

Tutorial Cyrus IMAP aggregator (murder) 2.3.16 sobre Debian GNU Linux 5.x Lenny

Author: André Felipe Machado<andremachado@techforce.com.br>

Este tutorial completo mostrará como montar um LABORATÓRIO de infra-estrutura de e-mail bastante escalável, para centenas de milhares de contas.

O que é Cyrus IMAP (Murder) Aggregator.

Cyrus IMAP Aggregator (Murder) é um sistema de alto desempenho análogo a um cluster de servidores de e-mail.

Extremamente escalável (para centenas de milhares de contas), permite recursos como compartilhamento de caixas postais entre servidores backend diferentes, mover caixas postais entre servidores, e adicionar novos servidores para aumento de capacidade em diferentes níveis de serviço, se for o caso.

Curiosidade: Murder é coletivo de corvo, em idioma inglês.

Agradecimentos a Lucas Zinato Carraro por apresentar o Cyrus Murder Aggregator.

Objetivos deste tutorial

Educacionais.

Não haverá tuning de recursos computacionais nem preocupações com segurança, para evitar demasiada complexidade e aumento de variáveis.

Cada ambiente de hardware e software, bem como cenários e perfis de utilização pelos usuários implicam em tunings diferentes.

Para este tutorial, foram baixados fontes de um repositório Debian em 2010, para pacotes de uma versão Cyrus 2.3.16, bastante estável na data.

Recomendamos utilizar em ambientes de produção os pacotes Debian em versões nos repositórios **atualmente**.

Pacotes Debian GNU/Linux 5.x Lenny experimentais Cyrus 2.3.16

Você deve recompilar os pacotes binários Debian GNU/Linux a partir destes pacotes fonte EXPERIMENTAIS.

[cyrus-imapd-2.3_2.3.16.orig.tar.gz](#)[cyrus-imapd-2.3_2.3.16-1.debian.tar.gz](#)[cyrus-imapd-2.3_2.3.16-1.dsc](#)[cyrus-imapd-2.3_2.3.16-1_i386.changes](#)

Todas as máquinas do
murder / aggregator

Configurar APT

Seguir instruções [configurando o APT em Debian](#)

Pacotes em todas as máquinas

```
apt-get install sasl2-bin libsasl2-modules libsasl2-2 libsasl2-modules-  
ldap \  
db4.6-util libdb4.6 db4.7-util libdb4.7 perl perl-base perl-modules  
postfix postfix-ldap \  
gawk libpcre3 libsnmp5 libzephyr3 libhesiod0 libsensors3 libsnmp-base \  
libperl5.10 ucf libsysfs2 libauthen-sasl-cyrus-perl libauthen-sasl-perla  
pt-get install db4.6-util db4.7-util gawk libdb4.6 libdb4.7 libhesiod0 \  
libpcre3 libperl5.10 libsasl2-2 libsasl2-modules libsasl2-modules-ldap \  

```

```
libsensors3 libsnp15 libsnp-base libsysfs2 libzephyr3 perl perl-base \  
perl-modules sasl2-bin ucf libwrap0 libcam0g libssl0.9.8 \  
libcomerr2 xutils ldap-utils
```

/etc/services

Acrescentar no arquivo

```
#AFM 23ago2010  
mupdate          3905/tcp #cyrus mupdate aggregator murder  
lmtp             24/tcp #
```

Senão vai acontecer o seguinte ERRO (por não saber qual porta conectar ao protocolo):

```
debian192_168_56_108:~# mupdatetest -u mupdateuser -a mupdateuser  
debian192_168_56_106  
getaddrinfo: Servname not supported for ai_socktype  
failure: Network initialization -- cannot connect to  
debian192_168_56_106:mupdate
```

DNS ou /etc/hosts

/etc/hosts ou DNS configurado pois o cyrus usa NOMES em vez de IP para encontrar as máquinas.

```
127.0.0.1          localhost  
192.168.56.105    debian192_168_56_105 #imap frontend 01  
192.168.56.106    debian192_168_56_106 #mupdate master unique  
192.168.56.107    debian192_168_56_107 #imap backend 01  
192.168.56.108    debian192_168_56_108 #imap backend 02  
# The following lines are desirable for IPv6 capable hosts  
::1               localhost ip6-localhost ip6-loopback  
fe00::0           ip6-localnet  
ff00::0           ip6-mcastprefix  
ff02::1           ip6-allnodes  
ff02::2           ip6-allrouters  
ff02::3           ip6-allhosts
```

Cuidado: localhost não pode ter como alias o nome da máquina que pretendemos usar, ou vai confundir o cyrus murder/aggregator

Usuários e administradores chave

É preciso criar o usuário e o admin na base sasl da máquina de mupdate no mínimo!!!!

Melhor criar esses usuarios/admins nas máquinas do murder.

O usuário e a senha devem ser os que estão configurados nos arquivos do cyrus.

```
debian192_168_56_106:~# saslpasswd2 -c mupdateuser
Password:
Again (for verification):
debian192_168_56_106:~#
debian192_168_56_108:~# sasldblistusers2
mupdateuser@debian192_168_56_108: userPassword
cyrus@debian192_168_56_108: userPassword
cyrus@localhost: userPassword
debian192_168_56_108:~#
```

/etc/default/cyrus2.3

Edite o nível de verbosidade dos logs do cyrus alterando o seguinte trecho:

```
# Set this to 1 or higher to enable debugging on cyrmaster
#AFM 07out2010
CYRUS_VERBOSE=7
```

/etc/default/saslauthd

No exemplo atual, nem precisaria usar daemon. Mas já vamos configurar para usar "sasldb" e aumentar a verbosidade. Numa aplicação em produção, usaria ldap ou kerberos, por exemplo. Usando sasldb, cada usuário tem de ser configurado manualmente em cada máquina. Como em nosso exemplo atual. Viável apenas em laboratório didático.

```
#
# Settings for saslauthd daemon
# Please read /usr/share/doc/sasl2-bin/README.Debian for details.
#
# Should saslauthd run automatically on startup? (default: no)
#AFM 07out2010
START=yes
# Description of this saslauthd instance. Recommended.
# (suggestion: SASL Authentication Daemon)
DESC="SASL Authentication Daemon"
# Short name of this saslauthd instance. Strongly recommended.
# (suggestion: saslauthd)
NAME="saslauthd"
# Which authentication mechanisms should saslauthd use? (default: pam)
#
# Available options in this Debian package:
# getpwent -- use the getpwent() library function
# kerberos5 -- use Kerberos 5
# pam -- use PAM
# rimap -- use a remote IMAP server
# shadow -- use the local shadow password file
# sasldb -- use the local sasldb database file
# ldap -- use LDAP (configuration is in /etc/saslauthd.conf)
#
# Only one option may be used at a time. See the saslauthd man page
# for more information.
```

```

#
# Example: MECHANISMS="pam"
#MECHANISMS="pam"
#AFM 07out2010
MECHANISMS="sasldb"
# Additional options for this mechanism. (default: none)
# See the saslauthd man page for information about mech-specific
options.
MECH_OPTIONS=""
# How many saslauthd processes should we run? (default: 5)
# A value of 0 will fork a new process for each connection.
THREADS=5
# Other options (default: -c -m /var/run/saslauthd)
# Note: You MUST specify the -m option or saslauthd won't run!
#
# WARNING: DO NOT SPECIFY THE -d OPTION.
# The -d option will cause saslauthd to run in the foreground instead
of as
# a daemon. This will PREVENT YOUR SYSTEM FROM BOOTING PROPERLY. If you
wish
# to run saslauthd in debug mode, please run it by hand to be safe.
#
# See /usr/share/doc/sasl2-bin/README.Debian for Debian-specific
information.
# See the saslauthd man page and the output of 'saslauthd -h' for
general
# information about these options.
#
# Example for postfix users: "-c -m
/var/spool/postfix/var/run/saslauthd"
#AFM 07out2010 verbose
OPTIONS="-c -m /var/run/saslauthd -v"

```

Arquivos de configuração do cyrus murder/aggregator

O Cyrus murder/aggregator é um complexo sistema integrado de vários servidores, com muitas "partes móveis".

Os arquivos de configuração possuem parâmetros que são ajustados EM CONJUNTO e ENTRE MÁQUINAS.

O conjunto de parâmetros de uma máquina reflete-se NO SISTEMA INTEGRADO. Portanto, completa atenção ao alterar ou configurar qualquer parâmetro. Conheça seus efeitos colaterais na própria máquina e NO SISTEMA INTEGRADO.

Recriar diretórios

Em todas as máquinas, após editar os arquivos de configuração, será necessário recriar os

diretórios e permissões.

cyrus-makedirs **Backends**

Pacotes para os backends

```
dpkg -i cyrus-admin-2.3_2.3.16-1_all.deb \
cyrus-clients-2.3_2.3.16-1_amd64.deb \
cyrus-common-2.3_2.3.16-1_amd64.deb \
cyrus-imapd-2.3_2.3.16-1_amd64.deb \
libcyrus-imap-perl23_2.3.16-1_amd64.deb
```

Cópia de segurança dos arquivos de configuração

```
mv /etc/cyrus.conf /etc/cyrus.conf.original
mv /etc/imapd.conf /etc/imapd.conf.original
```

/etc/cyrus.conf nos backends

```
# Debian defaults for Cyrus IMAP server/cluster implementation
# see cyrus.conf(5) for more information
#
# All the tcp services are tcpd-wrapped. see hosts_access(5)
#AFM 05out2010 backend server

START {
    # do not delete this entry!
    recover          cmd="/usr/sbin/ctl_cyrusdb -r"

    # this is only necessary if idlemethod is set to "idled" in
    imapd.conf
    #AFM 20ago2010 pode ser necessario habilitar
    #idled           cmd="idled"

    # this is useful on backend nodes of a Murder cluster
    # it causes the backend to synchronize its mailbox list with
    # the mupdate master upon startup
    #AFM 20ago2010
    mupdatepush     cmd="/usr/sbin/ctl_mboxlist -m"

    # this is recommended if using duplicate delivery suppression
    delprune        cmd="/usr/sbin/cyr_expire -E 3"
    # this is recommended if caching TLS sessions
    #AFM 20ago2010 pode não ser necessario
    tlsprune        cmd="/usr/sbin/tls_prune"
}

# UNIX sockets start with a slash and are absolute paths
# you can use a maxchild=# to limit the maximum number of forks of a
service
# you can use babysit=true and maxforkrate=# to keep tight tabs on the
service
# most services also accept -U (limit number of reuses) and -T (timeout)
SERVICES {
    # --- Normal cyrus spool, or Murder backends ---
    # add or remove based on preferences
```

```

#AFM 05out2010 deployments may have maxchild 10000. babysit exceeds
maxchild + 1
#AFM parameters from master/service.c
#AFM -C: alternate config file
#AFM -U: max process uses
#AFM -T: reuse timeout
#AFM -D: call debugger
imap          cmd="imapd -U 30" listen="imap" prefork=1
maxchild=100 maxforkrate=20 proto=tcp4 maxfds=256 -U 5 -T 10
#imaps        cmd="imapd -s -U 30" listen="imaps" prefork=0
maxchild=100
#pop3         cmd="pop3d -U 20" listen="pop3" prefork=0
maxchild=50
#pop3s        cmd="pop3d -s -U 30" listen="pop3s" prefork=0
maxchild=50
#nntp         cmd="nntpd -U 10" listen="nntp" prefork=0
maxchild=100
#nntps        cmd="nntpd -s -U 30" listen="nntps" prefork=0
maxchild=100

# At least one form of LMTP is required for delivery
# (you must keep the Unix socket name in sync with imap.conf)
#AFM 05out2010 separate machines. parameters a bit higher than
frontends.
#AFM 05out2010 babysit ONLY at backends to not exhaust mupdate master
resources too.
lmtpl         cmd="lmtpl" listen="debian192_168_56_108:lmtpl"
prefork=1 maxchild=20 babysit=true maxforkrate=2 proto=tcp4 maxfds=256 -
U 5 -T 10
#lmtplunix    cmd="lmtpl" listen="/var/run/cyrus/socket/lmtpl"
prefork=0 maxchild=20
# -----

# useful if you need to give users remote access to sieve
# by default, we limit this to localhost in Debian
#AFM 22nov2010 do not limit to localhost in a cyrus murder
sieve         cmd="timsieved" listen="sieve" prefork=0
maxchild=100

# this one is needed for the notification services
notify        cmd="notifyd"
listen="/var/run/cyrus/socket/notify" proto="udp" prefork=1

# --- Murder frontends -----
# enable these and disable the matching services above,
# except for sieve (which deals automatically with Murder)

# mupdate database service - must prefork at least 1
# (mupdate slaves)
#mupdate      cmd="mupdate" listen=3905 prefork=1
# (mupdate master, only one in the entire cluster)
#mupdate      cmd="mupdate -m" listen=3905 prefork=1

# proxies that will connect to the backends
#imap         cmd="proxyd" listen="imap" prefork=0
maxchild=100
#imaps        cmd="proxyd -s" listen="imaps" prefork=0
maxchild=100
#pop3         cmd="pop3proxyd" listen="pop3" prefork=0
maxchild=50
#pop3s        cmd="pop3proxyd -s" listen="pop3s" prefork=0
maxchild=50

```

```

        #lmtplib          cmd="lmtplib" listen="lmtplib" prefork=1
maxchild=20
        # -----
    }
EVENTS {
    # this is required
#AFM 20ago2010 baixar para 5 minutos
#    checkpoint          cmd="/usr/sbin/ctl_cyrusdb -c" period=30
#    checkpoint          cmd="/usr/sbin/ctl_cyrusdb -c" period=5

    # this is only necessary if using duplicate delivery suppression
delprune          cmd="/usr/sbin/cyr_expire -E 3" at=0401

    # this is only necessary if caching TLS sessions
tlsprune          cmd="/usr/sbin/tls_prune" at=0401

    # indexing of mailboxes for server side fulltext searches

    # reindex changed mailboxes (fulltext) approximately every
other hour
#squatter_1      cmd="/usr/bin/nice -n 19 /usr/sbin/squatter -s"
period=120

    # reindex all mailboxes (fulltext) daily
#squatter_a      cmd="/usr/sbin/squatter" at=0517

#AFM 17nov2010
## Expirar mensagens do delay Expunge
delprune          cmd="/usr/sbin/cyr_expire -X 14" at=0200

## Expirar pastas deletadas a mais de 14 dias
delprune          cmd="/usr/sbin/cyr_expire -D 14" at=0400
}
</pre>/etc/imapd.conf nos backends

```

```

# Debian Cyrus imapd.conf
# See imapd.conf(5) for more information and more options
#AFM 05out2010 backend server
# Configuration directory
configdirectory: /var/lib/cyrus

# Which partition to use for default mailboxes
#AFM 27ago2010 one MUST NOT define "defaultpartition" AND "partition-
default"
# at a proxy/frontend/mupdate or it will create mbx locally.
defaultpartition: default
partition-default: /var/spool/cyrus/mail

#AFM 20ago2010 pode-se especificar diferentes particoes alternativas,
por ex. UF
#partition-ac: /var/spool/correio/ac
#partition-al: /var/spool/correio/al
#partition-am: /var/spool/correio/am
#partition-ap: /var/spool/correio/ap
#partition-ba: /var/spool/correio/ba
#partition-ce: /var/spool/correio/ce
#partition-df: /var/spool/correio/df

#AFM 20ago2010 se usar diferentes particoes e

```

```
# Para permitir a movimentacao entre backends
allowusermoves: yes

#AFM 20ago2010
# Colocado para compatibilizacao com Clientes para subscrever em caixas
# pertencentes a diferentes backends
allowallsubscribe: 1

#AFM 20ago2010
# Eliminar mensagens duplicadas
duplicatesuppression: 1

#AFM 20ago2010
# Habilitar que as mensagens nao sejam deletadas
# imediatamente e possam ser recuperadas.
expunge_mode: delayed

# News setup
partition-news: /var/spool/cyrus/news
newsspool: /var/spool/news

# Alternate namespace
# If enabled, activate the alternate namespace as documented in
# /usr/share/doc/cyrus-doc-2.3/html/altnamespace.html, where an user's
# subfolders are in the same level as the INBOX
# See also userprefix and sharedprefix on imapd.conf(5)
altnamespace: no

# UNIX Hierarchy Convention
# Set to yes, and cyrus will accept dots in names, and use the forward
# slash "/" to delimit levels of the hierarchy. This is done by
# converting
# internally all dots to "^", and all "/" to dots. So the "rabbit.holes"
# mailbox of user "helmer.fudd" is stored in
# "user.elmer^fud.rabbit^holes"
#AFM 12ago2010
#unixhierarchysep: no
unixhierarchysep: yes

# Rejecting illegal characters in headers
# Headers of RFC2882 messages must not have characters with the 8th bit
# set. However, too many badly-written MUAs generate this, including
# most
# spamware. Enable this to reject such messages.
#reject8bit: yes

# Munging illegal characters in headers
# Headers of RFC2882 messages must not have characters with the 8th bit
# set. However, too many badly-written MUAs generate this, including
# most
# spamware. If you kept reject8bit disabled, you can choose to leave the
# crappage untouched by disabling this (if you don't care that IMAP
# SEARCH
# won't work right anymore.
#munge8bit: no

# Forcing recipient user to lowercase
# Cyrus 2.3 is case-sensitive. If all your mail users are in
# lowercase, it is
# probably a very good idea to set lmtpl_downcase_rcpt to true. This is
# set by
```

```

# default, per RFC2821. This was not set by default in debian versions
up to
# and including 2.2.12-4.
lmtp_downcase_rcpt: yes

#AFM 20ago2010
# Setando este valor para 0 a mensagem de falha
# nao e enviada imediatamente ao cliente
lmtp_over_quota_perm_failure: 0

# Uncomment the following and add the space-separated users who
# have admin rights for all services.
#AFM 12ago2010
#admins: cyrus
admins: cyrus techforce-admin cyrmaster mupdateuser

# Space-separated list of users that have lmtp "admin" status (i.e. that
# can deliver email through TCP/IP lmtp). If specified, this parameter
# overrides the "admins" parameter above
#lmtp_admins: postman
#AFM 20ago2010
lmtp_admins: mupdateuser postman

# Space-separated list of users that have mupdate "admin" status, in
# addition to those in the admins: entry above. Note that mupdate
slaves and
# backends in a Murder cluster need to authenticate against the mupdate
master
# as admin users.
#mupdate_admins: mupdateman
#AFM 20ago2010
mupdate_admins: mupdateman mupdateuser

# Space-separated list of users that have imapd "admin" status, in
# addition to those in the admins: entry above
#imap_admins: cyrus
#AFM 13out2010
imap_admins: cyrus mupdateuser techforce-admin

# Space-separated list of users that have sieve "admin" status, in
# addition to those in the admins: entry above
#sieve_admins: cyrus

# List of users and groups that are allowed to proxy for other users,
# seperated by spaces. Any user listed in this will be allowed to login
# for any other user. Like "admins:" above, you can have
imap_proxyservers
# and sieve_proxyservers.
#proxyservers: cyrus
#AFM 01out2010 you MUST NOT set proxyservers on frontends ONLY at
backends
proxyservers: mupdateuser cyrus
proxy_authname: mupdateuser
proxy_password: senha

# No anonymous logins
allowanonymouslogin: no

# Minimum time between POP mail fetches in minutes
popminpoll: 1

```

```
# If nonzero, normal users may create their own IMAP accounts by
creating
# the mailbox INBOX.  The user's quota is set to the value if it is
positive,
# otherwise the user has unlimited quota.
autocreatequota: 0

# umask used by Cyrus programs
umask: 077

# Sendmail binary location
# DUE TO A BUG, Cyrus sends CRLF EOLs to this program. This breaks Exim
3.
# For now, to work around the bug, set this to a wrapper that calls
# /usr/sbin/sendmail -dropcr instead if you use Exim 3.
#AFM 20ago2010
sendmail: /usr/sbin/sendmail

# If enabled, cyrdeliver will look for Sieve scripts in user's home
# directories: ~user/.sieve.
sieveusehomedir: false

# If sieveusehomedir is false, this directory is searched for Sieve
scripts.
sievedir: /var/spool/sieve

# notifyd(8) method to use for "MAIL" notifications.  If not set, "MAIL"
# notifications are disabled.  Valid methods are: null, log, zephyr
#mailnotifier: zephyr

# notifyd(8) method to use for "SIEVE" notifications.  If not set,
"SIEVE"
# notifications are disabled.  This method is only used when no method
is
# specified in the script.  Valid methods are null, log, zephyr, mailto
#sievenotifier: zephyr

# DRAC (pop-before-smtp, imap-before-smtp) support
# Set dracinterval to the time in minutes to call DRAC while a user is
# connected to the imap/pop services. Set to 0 to disable DRAC (default)
# Set drachost to the host where the rpc drac service is running
#dracinterval: 0
#drachost: localhost

# If enabled, the partitions will also be hashed, in addition to the
hashing
# done on configuration directories. This is recommended if one
partition has a
# very bushy mailbox tree.
hashimapspool: true

# Allow plaintext logins by default (SASL PLAIN)
allowplaintext: yes
# Mesmo colocando o metodo PLAIN a autenticacao e passada
# somente apos o STARTTLS que criptografa a comunicacao
# clientes usam o IMAPS

# Force PLAIN/LOGIN authentication only
# (you need to uncomment this if you are not using an auxprop-based SASL
# mechanism.  saslauthd users, that means you!). And pay attention to
# sasl_minimum_layer and allowpop below, too.
```

```

#sasl_mech_list: PLAIN
#AFM 12ago2010
sasl_mech_list: PLAIN

# Allow use of the POP3 APOP authentication command.
# Note that this command requires that the plaintext passwords are
# available in a SASL auxprop backend (eg. sasldb), and that the system
# can provide enough entropy (eg. from /dev/urandom) to create a
challenge
# in the banner.
#allowapop: no

# The minimum SSF that the server will allow a client to negotiate. A
# value of 1 requires integrity protection; any higher value requires
some
# amount of encryption.
#sasl_minimum_layer: 0
#AFM 12ago2010
sasl_minimum_layer: 0

# The maximum SSF that the server will allow a client to negotiate. A
# value of 1 requires integrity protection; any higher value requires
some
# amount of encryption.
#sasl_maximum_layer: 256

# List of remote realms whose users may log in using cross-realm
# authentications. Separate each realm name by a space. A cross-realm
# identity is considered any identity returned by SASL with an "@" in
it.
# NOTE: To support multiple virtual domains on the same interface/IP,
# you need to list them all as loginrealms. If you don't list them here,
# (most of) your users probably won't be able to log in.
#loginrealms: example.com
#AFM 24ago2010
#loginrealms: localhost techforce.com.br
#AFM 02set2010 trying to avoid asking for passwd
loginrealms: localhost techforce.com.br debian192_168_56_108
debian192_168_56_107

# Enable virtual domain support. If enabled, the user's domain will
# be determined by splitting a fully qualified userid at the last '@'
# or '%' symbol. If the userid is unqualified, and the virdomains
# option is set to "on", then the domain will be determined by doing
# a reverse lookup on the IP address of the incoming network
# interface, otherwise the user is assumed to be in the default
# domain (if set).
#AFM 20ago2010
virdomains: userid

# The default domain for virtual domain support
# If the domain of a user can't be taken from its login and it can't
# be determined by doing a reverse lookup on the interface IP, this
# domain is used.
#defaultdomain:
#AFM 23ago2010
defaultdomain: techforce.com.br

#
# SASL library options (these are handled directly by the SASL
libraries,
# refer to SASL documentation for an up-to-date list of these)

```

```

#

# The mechanism(s) used by the server to verify plaintext passwords.
Possible
# values are "saslauthd", "auxprop", "pwcheck" and "alwaystrue". They
# are tried in order, you can specify more than one, separated by
spaces.
#
# Do note that, since sasl will be run as user cyrus, you may have a
lot of
# trouble to set this up right.
#AFM 20ago2010
#sasl_pwcheck_method: auxprop
#sasl_pwcheck_method: saslauthd auxprop
#AFM 02set2010 tentando evitar pedir senha qdo especifica servidor ao
creatembox
sasl_pwcheck_method: alwaystrue

# What auxpropd plugins to load, if using sasl_pwcheck_method: auxprop
# by default, all plugins are tried (which is probably NOT what you
want).
#AFM 20ago2010
sasl_auxprop_plugin: sasldb

# If enabled, the SASL library will automatically create authentication
secrets
# when given a plaintext password. Refer to SASL documentation
sasl_auto_transition: no

#
# SSL/TLS Options
#

# File containing the global certificate used for ALL services (imap,
pop3,
# lmtp, sieve)
#tls_cert_file: /etc/ssl/certs/ssl-cert-snakeoil.pem

# File containing the private key belonging to the global server
certificate.
#tls_key_file: /etc/ssl/private/ssl-cert-snakeoil.key

# File containing the certificate used for imap. If not specified, the
global
# certificate is used. A value of "disabled" will disable SSL/TLS for
imap.
#imap_tls_cert_file: /etc/ssl/certs/cyrus-imap.pem

# File containing the private key belonging to the imap-specific server
# certificate. If not specified, the global private key is used. A
value of
# "disabled" will disable SSL/TLS for imap.
#imap_tls_key_file: /etc/ssl/private/cyrus-imap.key

# File containing the certificate used for pop3. If not specified, the
global
# certificate is used. A value of "disabled" will disable SSL/TLS for
pop3.
#pop3_tls_cert_file: /etc/ssl/certs/cyrus-pop3.pem

# File containing the private key belonging to the pop3-specific server
# certificate. If not specified, the global private key is used. A

```

```
value of
# "disabled" will disable SSL/TLS for pop3.
#pop3_tls_key_file: /etc/ssl/private/cyrus-pop3.key

# File containing the certificate used for lmtp. If not specified, the
global
# certificate is used. A value of "disabled" will disable SSL/TLS for
lmtp.
#lmtp_tls_cert_file: /etc/ssl/certs/cyrus-lmtp.pem

# File containing the private key belonging to the lmtp-specific server
# certificate. If not specified, the global private key is used. A
value of
# "disabled" will disable SSL/TLS for lmtp.
#lmtp_tls_key_file: /etc/ssl/private/cyrus-lmtp.key

# File containing the certificate used for sieve. If not specified, the
global
# certificate is used. A value of "disabled" will disable SSL/TLS for
sieve.
#sieve_tls_cert_file: /etc/ssl/certs/cyrus-sieve.pem

# File containing the private key belonging to the sieve-specific server
# certificate. If not specified, the global private key is used. A
value of
# "disabled" will disable SSL/TLS for sieve.
#sieve_tls_key_file: /etc/ssl/private/cyrus-sieve.key

# File containing one or more Certificate Authority (CA) certificates.
#tls_ca_file: /etc/ssl/certs/cyrus-imapd-ca.pem

# Path to directory with certificates of CAs.
tls_ca_path: /etc/ssl/certs

# The length of time (in minutes) that a TLS session will be cached for
later
# reuse. The maximum value is 1440 (24 hours), the default. A value
of 0 will
# disable session caching.
tls_session_timeout: 1440

# The list of SSL/TLS ciphers to allow, in decreasing order of
precedence.
# The format of the string is described in ciphers(1). The Debian
default
# selects TLSv1 high-security ciphers only, and removes all anonymous
ciphers
# from the list (because they provide no defense against man-in-the-
middle
# attacks). It also orders the list so that stronger ciphers come
first.
tls_cipher_list: TLSv1+HIGH:!aNULL:@STRENGTH

# Require a client certificate for ALL services (imap, pop3, lmtp,
sieve).
#tls_require_cert: false

# Require a client certificate for imap ONLY.
#imap_tls_require_cert: false

# Require a client certificate for pop3 ONLY.
#pop3_tls_require_cert: false
```

```

# Require a client certificate for lmtp ONLY.
#lmtp_tls_require_cert: false

# Require a client certificate for sieve ONLY.
#sieve_tls_require_cert: false

#
# Cyrus Murder cluster configuration
#
# Set the following options to the values needed for this server to
# authenticate against the mupdate master server:
# mupdate_server
# mupdate_port
# mupdate_username
# mupdate_authname
# mupdate_realm
# mupdate_password
# mupdate_retry_delay

#AFM20ago2010
## Mupdate Server
mupdate_server: debian192_168_56_106
mupdate_username: mupdateuser
mupdate_authname: mupdateuser
mupdate_password: senha

##
## KEEP THESE IN SYNC WITH cyrus.conf
##
# Unix domain socket that lmtpd listens on.
lmtpsocket: /var/run/cyrus/socket/lmtp

# Unix domain socket that idled listens on.
idlesocket: /var/run/cyrus/socket/idle

# Unix domain socket that the new mail notification daemon listens on.
notifysocket: /var/run/cyrus/socket/notify

# Syslog prefix. Defaults to cyrus (so logging is done as cyrus/imap
etc.)
syslog_prefix: cyrus

##
## DEBUGGING
##
# Debugging hook. See /usr/share/doc/cyrus-common-
2.3/README.Debian.debug
# Keep the hook disabled when it is not in use
#
# gdb Back-traces
#debug_command: /usr/bin/gdb -batch -cd=/tmp -x /usr/lib/cyrus/get-
backtrace.gdb /usr/lib/cyrus/bin/%s %d >/tmp/gdb-
backtrace.cyrus.%1$s.%2$d <&- 2>&1 &
#
# system-call traces
#debug_command: /usr/bin/strace -tt -o /tmp/strace.cyrus.%s.%d -p %2$d

```

```

<&- 2>&l &
#
# library traces
#debug_command: /usr/bin/ltrace -tt -n 2 -o /tmp/ltrace.cyrus.%s.%d -p
%2$d <&- 2>&l &

#AFM 09mai2011 database formats
statuscache_db: skiplist
userdeny_db: skiplist
#AFM 09mai2011 debian defaults proved to have best performance
# cat /usr/lib/cyrus/cyrus-db-types.active
#annotation_db: skiplist
#duplicate_db: berkeley-nosync
#mboxlist_db: skiplist
#ptscache_db: berkeley
#quota_db: quotalegacy
#seenstate_db: skiplist
#subscription_db: flat
#tlscache_db: berkeley-nosync

# If enabled, this option forces the skiplist cyrusdb backend to
# always checkpoint when doing a recovery. This causes slightly
# more IO, but on the other hand leads to more efficient databases,
# and the entire file is already "hot".
#AFM 25ago2010
skiplist_always_checkpoint: 1

# If enabled, imapd, lmtpd and nntpd attempt to only write one copy
# of a message per partition and create hard links, resulting in a
# potentially large disk savings.
#AFM 25ago2010
singleinstancestore: 1

#AFM 24ago2010 para evitar travar frontend ao criar mbox sem
especificar onde
# Whitespace separated list of backend server names. Used for find-
# ing server with the most available free space for proxying CREATE.
serverlist: debian192_168_56_107 debian192_168_56_108

#AFM 24ago2010 para evitar criar mbox no frontend
# The backend server name used by default for new mailboxes. If not
# specified, the server with the most free space will be used for
# new mailboxes.
#AFM 03set2010 it works but we will try to leave dynamic commenting out
#defaultserver: debian192_168_56_107

#AFM 25ago2010 nao consegue mover cx postal sem autenticar mutuamente
# hostname_mechs: <none>
# Force a particular list of SASL mechanisms to be used when authen

```

```

# ticating to the backend server hostname (where hostname is the
# short hostname of the server in question). If it is not specified
# it will query the server for available mechanisms and pick one to
# use. - Cyrus Murder

# hostname_password: <none>
# The password to use for authentication to the backend server host
# name (where hostname is the short hostname of the server) - Cyrus
# Murder

debian192_168_56_107_authname: mupdateuser
debian192_168_56_107_password: senha
debian192_168_56_107_mechs: PLAIN
debian192_168_56_108_authname: mupdateuser
debian192_168_56_108_password: senha
debian192_168_56_108_mechs: PLAIN

#AFM 02set2010 trying to avoid pwd requests on mbx creation, as even
#AFM on backend issues a referral to itself at murder
proxyd_disable_mailbox_referrals: 1
sieve_allowreferrals: 0
proxyd_allow_status_referral: 0

```

Mupdate Master

Pacotes para o mupdate master

```

debian192_168_56_106:~# dpkg -i cyrus-murder-2.3_2.3.16-1_amd64.deb \
  cyrus-clients-2.3_2.3.16-1_amd64.deb \
  cyrus-common-2.3_2.3.16-1_amd64.deb \
  cyrus-admin-2.3_2.3.16-1_all.deb \
  libcyrus-imap-perl23_2.3.16-1_amd64.deb

```

Cópia de segurança dos arquivos de configuração

```

# mv /etc/cyrus.conf /etc/cyrus.conf.original
# mv /etc/imapd.conf /etc/imapd.conf.original

```

único mupdate master

```

# Debian defaults for Cyrus IMAP server/cluster implementation
# see cyrus.conf(5) for more information
#
# All the tcp services are tcpd-wrapped. see hosts_access(5)
#AFM 05out2010 mupdate master

START {
    # do not delete this entry!
    recover          cmd="/usr/sbin/ctl_cyrusdb -r"

    # this is only necessary if idlemethod is set to "idled" in
    # imapd.conf
    #AFM 20ago2010 pode ser necessario habilitar nos backends
    #idled           cmd="idled"

    # this is useful on backend nodes of a Murder cluster
    # it causes the backend to synchronize its mailbox list with

```

```

# the mupdate master upon startup
#mupdatepush cmd="/usr/sbin/ctl_mboxlist -m"

# this is recommended if using duplicate delivery suppression
#AFM 23ago2010 not for murder masters
#delprune cmd="/usr/sbin/cyr_expire -E 3"
# this is recommended if caching TLS sessions
#AFM 23ago2010 not for murder masters
#tlsprune cmd="/usr/sbin/tls_prune"
}

# UNIX sockets start with a slash and are absolute paths
# you can use a maxchild=# to limit the maximum number of forks of a
service
# you can use babysit=true and maxforkrate=# to keep tight tabs on the
service
# most services also accept -U (limit number of reuses) and -T (timeout)
SERVICES {
# --- Normal cyrus spool, or Murder backends ---
# add or remove based on preferences
#imap cmd="imapd -U 30" listen="imap" prefork=0
maxchild=100
#imaps cmd="imapd -s -U 30" listen="imaps" prefork=0
maxchild=100
#AFM 23ago2010 not for murder masters
#pop3 cmd="pop3d -U 30" listen="pop3" prefork=0
maxchild=50
#pop3s cmd="pop3d -s -U 30" listen="pop3s" prefork=0
maxchild=50
#AFM 23ago2010 not for murder masters
#nntp cmd="nntpd -U 30" listen="nntp" prefork=0
maxchild=100
#nntps cmd="nntpd -s -U 30" listen="nntps" prefork=0
maxchild=100

# At least one form of LMTP is required for delivery
# (you must keep the Unix socket name in sync with imap.conf)
#lmtpl cmd="lmtpl" listen="localhost:lmtpl" prefork=0
maxchild=20
#AFM 23ago2010 not for murder masters
#lmtplunix cmd="lmtpl" listen="/var/run/cyrus/socket/lmtpl"
prefork=0 maxchild=20
# -----

# useful if you need to give users remote access to sieve
# by default, we limit this to localhost in Debian
#AFM 23ago2010 not for murder masters
#sieve cmd="timsieved" listen="localhost:sieve"
prefork=0 maxchild=100

# this one is needed for the notification services
#AFM 23ago2010 not for murder masters
#notify cmd="notifyd"
listen="/var/run/cyrus/socket/notify" proto="udp" prefork=1

# --- Murder frontends -----
# enable these and disable the matching services above,
# except for sieve (which deals automatically with Murder)

# mupdate database service - must prefork at least 1
# (mupdate slaves)
#mupdate cmd="mupdate" listen=3905 prefork=1

```

```

        # (mupdate master, only one in the entire cluster)
#AFM 05out2010 ONLY for the single murder master
#AFM 05out2010 deployments may have maxchild 10000. babysit exceeds
maxchild + 1
#AFM deployments may have high prefork and maxforkrate for performance
tuning
#AFM parameters from master/service.c
#AFM -C: alternate config file
#AFM -U: max process uses
#AFM -T: reuse timeout
#AFM -D: call debugger
        # proxies that will connect to the backends
        #imap          cmd="proxyd" listen="imap" prefork=0
maxchild=100
        #imaps         cmd="proxyd -s" listen="imaps" prefork=0
maxchild=100
        #pop3          cmd="pop3proxyd" listen="pop3" prefork=0
maxchild=50
        #pop3s         cmd="pop3proxyd -s" listen="pop3s" prefork=0
maxchild=50
#AFM 30set2010
        #lmtpproxyd   cmd="lmtpproxyd" listen="lmtpproxyd" prefork=1
maxchild=20
        # -----

        # --- Murder master -----
#AFM 10dez2010 prefork from 4 to 1 or will download mbox for all 4
instances, timeout, fds from 1024 to 1024000
        mupdate       cmd="mupdate -m -T 1800" listen=3905 prefork=1
maxfds=1024000
        # -----
}

EVENTS {
        # this is required
#AFM 20ago2010 baixar para 5 minutos
#       checkpoint   cmd="/usr/sbin/ctl_cyrusdb -c" period=30
        checkpoint   cmd="/usr/sbin/ctl_cyrusdb -c" period=5

        # this is only necessary if using duplicate delivery suppression
delprune      cmd="/usr/sbin/cyr_expire -E 3" at=0401

        # this is only necessary if caching TLS sessions
tlsprune     cmd="/usr/sbin/tls_prune" at=0401

        # indexing of mailboxes for server side fulltext searches

        # reindex changed mailboxes (fulltext) approximately every
other hour
        #squatter_1   cmd="/usr/bin/nice -n 19 /usr/sbin/squatter -s"
period=120

        # reindex all mailboxes (fulltext) daily
        #squatter_a   cmd="/usr/sbin/squatter" at=0517

#AFM 17nov2010
        ## Expirar mensagens do delay Expunge
delprune     cmd="/usr/sbin/cyr_expire -X 14" at=0200

        ## Expirar pastas deletadas a mais de 14 dias
delprune     cmd="/usr/sbin/cyr_expire -D 14" at=0400

```

```
}  
</pre>/etc/imapd.conf no único mupdate master
```

```
# Debian Cyrus imapd.conf  
# See imapd.conf(5) for more information and more options  
#AFM 05out2010 mupdate master  
# Configuration directory  
configdirectory: /var/lib/cyrus  
  
# Which partition to use for default mailboxes  
#AFM 27ago2010 one MUST NOT define "defaultpartition" AND "partition-  
default"  
# at a proxy/frontend/mupdate or it will create mbx locally.  
#defaultpartition: default  
#AFM 31ago2010 cyrus doc says to use bogus partition on mupdate master  
#partition-default: /var/spool/cyrus/mail  
partition-default: /tmp  
  
#AFM 20ago2010 pode-se especificar diferentes particoes alternativas,  
por ex. UF  
#partition-ac: /var/spool/correio/ac  
#partition-al: /var/spool/correio/al  
#partition-am: /var/spool/correio/am  
#partition-ap: /var/spool/correio/ap  
#partition-ba: /var/spool/correio/ba  
#partition-ce: /var/spool/correio/ce  
#partition-df: /var/spool/correio/df  
  
#AFM 20ago2010 se usar diferentes particoes e  
# Para permitir a movimentacao entre backends  
#allowusermoves: yes  
  
#AFM 20ago2010  
# Colocado para compatibilizacao com Clientes para subscrever em caixas  
# pertencentes a diferentes backends  
#allowallsubscribe: 1  
  
#AFM 20ago2010  
# Eliminar mensagens duplicadas  
#duplicatesuppression: 1  
  
#AFM 20ago2010  
# Habilitar que as mensagens nao sejam deletadas  
# imediatamente e possam ser recuperadas.  
#expunge_mode: delayed  
  
# News setup  
partition-news: /var/spool/cyrus/news  
newsspool: /var/spool/news  
  
# Alternate namespace  
# If enabled, activate the alternate namespace as documented in  
# /usr/share/doc/cyrus-doc-2.3/html/altnamespace.html, where an user's  
# subfolders are in the same level as the INBOX  
# See also userprefix and sharedprefix on imapd.conf(5)  
altnamespace: no  
  
# UNIX Hierarchy Convention  
# Set to yes, and cyrus will accept dots in names, and use the forward  
# slash "/" to delimit levels of the hierarchy. This is done by
```

```

converting
# internally all dots to "^", and all "/" to dots. So the "rabbit.holes"
# mailbox of user "helmer.fudd" is stored in
"user.elmer^fud.rabbit^holes"
#AFM 12ago2010
#unixhierarchysep: no
unixhierarchysep: yes

# Rejecting illegal characters in headers
# Headers of RFC2882 messages must not have characters with the 8th bit
# set. However, too many badly-written MUAs generate this, including
most
# spamware. Enable this to reject such messages.
#reject8bit: yes

# Munging illegal characters in headers
# Headers of RFC2882 messages must not have characters with the 8th bit
# set. However, too many badly-written MUAs generate this, including
most
# spamware. If you kept reject8bit disabled, you can choose to leave the
# crappage untouched by disabling this (if you don't care that IMAP
SEARCH
# won't work right anymore.
#munge8bit: no

# Forcing recipient user to lowercase
# Cyrus 2.3 is case-sensitive. If all your mail users are in
lowercase, it is
# probably a very good idea to set lmtp_downcase_rcpt to true. This is
set by
# default, per RFC2821. This was not set by default in debian versions
up to
# and including 2.2.12-4.
lmtp_downcase_rcpt: yes

#AFM 20ago2010
# Setando este valor para 0 a mensagem de falha
# nao e enviada imediatamente ao cliente
lmtp_over_quota_perm_failure: 0

# Uncomment the following and add the space-separated users who
# have admin rights for all services.
#AFM 12ago2010
#admins: cyrus
#admins: cyrus techforce-admin cyrmaster mupdateuser
#AFM 27ago2010 mupdateuser could not create mboxs on frontend
#admins: cyrus techforce-admin cyrmaster cyrlmtp
#AFM 02set2010 trying to not ask for passwd on create mbx
admins: cyrus techforce-admin cyrmaster cyrlmtp mupdateuser

# Space-separated list of users that have lmtp "admin" status (i.e. that
# can deliver email through TCP/IP lmtp). If specified, this parameter
# overrides the "admins" parameter above
#lmtp_admins: postman
#AFM 20ago2010
lmtp_admins: mupdateuser postman

# Space-separated list of users that have mupdate "admin" status, in
# addition to those in the admins: entry above. Note that mupdate
slaves and
# backends in a Murder cluster need to authenticate against the mupdate
master

```

```

# as admin users.
#mupdate_admins: mupdateman
#AFM 20ago2010
mupdate_admins: mupdateman mupdateuser

# Space-separated list of users that have imapd "admin" status, in
# addition to those in the admins: entry above
#imap_admins: cyrus
#AFM 13out2010
imap_admins: cyrus mupdateuser techforce-admin

# Space-separated list of users that have sieve "admin" status, in
# addition to those in the admins: entry above
#sieve_admins: cyrus

# List of users and groups that are allowed to proxy for other users,
# seperated by spaces. Any user listed in this will be allowed to login
# for any other user. Like "admins:" above, you can have
imap_proxyservers
# and sieve_proxyservers.
#proxyservers: cyrus
#AFM 01out2010 you MUST NOT set proxyservers on frontends ONLY at
backends
#proxyservers: mupdateuser cyrus
proxy_authname: mupdateuser
proxy_password: senha

# No anonymous logins
allowanonymouslogin: no

# Minimum time between POP mail fetches in minutes
popminpoll: 1

# If nonzero, normal users may create their own IMAP accounts by
creating
# the mailbox INBOX. The user's quota is set to the value if it is
positive,
# otherwise the user has unlimited quota.
autocreatequota: 0

# umask used by Cyrus programs
umask: 077

# Sendmail binary location
# DUE TO A BUG, Cyrus sends CRLF EOLs to this program. This breaks Exim
3.
# For now, to work around the bug, set this to a wrapper that calls
# /usr/sbin/sendmail -dropcr instead if you use Exim 3.
#AFM 20ago2010
sendmail: /usr/sbin/sendmail

# If enabled, cyrdeliver will look for Sieve scripts in user's home
# directories: ~user/.sieve.
sieveusehomedir: false

# If sieveusehomedir is false, this directory is searched for Sieve
scripts.
sievedir: /var/spool/sieve

# notifyd(8) method to use for "MAIL" notifications. If not set, "MAIL"
# notifications are disabled. Valid methods are: null, log, zephyr
#mailnotifier: zephyr

```

```

# notifyd(8) method to use for "SIEVE" notifications.  If not set,
"SIEVE"
# notifications are disabled.  This method is only used when no method
is
# specified in the script.  Valid methods are null, log, zephyr, mailto
#sievenotifier: zephyr

# DRAC (pop-before-smtp, imap-before-smtp) support
# Set dracinterval to the time in minutes to call DRAC while a user is
# connected to the imap/pop services. Set to 0 to disable DRAC (default)
# Set drachost to the host where the rpc drac service is running
#dracinterval: 0
#drachost: localhost

# If enabled, the partitions will also be hashed, in addition to the
hashing
# done on configuration directories. This is recommended if one
partition has a
# very bushy mailbox tree.
hashimapspool: true

# Allow plaintext logins by default (SASL PLAIN)
allowplaintext: yes
# Mesmo colocando o metodo PLAIN a autenticacao e passada
# somente apos o STARTTLS que criptografa a comunicacao
# clientes usam o IMAPS

# Force PLAIN/LOGIN authentication only
# (you need to uncomment this if you are not using an auxprop-based SASL
# mechanism.  saslauthd users, that means you!). And pay attention to
# sasl_minimum_layer and allowapop below, too.
#sasl_mech_list: PLAIN
#AFM 12ago2010
sasl_mech_list: PLAIN

# Allow use of the POP3 APOP authentication command.
# Note that this command requires that the plaintext passwords are
# available in a SASL auxprop backend (eg. sasldb), and that the system
# can provide enough entropy (eg. from /dev/urandom) to create a
challenge
# in the banner.
#allowapop: no

# The minimum SSF that the server will allow a client to negotiate. A
# value of 1 requires integrity protection; any higher value requires
some
# amount of encryption.
#sasl_minimum_layer: 0
#AFM 12ago2010
sasl_minimum_layer: 0

# The maximum SSF that the server will allow a client to negotiate. A
# value of 1 requires integrity protection; any higher value requires
some
# amount of encryption.
#sasl_maximum_layer: 256

# List of remote realms whose users may log in using cross-realm
# authentications. Seperate each realm name by a space. A cross-realm
# identity is considered any identity returned by SASL with an "@" in
it.

```

```

# NOTE: To support multiple virtual domains on the same interface/IP,
# you need to list them all as loginrealms. If you don't list them here,
# (most of) your users probably won't be able to log in.
#loginrealms: example.com
#AFM 24ago2010
loginrealms: localhost techforce.com.br

# Enable virtual domain support. If enabled, the user's domain will
# be determined by splitting a fully qualified userid at the last '@'
# or '%' symbol. If the userid is unqualified, and the virtdomains
# option is set to "on", then the domain will be determined by doing
# a reverse lookup on the IP address of the incoming network
# interface, otherwise the user is assumed to be in the default
# domain (if set).
#AFM 20ago2010
virtdomains: userid

# The default domain for virtual domain support
# If the domain of a user can't be taken from its login and it can't
# be determined by doing a reverse lookup on the interface IP, this
# domain is used.
#defaultdomain:
#AFM 23ago2010
defaultdomain: techforce.com.br

#
# SASL library options (these are handled directly by the SASL
# libraries,
# refer to SASL documentation for an up-to-date list of these)
#

# The mechanism(s) used by the server to verify plaintext passwords.
# Possible
# values are "saslauthd", "auxprop", "pwcheck" and "alwaystrue". They
# are tried in order, you can specify more than one, separated by
# spaces.
#
# Do note that, since sasl will be run as user cyrus, you may have a
# lot of
# trouble to set this up right.
#AFM 20ago2010
#sasl_pwcheck_method: auxprop
sasl_pwcheck_method: saslauthd auxprop

# What auxpropd plugins to load, if using sasl_pwcheck_method: auxprop
# by default, all plugins are tried (which is probably NOT what you
# want).
#AFM 20ago2010
sasl_auxprop_plugin: sasldb

# If enabled, the SASL library will automatically create authentication
# secrets
# when given a plaintext password. Refer to SASL documentation
sasl_auto_transition: no

#
# SSL/TLS Options
#

```

```
# File containing the global certificate used for ALL services (imap,
pop3,
# lmtp, sieve)
#tls_cert_file: /etc/ssl/certs/ssl-cert-snakeoil.pem
#AFM 23ago2010 verificar local correto
#tls_cert_file: /etc/pki/tls/server.pem

# File containing the private key belonging to the global server
certificate.
#tls_key_file: /etc/ssl/private/ssl-cert-snakeoil.key
#AFM 23ago2010 verificar local correto
#tls_key_file: /etc/pki/tls/server.pem

# File containing the certificate used for imap. If not specified, the
global
# certificate is used. A value of "disabled" will disable SSL/TLS for
imap.
#imap_tls_cert_file: /etc/ssl/certs/cyrus-imap.pem

# File containing the private key belonging to the imap-specific server
# certificate. If not specified, the global private key is used. A
value of
# "disabled" will disable SSL/TLS for imap.
#imap_tls_key_file: /etc/ssl/private/cyrus-imap.key

# File containing the certificate used for pop3. If not specified, the
global
# certificate is used. A value of "disabled" will disable SSL/TLS for
pop3.
#pop3_tls_cert_file: /etc/ssl/certs/cyrus-pop3.pem

# File containing the private key belonging to the pop3-specific server
# certificate. If not specified, the global private key is used. A
value of
# "disabled" will disable SSL/TLS for pop3.
#pop3_tls_key_file: /etc/ssl/private/cyrus-pop3.key

# File containing the certificate used for lmtp. If not specified, the
global
# certificate is used. A value of "disabled" will disable SSL/TLS for
lmtp.
#lmtp_tls_cert_file: /etc/ssl/certs/cyrus-lmtp.pem

# File containing the private key belonging to the lmtp-specific server
# certificate. If not specified, the global private key is used. A
value of
# "disabled" will disable SSL/TLS for lmtp.
#lmtp_tls_key_file: /etc/ssl/private/cyrus-lmtp.key

# File containing the certificate used for sieve. If not specified, the
global
# certificate is used. A value of "disabled" will disable SSL/TLS for
sieve.
#sieve_tls_cert_file: /etc/ssl/certs/cyrus-sieve.pem

# File containing the private key belonging to the sieve-specific server
# certificate. If not specified, the global private key is used. A
value of
# "disabled" will disable SSL/TLS for sieve.
#sieve_tls_key_file: /etc/ssl/private/cyrus-sieve.key

# File containing one or more Certificate Authority (CA) certificates.
```

```

#tls_ca_file: /etc/pki/tls/certs/ca-bundle.crt
#AFM 23ago2010 verifical local correto
#tls_ca_file: /etc/ssl/certs/cyrus-imapd-ca.pem

# Path to directory with certificates of CAs.
tls_ca_path: /etc/ssl/certs

# The length of time (in minutes) that a TLS session will be cached for
later
# reuse. The maximum value is 1440 (24 hours), the default. A value
of 0 will
# disable session caching.
tls_session_timeout: 1440

# The list of SSL/TLS ciphers to allow, in decreasing order of
precedence.
# The format of the string is described in ciphers(1). The Debian
default
# selects TLSv1 high-security ciphers only, and removes all anonymous
ciphers
# from the list (because they provide no defense against man-in-the-
middle
# attacks). It also orders the list so that stronger ciphers come
first.
tls_cipher_list: TLSv1+HIGH:!aNULL:@STRENGTH

# Require a client certificate for ALL services (imap, pop3, lmtpl,
sieve).
#tls_require_cert: false

# Require a client certificate for imap ONLY.
#imap_tls_require_cert: false

# Require a client certificate for pop3 ONLY.
#pop3_tls_require_cert: false

# Require a client certificate for lmtpl ONLY.
#lmtpl_tls_require_cert: false

# Require a client certificate for sieve ONLY.
#sieve_tls_require_cert: false

#
# Cyrus Murder cluster configuration
#
# Set the following options to the values needed for this server to
# authenticate against the mupdate master server:
# mupdate_server
# mupdate_port
# mupdate_username
# mupdate_authname
# mupdate_realm
# mupdate_password
# mupdate_retry_delay

##
## KEEP THESE IN SYNC WITH cyrus.conf
##
# Unix domain socket that lmtpl listens on.
lmtplsocket: /var/run/cyrus/socket/lmtpl

# The idle backend to use for IDLE command.

```

```

# Options: poll (default), idled, no
# poll doesn't need the idled daemon and is supposed to be more robust.
# however it doesn't update as quickly as the idled backend does. "no"
# turns off IDLE support. If set to "idled", you will also need to
enable
# the "idled" entry in cyrus.conf.
#AFM 05out2010
idlemethod: idled

# Unix domain socket that idled listens on.
idlesocket: /var/run/cyrus/socket/idle

# Unix domain socket that the new mail notification daemon listens on.
notifysocket: /var/run/cyrus/socket/notify

# Syslog prefix. Defaults to cyrus (so logging is done as cyrus/imap
etc.)
syslog_prefix: cyrus

##
## DEBUGGING
##
# Debugging hook. See /usr/share/doc/cyrus-common-
2.3/README.Debian.debug
# Keep the hook disabled when it is not in use
#
# gdb Back-traces
#debug_command: /usr/bin/gdb -batch -cd=/tmp -x /usr/lib/cyrus/get-
backtrace.gdb /usr/lib/cyrus/bin/%s %d >/tmp/gdb-
backtrace.cyrus.%1$s.%2$d <&- 2>&1 &
#
# system-call traces
#debug_command: /usr/bin/strace -tt -o /tmp/strace.cyrus.%s.%d -p %2$d
<&- 2>&1 &
#
# library traces
#debug_command: /usr/bin/ltrace -tt -n 2 -o /tmp/ltrace.cyrus.%s.%d -p
%2$d <&- 2>&1 &

#AFM 09mai2011 database formats
statuscache_db: skiplist
userdeny_db: skiplist
#AFM 09mai2011 debian defaults proved to have best performance
# cat /usr/lib/cyrus/cyrus-db-types.active
#annotation_db: skiplist
#duplicate_db: berkeley-nosync
#mboxlist_db: skiplist
#ptscache_db: berkeley
#quota_db: quotalegacy
#seenstate_db: skiplist
#subscription_db: flat
#tlscache_db: berkeley-nosync

# If enabled, this option forces the skiplist cyrusdb backend to
# always checkpoint when doing a recovery. This causes slightly
# more IO, but on the other hand leads to more efficient databases,
# and the entire file is already "hot".
#AFM 25ago2010
skiplist_always_checkpoint: 1

# If enabled, imapd, lmtpd and nntpd attempt to only write one copy

```

```

# of a message per partition and create hard links, resulting in a
# potentially large disk savings.
#AFM 25ago2010
singleinstancestore: 1

#AFM 24ago2010 para evitar travar frontend ao criar mbox sem
especificar onde
# Whitespace separated list of backend server names. Used for find-
# ing server with the most available free space for proxying CREATE.
serverlist: debian192_168_56_107 debian192_168_56_108

#AFM 24ago2010 para evitar criar mbox no frontend
# The backend server name used by default for new mailboxes. If not
# specified, the server with the most free space will be used for
# new mailboxes.
#defaultserver: debian192_168_56_107

#AFM 01set2010 nao consegue mover cx postal sem autenticar mutuamente
# hostname_mechs: <none>
# Force a particular list of SASL mechanisms to be used when authen-
# ticating to the backend server hostname (where hostname is the
# short hostname of the server in question). If it is not specified
# it will query the server for available mechanisms and pick one to
# use. - Cyrus Murder

# hostname_password: <none>
# The password to use for authentication to the backend server host
# name (where hostname is the short hostname of the server) - Cyrus
# Murder

debian192_168_56_107_authname: mupdateuser
debian192_168_56_107_password: senha
debian192_168_56_107_mechs: PLAIN
debian192_168_56_108_authname: mupdateuser
debian192_168_56_108_password: senha
debian192_168_56_108_mechs: PLAIN

# You MUST set "mupdate_config: standard" and MUST NOT set
# "proxyservers: <proxyadmins>" at frontend in order to "defaultserver"
# and or "serverlist" take effect. Read imapd.c code, lines 4982 to
5008.
#AFM 27ago2010
mupdate_config: standard

#AFM 02set2010 tentativa de evitar pedir senha na criacao mbx no backend
mupdate_server: debian192_168_56_106
mupdate_username: mupdateuser
mupdate_authname: mupdateuser
mupdate_password: senha

#AFM 02set2010 trying to avoid pwd requests on mbx creation, as even
#AFM on backend issues a referral to itself at murder
#proxyd_disable_mailbox_referrals: 1
#sieve_allowreferrals: 0
#proxyd_allow_status_referral: 0

#AFM 05out2010 performance tuning
#mupdate_connections_max: 128
# The max number of connections that a mupdate process will allow,
this is
# related to the number of file descriptors in the mupdate process.

```

```
# Beyond this number connections will be immediately issued a BYE
response.
# mupdate_port: 3905
#mupdate_retry_delay: 20
#mupdate_workers_max: 50
# The maximum number of mupdate worker threads (overall)
#mupdate_workers_maxspare: 10
#mupdate_workers_min spare: 2
#mupdate_workers_start: 5
</pre>
```

Frontend

Pacotes para o frontend

```
debian192_168_56_105:~# dpkg -i cyrus-admin-2.3_2.3.16-1_all.deb
cyrus-clients-2.3_2.3.16-1_amd64.deb \
cyrus-common-2.3_2.3.16-1_amd64.deb \
libcyrus-imap-perl23_2.3.16-1_amd64.deb \
cyrus-imapd-2.3_2.3.16-1_amd64.deb \
cyrus-murder-2.3_2.3.16-1_amd64.deb
```

Cópia de segurança dos arquivos de configuração

```
# mv /etc/cyrus.conf /etc/cyrus.conf.original
# mv /etc/imapd.conf /etc/imapd.conf.original
```

/etc/cyrus.conf para frontend

SE FOR SEU CASO de não autenticar lmtmp, editar o /etc/cyrus.conf dos frontends para NÃO autenticar lmtmp.

```
#AFM 20111028 you should not stress mupdate master. use local db copy
by mupdate. reduced forkrate
    lmtmp          cmd="lmtpproxyd -a -T 30 -C /etc/lmtpd.conf"
listen="lmtmp" prefork=1
#AFM 20111028 parece precisar lmtpunix no frontend para murder e smtp
postfix. reduced forkrate
    lmtpunix      cmd="lmtpproxyd -a -T 30"
listen="/indicesimap/var/run/cyrus/socket/lmtmp" prefork=1 # Debian
defaults for Cyrus IMAP server/cluster implementation
# see cyrus.conf(5) for more information
#
# All the tcp services are tcpd-wrapped. see hosts_access(5)
#AFM 05out2010 frontend server

START {
    # do not delete this entry!
    recover          cmd="/usr/sbin/ctl_cyrusdb -r"

    # this is only necessary if idlemethod is set to "idled" in
imapd.conf
#AFM 05out2010 pode ser necessario habilitar
    idled           cmd="idled"
```

```

        # this is useful on backend nodes of a Murder cluster
        # it causes the backend to synchronize its mailbox list with
        # the mupdate master upon startup
#AFM 23ago2010
        #mupdatepush    cmd="/usr/sbin/ctl_mboxlist -m"

        # this is recommended if using duplicate delivery suppression
        delprune        cmd="/usr/sbin/cyr_expire -E 3"
        # this is recommended if caching TLS sessions
#AFM 20ago2010 pode não ser necessario
        tlsprune        cmd="/usr/sbin/tls_prune"
}

# UNIX sockets start with a slash and are absolute paths
# you can use a maxchild=# to limit the maximum number of forks of a
service
# you can use babysit=true and maxforkrate=# to keep tight tabs on the
service
# most services also accept -U (limit number of reuses) and -T (timeout)
SERVICES {
    # --- Normal cyrus spool, or Murder backends ---
    # add or remove based on preferences
#AFM 23ago2010 deixar apenas secao frontend
    # imap                cmd="imapd -U 30" listen="imap" prefork=0
maxchild=100
    #imap                cmd="imapd -U 30" listen="imap" prefork=0
maxchild=100 babysit=true
    #imaps               cmd="imapd -s -U 30" listen="imaps" prefork=0
maxchild=100
#AFM 23ago2010 deixar apenas secao frontend
    #pop3                cmd="pop3d -U 30" listen="pop3" prefork=0
maxchild=50
    #pop3s               cmd="pop3d -s -U 30" listen="pop3s" prefork=0
maxchild=50
#AFM 23ago2010 deixar apenas secao frontend
    #nntp                cmd="nntpd -U 30" listen="nntp" prefork=0
maxchild=100
    #nntps               cmd="nntpd -s -U 30" listen="nntps" prefork=0
maxchild=100

    # At least one form of LMTP is required for delivery
    # (you must keep the Unix socket name in sync with imap.conf)
    #lmtp                cmd="lmtpd" listen="localhost:lmtp" prefork=0
maxchild=20
#AFM 23ago2010 deixar apenas secao frontend
    #lmtpunix            cmd="lmtpd" listen="/var/run/cyrus/socket/lmtp"
prefork=0 maxchild=20
    # -----

    # useful if you need to give users remote access to sieve
    # by default, we limit this to localhost in Debian
#AFM 23ago2010 pode ficar com a secao frontend, leia mais adiante
#AFM 22nov2010 do not limit to localhost in a cyrus murder
    sieve                cmd="timsieved" listen="sieve" prefork=0
maxchild=100

    # this one is needed for the notification services
#AFM 23ago2010 deixar apenas secao frontend
    #notify              cmd="notifyd"
listen="/var/run/cyrus/socket/notify" proto="udp" prefork=1

    # --- Murder frontends -----

```

```

# enable these and disable the matching services above,
# except for sieve (which deals automatically with Murder)

# mupdate database service - must prefork at least 1
# (mupdate slaves)
#AFM 23ago2010 deixar apenas secao frontend
#AFM 05out2010 deployments may have maxchild
(mupdatemastermaxchilds/qty_frontends)
#AFM each lmtmp also connects to mupdate master
#AFM babysit exceeds maxchild + 1
#AFM deployments may have high prefork and maxforkrate
#AFM parameters from master/service.c
#AFM -C: alternate config file
#AFM -U: max process uses
#AFM -T: reuse timeout
#AFM -D: call debugger
mupdate cmd="mupdate" listen=3905 prefork=1 maxchild=100
maxforkrate=20 proto=tcp4 maxfds=256 -U 5 -T 10
# (mupdate master, only one in the entire cluster)
#mupdate cmd="mupdate -m" listen=3905 prefork=1

# proxies that will connect to the backends
#AFM 05out2010 deixar apenas secao frontend, one prefork at least
imap cmd="proxyd" listen="imap" prefork=1
maxchild=100 maxforkrate=2 proto=tcp4 maxfds=256 -U 5 -T 10
#AFM 24set2010
#imaps cmd="proxyd -s" listen="imaps" prefork=0
maxchild=100
#pop3 cmd="pop3proxyd" listen="pop3" prefork=0
maxchild=50
#pop3s cmd="pop3proxyd -s" listen="pop3s" prefork=0
maxchild=50
#AFM 05out2010 you should not stress mupdate master
lmtmp cmd="lmtpproxyd" listen="lmtmp" prefork=1
maxchild=20 maxforkrate=2 proto=tcp4 maxfds=256 -U 5 -T 10
#AFM 30set2010 parece precisar lmtmpunix no frontend para murder e smtp
postfix
lmtmpunix cmd="lmtpproxyd"
listen="/var/run/cyrus/socket/lmtmp" prefork=1 maxchild=20 maxforkrate=2
maxfds=256 -U 5 -T 10

# -----
}

EVENTS {
# this is required
#AFM 20ago2010 baixar para 5 minutos
# checkpoint cmd="/usr/sbin/ctl_cyrusdb -c" period=30
# checkpoint cmd="/usr/sbin/ctl_cyrusdb -c" period=5

# this is only necessary if using duplicate delivery suppression
delprune cmd="/usr/sbin/cyr_expire -E 3" at=0401

# this is only necessary if caching TLS sessions
tlsprune cmd="/usr/sbin/tls_prune" at=0401

# indexing of mailboxes for server side fulltext searches

# reindex changed mailboxes (fulltext) approximately every
other hour
#squatter_1 cmd="/usr/bin/nice -n 19 /usr/sbin/squatter -s"
period=120

```

```

# reindex all mailboxes (fulltext) daily
#squatter_a      cmd="/usr/sbin/squatter" at=0517

#AFM 17nov2010
## Expirar mensagens do delay Expunge
delprune         cmd="/usr/sbin/cyr_expire -X 14" at=0200

## Expirar pastas deletadas a mais de 14 dias
delprune         cmd="/usr/sbin/cyr_expire -D 14" at=0400
}
</pre>

```

/etc/imapd.conf em frontend

```

# Debian Cyrus imapd.conf
# See imapd.conf(5) for more information and more options
#AFM 05out2010 frontend server
# Configuration directory
configdirectory: /var/lib/cyrus

# Which partition to use for default mailboxes
#AFM 27ago2010 one MUST NOT define "defaultpartition" AND "partition-
default"
# at a proxy/frontend or it will create mbx locally.
#defaultpartition: default
partition-default: /var/spool/cyrus/mail

#AFM 20ago2010 pode-se especificar diferentes particoes alternativas,
por ex. UF
#partition-ac: /var/spool/correio/ac
#partition-al: /var/spool/correio/al
#partition-am: /var/spool/correio/am
#partition-ap: /var/spool/correio/ap
#partition-ba: /var/spool/correio/ba
#partition-ce: /var/spool/correio/ce
#partition-df: /var/spool/correio/df

#AFM 20ago2010 se usar diferentes particoes e
# Para permitir a movimentacao entre backends
allowusermoves: yes

#AFM 23ago2010
# Colocado para compatibilizacao com Clientes para subscrever em caixas
# pertencentes a diferentes backends
#allowallsubscribe: 1

#AFM 23ago2010
# Eliminar mensagens duplicadas
#duplicatesuppression: 1

#AFM 23ago2010
# Habilitar que as mensagens nao sejam deletadas
# imediatamente e possam ser recuperadas.
#expunge_mode: delayed

#AFM 23ago2010
# News setup
#partition-news: /var/spool/cyrus/news
#newspool: /var/spool/news

# Alternate namespace
# If enabled, activate the alternate namespace as documented in

```

```

# /usr/share/doc/cyrus-doc-2.3/html/altnamespace.html, where an user's
# subfolders are in the same level as the INBOX
# See also userprefix and sharedprefix on imapd.conf(5)
altnamespace: no

# UNIX Hierarchy Convention
# Set to yes, and cyrus will accept dots in names, and use the forward
# slash "/" to delimit levels of the hierarchy. This is done by
# converting
# internally all dots to "^", and all "/" to dots. So the "rabbit.holes"
# mailbox of user "helmer.fudd" is stored in
# "user.elmer^fud.rabbit^holes"
#AFM 12ago2010
#unixhierarchysep: no
unixhierarchysep: yes

# Rejecting illegal characters in headers
# Headers of RFC2882 messages must not have characters with the 8th bit
# set. However, too many badly-written MUAs generate this, including
# most
# spamware. Enable this to reject such messages.
#reject8bit: yes

# Munging illegal characters in headers
# Headers of RFC2882 messages must not have characters with the 8th bit
# set. However, too many badly-written MUAs generate this, including
# most
# spamware. If you kept reject8bit disabled, you can choose to leave the
# crappage untouched by disabling this (if you don't care that IMAP
# SEARCH
# won't work right anymore.
#munge8bit: no

# Forcing recipient user to lowercase
# Cyrus 2.3 is case-sensitive. If all your mail users are in
# lowercase, it is
# probably a very good idea to set lmtp_downcase_rcpt to true. This is
# set by
# default, per RFC2821. This was not set by default in debian versions
# up to
# and including 2.2.12-4.
lmtp_downcase_rcpt: yes

#AFM 20ago2010
# Setando este valor para 0 a mensagem de falha
# nao e enviada imediatamente ao cliente
lmtp_over_quota_perm_failure: 0

# Uncomment the following and add the space-separated users who
# have admin rights for all services.
#AFM 23ago2010
#admins: cyrus
#admins: cyrus techforce-admin cyrmaster mupdateuser cyrlmtp
#AFM 27ago2010 mupdateuser could not create mboxs on frontend
#admins: cyrus techforce-admin cyrmaster cyrlmtp
#AFM 02set2010 to not ask for passwd on create mbx
admins: cyrus techforce-admin cyrmaster cyrlmtp mupdateuser

# Space-separated list of users that have lmtp "admin" status (i.e. that
# can deliver email through TCP/IP lmtp). If specified, this parameter
# overrides the "admins" parameter above
#lmtp_admins: postman

```

```

#AFM 23ago2010
lmtp_admins: mupdateuser postman cyrlmtp

# Space-separated list of users that have mupdate "admin" status, in
# addition to those in the admins: entry above. Note that mupdate
slaves and
# backends in a Murder cluster need to authenticate against the mupdate
master
# as admin users.
#mupdate_admins: mupdateman
#AFM 20ago2010
mupdate_admins: mupdateman mupdateuser

# Space-separated list of users that have imapd "admin" status, in
# addition to those in the admins: entry above
#imap_admins: cyrus
#AFM 13out2010
imap_admins: cyrus mupdateuser techforce-admin

# Space-separated list of users that have sieve "admin" status, in
# addition to those in the admins: entry above
#sieve_admins: cyrus

# List of users and groups that are allowed to proxy for other users,
# seperated by spaces. Any user listed in this will be allowed to login
# for any other user. Like "admins:" above, you can have
imap_proxyservers
# and sieve_proxyservers.
#proxyservers: cyrus
#AFM 01out2010 you MUST NOT set proxyservers on frontends ONLY at
backends
#proxyservers: mupdateuser cyrus
proxy_authname: mupdateuser
proxy_password: senha

# No anonymous logins
allowanonymouslogin: no

# Minimum time between POP mail fetches in minutes
popminpoll: 1

# If nonzero, normal users may create their own IMAP accounts by
creating
# the mailbox INBOX. The user's quota is set to the value if it is
positive,
# otherwise the user has unlimited quota.
autocreatequota: 0

# umask used by Cyrus programs
umask: 077

# Sendmail binary location
# DUE TO A BUG, Cyrus sends CRLF EOLs to this program. This breaks Exim
3.
# For now, to work around the bug, set this to a wrapper that calls
# /usr/sbin/sendmail -dropcr instead if you use Exim 3.
#AFM 20ago2010
sendmail: /usr/sbin/sendmail

# If enabled, cyrdeliver will look for Sieve scripts in user's home
# directories: ~user/.sieve.
sieveusehomedir: false

```

```
# If sieveusehomedir is false, this directory is searched for Sieve
scripts.
sievedir: /var/spool/sieve

# notifyd(8) method to use for "MAIL" notifications. If not set, "MAIL"
# notifications are disabled. Valid methods are: null, log, zephyr
#mailnotifier: zephyr

# notifyd(8) method to use for "SIEVE" notifications. If not set,
"SIEVE"
# notifications are disabled. This method is only used when no method
is
# specified in the script. Valid methods are null, log, zephyr, mailto
#sievenotifier: zephyr

# DRAC (pop-before-smtp, imap-before-smtp) support
# Set dracinterval to the time in minutes to call DRAC while a user is
# connected to the imap/pop services. Set to 0 to disable DRAC (default)
# Set drachost to the host where the rpc drac service is running
#dracinterval: 0
#drachost: localhost

# If enabled, the partitions will also be hashed, in addition to the
hashing
# done on configuration directories. This is recommended if one
partition has a
# very bushy mailbox tree.
hashimapspool: true

# Allow plaintext logins by default (SASL PLAIN)
allowplaintext: yes
# Mesmo colocando o metodo PLAIN a autenticacao e passada
# somente apos o STARTTLS que criptografa a comunicacao
# clientes usam o IMAPS

# Force PLAIN/LOGIN authentication only
# (you need to uncomment this if you are not using an auxprop-based SASL
# mechanism. saslauthd users, that means you!). And pay attention to
# sasl_minimum_layer and allowapop below, too.
#sasl_mech_list: PLAIN
#AFM 12ago2010
sasl_mech_list: PLAIN

# Allow use of the POP3 APOP authentication command.
# Note that this command requires that the plaintext passwords are
# available in a SASL auxprop backend (eg. sasldb), and that the system
# can provide enough entropy (eg. from /dev/urandom) to create a
challenge
# in the banner.
#allowapop: no

# The minimum SSF that the server will allow a client to negotiate. A
# value of 1 requires integrity protection; any higher value requires
some
# amount of encryption.
#sasl_minimum_layer: 0
#AFM 12ago2010
sasl_minimum_layer: 0

# The maximum SSF that the server will allow a client to negotiate. A
# value of 1 requires integrity protection; any higher value requires
```

```

some
# amount of encryption.
#sasl_maximum_layer: 256

# List of remote realms whose users may log in using cross-realm
# authentications. Seperate each realm name by a space. A cross-realm
# identity is considered any identity returned by SASL with an "@" in
# it.
# NOTE: To support multiple virtual domains on the same interface/IP,
# you need to list them all as loginreals. If you don't list them here,
# (most of) your users probably won't be able to log in.
#loginrealms: example.com
#AFM 24ago2010
loginrealms: localhost techforce.com.br

# Enable virtual domain support.  If enabled, the user's domain will
# be determined by splitting a fully qualified userid at the last '@'
# or '%' symbol.  If the userid is unqualified, and the virdomains
# option is set to "on", then the domain will be determined by doing
# a reverse lookup on the IP address of the incoming network
# interface, otherwise the user is assumed to be in the default
# domain (if set).
#AFM 20ago2010
virdomains: userid

# The default domain for virtual domain support
# If the domain of a user can't be taken from its login and it can't
# be determined by doing a reverse lookup on the interface IP, this
# domain is used.
#defaultdomain:
#AFM 23ago2010
defaultdomain: techforce.com.br

#
# SASL library options (these are handled directly by the SASL
# libraries,
# refer to SASL documentation for an up-to-date list of these)
#

# The mechanism(s) used by the server to verify plaintext passwords.
# Possible
# values are "saslauthd", "auxprop", "pwcheck" and "alwaystrue".  They
# are tried in order, you can specify more than one, separated by
# spaces.
#
# Do note that, since sasl will be run as user cyrus, you may have a
# lot of
# trouble to set this up right.
#AFM 20ago2010
#sasl_pwcheck_method: auxprop
sasl_pwcheck_method: saslauthd auxprop

# What auxpropd plugins to load, if using sasl_pwcheck_method: auxprop
# by default, all plugins are tried (which is probably NOT what you
# want).
#AFM 20ago2010
sasl_auxprop_plugin: sasldb

# If enabled, the SASL library will automatically create authentication
# secrets
# when given a plaintext password. Refer to SASL documentation

```

```
sasl_auto_transition: no

#
# SSL/TLS Options
#

# File containing the global certificate used for ALL services (imap,
pop3,
# lmtp, sieve)
#tls_cert_file: /etc/ssl/certs/ssl-cert-snakeoil.pem

# File containing the private key belonging to the global server
certificate.
#tls_key_file: /etc/ssl/private/ssl-cert-snakeoil.key

# File containing the certificate used for imap. If not specified, the
global
# certificate is used. A value of "disabled" will disable SSL/TLS for
imap.
#imap_tls_cert_file: /etc/ssl/certs/cyrus-imap.pem

# File containing the private key belonging to the imap-specific server
# certificate. If not specified, the global private key is used. A
value of
# "disabled" will disable SSL/TLS for imap.
#imap_tls_key_file: /etc/ssl/private/cyrus-imap.key

# File containing the certificate used for pop3. If not specified, the
global
# certificate is used. A value of "disabled" will disable SSL/TLS for
pop3.
#pop3_tls_cert_file: /etc/ssl/certs/cyrus-pop3.pem

# File containing the private key belonging to the pop3-specific server
# certificate. If not specified, the global private key is used. A
value of
# "disabled" will disable SSL/TLS for pop3.
#pop3_tls_key_file: /etc/ssl/private/cyrus-pop3.key

# File containing the certificate used for lmtp. If not specified, the
global
# certificate is used. A value of "disabled" will disable SSL/TLS for
lmtp.
#lmtp_tls_cert_file: /etc/ssl/certs/cyrus-lmtp.pem

# File containing the private key belonging to the lmtp-specific server
# certificate. If not specified, the global private key is used. A
value of
# "disabled" will disable SSL/TLS for lmtp.
#lmtp_tls_key_file: /etc/ssl/private/cyrus-lmtp.key

# File containing the certificate used for sieve. If not specified, the
global
# certificate is used. A value of "disabled" will disable SSL/TLS for
sieve.
#sieve_tls_cert_file: /etc/ssl/certs/cyrus-sieve.pem

# File containing the private key belonging to the sieve-specific server
# certificate. If not specified, the global private key is used. A
value of
# "disabled" will disable SSL/TLS for sieve.
#sieve_tls_key_file: /etc/ssl/private/cyrus-sieve.key
```

```

# File containing one or more Certificate Authority (CA) certificates.
#tls_ca_file: /etc/ssl/certs/cyrus-imapd-ca.pem

# Path to directory with certificates of CAs.
tls_ca_path: /etc/ssl/certs

# The length of time (in minutes) that a TLS session will be cached for
later
# reuse. The maximum value is 1440 (24 hours), the default. A value
of 0 will
# disable session caching.
tls_session_timeout: 1440

# The list of SSL/TLS ciphers to allow, in decreasing order of
precedence.
# The format of the string is described in ciphers(1). The Debian
default
# selects TLSv1 high-security ciphers only, and removes all anonymous
ciphers
# from the list (because they provide no defense against man-in-the-
middle
# attacks). It also orders the list so that stronger ciphers come
first.
tls_cipher_list: TLSv1+HIGH:!aNULL:@STRENGTH

# Require a client certificate for ALL services (imap, pop3, lmtp,
sieve).
#tls_require_cert: false

# Require a client certificate for imap ONLY.
#imap_tls_require_cert: false

# Require a client certificate for pop3 ONLY.
#pop3_tls_require_cert: false

# Require a client certificate for lmtp ONLY.
#lmtp_tls_require_cert: false

# Require a client certificate for sieve ONLY.
#sieve_tls_require_cert: false

#
# Cyrus Murder cluster configuration
#
# Set the following options to the values needed for this server to
# authenticate against the mupdate master server:
# mupdate_server
# mupdate_port
# mupdate_username
# mupdate_authname
# mupdate_realm
# mupdate_password
# mupdate_retry_delay

#AFM20ago2010
## Mupdate Server
mupdate_server: debian192_168_56_106
mupdate_username: mupdateuser
mupdate_authname: mupdateuser
mupdate_password: senha

```

```

##
## KEEP THESE IN SYNC WITH cyrus.conf
##

# Unix domain socket that lmtpd listens on.
lmtpsocket: /var/run/cyrus/socket/lmtp

# The idle backend to use for IDLE command.
# Options: poll (default), idled, no
# poll doesn't need the idled daemon and is supposed to be more robust.
# however it doesn't update as quickly as the idled backend does. "no"
# turns off IDLE support. If set to "idled", you will also need to
enable
# the "idled" entry in cyrus.conf.
#AFM 05out2010
idlemethod: idled

# Unix domain socket that idled listens on.
idlesocket: /var/run/cyrus/socket/idle

# Unix domain socket that the new mail notification daemon listens on.
notifysocket: /var/run/cyrus/socket/notify

# Syslog prefix. Defaults to cyrus (so logging is done as cyrus/imap
etc.)
syslog_prefix: cyrus

#####

##
## DEBUGGING
##
# Debugging hook. See /usr/share/doc/cyrus-common-
2.3/README.Debian.debug
# Keep the hook disabled when it is not in use
#
# gdb Back-traces
#debug_command: /usr/bin/gdb -batch -cd=/tmp -x /usr/lib/cyrus/get-
backtrace.gdb /usr/lib/cyrus/bin/%s %d >/tmp/gdb-
backtrace.cyrus.%1$s.%2$d <&- 2>&1 &
#
# system-call traces
#debug_command: /usr/bin/strace -tt -o /tmp/strace.cyrus.%s.%d -p %2$d
<&- 2>&1 &
#
# library traces
#debug_command: /usr/bin/ltrace -tt -n 2 -o /tmp/ltrace.cyrus.%s.%d -p
%2$d <&- 2>&1 &

#####

#AFM 09mai2011 database formats
statuscache_db: skiplist

```

```

userdeny_db: skiplist
#AFM 09mai2011 debian defaults proved to have best performance
# cat /usr/lib/cyrus/cyrus-db-types.active
#annotation_db: skiplist
#duplicate_db: berkeley-nosync
#mboxlist_db: skiplist
#ptscache_db: berkeley
#quota_db: quotalegacy
#seenstate_db: skiplist
#subscription_db: flat
#tlscache_db: berkeley-nosync

# If enabled, this option forces the skiplist cyrusdb backend to
# always checkpoint when doing a recovery. This causes slightly
# more IO, but on the other hand leads to more efficient databases,
# and the entire file is already "hot".
#AFM 25ago2010
skiplist_always_checkpoint: 1

# If enabled, imapd, lmtpd and nntpd attempt to only write one copy
# of a message per partition and create hard links, resulting in a
# potentially large disk savings.
#AFM 25ago2010
singleinstancestore: 1

#AFM 23ago2010 Para Desabilitar o referral
#AFM 31ago2010 cyrus doc does not list this option for frontend...
#AFM 02set2010 trying to avoid pwd requests on mbx creation, as even
#AFM on backend issues a referral to itself at murder
proxyd_disable_mailbox_referrals: 1
sieve_allowreferrals: 0
proxyd_allow_status_referral: 0

#AFM 23ago2010 Nao enviar detalhes sobre o servidor
#serverinfo: off

#AFM 24ago2010 para evitar travar frontend ao criar mbox sem
especificar onde
# Whitespace separated list of backend server names. Used for find-
# ing server with the most available free space for proxying CREATE.
serverlist: debian192_168_56_107 debian192_168_56_108

#AFM 24ago2010 para evitar criar mbox no frontend
# The backend server name used by default for new mailboxes. If not
# specified, the server with the most free space will be used for
# new mailboxes.
#AFM 03set2010 it works but we will try to leave dynamic commenting out
#defaultserver: debian192_168_56_107

#AFM 25ago2010 nao consegue mover cx postal sem autenticar mutuamente
# hostname_mechs: <none>
# Force a particular list of SASL mechanisms to be used when authen
# ticating to the backend server hostname (where hostname is the
# short hostname of the server in question). If it is not specified
# it will query the server for available mechanisms and pick one to

```

```

# use. - Cyrus Murder

# hostname_password: <none>
# The password to use for authentication to the backend server host
# name (where hostname is the short hostname of the server) - Cyrus
# Murder

debian192_168_56_107_authname: mupdateuser
debian192_168_56_107_password: senha
debian192_168_56_107_mechs: PLAIN
debian192_168_56_108_authname: mupdateuser
debian192_168_56_108_password: senha
debian192_168_56_108_mechs: PLAIN

# You MUST set "mupdate_config: standard" and MUST NOT set
# "proxyservers: <proxyadmins>" at frontend in order to "defaultserver"
# and or "serverlist" take effect. Read imapd.c code, lines 4982 to
5008.
#AFM 01out2010
mupdate_config: standard

#AFM 05out2010 performance tuning
#mupdate_connections_max: 128
# The max number of connections that a mupdate process will allow,
this is
# related to the number of file descriptors in the mupdate process.
# Beyond this number connections will be immediately issued a BYE
response.
# mupdate_port: 3905
#mupdate_retry_delay: 20
#mupdate_workers_max: 50
# The maximum number of mupdate worker threads (overall)
#mupdate_workers_maxspare: 10
#mupdate_workers_min spare: 2
#mupdate_workers_start: 5

```

Postfix para frontends

O serviço smtp PODE estar em outras máquinas. Atenção em evitar comunicação via sockets nesse caso.

Em nosso exemplo instalamos no mesmo frontend do cyrus murder aggregator.

Em nosso exemplo usamos autenticação texto sasldb em vez de ldap, apenas para laboratório.

Pacotes para servidores com smtp postfix

```

#apt-get install postfix postfix-ldap libauthen-sasl-cyrus-perl \
libauthen-sasl-perl sasl2-bin libsasl2-modules libsasl2-2 \
libsasl2-modules-ldap /etc/postfix/imap_passwd nos

```

frontends

O conteúdo deste arquivo depende do parâmetro mailbox_transport no main.cf

```
192.168.56.105 mupdateuser:senha
```

Cyrus murder lmtpl ALWAYS require authentication, even if you configure smtp to NOT require it.
Or you will read at syslog

```
# Sep 28 21:33:53 debian192_168_56_105 postfix/lmtpl[2877]: 8B5AB3E043: to=<
usuario99@techforce.com.br>, relay=192.168.56.105[192.168.56.105]:24,
```

```
delay=46,          delays=46/0.06/0.15/0,          dsn=4.0.0,          status=deferred          (host
192.168.56.105[192.168.56.105] said: 430 Authentication required (in reply to MAIL FROM
```

```
command))
```

After config, generate the postmap db file:

```
debian192_168_56_105:~# postmap /etc/postfix/lmtpl_passwd
```

Test the authentication:

```
andremachado@debian192_168_56_105:~$ lmtpltest -a mupdateuser -u
mupdateuser debian192_168_56_105
```

```
techforce.com.br
```

```
pwcheck_method: saslauthd
saslauthd_path: /var/run/saslauthd
mech_list: PLAIN LOGIN
log_level: 7
```

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete
version
```

```
# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
```

```
#myorigin = /etc/mailname
```

```
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
```

```
biff = no
```

```
# appending .domain is the MUA's job.
```

```
append_dot_mydomain = no
```

```
# Uncomment the next line to generate "delayed mail" warnings
```

```
#delay_warning_time = 4h
```

```
readme_directory = no
```

```
# TLS parameters
```

```
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
```

```
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
```

```
smtpd_use_tls=yes
```

```

smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package
for
# information on enabling SSL in the smtp client.
myhostname = debian192_168_56_105
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = localdomain, localhost, localhost.localdomain,
localhost, techforce.com.br
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.56.105
mailbox_size_limit = 20000000
recipient_delimiter = +
inet_interfaces = all
myorigin = /etc/mailname
inet_protocols = ipv4
#AFM 28set2010 only for lab! not for production
# SASL SUPPORT FOR CLIENTS
# The following options set parameters needed by Postfix to enable
# Cyrus-SASL support for authentication of mail clients.
#
#smtpd_sasl_auth_enable = yes
#smtpd_sasl_security_options = noanonymous
#smtpd_sasl_local_domain = $myhostname
#broken_sasl_auth_clients = yes
relay_domains = $myorigin
#smtpd_recipient_restrictions = permit_mynetworks,
permit_sasl_authenticated, check_relay_domains
smtpd_recipient_restrictions = permit_mynetworks, check_relay_domains
#AFM
mailbox_transport = lmtp:inet:192.168.56.105:lmtp
#mailbox_transport = lmtp:inet:debian192_168_56_105:lmtp
#AFM 28sep 2010
# 550 5.1.1 <usuario99@techforce.com.br>: Recipient address rejected:
User unknown in local recipient table
# To turn off local recipient checking in the SMTP server, specify
# local_recipient_maps = (i.e. empty).
local_recipient_maps =
# Sep 28 21:33:53 debian192_168_56_105 postfix/lmtp[2877]: 8B5AB3E043:
to=<usuario99@techforce.com.br>,
# relay=192.168.56.105[192.168.56.105]:24, delay=46,
delays=46/0.06/0.15/0, dsn=4.0.0, status=deferred
# (host 192.168.56.105[192.168.56.105] said: 430 Authentication
required (in reply to MAIL FROM command))
#AFM 28sep2010 cyrus murder lmtp ALWAYS require authentication
# after config, run debian192_168_56_105:~# postmap
/etc/postfix/lmtp_passwd
# andremachado@debian192_168_56_105:~$ lmtptest -a mupdateuser -u
mupdateuser debian192_168_56_105
lmtp_sasl_auth_enable = yes
lmtp_sasl_password_maps = hash:/etc/postfix/lmtp_passwd
lmtp_sasl_security_options = noanonymous
lmtp_sasl_mechanism_filter = plain
#AFM 29set2010
lmtpd_recipient_restrictions = permit_mynetworks,
permit_sasl_authenticated
# andremachado@debian192_168_56_105:~$ imtest -v -m plain -a
mupdateuser -u usuario99 debian192_168_56_105
#AFM 01out2010
#debug_peer_level = 12/etc/postfix/master.cf para frontends

```

Mesmo que o smtp seja instalado noutra máquina, NÃO precisa alterar parâmetros de lmtmp para "inet".

Deixe como socket em chroot pois ele usa internamente, e o lmtmp será usado no mailbox_transport indicado no outro main.cf.

```
#
# Postfix master process configuration file. For details on the format
# of the file, see the master(5) manual page (command: "man 5 master").
#
# Do not forget to execute "postfix reload" after editing this file.
#
#
=====
==
# service type private unpriv chroot wakeup maxproc command + args
#          (yes)    (yes)    (yes)    (never) (100)
#
=====
==
#AFM 08out2010 verbose
smtp      inet n      -       -       -       -       smtpd -v
#submission inet n      -       -       -       -       smtpd
# -o smtpd_tls_security_level=encrypt
# -o smtpd_sasl_auth_enable=yes
# -o smtpd_client_restrictions=permit_sasl_authenticated,reject
# -o milter_macro_daemon_name=ORIGINATING
#smtps     inet n      -       -       -       -       smtpd
# -o smtpd_tls_wrappermode=yes
# -o smtpd_sasl_auth_enable=yes
# -o smtpd_client_restrictions=permit_sasl_authenticated,reject
# -o milter_macro_daemon_name=ORIGINATING
#628      inet n      -       -       -       -       qmqpd
pickup    fifo n      -       -       60      1       pickup
cleanup   unix n      -       -       -       0       cleanup
qmgr      fifo n      -       n       300     1       qmgr
#qmgr     fifo n      -       -       300     1       oqmgr
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
# When relaying mail as backup MX, disable fallback_relay to avoid MX
loops
relay     unix -      -       -       -       -       smtp
        -o smtp_fallback_relay=
#        -o smtp_helo_timeout=5 -o smtp_connect_timeout=5
showq     unix n      -       -       -       -       showq
error     unix -      -       -       -       -       error
retry     unix -      -       -       -       -       error
discard   unix -      -       -       -       -       discard
local     unix -      n       n       -       -       local
virtual   unix -      n       n       -       -       virtual
#AFM 08out2010 needs own socket to send out to remote inet, verbose
lmtmp     unix -      -       -       -       -       lmtmp -v
anvil     unix -      -       -       -       1       anvil
```

```

scache    unix -      -      -      -      1      scache
#
# =====
# Interfaces to non-Postfix software. Be sure to examine the manual
# pages of the non-Postfix software to find out what options it wants.
#
# Many of the following services use the Postfix pipe(8) delivery
# agent. See the pipe(8) man page for information about ${recipient}
# and other message envelope options.
# =====
#
# maildrop. See the Postfix MAILDROP_README file for details.
# Also specify in main.cf: maildrop_destination_recipient_limit=1
#
maildrop  unix -      n      n      -      -      pipe
         flags=DRhu user=vmail argv=/usr/bin/maildrop -d ${recipient}
#
# See the Postfix UUCP_README file for configuration details.
#
uucp      unix -      n      n      -      -      pipe
         flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail
($recipient)
#
# Other external delivery methods.
#
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}

```

Verificação de bancos de dados

Se algum banco de dados interno estiver corrompido em algum dos servidores, o cyrus murder/aggregator inteiro não vai funcionar corretamente.

Pode ficar errático, perder mensagens ou até caixas postais, ou simplesmente "emperrar" sem enviar ou receber mensagens sem motivo aparente.

Pior. Não vai avisar, ou registrar nos logs, a causa real.

Você TEM de verificar TODOS os logs de TODOS os servidores em busca de quaisquer erros a respeito dos bancos de dados internos.

Examine o `/var/log/syslog`, e todos os `/var/log/mail.*`.

Nem tente operar o cyrus murder/aggregator sem ter elevado grau de confiança na integridade nos arquivos de bancos de dados internos. Você perderia muito tempo depurando problemas em máquinas remotas, onde um problema em uma delas reflete em outras, com poucas ou nenhuma mensagem clara de log para orientar. O cyrus murder opera como um sistema integrado, com várias "partes móveis".

Por exemplo, se o `/var/lib/cyrus/deliver.db` estiver corrompido, o sistema SILENCIOSAMENTE não receberá mensagens, o LMTP não registrará erros e o SMTP apenas registrará "deferred" até que haja time-out.

Para o caso deste arquivo pode ser mais simples parar o serviço, mover o arquivo para uma área temporária e reiniciar o serviço, que então ele será recriado "sem registros de dados". Em seguida, examinar novamente os logs.

Os outros arquivos de bancos de dados devem ser recuperados de backups, pois o conserto deles é complexo, envolvendo vários comandos de verificação e reconstrução, conversão para texto flat, edição MANUAL e reconversão para binário.

Ou reconstrução a partir de dados que possam ser extraídos do próprio sistema de arquivos contendo as caixas postais. Nem todos os dados podem ser recuperados assim.

Num laboratório, pode ser mais simples parar os serviços, mover os corrompidos arquivos de dados para um local temporário, executar `cyrus-makedirs`, `cyrreconstruct`, reiniciar os serviços e deixar o cyrus recriar e ou repopular.

Configuração com LDAP

Em todas as máquinas

A autenticação será feita por LDAP, acessado por `saslauthd`.

Portanto, os usuários e senhas dos arquivos de configuração TEM de estar presentes no LDAP, tais como `mupdateuser` e o `techforce-admin`.

"techforce-admin" precisa ser incluído como "imap_admins:" nas configurações do `imapd.conf` para poder criar caixas postais.

`/etc/default/saslauthd`

```

#
# Settings for saslauthd daemon
# Please read /usr/share/doc/sasl2-bin/README.Debian for details.
#
# Should saslauthd run automatically on startup? (default: no)
#AFM 11out2010
START=yes
# Description of this saslauthd instance. Recommended.
# (suggestion: SASL Authentication Daemon)
DESC="SASL Authentication Daemon"
# Short name of this saslauthd instance. Strongly recommended.
# (suggestion: saslauthd)
NAME="saslauthd"
# Which authentication mechanisms should saslauthd use? (default: pam)
#
# Available options in this Debian package:
# getpwent -- use the getpwent() library function
# kerberos5 -- use Kerberos 5
# pam -- use PAM
# rimap -- use a remote IMAP server
# shadow -- use the local shadow password file
# sasldb -- use the local sasldb database file
# ldap -- use LDAP (configuration is in /etc/saslauthd.conf)
#
# Only one option may be used at a time. See the saslauthd man page
# for more information.
#
# Example: MECHANISMS="pam"
#AFM 11out2010
MECHANISMS="ldap"
# Additional options for this mechanism. (default: none)
# See the saslauthd man page for information about mech-specific
options.
MECH_OPTIONS=""
# How many saslauthd processes should we run? (default: 5)
# A value of 0 will fork a new process for each connection.
THREADS=5
# Other options (default: -c -m /var/run/saslauthd)
# Note: You MUST specify the -m option or saslauthd won't run!
#
# WARNING: DO NOT SPECIFY THE -d OPTION.
# The -d option will cause saslauthd to run in the foreground instead
of as
# a daemon. This will PREVENT YOUR SYSTEM FROM BOOTING PROPERLY. If you
wish
# to run saslauthd in debug mode, please run it by hand to be safe.
#
# See /usr/share/doc/sasl2-bin/README.Debian for Debian-specific
information.
# See the saslauthd man page and the output of 'saslauthd -h' for
general
# information about these options.
#
# Example for postfix users: "-c -m
/var/spool/postfix/var/run/saslauthd"
#AFM 07out2010 verbose
OPTIONS="-c -m /var/run/saslauthd -v"/etc/saslauthd.conf

ldap_servers: ldap://your_ldap_server_ip_address_or_name
ldap_port: 389
ldap_version: 3

```

```
ldap_referrals: no
ldap_search_base: dc=techforce,dc=com,dc=br
```

Testar a configuração LDAP e SASLAUTHD

Execute em TODAS as máquinas. Sem ao menos esses dois usuários e senhas configurados, não vai funcionar.

```
~# invoke-rc.d saslauthd restart
~# testsaslauthd -p senha -u mupdateuser
0: OK "Success."
~# testsaslauthd -p senha -u techforce-admin
0: OK "Success."
```

Nas máquinas que terão o SMTP Postfix

Nas máquinas que terão SMTP Postfix com LDAP, além das alterações já feitas, você terá de alterar conforme abaixo.

/etc/postfix/techforce-dominios

```
techforce.com.br OK
```

Crie o arquivo de mapeamentos:

```
#postmap /etc/postfix/techforce-dominios/etc/postfix/main.cf

# See /usr/share/postfix/main.cf.dist for a commented, more complete
version

# Debian specific:  Specifying a file name will cause the first
# line of that file to be used as the name.  The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

readme_directory = no

# TLS parameters
```

```

smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

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

myhostname = nuvem-postfix
#AFM 11out2010 ldap does not have local aliases. leave empty
#alias_maps = hash:/etc/aliases
#alias_database = hash:/etc/aliases
alias_maps =
#AFM 11out2010
mydestination = localdomain, localhost, localhost.localdomain,
localhost, $myhostname, $myhostname.techforce.com.br, techforce.com.br
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 10.200.113.228
mailbox_size_limit = 20000000
recipient_delimiter = +
inet_interfaces = all
myorigin = /etc/mailname
inet_protocols = ipv4

#AFM 28set2010 only for lab! not for production
# SASL SUPPORT FOR CLIENTS
# The following options set parameters needed by Postfix to enable
# Cyrus-SASL support for authentication of mail clients.
#
#smtpd_sasl_auth_enable = yes
#smtpd_sasl_security_options = noanonymous
#smtpd_sasl_local_domain = $myhostname
#broken_sasl_auth_clients = yes

relay_domains = $myorigin
#smtpd_recipient_restrictions = permit_mynetworks,
permit_sasl_authenticated, check_relay_domains
smtpd_recipient_restrictions = permit_mynetworks, check_relay_domains

#AFM
mailbox_transport = lmtp:inet:10.200.113.219:lmtp
#mailbox_transport = lmtp:inet:nuvem-cyrus-pr:lmtp

#AFM 11out2010
# Avoid errors "Recipient address rejected: User unknown in local
recipient table"
# To turn off local recipient checking in the SMTP server, specify
# local_recipient_maps = (i.e. empty).
local_recipient_maps =

#AFM 11out2010 avoid errors "status=deferred" 430 authentication
required
#AFM 28sep2010 cyrus murder lmtp ALWAYS require authentication
#AFM 28sep2010 after config, run ~# postmap /etc/postfix/lmtp_passwd
#AFM 28sep2010 test with something like
#AFM ~$ lmtptest -a mupdateuser -u mupdateuser debian192_168_56_105

lmtp_sasl_auth_enable = yes
lmtp_sasl_password_maps = hash:/etc/postfix/lmtp_passwd

```

```

lmtp_sasl_security_options = noanonymous

lmtp_sasl_mechanism_filter = plain

#AFM 29set2010
#lmtpd_recipient_restrictions = permit_mynetworks,
permit_sasl_authenticated
#AFM 07out2010
lmtpd_recipient_restrictions = permit_sasl_authenticated

# ~$ imtest -v -m plain -a mupdateuser -u usuario99 debian192_168_56_105

#AFM 01out2010
#debug_peer_level = 12

#AFM 11out2010 parametros do arquivo do techforce
#append_at_myorigin = no
unknown_local_recipient_reject_code = 450
disable_dns_lookups = no

virtual_alias_maps = ldap:aliasas, ldap:mailboxes, ldap:grupos,
ldap:listas, ldap:cxinstitucionais

#Caixas Postais
mailboxes_server_host = 10.200.113.217
# host do servidor LDAP.
mailboxes_version = 3
# versao do ldap
mailboxes_timeout = 10
# tempo em segundo para gerar um timeout na consulta
mailboxes_chase_referral = 0
# seguir referral? (false = 0 = nao)
mailboxes_search_base = dc=techforce,dc=com,dc=br
#Base do servidor LDAP.
mailboxes_query_filter =
(&(|(mail=%s)(mailAlternateAddress=%s))(objectClass=posixAccount)(phpgwA
ccountType=u)(accountStatus=active))
# A pesquisa que sera feita. Será retornado o UID e o
MailForwardingAddress (result_attribute) da Entrada
# correspondente ao query_filter. %s eh oq vem do postfix.
mailboxes_bind = no
mailboxes_domain = hash:/etc/postfix/techforce-dominios
# utilizar anonymous.
mailboxes_result_attribute = uid, mailForwardingAddress
# o LDAP retornará estes atributos.

#Aliasas
aliasas_server_host = 10.200.113.217
aliasas_version = 3
aliasas_timeout = 10
aliasas_chase_referral = 0
aliasas_search_base = dc=techforce,dc=com,dc=br
aliasas_query_filter =
(&(|(mail=%s)(mailAlternateAddress=%s))(objectClass=posixAccount)(phpgwA
ccountType=u)(deliveryMode=forwardOnly)(accountStatus=active))
aliasas_domain = hash:/etc/postfix/techforce-dominios
aliasas_result_attribute = mailForwardingAddress

#Listas
listas_server_host = 10.200.113.217
listas_version = 3

```

```

listas_timeout = 10
listas_chase_referral = 0
listas_search_base = dc=techforce,dc=com,dc=br
listas_query_filter =
(&(mail=%s)(phpgwAccountType=l)(objectClass=posixAccount)(deliveryMode=f
orwardOnly)(accountStatus=active))
listas_domain = hash:/etc/postfix/techforce-dominios
listas_result_attribute = mailForwardingAddress

#Grupos
grupos_server_host = 10.200.113.217
grupos_version = 3
grupos_timeout = 10
grupos_chase_referral = 0
grupos_search_base = dc=techforce,dc=com,dc=br
grupos_query_filter =
(&(cn=%u)(objectClass=posixGroup)(phpgwAccountType=g))
grupos_bind = no
grupos_domain = hash:/etc/postfix/techforce-dominios
grupos_result_attribute = memberUid

#Contas institucionais
cxinstitucionais_server_host = 10.200.113.217
cxinstitucionais_version = 3
cxinstitucionais_timeout = 10
cxinstitucionais_chase_referral = 0
cxinstitucionais_search_base = dc=techforce,dc=com,dc=br
cxinstitucionais_query_filter =
(&(mail=%s)(mailAlternateAddress=%s)(objectClass=phpgwAccount)(phpgwA
ccountType=i)(accountStatus=active))
cxinstitucionais_domain = hash:/etc/postfix/techforce-dominios
cxinstitucionais_result_attribute = mailForwardingAddress

#####
# CONTROLE DE FALHA DE ENTREGA.

# O tempo entre as tentativas de entrega da fila.
# The time between deferred queue scans by the queue manager.
queue_run_delay = 480s

# The maximal time a bounce message is queued before it is considered
undeliverable.
bounce_queue_lifetime = 5400s
#2400

# O tempo maximo que uma mensagem fica na fila de adiadas, antes de
voltar ao sender.
# How long a message stays in the queue before it is sent back as
undeliverable.
maximal_queue_lifetime = 5400s
#2400

# O tempo maxima entre tentativas de entregar uma mensagem adiada
(deferida)
# The maximal time between attempts to deliver a deferred message.
maximal_backoff_time = 480s

# O tempo minimo entre tentativas de entregar uma mensagem adiada
(deferida)
# The minimal time between attempts to deliver a deferred message.
minimal_backoff_time = 240s

```

TESTES (parte 1)

SMTP

As máquinas que possuem SMTP Postfix são bons pontos para fazer os testes de conexão e envio de mensagens.

São um dos pontos de contato com os programas externos. Os mesmos comandos podem ser usados em outras máquinas caso seja necessário isolar algum problema.

O protocolo LMTP é usado para comunicações "internas" entre as máquinas participantes do murder e com as máquinas com o SMTP. O protocolo SMTP é usado para comunicar-se com servidores e clientes "externos".

É preferível usar netcat (nc) ao invés de telnet, pois trata melhor erros e lida melhor com problemas de comunicação sem ficar preso.

```
nuvem-postfix:/etc/postfix# nc nuvem-postfix 25
220 nuvem-postfix ESMTP Postfix (Debian/GNU)
ehlo nuvem-postfix
250-nuvm-postfix
250-PIPELINING
250-SIZE 10240000
250-VERFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
mail from:<testesmtpl>
250 2.1.0 Ok
rcpt to:<techforce-admin@techforce.com.br>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: teste smtp nrol
teste
.
250 2.0.0 Ok: queued as 6C44161F7E
quit
221 2.0.0 Bye
nuvem-postfix:/etc/postfix#
```

LMTP

O protocolo LMTP é usado para comunicações "internas" entre as máquinas participantes do murder e com as máquinas com o SMTP. O protocolo SMTP é usado para comunicar-se com servidores e clientes "externos".

Os mesmos comandos podem ser usados em outras máquinas caso seja necessário isolar

algum problema.

O protocolo lmtptem TOLERÂNCIA ZERO para desvios do formato RFC. Digite EXATAMENTE formatado como abaixo, maiúsculas, minúsculas, pontuação e

ESPAÇOS exatos. O endereço origem não precisa existir. Mas o endereço destino TEM de estar funcionando corretamente, pois durante o comando faz a verificação do destinatário ANTES de terminar a mensagem. Se houver problema de conexão ou configuração, não vai aparecer a resposta "250 2.1.5 ok"

```
RCPT TO:<techforce-admin@techforce.com.br>
250 2.1.5 ok
```

Depois de "354 go ahead" é uma nova linha. Cuidado com espaços em branco no final das linhas. Finaliza a sessão com um "." sozinho na última linha.

```
nuvem-postfix:/etc/postfix# lmtptest -a mupdateuser -u mupdateuser
nuvem-cyrus-pr
S: 220 nuvem-cyrus-pr Cyrus LMTP Murder v2.3.16-Debian-2.3.16-1 server
ready
C: LHLO lmtptest
S: 250-nuvm-cyrus-pr
S: 250-8BITMIME
S: 250-ENHANCEDSTATUSCODES
S: 250-PIPELINING
S: 250-SIZE
S: 250-STARTTLS
S: 250-AUTH PLAIN
S: 250 IGNOREQUOTA
Please enter your password:
C: AUTH PLAIN bXVwZGF0ZXVzZXIAbXVwZGF0ZXVzZXIAC2VuaGE=
S: 235 Authenticated!
Authenticated.
Security strength factor: 0
MAIL FROM:<TESTELMTP1>
250 2.1.0 ok
RCPT TO:<techforce-admin@techforce.com.br>
250 2.1.5 ok
DATA
354 go ahead
Subject: teste lmtpl
testel
.
250 2.1.5 Ok
quit
221 2.0.0 bye
Connection closed.
nuvem-postfix:/etc/postfix#
```

IMAP

Testar a conexão não segura via imtest pois via telnet ou netcat não faz negociação e não se pode ver nada:

```

nuvem-cyrus-pr:~# imtest -v -m plain -a techforce-
admin@techforce.com.br -u techforce-admin@techforce.com.br nuvem-cyrus-
pr
S: * OK [CAPABILITY IMAP4 IMAP4rev1 LITERAL+ ID MUPDATE=mupdate://nuvem-
cyrus-mu/ STARTTLS AUTH=PLAIN SASL-IR
COMPRESS=DEFLATE] nuvem-cyrus-pr Cyrus IMAP Murder v2.3.16-Debian-
2.3.16-1 server ready
Please enter your password:
C: A01 AUTHENTICATE PLAIN
ZXhwcmVzc28tYWRtaW5AZXhwcmVzc28uZ292LmJyAGV4cHJlc3NvLWFkbWluQGV4cHJlc3Nv
Lmdvdi5icgBzZW5oYQ==
S: A01 OK [CAPABILITY IMAP4 IMAP4rev1 LITERAL+ ID
MUPDATE=mupdate://nuvem-cyrus-mu/ LOGINDISABLED COMPRESS=DEFLATE
ACL RIGHTS=kxte QUOTA MAILBOX-REFERRALS NAMESPACE UIDPLUS
NO_ATOMIC_RENAME UNSELECT CHILDREN MULTIAPPEND BINARY
SORT SORT=MODSEQ THREAD=ORDEREDSUBJECT THREAD=REFERENCES ANNOTATEMORE
CATENATE CONDSTORE SCAN IDLE
URLAUTH] Success (no protection)
Authenticated.
Security strength factor: 0
1 select inbox
* FLAGS (\Answered \Flagged \Draft \Deleted \Seen)
* OK [PERMANENTFLAGS (\Answered \Flagged \Draft \Deleted \Seen \*)]
* 3 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1286830893]
* OK [UIDNEXT 4]
* OK [NOMODSEQ] Sorry, modsequences have not been enabled on this
mailbox
* OK [URLMECH INTERNAL]
1 OK [READ-WRITE] Completed
2 logout
* BYE LOGOUT received
2 OK Completed
Connection closed.
nuvem-cyrus-pr:~#

```

TLS e SSL

Quando o php executa funções imap em um servidor diferente de onde está, requer segurança melhorada.

Sem conexão segura, funções php para criar caixas postais falharão com uma mensagem citando algo como "insecure server advertised AUTH=PLAIN", embora seja um warning e não um erro fatal.

Será preciso configurar TLS e SSL, para que o Techforce possa usar encriptação e conexão segura já iniciando na porta 143 (no menu de configuração do servidor de correio IMAP).

Você precisará configurar os IMAP frontends para conexão segura.

/etc/cyrus.conf para frontends

Habilitar a seguinte linha

```
#AFM 13out2010
    imaps cmd="proxyd -s" listen="imaps" prefork=1 maxchild=100
maxforkrate=2 proto=tcp4 maxfds=256 -U 5 -T 10
```

Ficará assim:

```
# Debian defaults for Cyrus IMAP server/cluster implementation
# see cyrus.conf(5) for more information
#
# All the tcp services are tcpd-wrapped. see hosts_access(5)
#AFM 05out2010 frontend server

START {
    # do not delete this entry!
    recover cmd="/usr/sbin/ctl_cyrusdb -r"

    # this is only necessary if idlemethod is set to "idled" in
imapd.conf
#AFM 05out2010 pode ser necessario habilitar
    idled cmd="idled"

    # this is useful on backend nodes of a Murder cluster
    # it causes the backend to synchronize its mailbox list with
    # the mupdate master upon startup
#AFM 23ago2010
    #mupdatepush cmd="/usr/sbin/ctl_mboxlist -m"

    # this is recommended if using duplicate delivery suppression
    delprune cmd="/usr/sbin/cyr_expire -E 3"
    # this is recommended if caching TLS sessions
#AFM 20ago2010 pode não ser necessario
    tlsprune cmd="/usr/sbin/tls_prune"
}

# UNIX sockets start with a slash and are absolute paths
# you can use a maxchild=# to limit the maximum number of forks of a
service
# you can use babysit=true and maxforkrate=# to keep tight tabs on the
service
# most services also accept -U (limit number of reuses) and -T (timeout)
SERVICES {
    # --- Normal cyrus spool, or Murder backends ---
    # add or remove based on preferences
#AFM 23ago2010 deixar apenas secas frontend
#    imap cmd="imapd -U 30" listen="imap" prefork=0
maxchild=100
#    #imap cmd="imapd -U 30" listen="imap" prefork=0
maxchild=100 babysit=true
#    #imaps cmd="imapd -s -U 30" listen="imaps" prefork=0
maxchild=100
#AFM 23ago2010 deixar apenas secas frontend
#    #pop3 cmd="pop3d -U 30" listen="pop3" prefork=0
maxchild=50
#    #pop3s cmd="pop3d -s -U 30" listen="pop3s" prefork=0
maxchild=50
#AFM 23ago2010 deixar apenas secas frontend
#    #nntp cmd="nntpd -U 30" listen="nntp" prefork=0
```

```

maxchild=100
#nntps          cmd="nntpd -s -U 30" listen="nntps" prefork=0
maxchild=100

# At least one form of LMTP is required for delivery
# (you must keep the Unix socket name in sync with imap.conf)
#lmt           cmd="lmtpd" listen="localhost:lmtp" prefork=0
maxchild=20
#AFM 23ago2010 deixar apenas secas frontend
#lmtunix       cmd="lmtpd" listen="/var/run/cyrus/socket/lmtp"
prefork=0 maxchild=20
# -----

# useful if you need to give users remote access to sieve
# by default, we limit this to localhost in Debian
#AFM 23ago2010 pode ficar com a secas frontend, leia mais adiante
#AFM 22nov2010 do not limit to localhost in a cyrus murder
sieve          cmd="timsieved" listen="sieve" prefork=0
maxchild=100

# this one is needed for the notification services
#AFM 23ago2010 deixar apenas secas frontend
#notify        cmd="notifyd"
listen="/var/run/cyrus/socket/notify" proto="udp" prefork=1

# --- Murder frontends -----
# enable these and disable the matching services above,
# except for sieve (which deals automatically with Murder)

# mupdate database service - must prefork at least 1
# (mupdate slaves)
#AFM 23ago2010 deixar apenas secas frontend
#AFM 05out2010 deployments may have maxchild
(mupdatemastermaxchilds/qty_frontends)
#AFM each lmt also connects to mupdate master
#AFM babysit exceeds maxchild + 1
#AFM deployments may have high prefork and maxforkrate
#AFM parameters from master/service.c
#AFM -C: alternate config file
#AFM -U: max process uses
#AFM -T: reuse timeout
#AFM -D: call debugger
#AFM 08out2010
mupdate        cmd="mupdate" listen=3905 prefork=1 maxchild=100
maxforkrate=20 proto=tcp4 maxfds=256 -U 5 -T 10
# mupdate      cmd="mupdate" listen=3905 prefork=1 maxchild=100
# (mupdate master, only one in the entire cluster)
#mupdate       cmd="mupdate -m" listen=3905 prefork=1

# proxies that will connect to the backends
#AFM 08out2010 deixar apenas secas frontend, one prefork at least
imap           cmd="proxyd" listen="imap" prefork=1
maxchild=100 maxforkrate=2 proto=tcp4 maxfds=256 -U 5 -T 10
# imap        cmd="proxyd" listen="imap" prefork=1
maxchild=100
#AFM 13out2010
imaps          cmd="proxyd -s" listen="imaps" prefork=1
maxchild=100 maxforkrate=2 proto=tcp4 maxfds=256 -U 5 -T 10
#pop3          cmd="pop3proxyd" listen="pop3" prefork=0
maxchild=50
#pop3s        cmd="pop3proxyd -s" listen="pop3s" prefork=0
maxchild=50

```

```

#AFM 08out2010 you should not stress mupdate master
    lmtplib          cmd="lmtplibproxyd" listen="lmtplib" prefork=1
maxchild=20 maxforkrate=2 proto=tcp4 maxfds=256 -U 5 -T 10
#AFM 07out2010
#    lmtplib          cmd="lmtplibproxyd" listen="lmtplib" prefork=1
maxchild=20
#AFM 30set2010 parece precisar lmtplibunix no frontend para murder e smtp
postfix
#    lmtplibunix      cmd="lmtplibproxyd"
listen="/var/run/cyrus/socket/lmtplib" prefork=1 maxchild=20 maxforkrate=2
maxfds=256 -U 5 -T 10
#AFM 08out2010
#lmtplibunix          cmd="lmtplibproxyd"
listen="/var/run/cyrus/socket/lmtplib" prefork=1 maxchild=20

# -----
}

EVENTS {
# this is required
#AFM 20ago2010 baixar para 5 minutos
#    checkpoint      cmd="/usr/sbin/ctl_cyrusdb -c" period=30
#    checkpoint      cmd="/usr/sbin/ctl_cyrusdb -c" period=5

# this is only necessary if using duplicate delivery suppression
delprune             cmd="/usr/sbin/cyr_expire -E 3" at=0401

# this is only necessary if caching TLS sessions
tlsprune             cmd="/usr/sbin/tls_prune" at=0401

# indexing of mailboxes for server side fulltext searches

# reindex changed mailboxes (fulltext) approximately every
other hour
#squatter_1         cmd="/usr/bin/nice -n 19 /usr/sbin/squatter -s"
period=120

# reindex all mailboxes (fulltext) daily
#squatter_a         cmd="/usr/sbin/squatter" at=0517

#AFM 17nov2010
## Expirar mensagens do delay Expunge
delprune             cmd="/usr/sbin/cyr_expire -X 14" at=0200

## Expirar pastas deletadas a mais de 14 dias
delprune             cmd="/usr/sbin/cyr_expire -D 14" at=0400
}
</pre>/etc/imapd.conf para frontends

```

Se você não conseguir conectar seguramente, e encontrar nos logs mensagens de erro como:

```
Fatal error: imaps: required OpenSSL options not present
```

Então precisa descomentar as linhas sobre certificados no /etc/imapd.conf:

```
# File containing the global certificate used for ALL services (imap,
pop3,
# lmtp, sieve)
tls_cert_file: /etc/ssl/certs/ssl-cert-snakeoil.pem
# File containing the private key belonging to the global server
certificate.
tls_key_file: /etc/ssl/private/ssl-cert-snakeoil.key
```

Se você se deparar com erros como os abaixo:

```
Oct 13 12:18:38 nuvem-cyrus-pr cyrus/imap[31365]: unable to get
private key from '/etc/ssl/private/ssl-cert-snakeoil.key'
Oct 13 12:18:38 nuvem-cyrus-pr cyrus/imap[31365]: TLS server engine:
cannot load cert/key data, may be a cert/key mismatch?
Oct 13 12:18:38 nuvem-cyrus-pr cyrus/imap[31365]: error initializing
TLS
Oct 13 12:18:38 nuvem-cyrus-pr cyrus/imap[31365]: Fatal error:
tls_init() failed
```

Então é preciso recriar os certificados snakeoil devido a erros de data (ainda sem ntp) no momento de instalação do cyrus

```
# make-ssl-cert generate-default-snakeoil --force-overwrite
```

Erros similares a:

```
Oct 13 12:37:16 nuvem-cyrus-pr cyrus/imap[31679]: Fatal error:
tls_start_servertls() failed
```

Indicam que precisa incluir usuário cyrus no grupo ssl-cert para poder ler os certificados

```
~# adduser cyrus ssl-cert
```

Erros como:

```
Oct 13 16:28:30 nuvem-cyrus-pr cyrus/imap[1934]: TLS server engine: No
CA file specified. Client side certs may not work
```

Indicam que os arquivos de Certificate Authority (CA) não estão corretamente instalados.

Verifique se a seguinte linha do /etc/imapd.conf está descomentada realmente:

```
tls_ca_path: /etc/ssl/certs
```

Instale os certificados corretos que você adquiriu da CA ou os do repositório.

```

nuvem-cyrus-pr:~# apt-get install ca-certificates
Lendo listas de pacotes... Pronto
Construindo arvore de dependencias
Lendo informacao de estado... Pronto
Os NOVOS pacotes a seguir serao instalados:
  ca-certificates
0 pacotes atualizados, 1 pacotes novos instalados, 0 a serem removidos
e 0 nao atualizados.
E preciso baixar 151kB de arquivos.
Depois desta operacao, 766kB adicionais de espaco em disco serao usados.
Obter:1 http://ftp.br.debian.org lenny/main ca-certificates 20080809
[151kB]
Baixados 151kB em 1s (106kB/s)
Pre-configurando pacotes ...
Selecionando pacote previamente nao selecionado ca-certificates.
(Lendo banco de dados ... 21420 arquivos e diretorios atualmente
instalados).
Desempacotando ca-certificates (de .../ca-
certificates_20080809_all.deb) ...
Processando gatilhos para man-db ...
Configurando ca-certificates (20080809) ...
Updating certificates in /etc/ssl/certs....done.
Running hooks in /etc/ca-certificates/update.d....done.
nuvem-cyrus-pr:~#

```

Verificar se os certificados não estão em blacklist

```

~$ openssl-vulnkey /etc/ssl/certs/ssl-cert-snakeoil.pem
Not blacklisted: 0ff365d9ac59f2ac2a7bfdb7bd3c6e71b97014f1
/etc/ssl/certs/ssl-cert-snakeoil.pem
:~$ sudo openssl-vulnkey /etc/ssl/private/ssl-cert-snakeoil.key
Not blacklisted: 0ff365d9ac59f2ac2a7bfdb7bd3c6e71b97014f1
/etc/ssl/private/ssl-cert-snakeoil.key

```

Então o arquivo /etc/imapd.conf ficará similar a este:

```

# Debian Cyrus imapd.conf
# See imapd.conf(5) for more information and more options
#AFM 05out2010 frontend server
# Configuration directory
configdirectory: /var/lib/cyrus

# Which partition to use for default mailboxes
#AFM 27ago2010 one MUST NOT define "defaultpartition" AND "partition-
default"
# at a proxy/frontend or it will create mbx locally.
#defaultpartition: default
partition-default: /var/spool/cyrus/mail

#AFM 20ago2010 pode-se especificar diferentes particoes alternativas,
por ex. UF
#partition-ac: /var/spool/correio/ac
#partition-al: /var/spool/correio/al
#partition-am: /var/spool/correio/am
#partition-ap: /var/spool/correio/ap
#partition-ba: /var/spool/correio/ba
#partition-ce: /var/spool/correio/ce

```

```
#partition-df: /var/spool/correio/df

#AFM 20ago2010 se usar diferentes particoes e
# Para permitir a movimentacao entre backends
allowusermoves: yes

#AFM 23ago2010
# Colocado para compatibilizacao com Clientes para subscrever em caixas
# pertencentes a diferentes backends
#allowallsubscribe: 1

#AFM 23ago2010
# Eliminar mensagens duplicadas
#duplicatesuppression: 1

#AFM 23ago2010
# Habilidade que as mensagens nao sejam deletadas
# imediatamente e possam ser recuperadas.
#expunge_mode: delayed

#AFM 23ago2010
# News setup
#partition-news: /var/spool/cyrus/news
#newsspool: /var/spool/news

# Alternate namespace
# If enabled, activate the alternate namespace as documented in
# /usr/share/doc/cyrus-doc-2.3/html/altnamespace.html, where an user's
# subfolders are in the same level as the INBOX
# See also userprefix and sharedprefix on imapd.conf(5)
altnamespace: no

# UNIX Hierarchy Convention
# Set to yes, and cyrus will accept dots in names, and use the forward
# slash "/" to delimit levels of the hierarchy. This is done by
# converting
# internally all dots to "^", and all "/" to dots. So the "rabbit.holes"
# mailbox of user "helmer.fudd" is stored in
# "user.elmer^fud.rabbit^holes"
#AFM 12ago2010
#unixhierarchysep: no
unixhierarchysep: yes

# Rejecting illegal characters in headers
# Headers of RFC2882 messages must not have characters with the 8th bit
# set. However, too many badly-written MUAs generate this, including
# most
# spamware. Enable this to reject such messages.
#reject8bit: yes

# Munging illegal characters in headers
# Headers of RFC2882 messages must not have characters with the 8th bit
# set. However, too many badly-written MUAs generate this, including
# most
# spamware. If you kept reject8bit disabled, you can choose to leave the
# crappage untouched by disabling this (if you don't care that IMAP
# SEARCH
# won't work right anymore.
#munge8bit: no

# Forcing recipient user to lowercase
# Cyrus 2.3 is case-sensitive. If all your mail users are in
```

```

lowercase, it is
# probably a very good idea to set lmtp_downcase_rcpt to true. This is
set by
# default, per RFC2821. This was not set by default in debian versions
up to
# and including 2.2.12-4.
lmtp_downcase_rcpt: yes

#AFM 20ago2010
# Setando este valor para 0 a mensagem de falha
# nao e enviada imediatamente ao cliente
lmtp_over_quota_perm_failure: 0

# Uncomment the following and add the space-separated users who
# have admin rights for all services.
#AFM 23ago2010
#admins: cyrus
#admins: cyrus techforce-admin cyrmaster mupdateuser cyrlmtp
#AFM 27ago2010 mupdateuser could not create mboxs on frontend
#admins: cyrus techforce-admin cyrmaster cyrlmtp
#AFM 02set2010 to not ask for passwd on create mbx
admins: cyrus techforce-admin cyrmaster cyrlmtp mupdateuser

# Space-separated list of users that have lmtp "admin" status (i.e. that
# can deliver email through TCP/IP lmtp). If specified, this parameter
# overrides the "admins" parameter above
#lmtp_admins: postman
#AFM 23ago2010
lmtp_admins: mupdateuser postman cyrlmtp

# Space-separated list of users that have mupdate "admin" status, in
# addition to those in the admins: entry above. Note that mupdate
slaves and
# backends in a Murder cluster need to authenticate against the mupdate
master
# as admin users.
#mupdate_admins: mupdateman
#AFM 20ago2010
mupdate_admins: mupdateman mupdateuser

# Space-separated list of users that have imapd "admin" status, in
# addition to those in the admins: entry above
#imap_admins: cyrus
#AFM 13out2010
imap_admins: cyrus mupdateuser techforce-admin

# Space-separated list of users that have sieve "admin" status, in
# addition to those in the admins: entry above
#sieve_admins: cyrus

# List of users and groups that are allowed to proxy for other users,
# seperated by spaces. Any user listed in this will be allowed to login
# for any other user. Like "admins:" above, you can have
imap_proxyserver
# and sieve_proxyserver.
#proxyserver: cyrus
#AFM 01out2010 you MUST NOT set proxyserver on frontends ONLY at
backends
#proxyserver: mupdateuser cyrus
proxy_authname: mupdateuser
proxy_password: senha

```

```

# No anonymous logins
allowanonymouslogin: no

# Minimum time between POP mail fetches in minutes
popminpoll: 1

# If nonzero, normal users may create their own IMAP accounts by
creating
# the mailbox INBOX. The user's quota is set to the value if it is
positive,
# otherwise the user has unlimited quota.
autocreatequota: 0

# umask used by Cyrus programs
umask: 077

# Sendmail binary location
# DUE TO A BUG, Cyrus sends CRLF EOLs to this program. This breaks Exim
3.
# For now, to work around the bug, set this to a wrapper that calls
# /usr/sbin/sendmail -dropcr instead if you use Exim 3.
#AFM 20ago2010
sendmail: /usr/sbin/sendmail

# If enabled, cyrdeliver will look for Sieve scripts in user's home
# directories: ~user/.sieve.
sieveusehomedir: false

# If sieveusehomedir is false, this directory is searched for Sieve
scripts.
sievedir: /var/spool/sieve

# notifyd(8) method to use for "MAIL" notifications. If not set, "MAIL"
# notifications are disabled. Valid methods are: null, log, zephyr
#mailnotifier: zephyr

# notifyd(8) method to use for "SIEVE" notifications. If not set,
"SIEVE"
# notifications are disabled. This method is only used when no method
is
# specified in the script. Valid methods are null, log, zephyr, mailto
#sievenotifier: zephyr

# DRAC (pop-before-smtp, imap-before-smtp) support
# Set dracinterval to the time in minutes to call DRAC while a user is
# connected to the imap/pop services. Set to 0 to disable DRAC (default)
# Set drachost to the host where the rpc drac service is running
#dracinterval: 0
#drachost: localhost

# If enabled, the partitions will also be hashed, in addition to the
hashing
# done on configuration directories. This is recommended if one
partition has a
# very bushy mailbox tree.
hashimapspool: true

# Allow plaintext logins by default (SASL PLAIN)
allowplaintext: yes
# Mesmo colocando o metodo PLAIN a autenticacao e passada
# somente apos o STARTTLS que criptografa a comunicacao
# clientes usam o IMAPS

```

```

# Force PLAIN/LOGIN authentication only
# (you need to uncomment this if you are not using an auxprop-based SASL
# mechanism. saslauthd users, that means you!). And pay attention to
# sasl_minimum_layer and allowapop below, too.
#sasl_mech_list: PLAIN
#AFM 12ago2010
sasl_mech_list: PLAIN

# Allow use of the POP3 APOP authentication command.
# Note that this command requires that the plaintext passwords are
# available in a SASL auxprop backend (eg. sasldb), and that the system
# can provide enough entropy (eg. from /dev/urandom) to create a
# challenge
# in the banner.
#allowapop: no

# The minimum SSF that the server will allow a client to negotiate. A
# value of 1 requires integrity protection; any higher value requires
# some
# amount of encryption.
#sasl_minimum_layer: 0
#AFM 12ago2010
sasl_minimum_layer: 0

# The maximum SSF that the server will allow a client to negotiate. A
# value of 1 requires integrity protection; any higher value requires
# some
# amount of encryption.
#sasl_maximum_layer: 256

# List of remote realms whose users may log in using cross-realm
# authentications. Seperate each realm name by a space. A cross-realm
# identity is considered any identity returned by SASL with an "@" in
# it.
# NOTE: To support multiple virtual domains on the same interface/IP,
# you need to list them all as loginrealms. If you don't list them here,
# (most of) your users probably won't be able to log in.
#loginrealms: example.com
#AFM 24ago2010
loginrealms: localhost techforce.com.br

# Enable virtual domain support. If enabled, the user's domain will
# be determined by splitting a fully qualified userid at the last '@'
# or '%' symbol. If the userid is unqualified, and the virdomains
# option is set to "on", then the domain will be determined by doing
# a reverse lookup on the IP address of the incoming network
# interface, otherwise the user is assumed to be in the default
# domain (if set).
#AFM 20ago2010
virdomains: userid

# The default domain for virtual domain support
# If the domain of a user can't be taken from its login and it can't
# be determined by doing a reverse lookup on the interface IP, this
# domain is used.
#defaultdomain:
#AFM 23ago2010
defaultdomain: techforce.com.br

#
# SASL library options (these are handled directly by the SASL

```

```
libraries,  
# refer to SASL documentation for an up-to-date list of these)  
#  
  
# The mechanism(s) used by the server to verify plaintext passwords.  
Possible  
# values are "saslauthd", "auxprop", "pwcheck" and "alwaystrue". They  
# are tried in order, you can specify more than one, separated by  
spaces.  
#  
# Do note that, since sasl will be run as user cyrus, you may have a  
lot of  
# trouble to set this up right.  
#AFM 20ago2010  
#sasl_pwcheck_method: auxprop  
sasl_pwcheck_method: saslauthd auxprop  
  
# What auxpropd plugins to load, if using sasl_pwcheck_method: auxprop  
# by default, all plugins are tried (which is probably NOT what you  
want).  
#AFM 20ago2010  
sasl_auxprop_plugin: sasldb  
  
# If enabled, the SASL library will automatically create authentication  
secrets  
# when given a plaintext password. Refer to SASL documentation  
sasl_auto_transition: no  
  
#  
# SSL/TLS Options  
#  
  
# File containing the global certificate used for ALL services (imap,  
pop3,  
# lmtp, sieve)  
#AFM 13out2010  
tls_cert_file: /etc/ssl/certs/ssl-cert-snakeoil.pem  
  
# File containing the private key belonging to the global server  
certificate.  
#AFM 13out2010  
tls_key_file: /etc/ssl/private/ssl-cert-snakeoil.key  
  
# File containing the certificate used for imap. If not specified, the  
global  
# certificate is used. A value of "disabled" will disable SSL/TLS for  
imap.  
#imap_tls_cert_file: /etc/ssl/certs/cyrus-imap.pem  
  
# File containing the private key belonging to the imap-specific server  
# certificate. If not specified, the global private key is used. A  
value of  
# "disabled" will disable SSL/TLS for imap.  
#imap_tls_key_file: /etc/ssl/private/cyrus-imap.key  
  
# File containing the certificate used for pop3. If not specified, the  
global  
# certificate is used. A value of "disabled" will disable SSL/TLS for  
pop3.  
#pop3_tls_cert_file: /etc/ssl/certs/cyrus-pop3.pem  
  
# File containing the private key belonging to the pop3-specific server
```

```

# certificate.  If not specified, the global private key is used.  A
value of
# "disabled" will disable SSL/TLS for pop3.
#pop3_tls_key_file: /etc/ssl/private/cyrus-pop3.key

# File containing the certificate used for lmtpl. If not specified, the
global
# certificate is used.  A value of "disabled" will disable SSL/TLS for
lmtpl.
#lmtpl_tls_cert_file: /etc/ssl/certs/cyrus-lmtpl.pem

# File containing the private key belonging to the lmtpl-specific server
# certificate.  If not specified, the global private key is used.  A
value of
# "disabled" will disable SSL/TLS for lmtpl.
#lmtpl_tls_key_file: /etc/ssl/private/cyrus-lmtpl.key

# File containing the certificate used for sieve. If not specified, the
global
# certificate is used.  A value of "disabled" will disable SSL/TLS for
sieve.
#sieve_tls_cert_file: /etc/ssl/certs/cyrus-sieve.pem

# File containing the private key belonging to the sieve-specific server
# certificate.  If not specified, the global private key is used.  A
value of
# "disabled" will disable SSL/TLS for sieve.
#sieve_tls_key_file: /etc/ssl/private/cyrus-sieve.key

# File containing one or more Certificate Authority (CA) certificates.
#tls_ca_file: /etc/ssl/certs/cyrus-imapd-ca.pem

# Path to directory with certificates of CAs.
tls_ca_path: /etc/ssl/certs

# The length of time (in minutes) that a TLS session will be cached for
later
# reuse.  The maximum value is 1440 (24 hours), the default.  A value
of 0 will
# disable session caching.
tls_session_timeout: 1440

# The list of SSL/TLS ciphers to allow, in decreasing order of
precedence.
# The format of the string is described in ciphers(1).  The Debian
default
# selects TLSv1 high-security ciphers only, and removes all anonymous
ciphers
# from the list (because they provide no defense against man-in-the-
middle
# attacks).  It also orders the list so that stronger ciphers come
first.
tls_cipher_list: TLSv1+HIGH:!aNULL:@STRENGTH

# Require a client certificate for ALL services (imap, pop3, lmtpl,
sieve).
#tls_require_cert: false

# Require a client certificate for imap ONLY.
#imap_tls_require_cert: false

# Require a client certificate for pop3 ONLY.

```

```

#pop3_tls_require_cert: false

# Require a client certificate for lmtp ONLY.
#lmtp_tls_require_cert: false

# Require a client certificate for sieve ONLY.
#sieve_tls_require_cert: false

#
# Cyrus Murder cluster configuration
#
# Set the following options to the values needed for this server to
# authenticate against the mupdate master server:
# mupdate_server
# mupdate_port
# mupdate_username
# mupdate_authname
# mupdate_realm
# mupdate_password
# mupdate_retry_delay

#AFM20ago2010
## Mupdate Server
mupdate_server: nuvem-cyrus-mu
mupdate_username: mupdateuser
mupdate_authname: mupdateuser
mupdate_password: senha

##
## KEEP THESE IN SYNC WITH cyrus.conf
##

# Unix domain socket that lmtpd listens on.
lmtpsocket: /var/run/cyrus/socket/lmtp

# The idle backend to use for IDLE command.
# Options: poll (default), idled, no
# poll doesn't need the idled daemon and is supposed to be more robust.
# however it doesn't update as quickly as the idled backend does. "no"
# turns off IDLE support. If set to "idled", you will also need to
enable
# the "idled" entry in cyrus.conf.
#AFM 05out2010
idlemethod: idled

# Unix domain socket that idled listens on.
idlesocket: /var/run/cyrus/socket/idle

# Unix domain socket that the new mail notification daemon listens on.
notifysocket: /var/run/cyrus/socket/notify

# Syslog prefix. Defaults to cyrus (so logging is done as cyrus/imap
etc.)
syslog_prefix: cyrus

#####

##
## DEBUGGING

```

```

##
# Debugging hook. See /usr/share/doc/cyrus-common-
2.3/README.Debian.debug
# Keep the hook disabled when it is not in use
#
# gdb Back-traces
#debug_command: /usr/bin/gdb -batch -cd=/tmp -x /usr/lib/cyrus/get-
backtrace.gdb /usr/lib/cyrus/bin/%s %d >/tmp/gdb-
backtrace.cyrus.%1$s.%2$d <&- 2>&1 &
#
# system-call traces
#debug_command: /usr/bin/strace -tt -o /tmp/strace.cyrus.%s.%d -p %2$d
<&- 2>&1 &
#
# library traces
#debug_command: /usr/bin/ltrace -tt -n 2 -o /tmp/ltrace.cyrus.%s.%d -p
%2$d <&- 2>&1 &

```

```
#####
```

```

#AFM 09mai2011 database formats
statuscache_db: skiplist
userdeny_db: skiplist
#AFM 09mai2011 debian defaults proved to have best performance
# cat /usr/lib/cyrus/cyrus-db-types.active
#annotation_db: skiplist
#duplicate_db: berkeley-nosync
#mbxlist_db: skiplist
#ptscache_db: berkeley
#quota_db: quotalegacy
#seenstate_db: skiplist
#subscription_db: flat
#tlscache_db: berkeley-nosync

```

```

# If enabled, this option forces the skiplist cyrusdb backend to
# always checkpoint when doing a recovery. This causes slightly
# more IO, but on the other hand leads to more efficient databases,
# and the entire file is already "hot".
#AFM 25ago2010
skiplist_always_checkpoint: 1

```

```

# If enabled, imapd, lmtpd and nntpd attempt to only write one copy
# of a message per partition and create hard links, resulting in a
# potentially large disk savings.
#AFM 25ago2010
singleinstancestore: 1

```

```

#AFM 23ago2010 Para Desabilitar o referral
#AFM 31ago2010 cyrus doc does not list this option for frontend...
#AFM 02set2010 trying to avoid pwd requests on mbx creation, as even
#AFM on backend issues a referral to itself at murder
proxyd_disable_mailbox_referrals: 1
sieve_allowreferrals: 0
proxyd_allow_status_referral: 0

```

```

#AFM 23ago2010 Nao enviar detalhes sobre o servidor
#serverinfo: off

```

```

#AFM 24ago2010 para evitar travar frontend ao criar mbox sem
especificar onde
# Whitespace separated list of backend server names. Used for find-
# ing server with the most available free space for proxying CREATE.
serverlist: nuvem-cyrus-bel nuvem-cyrus-be2

#AFM 24ago2010 para evitar criar mbox no frontend
# The backend server name used by default for new mailboxes. If not
# specified, the server with the most free space will be used for
# new mailboxes.
#AFM 03set2010 it works but we will try to leave dynamic commenting out
#defaultserver: nuvem-cyrus-bel

#AFM 25ago2010 nao consegue mover cx postal sem autenticar mutuamente
# hostname_mechs: <none>
# Force a particular list of SASL mechanisms to be used when authen
# ticating to the backend server hostname (where hostname is the
# short hostname of the server in question). If it is not specified
# it will query the server for available mechanisms and pick one to
# use. - Cyrus Murder

# hostname_password: <none>
# The password to use for authentication to the backend server host
# name (where hostname is the short hostname of the server) - Cyrus
# Murder

nuvem-cyrus-bel_authname: mupdateuser
nuvem-cyrus-bel_password: senha
nuvem-cyrus-bel_mechs: PLAIN
nuvem-cyrus-be2_authname: mupdateuser
nuvem-cyrus-be2_password: senha
nuvem-cyrus-be2_mechs: PLAIN

# You MUST set "mupdate_config: standard" and MUST NOT set
# "proxyservers: <proxyadmins>" at frontend in order to "defaultserver"
# and or "serverlist" take effect. Read imapd.c code, lines 4982 to
5008.
#AFM 01out2010
mupdate_config: standard

#AFM 05out2010 performance tuning
#mupdate_connections_max: 128
# The max number of connections that a mupdate process will allow,
this is
# related to the number of file descriptors in the mupdate process.
# Beyond this number connections will be immediately issued a BYE
response.
# mupdate_port: 3905
#mupdate_retry_delay: 20
#mupdate_workers_max: 50
# The maximum number of mupdate worker threads (overall)
#mupdate_workers_maxspare: 10
#mupdate_workers_min spare: 2
#mupdate_workers_start: 5

```

Reiniciar e esperar uns 20 segundos para dar tempo dos daemons inicializarem.

```
~# invoke-rc.d cyrus2.3 restart
```

Examine TODOS os /var/log/mail.* , /var/log/authd.log e /var/log/syslog

TESTES (parte 2)

Testar a conexão segura IMAP.

Testar com imtest via imaps pois via telnet ou nc não faz negociação e não dá para ver nada (você pode usar -p port_nr também):

```
nuvem-cyrus-pr:~# imtest -s -v -m plain -a <span
class="nospam1">techforce-admin</span>@<span
class="nospam2">techforce.com.br</span> -u techforce-
admin@techforce.com.br nuvem-cyrus-pr
starting TLS engine
setting up TLS connection
SSL_connect:before/connect initialization
write to 083E1AD0 [083EFC8] (93 bytes => 93 (0x5D))
0000 16 03 01 00 58 01 00 00|54 03 01 4c b7 07 8f 40
0010 8d 06 c8 f8 6d cf a9 a9|9d 78 ac c1 9c e1 e7 a6
0020 73 07 aa 25 da 5f 61 ff|a4 28 9d 00 00 26 00 39
0030 00 38 00 35 00 16 00 13|00 0a 00 33 00 32 00 2f
0040 00 05 00 04 00 15 00 12|00 09 00 14 00 11 00 08
0050 00 06 00 03 02 01 00 00|04 00 23
005d - <SPACES/NULS>

SSL_connect:SSLv3 write client hello A
read from 083E1AD0 [083E77B8] (5 bytes => 5 (0x5))
0000 16 03 01 00 30
read from 083E1AD0 [083E77BD] (48 bytes => 48 (0x30))
0000 02 00 00 2c 03 01 4c b7|07 8f f1 31 e3 f8 e1 26
0010 0b 16 77 6b 78 2c 0e 23|66 02 75 55 91 10 ba b1
0020 de b5 a0 7b 1e f5 00 00|39 01 00 04 00 23
0030 - <SPACES/NULS>

SSL_connect:SSLv3 read server hello A
read from 083E1AD0 [083E77B8] (5 bytes => 5 (0x5))
0000 16 03 01 01 b7
read from 083E1AD0 [083E77BD] (439 bytes => 439 (0x1B7))
0000 0b 00 01 b3 00 01 b0 00|01 ad 30 82 01 a9 30 82
0010 01 12 02 09 00 e9 6c d2|b9 7b 5d 0b 84 30 0d 06
0020 09 2a 86 48 86 f7 0d 01|01 05 05 00 30 19 31 17
0030 30 15 06 03 55 04 03 13|0e 6e 75 76 65 6d 2d 63
0040 79 72 75 73 2d 70 72 30|1e 17 0d 31 30 31 30 31
0050 33 31 35 32 35 30 37 5a|17 0d 32 30 31 30 31 30
0060 31 35 32 35 30 37 5a 30|19 31 17 30 15 06 03 55
0070 04 03 13 0e 6e 75 76 65|6d 2d 63 79 72 75 73 2d
0080 70 72 30 81 9f 30 0d 06|09 2a 86 48 86 f7 0d 01
0090 01 01 05 00 03 81 8d 00|30 81 89 02 81 81 00 e2
00a0 a9 60 6f 72 46 f1 7e ac|bc 88 61 15 47 3f 05 b5
00b0 84 7b 35 3f 5f 55 c5 87|e6 76 43 c4 a8 6a 70 ca
00c0 c4 7a 33 5d 43 f7 d3 68|00 62 c2 37 61 59 cb 4f
```

```

00d0 cb 6b 73 65 2d 12 83 04 c7 f4 c7 e1 bc d3 ab 69
00e0 18 2b 60 a5 f6 77 fc 3e 9b 64 7e bd df 48 ce e3
00f0 cc bf 1e 6c e1 71 b6 73 6e e4 61 c3 2b b4 54 c4
0100 03 cd 93 bd cc 86 ea 2e 79 94 4a d5 6a b1 5a 29
0110 bf 2d c9 81 5f da d3 05 11 76 14 98 e3 f5 4f 02
0120 03 01 00 01 30 0d 06 09 2a 86 48 86 f7 0d 01 01
0130 05 05 00 03 81 81 00 0b c0 4b a4 ef 79 04 38 0c
0140 b5 3a c1 ec 9a 3c 26 15 b1 55 50 fe 85 a8 ce b9
0150 04 c6 c8 af 61 1b f5 98 95 f4 d6 2c 19 7f 38 12
0160 b5 2e aa 66 7e 1e e8 63 a3 98 60 f1 46 24 52 9d
0170 8f 5a e8 c0 b3 7e f7 79 43 08 c5 cf 56 e2 3e f1
0180 e6 b7 3a 1b 27 79 fe 0c a2 12 4c a5 f0 6a f2 5b
0190 68 53 41 a4 ba 4e 84 24 90 84 71 c1 b2 89 59 8b
01a0 6e fa 8d 30 34 da 81 2a 57 50 f1 a6 75 d4 a6 79
01b0 cc 8b 97 26 6f 9b ba
Peer cert verify depth=0 /CN=nuvem-cyrus-pr
verify error:num=18:self signed certificate
verify return:1
Peer cert verify depth=0 /CN=nuvem-cyrus-pr
verify return:1
SSL_connect:SSLv3 read server certificate A
read from 083E1AD0 [083E77B8] (5 bytes => 5 (0x5))
0000 16 03 01 01 8d
read from 083E1AD0 [083E77BD] (397 bytes => 397 (0x18D))
0000 0c 00 01 89 00 80 ff ff ff ff ff ff c9 0f
0010 da a2 21 68 c2 34 c4 c6 62 8b 80 dc 1c d1 29 02
0020 4e 08 8a 67 cc 74 02 0b be a6 3b 13 9b 22 51 4a
0030 08 79 8e 34 04 dd ef 95 19 b3 cd 3a 43 1b 30 2b
0040 0a 6d f2 5f 14 37 4f e1 35 6d 6d 51 c2 45 e4 85
0050 b5 76 62 5e 7e c6 f4 4c 42 e9 a6 37 ed 6b 0b ff
0060 5c b6 f4 06 b7 ed ee 38 6b fb 5a 89 9f a5 ae 9f
0070 24 11 7c 4b 1f e6 49 28 66 51 ec e6 53 81 ff ff
0080 ff ff ff ff ff ff 00 01 02 00 80 60 dd 5f be db
0090 33 7c ef 6e 29 d1 ba 14 cf 1f 8e e2 54 16 27 d4
00a0 ee 3c 74 0b d7 74 82 8e b6 77 6f bd 94 01 5d bf
00b0 78 a6 8d be 68 87 97 5b cd bc b5 9e aa 0c cd 62
00c0 2c da 6b 2d 0f 36 01 6e 9c b3 17 91 32 92 b0 d5
00d0 bd 1f 28 fc 54 4b 01 b5 0b ab 9d 48 db 91 c1 58
00e0 9e fe 1b 64 8b e9 af 84 69 cc 6e c7 f9 54 70 56
00f0 8c c7 66 1c b1 c7 9e 04 2d aa 4f 9a fb 3d 19 c5
0100 c0 0a 50 b2 8a 58 f6 18 d0 98 a4 00 80 a2 e1 50
0110 bf e8 34 f2 5b 79 24 87 a3 79 ae ea fe 75 cc 48
0120 fe dd 00 b8 86 c3 5e 7e 0f 1d eb fe 51 37 5a 92
0130 19 e9 f3 dc 7e 4c 73 17 76 65 bd 41 3b 26 82 79
0140 e2 78 82 92 fe bb 06 3f d2 b8 d8 81 79 b6 e1 1a
0150 e5 6e 2f bf 25 cc 22 dd 75 36 e7 47 a0 72 df 40
0160 0a b7 02 7a 34 04 73 e0 d6 33 17 bf ee ea e8 3a
0170 62 f9 5a c2 48 5a e1 61 38 4a 7b 3b 6c 52 37 23
0180 d3 7d dd 42 1a 9d 22 ff 06 54 00 e5 1c
SSL_connect:SSLv3 read server key exchange A
read from 083E1AD0 [083E77B8] (5 bytes => 5 (0x5))
0000 16 03 01 00 04
read from 083E1AD0 [083E77BD] (4 bytes => 4 (0x4))
0000 0e
0004 - <SPACES/NULS>

SSL_connect:SSLv3 read server done A
SSL_connect:SSLv3 write client key exchange A
SSL_connect:SSLv3 write change cipher spec A
SSL_connect:SSLv3 write finished A
write to 083E1AD0 [083F5908] (198 bytes => 198 (0xC6))
0000 16 03 01 00 86 10 00 00 82 00 80 94 0a 88 46 c5

```

```

0010 29 a8 b9 ae bc 8f 20 7b|9a d9 12 dc 43 9d eb d9
0020 0e f8 61 5e 3b a6 f5 62|bf eb 74 6e 6f 9c 25 3b
0030 e0 33 fb b1 95 6f 72 8a|25 65 c8 f2 45 d5 d2 47
0040 90 50 85 17 f9 95 de 93|46 2d 13 eb 57 b7 f3 7b
0050 34 96 14 e8 03 85 3f 06|48 ec 12 14 e3 0e f1 e5
0060 5d 73 c3 95 4b 6c 13 04|27 b3 0d 35 26 39 af 1e
0070 dc f0 29 70 a2 fe 5c b5|18 e5 36 69 88 04 d9 b9
0080 bb 28 71 fe 0c a8 d2 16|c5 eb aa 14 03 01 00 01
0090 01 16 03 01 00 30 15 ae|d5 4c c2 b4 bf 43 e5 55
00a0 fe 21 0b be 12 74 3b ee|99 87 03 38 85 e5 0d 82
00b0 83 6f 48 87 bf 7c 49 66|18 8c 37 07 86 28 ad 8d
00c0 62 21 99 93 26 cb
SSL_connect:SSLv3 flush data
read from 083E1AD0 [083E77B8] (5 bytes => 5 (0x5))
0000 16 03 01 00 aa
read from 083E1AD0 [083E77BD] (170 bytes => 170 (0xAA))
0000 04 00 00 a6 00 00 00 00|00 a0 ef e3 dd 84 2e e7
0010 92 1c 17 92 97 a5 38 a4|64 79 3f 92 a6 ba 0e e2
0020 32 3c 38 3b b2 30 7c 4f|ca 34 8b b4 1d cb 26 2a
0030 a7 da 1b 4b bd 3b 4e df|41 cd 69 d8 7a a4 88 0d
0040 a7 a1 ed b1 89 0c a3 4e|f7 de 07 26 96 8c b9 26
0050 40 e9 f1 75 d6 01 e8 7a|d6 74 bc 7a 07 93 60 e9
0060 fe fa 78 6e 53 eb aa c4|8f 9b a6 9c a6 34 a6 33
0070 08 a1 1e c9 62 1f 2f ac|7c 55 85 22 d7 c3 19 ef
0080 6b 94 a3 40 97 2f 69 5e|b0 43 71 2d 82 e4 c7 5b
0090 ed c9 31 a8 c6 cf 7f 53|4d b2 39 25 fe 57 c0 ad
00a0 18 d7 0e c1 fa 6c 1a a0|a1 ad
SSL_connect:unknown state
read from 083E1AD0 [083E77B8] (5 bytes => 5 (0x5))
0000 14 03 01 00 01
read from 083E1AD0 [083E77BD] (1 bytes => 1 (0x1))
0000 01
read from 083E1AD0 [083E77B8] (5 bytes => 5 (0x5))
0000 16 03 01 00 30
read from 083E1AD0 [083E77BD] (48 bytes => 48 (0x30))
0000 80 21 e8 51 3e 62 0d 12|cd 38 ac 4b 7c d8 31 d6
0010 62 ce 49 9a 8b 7c 52 56|50 13 b8 e4 7c d3 f5 1a
0020 88 27 78 2b 06 0d 91 38|0e c6 99 62 91 a7 78 66
SSL_connect:SSLv3 read finished A
subject_CN=nuvem-cyrus-pr, issuer_CN=nuvem-cyrus-pr
TLS connection established: TLSv1 with cipher DHE-RSA-AES256-SHA
(256/256 bits)
read from 083E1AD0 [083E77B8] (5 bytes => 5 (0x5))
0000 17 03 01 00 b0
read from 083E1AD0 [083E77BD] (176 bytes => 176 (0xB0))
0000 fa 70 e7 1e 88 b0 db d6|95 0c 90 d0 2d ac 54 6f
0010 bd b5 fd 13 e5 1c 74 09|4f a6 2f 72 b6 24 20 16
0020 5c 52 71 02 33 d7 df 50|9f b9 9e 12 39 23 fb b6
0030 a8 7f 4a 29 3d ac 71 a1|ec 1f 01 06 25 e5 90 06
0040 ec ff bc af 93 a1 c3 af|89 ad 37 22 8b b2 f2 95
0050 f1 08 be 6e f4 01 93 8c|59 96 6a f5 88 3b 03 8f
0060 97 5d a3 25 b9 82 ca 2d|de 1d b0 ea f4 63 d4 11
0070 2f 31 05 67 07 f6 63 b3|d6 98 e6 4e 64 a3 ae 1c
0080 fc 2e 8b f0 91 4b 03 8d|f4 72 63 60 7a 16 83 65
0090 5f 02 f8 1a 6b 8c ba a6|f0 59 24 d4 a8 b6 7c 6a
00a0 7d eb 95 b5 f3 37 b9 d0|28 44 51 76 eb fa 4a bb
S: * OK [CAPABILITY IMAP4 IMAP4rev1 LITERAL+ ID MUPDATE=mupdate://nuvem-
cyrus-mu/
AUTH=PLAIN SASL-IR] nuvem-cyrus-pr Cyrus IMAP Murder v2.3.16-Debian-
2.3.16-1 server ready
Please enter your password:
C: A01 AUTHENTICATE PLAIN

```

ZXhwcmVzc28tYWRtaW5AZXhwcmVzc28uZ292LmJyAGV4cHJlc3NvLWFkbWluQGV4cHJlc3Nv
Lmdvdi5icgBzZW5oYQ==

write to 083E1AD0 [083E77B8] (133 bytes => 133 (0x85))

```
0000 17 03 01 00 80 bf 86 11 | 49 81 ba c9 2e 7a af e5
0010 e7 18 bd c4 12 ac 43 f3 | d0 90 30 91 87 fd 31 eb
0020 d7 12 a2 25 1d d0 01 de | c3 ea 7b 98 25 64 e9 42
0030 8f 39 fe 3b 5e 15 d9 ef | e0 dc 2e df 8e 4f 18 aa
0040 0a 32 8f 01 59 89 2c 50 | 0c c5 2f a6 06 90 9d c1
0050 f3 4e 3b 14 cc 22 ad 6d | 64 f1 9c c7 b7 a7 be a7
0060 b9 73 0c 4e fe 3c 06 f5 | 35 42 16 69 03 b4 b2 a2
0070 9f e7 dc c7 eb f2 90 b9 | d0 83 0c 88 ac cd 23 15
0080 ad 82 cc 52 b1
```

read from 083E1AD0 [083E77B8] (5 bytes => 5 (0x5))

```
0000 17 03 01 00 f0
```

read from 083E1AD0 [083E77BD] (240 bytes => 240 (0xF0))

```
0000 b0 10 f7 75 78 04 fe 92 | c5 3a 2d ac 47 e9 aa 04
0010 4f 36 ef 07 c0 be 30 c6 | 52 ba ce 1b 72 a9 91 16
0020 a2 07 3f ae fa 3c 33 1a | 22 72 b5 af 4e 8d d9 c8
0030 e5 3f 37 93 23 61 46 e1 | 74 f3 14 a4 2a be d7 3b
0040 a9 0c 86 db 9f 15 35 63 | df 08 3b 7d ca 88 7c c9
0050 b7 80 82 1c 0d c0 6d ed | be 8e 23 b0 bd c5 89 1b
0060 8c 39 b5 1c c2 f6 ce ac | 20 af f0 9b 22 93 67 20
0070 1b ff e7 fe 6e 7b bf 8b | 9a 84 0f 53 15 ef 68 5a
0080 2c e1 df 59 86 dc 63 e7 | 36 0f a4 62 2a 0c 5d 4d
0090 40 38 27 55 40 f5 b5 2a | 9f d8 e1 d9 c8 97 74 35
00a0 46 27 a7 66 7c bc 0f c2 | 84 19 43 f2 af bf 15 fb
00b0 17 f6 ee 4e fd 4a 41 32 | 0d 1e 19 b1 d6 c6 be 06
00c0 dd d2 e1 cb 5d 99 ba 43 | 1d 38 2c 55 40 9b f0 a0
00d0 0a 0a a6 df f4 71 82 bf | 7d 86 6a 13 ee a9 be 2d
00e0 08 6c e4 ec 1e 8c e7 3d | 1b fc 55 24 8b 17 18 50
```

S: A01 OK [CAPABILITY IMAP4 IMAP4rev1 LITERAL+ ID

MUPDATE=mupdate://nuvem-cyrus-mu/

LOGINDISABLED ACL RIGHTS=kxte QUOTA MAILBOX-REFERRALS NAMESPACE UIDPLUS
NO_ATOMIC_

RENAME UNSELECT CHILDREN MULTIAPPEND BINARY SORT SORT=MODSEQ

THREAD=ORDEREDSUBJECT

THREAD=REFERENCES ANNOTATEMORE CATENATE CONDSTORE SCAN IDLE

URLAUTH] Success (tls protection)

Authenticated.

Security strength factor: 256

1 select inbox

write to 083E1AD0 [083E77B8] (53 bytes => 53 (0x35))

```
0000 17 03 01 00 30 8f 22 4f | 37 8a aa f5 0a eb 17 ce
0010 17 23 09 58 79 b3 dd a1 | fa 83 92 df 32 1a ef 1e
0020 6a 3d 11 ce 31 0b b1 d6 | 92 97 e9 3d 57 ac 8e f4
0030 c0 37 e3 44 a4
```

read from 083E1AD0 [083E77B8] (5 bytes => 5 (0x5))

```
0000 17 03 01 01
```

```
0005 - <SPACES/NULS>
```

read from 083E1AD0 [083E77BD] (256 bytes => 256 (0x100))

```
0000 64 db 46 e1 07 90 4f 8e | 82 fb 88 5e 64 d9 7a 76
0010 b9 5a dd 9b 92 39 d6 d6 | e7 ff 16 b4 79 f5 3e 5a
0020 aa c0 04 06 17 3c 24 41 | aa e0 a5 72 6d 82 f5 25
0030 e9 96 40 f1 8a ac 76 f7 | 14 29 3d 83 10 11 e2 d0
0040 9c e5 31 e0 12 8c 15 06 | 09 db d0 8f 5a 98 17 52
0050 a2 d9 0d ca a7 44 cf 89 | c2 2d 05 5c f1 54 a3 fa
0060 34 03 ec ae 93 f1 3a 97 | f3 57 fe fc cd be 08 8f
0070 b7 e2 ff 85 3e 7e db d7 | 7a ce 83 13 49 fc c2 c7
0080 2c ed 0c 18 f5 ca 9b 96 | e3 61 20 60 d1 17 85 67
0090 39 fc 02 a2 e1 f9 e8 d6 | 2d 45 ae 23 73 3b f4 86
00a0 28 4d 2f aa f8 6a 8d 87 | 5c 49 c2 5e 82 bc cd 94
```

```

00b0 7d dc c0 c1 4e 60 c3 29|a5 45 71 8a 2b 1e 36 d9
00c0 50 c1 68 a3 f6 64 9a f2|f8 3f 07 6c 03 47 0b 7c
00d0 05 04 5d cb 88 5f 8e 00|a2 87 d4 89 01 36 0e cb
00e0 e8 42 f3 23 28 f7 26 86|29 d4 34 90 d2 cd 39 8d
00f0 81 46 fe 3f e9 02 85 81|bf cd ee a7 cc 30 7e bf
* FLAGS (\Answered \Flagged \Draft \Deleted \Seen)
* OK [PERMANENTFLAGS (\Answered \Flagged \Draft \Deleted \Seen \*)]
* 3 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1286830893]
* OK [UIDNEXT 4]
* OK [NOMODSEQ] Sorry, modsequences have not been enabled on this
mailbox
* OK [URLMECH INTERNAL]
1 OK [READ-WRITE] Completed
2 logout
write to 083E1AD0 [083E7FC8] (53 bytes => 53 (0x35))
0000 17 03 01 00 30 4f 54 5d|09 2c 42 85 7a 75 23 0e
0010 b4 48 59 61 1d 27 ff 9d|b1 14 bc 9b b8 65 eb d3
0020 9c de 47 03 8a 12 74 83|f9 6c ec 32 ba c2 a4 89
0030 9d 3a 3a 5d b1
read from 083E1AD0 [083E77B8] (5 bytes => 5 (0x5))
0000 17 03 01 00 40
read from 083E1AD0 [083E77BD] (64 bytes => 64 (0x40))
0000 32 48 d6 ca 83 0a 63 f6|00 42 33 8c 29 56 9e dd
0010 6b 98 30 65 09 3f b2 11|73 63 69 4a 9b fb c3 52
0020 d8 eb 52 ea 55 40 27 56|d6 d2 cf be 48 24 13 43
0030 bc 00 4d ca 5f e6 3c 3c|bd 10 e5 de b6 25 da 95
* BYE LOGOUT received
2 OK Completed
read from 083E1AD0 [083E77B8] (5 bytes => 0 (0x0))
Connection closed.
nuvem-cyrus-pr:~#
</pre>

```

Links úteis

<http://james.apache.org/server/rfclist/imap4/rfc2060.txt>

<http://linux.die.net/man/1/cyradm>

http://linux.die.net/man/8/ctl_cyrusdb

http://linux.die.net/man/8/cvt_cyrusdb

<http://oreilly.com/catalog/mimap/chapter/ch09.html>

<http://www.faqs.org/docs/Linux-HOWTO/Cyrus-IMAP.html>

<http://nakedape.cc/info/Cyrus-IMAP-HOWTO/maintenance.html>

<http://morison.biz/technotes/articles/44>

<http://www.washington.edu/imap/IMAP-FAQs/index.html#7.46>

<http://www.comfsm.fm/computing/cyrus-imapd/install-testing.html>

<http://www.owlriver.com/projects/exchange/www.arrayservices.com/projects/Exchange-HOWTO/html/x450.html>

<http://openmailadmin.ossdl.de/wiki/howto/Postfix-SASL-Cyrus-MySQL-Amavis-Postgrey-SpamAssassin-ClamAV-Squirrelmail-Mailman-Mailgraph-OMA>

http://www.expressolivre.org/html/modules/newbb/viewtopic.php?topic_id=160&forum=3

http://www.postfix.org/SASL_README.html

<http://www.devheads.net/server/postfix/user/lmtp-over-tcp-connection-refused.htm>

<http://www.puschitz.com/TuningLinuxForOracle.shtml#LimitingMaximumNumberOfOpenFileDescriptorsForTheOracleUser>

<http://www.cyberciti.biz/faq/linux-increase-the-maximum-number-of-open-files/>

<http://linuxgazette.net/124/pfeiffer.html>

<http://nlinuxadmin.blogspot.com/2010/03/cyrus-imap-configuration-with-ldap.html>

<http://www-uxsup.csx.cam.ac.uk/~dpc22/cyrus/performance.html>

<http://www.spinics.net/lists/info-cyrus/msg10252.html>

<http://www.spinics.net/lists/info-cyrus/msg04766.html>

<http://www.spinics.net/lists/info-cyrus/msg04755.html>

<http://www.irbs.net/internet/info-cyrus/0702/0054.html>

http://www.cyrusimap.org/mediawiki/index.php/Cyrus_Murder_Failure_Modes

<http://www.cyrusimap.org/docs/cyrus-imapd/2.3.16/install-murder.php>