vda-
v13-2.11.3.patch
patching file README_FILES/VDA_README
patching file src/global/mail_params.h
Hunk #1 succeeded at 2413 (offset 46 lines).
patching file src/util/file_limit.c
patching file src/virtual/mailbox.c
patching file src/virtual/maildir.c
patching file src/virtual/virtual.c
```

```
patching file src/virtual/virtual.h
```

Agora vamos ajustar as variáveis do debian para a instalação do postfix

```
export DEBIAN_PRIORITY=critical
export DEBIAN_FRONTEND=noninteractive
```

Agora que já obtemos o pacote do Postfix e aplicamos o patch precisamos instalar as dependências para compilar o pacote.

```
aptitude update && apt-get build-dep postfix -y && apt-get install ssl-cert
-y
```

Agora vamos criar os pacotes .deb

```
cd /usr/src/postfix-2.11.3/
dpkg-buildpackage
cd ../
apt-get remove --purge postfix -y
apt-get remove --purge exim4-daemon-light exim4-daemon-heavy exim4 exim4-
config -y
dpkg -i postfix_*.deb
```

Aqui vamos ter que responder algumas perguntas na instalação dos pacotes.

- Irá perguntar o tipo de configuração do Postfix, No configuration ou Sem Configuração.
- Irá perguntar o nome do domínio kque será utilizado, informe douglasqsantos.com.br

Agora vamos instalar os pacotes adicionais necessários.

```
dpkg -i postfix-*.deb
```

Agora vamos voltar as variáveis ao padrão

```
unset DEBIAN_PRIORITY
unset DEBIAN_FRONTEND
```

Será instalado agora o mailx que é o tradicional agente de mail do utilizador de linha de comandos.

```
aptitude install bsd-mailx -y
```

Agora vamos ajustar o Debian para ele não atualizar o postfix e sobreescrever o nosso postfix com patch

```
vim /etc/apt/preferences
#Pacote core do postfix
Package: postfix
Pin: release a=stable
Pin-Priority: -1
```

```
Package: postfix
Pin: release a=testing
Pin-Priority: -1

Package: postfix
Pin: release a=unstable
Pin-Priority: -1

#Pacotes adicionais do postfix
Package: postfix-*
Pin: release a=stable
Pin-Priority: -1

Package: postfix-*
Pin: release a=testing
Pin-Priority: -1

Package: postfix-*
Pin: release a=unstable
Pin-Priority: -1
```

Ajuste de alguns parâmetros do sistema

Agora vamos acertar alguns parâmetros do sistema Nome e ip do servidor

```
vim /etc/hosts
127.0.0.1       localhost
ip_servidor     mail.douglasqsantos.com.br    mail
```

Agora vamos acertar o hostname

```
vim /etc/hostname
mail.douglasqsantos.com.br
```

Agora vamos acertar o mailname do servidor

```
vim /etc/mailname
mail.douglasqsantos.com.br
```

Agora vamos reiniciar o servidor para acertar o resto do sistema

```
reboot
```

Instalação do Nginx e MySQL para a utilização do

Postfixadmin

```
aptitude update && aptitude dist-upgrade -y
aptitude install mysql-server mysql-client nginx-full php5 php5-fpm php-pear
php5-mysql php5-imap \
 libpam-mysql apache2-utils -y
```

Será solicitado a senha do banco de dados, informe e confirme ela. Agora precisamos instalar alguns pacotes para que o postfixadmin funcione corretamente

```
aptitude install php5-gd php5-mcrypt php5-json php5-xmlrpc php5-dev php5-
common \
 php5-intl php5-curl -y
```

Agora vamos criar um backup da configuração do Nginx

```
cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf.bkp
```

Agora vamos ajustar as confs

```
vim /etc/nginx/nginx.conf
#/etc/nginx/nginx.conf
## Usuário que vai ser utilizado pelo daemon
user www-data;
## Quantas instancias do nginx vão rodar.
worker_processes 4;
## Local para armazenar o pid do serviço.
pid /var/run/nginx.pid;

## Definições globais do servidor
events {
        ## Quantas conexões uma instancia vai poder manupular.
        worker_connections 768;
        ## Continua aceitando conexões mesmo que o servidor não tenha
manipulado as que estão em aberto.
        # multi_accept on;
}

## Aqui aonde temos as customizações necessárias
http {
        ## GLOBAL
        ## Habilitando está opção aumenta a velocidade do Nginx faz cache e
lê do cache.
        sendfile on;
        ## Está opção habilita o Nginx a tentar enviar cabeçalho de
responstas HTTP em um pacote.
        tcp_nopush on;
        ## Está opção desabilita buffer que quando usado com keep-alive
connections pode deixar as coisas lentas.
```

```
        tcp_nodelay on;
        ## Define o tamanho máximo da tabela de hash. Esta diretiva
influencia na performace do cache. Quanto maior o numero mais memória é
utilizada, oferecendo maior performace.
        types_hash_max_size 2048;
        ## Habilita ou desabilita o Nginx mostrar a versão em mensagens de
erro ou em Server no  response header field.
        server_tokens off;
        ## Define o bucket size para tabela de hash de servidores de nome.
        # server_names_hash_bucket_size 64;
        ## Habilita ou desabilita o uso do servidor de nome primário,
especificado na diretiva server_name nas questões de redirects feitas pelo
Nginx.
        # server_name_in_redirect off;
        ## Inclusão das configurações de mime.types
        include /etc/nginx/mime.types;
        ## Define o  MIME type padrão para as respostas do servidor.
Mapeamento da extensão do arquivo para o  MIME types pode ser definida na
diretiva de types.
        default_type application/octet-stream;

        ## Configurações de Log
        access_log /var/log/nginx/access.log combined;
        error_log /var/log/nginx/error.log;

        ## Configurações de Gzip
        ## Habilita ou desabilita respostas no formato gzip.
        gzip on;
        ## Desabilita respostas gzip para as requisições com campo de
cabeçalho "User-Agent" combinando com qualquer expressão regular.
        gzip_disable "msie6";
        ## Habilita ou desabilita a inserção de no campo de cabeçalho "Vary:
Accept-Encoding" se as diretivas gzip, gzip_static, or gunzip estiverem
habilitadas.
        gzip_vary on;
        ## Habilita ou desabilita respostas gzip para requisições de proxy
dependendo da requisição e da respostas.
        gzip_proxied any;
        ## Define nível da compressão gzip para resposta. Valores aceitaveis
são de 1 até 9.
        gzip_comp_level 6;
        ## Define o numero e tamanho do buffer usado para comprimir a
resposta. Por padrão o tamanho do buffer é igual uma pagina de memória.
        gzip_buffers 16 8k;
        ## Define a versão miníma da requisição HTTP para a compressão da
resposta.
        gzip_http_version 1.1;
        ##  Habilita respostas gzip para especificos MIME types adicionais a
"text/html".
        gzip_types text/plain text/css application/json application/x-
```

```
javascript text/xml application/xml application/xml+rss text/javascript;

        ## Controlando : Size Limits & Buffer Overflows ##
        # (padrão é 8k ou 16k) esta diretiva define o tamanho do buffer do
corpo da requisição
        client_body_buffer_size  1K;
        # Esta diretiva define o tamanho headerbuffer para cabeçalhos de
requisições dos clientes.
        client_header_buffer_size 1k;
        # Diretiva Define o bamaho maximo do corpo da requisição do cliente,
indicado pela linha Content-Length no cabeçalho da requisição
        client_max_body_size 20M;
        # Diretiva deinfe o numero e o tamanho do buffer para cabeçalhos
grandes para leitura da requisição do cliente.
        large_client_header_buffers 2 1k;
        ## Fim: Size Limits & Buffer Overflows ##
        ## Timeouts ##
        # Diretiva define o timeout para leitura de corpo de requisições
pelo cliente.
        client_body_timeout   10;
        # Diretiva define o timeout para leitura do titulo da requisição do
cliente.
        client_header_timeout 10;
        # O primeiro parametro define o timout para o keep-alive de conexões
com o cliente. O segundo vai fechar as requisições depois do tempo definido.
        keepalive_timeout     5 5;
        # Diretiva define o temeout para respostas do cliente.
        send_timeout          10;
        ## Timeouts ##

        ## Inserindo configurações dos Hosts Virtuais.
        include /etc/nginx/conf.d/*.conf;
        include /etc/nginx/sites-enabled/*;
}
```

Agora vamos fazer uma copia do arquivo de configuração do Virtual Host padrão do Nginx

```
cp -Rfa /etc/nginx/sites-available/default{,.bkp}
```

Agora vamos ajustar este arquivo

```
vim /etc/nginx/sites-available/default
# /etc/nginx/sites-available/default
server {
        # Porta que vai estar escutando
        listen 80 default_server;
        # Raiz do Servidor
        root /var/www/html;
        # Possiveis arquivos de index
        index index.html index.htm index.nginx-debian.html index.php;
        server_name _;
```

```
        location / {
                try_files $uri $uri/ =404;
        }
        # PHP Configuration for Nginx
        location ~ \.php$ {
                include snippets/fastcgi-php.conf;
                fastcgi_pass unix:/var/run/php5-fpm.sock;
        }
}
```

Agora vamos ajustar as configurações do PHP

```
vim /etc/php5/fpm/php.ini
[...]
disable_functions =
pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifsto
pped,pcntl_wifsignaled,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl
_signal,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigp
rocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pc
ntl_setpriority,phpinfo,system,mail,exec
[...]
display_errors = Off
[...]
sql.safe_mode = On
[...]
allow_url_fopen = Off
[...]
; Tamanho máximo do arquivo de upload
upload_max_filesize = 20M
[...]
; Tamanho máximo do post que pode ser enviado
post_max_size = 20M
```

Agora precisamos reiniciar o servidor PHP

```
systemctl restart php5-fpm
```

Criação do banco de dados dos usuários de e-mail

```
mysql -u root -p
CREATE DATABASE mail;
GRANT ALL PRIVILEGES ON mail.* TO mail@localhost IDENTIFIED BY "123";
FLUSH PRIVILEGES;
quit;
```

Instalação e configuração do PostFixAdmin

A versão 2.3.5 do postfixadmin ta com bug no envio de email para Alias, por isso estou utilizando a

versão 2.3.3.

```
cd /var/www/html/
rm -rf *
wget -c
http://wiki.douglasqsantos.com.br/Downloads/mail/postfixadmin-2.93.tar.gz
tar -xzvf postfixadmin-2.93.tar.gz
mv postfixadmin-2.93 postfixadmin
rm -rf postfixadmin-2.93*
chown -R www-data:www-data *
```

Faça as alterações necessárias para o postfixadmin, aqui o que você vai precisar mudar com certeza é douglasqsantos.com.br que é o domínio e a senha que eu coloquei como 123 ;)

```
sed -i "s/change-this-to-your.domain.tld/douglasqsantos.com.br/g"
/var/www/html/postfixadmin/config.inc.php
sed -i "s/\$CONF\['configured'\] = false;/\$CONF\['configured'\] = true;/"
/var/www/html/postfixadmin/config.inc.php
sed -i "s/\$CONF\['default_language'\] = 'en';/\$CONF\['default_language'\]
= 'pt-br';/" /var/www/html/postfixadmin/config.inc.php
sed -i "s/\$CONF\['database_user'\] = 'postfix';/\$CONF\['database_user'\] =
'mail';/" /var/www/html/postfixadmin/config.inc.php
sed -i "s/\$CONF\['database_password'\] =
'postfixadmin';/\$CONF\['database_password'\] = '123';/"
/var/www/html/postfixadmin/config.inc.php
sed -i "s/\$CONF\['database_name'\] = 'postfix';/\$CONF\['database_name'\] =
'mail';/" /var/www/html/postfixadmin/config.inc.php
sed -i "s/\$CONF\['quota'\] = 'NO';/\$CONF\['quota'\] = 'YES';/"
/var/www/html/postfixadmin/config.inc.php
sed -i "s/\$CONF\['transport'\] = 'NO';/\$CONF\['transport'\] = 'YES';/"
/var/www/html/postfixadmin/config.inc.php
sed -i "s/\$CONF\['vacation'\] = 'NO';/\$CONF\['vacation'\] = 'YES';/"
/var/www/html/postfixadmin/config.inc.php
sed -i
"s/\$CONF\['emailcheck_resolve_domain'\]='YES';/\$CONF\['emailcheck_resolve_
domain'\]='NO';/" /var/www/html/postfixadmin/config.inc.php
sed -i "s/\$CONF\['used_quotas'\] = 'NO';/\$CONF\['used_quotas'\] = 'YES';/"
/var/www/html/postfixadmin/config.inc.php
sed -i "s/\$CONF\['aliases'\] = '10';/\$CONF\['aliases'\] = '0';/"
/var/www/html/postfixadmin/config.inc.php
sed -i "s/\$CONF\['mailboxes'\] = '10';/\$CONF\['mailboxes'\] = '0';/"
/var/www/html/postfixadmin/config.inc.php
sed -i "s/\$CONF\['maxquota'\] = '10';/\$CONF\['maxquota'\] = '0';/"
/var/www/html/postfixadmin/config.inc.php
sed -i "s/\$CONF\['domain_quota_default'\] =
'2048';/\$CONF\['domain_quota_default'\] = '0';/"
/var/www/html/postfixadmin/config.inc.php
sed -i "s/\$CONF\['vacation_domain'\] =
'autoreply.douglasqsantos.com.br';/\$CONF\['vacation_domain'\] =
'autoreply2.douglasqsantos.com.br';/"
/var/www/html/postfixadmin/config.inc.php
```

Insira as configurações adicionais do vacation no final do arquivo config.inc.php

```
sed -i -e '301i\' -e "    'vacation',  //for system accounts"
/var/www/html/postfixadmin/config.inc.php
```

Reinicie o serviço do Nginx e o PHP

```
systemctl restart nginx
systemctl restart php5-fpm
```

Acesse pelo seu navegador o menu de configuração do PostfixAdmin para terminar a instalação pelo endereço: http://ip_servidor/postfixadmin/setup.php

- Na primeira tela ele irá fazer a verificação se todos os critérios para funcionar estão instalados e funcionando.
- No final da página, informe a senha para de acesso como administrador
- Depois de alterada a senha, ele vai mostrar a linha com a senha, copie a linha e substitua a linha no arquivo config.inc.php

```
vim /var/www/html/postfixadmin/config.inc.php
 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
the field,
 on submission it will be echoed out to you as a hashed value.
#$CONF['setup_password'] = 'changeme';
$CONF['setup_password'] =
'e41f87fe3d8bd1f5ba8b09ebf08f9fc6:f2a27ac501bdb8de504dd49d57bb643b654fe877';
```

Depois de alterado o arquivo, volte na tela do postfixadmin e informe o e-mail do administrador e a senha, para testar a autenticação. Agora vamos continuar a nossa configuração.

Vacation

O Vacation funciona para gerenciar as mensagens de ausência ou ferias do usuários. Útil quando você sai de férias por exemplo e não vai ler e-mails por um tempo e deixa uma mensagem pré-definida com as informações sobre as pessoas que vão ser contactadas no tempo que você estará fora.
Preparando o ambiente:

Vamos criar o grupo e o usuário vacation

```
groupadd vacation
useradd -d /var/spool/vacation -g vacation -s /bin/false -m vacation
```

Agora vamos copiar o arquivo do vacation para o seu home

```
cp /var/www/html/postfixadmin/VIRTUAL_VACATION/vacation.pl
/var/spool/vacation/
```

Agora vamos criar o diretório que vai armazenar os logs e acertar as permissões dos diretórios e arquivos

```
mkdir /var/log/vacation/
chown -R vacation:vacation /var/spool/vacation/
chown -R vacation:vacation /var/log/vacation/
chmod 750 /var/spool/vacation/
chmod 700 /var/spool/vacation/vacation.pl
touch /var/log/vacation.log
chown vacation:vacation /var/log/vacation.log
```

Agora vamos instalar as dependências para o vacation funcionar corretamente

```
aptitude install libmail-sender-perl libemail-valid-perl libmime-tools-perl
liblog-log4perl-perl liblog-dispatch-perl -y
aptitude install libgetopt-argvfile-perl libmime-charset-perl libmime-
encwords-perl  -y
```

Vamos acertar as configurações no arquivo vacation.pl

```
vim /var/spool/vacation/vacation.pl
[...]
#our $db_type = 'Pg'; ->temos que comentar essa linha
our $db_type = 'mysql';

# leave empty for connection via UNIX socket
our $db_host = '';

# connection details
our $db_username = 'mail';
our $db_password = '123';
our $db_name     = 'mail';

our $vacation_domain = 'autoreply.douglasqsantos.com.br';

[...]
# Set to 1 to enable logging to syslog.
our $syslog = 1;

# path to logfile, when empty logging is suppressed
# change to e.g. /dev/null if you want nothing logged.
# if we can't write to this, and $log_to_file is 1 (below) the script will
abort.
our $logfile='/var/log/vacation.log';
# 2 = debug + info, 1 = info only, 0 = error only
our $log_level = 1;
# Whether to log to file or not, 0 = do not write to a log file
our $log_to_file = 1;

# notification interval, in seconds
```

```
# set to 0 to notify only once
# e.g. 1 day ...
#our $interval = 60*60*24;
# disabled by default
our $interval = 1*1*1;
[...]
```

Agora vamos criar dois domínios um principal e um domínio para o vacation que vão ser as auto repostas de ferias ou ausência. Logue na tela web http://ip_servidor/postfixadmin

- Selecione Domínios/Criar domínio
  - Agora informe o domínio: douglasqsantos.com.br
  - A sua informe uma descrição: DOUGLAS Principal
  - Agora informe quantos Alias podem haver ou deixe 0 para ilimitados
  - Agora informe Contas de email que pode haver ou deixe 0 para ilimitadas
  - Agora Cota de Espaço (MB) informe um valor ou deixe 0 para ilimitado
  - Agora Domain Quota informe um valor ou deixe 0 para ilimitado
  - Transporte deixe o virtual
  - Selecione Adicionar aliases padrão
  - E selecione Criar domínio
- Selecione Domínios/Criar domínio
  - Agora informe o domínio: autoreply.douglasqsantos.com.br
  - A sua informe uma descrição: DOUGLAS Vacations
  - Agora informe quantos Alias podem haver ou deixe 0 para ilimitados
  - Agora informe Contas de email que pode haver ou deixe 0 para ilimitadas
  - Agora Cota de Espaço (MB) informe um valor ou deixe 0 para ilimitado
  - Agora Domain Quota informe um valor ou deixe 0 para ilimitado
  - Transporte deixe o: vacation
  - Selecione Adicionar aliases padrão
  - E selecione Criar domínio

Agora vamos habilitar o domínio de férias no postfixadmin

```
sed -i "s/\$CONF\['vacation_domain'\] =
'autoreply2.douglasqsantos.com.br';/\$CONF\['vacation_domain'\] =
'autoreply.douglasqsantos.com.br';/"
/var/www/html/postfixadmin/config.inc.php
```

Após terminar de configurar o servidor de email podemos definir a conta como **Modo de férias** e configurar a mensagem de auto-resposta.

Configuração do Postifx

Vamos instalar os módulos que serão usados para autenticação.

```
aptitude install libsasl2-2 libsasl2-modules-sql -y
aptitude install libsasl2-modules libsasl2-dev sasl2-bin openssl   -y
```

Agora vamos obter o gid do Postfix

```
grep postfix /etc/passwd
postfix:x:109:116::/var/spool/postfix:/bin/false
```

Como podemos notar o gid do postfix é 116 esse valor vai ser usado para criarmos o vmail que vai ser responsável pelas mensagens e pela identificação dos modulos do courierauthmysql

```
adduser --system --shell /bin/false --uid 116 --gid 116 vmail
Adicionando usuário de sistema 'vmail' (UID 116) ...
Adicionando novo usuário 'vmail' (UID 116) com grupo 'postfix' ...
Criando diretório pessoal '/home/vmail' ...
```

Instalando os módulos do postfix

```
aptitude install postfix-policyd-spf-perl -y
```

Caso de algum erro no pacote acima que eu estou enfrentando hoje, tem que obter o pacote manualmente e mandar instalar

```
wget -c
http://ftp.br.debian.org/debian/pool/main/p/postfix-policyd-spf-perl/postfix
-policyd-spf-perl_2.010-1_all.deb
dpkg -i postfix-policyd-spf-perl_2.010-1_all.deb
apt-get -f install -y
rm -rf postfix-policyd-spf-perl_2.010-1_all.deb
```

Agora vamos acertar as permissões do diretório do vmail

```
chown -R vmail:postdrop /home/vmail
```

Vamos fazer um backup do arquivo original

```
cp -Rfa /etc/postfix/main.cf{,.bkp}
```

Agora vamos configurar o nosso postfix

```
vim /etc/postfix/main.cf
#---------------------------------MAIN-----------------------------------
---
smtpd_banner                    = $myhostname ESMTP
biff                            = no
append_dot_mydomain             = no
readme_directory                = no
alias_maps                      = hash:/etc/postfix/aliases
alias_database                  = hash:/etc/postfix/aliases
myhostname                      = mail.douglasqsantos.com.br
mydomain                        = douglasqsantos.com.br
myorigin                        = $myhostname
mydestination                   = $myhostname, localhost
```

```
relayhost                       =
mynetworks                      = 127.0.0.0/8, 192.168.254.0/24,
[::ffff:127.0.0.0]/104, [::1]/128
relay_domains                   = $mydestination
home_mailbox                    = Maildir/
mailbox_command                 = /usr/bin/procmail -a "$EXTENSION"
DEFAULT=$HOME/Maildir/ MAILDIR=$HOME/Maildir/
mailbox_size_limit              = 0
message_size_limit              = 10240000
recipient_delimiter             = +
mynetworks_style                = subnet
inet_interfaces                 = all
default_transport               = smtp
smtpd_recipient_limit           = 30
bounce_queue_lifetime           = 300s
maximal_queue_lifetime          = 300s
#-----------------------------END MAIN-------------------------------------
---
#-----------------------------SASL-----------------------------------------
---
smtpd_sasl_auth_enable          = yes
smtpd_sasl_security_options     = noanonymous
broken_sasl_auth_clients        = yes
smtpd_sasl_local_domain         = $mydomain
#-----------------------------END SASL-------------------------------------
---
#-------------------------------TLS----------------------------------------
---
smtp_tls_CAfile                 = /etc/postfix/ssl/cacert.pem
smtp_tls_cert_file              = /etc/postfix/ssl/smtpd.crt
smtp_tls_key_file               = /etc/postfix/ssl/smtpd.key
smtp_tls_session_cache_database =
btree:/var/lib/postfix/smtp_tls_session_cache
smtp_tls_security_level         = may
smtpd_tls_CAfile                = /etc/postfix/ssl/cacert.pem
smtpd_tls_cert_file             = /etc/postfix/ssl/smtpd.crt
smtpd_tls_key_file              = /etc/postfix/ssl/smtpd.key
smtpd_tls_session_cache_database =
btree:/var/lib/postfix/smtpd_tls_session_cache
smtpd_tls_dh1024_param_file     = /etc/postfix/ssl/dh_1024.pem
smtpd_tls_dh512_param_file      = /etc/postfix/ssl/dh_512.pem
smtpd_tls_security_level        = may
smtpd_tls_received_header       = yes
smtpd_tls_ask_ccert             = yes
smtpd_tls_loglevel              = 1
tls_random_source               = dev:/dev/urandom
smtpd_enforce_tls               = yes
#-----------------------------END TLS--------------------------------------
-----
#-------------------------------MYSQL--------------------------------------
```

```
-----
transport_maps                  =
proxy:mysql:/etc/postfix/mysql_transport_maps.cf
virtual_alias_maps              =
proxy:mysql:/etc/postfix/mysql_virtual_alias_maps.cf
virtual_mailbox_domains         =
proxy:mysql:/etc/postfix/mysql_virtual_domains_maps.cf
virtual_mailbox_maps            =
proxy:mysql:/etc/postfix/mysql_virtual_mailbox_maps.cf
virtual_transport               = virtual
virtual_minimum_uid             = 116
virtual_uid_maps                = static:116
virtual_gid_maps                = static:116
virtual_mailbox_base            = /home/vmail
#-----------------------------END MYSQL-------------------------------------
------
#-----------------------------QUOTA-----------------------------------------
------
virtual_mailbox_limit           = 512000000
virtual_maildir_extended        = yes
virtual_mailbox_limit_override  = yes
virtual_mailbox_limit_maps      =
mysql:/etc/postfix/mysql_virtual_mailbox_limit_maps.cf
virtual_overquota_bounce        = yes
virtual_maildir_limit_message   = Desculpe, o diretorio de correio do
usuario estourou sua quota, por favor tente novamente depois.
#----------------------------END QUOTA--------------------------------------
-----
#----------------------------CONTROLS---------------------------------------
-----
content_filter = smtp-amavis:[127.0.0.1]:10024
receive_override_options = no_address_mappings
smtpd_helo_restrictions =
 permit_mynetworks,
 permit_sasl_authenticated,
 reject_invalid_hostname,
 reject_unknown_hostname,
 reject_non_fqdn_hostname,
 reject_unauth_pipelining
smtpd_client_restrictions =
 permit_mynetworks,
 permit_sasl_authenticated,
 reject_unauth_pipelining,
 reject_rbl_client dnsbl.sorbs.net,
 reject_rbl_client rbl.schulte.org,
 reject_rbl_client dnsbl.anticaptcha.net,
 reject_rbl_client bl.spamcannibal.org,
 reject_rbl_client bl.spamcop.net,
 reject_rbl_client cart00ney.surriel.com,
 reject_rbl_client korea.services.net,
 reject_rbl_client cbl.abuseat.org,
```

```
 reject_unknown_client
smtpd_sender_restrictions =
 permit_mynetworks,
 permit_sasl_authenticated,
 check_policy_service unix:private/policy,
 reject_non_fqdn_sender,
 reject_unauth_pipelining,
 reject_unknown_sender_domain,
smtpd_recipient_restrictions =
 permit_mynetworks,
 permit_sasl_authenticated,
 reject_invalid_hostname,
 reject_non_fqdn_hostname,
 reject_non_fqdn_recipient,
 reject_unauth_destination,
 reject_unauth_pipelining,
 reject_unknown_recipient_domain,
 check_policy_service inet:127.0.0.1:60000,
 reject_unknown_client
#-----------------------END CONTROLS---------------------------------------
----
```

Geração das chaves para a conexão via TLS no Postfix

Vamos gerar as chaves de autenticação

```
mkdir /etc/postfix/ssl
cd /etc/postfix/ssl/
openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 1024
52 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.......++++++
.....................................................................++++++
e is 65537 (0x10001)
Enter pass phrase for smtpd.key: senha
Verifying - Enter pass phrase for smtpd.key: senha
```

Acertando permissão da key gerada

```
chmod 600 smtpd.key
```

Agora vamos gerar o pedido de assinatura

```
openssl req -new -key smtpd.key -out smtpd.csr
Enter pass phrase for smtpd.key: senha
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
```

```
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:Parana
Locality Name (eg, city) []:Curitiba
Organization Name (eg, company) [Internet Widgits Pty Ltd]:DOUGLAS
Organizational Unit Name (eg, section) []:IT
Common Name (eg, YOUR name) []:mail.douglasqsantos.com.br
Email Address []:douglas@douglasqsantos.com.br

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:DOUGLAS
```

Vamos assinar agora o nosso certificado

```
openssl x509 -req -days 3650 -in smtpd.csr -signkey smtpd.key -out smtpd.crt
Signature ok
subject=/C=BR/ST=Parana/L=Curitiba/O=DOUGLAS/OU=IT/CN=mail.douglasqsantos.co
m.br/emailAddress=douglas@douglasqsantos.com.br
Getting Private key
Enter pass phrase for smtpd.key:
```

Agora vamos tirar a senha do certificado agora

```
openssl rsa -in smtpd.key -out smtpd.key.unencrypted
Enter pass phrase for smtpd.key: senha
writing RSA key
```

Gerando o CA

```
mv -f smtpd.key.unencrypted smtpd.key
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -
days 3650
Generating a 1024 bit RSA private key
.++++++
......++++++
writing new private key to 'cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

```
Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:Parana
Locality Name (eg, city) []:Curitiba
Organization Name (eg, company) [Internet Widgits Pty Ltd]:DOUGLAS
Organizational Unit Name (eg, section) []:IT
Common Name (eg, YOUR name) []:mail.douglasqsantos.com.br
Email Address []:douglas@douglasqsantos.com.br
```

Ultimas chaves de Diffie Hellman

```
openssl dhparam 1024 -out dh_1024.pem
openssl dhparam 512 -out dh_512.pem
```

Configuração da conexão do MySQL + Postfix

Vamos configurar o arquivo que tem o controle do tipo de transporte se vai ser virtual ou vacation por exemplo

```
vim /etc/postfix/mysql_transport_maps.cf
user = mail
password = 123
hosts = localhost
dbname = mail
table = domain
select_field = transport
where_field = domain
```

Aqui vamos configurar o arquivo que controla as contas de email

```
vim /etc/postfix/mysql_virtual_alias_maps.cf
user = mail
password = 123
hosts = localhost
dbname = mail
table = alias
select_field = goto
where_field = address
```

Aqui vamos configurar o arquivo que controla os domínios do postfix

```
vim /etc/postfix/mysql_virtual_domains_maps.cf
user = mail
password = 123
hosts = localhost
dbname = mail
table = domain
select_field = domain
where_field = domain
```

Aqui vamos acertar o arquivo que controla as cotas do usuários e domínios

```
vim /etc/postfix/mysql_virtual_mailbox_limit_maps.cf
user = mail
password = 123
hosts = localhost
dbname = mail
table = mailbox
select_field = quota
where_field = username
```

Aqui vamos acertar o arquivo que controla as mailbox

```
vim /etc/postfix/mysql_virtual_mailbox_maps.cf
user = mail
password = 123
hosts = localhost
dbname = mail
query = SELECT maildir FROM mailbox WHERE username='%s' AND active = 1
```

Vamos acertar as permissões

```
chmod o= /etc/postfix/mysql_*
chgrp postfix /etc/postfix/mysql_*
```

Vamos fazer o acerto dos aliases agora

```
mv /etc/aliases /etc/postfix
```

Ajustando arquivos de aliases para os redirecionamentos

```
vim /etc/postfix/aliases
[...]
root: douglas@douglasqsantos.com.br
```

Agora vamos gerar a nova base de dados dos aliases

```
newaliases
```

Vamos fazer backup do arquivo de configuração

```
cp /etc/postfix/master.cf{,.bkp}
```

Ajustando arquivo de serviços do postfix

```
vim /etc/postfix/master.cf
#-------------------------SERVICES---------------------------------------
--
#-----------------------------------------------------------------------
```

```
--
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
#----------------------------------------------------------------------
--
smtp      inet  n       -       -       -       -       smtpd
submission inet n       -       -       -       -       smtpd
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
#smtps     inet  n       -       -       -       -       smtpd
  -o smtpd_sasl_auth_enable=yes
pickup    fifo  n       -       -       60      1       pickup
cleanup   unix  n       -       -       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
tlsmgr    unix  -       -       -       1000?   1       tlsmgr
rewrite   unix  -       -       -       -       -       trivial-rewrite
bounce    unix  -       -       -       -       0       bounce
defer     unix  -       -       -       -       0       bounce
trace     unix  -       -       -       -       0       bounce
verify    unix  -       -       -       -       1       verify
flush     unix  n       -       -       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
proxywrite unix -       -       n       -       1       proxymap
smtp      unix  -       -       -       -       -       smtp
relay     unix  -       -       -       -       -       smtp
        -o smtp_fallback_relay=
showq     unix  n       -       -       -       -       showq
error     unix  -       -       -       -       -       error
retry     unix  -       -       -       -       -       error
discard   unix  -       -       -       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       -       -       -       lmtp
anvil     unix  -       -       -       -       1       anvil
scache    unix  -       -       -       -       1       scache
#-----------------------------END SERVICES---------------------------------
------
#----------------------------DELIVERY METHODS------------------------------
------
maildrop  unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail argv=/usr/bin/maildrop -d ${recipient}
uucp      unix  -       n       n       -       -       pipe
  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail
($recipient)
ifmail    unix  -       n       n       -       -       pipe
  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
bsmtp     unix  -       n       n       -       -       pipe
  flags=Fq. user=bsmtp argv=/usr/lib/bsmtp/bsmtp -t$nexthop -f$sender
$recipient
scalemail-backend unix  -       n       n       -       2       pipe
```

```
  flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store
${nexthop} ${user} ${extension}
mailman   unix  -       n       n       -       -       pipe
  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
  ${nexthop} ${user}
#--------------------------END DELIVERY METHODS----------------------------
------------------
#---------------------------SPF-----------------------------------------
------------------
policy  unix  -       n       n       -       -       spawn
 user=nobody argv=/usr/bin/perl /usr/sbin/postfix-policyd-spf-perl
#---------------------------END SPF-------------------------------------
------------------
#----------------------------VACATION-----------------------------------
------------------
vacation    unix  -       n       n       -       -       pipe
  flags=Rq user=vacation argv=/var/spool/vacation/vacation.pl -f ${sender} -
- ${recipient}
#----------------------------END VACATION-------------------------------
------------------
#-------------------------------------AMAVIS-----------------------------
------------------
smtp-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
        -o smtp_generic_maps=

127.0.0.1:10025 inet    n -     -       -       -       smtpd
        -o content_filter=
        -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_end_of_data_restrictions=
        -o smtpd_restriction_classes=
        -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
        -o local_header_rewrite_clients=
        -o local_recipient_maps=
        -o relay_recipient_maps=
        -o strict_rfc821_envelopes=yes
#-----------------------------------END AMAVIS----------------------------
```

```
--------------------
```

Configuração do controle de autenticação do Postfix

Agora vamos configurar o sasl

```
vim /usr/lib/sasl2/smtpd.conf
#/usr/lib/sasl2/smtpd.conf
pwcheck_method: saslauthd
mech_list: PLAIN LOGIN
auxprop_plugin: sql
sql_engine: mysql
sql_hostnames: 127.0.0.1
sql_user: mail
sql_passwd: 123
sql_database: mail
sql_select: select password from mailbox where username = '%u@%r'
allowanonymouslogin: no
allowplaintext: yes
#Para efetuar debug de problemas analisar o arquivo /var/log/auth.log
#sql_verbose: yes
#log_level: 9
```

Vamos acertar a localização do arquivo com um link

```
ln -sf /usr/lib/sasl2/smtpd.conf /etc/postfix/sasl/smtpd.conf
```

Vamos colocar o sasl no grupo do postfix

```
usermod -G sasl postfix
```

Agora vamos acertar o sasauthd mais primeiro vamos fazer o backup do arquivo

```
cp /etc/default/saslauthd{,.bkp}
```

Agora vamos acertar a configuração do arquivo saslauthd

```
vim /etc/default/saslauthd
#/etc/default/saslauthd
START=yes
DESC="SASL Authentication Daemon"
NAME="saslauthd"
MECHANISMS="pam"
MECH_OPTIONS=""
THREADS=5
OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd -r"
```

Vamos acertar os arquivos do saslauthd para o postfix

```
mkdir -p /var/spool/postfix/var/run/saslauthd
chown postfix /var/spool/postfix/var/run/saslauthd/
cd /var/run
mv saslauthd saslauthd.bkp
ln -sf /var/spool/postfix/var/run/saslauthd
```

Agora vamos preparar o mysql para trabalhar com o Postfix

```
mkdir -p /var/spool/postfix/var/run/mysqld
```

Agora vamos acertar o arquivo de inicialização do MySQL

```
vim /etc/init.d/mysql
[...]
        fi
#insira a linha abaixo antes do ;; por quando o mysql for iniciar ele cria o
socket e o link
/bin/ln -sf /var/run/mysqld/mysqld.sock
/var/spool/postfix/var/run/mysqld/mysqld.sock
        ;;

  'stop')
```

Agora vamos acertar a permissão do diretório /var/run/mysqld

```
chown -R vmail:mysql /var/run/mysqld && chmod -R 775 /var/run/mysqld
```

Agora vamos reiniciar os serviços

```
systemctl daemon-reload
systemctl restart mysql
/etc/init.d/saslauthd restart
```

Galera aqui vou demostrar a instalação do Courier e do Dovecot na minha opinião o Dovecot é um pouco mais chato, e o Courier mais simples de manipular.

Instalação do e configuração do Courier

```
aptitude install courier-imap courier-imap-ssl courier-pop courier-pop-ssl
courier-authlib-mysql courier-authdaemon -y
#Resposta1) No
2) Ok
```

Agora vamos fazer backup dos arquivos de configuração do courier

```
cp /etc/courier/authdaemonrc{,.bkp}
cp /etc/courier/authmysqlrc{,.bkp}
```

Agora vamos acertar o arquivo de conexão do Courier com o Mysql

```
vim /etc/courier/authmysqlrc
#/etc/courier/authmysqlrc
MYSQL_SERVER localhost
MYSQL_USERNAME mail
MYSQL_PASSWORD 123
MYSQL_SOCKET /var/run/mysqld/mysqld.sock
MYSQL_PORT 3306
MYSQL_OPT 0
MYSQL_DATABASE mail
MYSQL_USER_TABLE mailbox
MYSQL_CRYPT_PWFIELD password
MYSQL_CLEAR_PWFIELD password
MYSQL_UID_FIELD '116'
MYSQL_GID_FIELD '116'
MYSQL_LOGIN_FIELD username
MYSQL_HOME_FIELD '/home/vmail'
MYSQL_NAME_FIELD name
MYSQL_MAILDIR_FIELD CONCAT("/home/vmail/",maildir)
MYSQL_QUOTA_FIELD concat(quota,'S')
```

Agora vamos acertar a configuração do serviço do Courier

```
vim /etc/courier/authdaemonrc
#/etc/courier/authdaemonrc
authmodulelist="authmysql"
authmodulelistorig="authmysql"
daemons=5
authdaemonvar=/var/run/courier/authdaemon
subsystem=mail
DEFAULTOPTIONS=""
LOGGEROPTS=""
```

Agora vamos acertar a configuração dos arquivos que vão gerar os nosso certificados para ssl. Primeiro vamos editar o arquivo do imap

```
vim /etc/courier/imapd.cnf

RANDFILE = /usr/lib/courier/imapd.rand

[ req ]
default_bits = 1024
encrypt_key = yes
distinguished_name = req_dn
x509_extensions = cert_type
prompt = no

[ req_dn ]
C=BR
```

```
ST=PR
L=Curitiba
O=Douglas Imap Server
OU=Douglas IMAP SSL key
CN=mail.douglasqsantos.com.br
emailAddress=postmaster@douglasqsantos.com.br


[ cert_type ]
nsCertType = server
```

Agora vamos editar o arquivo do pop

```
vim /etc/courier/pop3d.cnf
RANDFILE = /usr/lib/courier/pop3d.rand

[ req ]
default_bits = 1024
encrypt_key = yes
distinguished_name = req_dn
x509_extensions = cert_type
prompt = no

[ req_dn ]
C=BR
ST=PR
L=Curitiba
O=Douglas Pop Server
OU=Douglas POP3 SSL key
CN=mail.douglasqsantos.com.br
emailAddress=postmaster@douglasqsantos.com.br


[ cert_type ]
nsCertType = server
```

Agora vamos fazer backup dos certificados antigos.

```
mv /etc/courier/pop3d.pem /etc/courier/pop3d.pem.bkp
mv /etc/courier/imapd.pem /etc/courier/imapd.pem.bkp
```

Agora vamos gerar o novo certificado para o Imap-ssl

```
mkimapdcert
```

Agora vamos gerar o novo certificado para o Pop-ssl

```
mkpop3dcert
```

Ajustando a forma de autenticação do POP3, IMAP e SMTP

```
vim /etc/pam.d/pop3
auth required pam_mysql.so user=mail passwd=123 host=localhost db=mail
table=mailbox usercolumn=username passwdcolumn=password crypt=1 sqllog=0
debug
account sufficient pam_mysql.so user=mail passwd=123 host=localhost db=mail
table=mailbox usercolumn=username passwdcolumn=password crypt=1 sqllog=0
debug
auth sufficient pam_unix.so debug
account sufficient pam_unix.so debug
```

Agora vamos copiar os arquivos da pam

```
cp -Rfa /etc/pam.d/pop3 /etc/pam.d/imap
cp -Rfa /etc/pam.d/pop3 /etc/pam.d/smtp
```

Agora é só reiniciar os serviços

```
systemctl restart courier-authdaemon
systemctl restart courier-imap
systemctl restart courier-imap-ssl
systemctl restart courier-pop
systemctl restart courier-pop-ssl
```

Instalação e configuração do Dovecot

Dovecot é um servidor de IMAP e POP3 open source para sistemas Linux e UNIX, escrito primariamente com segurança em mente. Dovecot tem o objetivo primário de ser um servidor de email open source leve, rápido e de fácil configuração.

Dovecot suporta mbox, Maildir e seu próprio formato nativo de alta performance Dbox. É 100% compatível com os servidores UW IMAP, Courier IMAP, e clientes de emails acessando as caixas de correio diretamente.

Dovecot também inclui um agente de entrega de emails (chamado “Local delivery agent” na documentação do Dovecot), com suporte opcional a filtros Sieve.

Vamos instalar o dovecot

```
aptitude install dovecot-dev dovecot-imapd dovecot-pop3d dovecot-mysql -y
```

Vamos acertar as chaves de criptografia para o nosso servidor

```
find /etc -iname "dovecot.pem" -exec rm -rf {} \;
```

Agora vamos gerar elas novamente com os valores necessários Vamos criar o diretório para armazenar as chaves

```
mkdir /etc/ssl/dovecot
```

```
cd /etc/ssl/dovecot
```

Gerar a chave principal

```
openssl genrsa -des3 -rand /etc/hosts -out dovecot.key 1024
302 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.....................................++++++
.................++++++
e is 65537 (0x10001)
Enter pass phrase for dovecot.key:
Verifying - Enter pass phrase for dovecot.key:
```

Agora vamos acertar a permissão

```
chmod 600 dovecot.key
```

Agora vamos gerar o csr

```
openssl req -new -key dovecot.key -out dovecot.csr
Enter pass phrase for dovecot.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:Parana
Locality Name (eg, city) []:Curitiba
Organization Name (eg, company) [Internet Widgits Pty Ltd]:DOUGLAS
Organizational Unit Name (eg, section) []:TI
Common Name (eg, YOUR name) []:mail.douglasqsantos.com.br
Email Address []:postmaster@douglasqsantos.com.br

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:DOUGLAS
```

Agora vamos assinar a nossa chave

```
openssl x509 -req -days 3650 -in dovecot.csr -signkey dovecot.key -out
dovecot.crt
Signature ok
subject=/C=BR/ST=Parana/L=Curitiba/O=DOUGLAS/OU=TI/CN=mail.douglasqsantos.co
m.br /emailAddress=postmaster@douglasqsantos.com.br
Getting Private key
Enter pass phrase for dovecot.key:
```

Vamos tirar a senha do nosso certificado

```
openssl rsa -in dovecot.key -out dovecot.key.unencrypted
Enter pass phrase for dovecot.key:
writing RSA key
```

Agora vamos acertar o nome dela

```
mv -f dovecot.key.unencrypted dovecot.key
```

Agora vamos gerar a nossa entidade certificadora

```
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -
days 3650
Generating a 1024 bit RSA private key
.....................................................++++++
...................++++++
writing new private key to 'cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PR
State or Province Name (full name) [Some-State]:Curitiba
Locality Name (eg, city) []:Parana
Organization Name (eg, company) [Internet Widgits Pty Ltd]:DOUGLAS
Organizational Unit Name (eg, section) []:TI
Common Name (eg, YOUR name) []:mail.douglasqsantos.com.br
Email Address []:postmaster@douglasqsantos.com.br
```

Agora vamos fazer um backup do arquivo do dovecot

```
cp /etc/dovecot/dovecot.conf{,.bkp}
```

Agora vamos acertar o dovecot

```
vim /etc/dovecot/dovecot.conf
### MAIN
mail_location = maildir:/home/mail/%d/%u
maildir_copy_with_hardlinks = yes
protocols = imap pop3
first_valid_uid = 116
last_valid_uid = 116
```

```
mail_plugins = quota

### SSL
ssl = yes
ssl_cert = </etc/ssl/dovecot/dovecot.crt
ssl_key = </etc/ssl/dovecot/dovecot.key

### IMAP
service imap {
  executable = /usr/lib/dovecot/rawlog /usr/lib/dovecot/imap
}
protocol imap {
  mail_plugins = $mail_plugins imap_quota
  imap_client_workarounds = delay-newmail tb-extra-mailbox-sep tb-lsub-flags
  mail_plugin_dir = /usr/lib/dovecot/modules
}

### POP3
service pop3 {
  executable = /usr/lib/dovecot/rawlog /usr/lib/dovecot/pop3
}
protocol pop3 {
  mail_plugins = quota
  pop3_client_workarounds = outlook-no-nuls oe-ns-eoh
}

### LDA
protocol lda {
  mail_plugins = quota
  postmaster_address = postmaster@douglasqsantos.com.br
}

### AUTH
service auth {
    unix_listener auth-client {
        group = postfix
        mode = 0660
        user = postfix
    }
    user = root
}

auth_username_chars =
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ01234567890.-_@
auth_mechanisms = plain login

passdb {
  args = /etc/dovecot/dovecot-sql.conf.ext
  driver = sql
}
```

```
userdb sql {
  args = /etc/dovecot/dovecot-sql.conf.ext
  driver = sql
}

### QUOTA
service dict {
  unix_listener dict {
    mode = 0660
    user = vmail
    group = postfix
  }
}

dict {
  quotadict = mysql:/etc/dovecot/dovecot-dict-sql.conf.ext
}

service quota-warning {
  executable = script /usr/local/bin/quota-warning.sh
  user = vmail
  unix_listener quota-warning {
    group = postfix
    mode = 0660
    user = vmail
  }
}

### PLUGINS
plugin {
   quota = dict:User quota::proxy::quotadict
   quota_rule2 = Trash:storage=+10%%
   quota_warning = storage=100%% quota-warning +100 %u
   quota_warning2 = storage=95%% quota-warning +95 %u
   quota_warning3 = storage=80%% quota-warning +80 %u
   quota_warning4 = -storage=100%% quota-warning -100 %u # user is no longer
over quota
   trash = /etc/dovecot/dovecot-trash.conf.ext
}
```

Agora vamos acertar a autenticação do dovecot no MySQL

```
vim /etc/dovecot/dovecot-sql.conf.ext
# /etc/dovecot/dovecot-sql.conf.ext
# Autenticação em MySQL
default_pass_scheme = CRYPT
# Driver utilizado pelo banco
driver = mysql
# Conexão com o Banco de Dados
connect = host=localhost dbname=mail user=mail password=123
```

```
# Query para obter o usuário, maildir, quota
user_query = SELECT concat('/home/vmail/', maildir) as home,
concat('maildir:/home/vmail/', maildir) as mail, 116 AS uid, 116 AS gid,
concat('*:bytes=', quota) AS quota_rule FROM mailbox WHERE username = '%u'
AND active = '1'
# Query para obter o usuário, senha, maildir
password_query = SELECT username as user, password, concat('/home/vmail/',
maildir) as userdb_home, concat('maildir:/home/vmail/', maildir) as
userdb_mail, 116 as userdb_uid, 116 as userdb_gid FROM mailbox WHERE
username = '%u' AND active = '1'
# Utilizado para o suporte a quota
iterate_query = SELECT username AS user FROM mailbox
```

Agora vamos Ajustar o arquivo de controle de quota

```
vim /etc/dovecot/dovecot-dict-sql.conf.ext
# /etc/dovecot/dovecot-dict-sql.conf.ext
connect = host=localhost dbname=mail user=mail password=123
map {
  pattern = priv/quota/storage
  table = quota2
  username_field = username
  value_field = bytes
}
map {
  pattern = priv/quota/messages
  table = quota2
  username_field = username
  value_field = messages
}
```

Vamos acertar o arquivo de controle de lixeira e spam.

```
vim /etc/dovecot/dovecot-trash.conf.ext
# Spam mailbox is emptied before Trash
1 Spam
# Trash mailbox is emptied before Sent
2 Trash
# If both Sent and "Sent Messages" mailboxes exist, the next oldest message
# to be deleted is looked up from both of the mailboxes.
3 Sent
3 Sent Messages
```

Agora vamos criar o script de warning das quotas

```
vim /usr/local/bin/quota-warning.sh
#!/bin/sh
BOUNDARY="$1"
USER="$2"
MSG=""
if [[ "$BOUNDARY" = "+100" ]]; then
```

```
  MSG="Your mailbox is now overfull (>100%). In order for your account to
continue functioning properly, you need to remove some emails NOW."
elif [[ "$BOUNDARY" = "+95" ]]; then
  MSG="Your mailbox is now over 95% full. Please remove some emails ASAP."
elif [[ "$BOUNDARY" = "+80" ]]; then
  MSG="Your mailbox is now over 80% full. Please consider removing some
emails to save space."
elif [[ "$BOUNDARY" = "-100" ]]; then
  MSG="Your mailbox is now back to normal (<100%)."
fi

cat << EOF | /usr/lib/dovecot/dovecot-lda -d $USER -o
"plugin/quota=maildir:User quota:noenforcing"
From: postmaster@douglasqsantos.com.br
Subject: Email Account Quota Warning

Dear User,

$MSG

Best regards,
Your Mail System
EOF
```

Ajustando a forma de autenticação do POP3, IMAP e SMTP

```
vim /etc/pam.d/pop3
auth required pam_mysql.so user=mail passwd=123 host=localhost db=mail
table=mailbox usercolumn=username passwdcolumn=password crypt=1 sqllog=0
debug
account sufficient pam_mysql.so user=mail passwd=123 host=localhost db=mail
table=mailbox usercolumn=username passwdcolumn=password crypt=1 sqllog=0
debug
auth sufficient pam_unix.so debug
account sufficient pam_unix.so debug
```

Agora vamos copiar os arquivos da pam

```
cp -Rfa /etc/pam.d/pop3 /etc/pam.d/imap
cp -Rfa /etc/pam.d/pop3 /etc/pam.d/smtp
```

As últimas configurações agora ocorrem no servidor posfix, precisamos alterar o virtual_transport para **dovecot**

```
vim /etc/postfix/main.cf
[...]
transport_maps                  =
proxy:mysql:/etc/postfix/mysql_transport_maps.cf
virtual_alias_maps              =
proxy:mysql:/etc/postfix/mysql_virtual_alias_maps.cf
```

```
virtual_mailbox_domains         =
proxy:mysql:/etc/postfix/mysql_virtual_domains_maps.cf
virtual_mailbox_maps            =
proxy:mysql:/etc/postfix/mysql_virtual_mailbox_maps.cf
virtual_transport               = dovecot
[...]
```

Agora precisamos alterar o master.cf para dar suporte a entrega de mensagens

```
vim /etc/posfix/master.cf
[...]
mailman   unix  -       n       n       -       -       pipe
  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
  ${nexthop} ${user}
# Adicione as linhas abaixos
dovecot    unix  -       n       n       -       -       pipe
 flags=DRhu user=vmail:vmail argv=/usr/lib/dovecot/deliver -f ${sender} -d
${recipient}
#--------------------------END DELIVERY METHODS----------------------------
------------------
[...]
```

Instalação e configuração de Anti-Virus e Anti-Spam

Instalação dos pacotes para do antivirus e do antispam.

```
aptitude install bzip2 unrar unzip zip arj pax arc ripole cabextract lzop
p7zip-full libgamin-dev gamin \
 lrzip liblz4-1 zoo rpm2cpio lhasa rpm cpio dspam libauthen-sasl-perl
libdbi-perl libmail-dkim-perl \
 libnet-ldap-perl libsnmp-perl libzeromq-perl nomarch  -y
aptitude install clamav amavisd-new clamav-freshclam clamav-daemon
spamassassin postgrey libpathtools-perl -y
```

Se precisar obter uma lista dos pacotes que podemos instalar adicionamente ao Amavis

```
apt-cache show amavisd-new|grep Suggests
```

Ajustando permissões

```
adduser clamav amavis
```

Vamos parar o freshclam

```
systemctl stop clamav-freshclam
```

Agora precisamos ajustar as permissões do Clamav quando for usar os diretórios do Amavis

```
vim /etc/clamav/clamd.conf
[...]
AllowSupplementaryGroups true
```

Vamos mandar atualizar a base do clamav

```
freshclam
ClamAV update process started at Sat Jan 30 19:41:54 2016
WARNING: Your ClamAV installation is OUTDATED!
WARNING: Local version: 0.98.7 Recommended version: 0.99
DON'T PANIC! Read http://www.clamav.net/support/faq
Downloading main.cvd [100%]
main.cvd updated (version: 55, sigs: 2424225, f-level: 60, builder: neo)
Downloading daily.cvd [100%]
daily.cvd updated (version: 21326, sigs: 1824272, f-level: 63, builder: neo)
Downloading bytecode.cvd [100%]
bytecode.cvd updated (version: 271, sigs: 47, f-level: 63, builder:
anvilleg)
Database updated (4248544 signatures) from db.local.clamav.net (IP:
198.148.78.4)
Clamd successfully notified about the update.
```

Instalando suporte a razor e pyzor

```
apt-get install libnet-dns-perl razor pyzor -y
```

Acertando as configurações do razor e do pyzor

```
su - amavis -c 'razor-admin -d --create'
su - amavis -c 'razor-admin -register'
su - amavis -c 'razor-admin -discover'
su - amavis -c 'pyzor discover'
```

Vamos fazer backup do arquivo de configuração do Spamassassin

```
cp /etc/default/spamassassin{,.bkp}
```

Agora vamos configurar o spamassassin

```
vim /etc/default/spamassassin
#/etc/default/spamassassin
ENABLED=1
OPTIONS="--create-prefs --max-children 5 --helper-home-dir"
PIDFILE="/var/run/spamd.pid"
CRON=0
```

Fazendo um backup do arquivo de configuração do SpamAssassin

```
cp /etc/spamassassin/local.cf{,.bkp}
```

Acertando o SpamAssassin

```
vim /etc/spamassassin/local.cf
#/etc/spamassassin/local.cf
#-------------------------MARKUP----------------------------------------
header DSPAM_SPAM X-DSPAM-Result =~ /^Spam$/
score DSPAM_SPAM 0.5
header DSPAM_HAM X-DSPAM-Result =~ /^Innocent$/
score DSPAM_HAM -0.1
#------------------------END MARKUP-------------------------------------
#---------------------DKIM-----------------------------------------------
score DKIM_VERIFIED -0.1
score DKIM_SIGNED    0
score DKIM_POLICY_SIGNALL  0
score DKIM_POLICY_SIGNSOME 0
score DKIM_POLICY_TESTING  0
score USER_IN_DKIM_WHITELIST -8.0
score USER_IN_DEF_DKIM_WL -1.5
def_whitelist_from_dkim   *@google.com
def_whitelist_from_dkim   *@googlemail.com
def_whitelist_from_dkim   *@*googlegroups.com
score ENV_AND_HDR_DKIM_MATCH -0.1
score ENV_AND_HDR_SPF_MATCH  -0.5
#--------------------END DKIM---------------------------------------------
#--------------------BLACK LIST AND WHITELIST-------------------------
blacklist_from  chakerv@att.net
whitelist_from_dkim  *@ebay.com
whitelist_from_dkim  *@*.ebay.com
whitelist_from_dkim  *@ebay.co.uk
whitelist_from_dkim  *@*.ebay.co.uk
whitelist_from_dkim  *@ebay.at
whitelist_from_dkim  *@ebay.ca
whitelist_from_dkim  *@ebay.de
whitelist_from_dkim  *@ebay.fr
whitelist_from_dkim  *@*.paypal.com
whitelist_from_dkim  *@paypal.com
whitelist_from_dkim  *@*paypal.com
whitelist_from_dkim  *@*.paypal.be
whitelist_from_dkim  *@cern.ch
whitelist_from_dkim  *@amazon.com
whitelist_from_dkim  *@cisco.com
whitelist_from_dkim  *@cnn.com
whitelist_from_dkim  *@*.cnn.com
whitelist_from_dkim  service@youtube.com
whitelist_from_dkim  googlealerts-noreply@google.com
#-------------------END BLACK LIST AND WHITE LIST----------------------
```

Agora precisamos habilitar o amavis a utilizar o spamassassim e o clamav Vamos fazer um backup do arquivo de configuração

```
cp /etc/amavis/conf.d/15-content_filter_mode{,.bkp}
```

Agora vamos deixar ele como abaixo

```
vim /etc/amavis/conf.d/15-content_filter_mode
#/etc/amavis/conf.d/15-content_filter_mode
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:

#precisamos deixar as duas linhas abaixo descomentadas
@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:

#precisamos deixar as duas linhas abaixo descomentadas
@bypass_spam_checks_maps = (
   \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);

1;  # ensure a defined return
```

Vamos fazer backup do arquivo de configuração do postgrey

```
cp /etc/default/postgrey{,.bkp}
```

Agora vamos acertar a configuração do postgrey

```
vim /etc/default/postgrey
#/etc/default/postgrey
POSTGREY_OPTS="--inet=60000 --delay=60"
POSTGREY_TEXT="Seu email sera entregue em aproximadamente 60 segundos."
```

Agora vamos fazer alguns ajustes na configuração do MySQL.

```
vim /etc/mysql/my.cnf
[...]
```

```
key_buffer              = 32M
max_allowed_packet      = 32M
[...]
query_cache_limit       = 4M
query_cache_size        = 32M
[...]
```

Agora precisamos reiniciar o serviço do MySQL

```
systemctl restart mysql
```

Restartando os serviços:

```
systemctl restart clamav-daemon
systemctl restart clamav-freshclam
systemctl restart spamassassin
systemctl restart postgrey
systemctl restart amavis
systemctl restart postfix
systemctl restart dovecot
```

Caso tenha utilizado o courier

```
systemctl restart clamav-daemon
systemctl restart clamav-freshclam
systemctl restart spamassassin
systemctl restart postgrey
systemctl restart amavis
systemctl restart postfix
systemctl restart courier-authdaemon
systemctl restart courier-imap
systemctl restart courier-imap-ssl
systemctl restart courier-pop
systemctl restart courier-pop-ssl
```

Verificando se os serviços estão sendo executados:

```
nmap -sS -T4 localhost

Starting Nmap 6.47 ( http://nmap.org ) at 2016-01-30 20:26 BRST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000090s latency).
Other addresses for localhost (not scanned): 127.0.0.1
Not shown: 987 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
```

```
143/tcp   open  imap
587/tcp   open  submission
783/tcp   open  spamassassin
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
10024/tcp open  unknown
10025/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
```

Agora já podemos testar o nosso servidor de email Acesse o postfixadmin

- Em Virtual/Criar conta de email
- Informe o nome da conta ex: douglas
- Selecione o domínio ex: douglasqsantos.com.br
- Informe uma senha e confirme ela
- Informe um nome para a conta de email
- Agora selecione Criar conta de email

Agora nos logs do servidor de email vamos ter algo como abaixo

```
tail -f /var/log/mail.log
Jan 30 20:41:15 mail postfix/smtpd[26966]: connect from localhost[::1]
Jan 30 20:41:15 mail postfix/smtpd[26966]: 22CD32085F: client=localhost[::1]
Jan 30 20:41:15 mail postfix/cleanup[26967]: 22CD32085F: message-
id=<20160130224115.22CD32085F@mail.douglasqsantos.com.br>
Jan 30 20:41:15 mail postfix/qmgr[26734]: 22CD32085F:
from=<admin@douglasqsantos.com.br>, size=465, nrcpt=1 (queue active)
Jan 30 20:41:15 mail postfix/smtpd[26966]: disconnect from localhost[::1]
Jan 30 20:41:16 mail postfix/smtpd[26818]: 39EF220863:
client=localhost[127.0.0.1]
Jan 30 20:41:16 mail postfix/cleanup[26967]: 39EF220863: message-
id=<20160130224115.22CD32085F@mail.douglasqsantos.com.br>
Jan 30 20:41:16 mail postfix/qmgr[26734]: 39EF220863:
from=<admin@douglasqsantos.com.br>, size=899, nrcpt=1 (queue active)
Jan 30 20:41:16 mail postfix/smtpd[26818]: disconnect from
localhost[127.0.0.1]
Jan 30 20:41:16 mail amavis[26468]: (26468-02) Passed CLEAN
{RelayedOutbound}, LOCAL [::1]:52367 <admin@douglasqsantos.com.br> ->
<douglas@douglasqsantos.com.br>, Queue-ID: 22CD32085F, Message-ID:
<20160130224115.22CD32085F@mail.douglasqsantos.com.br>, mail_id:
aOSeu7mn5lhC, Hits: -1, size: 465, queued_as: 39EF220863, 1072 ms
Jan 30 20:41:16 mail postfix/smtp[26968]: 22CD32085F:
to=<douglas@douglasqsantos.com.br>, relay=127.0.0.1[127.0.0.1]:10024,
delay=1.1, delays=0.02/0.03/0/1.1, dsn=2.0.0, status=sent (250 2.0.0 from
MTA(smtp:[127.0.0.1]:10025): 250 2.0.0 Ok: queued as 39EF220863)
Jan 30 20:41:16 mail postfix/qmgr[26734]: 22CD32085F: removed
Jan 30 20:41:16 mail postfix/virtual[26972]: 39EF220863:
to=<douglas@douglasqsantos.com.br>, relay=virtual, delay=0.04,
```

```
delays=0.01/0.02/0/0.02, dsn=2.0.0, status=sent (delivered to maildir)
Jan 30 20:41:16 mail postfix/qmgr[26734]: 39EF220863: removed
```

Agora vamos testar a autenticação do Cliente.

```
testsaslauthd -u douglas@douglasqsantos.com.br -p doug123
0: OK "Success."
```

Vamos fazer um teste para verificar se o smtp esta funcionando

```
telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.douglasqsantos.com.br ESMTP
ehlo mail.douglasqsantos.com.br
250-mail.douglasqsantos.com.br
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
starttls
220 2.0.0 Ready to start TLS
quit
quit
Connection closed by foreign host.
```

Agora vamos fazer um teste de envio de email utilizando smtp + tls

Vamos criar um script para gerar o nosso usuário e senha em base64

```
vim /srv/base64
#!/usr/bin/env ruby
# encoding: UTF-8
require 'base64'

result = nil
until result == "quit"
  print "Insira a string ou digite quit para sair: "
  result = gets.chomp.strip

  unless result == "quit"
   puts "Base64 enconde é: " + Base64.encode64("#{result}").to_s
  end
```

```
end
```

Agora precisamos dar a permissão para o nosso script

```
chmod +x /srv/base64
```

Vamos gerar o usuário e a senha em base64 que o postfix utiliza para validar o usuário e senha

```
/srv/base64
Insira a string ou digite quit para sair:  douglas@douglasqsantos.com.br
Base64 encode é : ZG91Z2xhc0BtY3EuY29tLmJy
Insira a string ou digite quit para sair:  doug123
Base64 encode é : ZG91ZzEyMw==
Insira a string ou digite quit para sair:  quit
```

```
openssl s_client -starttls smtp -crlf -connect localhost:25 -quiet
depth=0
/C=BR/ST=Parana/L=Curitiba/O=DOUGLAS/OU=TI/CN=mail.douglasqsantos.com.br/ema
ilAddress=douglas@douglasqsantos.com.br
verify error:num=18:self signed certificate
verify return:1
depth=0
/C=BR/ST=Parana/L=Curitiba/O=DOUGLAS/OU=TI/CN=mail.douglasqsantos.com.br/ema
ilAddress=douglas@douglasqsantos.com.br
verify return:1
250 DSN
EHLO mail.douglasqsantos.com.br
250-mail.douglasqsantos.com.br
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
auth login
334 VXNlcm5hbWU6
#A Linha abaixo é o codigo base64 que foi gerado para o usuário
douglas@douglasqsantos.com.br
ZG91Z2xhc0Bkb3VnbGFzLndpa2kuYnI=
334 UGFzc3dvcmQ6
#A linha abaixo é o codigo base64 que foi gerado para a senha doug123
ZG91ZzEyMw==
235 2.7.0 Authentication successful
mail from: <douglas@douglasqsantos.com.br>
250 2.1.0 Ok
rcpt to: <douglas@douglasqsantos.com.br>
250 2.1.5 Ok
```

```
data
354 End data with <CR><LF>.<CR><LF>
From: Douglas <douglas@douglasqsantos.com.br>
To: Douglas <douglas@douglasqsantos.com.br>
Subject: Teste de tls
Teste de Envio de email utilizando TLS
.
250 2.0.0 Ok: queued as 5C72411F4E
quit
221 2.0.0 Bye
```

Para somente visualizarmos o certificado do smtp podemos fazer da seguinte maneira

```
openssl s_client -starttls smtp -crlf -connect localhost:25 -showcerts
CONNECTED(00000003)
depth=0 C = BR, ST = Parana, L = Curitiba, O = DOUGLAS, OU = IT, CN =
mail.douglasqsantos.com.br, emailAddress = douglas@douglasqsantos.com.br
verify error:num=18:self signed certificate
verify return:1
depth=0 C = BR, ST = Parana, L = Curitiba, O = DOUGLAS, OU = IT, CN =
mail.douglasqsantos.com.br, emailAddress = douglas@douglasqsantos.com.br
verify return:1
---
Certificate chain
 0
s:/C=BR/ST=Parana/L=Curitiba/O=DOUGLAS/OU=IT/CN=mail.douglasqsantos.com.br/e
mailAddress=douglas@douglasqsantos.com.br
i:/C=BR/ST=Parana/L=Curitiba/O=DOUGLAS/OU=IT/CN=mail.douglasqsantos.com.br/e
mailAddress=douglas@douglasqsantos.com.br
-----BEGIN CERTIFICATE-----
MIICizCCAfQCCQC8OOw3WZt+BzANBgkqhkiG9w0BAQsFADCBiTELMAkGA1UEBhMC
QlIxDzANBgNVBAgMBlBhcmFuYTERMA8GA1UEBwwIQ3VyaXRpYmExDDAKBgNVBAoM
A01DUTELMAkGA1UECwwCSVQxGDAWBgNVBAMMD21haWwubWNxLmNvbS5icjEhMB8G
CSqGSIb3DQEJARYSZG91Z2xhc0BtY3EuY29tLmJyMB4XDTE2MDEzMDIwNTUxOVoX
DTI2MDEyNzIwNTUxOVowgYkxCzAJBgNVBAYTAkJSMQ8wDQYDVQQIDAZQYXJhbmEx
ETAPBgNVBAcMCEN1cml0aWJhMQwwCgYDVQQKDANNQ1ExCzAJBgNVBAsMAklUMRgw
FgYDVQQDDA9tYWlsLm1jcS5jb20uYnIxITAfBgkqhkiG9w0BCQEWEmRvdWdsYXNA
bWNxLmNvbS5icjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAs6tyMimHupZd
YNj0kopdaURHac+ZQ8jOth8WBW5R1r3aazwAT3AejAMzWIU9X0J0Vo0ci0EW12cK
Dc5fx0G8Ij7X69M80SnV2RiLyeHoqRjA48bG+5F/DeZez3k8U2lbXs/O+OLMHHeh
T6HL/ZoEhBTK5/KvNugf/0dh5N6UnBMCAwEAATANBgkqhkiG9w0BAQsFAAOBgQAt
QfFZQfNGyf7vyw6sfaLyhZvoTz6wP1k0hn3LAD2ynJ1e2Pduyn4OEThhgUa8xKB3
l0JkhPQMspB4IL7aL02ToqKbwOi/ERIiKkW1lfeazeA7V+ZxzLl2gTDLim4pHV7h
PE6EXgkEa53TWT+DJrR4pJX8wtZVBOhKzgCWI4x7bQ==
-----END CERTIFICATE-----
---
Server certificate
subject=/C=BR/ST=Parana/L=Curitiba/O=DOUGLAS/OU=IT/CN=mail.douglasqsantos.co
m.br/emailAddress=douglas@douglasqsantos.com.br
issuer=/C=BR/ST=Parana/L=Curitiba/O=DOUGLAS/OU=IT/CN=mail.douglasqsantos.com
.br/emailAddress=douglas@douglasqsantos.com.br
```

```
---
Acceptable client certificate CA names
/C=BR/ST=Parana/L=Curitiba/O=DOUGLAS/OU=IT/CN=mail.douglasqsantos.com.br/ema
ilAddress=douglas@douglasqsantos.com.br
---
SSL handshake has read 1609 bytes and written 468 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID:
C6B0455A970F6AF34E0561BE91439175F0ABED6D57AD9C21EC25ABEACFDD11B8
    Session-ID-ctx:
    Master-Key:
FB6056B94B25D0415DE8FCA7FB68A05EDFF227110EA3692731ACE25077C0D601863987786DF7
D078E84D4C6EA5273FE3
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - e0 f8 cc fe 52 28 7d 2f-62 21 2b 35 dc 67 fc d6
....R(}/b!+5.g..
    0010 - 1d d9 3e 05 e7 f0 70 59-b6 f6 dd 2c 7c 7c 3c 0f
..>...pY...,||<.
    0020 - e0 6c d3 d6 10 70 68 5e-b0 de 52 11 88 5f 28 0a
.l...ph^..R.._(.
    0030 - 56 a8 2b 38 5d 99 db 34-90 63 d3 30 19 b3 11 84
V.+8]..4.c.0....
    0040 - 22 29 da 81 8a 6b 40 26-67 83 0f 07 3f 3c 9b b0
").../k@&g...?<..
    0050 - 99 fd 45 34 79 21 1f b0-d2 c2 9f 9b d1 93 ad 5d
..E4y!.........]
    0060 - 8a d9 d8 6b 77 8c d9 06-a0 52 6c be e8 a5 b9 5b
...kw....Rl....[
    0070 - 78 3c fe a0 b3 fb e8 a9-bb 71 46 e8 ca a6 17 ba
x<.......qF.....
    0080 - a3 c6 e1 dd 52 79 4a 8e-39 6b f8 09 ea 35 fa 28
....RyJ.9k...5.(
    0090 - f7 77 92 f2 54 2b 3d 39-7c cb 72 57 ae 5c be d9
.w..T+=9|.rW.\..

    Start Time: 1454195231
    Timeout   : 300 (sec)
```

```
    Verify return code: 18 (self signed certificate)
---
250 DSN
quit
221 2.0.0 Bye
closed
```

Vamos fazer um teste de acesso pop

```
telnet localhost 110
Trying ::1...
Connected to localhost.
Escape character is '^]'.
+OK Hello there.
user douglas@douglasqsantos.com.br
+OK Password required.
pass doug123
+OK logged in.
list
+OK POP3 clients that break here, they violate STD53.
1 1017
2 1079
.
retr 2
+OK 1079 octets follow.
Return-Path: <douglas@douglasqsantos.com.br>
X-Original-To: douglas@douglasqsantos.com.br
Delivered-To: douglas@douglasqsantos.com.br
Received: from localhost (localhost [127.0.0.1])
  by mail.douglasqsantos.com.br (Postfix) with ESMTP id 81A4120863
  for <douglas@douglasqsantos.com.br>; Sat, 30 Jan 2016 21:05:48 -0200
(BRST)
X-Virus-Scanned: Debian amavisd-new at mail.douglasqsantos.com.br
Received: from mail.douglasqsantos.com.br ([127.0.0.1])
  by localhost (mail.douglasqsantos.com.br [127.0.0.1]) (amavisd-new, port
10024)
  with ESMTP id R8c-jhKlRquT for <douglas@douglasqsantos.com.br>;
  Sat, 30 Jan 2016 21:05:47 -0200 (BRST)
Received: from mail.douglasqsantos.com.br (localhost [127.0.0.1])
  (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
  (Client did not present a certificate)
  by mail.douglasqsantos.com.br (Postfix) with ESMTPSA id 730522085F
  for <douglas@douglasqsantos.com.br>; Sat, 30 Jan 2016 21:05:22 -0200
(BRST)
From: Douglas <douglas@douglasqsantos.com.br>
To: Douglas <douglas@douglasqsantos.com.br>
Subject: Teste de tls
Message-Id: <20160130230528.730522085F@mail.douglasqsantos.com.br>
Date: Sat, 30 Jan 2016 21:05:22 -0200 (BRST)

Teste de Envio de email utilizando TLS
```

```
.
quit
+OK Bye-bye.
Connection closed by foreign host.
```

Agora vamos efetuar um teste de pop com ssl

```
openssl s_client -connect localhost:995 -quiet
depth=0 C = BR, ST = PR, L = Curitiba, O = Douglas Pop Server, OU = Douglas
POP3 SSL key, CN = mail.douglasqsantos.com.br, emailAddress =
postmaster@douglasqsantos.com.br
verify error:num=18:self signed certificate
verify return:1
depth=0 C = BR, ST = PR, L = Curitiba, O = Douglas Pop Server, OU = Douglas
POP3 SSL key, CN = mail.douglasqsantos.com.br, emailAddress =
postmaster@douglasqsantos.com.br
verify return:1
+OK Hello there.
user douglas@douglasqsantos.com.br
+OK Password required.
pass doug123
+OK logged in.
list
+OK POP3 clients that break here, they violate STD53.
1 1017
2 1079
.
retr 1
+OK 1017 octets follow.
Return-Path: <admin@douglasqsantos.com.br>
X-Original-To: douglas@douglasqsantos.com.br
Delivered-To: douglas@douglasqsantos.com.br
Received: from localhost (localhost [127.0.0.1])
  by mail.douglasqsantos.com.br (Postfix) with ESMTP id 8B56E20863
  for <douglas@douglasqsantos.com.br>; Sat, 30 Jan 2016 20:32:49 -0200
(BRST)
X-Virus-Scanned: Debian amavisd-new at mail.douglasqsantos.com.br
Received: from mail.douglasqsantos.com.br ([127.0.0.1])
  by localhost (mail.douglasqsantos.com.br [127.0.0.1]) (amavisd-new, port
10024)
  with ESMTP id GmzU8IuRAdvP for <douglas@douglasqsantos.com.br>;
  Sat, 30 Jan 2016 20:32:34 -0200 (BRST)
Received: from mail (localhost [IPv6::1])
  by mail.douglasqsantos.com.br (Postfix) with ESMTP id 8F7BC2085F
  for <douglas@douglasqsantos.com.br>; Sat, 30 Jan 2016 20:32:34 -0200
(BRST)
To: douglas@douglasqsantos.com.br
From: admin@douglasqsantos.com.br
Subject: Bem-vindo(a)
MIME-Version: 1.0
```

```
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: 8bit
Message-Id: <20160130223234.8F7BC2085F@mail.douglasqsantos.com.br>
Date: Sat, 30 Jan 2016 20:32:34 -0200 (BRST)

Hi,

Welcome to your new account.
.
quit
+OK Bye-bye.
```

Agora vamos efetuar um teste com o Imap

```
telnet localhost 143
Trying ::1...
Connected to localhost.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT
THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION STARTTLS] Courier-IMAP
ready. Copyright 1998-2011 Double Precision, Inc.  See COPYING for
distribution information.
a login douglas@douglasqsantos.com.br doug123
a OK LOGIN Ok.
a list ""  "*"
* LIST (\Unmarked \HasNoChildren) "." "INBOX"
a OK LIST completed
a examine inbox
* FLAGS (\Draft \Answered \Flagged \Deleted \Seen \Recent)
* OK [PERMANENTFLAGS ()] No permanent flags permitted
* 2 EXISTS
* 2 RECENT
* OK [UIDVALIDITY 454196026] Ok
* OK [MYRIGHTS "acdilrsw"] ACL
a OK [READ-ONLY] Ok
a fetch 1 body[]
* 1 FETCH (BODY[] {1017}
Return-Path: <admin@douglasqsantos.com.br>
X-Original-To: douglas@douglasqsantos.com.br
Delivered-To: douglas@douglasqsantos.com.br
Received: from localhost (localhost [127.0.0.1])
  by mail.douglasqsantos.com.br (Postfix) with ESMTP id 8B56E20863
  for <douglas@douglasqsantos.com.br>; Sat, 30 Jan 2016 20:32:49 -0200
(BRST)
X-Virus-Scanned: Debian amavisd-new at mail.douglasqsantos.com.br
Received: from mail.douglasqsantos.com.br ([127.0.0.1])
  by localhost (mail.douglasqsantos.com.br [127.0.0.1]) (amavisd-new, port
10024)
  with ESMTP id GmzU8IuRAdvP for <douglas@douglasqsantos.com.br>;
  Sat, 30 Jan 2016 20:32:34 -0200 (BRST)
Received: from mail (localhost [IPv6::1])
```

```
  by mail.douglasqsantos.com.br (Postfix) with ESMTP id 8F7BC2085F
  for <douglas@douglasqsantos.com.br>; Sat, 30 Jan 2016 20:32:34 -0200
(BRST)
To: douglas@douglasqsantos.com.br
From: admin@douglasqsantos.com.br
Subject: Bem-vindo(a)
MIME-Version: 1.0
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: 8bit
Message-Id: <20160130223234.8F7BC2085F@mail.douglasqsantos.com.br>
Date: Sat, 30 Jan 2016 20:32:34 -0200 (BRST)

Hi,

Welcome to your new account.
)
a OK FETCH completed.
a logout
* BYE Courier-IMAP server shutting down
a OK LOGOUT completed
Connection closed by foreign host.
```

Agora vamos efetuar um teste do imap com ssl

```
openssl s_client -connect localhost:993 -quiet
depth=0 C = BR, ST = PR, L = Curitiba, O = Douglas Imap Server, OU = Douglas
IMAP SSL key, CN = mail.douglasqsantos.com.br, emailAddress =
postmaster@douglasqsantos.com.br
verify error:num=18:self signed certificate
verify return:1
depth=0 C = BR, ST = PR, L = Curitiba, O = Douglas Imap Server, OU = Douglas
IMAP SSL key, CN = mail.douglasqsantos.com.br, emailAddress =
postmaster@douglasqsantos.com.br
verify return:1
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT
THREAD=REFERENCES SORT QUOTA IDLE AUTH=PLAIN ACL ACL2=UNION] Courier-IMAP
ready. Copyright 1998-2011 Double Precision, Inc.  See COPYING for
distribution information.
a login douglas@douglasqsantos.com.br doug123
a OK LOGIN Ok.
a list "" "*"
* LIST (\Unmarked \HasNoChildren) "." "INBOX"
a OK LIST completed
a examine inbox
* FLAGS (\Draft \Answered \Flagged \Deleted \Seen \Recent)
* OK [PERMANENTFLAGS ()] No permanent flags permitted
* 2 EXISTS
* 2 RECENT
* OK [UIDVALIDITY 454196107] Ok
* OK [MYRIGHTS "acdilrsw"] ACL
```

```
a OK [READ-ONLY] Ok
a fetch 1 body[]
* 1 FETCH (BODY[] {1017}
Return-Path: <admin@douglasqsantos.com.br>
X-Original-To: douglas@douglasqsantos.com.br
Delivered-To: douglas@douglasqsantos.com.br
Received: from localhost (localhost [127.0.0.1])
  by mail.douglasqsantos.com.br (Postfix) with ESMTP id 8B56E20863
  for <douglas@douglasqsantos.com.br>; Sat, 30 Jan 2016 20:32:49 -0200
(BRST)
X-Virus-Scanned: Debian amavisd-new at mail.douglasqsantos.com.br
Received: from mail.douglasqsantos.com.br ([127.0.0.1])
  by localhost (mail.douglasqsantos.com.br [127.0.0.1]) (amavisd-new, port
10024)
  with ESMTP id GmzU8IuRAdvP for <douglas@douglasqsantos.com.br>;
  Sat, 30 Jan 2016 20:32:34 -0200 (BRST)
Received: from mail (localhost [IPv6:::1])
  by mail.douglasqsantos.com.br (Postfix) with ESMTP id 8F7BC2085F
  for <douglas@douglasqsantos.com.br>; Sat, 30 Jan 2016 20:32:34 -0200
(BRST)
To: douglas@douglasqsantos.com.br
From: admin@douglasqsantos.com.br
Subject: Bem-vindo(a)
MIME-Version: 1.0
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: 8bit
Message-Id: <20160130223234.8F7BC2085F@mail.douglasqsantos.com.br>
Date: Sat, 30 Jan 2016 20:32:34 -0200 (BRST)

Hi,

Welcome to your new account.
)
a OK FETCH completed.
a logout
* BYE Courier-IMAP server shutting down
a OK LOGOUT completed
```

Até aqui já temos o Postfix trabalhando corretamente porém vamos adicionar mais funcionalidades a ele ;) Agora vamos testar o envio de uma mensagem de SPAM

```
mail -s "TESTE" douglas@douglasqsantos.com.br < /usr/share/doc/spamc/sample-
spam.txt && tail -f /var/log/syslog
Jan 30 21:24:44 mail postfix/pickup[27180]: 1B23B20870: uid=0 from=<root>
Jan 30 21:24:44 mail postfix/cleanup[27730]: 1B23B20870: message-
id=<20160130232444.1B23B20870@mail.douglasqsantos.com.br>
Jan 30 21:24:44 mail postfix/qmgr[27181]: 1B23B20870:
from=<root@mail.douglasqsantos.com.br>, size=1116, nrcpt=1 (queue active)
Jan 30 21:24:45 mail amavis[27274]: (27274-03) Blocked SPAM
{NoBounceOpenRelay,Quarantined}, [127.0.0.1]
<root@mail.douglasqsantos.com.br> -> <douglas@douglasqsantos.com.br>,
```

```
quarantine: t/spam-te_b4qKNGzsO.gz, Message-ID:
<20160130232444.1B23B20870@mail.douglasqsantos.com.br>, mail_id:
te_b4qKNGzsO, Hits: 999.999, size: 1116, 1164 ms
Jan 30 21:24:45 mail postfix/smtp[27732]: 1B23B20870:
to=<douglas@douglasqsantos.com.br>, relay=127.0.0.1[127.0.0.1]:10024,
delay=1.2, delays=0.02/0/0/1.2, dsn=2.5.0, status=sent (250 2.5.0 Ok,
id=27274-03, DISCARD(bounce.suppressed))
Jan 30 21:24:45 mail postfix/qmgr[27181]: 1B23B20870: removed
```

Agora vamos fazer um teste de envio de uma mensagem não spam

```
cd /usr/share/doc/spamc/
gunzip sample-nonspam.txt.gz
```

Agora vamos enviar a mensagem de teste

```
mail -s "TESTE" douglas@douglasqsantos.com.br < sample-nonspam.txt && tail -
f /var/log/mail.log
Jan 30 21:25:34 mail postfix/pickup[27180]: E9DA920870: uid=0 from=<root>
Jan 30 21:25:34 mail postfix/cleanup[27730]: E9DA920870: message-
id=<20160130232534.E9DA920870@mail.douglasqsantos.com.br>
Jan 30 21:25:34 mail postfix/qmgr[27181]: E9DA920870:
from=<root@mail.douglasqsantos.com.br>, size=6932, nrcpt=1 (queue active)
Jan 30 21:25:49 mail postfix/smtpd[27762]: connect from localhost[127.0.0.1]
Jan 30 21:25:49 mail postfix/smtpd[27762]: 126772086C:
client=localhost[127.0.0.1]
Jan 30 21:25:49 mail postfix/cleanup[27730]: 126772086C: message-
id=<20160130232534.E9DA920870@mail.douglasqsantos.com.br>
Jan 30 21:25:49 mail postfix/qmgr[27181]: 126772086C:
from=<root@mail.douglasqsantos.com.br>, size=7374, nrcpt=1 (queue active)
Jan 30 21:25:49 mail postfix/smtpd[27762]: disconnect from
localhost[127.0.0.1]
Jan 30 21:25:49 mail amavis[27273]: (27273-03) Passed CLEAN
{RelayedOpenRelay}, [127.0.0.1] <root@mail.douglasqsantos.com.br> ->
<douglas@douglasqsantos.com.br>, Message-ID:
<20160130232534.E9DA920870@mail.douglasqsantos.com.br>, mail_id:
MVujYp3n5AEq, Hits: 0, size: 6932, queued_as: 126772086C, 14128 ms
Jan 30 21:25:49 mail postfix/smtp[27732]: E9DA920870:
to=<douglas@douglasqsantos.com.br>, relay=127.0.0.1[127.0.0.1]:10024,
delay=14, delays=0.02/0/0/14, dsn=2.0.0, status=sent (250 2.0.0 from
MTA(smtp:[127.0.0.1]:10025): 250 2.0.0 Ok: queued as 126772086C)
Jan 30 21:25:49 mail postfix/qmgr[27181]: E9DA920870: removed
Jan 30 21:25:49 mail postfix/virtual[27766]: 126772086C:
to=<douglas@douglasqsantos.com.br>, relay=virtual, delay=0.04,
delays=0.01/0.02/0/0.01, dsn=2.0.0, status=sent (delivered to maildir)
Jan 30 21:25:49 mail postfix/qmgr[27181]: 126772086C: removed
```

Agora vamos fazer um teste de envio de virus

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

```
> /tmp/arquivo.doc
```

Agora vamos enviar o arquivo

```
mail -s "Arquivo Doc" douglas@douglasqsantos.com.br < /tmp/arquivo.doc &&
tail -f /var/log/mail.log
Jan 30 21:26:19 mail postfix/pickup[27180]: 316C620870: uid=0 from=<root>
Jan 30 21:26:19 mail postfix/cleanup[27730]: 316C620870: message-
id=<20160130232619.316C620870@mail.douglasqsantos.com.br>
Jan 30 21:26:19 mail postfix/qmgr[27181]: 316C620870:
from=<root@mail.douglasqsantos.com.br>, size=367, nrcpt=1 (queue active)
Jan 30 21:26:19 mail postfix/smtpd[27762]: connect from localhost[127.0.0.1]
Jan 30 21:26:19 mail postfix/smtpd[27762]: 47C6D2086C:
client=localhost[127.0.0.1]
Jan 30 21:26:19 mail postfix/cleanup[27730]: 47C6D2086C: message-
id=<VA1WTHp1MbBdkQ@mail.douglasqsantos.com.br>
Jan 30 21:26:19 mail postfix/qmgr[27181]: 47C6D2086C:
from=<postmaster@mail.douglasqsantos.com.br>, size=2017, nrcpt=1 (queue
active)
Jan 30 21:26:19 mail postfix/smtpd[27762]: disconnect from
localhost[127.0.0.1]
Jan 30 21:26:19 mail amavis[27274]: (27274-04) Blocked INFECTED (Eicar-Test-
Signature) {DiscardedOpenRelay,Quarantined}, [127.0.0.1]
<root@mail.douglasqsantos.com.br> -> <douglas@douglasqsantos.com.br>,
quarantine: 1/virus-1WTHp1MbBdkQ, Message-ID:
<20160130232619.316C620870@mail.douglasqsantos.com.br>, mail_id:
1WTHp1MbBdkQ, Hits: -, size: 367, 109 ms
Jan 30 21:26:19 mail postfix/cleanup[27730]: 4E96D20872: message-
id=<VA1WTHp1MbBdkQ@mail.douglasqsantos.com.br>
Jan 30 21:26:19 mail postfix/smtp[27732]: 316C620870:
to=<douglas@douglasqsantos.com.br>, relay=127.0.0.1[127.0.0.1]:10024,
delay=0.13, delays=0.01/0/0/0.12, dsn=2.7.0, status=sent (250 2.7.0 Ok,
discarded, id=27274-04 - INFECTED: Eicar-Test-Signature)
Jan 30 21:26:19 mail postfix/qmgr[27181]: 316C620870: removed
Jan 30 21:26:19 mail postfix/qmgr[27181]: 4E96D20872:
from=<postmaster@mail.douglasqsantos.com.br>, size=2155, nrcpt=1 (queue
active)
Jan 30 21:26:19 mail postfix/local[27777]: 47C6D2086C:
to=<postmaster@mail.douglasqsantos.com.br>, relay=local, delay=0.04,
delays=0.01/0.01/0/0.02, dsn=2.0.0, status=sent (forwarded as 4E96D20872)
Jan 30 21:26:19 mail postfix/qmgr[27181]: 47C6D2086C: removed
Jan 30 21:26:19 mail postfix/virtual[27766]: 4E96D20872:
to=<douglas@douglasqsantos.com.br>,
orig_to=<postmaster@mail.douglasqsantos.com.br>, relay=virtual, delay=0.02,
delays=0.01/0/0/0, dsn=2.0.0, status=sent (delivered to maildir)
Jan 30 21:26:19 mail postfix/qmgr[27181]: 4E96D20872: removed
```

Os arquivos bloqueados vão ficar em **/var/lib/amavis/virusmails/**

Migrando as contas do Servidor Atual para o Novo Servidor com o ImapSync

Vamos obter o imapsync

```
cd /usr/src
git clone https://github.com/imapsync/imapsync.git
```

Vamos instalar as dependências do ImapSync

```
aptitude install  libmail-imapclient-perl libdigest-md5-file-perl libterm-readkey-perl \
 libio-socket-ssl-perl libfile-spec-perl libdigest-hmac-perl makepasswd libauthen-ntlm-perl \
 libio-tee-perl libtest-pod-perl libunicode-string-perl -y
```

Agora precisamos instalar uma dependencia via cpan

```
cpan -i Data::Uniqid
```

Agora vamos acessar o diretório do imapsync

```
cd /usr/src/imapsync
```

Agora precisamos criar um diretório de controle interno dele

```
mkdir dist
```

Agora vamos compilar ele

```
make
```

Agora vamos mandar instalar ele

```
make install clean
```

Agora vamos pegar por exemplo a conta do nerso para sincronizar

Vamos criar um arquivo contendo o usuário e senha do servidor de email atual e o usuário e senha do servidor novo, nós podemos ter um usuário por linha

```
vim /usr/src/users
nerso@douglasqsantos.com.br;senha1;nerso@douglasqsantos.com.br;senha2
douglas@douglasqsantos.com.br;senha1;douglas@douglasqsantos.com.br;senha2
```

O arquivo deve ser no seguinte formato:

```
usuário1;senha1;usuário2;senha2
```

Onde:

- **usuário1:** é o usuário do servidor atual que está sendo migrado
- **senha1:** é a senha do usuário atual que está sendo migrado
- **usuário2:** é o usuário do servidor novo que acabamos de montar
- **senha2:** é a senha do usuário do servidor novo que acabamos de montar

Nós vamos fazer o sincronismo de todas as contas que estiverem no arquivo /tmp/users

Agora vamos ao script de sincronismo

```
vim /usr/src/sincroniza.sh
#!/bin/bash
#----------------------------------------------------------------------------
# sincroniza.sh
#
# Site  : http://wiki.douglasqsantos.com.br
# Autor : Douglas Q. dos Santos <douglas.q.santos@gmail.com>
# Manutenção: Douglas Q. dos Santos <douglas.q.santos@gmail.com>
#
#----------------------------------------------------------------------------
# Efetua o sincronismo das caixas de mensagens entre servidor de email
#----------------------------------------------------------------------------
# Histórico:
#
# Versão 1:
# Data: 22/02/2011
# Descrição: Efetua o sincronismo das caizas de mensagens entre servidores
# de email utilizando o imapsync no Debian Squeeze
#
#----------------------------------------------------------------------------
#Licença: http://creativecommons.org/licenses/by-sa/3.0/legalcode
#
#----------------------------------------------------------------------------

#VARIAVEIS GLOBAIS UTILIZADAS NO SCIRPT
RED="\033[01;31m"
GREEN="\033[01;32m"
WHITE="\033[01;37m"
CLOSE="\033[m"
IMAPSYNC=$(which imapsync)
SERVER1="mail.douglasqsantos.com.br"
SERVER2="localhost"
LISTA="/usr/src/users"
LOGS="/var/log/sincroniza.log"


#FUNÇÃO PARA SINCRONIZAR AS MENSAGENS
_Sincronizar()
{
```

```
for END in $(cat ${LISTA});
do
#O ARQUIVO DEVE ESTAR SEPARADO POR ;
USER1=$(echo ${END} | cut -d ';' -f 1)
SENHA1=$(echo ${END} | cut -d ';' -f 2)
USER2=$(echo ${END} | cut -d ';' -f 3)
SENHA2=$(echo ${END} | cut -d ';' -f 4)
echo -e "${GREEN}SINCRONIZANDO A CONTA DE EMAIL ${RED}${USER1}${CLOSE}
${GREEN}DO SERVIDOR${CLOSE} ${RED}${SERVER1}${CLOSE} ${GREEN}PARA O
SERVIDOR${CLOSE} ${RED}${SERVER2}${CLOSE} ${CLOSE}"
sleep 2
${IMAPSYNC} --host1 ${SERVER1} --user1 ${USER1} --password1 ${SENHA1} --
host2 localhost --user2 ${USER2} --password2 ${SENHA2}
_Validar ${USER1}
done
}

#FUNÇÃO PARA VALIDAR SE A CONTA CONSEGUIU SER SINCRONIZADA
_Validar()
{
if [ $? -eq 0 ]; then
  echo -e "${GREEN}CONTA DE EMAIL ${RED}${1}${CLOSE} ${GREEN}SINCRONIZADA
COM SUCESSO ${CLOSE}"
else
      echo -e "${RED}FALHA AO SINCRONIZAR A CONTA DE EMAIL
${WHITE}${1}${CLOSE}${CLOSE}"
  #GERANDO LOGS DAS CONTAS QUE DERAO PROBLEMAS PARA SINCRONIZAR
      echo -e "FALHA AO SINCRONIZAR A CONTA DE EMAIL ${1} NA DATA: $(date)"
>> ${LOGS}
fi

}

_Sincronizar
```

Agora precisamos dar permissão para o nosso script

```
chmod +x /usr/src/sincroniza.sh
```

Agora é só mandar executar ele

```
/usr/src/sincroniza.sh
```

Quando acabar o sincronismo vamos ter algo como abaixo

```
Host2 Nb messages:             494 messages
Host2 Total size:        117416141 bytes (111.98 MiB)
Host2 Biggest message:     7830835 bytes (7.47 MiB)
Host2 Time spent:              0.7 seconds
++++ Statistics
```

```
Transfer started on               : Sun Jan 13 16:39:00 2013
Transfer ended on                 : Sun Jan 13 16:39:13 2013
Transfer time                     : 13.0 sec
Messages transferred              : 0
Messages skipped                  : 496
Messages found duplicate on host1 : 12
Messages found duplicate on host2 : 0
Messages void (noheader) on host1 : 0
Messages void (noheader) on host2 : 0
Messages deleted on host1         : 0
Messages deleted on host2         : 0
Total bytes transferred           : 0 (0.00 KiB)
Total bytes duplicate host1       : 383100 (374.12 KiB)
Total bytes duplicate host2       : 0 (0.00 KiB)
Total bytes skipped               : 117384026 (111.95 MiB)
Total bytes error                 : 0 (0.00 KiB)
Message rate                      : 0.0 messages/s
Average bandwidth rate            : 0.0 KiB/s
Reconnections to host1            : 0
Reconnections to host2            : 0
Memory consumption                : 82.4 MiB
Biggest message                   : 0 bytes
Initial difference host2 - host1  : -2 messages, -350985 bytes (-342.76 KiB)
Final   difference host2 - host1  : -2 messages, -350985 bytes (-342.76 KiB)
Detected 0 errors

This current imapsync is up to date
Homepage: http://imapsync.lamiral.info/
CONTA DE EMAIL nerso@douglasqsantos.com.br SINCRONIZADA COM SUCESSO
```

Caso alguma conta de problemas para sincronizar vamos ter o arquivo de log em **/var/log/sincroniza.log**

Instalando e configurando o RoundCubeMail

Vamos obter ele e desempacotar

```
mkdir /var/www/html/webmail
cd /var/www/html/webmail
wget -c
http://wiki.douglasqsantos.com.br/Downloads/mail/roundcubemail-1.1.4-complet
e.tar.gz
tar -xzvf roundcubemail-1.1.4-complete.tar.gz
rm -rf roundcubemail-1.1.4-complete.tar.gz
mv roundcubemail-1.1.4/* .
mv roundcubemail-1.1.4/.htaccess .
rm -rf roundcubemail-1.1.4
```

Agora vamos criar o diretório para armazenar os logs

```
mkdir -p /var/log/roundcube/logs
chown -R www-data:www-data /var/log/roundcube/logs
```

Agora vamos preparar o banco de dados para o webmail

```
mysql -u root -p
CREATE DATABASE roundcubemail;
GRANT ALL PRIVILEGES ON roundcubemail.* TO webmail@localhost IDENTIFIED BY
'senha';
flush privileges;
quit;
```

Vamos acertar as permissões do webmail

```
chown -R www-data:www-data /var/www/html/webmail
```

Vamos acertar o arquivo /etc/php5/fpm/php.ini

```
vim /etc/php5/fpm/php.ini
[...]
date.timezone = America/Sao_Paulo
```

Agora precisamos reiniciar o PHP

```
systemctl restart php5-fpm
```

Agora vamos acertar os arquivos de configuração, aqui o que pode ter modificações é somente o usuário e senha do banco de dados o resto deixe como está.

```
vim /var/www/html/webmail/config/config.inc.php
<?php

/* Local configuration for Roundcube Webmail */

// ----------------------------------
// SQL DATABASE
// ----------------------------------
// Database connection string (DSN) for read+write operations
// Format (compatible with PEAR MDB2):
db_provider://user:password@host/database
// Currently supported db_providers: mysql, pgsql, sqlite, mssql or sqlsrv
// For examples see
http://pear.php.net/manual/en/package.database.mdb2.intro-dsn.php
// NOTE: for SQLite use absolute path:
'sqlite:////full/path/to/sqlite.db?mode=0646'
$config['db_dsnw'] = 'mysql://webmail:senha@localhost/roundcubemail';

// skin name: folder from skins/
$config['skin'] = 'classic';
```

```
// ----------------------------------
// IMAP
// ----------------------------------
// The mail host chosen to perform the log-in.
// Leave blank to show a textbox at login, give a list of hosts
// to display a pulldown menu or set one host as string.
// To use SSL/TLS connection, enter hostname with prefix ssl:// or tls://
// Supported replacement variables:
// %n - hostname ($_SERVER['SERVER_NAME'])
// %t - hostname without the first part
// %d - domain (http hostname $_SERVER['HTTP_HOST'] without the first part)
// %s - domain name after the '@' from e-mail address provided at login
screen
// For example %n = mail.domain.tld, %t = domain.tld
// WARNING: After hostname change update of mail_host column in users table
is
//          required to match old user data records with the new host.
$config['default_host'] = 'ssl://mail.douglasqsantos.com.br';

// TCP port used for IMAP connections
$config['default_port'] = '993';

// IMAP socket context options
// See http://php.net/manual/en/context.ssl.php
// The example below enables server certificate validation
$config['imap_conn_options'] = array(
  'ssl'         => array(
     'verify_peer'  => false,
   ),
);

// ----------------------------------
// SMTP
// ----------------------------------
// SMTP server host (for sending mails).
// To use SSL/TLS connection, enter hostname with prefix ssl:// or tls://
// If left blank, the PHP mail() function is used
// Supported replacement variables:
// %h - user's IMAP hostname
// %n - hostname ($_SERVER['SERVER_NAME'])
// %t - hostname without the first part
// %d - domain (http hostname $_SERVER['HTTP_HOST'] without the first part)
// %z - IMAP domain (IMAP hostname without the first part)
// For example %n = mail.domain.tld, %t = domain.tld
$config['smtp_server'] = 'tls://mail.douglasqsantos.com.br';

// SMTP port (default is 25; use 587 for STARTTLS or 465 for the
// deprecated SSL over SMTP (aka SMTPS))
$config['smtp_port'] = 587;

// SMTP username (if required) if you use %u as the username Roundcube
```

```
// will use the current username for login
$config['smtp_user'] = '%u';

// SMTP password (if required) if you use %p as the password Roundcube
// will use the current user's password for login
$config['smtp_pass'] = '%p';

// SMTP socket context options
// See http://php.net/manual/en/context.ssl.php
// The example below enables server certificate validation, and
// requires 'smtp_timeout' to be non zero.
$config['smtp_conn_options'] = array(
  'ssl'         => array(
    'verify_peer'  => false,
   ),
);



// provide an URL where a user can get support for this Roundcube
installation
// PLEASE DO NOT LINK TO THE ROUNDCUBE.NET WEBSITE HERE!
$config['support_url'] = '';

// this key is used to encrypt the users imap password which is stored
// in the session record (and the client cookie if remember password is
enabled).
// please provide a string of exactly 24 chars.
$config['des_key'] = '644de9406dfe77b51770d620';

// ----------------------------------
// PLUGINS
// ----------------------------------
// List of active plugins (in plugins/ directory)
$config['plugins'] = array('emoticons', 'jqueryui', 'new_user_dialog',
'password');

// the default locale setting (leave empty for auto-detection)
// RFC1766 formatted language name like en_US, de_DE, de_CH, fr_FR, pt_BR
$config['language'] = 'pt_BR';

// store draft message is this mailbox
// leave blank if draft messages should not be stored
// NOTE: Use folder names with namespace prefix (INBOX. on Courier-IMAP)
$config['drafts_mbox'] = 'Drafts';

// store spam messages in this mailbox
// NOTE: Use folder names with namespace prefix (INBOX. on Courier-IMAP)
$config['junk_mbox'] = 'Spam';

// store sent message is this mailbox
```

```
// leave blank if sent messages should not be stored
// NOTE: Use folder names with namespace prefix (INBOX. on Courier-IMAP)
$config['sent_mbox'] = 'Sent';

// move messages to this folder when deleting them
// leave blank if they should be deleted directly
// NOTE: Use folder names with namespace prefix (INBOX. on Courier-IMAP)
$config['trash_mbox'] = 'Trash';

// automatically create the above listed default folders on first login
$config['create_default_folders'] = true;

// use this folder to store log files
// must be writeable for the user who runs PHP process (Apache user if
mod_php is being used)
// This is used by the 'file' log driver.
//$config['log_dir'] = RCUBE_INSTALL_PATH . 'logs/';
$config['log_dir'] = '/var/log/roundcube/';

// Log successful/failed logins to <log_dir>/userlogins or to syslog
$config['log_logins'] = true;
```

Agora vamos acertar o plugin do roundcubemail para que o usuário possa trocar a senha.

```
cd /var/www/html/webmail/plugins/password
cp config.inc.php.dist config.inc.php
```

Agora vamos acertar a configuração sobre qual tabela o webmail vai ter que atualizar no banco, e a query que vamos enviar para o banco para mandar atualizar a senha. Aqui o que pode mudar é o usuário e senha do banco de dados o resto deixe como está.

```
vim /var/www/html/webmail/plugins/password/config.inc.php
[...]
// SQL Driver options
// -------------------
// PEAR database DSN for performing the query. By default
// Roundcube DB settings are used.
$config['password_db_dsn'] = 'mysql://webmail:senha@localhost/mail';

// The SQL query used to change the password.
// The query can contain the following macros that will be expanded as
follows:
//      %p is replaced with the plaintext new password
//      %c is replaced with the crypt version of the new password, MD5 if
available
//         otherwise DES. More hash function can be enabled using the
password_crypt_hash
//         configuration parameter.
//      %D is replaced with the dovecotpw-crypted version of the new
password
//      %o is replaced with the password before the change
```

```
//      %n is replaced with the hashed version of the new password
//      %q is replaced with the hashed password before the change
//      %h is replaced with the imap host (from the session info)
//      %u is replaced with the username (from the session info)
//      %l is replaced with the local part of the username
//         (in case the username is an email address)
//      %d is replaced with the domain part of the username
//         (in case the username is an email address)
// Escaping of macros is handled by this module.
// Default: "SELECT update_passwd(%c, %u)"
$config['password_query'] = 'UPDATE mailbox SET password=%c,modified=NOW()
WHERE username=%u';
[...]
```

Agora precisamos dar permissão para o webmail atualizar a tabela mailbox do banco mail.

```
mysql -u root -p
GRANT SELECT,UPDATE on mail.mailbox to webmail@localhost IDENTIFIED BY
'senha';
FLUSH PRIVILEGES;
quit
```

Inicialize o banco

```
mysql -u root -p roundcubemail < /var/www/html/webmail/SQL/mysql.initial.sql
```

Removendo o instalador do Webmail:

```
rm -rf /var/www/html/webmail/installer
```

Nosso webmail já esta no ar para testar acesse http://ip_servidor/webmail informe o usuário e senha

Instalação e configuração do AfterLogicWebmail

Vamos obter ele e desempacotar

```
mkdir /var/www/html/webmail2
cd /var/www/html/webmail2
wget -c
http://wiki.douglasqsantos.com.br/Downloads/mail/afterlogicwebmail-01-2016.z
ip
unzip afterlogicwebmail-01-2016.zip
rm -rf changelog.txt readme.txt afterlogicwebmail-01-2016.zip
mv webmail/* .
rm -rf webmail
```

Agora vamos acertar as permissões do nosso webmail.

```
cd /var/www/html/webmail2
find . -type f -exec chmod 644 {} \;
find . -type d -exec chmod 755 {} \;
chown -R www-data:www-data /var/www/html/webmail2
```

Agora vamos preparar o banco de dados para o webmail

```
mysql -u root -p
CREATE DATABASE webmail2;
GRANT ALL PRIVILEGES ON webmail2.* TO webmail2@localhost IDENTIFIED BY
'senha';
flush privileges;
quit;
```

Agora vamos acessar pelo navegador a tela de configuração do webmail
http://ip_servidor/webmail2/install/

1. Nesta página inicial de instalação os requisitos devem estar todos em Verde, no final da página selecione Next.
2. Agora leia o termo de licença e selecione I Agree para continuar.
3. Agora aqui nesta tela temos que informar:
    1. **SQL login:** webmail2
    2. **SQL password:** senha
    3. **Database name:** webmail2
    4. **Host:** localhost
4. Agora selecione Test database, o resultado deve ser Connected successfully se os dados estiverem corretos.
5. Deixe selecionado **Create Database Tables**.
6. Agora selecione Next.
7. Agora precisamos informar a senha e confirmar para o nosso mailadm que vai poder gerenciar a configuração global do nosso webmail.
8. Agora selecione Next.
9. Agora vamos selecionar os protocolos que o nosso webmail vai utilizar, vou selecionar SMTP e IMAP4 em E-mail server host informe: mail.douglasqsantos.com.br
10. Agora selecione Test connection, caso tenha sucesso vai aparecer: SMTP connection to port 25 successful, sending outgoing e-mail over SMTP should work, IMAP connection to port 143 successful, checking and downloading incoming e-mail over IMAP should work.
11. Agora selecione Next.
12. Agora nós fomos redirecionados para uma página sobre a conclusão da nossa instalação. Volte a instalação do nosso webmail.
13. Agora selecione Exit

Agora precisamos excluir a pasta install do nosso webmail.

```
rm -rf /var/www/html/webmail2/install/
```

Agora vamos acertar a configuração global do nosso webmail em
http://ip_servidor/webmail2/adminpanel/ informe o usuário mailadm e a senha que você definiu para ele.

- Selecione a Parte seperior da tela Domains

- Agora selecione Default domain settings
- Agora do lado direito da tela temos a configuração geral do webmail
- Em Default Settings:
    - **Incoming mail:** mail.douglasqsantos.com.br **port:** 993 **Marcar** Use SSL
    - **Outgoing mail:** mail.douglasqsantos.com.br **port:** 587 **Marcar** Use SSL
- Em site name informe o nome para o seu Webmail
- Agora em skin selecione o Skin padrão para os seus usuários.
- Agora fica a sua escolha a opção allow users to access interface settings, que habilita o usuário a efetuar alterações na configuração do webmail.
- Agora em Language selecione: Portuguese-Brazil
- Agora em Timezone selecione: (GMT -03:00) Brasilia
- Agora em time format selecione: 13:00
- Agora em Date format selecione: DD/MM/YYYY
- Agora selecione Save no final da tela do lado direito.
    - Agora na guia Webmail vamos mudar Messages per page para 50.
    - Agora em Refresh every selecione: 1 minute
    - Agora selecione Save
- Selecione agora na parte superior da tela System.
- Aqui temos a configuração do nosso banco de dados caso necessite efetuar alguma alteração.
- Do lado esquerdo da tela temos o link Security aonde temos o nome do usuário que pode efetuar login no painel de controle e temos a opção de alterar a senha para ele.

O Webmail é bem simples de utilizar não vou entrar em detalhes, basta acessar http://ip_servidor/webmail2 e informar o usuário e senha que foi criado no postfixadmin.

Instalando o Fail2ban

O Fail2Ban é uma aplicação que analisa continuamente os ficheiros log e bloqueia os endereços Internet de onde originaram várias tentativas falhadas de acesso com senha inválida.

O Fail2Ban é extremamente eficaz na prevenção de ataques de força bruta e de negação de serviço (DoS).

Vamos instalar o fail2ban

```
aptitude install fail2ban ipset -y
```

Vamos fazer backup do arquivo de configuração

```
cp /etc/fail2ban/jail.conf{,.bkp}
```

Vamos acertar o arquivo de configuração do fail2ban

```
vim /etc/fail2ban/jail.conf
#/etc/fail2ban/jail.conf

#  O DEFAULT habilita a configuração global de opções. Elas podem ser
sobreescritas
# nas definições das jaulas que são as diretivas como [ssh]
```

```
[DEFAULT]

# Esta diretiva pode receber um endereço ip, uma mascara CIDR ou um endereço
DNS.
# EX: 192.168.254.110, 192.168.254.0/24, mail.douglasqsantos.com.br
# Varios endereços podem ser utilizados desde que sejam separados por espaço
ignoreip = 127.0.0.1/8 192.168.254.0/24 192.168.25.0/24

# Esta diretiva vai pegar um argumento para alvo e vai ignorar ex: <ip>
# e vai retornar true se o IP é para ser ignorado ou False caso contrário.
ignorecommand =

# Esta diretiva define o numero em segundos que um host vai ser banido
bantime  = 600

# Um host vai ser banido se tem a diretiva maxretry for definida durante o
ultimo findtime
findtime = 600

# Diretiva define quantas vezes é necessário a negação do serviço ou da
solicitação para que um host seja banido.
maxretry = 3

# Esta diretiva define o backend que vai ser utilizado para obter as
modificações dos arquivos
# Disponíveis "pyinotify", "gamin", "polling" e "auto"
# Esta configuração pode ser sobreposta na configuração das jaulas
# auto:      Esta opção vai tantar os seguintes backends, na seguinte ordem
#            pyinotify, gamin, polling.
backend = polling

# Está diretiva especifica se as jaulas devem confiar nos hostnames nos
logs,
# aviso quando a consulta de DNS reverso for efetuada, ou ignorar todos os
hostnames nos logs.
# yes:   Se um hostname for encontrado, uma consulta dns vai ser executada
para obter o endereço ip para ser banido
#
# warn:  Se um hostname for encontrado, uma consulta dns vai ser executada
para obter o endereço ip para ser banido,
#        mas ele vai ser logado como warning
#
# no:    Se um hostname for encontrado, ele não vai ser usado para banir
#        mas vai ser logado como info.
usedns = warn

# Esta diretiva especifica o endereço de email que vai receber os emails de
notificação sobre os hosts banidos
# O correto é criar um alias para o endereço de email
fail2ban@douglasqsantos.com.br com os endereços de email que devem receber
os alertas
```

```
destemail = fail2ban@douglasqsantos.com.br

# Esta diretiva define o nome do Remetente da mensagem.
sendername = Fail2Ban

# Esta diretiva define o remetente das mensagems.
sender = fail2ban@douglasqsantos.com.br

#
# Ações
#

# Esta diretiva define o tipo de ação que vai ser tomada para banir um host
(ex: iptables, iptables-new,
# iptables-multiport, shorewall, etc) É usado para definir as variaveis de
action_*
# Pode ser definido globalmente ou pode ser definido por jaula
banaction = iptables-multiport

# Esta diretiva define a ação de email. Desde a vesão 0.8.1 o fail2ban usa
sendmail
# MTA para o envio de emails. Altere os parametros para email se você quiser
converter para
# o padrão convencional 'mail'
mta = sendmail

# Esta diretiva define o protoloco padrão para ser monitorado
protocol = tcp

# Esta diretiva define a Chain que vai ser adiciona as regras do fail2ban
chain = INPUT

# Atalhos para as ações. Usado para definir as ações dos parametros

# A ação mai simples para ser utilizada: so banir
action_ = %(banaction)s[name=%(__name__)s, port="%(port)s",
protocol="%(protocol)s", chain="%(chain)s"]

# Banir e enviar um email com o whois para o destinatário de email
action_mw = %(banaction)s[name=%(__name__)s, port="%(port)s",
protocol="%(protocol)s", chain="%(chain)s"]
              %(mta)s-whois[name=%(__name__)s, dest="%(destemail)s",
protocol="%(protocol)s", chain="%(chain)s", sendername="%(sendername)s"]

# Banir e enviar um email com o whois e as linhas relevantes do log para o
detinatário de email.
action_mwl = %(banaction)s[name=%(__name__)s, port="%(port)s",
protocol="%(protocol)s", chain="%(chain)s"]
               %(mta)s-whois-lines[name=%(__name__)s, dest="%(destemail)s",
logpath=%(logpath)s, chain="%(chain)s", sendername="%(sendername)s"]
```

```
# Esta diretiva define a ação padrão.  Para alterar so troque o 'action'
com o valor escolhido dos atalhos
# (ex:  action_mw, action_mwl, etc), podemos definir por definição global ou
por jaula.
action = %(action_mwl)s

#
# Jaulas
#

# As próximas jaulas correspondem a configuração padrão do Fail2ban na
versão 0.6 nas qual é utilizado pelo Debian.
# Habilitando uma definição de jaula aqui incluido uma seção.
#
# [NOME_SECAO]
# enabled = true

# Jaula para o serviço de SSH
[ssh]
enabled  = true
port     = ssh
filter   = sshd
logpath  = /var/log/auth.log
maxretry = 6

# Jaula para o serviço de dropbear
[dropbear]
enabled  = false
port     = ssh
filter   = dropbear
logpath  = /var/log/auth.log
maxretry = 6

# Jaula para o pam generico. Tem que ser usado com ação para bloquear todas
as portas.
# Ações como: iptables-allports, shorewall
[pam-generic]
enabled  = true
filter   = pam-generic
port     = all
logpath  = /var/log/auth.log
action   = iptables-allports

# Jaula para o serviço de Xinetd
[xinetd-fail]
enabled   = false
filter    = xinetd-fail
port      = all
logpath   = /var/log/daemon.log

# Jaula para o serviço de ssh com tentativas de ddos
```

```
[ssh-ddos]
enabled  = true
port     = ssh
filter   = sshd-ddos
logpath  = /var/log/auth.log

# Jaula para o serviço de ssh. Aqui nós usamos blackhole routers para não
necessitar de nenhum
# recurso adicional de kernel para armazenar um grande volume de endereços
IP.
[ssh-route]
enabled = false
filter = sshd
action = route
logpath = /var/log/sshd.log
maxretry = 6

# Jaula para o serviço de ssh. Aqui nós usamos uma combinação de
Netfilter/Iptables e IPsets
# para armazenar um grande volume de ips banidos.
# IPset vem em duas versões. Veja ipset -V para ver qual versão utilizar.
# Necessita o pacote ipset e suporte no kernel.
[ssh-iptables-ipset4]
enabled  = false
port     = ssh
filter   = sshd
banaction = iptables-ipset-proto4
logpath  = /var/log/sshd.log
maxretry = 6

# Jaula para o serviço de ssh. Aqui nós usamos uma combinação de
Netfilter/Iptables e IPsets
# para armazenar um grande volume de ips banidos.
# IPset vem em duas versões. Veja ipset -V para ver qual versão utilizar.
# Necessita o pacote ipset e suporte no kernel.
[ssh-iptables-ipset6]
enabled  = false
port     = ssh
filter   = sshd
banaction = iptables-ipset-proto6
logpath  = /var/log/sshd.log
maxretry = 6

# Jaula padrão para o serviço do Apache
[apache]
enabled  = false
port     = http,https
filter   = apache-auth
logpath  = /var/log/apache*/*error.log
maxretry = 6
```

```
# Jaula padrão para o serviço do Apache-multiport
# A ação padrão agora é multiport, então o apache-multiport foi deixado
# para manter comtabilidade com versões anteriores (<0.7.6-2)
[apache-multiport]
enabled   = false
port      = http,https
filter    = apache-auth
logpath   = /var/log/apache*/*error.log
maxretry  = 6


# Jaula padrão para o serviço do Apache-nonscript
[apache-noscript]
enabled  = false
port     = http,https
filter   = apache-noscript
logpath  = /var/log/apache*/*error.log
maxretry = 6


# Jaula padrão para o serviço do Apache-overflows
[apache-overflows]
enabled  = false
port     = http,https
filter   = apache-overflows
logpath  = /var/log/apache*/*error.log
maxretry = 2


# Jaula padrão para o serviço do Apache-modsecurity
[apache-modsecurity]
enabled  = false
filter   = apache-modsecurity
port     = http,https
logpath  = /var/log/apache*/*error.log
maxretry = 2


# Jaula padrão para o serviço do Apache-nohome
[apache-nohome]
enabled  = false
filter   = apache-nohome
port     = http,https
logpath  = /var/log/apache*/*error.log
maxretry = 2

# Jaula padrão para o serviço do php-url-fopen
# Banir atacantes que tentam utilizar a funcionalidade PHP's URL-fopen()
# possando por variáveis GET/POST. Experimental, com mais de um ano
# de uso em ambientes de produção.
[php-url-fopen]
```

```
enabled = false
port    = http,https
filter  = php-url-fopen
logpath = /var/www/*/logs/access_log

# Jaula padrão para o serviço do lighttpd-fastcgi
# Uma simples jaula que trabalha com lighttpd
# Se você roda um servidor lighttpd, então provavélmente você irá
# encontrar estes tipos de mensagens no seu error_log
#   ALERT – tried to register forbidden variable ‘GLOBALS’
#   Variaveis GET atraves de ataque (attacker '1.2.3.4', file
'/var/www/default/htdocs/index.php')
[lighttpd-fastcgi]
enabled = false
port    = http,https
filter  = lighttpd-fastcgi
logpath = /var/log/lighttpd/error.log

# Mesma diretiva que acima pra o mod_auth
# Ele obtem as mensagem de erro de autenticação.
[lighttpd-auth]
enabled = false
port    = http,https
filter  = suhosin
logpath = /var/log/lighttpd/error.log

# Jaula padrão para o Ngixn com o modulo de autenticação
# Vai banir clientes por tentavas de login mal sucedidas.
[nginx-http-auth]
enabled = true
filter  = nginx-http-auth
port    = http,https
logpath = /var/log/nginx/*error.log



# Jaula padrão para o Ngixn com o modulo de nonscript
# Vai banir clientes que estão pesquisando por scripts no servidor para
# Execuar e explorar
[nginx-noscript]
enabled  = true
port     = http,https
filter   = nginx-noscript
logpath  = /var/log/nginx/*access.log

# Jaula padrão para o Ngixn com o modulo de badboots
# Vai banir requisições de bot maliciosos
[nginx-badbots]
enabled  = true
port     = http,https
filter   = nginx-badbots
```

```
logpath  = /var/log/nginx/*access.log
maxretry = 2

# Jaula padrão para o Ngixn com o modulo de nohome
# Vai banir requisições de tentava de acesso a diretório home de usuários
[nginx-nohome]
enabled  = true
port     = http,https
filter   = nginx-nohome
logpath  = /var/log/nginx/*access.log

# Jaula padrão para o Ngixn com o modulo de noproxy
# Vai banir requisições de tentava de uso do nginx como servidor proxy
aberto
[nginx-noproxy]
enabled  = true
port     = http,https
filter   = nginx-noproxy
logpath  = /var/log/nginx/*access.log
maxretry = 2

# Jaula para o serviço roundcube
[roundcube-auth]
enabled  = true
filter   = roundcube-auth
port     = http,https
logpath  = /var/log/roundcube/userlogins

# Jaula para o serviço sogo
[sogo-auth]
enabled  = false
filter   = sogo-auth
port     = http, https
# without proxy this would be:
# port    = 20000
logpath  = /var/log/sogo/sogo.log


#
# Servidores FTP
#
# Jaula para o serviço vsftpd
[vsftpd]
enabled  = false
port     = ftp,ftp-data,ftps,ftps-data
filter   = vsftpd
logpath  = /var/log/vsftpd.log
# logpath = /var/log/auth.log
# Se você quer depender das falhas de login nos logs da pam
#  as failregex vsftpd devem combinar ambos os formatos
maxretry = 6
```

```
# Jaula para o serviço vsftpd
[proftpd]
enabled  = false
port     = ftp,ftp-data,ftps,ftps-data
filter   = proftpd
logpath  = /var/log/proftpd/proftpd.log
maxretry = 6


# Jaula para o serviço pure-ftpd
[pure-ftpd]
enabled  = false
port     = ftp,ftp-data,ftps,ftps-data
filter   = pure-ftpd
logpath  = /var/log/syslog
maxretry = 6


# Jaula para o serviço wuftpd
[wuftpd]
enabled  = false
port     = ftp,ftp-data,ftps,ftps-data
filter   = wuftpd
logpath  = /var/log/syslog
maxretry = 6


#
# Servidores de EMail
#

# Jaula para o serviço postfix
[postfix]
enabled  = true
port     = smtp,ssmtp,submission
filter   = postfix
logpath  = /var/log/mail.log


# Jaula para o serviço couriersmtp
[couriersmtp]
enabled  = false
port     = smtp,ssmtp,submission
filter   = couriersmtp
logpath  = /var/log/mail.log


#
# Autenticação de servidores de email: podem user usados para: smtp,ftp,imap
servers, então
```

```
# todas as portas relevantes podem ser banidas

# Jaula para o serviço courierauth
[courierauth]
enabled  = true
port     = smtp,ssmtp,submission,imap2,imap3,imaps,pop3,pop3s
filter   = courierlogin
logpath  = /var/log/mail.log


# Jaula para o serviço sasl
[sasl]
enabled  = true
port     = smtp,ssmtp,submission,imap2,imap3,imaps,pop3,pop3s
filter   = postfix-sasl
# Você talvez possa considerar monitorar /var/log/mail.warn ao se você
# estiver rodando postfix pode prover as mesmas linhas de log que são de
tamanho menor
logpath  = /var/log/mail.log


# Jaula para o serviço dovecot
[dovecot]
enabled = true
port    = smtp,ssmtp,submission,imap2,imap3,imaps,pop3,pop3s
filter  = dovecot
logpath = /var/log/mail.log

# Parar logar tentavas de login efetuadas sem exito adicione as linhas
abaixo no seu arquivo /etc/my.cnf:
# log-error=/var/log/mysqld.log
# log-warning = 2
[mysqld-auth]
enabled  = false
filter   = mysqld-auth
port     = 3306
logpath  = /var/log/mysqld.log


# Servidores de DNS
# Estas jaulas bloqueiam ataques contra o servidor named (bind9). Por
padrão, os logs estão como desligados
# com a instalação do bind9. Você vai precisar de uma configuração como
abaixo.
#
# logging {
#     channel security-file {
#         file "/var/log/named-security.log" versions 3 size 30m;
#         severity dynamic;
#         print-time yes;
#     };
```

```
#     category security {
#         security-file;
#     };
# };
#
# no seu named.options.conf  para prover o log adequado

# !!! AVISO !!!
#   Desde que UDP é um protocolo connection-less, spoofing de IP  e imitação
#   ou ações inlegais é um meio simples demais. Assim habilitando este
filtro
#   Talvez vai prover uma maneira facil de implentar um Dos contra a vitima
escolhida.
#   Veja: http://nion.modprobe.de/blog/archives/690-fail2ban-+-dns-fail.html
#   Por favor não use está jaula a menos que você saiba o que esteja
fazendo.
#[named-refused-udp]
#
#enabled  = false
#port     = domain,953
#protocol = udp
#filter   = named-refused
#logpath  = /var/log/named-security.log

# Jaula para o serviço named-refused-tcp
[named-refused-tcp]
enabled  = false
port     = domain,953
protocol = tcp
filter   = named-refused
logpath  = /var/log/named-security.log


# Jaula para o serviço freeswitch
[freeswitch]
enabled  = false
filter   = freeswitch
logpath  = /var/log/freeswitch.log
maxretry = 10
action   = iptables-multiport[name=freeswitch-tcp,
port="5060,5061,5080,5081", protocol=tcp]
           iptables-multiport[name=freeswitch-udp,
port="5060,5061,5080,5081", protocol=udp]


# Jaula para o serviço ejabberd-auth
[ejabberd-auth]
enabled  = false
filter   = ejabberd-auth
port     = xmpp-client
```

```
protocol = tcp
logpath  = /var/log/ejabberd/ejabberd.log


# Jaula para o serviço asterisk-tcp
# Muliplas jaulas, 1 por protocolo, não necessárias ATM:
# Veja: https://github.com/fail2ban/fail2ban/issues/37
[asterisk-tcp]
enabled  = false
filter   = asterisk
port     = 5060,5061
protocol = tcp
logpath  = /var/log/asterisk/messages

# Jaula para o serviço asterisk-udp
[asterisk-udp]
enabled  = false
filter   = asterisk
port     = 5060,5061
protocol = udp
logpath  = /var/log/asterisk/messages


# Jaula para banir abusados persistentes
# !!! AVISO !!!
#   Certifique-se que seu nivel de log está definido em fail2ban.conf/.local
#   não é em nível de DEBUG -- Qual pode cause o fail2ban cair em loop
infinito
#   alimentando-o com linhas de informações inuteis.
[recidive]
enabled  = false
filter   = recidive
logpath  = /var/log/fail2ban.log
action   = iptables-allports[name=recidive]
           sendmail-whois-lines[name=recidive,
logpath=/var/log/fail2ban.log]
bantime  = 604800  ; 1 week
findtime = 86400   ; 1 day
maxretry = 5

# Veja a importa nota em action.d/blocklist_de.conf para quando for utilizar
está ação.
#
# Relatório de bloqueio via blocklist.de fail2ban API de relatório de
serviço.
# Veja em action.d/blocklist_de.conf para mais informações.
[ssh-blocklist]
enabled  = false
filter   = sshd
action   = iptables[name=SSH, port=ssh, protocol=tcp]
           sendmail-whois[name=SSH, dest="%(destemail)s",
```

```
sender="%(sender)s", sendername="%(sendername)s"]
           blocklist_de[email="%(sender)s", apikey="xxxxxx",
service="%(filter)s"]
logpath  = /var/log/sshd.log
maxretry = 20


# Considerar um baixo maxretry e um alto bantime
# Ninguém exceto o proprio servidor Naior devem utilizar o nrpe
[nagios]
enabled  = false
filter   = nagios
action   = iptables[name=Nagios, port=5666, protocol=tcp]
           sendmail-whois[name=Nagios, dest="%(destemail)s",
sender="%(sender)s", sendername="%(sendername)s"]
logpath  = /var/log/messages     ; nrpe.cfg may define a different
log_facility
maxretry = 1
```

Agora precisamos ajustar os filtros, vamos acessar o diretório dos filtros.

```
cd /etc/fail2ban/filter.d
```

Agora vamos ajustar os filtros

```
vim nginx-http-auth.conf
# fail2ban filter configuration for nginx


[Definition]


failregex = ^ \[error\] \d+#\d+: \*\d+ user "\S+":? (password mismatch|was
not found in ".*"), client: <HOST>, server: \S+, request: "\S+ \S+
HTTP/\d+\.\d+", host: "\S+"\s*$
            ^ \[error\] \d+#\d+: \*\d+ no user/password was provided for
basic authentication, client: <HOST>, server: \S+, request: "\S+ \S+
HTTP/\d+\.\d+", host: "\S+"\s*$


ignoreregex =

# DEV NOTES:
# Based on samples in https://github.com/fail2ban/fail2ban/pull/43/files
# Extensive search of all nginx auth failures not done yet.
#
# Author: Daniel Black
```

Agora vamos copiar o badbots do Apache para o Nginx

```
cp apache-badbots.conf nginx-badbots.conf
```

Agora precisamos criar o nginx-noscript.conf

```
vim nginx-noscript.conf
#/etc/fail2ban/filter.d/nginx-noscript.conf
[Definition]

failregex = ^<HOST> -.*GET.*(\.php|\.rb|\.erb|\.arb)

ignoreregex =
```

Agora precisamos criar o nginx-nohome.conf

```
vim nginx-nohome.conf
#/etc/fail2ban/filter.d/nginx-nohome.conf

[Definition]

failregex = ^<HOST> -.*GET .*/~.*

ignoreregex =
```

Agora precisamos criar o nginx-noproxy.conf

```
vim nginx-noproxy.conf
#/etc/fail2ban/filter.d/nginx-noproxy.conf

[Definition]

failregex = ^<HOST> -.*GET http.*

ignoreregex =
```

Agora é so reiniciar o serviço

```
systemctl restart fail2ban
```

Agora podemos consultar o status das jaulas

```
fail2ban-client status
Status
|- Number of jail:  13
`- Jail list:   courierauth, pam-generic, nginx-noscript, postfix, nginx-
nohome, nginx-badbots, ssh-ddos, roundcube-auth, ssh, sasl, dovecot, nginx-
http-auth, nginx-noproxy
```

Agora podemos consultar as regras de firewall e verificar que o fail2ban criou um framework para banir os clientes que acabarem caindo nas regras.

```
iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-N fail2ban-courierauth
-N fail2ban-default
-N fail2ban-dovecot
-N fail2ban-nginx-badbots
-N fail2ban-nginx-http-auth
-N fail2ban-nginx-nohome
-N fail2ban-nginx-noproxy
-N fail2ban-nginx-noscript
-N fail2ban-postfix
-N fail2ban-roundcube-auth
-N fail2ban-sasl
-N fail2ban-ssh
-N fail2ban-ssh-ddos
-A INPUT -p tcp -m multiport --dports 25,465,587,143,220,993,110,995 -j
fail2ban-dovecot
-A INPUT -p tcp -m multiport --dports 25,465,587,143,220,993,110,995 -j
fail2ban-sasl
-A INPUT -p tcp -m multiport --dports 25,465,587,143,220,993,110,995 -j
fail2ban-courierauth
-A INPUT -p tcp -m multiport --dports 80,443 -j fail2ban-nginx-badbots
-A INPUT -p tcp -m multiport --dports 25,465,587 -j fail2ban-postfix
-A INPUT -p tcp -m multiport --dports 80,443 -j fail2ban-roundcube-auth
-A INPUT -p tcp -m multiport --dports 80,443 -j fail2ban-nginx-noproxy
-A INPUT -p tcp -m multiport --dports 80,443 -j fail2ban-nginx-nohome
-A INPUT -p tcp -m multiport --dports 80,443 -j fail2ban-nginx-noscript
-A INPUT -p tcp -m multiport --dports 80,443 -j fail2ban-nginx-http-auth
-A INPUT -p tcp -m multiport --dports 22 -j fail2ban-ssh-ddos
-A INPUT -p tcp -j fail2ban-default
-A INPUT -p tcp -m multiport --dports 22 -j fail2ban-ssh
-A fail2ban-courierauth -j RETURN
-A fail2ban-default -j RETURN
-A fail2ban-dovecot -j RETURN
-A fail2ban-nginx-badbots -j RETURN
-A fail2ban-nginx-http-auth -j RETURN
-A fail2ban-nginx-nohome -j RETURN
-A fail2ban-nginx-noproxy -j RETURN
-A fail2ban-nginx-noscript -j RETURN
-A fail2ban-postfix -j RETURN
-A fail2ban-roundcube-auth -j RETURN
-A fail2ban-sasl -j RETURN
-A fail2ban-ssh -j RETURN
-A fail2ban-ssh-ddos -j RETURN
```

Para obter detalhes de uma jaula especifica podemos consultar da seguinte forma

```
fail2ban-client status nginx-http-auth
```

```
Status for the jail: nginx-http-auth
|- filter
|  |- File list:  /var/log/nginx/error.log
|  |- Currently failed: 0
|  `- Total failed: 0
`- action
   |- Currently banned: 0
   |  `- IP list:
   `- Total banned: 0
```

Podemos efetuar testes contra o nginx-http-auth errando o usuário e senha para chegarmos no que precisamos e bloquear um determinado ip

```
fail2ban-client status nginx-http-auth
Status for the jail: nginx-http-auth
|- filter
|  |- File list:        /var/log/nginx/error.log
|  |- Currently failed: 0
|  `- Total failed:     12
`- action
   |- Currently banned: 1
   |  `- IP list:       111.111.111.111
   `- Total banned:     1
```

Após ter certeza que está tudo ok podemos liberar o ip novamente

```
fail2ban-client set nginx-http-auth unbanip 111.111.111.111
```

Instação e configuração do Knock

Agora vamos instalar o knockd para fazer o controle da porta do ssh

- “O knockd é uma implementação de port-knocking. Resumidamente falando, com ele podemos deixar todas as portas do servidor fechadas e tê-lo configurado para ouvir “batidas” em algumas portas específicas, sendo que as batidas (corretas) podem gerar a execução de uma regra de firewall para abrir uma porta ou executar qualquer outro comando.”

Vamos fazer a instalação do knock

```
aptitude install knockd -y
```

Agora vamos fazer backup do arquivo

```
cp /etc/default/knockd{,.bkp}
```

Vamos editar o arquivo e liberar para qual interface ele vai ficar escutando

```
vim /etc/default/knockd
#/etc/default/knockd
```

```
##################################################
#
# knockd's default file, for generic sys config
#
##################################################

# control if we start knockd at init or not
# 1 = start
# anything else = don't start
#
# PLEASE EDIT /etc/knockd.conf BEFORE ENABLING
START_KNOCKD=1

# command line options
KNOCKD_OPTS="-i eth0"
```

Vamos fazer backup do arquivo de configuração

```
cp /etc/knockd.conf{,.bkp}
```

Vamos ao arquivo de configuração

```
vim /etc/knockd.conf
[options]
        UseSyslog
        LogFile = /var/log/knockd.log
[openSSH]
        sequence    = 1234:udp,4321:tcp,6789:udp
        seq_timeout = 5
        command     = /sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j
ACCEPT
        tcpflags    = syn

[closeSSH]
        sequence    = 6789:tcp,4321:udp,1234:tcp
        seq_timeout = 5
        command     = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j
ACCEPT
        tcpflags    = syn
```

Vamos restartar o serviço:

```
systemctl restart knockd
```

Agora no cliente é so instalar o pacote do knockd

```
apt-get install knockd -y
```

Agora para abrir a porta do servidor para o nosso cliente fazemos como abaixo

```
knock ip_servidor     1234:udp 4321:tcp 6789:udp
```

Agora vamos ver o log no servidor

```
tail -f /var/log/knockd.log
[2016-01-31 04:51] starting up, listening on eth0
[2016-01-31 04:52] 192.168.25.2: openSSH: Stage 1
[2016-01-31 04:52] 192.168.25.2: openSSH: Stage 2
[2016-01-31 04:52] 192.168.25.2: openSSH: Stage 3
[2016-01-31 04:52] 192.168.25.2: openSSH: OPEN SESAME
[2016-01-31 04:52] openSSH: running command: /sbin/iptables -A INPUT -s
192.168.25.2 -p tcp --dport 22 -j ACCEPT
```

A porta foi aberta vamos analizar no firewall

```
iptables -L -n -v | egrep 22
 1096  136K fail2ban-dovecot  tcp  --  *      *       0.0.0.0/0
0.0.0.0/0           multiport dports 25,465,587,143,220,993,110,995
 1096  136K fail2ban-sasl  tcp  --  *      *       0.0.0.0/0
0.0.0.0/0           multiport dports 25,465,587,143,220,993,110,995
 1096  136K fail2ban-courierauth  tcp  --  *      *       0.0.0.0/0
0.0.0.0/0           multiport dports 25,465,587,143,220,993,110,995
 3649  244K fail2ban-ssh-ddos  tcp  --  *      *       0.0.0.0/0
0.0.0.0/0           multiport dports 22
 3652  244K fail2ban-ssh  tcp  --  *      *       0.0.0.0/0
0.0.0.0/0           multiport dports 22
   13   960 ACCEPT     tcp  --  *      *       192.168.25.2
0.0.0.0/0           tcp dpt:22
```

- Como pode ser notado foi aberta a porta 22 somente para o cliente 10.0.0.20

Para fechar a porta é a sequencia do closeSSH

```
knock ip_servidor 6789:tcp 4321:udp 1234:tcp
```

Agora vamos ver nos logs para ver se fechou a porta

```
tail -f /var/log/knockd.log
[2016-01-31 04:53] 192.168.25.2: closeSSH: Stage 1
[2016-01-31 04:53] 192.168.25.2: closeSSH: Stage 2
[2016-01-31 04:53] 192.168.25.2: closeSSH: Stage 3
[2016-01-31 04:53] 192.168.25.2: closeSSH: OPEN SESAME
[2016-01-31 04:53] closeSSH: running command: /sbin/iptables -D INPUT -s
192.168.25.2 -p tcp --dport 22 -j ACCEPT
```

Habilitando os VirtualHosts com https

Vamos gerar a key para o https

Preparando o diretório que vai armazenar os nosso certificados

```
mkdir /etc/nginx/ssl
cd /etc/nginx/ssl
```

Gerando a key

```
openssl genrsa -des3 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
.............................++++++
.++++++
e is 65537 (0x10001)
Enter pass phrase for server.key: #senha
Verifying - Enter pass phrase for server.key: #senha
```

Vamos gerar agora a requisição de assinatura para o certificado

```
openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:Parana
Locality Name (eg, city) []:Curitiba
Organization Name (eg, company) [Internet Widgits Pty Ltd]:DOUGLAS
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:*.douglasqsantos.com.br
Email Address []:douglas@douglasqsantos.com.br

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:DOUGLAS
```

Agora vamos auto assinar o nosso certificado

```
openssl x509 -req -days 3650 -in server.csr -signkey server.key -out
server.crt
Signature ok
subject=/C=BR/ST=Parana/L=Curitiba/O=DOUGLAS/OU=IT/CN=*.douglasqsantos.com.b
r/emailAddress=douglas@douglasqsantos.com.br
Getting Private key
Enter pass phrase for server.key:
```

Agora vamos acertar as permissões das chaves

```
chmod 0400 server.*
 cp server.key server.key.orig
```

Agora vamos tirar a senha do certificado assinado para que o apache não fique pedindo senha a cada vez que for inicializar

```
openssl rsa -in server.key.orig -out server.key
 Enter pass phrase for server.key.orig: senha
 writing RSA key
```

Vamos acertar as permissões de todas as chaves

```
chmod 0400 /etc/nginx/ssl/*
```

Vamos agora configurar o host virtual com o acesso via http e https para o nosso postfixadmin.

OBS:. Não esqueça de inserir uma entrada no servidor DNS para resolver o seu endereço http://postfixadmin.douglasqsantos.com.br para o ip do servidor.

Você também pode testar editando o arquivo /etc/hosts do cliente que vai acessar da seguinte formar

```
vim /etc/hosts
[...]
ip_servidor  postfixadmin.douglasqsantos.com.br mailadmin
ip_servidor  webmail.douglasqsantos.com.br webmail
ip_servidor  isoqlog.douglasqsantos.com.br isoqlog
ip_servidor  monitor.douglasqsantos.com.br monitor
```

Os endereços configurados acima são para não precisar configurar o servidor de dns para resolver os nomes com isso da para efetuar os testes necessários.

Nota: Se for utilizar o Google Chrome não esqueça de utilizar o http: *ou https:* antes do nome do domínio caso contrário você vai obter erros.

Aqui vamos ter duas opções de acesso via http ou https as duas vão estar disponíveis dai fica a seu critério escolher é o que é melhor pra o seu uso.

```
vim /etc/nginx/sites-available/postfixadmin.douglasqsantos.com.br
#/etc/nginx/sites-available/postfixadmin.douglasqsantos.com.br
## Configurações para o virtualhost.
server {
      ## Define a porta que o servidor está escutando.
      listen 80;
      ## Define o nome do virtual host.
      server_name postfixadmin.douglasqsantos.com.br;
      ## Remove a versão do campo Server no cabeçalho da resposta do server.
      server_tokens off;

      ## Configurações de Log.
      access_log /var/log/nginx/postfixadmin.douglasqsantos.com.br-
access.log combined;
```

```
      error_log /var/log/nginx/postfixadmin.douglasqsantos.com.br-error.log;
      ## Diretório raiz do website.
      root /var/www/html/postfixadmin;
      ## A configuração depende da requisição URI.
      location / {
        ## Checa os arquivos e se existirem são processador na ordem
especifica abaixo.
        try_files $uri $uri/ =404;
      }

      ## Definição dos arquivos de Index
      index index.php index.htm index.html;
      ## Configuração para arquivos php.
      location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/var/run/php5-fpm.sock;
     }
}

## Configurações para o virtualhost.
server {
      ## Define a porta que o servidor está escutando.
      listen 443;
      ## Habilita o protocolo https para este virtual host.
      ssl on;
      ## Define o caminho para o arquivo crt.
      # Caso o arquivo não seja auto assinado temos que contenar os arquivos
ca e crt do server.
      # cat server_name.crt CertCA.crt >> server.crt
      ssl_certificate /etc/nginx/ssl/server.crt;
      ## Define o caminho que contem o certificado key para o servidor.
      ssl_certificate_key /etc/nginx/ssl/server.key;
      ## Define os ciphers disponíveis.
      ssl_protocols SSLv3 TLSv1 TLSv1.1 TLSv1.2;

      ## Define que os ciphers do servidor devem ter preferencia sobre os
dos clientes quenao utilizado o SSLv3 e protocolos TLS.
      ssl_prefer_server_ciphers on;

      ## Define os ciphers habilitados.
      ssl_ciphers HIGH:!aNULL:!MD5;

      ## Sets names of a virtual server
      server_name postfixadmin.douglasqsantos.com.br;
      ## Remove a versão do campo Server no cabeçalho da resposta do server.
      server_tokens off;

      ## Configurações de Log.
      access_log /var/log/nginx/postfixadmin.douglasqsantos.com.br-
ssl.access.log combined;
```

```
      error_log /var/log/nginx/postfixadmin.douglasqsantos.com.br-
ssl.error.log;
      ## Diretório raiz do website.
      root /var/www/html/postfixadmin;
      ## A configuração depende da requisição URI.
      location / {
        ## Checa os arquivos e se existirem são processador na ordem
especifica abaixo.
        try_files $uri $uri/ =404;
      }

      ## Definição dos arquivos de Index
      index index.php index.htm index.html;
      ## Configuração para arquivos php.
      location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/var/run/php5-fpm.sock;
     }
}
```

Vamos acertar as permissões do diretório

```
chown -R www-data:www-data /var/www/html/postfixadmin/
```

Agora vamos desativar o virtual host padrão

```
unlink /etc/nginx/sites-enabled/default
```

Vamos ativar o nosso virtual host para o postfixadmin

```
ln -s /etc/nginx/sites-available/postfixadmin.douglasqsantos.com.br
/etc/nginx/sites-enabled/postfixadmin.douglasqsantos.com.br
```

Agora vamos reiniciar o Nginx para testar

```
systemctl restart nginx
```

Agora já podemos testar acessando:

- http://postfixadmin.douglasqsantos.com.br
- https://postfixadmin.douglasqsantos.com.br

Agora vamos criar o virtual host para o webmail

```
vim /etc/nginx/sites-available/webmail.douglasqsantos.com.br
#/etc/nginx/sites-available/webmail.douglasqsantos.com.br
## Configurações para o virtualhost.
server {
      ## Define a porta que o servidor está escutando.
      listen 80;
      ## Define o nome do virtual host.
```

```
      server_name webmail.douglasqsantos.com.br;
      ## Remove a versão do campo Server no cabeçalho da resposta do server.
      server_tokens off;

      ## Configurações de Log.
      access_log /var/log/nginx/webmail.douglasqsantos.com.br-access.log
combined;
      error_log /var/log/nginx/webmail.douglasqsantos.com.br-error.log;
      ## Diretório raiz do website.
      root /var/www/html/webmail;
      ## A configuração depende da requisição URI.
      location / {
        ## Checa os arquivos e se existirem são processador na ordem
especifica abaixo.
        try_files $uri $uri/ =404;
      }

      ## Definição dos arquivos de Index
      index index.php index.htm index.html;
      ## Configuração para arquivos php.
      location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/var/run/php5-fpm.sock;
     }
}

## Configurações para o virtualhost.
server {
      ## Define a porta que o servidor está escutando.
      listen 443;
      ## Habilita o protocolo https para este virtual host.
      ssl on;
      ## Define o caminho para o arquivo crt.
      # Caso o arquivo não seja auto assinado temos que contenar os arquivos
ca e crt do server.
      # cat server_name.crt CertCA.crt >> server.crt
      ssl_certificate /etc/nginx/ssl/server.crt;
      ## Define o caminho que contem o certificado key para o servidor.
      ssl_certificate_key /etc/nginx/ssl/server.key;
      ## Define os ciphers disponíveis.
      ssl_protocols SSLv3 TLSv1 TLSv1.1 TLSv1.2;

      ## Define que os ciphers do servidor devem ter preferencia sobre os
dos clientes quenao utilizado o SSLv3 e protocolos TLS.
      ssl_prefer_server_ciphers on;

      ## Define os ciphers habilitados.
      ssl_ciphers HIGH:!aNULL:!MD5;

      ## Sets names of a virtual server
```

```
      server_name webmail.douglasqsantos.com.br;
      ## Remove a versão do campo Server no cabeçalho da resposta do server.
      server_tokens off;

      ## Configurações de Log.
      access_log /var/log/nginx/webmail.douglasqsantos.com.br-ssl.access.log
combined;
      error_log /var/log/nginx/webmail.douglasqsantos.com.br-ssl.error.log;
      ## Diretório raiz do website.
      root /var/www/html/webmail;
      ## A configuração depende da requisição URI.
      location / {
        ## Checa os arquivos e se existirem são processador na ordem
especifica abaixo.
        try_files $uri $uri/ =404;
      }

      ## Definição dos arquivos de Index
      index index.php index.htm index.html;
      ## Configuração para arquivos php.
      location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/var/run/php5-fpm.sock;
     }
}
```

Vamos ativar o nosso virtual host para o webmail

```
ln -s /etc/nginx/sites-available/webmail.douglasqsantos.com.br
/etc/nginx/sites-enabled/webmail.douglasqsantos.com.br
```

Agora vamos recarregar as configurações para o Nginx para testar

```
systemctl force-reload nginx
```

Agora já podemos testar acessando:

- http://webmail.douglasqsantos.com.br
- https://webmail.douglasqsantos.com.br

Agora vamos criar o virtual host para o webmail

```
vim /etc/nginx/sites-available/webmail2.douglasqsantos.com.br
#/etc/nginx/sites-available/webmail2.douglasqsantos.com.br
## Configurações para o virtualhost.
server {
      ## Define a porta que o servidor está escutando.
      listen 80;
      ## Define o nome do virtual host.
      server_name webmail2.douglasqsantos.com.br;
      ## Remove a versão do campo Server no cabeçalho da resposta do server.
```

```
      server_tokens off;

      ## Configurações de Log.
      access_log /var/log/nginx/webmail2.douglasqsantos.com.br-access.log
combined;
      error_log /var/log/nginx/webmail2.douglasqsantos.com.br-error.log;
      ## Diretório raiz do website.
      root /var/www/html/webmail2;
      ## A configuração depende da requisição URI.
      location / {
        ## Checa os arquivos e se existirem são processador na ordem
especifica abaixo.
        try_files $uri $uri/ =404;
      }

      ## Nega acesso ao diretório data
      location ^~ /data {
        deny all;
      }
      ## Definição dos arquivos de Index
      index index.php index.htm index.html;
      ## Configuração para arquivos php.
      location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/var/run/php5-fpm.sock;
     }
}

## Configurações para o virtualhost.
server {
      ## Define a porta que o servidor está escutando.
      listen 443;
      ## Habilita o protocolo https para este virtual host.
      ssl on;
      ## Define o caminho para o arquivo crt.
      # Caso o arquivo não seja auto assinado temos que contenar os arquivos
ca e crt do server.
      # cat server_name.crt CertCA.crt >> server.crt
      ssl_certificate /etc/nginx/ssl/server.crt;
      ## Define o caminho que contem o certificado key para o servidor.
      ssl_certificate_key /etc/nginx/ssl/server.key;
      ## Define os ciphers disponíveis.
      ssl_protocols SSLv3 TLSv1 TLSv1.1 TLSv1.2;

      ## Define que os ciphers do servidor devem ter preferencia sobre os
dos clientes quenao utilizado o SSLv3 e protocolos TLS.
      ssl_prefer_server_ciphers on;

      ## Define os ciphers habilitados.
      ssl_ciphers HIGH:!aNULL:!MD5;
```

```
      ## Sets names of a virtual server
      server_name webmail2.douglasqsantos.com.br;
      ## Remove a versão do campo Server no cabeçalho da resposta do server.
      server_tokens off;

      ## Configurações de Log.
      access_log /var/log/nginx/webmail2.douglasqsantos.com.br-
ssl.access.log combined;
      error_log /var/log/nginx/webmail2.douglasqsantos.com.br-ssl.error.log;
      ## Diretório raiz do website.
      root /var/www/html/webmail2;
      ## A configuração depende da requisição URI.
      location / {
        ## Checa os arquivos e se existirem são processador na ordem
especifica abaixo.
        try_files $uri $uri/ =404;
      }
      ## Nega acesso ao diretório data
      location ^~ /data {
        deny all;
      }

      ## Definição dos arquivos de Index
      index index.php index.htm index.html;
      ## Configuração para arquivos php.
      location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/var/run/php5-fpm.sock;
     }
}
```

Vamos ativar o nosso virtual host para o webmail2

```
ln -s /etc/nginx/sites-available/webmail2.douglasqsantos.com.br
/etc/nginx/sites-enabled/webmail2.douglasqsantos.com.br
```

Agora vamos recarregar as configurações para o Nginx para testar

```
systemctl force-reload nginx
```

Agora já podemos testar acessando:

- http://webmail2.douglasqsantos.com.br
- https://webmail2.douglasqsantos.com.br

Geradores de relatórios

Iremos instalar alguns geradores de relatórios para acompanharmos o desenpenho dos serviços do servidor:

```
aptitude install rrdtool mailgraph queuegraph isoqlog munin munin-plugins-extra munin-node munin-common mailping -y
```

- Será perguntado qual o servidor de e-mail utilizado, selecione **postfix** ;
- Será perguntado onde será gravado os relatórios: **/var/www/html/isoqlog**
- Será perguntado o nome da máquina, deixe o mostrado;
- Será perguntado a Língua usada para as saídas dos relatórios, seleciona **Português**
- Será perguntado os domínios que serão gerados relatórios, informe os domínios separados por espaços:
    - **douglasqsantos.com.br**

Agora vamos acertar algumas configurações dos geradores de relatórios mailgraph

```
dpkg-reconfigure mailgraph
```

- Responda da seguinte forma

1. Mailgraph pode iniciar junto ao sistema como serviço: **Sim**
2. Informe o caminho para os arquivos de log do email: **/var/log/mail.log**
3. Ignorar emails vindos ou indo para o localhost: **NO**

Aqui no caso do isoqlog temos que executar /usr/bin/isoqlog para ele gerar os nossos relátorios ele ta no cron.daily então ele vai ser executado uma vez por dia.

No meu ponto de vista acho interresante executar ele a cada hora então podemos mudar ele.

```
cp -rfa /etc/cron.daily/isoqlog /etc/cron.hourly/
```

Como o isoqlog utilizar cgi precisamos adicionar está funcionalidade ao Nginx.

```
apt-get install fcgiwrap -y
```

Como o isoqlog não prove nenhum method de autenticação vamos criar um usuário para acessar os relatórios.

```
htpasswd -c /etc/nginx/.htpasswd-isoqlog mcq
New password:
Re-type new password:
Adding password for user mcq
```

Agora vamos configurar o virtual host do isoqlog

```
vim /etc/nginx/sites-available/isoqlog.douglasqsantos.com.br
#/etc/nginx/sites-available/isoqlog.douglasqsantos.com.br
## Configurações para o virtualhost.
server {
      ## Define a porta que o servidor está escutando.
      listen 80;
      ## Define o nome do virtual host.
      server_name isoqlog.douglasqsantos.com.br;
      ## Remove a versão do campo Server no cabeçalho da resposta do server.
```

```
      server_tokens off;

      ## Configurações de Log.
      access_log /var/log/nginx/isoqlog.douglasqsantos.com.br-access.log
combined;
      error_log /var/log/nginx/isoqlog.douglasqsantos.com.br-error.log;
      ## Diretório raiz do website.
      root /var/www/html/isoqlog;
      ## A configuração depende da requisição URI.
      location / {
        ## Checa os arquivos e se existirem são processador na ordem
especifica abaixo.
        try_files $uri $uri/ =404;
        auth_basic "Acesso Restrito";
        auth_basic_user_file /etc/nginx/.htpasswd-isoqlog;
      }

      ## Definição dos arquivos de Index
      index index.php index.htm index.html;
      ## Configuração para arquivos php.
      location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/var/run/php5-fpm.sock;
     }
     ## Configuração para arquivos cgi.
     location ~ ^/cgi-bin/.*\.cgi$ {
        root    /usr/lib;
  include fastcgi.conf;
        fastcgi_pass   unix:/var/run/fcgiwrap.socket;
    }
}

## Configurações para o virtualhost.
server {
      ## Define a porta que o servidor está escutando.
      listen 443;
      ## Habilita o protocolo https para este virtual host.
      ssl on;
      ## Define o caminho para o arquivo crt.
      # Caso o arquivo não seja auto assinado temos que contenar os arquivos
ca e crt do server.
      # cat server_name.crt CertCA.crt >> server.crt
      ssl_certificate /etc/nginx/ssl/server.crt;
      ## Define o caminho que contem o certificado key para o servidor.
      ssl_certificate_key /etc/nginx/ssl/server.key;
      ## Define os ciphers disponíveis.
      ssl_protocols SSLv3 TLSv1 TLSv1.1 TLSv1.2;

      ## Define que os ciphers do servidor devem ter preferencia sobre os
dos clientes quenao utilizado o SSLv3 e protocolos TLS.
      ssl_prefer_server_ciphers on;
```

```
      ## Define os ciphers habilitados.
      ssl_ciphers HIGH:!aNULL:!MD5;

      ## Sets names of a virtual server
      server_name isoqlog.douglasqsantos.com.br;
      ## Remove a versão do campo Server no cabeçalho da resposta do server.
      server_tokens off;

      ## Configurações de Log.
      access_log /var/log/nginx/isoqlog.douglasqsantos.com.br-ssl.access.log
combined;
      error_log /var/log/nginx/isoqlog.douglasqsantos.com.br-ssl.error.log;
      ## Diretório raiz do website.
      root /var/www/html/isoqlog;
      ## A configuração depende da requisição URI.
      location / {
        ## Checa os arquivos e se existirem são processador na ordem
especifica abaixo.
        try_files $uri $uri/ =404;
        auth_basic "Acesso Restrito";
        auth_basic_user_file /etc/nginx/.htpasswd-isoqlog;
      }

      ## Definição dos arquivos de Index
      index index.php index.htm index.html;
      ## Configuração para arquivos php.
      location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/var/run/php5-fpm.sock;
     }
     ## Configuração para arquivos cgi.
     location ~ ^/cgi-bin/.*\.cgi$ {
        root    /usr/lib;
  include fastcgi.conf;
        fastcgi_pass   unix:/var/run/fcgiwrap.socket;
    }
}
```

Vamos ativar o nosso virtual host para o isoqlog

```
ln -s /etc/nginx/sites-available/isoqlog.douglasqsantos.com.br
/etc/nginx/sites-enabled/isoqlog.douglasqsantos.com.br
```

Agora vamos recarregar as configurações para o Nginx para testar

```
systemctl force-reload nginx
```

Agora vamos executar o isoqlog para gerar os nosso relátorio

```
/usr/bin/isoqlog
```

```
Year: 2016 Month: 1
outputdir:/var/www/html/isoqlog
htmldir:/usr/share/isoqlog/htmltemp
logtype:postfix
logstore:/var/log/mail.log
langfile:/usr/share/isoqlog/lang/portuguese
maxsender:100
maxreceiver:100
maxtotal:100
maxbyte:100
hostname: mail.douglasqsantos.com.br
Domains douglasqsantos.com.br
The Created directory : /var/www/html/isoqlog/douglasqsantos.com.br
The Created directory : /var/www/html/isoqlog/douglasqsantos.com.br/2016
The Created directory : /var/www/html/isoqlog/douglasqsantos.com.br/2016/1
The Created directory : /var/www/html/isoqlog/general
The Created directory : /var/www/html/isoqlog/general/2016
The Created directory : /var/www/html/isoqlog/general/2016/1
```

A configuração do nosso isoqlog se baseia em dois arquivos

Primeiro arquivo que tem a configuração principal do isoqlog

```
vim /etc/isoqlog/isoqlog.conf
#isoqlog 2.0 Configuration file

logtype     = "postfix"
logstore    = "/var/log/mail.log"
domainsfile = "/etc/isoqlog/isoqlog.domains"
outputdir   = "/var/www/html/isoqlog"
htmldir     = "/usr/share/isoqlog/htmltemp"
langfile    = "/usr/share/isoqlog/lang/portuguese"
hostname    = "mail.douglasqsantos.com.br"

maxsender   = 100
maxreceiver = 100
maxtotal    = 100

maxbyte     = 100
```

Arquivo que controla os domínios que vão ser gerados relatórios, informe um domínio por linha caso tenha mais de um domínio.

```
vim /etc/isoqlog/isoqlog.domains
douglasqsantos.com.br
```

Agora vamos acessar os relatórios em **Nota:** Vai ser solicitado um usuário e senha que são os que definimos antes da criação do virtual host para o isoqlog.

- Isoqlog em:
  - http://isoqlog.douglasqsantos.com.br

    - https://isoqlog.douglasqsantos.com.br
- MailGraph em:
    - http://isoqlog.douglasqsantos.com.br/cgi-bin/mailgraph.cgi
    - https://isoqlog.douglasqsantos.com.br/cgi-bin/mailgraph.cgi
- QueueGraph em:
    - http://isoqlog.douglasqsantos.com.br/cgi-bin/queuegraph.cgi
    - https://isoqlog.douglasqsantos.com.br/cgi-bin/queuegraph.cgi

Ajustando o munin

```
vim /etc/munin/munin.conf
[...]
dbdir  /var/lib/munin
htmldir /var/www/html/monitor
logdir /var/log/munin
rundir  /var/run/munin
[...]
tmpldir /etc/munin/templates

# a simple host tree
[localhost.localdomain]
   address 127.0.0.1
   use_node_name yes
```

Vamos reiniciar o munin

```
systemctl restart munin-node
```

Vamos acertar o virtual host do munin Como o isoqlog não prove nenhum method de autenticação vamos criar um usuário para acessar os relatórios.

```
htpasswd -c /etc/nginx/.htpasswd-monitor mcq
New password:
Re-type new password:
Adding password for user mcq
```

Agora vamos configurar o virtual host do isoqlog

```
vim /etc/nginx/sites-available/monitor.douglasqsantos.com.br
#/etc/nginx/sites-available/monitor.douglasqsantos.com.br
## Configurações para o virtualhost.
server {
      ## Define a porta que o servidor está escutando.
      listen 80;
      ## Define o nome do virtual host.
      server_name monitor.douglasqsantos.com.br;
      ## Remove a versão do campo Server no cabeçalho da resposta do server.
      server_tokens off;

      ## Configurações de Log.
```

```
      access_log /var/log/nginx/monitor.douglasqsantos.com.br-access.log
combined;
      error_log /var/log/nginx/monitor.douglasqsantos.com.br-error.log;
      ## Diretório raiz do website.
      root /var/www/html/monitor;
      ## A configuração depende da requisição URI.
      location / {
        ## Checa os arquivos e se existirem são processador na ordem
especifica abaixo.
        try_files $uri $uri/ =404;
        auth_basic "Acesso Restrito";
        auth_basic_user_file /etc/nginx/.htpasswd-monitor;
      }

      ## Definição dos arquivos de Index
      index index.htm index.html;
}

## Configurações para o virtualhost.
server {
      ## Define a porta que o servidor está escutando.
      listen 443;
      ## Habilita o protocolo https para este virtual host.
      ssl on;
      ## Define o caminho para o arquivo crt.
      # Caso o arquivo não seja auto assinado temos que contenar os arquivos
ca e crt do server.
      # cat server_name.crt CertCA.crt >> server.crt
      ssl_certificate /etc/nginx/ssl/server.crt;
      ## Define o caminho que contem o certificado key para o servidor.
      ssl_certificate_key /etc/nginx/ssl/server.key;
      ## Define os ciphers disponíveis.
      ssl_protocols SSLv3 TLSv1 TLSv1.1 TLSv1.2;

      ## Define que os ciphers do servidor devem ter preferencia sobre os
dos clientes quenao utilizado o SSLv3 e protocolos TLS.
      ssl_prefer_server_ciphers on;

      ## Define os ciphers habilitados.
      ssl_ciphers HIGH:!aNULL:!MD5;

      ## Sets names of a virtual server
      server_name monitor.douglasqsantos.com.br;
      ## Remove a versão do campo Server no cabeçalho da resposta do server.
      server_tokens off;

      ## Configurações de Log.
      access_log /var/log/nginx/monitor.douglasqsantos.com.br-ssl.access.log
combined;
      error_log /var/log/nginx/monitor.douglasqsantos.com.br-ssl.error.log;
      ## Diretório raiz do website.
```

```
      root /var/www/html/monitor;
      ## A configuração depende da requisição URI.
      location / {
        ## Checa os arquivos e se existirem são processador na ordem
especifica abaixo.
        try_files $uri $uri/ =404;
        auth_basic "Acesso Restrito";
        auth_basic_user_file /etc/nginx/.htpasswd-monitor;
      }

      ## Definição dos arquivos de Index
      index index.htm index.html;
}
```

Vamos ativar o nosso virtual host para o monitor

```
ln -s /etc/nginx/sites-available/monitor.douglasqsantos.com.br
/etc/nginx/sites-enabled/monitor.douglasqsantos.com.br
```

Agora vamos recarregar as configurações para o Nginx para testar

```
systemctl force-reload nginx
```

Agora vamos fazer um acerto

```
cd /var/www/html
ln -sf /var/cache/munin/www monitor
```

Nota: Vai ser solicitado um usuário e senha que são os que definimos antes da criação do virtual host para o monitor. Agora para acessar o nosso monitor é só acessar

- Munin em:
  - http://monitor.douglasqsantos.com.br
  - https://monitor.douglasqsantos.com.br

Aqui vamos ter as estatísticas do nosso servidor de vários fatores.

Configuração do SPF

Agora vamos a configuração do SPF, aqui nós precisamos inserir em nosso servidor DNS quais são os hosts que podem enviar email em nome de nosso domínio.

Configuração para a Zona interna.

```
vim /var/lib/named/var/cache/bind/master/db.douglasqsantos.com.br-internal
$TTL 86400
@ IN SOA  dns.douglasqsantos.com.br. root.dns.douglasqsantos.com.br. (
                              2016020101  ; Serial
```

```
                              3600       ; Refresh
                              1800        ; Retry
                              1209600      ; Expire
                              3600 )     ; Minimum

;
@               IN      NS   douglasqsantos.com.br.
douglasqsantos.com.br. IN TXT "v=spf1 a mx ip4:192.168.254.0/24 -all"
douglasqsantos.com.br. IN SPF "v=spf1 a mx ip4:192.168.254.0/24 -all"
mail.douglasqsantos.com.br IN TXT "v=spf1 a -all"
mail.douglasqsantos.com.br IN SPF "v=spf1 a -all"
[...]
```

Configuração para a Zona externa.

```
vim /var/lib/named/var/cache/bind/master/db.douglasqsantos.com.br-external
$TTL 86400
@ IN SOA  dns.douglasqsantos.com.br. root.dns.douglasqsantos.com.br. (
                              2016020101  ; Serial
                              3600       ; Refresh
                              1800        ; Retry
                              1209600      ; Expire
                              3600 )     ; Minimum

;
@               IN      NS   douglasqsantos.com.br.
douglasqsantos.com.br. IN TXT "v=spf1 a mx ip4:177.177.177.177/29 -all"
douglasqsantos.com.br. IN SPF "v=spf1 a mx ip4:177.177.177.177/29 -all"
mail.douglasqsantos.com.br IN TXT "v=spf1 a -all"
mail.douglasqsantos.com.br IN SPF "v=spf1 a -all"
[...]
```

Aqui estamos especificando que estamos utilizando a versão 1 do spf e que os endereços que podem enviar email pelo nosso domínio são 177.177.177.177/29, com isso qualquer servidor que faça a validação de spf a nossa rede vai podem enviar email sem problemas. aqui precisamos trocar o 177.177.177.177/29 pela sua faixa de endereços pública que é o que a internet vai precisar validar.

O spf também foi adicionado na configuração do nosso master.cf como mostrado abaixo

```
vim /etc/postfix/master.cf
[...]
#-------------------------SPF-----------------------------------------------
------------------
policy  unix  -       n       n       -       -       spawn
 user=nobody argv=/usr/bin/perl /usr/sbin/postfix-policyd-spf-perl
#-------------------------END SPF-------------------------------------------
------------------
```

Com isso estamos fazendo a validação de spf dos domínios que nos enviarem email, e adicionando a configuração no dns estamos habilitando o spf e especificando quais ips podem enviar emails em nosso nome ;)

Configuração do DKIM

Aqui vamos configurar o DKIM com o Amavis, aqui sempre que enviarmos uma mensagem vai anexado a ela uma assinatura DKIM, o destinatário pode obter a chave pública por dns e validar se a mensagem bate com quem assinou, com isso conseguimos garantir a autenticidade da mensagem.

Precisamos primeiro gerar a nossa chave para assinar as mensagens

```
amavisd-new genrsa /etc/amavis/conf.d/mail.douglasqsantos.com.br.pem
Private RSA key successfully written to file
"mail.douglasqsantos.com.br.pem" (1024 bits, PEM format)
```

Agora precisamos adicionar no arquivo do Amavis o nosso certificado

```
vim /etc/amavis/conf.d/50-user
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
#
#Aqui vamos habilitar a verificação com dkim
$enable_dkim_verification = 1;
#Aqui vamos habilitar a assinatura com dkim
$enable_dkim_signing = 1;
#Aqui vamos especificar o nosso domínio que temos o reverso no provedor,
depois o nome do servidor e por último a localização da chave
dkim_key('douglasqsantos.com.br', 'mail',
'/etc/amavis/conf.d/mail.douglasqsantos.com.br.pem');
#Agora vamos passar algumas informações sobre o ttl, forma de trabalho e
quais são as nossas redes internas
@dkim_signature_options_bysender_maps = (
   { '.' => { ttl => 21*24*3600, c => 'relaxed/simple' } } );
@mynetworks = qw(127.0.0.0/8 192.168.254.0/24);  # list your internal
networks

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

Agora vamos mandar visualizar a nossa chave

```
amavisd-new showkeys
; key#1 1024 bits, i=mail, d=douglasqsantos.com.br,
/etc/amavis/conf.d/mail.douglasqsantos.com.br.pem
mail._domainkey.douglasqsantos.com.br. 3600 TXT (
  "v=DKIM1; p="
```

```
  "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDmnmTHBZ5iqiGePhZE6buzqQk1"
  "KBZCTFax52k1va8Gds4PLj+UINmnDxgAeOSyPfvXAJlA5+r0ZNmzKnTtJYd4SBft"
  "YRK9Zrw7E7tK+5mBV9jVCk9Z4/c0wPQD4b04vhi+VgiGeFcMNIfQvFAsHCj4z5w4"
  "CQC5HCYqb6bqFDIiBQIDAQAB")
```

Nós precisamos inserir a informação do domainkey no servidor dns não esqueça de atualizar o serial, vamos inserir o dkim nas duas Views interna e externa.

Alterando a View externa.

```
vim /var/lib/named/var/cache/bind/master/db.douglasqsantos.com.br-external
$TTL 86400
@ IN SOA  dns.douglasqsantos.com.br. root.dns.douglasqsantos.com.br. (
                              2016020101  ; Serial
                              3600       ; Refresh
                              1800        ; Retry
                              1209600      ; Expire
                              3600 )     ; Minimum

;
@               IN      NS   douglasqsantos.com.br.
douglasqsantos.com.br. IN TXT "v=spf1 a mx ip4:177.177.177.177/29 -all"
douglasqsantos.com.br. IN SPF "v=spf1 a mx ip4:177.177.177.177/29 -all"
mail.douglasqsantos.com.br IN TXT "v=spf1 a -all"
mail.douglasqsantos.com.br IN SPF "v=spf1 a -all"

mail._domainkey.douglasqsantos.com.br.     3600 TXT (
  "v=DKIM1; p="
  "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDmnmTHBZ5iqiGePhZE6buzqQk1"
  "KBZCTFax52k1va8Gds4PLj+UINmnDxgAeOSyPfvXAJlA5+r0ZNmzKnTtJYd4SBft"
  "YRK9Zrw7E7tK+5mBV9jVCk9Z4/c0wPQD4b04vhi+VgiGeFcMNIfQvFAsHCj4z5w4"
  "CQC5HCYqb6bqFDIiBQIDAQAB")
[...]
```

Alterando a View interna

```
vim /var/lib/named/var/cache/bind/master/db.douglasqsantos.com.br-internal
$TTL 86400
@ IN SOA  dns.douglasqsantos.com.br. root.dns.douglasqsantos.com.br. (
                              2016020101  ; Serial
                              3600       ; Refresh
                              1800        ; Retry
                              1209600      ; Expire
                              3600 )     ; Minimum

;
@               IN      NS   douglasqsantos.com.br.
douglasqsantos.com.br. IN TXT "v=spf1 a mx ip4:192.168.25.0/24 -all"
douglasqsantos.com.br. IN SPF "v=spf1 a mx ip4:192.168.25.0/24 -all"
mail.douglasqsantos.com.br IN TXT "v=spf1 a -all"
mail.douglasqsantos.com.br IN SPF "v=spf1 a -all"
```

```
; key#1 1024 bits, i=mail, d=douglasqsantos.com.br,
/etc/amavis/conf.d/mail.douglasqsantos.com.br.pem
mail._domainkey.douglasqsantos.com.br.     3600 TXT (
  "v=DKIM1; p="
  "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDmnmTHBZ5iqiGePhZE6buzqQk1"
  "KBZCTFax52k1va8Gds4PLj+UINmnDxgAeOSyPfvXAJlA5+r0ZNmzKnTtJYd4SBft"
  "YRK9Zrw7E7tK+5mBV9jVCk9Z4/c0wPQD4b04vhi+VgiGeFcMNIfQvFAsHCj4z5w4"
  "CQC5HCYqb6bqFDIiBQIDAQAB")
[...]
```

Após isso precisamos reiniciar o serviço do bind

```
systemctl restart bind9
```

Após isso já podemos testar a nossa chave DKIM

```
amavisd-new testkeys
TESTING#1: mail._domainkey.douglasqsantos.com.br   => pass
```

Agora vamos reiniciar o amavis

```
systemctl restart amavis
```

Agora envie uma nova mensagem e vamos testar o dkim.

Agora vamos visualizar uma mensagem com o dkim

```
telnet localhost 110
Trying ::1...
Connected to localhost.
Escape character is '^]'.
+OK Hello there.
user bob@douglasqsantos.com.br
+OK Password required.
pass doug123
+OK logged in.
list
+OK POP3 clients that break here, they violate STD53.
1 993
2 1746
.
retr 2
+OK 1746 octets follow.
Return-Path: <douglas@douglasqsantos.com.br>
X-Original-To: bob@douglasqsantos.com.br
Delivered-To: bob@douglasqsantos.com.br
Received: from localhost (localhost [127.0.0.1])
  by mail.douglasqsantos.com.br (Postfix) with ESMTP id 0306722059
  for <bob@douglasqsantos.com.br>; Sun, 31 Jan 2016 21:14:41 -0200 (BRST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
```

```
d=douglasqsantos.com.br; h=
  user-agent:message-id:organization:subject:subject:from:from
  :date:date:content-transfer-encoding:content-type:content-type
  :mime-version:received:received; s=mail; t=1454282079; x=
  1456096480; bh=Xr9JuuHKcwvCRl8lGAv9+DdWWoY5EBi1X5KjgXMcac4=; b=b
  YK13Bom8wqylCIH7BbDr5RD5Q6M031HzUY9suxuJqv73FNFMI/f4SNi9NRQ5P+ZK
  5u1qZoI38DaKjD1tIjEgFuwuaaO+1YM2PhVcfovKQD9XI7wA9DumdId/SPHYJfRS
  bE8sSHNRRWTjpgJm61qAT1iyAxZ/4QYti9+HnKD0Xc=
X-Virus-Scanned: Debian amavisd-new at mail.douglasqsantos.com.br
Received: from mail.douglasqsantos.com.br ([127.0.0.1])
  by localhost (mail.douglasqsantos.com.br [127.0.0.1]) (amavisd-new, port
10024)
  with ESMTP id rVdxNzyjwXt4 for <bob@douglasqsantos.com.br>;
  Sun, 31 Jan 2016 21:14:39 -0200 (BRST)
Received: from webmail.douglasqsantos.com.br (mail.douglasqsantos.com.br
[192.168.25.110])
  (using TLSv1.2 with cipher ECDHE-RSA-AES128-GCM-SHA256 (128/128 bits))
  (Client did not present a certificate)
  by mail.douglasqsantos.com.br (Postfix) with ESMTPSA id 18EA422058
  for <bob@douglasqsantos.com.br>; Sun, 31 Jan 2016 21:14:39 -0200 (BRST)
MIME-Version: 1.0
Content-Type: text/plain; charset=US-ASCII;
 format=flowed
Content-Transfer-Encoding: 7bit
Date: Sun, 31 Jan 2016 21:14:38 -0200
From: Douglas Quintiliano dos Santos <douglas@douglasqsantos.com.br>
To: bob@douglasqsantos.com.br
Subject: Douglas
Organization: DOUGLAS
Message-ID: <5258bbcd57e77dd83ae18a3ad4bcca70@douglasqsantos.com.br>
X-Sender: douglas@douglasqsantos.com.br
User-Agent: Roundcube Webmail/1.1.4

Douglas
.
quit
+OK Bye-bye.
Connection closed by foreign host.
```

Agora vamos criar um script para gerenciar os nossos serviços de Email o primeiro vamos levar em consideração que instalamos o Courier.

```
vim /etc/init.d/servmail.sh
#!/bin/bash
### CORES UTILIZADAS NO SCRIPT ###
GREY="\033[01;30m"
RED="\033[01;31m"
GREEN="\033[01;32m"
YELLOW="\033[01;33m"
BLUE="\033[01;34m"
PURPLE="\033[01;35m"
```

```
CYAN="\033[01;36m"
WHITE="\033[01;37m"
CLOSE="\033[m"

#VALIDA RETORNO DE COMANDO
_CHECAR () {
if [ $? -eq 0 ]; then
  echo -e "${GREEN}[  OK  ]${CLOSE}"
else
  echo -e " ${RED}[ FALHOU ]${CLOSE}"
fi
}


STOP="nginx php5-fpm saslauthd amavis spamassassin postgrey clamav-daemon
clamav-freshclam courier-authdaemon courier-imap courier-imap-ssl courier-
pop courier-pop-ssl postfix"

START="saslauthd amavis spamassassin postgrey clamav-daemon clamav-freshclam
courier-authdaemon courier-imap courier-imap-ssl courier-pop courier-pop-ssl
postfix php5-fpm nginx"


case $1 in
stop)
echo -e "${RED} PARANDO OS SERVICOS ${CLOSE}"
for END in ${STOP}
do
systemctl stop ${END}
echo -e "${RED} SERVICO ${END} PARADO COM SUCESSO ${CLOSE} $(_CHECAR)";
done
echo -e "${RED} SERVICOS PARADOS ${CLOSE}"
;;

start)
echo -e "${BLUE} INICIANDO OS SERVICOS ${CLOSE}"
for END in ${START}
do
systemctl start ${END}
echo -e "${BLUE} SERVICO ${END} INICIADO COM SUCESSO ${CLOSE} $(_CHECAR)";
done
echo -e "${BLUE} SERVICOS INICIADOS ${CLOSE}"
;;

restart)
  $0 stop
  $0 start
;;

  *)
```

```
   echo  "${RED}Opcoes Validas:(start|stop|restart)${CLOSE}"
  ;;

esac
```

Agora vamos criar um script levando em consideração que instalamos o dovecot.

```
vim /etc/init.d/servmail.sh
#!/bin/bash
### CORES UTILIZADAS NO SCRIPT ###
GREY="\033[01;30m"
RED="\033[01;31m"
GREEN="\033[01;32m"
YELLOW="\033[01;33m"
BLUE="\033[01;34m"
PURPLE="\033[01;35m"
CYAN="\033[01;36m"
WHITE="\033[01;37m"
CLOSE="\033[m"

#VALIDA RETORNO DE COMANDO
_CHECAR () {
if [ $? -eq 0 ]; then
  echo -e "${GREEN}[  OK  ]${CLOSE}"
else
  echo -e " ${RED}[ FALHOU ]${CLOSE}"
fi
}


STOP="nginx php5-fpm saslauthd amavis spamassassin postgrey clamav-daemon
clamav-freshclam dovecot postfix"
START="saslauthd amavis spamassassin postgrey clamav-daemon clamav-freshclam
dovecot postfix php5-fpm nginx"


case $1 in
stop)
echo -e "${RED} PARANDO OS SERVICOS ${CLOSE}"
for END in ${STOP}
do
systemclt stop ${END}
echo -e "${RED} SERVICO ${END} PARADO COM SUCESSO ${CLOSE} $(_CHECAR)";
done
echo -e "${RED} SERVICOS PARADOS ${CLOSE}"
;;

start)
echo -e "${BLUE} INICIANDO OS SERVICOS ${CLOSE}"
for END in ${START}
do
```

```
systemclt start ${END}
echo -e "${BLUE} SERVICO ${END} INICIADO COM SUCESSO ${CLOSE} $(_CHECAR)";
done
echo -e "${BLUE} SERVICOS INICIADOS ${CLOSE}"
;;

restart)
  $0 stop
  $0 start
;;

  *)
   echo  "${RED}Opcoes Validas:(start|stop|restart)${CLOSE}"
  ;;

esac
```

Agora vamos acertar as permissões do script.

```
chmod 755 /etc/init.d/servmail.sh
```

Agora para parar os serviços de email.

```
/etc/init.d/servmail.sh stop
```

Agora para iniciar os serviços de email.

```
/etc/init.d/servmail.sh start
```

Agora para reiniciar os serviços de email.

```
/etc/init.d/servmail.sh restart
```

Agora é só ir ajustando de acordo com o seu ambiente.

Referências

1. http://www.postfix.org/
2. http://www.postfix.org/documentation.html
3. http://www.postfix.org/docs.html
4. http://www.postfix.org/SASL_README.html
5. http://pam-mysql.sourceforge.net/
6. http://pam-mysql.sourceforge.net/Documentation/
7. http://httpd.apache.org/
8. http://httpd.apache.org/docs/
9. http://httpd.apache.org/docs/2.2/ssl/
10. http://wiki.apache.org/httpd/

11. http://httpd.apache.org/docs/2.2/vhosts/
12. http://postfixadmin.sourceforge.net/
13. http://dev.mysql.com/
14. http://dev.mysql.com/doc/
15. http://php.net/
16. http://www.dovecot.org/
17. http://www.dovecot.org/documentation.html
18. http://postgrey.schweikert.ch/
19. http://www.postfix.org/SMTPD_POLICY_README.html
20. http://www.eicar.org/86-0-Intended-use.html
21. http://www.clamav.net/lang/en/
22. http://roundcube.net/
23. http://roundcube.net/about
24. http://trac.roundcube.net/wiki/Howto_Install
25. http://vda.sourceforge.net/
26. http://www.enderunix.org/isoqlog/
27. http://www.enderunix.org/isoqlog/isoqlog-2.2/INSTALL
28. http://www200.pair.com/mecham/spam/ubuntu104-maia.html
29. http://www.maiamailguard.com/maia/wiki
30. http://www.maiamailguard.com/maia/wiki/FAQ
31. http://www.openspf.org/
32. http://www.openspf.org/Software
33. http://www.fail2ban.org/wiki/index.php/Main_Page
34. http://www.fail2ban.org/wiki/index.php/HOWTOs
35. http://www.zeroflux.org/projects/knock
36. http://www.openssl.org/
37. http://www.amavis.org/
38. http://www.ijs.si/software/amavisd/
39. http://www.ijs.si/software/amavisd/amavisd-new-docs.html
40. https://www.ijs.si/software/amavisd/INSTALL.txt
41. http://www.cacert.org/
42. http://wiki.cacert.org/ServerCerts
43. http://wiki.cacert.org/HowToDocuments
44. http://munin-monitoring.org/
45. http://munin-monitoring.org/wiki/Documentation
46. http://munin-monitoring.org/wiki/LinuxInstallation
47. http://munin-monitoring.org/wiki/munin.conf
48. http://munin-monitoring.org/wiki/munin-node.conf
49. http://www.ijs.si/software/amavisd/amavisd-new-docs.html#dkim
50. http://ruby-doc.org/stdlib-2.2.0/libdoc/base64/rdoc/Base64.html
51. https://www.digitalocean.com/community/tutorials/how-to-protect-an-nginx-server-with-fail2ban-on-ubuntu-14-04
52. https://easyengine.io/tutorials/nginx/fail2ban/
53. https://www.nginx.com/resources/wiki/start/topics/examples/simplecgi/#
54. https://wiki.debian.org/nginx/FastCGI
55. https://www.digitalocean.com/community/tutorials/how-to-set-up-http-authentication-with-nginx-on-ubuntu-12-10
56. https://www.howtoforge.com/serving-cgi-scripts-with-nginx-on-debian-squeeze-ubuntu-11.04-p3
57. https://www.digicert.com/ssl-certificate-installation-nginx.htm
58. http://www.cyberciti.biz/tips/linux-unix-bsd-nginx-webserver-security.html
59. http://www.afterlogic.com/wiki/Protecting_data_directory_(WebMail_Pro)

60. http://www.afterlogic.com/wiki/Installation_Instructions_for_Linux_(WebMail_Lite)
61. http://jaqque.sbih.org/kplug/apt-pinning.html
62. https://wiki.debian.org/AptPreferences
63. http://nginx.org/en/linux_packages.html
64. https://wiki.archlinux.org/index.php/Virtual_user_mail_system