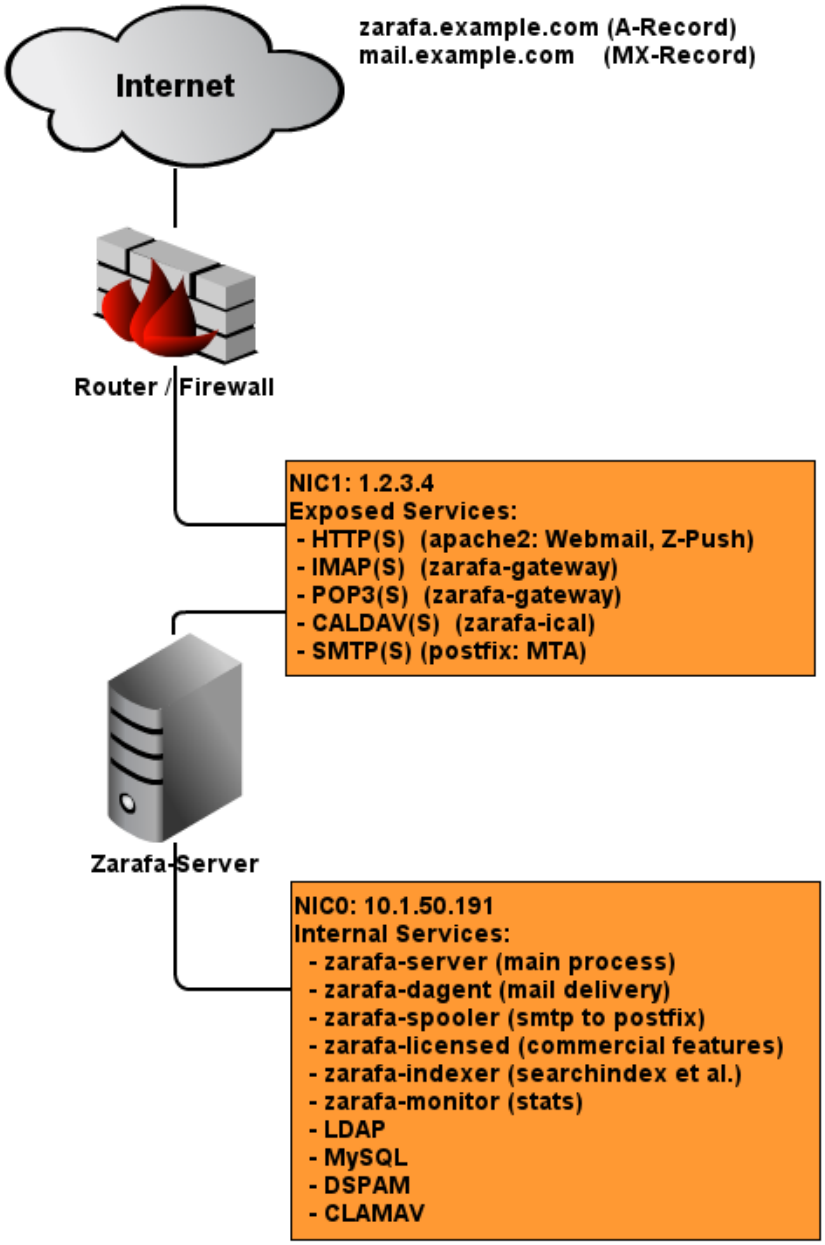
Serversetup multi-tenant Zarafa+Postfix+SASL+Dspam+Clamav+openLDAP (Ubuntu 10.04 LTS)

This guide is deprecated as of 2014-12-26 in favor of a new one:

Serversetup multi-tenant Zarafa+Postfix+SASL+SpamAssassin+Clamav+openLDAP (Ubuntu 14.04 LTS)

See further below for the old guide. Thank you for your attention.

Zarafa Groupware and dependent infrastructure setup guidelines.



Preface

As nearly all online guides about setting up a useable zarafa server lack in one or another detail, here comes another attempt of describing the process. Throughout the guide only lines in config files that need to be changed are shown.
This guide assumes:

- general linux knowledge: basic commands and system administration know-how
- basic mysql knowledge
- basic ldap knowledge
- basic apache knowledge
- intermediate postfix / clamav / dspam knowledge

The Server will be directly exposed to the internet on the ports shown in the diagram above. Therefore another interface is assigned to the server that will handle internal connections that need not be seen from the internet and are only used for local or server internal communication.

- Note:
    - This is NOT a copy-and-paste how-to!

- The domain 'example.com' is used, replace all instances with your own domain (in ldap too, like: dc=example,dc=com).
- The external interface is assumed to have the IP 1.2.3.4. Replace with your own external interface address.
- The internal interface is assumed to have the IP 10.1.50.191. Replace with your own internal interface address.
- The password 'secret' will be used for all passwords. Replace with DIFFERENT, STRONG passwords accordingly!
- This setup assumes a local MySQL database. If you use a remote, dedicated database you will need to change the database settings and grants in various config files or the database itself.

Server

- Distro: Ubuntu 10.04 LTS 64bit
  - Zarafa 7.0 from http://community.zarafa.com/
  - MySQL 5.1 (or 5.5), openLDAP, postfix, dspam from Ubuntu Repository
  - phpldapadmin, z-push from source

Certificates

For this setup two different certificates are needed. One for the Webserver (webmail.example.com) and one for the mail server (mail.example.com). It is advised to use official certificates, however for testing purposes you can create your own ones with openssl.

- Note:
  - The web certificates will be called 'web.crt' and 'web.key'. Replace with your own certificate filenames.
  - The mail certificates will be called 'mail.crt' and 'mail.key'. Replace with your own certificate filenames.

Install Packages

Grab packages from the zarafa-site, install per their instructions. Also install postfix, dspam, clamav, slapd and mysql. The zarafa packages should have already installed apache2. If not, something is definitely wrong...

```
~# aptitude install postfix postfix-ldap dspam libdspam7 libdspam7-drv-mysql mysql-server-5.1 slapd ldap-utils
php5-ldap clamav clamav-freshclam sasl2-bin
```

MySQL Setup

Not much to do here, just create databases, users and permissions for zarafa and dspam:

```
~# mysql -uroot -p
mysql> create database zarafa;
mysql> create database dspam;
mysql> grant all on zarafa.* to 'zarafa'@'localhost' identified by 'secret';
mysql> grant all on dspam.* to 'dspam'@'localhost' identified by 'secret';
mysql> flush privileges;
```

LDAP Setup

LDAP Server Setup

Probably the part that generates the most head-scratching. Although the latest Ubuntu LTS server already uses the 'cn=config' format zarafa admin guide still works with the old 'slapd.conf' format, so we stick with that too.
First adjust the default-file:

/etc/default/slapd

```
SLAPD_CONF=/etc/ldap/slapd.conf
SLAPD_SERVICES="ldap://10.1.50.191:389/ ldap://127.0.0.1:389/ ldapi:///"
SLAPD_OPTIONS="-4"
```

Client config file:

/etc/ldap/ldap.conf

```
ldap_version 3
URI ldap://10.1.50.191
SIZELIMIT 0
TIMELIMIT 0
DEREF never
BASE dc=example, dc=com
```

Server config file. I included the 'nis' schema here too, some might need it for nis domain setups. Copy the zarafa-schema to **'/etc/ldap/schema'** and generate a ldap password first, however:

```
~# cp /usr/share/doc/zarafa/zarafa.schema.gz /etc/ldap/schema/
~# gunzip /etc/ldap/schema/zarafa.schema.gz
~# slappasswd
```

Now include the newly generated ldap password hash in the slapd.conf after the 'rootpw' variable:

/etc/ldap/slapd.conf

```
# Schema and objectClass definitions, depending on your
# LDAP setup
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/inetorgperson.schema
include         /etc/ldap/schema/openldap.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/misc.schema
include         /etc/ldap/schema/zarafa.schema


# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile         /var/run/slapd/slapd.pid

# List of arguments that were passed to the server
argsfile        /var/run/slapd/slapd.args

# Read slapd.conf(5) for possible values
loglevel        8192

# Where the dynamically loaded modules are stored
modulepath      /usr/lib/ldap
moduleload      back_hdb

# The maximum number of entries that is returned for a search operation
sizelimit 500

# The tool-threads parameter sets the actual amount of cpu's that is used
# for indexing.
tool-threads 1

#######################################################################
# Specific Backend Directives for hdb:
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
backend         hdb

#######################################################################
# Specific Backend Directives for 'other':
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
```

```
#backend                <other>

#######################################################################
# Specific Directives for database #1, of type hdb:
# Database specific directives apply to this databasse until another
# 'database' directive occurs
database        hdb

# The base of your directory in database #1
suffix          "dc=example,dc=com"

# rootdn directive for specifying a superuser on the database. This is needed
# for syncrepl.
rootdn          "cn=admin,dc=example,dc=com"
rootpw          {SSHA}secret


# Where the database file are physically stored for database #1
directory       "/var/lib/ldap"

# The dbconfig settings are used to generate a DB_CONFIG file the first
# time slapd starts.  They do NOT override existing an existing DB_CONFIG
# file.  You should therefore change these settings in DB_CONFIG directly
# or remove DB_CONFIG and restart slapd for changes to take effect.

# For the Debian package we use 2MB as default but be sure to update this
# value if you have plenty of RAM
dbconfig set_cachesize 0 2097152 0

# Sven Hartge reported that he had to set this value incredibly high
# to get slapd running at all. See http://bugs.debian.org/303057 for more
# information.

# Number of objects that can be locked at the same time.
dbconfig set_lk_max_objects 1500
# Number of locks (both requested and granted)
dbconfig set_lk_max_locks 1500
# Number of lockers
dbconfig set_lk_max_lockers 1500

# Indexing options for database #1
index           objectClass eq

# Save the time that the entry gets modified, for database #1
lastmod         on

# Checkpoint the BerkeleyDB database periodically in case of system
# failure and to speed slapd shutdown.
checkpoint      512 30

# Where to store the replica logs for database #1
# replogfile    /var/lib/ldap/replog

# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
# These access lines apply to database #1 only
access to attrs=userPassword,shadowLastChange
        by dn="cn=admin,dc=example,dc=com" write
        by anonymous auth
        by self write
        by * none

# Ensure read access to the base for things like
# supportedSASLMechanisms.  Without this you may
# have problems with SASL not knowing what
# mechanisms are available and the like.
# Note that this is covered by the 'access to *'
# ACL below too but if you change that as people
# are wont to do you'll still need this if you
```

```
# want SASL (and possible other things) to work
# happily.
access to dn.base="" by * read

# The admin dn has full write access, everyone else
# can read everything.
access to *
        by dn="cn=admin,dc=example,dc=com" write
        by * read
```

Now (re)start the ldap server.

```
~# service slapd restart
```

- Hint: If the server throws an error change the log level to '8' or '4', this should output enough info to give you an idea what is wrong. LDAP logs to syslog in Ubuntu.

LDAP Admin Setup

Create a .ldif file to load into LDAP:

/tmp/admin.ldif

```
dn:dc=example,dc=com
objectClass: dcObject
objectClass: organization
o: example
dc: example

dn:cn=admin,dc=example,dc=com
objectClass: organizationalRole
cn: admin
```

Load the template into the LDAP database (you will be asked for the password you generated with 'slappasswd' before):

```
~# ldapadd -x -W -D cn=admin,dc=example,dc=com -f /tmp/admin.ldif
```

Install phpldapadmin

Grab the latest .tar.gz from sourceforge and unzip to '**/var/www/**'. Create a symlink for easier management, fix permissions too. It's ok to give it to 'root', apache only needs 'o+rX' on the files.

```
~# tar xzvf phpldapadmin.tar.gz -C /var/www
~# cd /var/www
~# ln -s phpldapadmin-w.x.y.z phpldapadmin
~# chown -R root: phpldapadmin-w.x.y.z
~# cp phpldapadmin/config/config.php.example phpldapadmin/config/config.php
```

Configure phpldapadmin

The config is somewhat big but most are comments and defaults that need not to be modified. Again only lines that were modified are shown.

/var/www/phpldapadmin/config/config.php

```
/* phpLDAPadmin can encrypt the content of sensitive cookies if you set this
   to a big random string. */
$config->custom->session['blowfish'] = secret;

/* The language setting. If you set this to 'auto', phpLDAPadmin will attempt
   to determine your language automatically. Otherwise, available lanaguages
   are: 'ct', 'de', 'en', 'es', 'fr', 'it', 'nl', and 'ru'
   Localization is not complete yet, but most strings have been translated.
   Please help by writing language files. See lang/en.php for an example. */
$config->custom->appearance['language'] = 'en';

/* Our local timezone
   This is to make sure that when we ask the system for the current time, we
   get the right local time. If this is not set, all time() calculations will
   assume UTC if you have not set PHP date.timezone. */
// $config->custom->appearance['timezone'] = null;
$config->custom->appearance['timezone'] = 'Europe/Vienna';

/* Hide the warnings for invalid objectClasses/attributes in templates. */
$config->custom->appearance['hide_template_warning'] = true;

/* A convenient name that will appear in the tree viewer and throughout
   phpLDAPadmin to identify this LDAP server to users. */
$servers->setValue('server','name','example.com');

/* Array of base DNs of your LDAP server. Leave this blank to have phpLDAPadmin
   auto-detect it for you. */
// $servers->setValue('server','base',array('dc=example,dc=com'));

/* The DN of the user for phpLDAPadmin to bind with. For anonymous binds or
   'cookie' or 'session' auth_types, LEAVE THE LOGIN_DN AND LOGIN_PASS BLANK. If
   you specify a login_attr in conjunction with a cookie or session auth_type,
   then you can also specify the bind_id/bind_pass here for searching the
   directory for users (ie, if your LDAP server does not allow anonymous binds. */
// $servers->setValue('login','bind_id','');
$servers->setValue('login','bind_id','cn=admin,dc=example,dc=com');
```

You should be able to access your server under http://example.com/phpldapadmin now. the 'User' field will be prefilled with 'cn=admin,dc=example, dc=com' and you can login with the password you generated with 'slappasswd' before.

After login create a new 'Security Object' called 'zarafaservice' and assign it a password. This will be the user which zarafa and postfix will use to access LDAP. If done correctly phpldapadmin should display a **dn of 'uid=zarafaservice,dc=example,dc=com'** for the user. Now adjust slapd.conf to grant the user read access to the tree. Put the entry between the 'access to attrs' and 'access to *' parameters:

/etc/ldap/slapd.conf

```
# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
# These access lines apply to database #1 only
access to attrs=userPassword,shadowLastChange
        by dn="cn=admin,dc=example,dc=com" write
        by anonymous auth
        by self write
        by * none

# !! NEW !! #
access to *
        by dn="uid=zarafaservice,dc=example,dc=com" read
# !! NEW !! #

# The admin dn has full write access, everyone else
# can read everything.
access to *
        by dn="cn=admin,dc=example,dc=com" write
        by * read
```

Install Zarafa phpldapadmin templates

Download the templates and extract the content to /var/www/phpldapadmin.

Create a Company, User and Alias

With the templates in place, log into phpldapadmin again and:

- create a company (Zarafa Company)
- create a user in the newly created company (Zarafa User Account)
- edit the user, add new attribute 'zarafaAlias'
    - assign at least one email alias to the user

This user and the mailalias will be needed later for testing the functionality of the server.

Zarafa Server Setup

Be sure to read the admin guide, this will cover only what needs to be changed so zarafa will work in this specific setup. All Zarafa server configuration files are stored in '**/etc/zarafa**'.
Zarafa v.7 Administrator Manual

zarafa-server and ldap.conf

The option 'enable_hosted_zarafa' will switch on multi-tenancy. If you don't want this feature set it to 'false'.

/etc/zarafa/server.cfg

```
server_bind             = 10.1.50.191

# Name for identifying the server in a multi-server environment
server_name = example.com

# local admin users who can connect to any store (use this for the zarafa-dagent)
# field is SPACE separated
local_admin_users       = root zarafa

# drop privileges and run the process as this user
run_as_user             = zarafa

# drop privileges and run the process as this group
run_as_group            = zarafa
```

```
# Database engine (mysql)
database_engine         = mysql

# e-mail address of the Zarafa System user
system_email_address    = postmaster@example.com

# The user under which we connect with MySQL
mysql_user              = zarafa

# The password for the user (leave empty for no password)
mysql_password          = secret

# Database to connect to
mysql_database          = zarafa

# Where to place attachments. Value can be 'database' or 'files'
attachment_storage      = database

# enable SSL support in server
server_ssl_enabled      = yes

# Listen for SSL connections on this port
server_ssl_port         = 237

# Required Server certificate, contains the certificate and the private key parts
server_ssl_key_file     = /etc/zarafa/ssl/mail.crt

# Password of Server certificate
server_ssl_key_pass     =

# Required Certificate Authority of server
server_ssl_ca_file      = /etc/zarafa/ssl/mail.key

# Path with CA certificates, e.g. /etc/ssl/certs
server_ssl_ca_path      = /etc/ssl/certs

# Path of SSL Public keys of clients
sslkeys_path            = /etc/zarafa/ssl

# Name of the plugin that handles users
# Required, default = ldap
# Values: ldap, unix, db, ldapms (available in enterprise license)
user_plugin             = ldap

# configuration file of the user plugin, examples can be found in /usr/share/zarafa/example-config
user_plugin_config      = /etc/zarafa/ldap.cfg

# Enable multi-tenancy environment
# When set to true it is possible to create tenants within the
# zarafa instance and assign all users and groups to particular
# tenants.
# When set to false, the normal single-tenancy environment is created.
enable_hosted_zarafa = true

# Use Indexing service for faster searching.
# Enabling this option requires the zarafa-indexer service to
# be running.
index_services_enabled = yes

# Path to the zarafa-indexer service, this option is only required
# if the server is going to make use of the indexing service.
index_services_path = file:///var/run/zarafa-indexer

# Time (in seconds) to wait for a connection to the zarafa-indexer service
# before terminating the indexed search request.
index_services_search_timeout = 10

# Allow enhanced ICS operations to speedup synchronization with cached profiles.
# default: yes
enable_enhanced_ics = yes
```

Copy the openldap configuration template to ldap.conf before you start editing.

/etc/zarafa/ldap.cfg

```
ldap_bind_user = userid=zarafaservice,dc=example,dc=com

# LDAP bind password
# Optional, default = empty (no password)
ldap_bind_passwd = secret

# Top level search base, every object should be available under this tree
ldap_search_base = dc=example,dc=com

# attribute name which is/(should: was) used in ldap_user_search_filter
ldap_object_type_attribute = objectClass
ldap_user_type_attribute_value = zarafa-user
ldap_group_type_attribute_value = zarafa-group
ldap_contact_type_attribute_value = zarafa-contact
ldap_company_type_attribute_value = organizationalUnit
ldap_addresslist_type_attribute_value = zarafa-addresslist
ldap_dynamicgroup_type_attribute_value = zarafa-dynamicgroup

# Optional, default = empty (match everything)
# For active directory, use:
#   (objectCategory=Person)
# For LDAP with posix users:
#   no need to use the search filter.
ldap_user_search_filter = (objectClass=zarafa-user)

# unique user id for find the user
# Note: contacts also use this field for uniqueness. If you change this,
# you might need to update the zarafa.schema file too, and change
# the MUST uidNumber to whatever you set here.dnl
ldap_user_unique_attribute = entryUUID

# Type of unique user id
# default: text
# For active directory, use:
#               binary
# For LDAP with posix user, use:
#               text
ldap_user_unique_attribute_type = text

# If set to bind, users are authenticated by trying to bind to the
# LDAP tree using their username + password.  Otherwise, the
# ldap_password_attribute is requested and checked.
ldap_authentication_method = bind

# unique company id for find the company
# Active directory: objectGUID
# LDAP: ou
ldap_company_unique_attribute = ou

# Optional, default = ou
# Active directory: ou
# LDAP: ou
ldap_companyname_attribute = ou

# Mapping from the quota attributes to a number of bytes.  Qmail-LDAP
# schema uses bytes (1), ADS uses kilobytes (1024*1024).
# We need to ajust this to 1MB in Bytes so we can use MB in phpldapadmin,
# otherwise quota won't work!
ldap_quota_multiplier = 1048576
```

zarafa-dagent

This is the service which talks to postfix and delivers mails to zarafa postboxes. The dagent must be enabled in zarafa's default file. We adjust some values for spam management here that will later tie in nicely with dspam.

/etc/default/zarafa

```
DAGENT_ENABLED=yes
DAGENT_CONFIG=/etc/zarafa/dagent.cfg
DAGENT_OPTS="-d"
```

/etc/zarafa/dagent.cfg

```
# drop privileges and run the process as this user
run_as_user             = zarafa

# drop privileges and run the process as this group
run_as_group            = zarafa

# Login to the Zarafa server using this SSL Key
sslkey_file = /etc/zarafa/ssl/mail.crt

# The following e-mail header will mark the mail as spam, so the mail
# is placed in the Junk Mail folder, and not the Inbox.
spam_header_name = X-DSPAM-Result

# If the above header is found, and contains the following value
# the mail will be considered as spam.
spam_header_value = Spam
```

zarafa-gateway

This service talks pop(s) and imap(s) to the outside world.

/etc/zarafa/dagent.cfg

```
# Set this value to a name to show in the logon greeting to clients.
# Leave empty to use DNS to find this name.
server_hostname = example.com

# Whether to show the hostname in the logon greeting to clients.
server_hostname_greeting = yes

# drop privileges and run the process as this user
run_as_user             = zarafa

# drop privileges and run the process as this group
run_as_group            = zarafa

# default connection to the Zarafa server
# Please refer to the administrator manual or manpage why HTTP is used rather than the UNIX socket.
server_socket = http://10.1.50.191:236/zarafa

# enable/disable POP3, and POP3 listen port
pop3_enable     =       yes
pop3_port       =       110

# enable/disable Secure POP3, and Secure POP3 listen port
pop3s_enable    =       yes
pop3s_port      =       995

# enable/disable IMAP, and IMAP listen port
imap_enable     =       yes
imap_port       =       143

# enable/disable Secure IMAP, and Secure IMAP listen port
imaps_enable    =       yes
imaps_port      =       993

# File with RSA key for SSL
ssl_private_key_file    =       /etc/zarafa/ssl/mail.key

#File with certificate for SSL
ssl_certificate_file    =       /etc/zarafa/ssl/mail.crt
```

zarafa-ical

This is the iCal / CALDAV Server. The preferred method is CALDAV though.

/etc/zarafa/ical.cfg

```
# wether normal connections can be made to the ical server
ical_enable = yes

# drop privileges and run the process as this user
run_as_user             = zarafa

# drop privileges and run the process as this group
run_as_group            = zarafa

# port which the ical server listens on for normal connections
ical_port = 8080

# default connection to the Zarafa server
# Please refer to the administrator manual or manpage why HTTP is used rather than the UNIX socket.
server_socket = http://10.1.50.191:236/zarafa

# wether ssl connections can be made to the ical server
icals_enable = yes

# port which the ical server listens on for ssl connections
icals_port = 8443

# File with RSA key for SSL
ssl_private_key_file = /etc/zarafa/ssl/web.key

# File with certificate for SSL
ssl_certificate_file = /etc/zarafa2/ssl/web.crt
```

zarafa-spooler

This service delivers mail to postfix to be sent into the intertubes. Luckily nothing must be adjusted here except the user and group settings.

/etc/zarafa/spooler.cfg

```
# drop privileges and run the process as this user
run_as_user             = zarafa

# drop privileges and run the process as this group
run_as_group            = zarafa
```

Z-Push Setup

Easy. Just get the source and unpack to '**/var/www**'. Create a symlink as we did with phpldapadmin before and you are done. (The same company that develops zarafa also develops z-push so all the defaults fit for the zarafa deployment). The directory 'state' has to be writeable by the webserver, so don't forget to chown it to the **www-data**-user. We also need to set up an apache alias so mobile devices that use Active Sync work correctly:

/etc/apache2/conf.d/zpush

```
 Alias /Microsoft-Server-ActiveSync /var/www/z-push/index.php
```

Apache2 Setup

We have to enable the rewrite and ssl modules and disable the default website. Also ports.conf has to be adjusted a little, otherwise apache barfs at startup.

```
~# a2enmod rewrite ssl
~# a2dissite default
```

/etc/apache2/ports.conf

```
NameVirtualHost 1.2.3.4:80
```

For webaccess we make sure **everything** gets rewritten to https.

/etc/apache2/sites-enabled/zarafa-webaccess

```
<VirtualHost 1.2.3.4:80>
  ServerName      zarafa.example.com
  ServerAdmin     webmaster@example.com

  RewriteEngine   On
  RewriteCond     %{HTTPS}        off
  RewriteRule     ^(.*)$          https://%{SERVER_NAME}%{REQUEST_URI} [L,R]

</VirtualHost>

<VirtualHost 1.2.3.4:443>

 ServerName      zarafa.example.com
 ServerAdmin     webmaster@example.com

 SSLEngine              on
 SSLCertificateFile     /etc/zarafa/ssl/web.crt
 SSLCertificateKeyFile  /etc/zarafa2/ssl/web.key

 DocumentRoot           /var/www

 Alias /phpldapadmin    /var/www/phpldapadmin
 Alias /webaccess       /usr/share/zarafa-webaccess

  <Directory /usr/share/zarafa-webaccess/>
    DirectoryIndex index.php
    Options -Indexes +FollowSymLinks
    AllowOverride Options

    Order allow,deny
    Allow from all
  </Directory>
</VirtualHost>
```

Syncing LDAP data to Zarafa

Every time you change things in LDAP you have to sync those changes to the Zarafa DB. Invoke the command 'zarafa-admin --sync' to do so. The option '-l' displays all users, use this to test if the synchronization worked.

```
~# zarafa-admin --sync
~# zarafa-admin -l
```

That's it. Now you should be able to log in to the Zarafa Webaccess with the user we configured with phpopenldap before.

postfix, sasl, dspam and clamav setup

postfix must be configured to do ldap user lookups which is done via ldap-users.cf and ldap-aliases.cf. Futher main.cf and master.cf need to be adjusted to scan mail for spam and viruses and deliver them to dagent via lmtp in the end. To authenticate users who are sending mails from external addresses we will use SASL with the remote IMAP (rimap) method, which basically performs a IMAP-login to check if the supplied password is correct.

postfix

This postfix config also contains enhanced recipient restrictions and mailq timeouts. If you do not know what they do you shouldn't use them.

main.cf

/etc/postfix/main.cf

```
smtpd_banner            = $myhostname ESMTP NO UCE
myhostname              = mail.example.com
biff                    = no
append_dot_mydomain     = no
mynetworks              = 127.0.0.0/8, 10.1.0.0/16
recipient_delimiter     = +
inet_interfaces         = all
myorigin                = $myhostname
mydestination           = $myhostname localhost.example.com, localhost

virtual_mailbox_domains = example.com, example.net, example.org
virtual_mailbox_maps    = ldap:/etc/postfix/ldap-users.cf
virtual_alias_maps      = ldap:/etc/postfix/ldap-aliases.cf
virtual_transport       = lmtp:127.0.0.1:2003

# SASL
smtpd_sasl_auth_enable          = yes
broken_sasl_auth_clients        = yes

# TLS encryptiion
smtpd_tls_security_level        = may
smtpd_tls_auth_only             = yes
smtpd_tls_cert_file             = /etc/postfix/keys/postfix.crt
smtpd_tls_key_file              = /etc/postfix/keys/postfix.key
smtpd_tls_CAfile                = /etc/postfix/keys/postfix.pem
smtpd_tls_loglevel              = 0
smtpd_tls_received_header       = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source               = dev:/dev/urandom

# check incoming mail for 'stuff'
smtpd_recipient_restrictions =
        permit_mynetworks,
        permit_sasl_authenticated,
        reject_unknown_recipient_domain,
        reject_non_fqdn_recipient,
        reject_non_fqdn_hostname,
        reject_non_fqdn_sender,
        reject_unauth_destination,
        reject_unauth_pipelining,
        reject_invalid_hostname

smtpd_data_restrictions =
        reject_unauth_pipelining

# client restrictions
smtpd_client_restrictions =
        permit_mynetworks,
        permit_auth_destination,
        permit_sasl_authenticated,
        check_client_access pcre:/etc/postfix/dspam_filter_access

# anybody out there?
smtpd_helo_restrictions =
        permit_mynetworks,
```

```
        reject_invalid_hostname,
        reject_non_fqdn_hostname

# who may send
smtpd_sender_restrictions =
        reject_unknown_sender_domain,
        reject_non_fqdn_sender,
        permit_sasl_authenticated,
        permit_mynetworks

# deferred mail intervals

# (default: 300 seconds; before Postfix 2.4: 1000s)
# How often the queue manager scans the queue for deferred mail.
queue_run_delay                = 900

# (default: 300 seconds; before Postfix 2.4: 1000s)
# The minimal amount of time a message won't be looked at, and the minimal amount of time to stay away from a
"dead" destination.
minimal_backoff_time           = 450

# (default: 4000 seconds)
# The maximal amount of time a message won't be looked at after a delivery failure.
maximal_backoff_time           = 1800

# (default: 5 days)
# How long a message stays in the queue before it is sent back as undeliverable. Specify 0 for mail that should
be returned immediately after the first unsuccessful delivery attempt.
maximal_queue_lifetime         = 14

# (default: 5 days, available with Postfix version 2.1 and later)
# How long a MAILER-DAEMON message stays in the queue before it is considered undeliverable. Specify 0 for mail
that should be tried only once.
bounce_queue_lifetime          = 14

# (default: 20000)
# The size of many in-memory queue manager data structures. Among others, this parameter limits the size of the
short-term, in-memory list of "dead" destinations. Destinations that don't fit the list are not added.
qmgr_message_recipient_limit   = 1000000

# max message size (15M)
message_size_limit             = 15360000
```

master.cf

The master transport file. Transport decisions are made here, in our case:
internet -> smpt:postfix -> socket:dspam -> socket:clamav -> dspam -> smtp:postfix -> lmtp:dagent

Notice: lmtp must not run chrooted, otherwise it won't be able to talk to dagent!

Edit: Added **smtps / submission** configuration, so postfix will also listen on ports 465 and 587, which is required by some clients to work correctly (TLS /SSL issues).

/etc/postfix/master.cf

```
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
smtp      inet  n       -       -       -       -       smtpd
 -o content_filter=lmtp:unix:/var/run/dspam/dspam.sock
submission inet n       -       -       -       -       smtpd
 -o content_filter=lmtp:unix:/var/run/dspam/dspam.sock
smtps     inet  n       -       -       -       -       smtpd
 -o smtpd_tls_wrappermode=yes
 -o smtpd_sasl_auth_enable=yes
pickup    fifo  n       -       -       60      1       pickup
cleanup   unix  n       -       -       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
tlsmgr    unix  -       -       -       1000?   1       tlsmgr
rewrite   unix  -       -       -       -       -       trivial-rewrite
bounce    unix  -       -       -       -       0       bounce
defer     unix  -       -       -       -       0       bounce
trace     unix  -       -       -       -       0       bounce
verify    unix  -       -       -       -       1       verify
flush     unix  n       -       -       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
proxywrite unix -       -       n       -       1       proxymap
smtp      unix  -       -       -       -       -       smtp
# 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
lmtp      unix  -       -       n       -       -       lmtp
anvil     unix  -       -       -       -       1       anvil
scache    unix  -       -       -       -       1       scache

# dspam
127.0.0.1:10026 inet    n       -       n       -       -       smtpd
        -o content_filter=
        -o receive_override_options=no_unknown_recipient_checks,no_header_body_checks
        -o smtpd_helo_restrictions=
        -o smtpd_client_restrictions=
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o mynetworks=127.0.0.0/8
        -o smtpd_authorized_xforward_hosts=127.0.0.0/8
```

ldap users and aliases

These files control ldap user and alias lookups

/etc/postfix/ldap-users.cf

```
server_host     = localhost
search_base     = dc=example,dc=com
version         = 3
bind            = yes
bind_dn         = uid=zarafaservice,dc=example,dc=com
bind_pw         = secret
scope           = sub
query_filter    = (mail=%s)
result_attribute        = mail
```

/etc/postfix/ldap-aliases.cf

```
server_host     = localhost
search_base     = dc=example,dc=com
version         = 3
bind            = yes
bind_dn         = uid=zarafaservice,dc=example,dc=com
bind_pw         = secret
scope           = sub
query_filter    = (zarafaAliases=%s)
result_attribute        = mail
```

Test LDAP connectivity

Test your setup by issuing the following commands. In both cases the email address of the user should be displayed.

```
~# postmap -q <insert-username-here>@example.com ldap:/etc/postfix/ldap-users.cf
~# postmap -q <insert-user-alias-here>@example.com ldap:/etc/postfix/ldap-aliases.cf
```

SASL

We have to add postfix to the sasl group and edit two files to make it work:

/etc/default/sasl

```
START=yes
DESC="SASL Authentication Daemon"
NAME="saslauthd"
MECHANISMS="rimap"
MECH_OPTIONS="127.0.0.1"
THREADS=5
OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd -r"
```

/etc/postfix/sasl/smtpd.conf

```
pwcheck_method: saslauthd
mech_list: plain login
```

add postfix to sasl

```
~# gpasswd -a postfix sasl
~# service postfix restart
~# service saslauthd restart
```

DSpam and ClamAV

DSpam can pass mails on the fly to clamav for virus scanning, all it need is a socket to pump the mails into. Therefore we need to adjust clamav a little. In the end we also set up 'group'-file for dspam so all users share a 'merged' anti-spam database. Furthermore we will integrate dspam with the Zarafa webinterface, so users can mark messages as spam or ham themselves.

First, however, setup the dspam database schemas. There are several schemas to choose from, please consult the documentation which one fits your needs best.

example dspam database setup

```
~# mysql -uroot -p dspam < /usr/share/doc/libdspam7-drv-mysql/mysql_objects-speed.sql
```

DSpam

/etc/dspam/dspam.d/mysql.conf

```
# --- MySQL ---
MySQLServer     /var/run/mysqld/mysqld.sock
MySQLPort         3306
MySQLUser       dspam
MySQLPass       secret
MySQLDb         dspam
MySQLConnectionCache    20
MySQLUIDInSignature    on
```

/etc/dspam/dspam.conf

```
Home /var/spool/dspam
StorageDriver   /usr/lib/dspam/libmysql_drv.so

DeliveryHost        127.0.0.1
DeliveryPort        10026
DeliveryIdent       localhost
DeliveryProto       SMTP
OnFail error

Trust root
Trust dspam
Trust zarafa
Trust www-data

TrainingMode teft
TestConditionalTraining on

Feature chained
Feature whitelist

Algorithm graham burton
PValue graham

SupressWebStats on
ImprobabilityDrive on
```

```
Preference "spamAction=tag"
Preference "showFactors=on"
Preference "spamSubject=**SPAM**"

AllowOverride trainingMode
AllowOverride spamAction spamSubject
AllowOverride statisticalSedation
AllowOverride enableBNR
AllowOverride enableWhitelist
AllowOverride signatureLocation
AllowOverride showFactors
AllowOverride optIn optOut
AllowOverride whitelistThreshold

HashRecMax              3145739
HashAutoExtend          on
HashMaxExtents          0
HashExtentSize          393241
HashMaxSeek             100
HashConnectionCache     10

IgnoreHeader Accept-Language
IgnoreHeader Approved
IgnoreHeader Archive
IgnoreHeader Authentication-Results
IgnoreHeader Cache-Post-Path
IgnoreHeader Cancel-Key
IgnoreHeader Cancel-Lock
IgnoreHeader Complaints-To
IgnoreHeader Content-Description
IgnoreHeader Content-Disposition
IgnoreHeader Content-ID
IgnoreHeader Content-Language
IgnoreHeader Content-Return
IgnoreHeader Content-Transfer-Encoding
IgnoreHeader Content-Type
IgnoreHeader DKIM-Signature
IgnoreHeader Date
IgnoreHeader Disposition-Notification-To
IgnoreHeader DomainKey-Signature
IgnoreHeader Importance
IgnoreHeader In-Reply-To
IgnoreHeader Injection-Info
IgnoreHeader Lines
IgnoreHeader Message-Id
IgnoreHeader Message-ID
IgnoreHeader NNTP-Posting-Date
IgnoreHeader NNTP-Posting-Host
IgnoreHeader Newsgroups
IgnoreHeader OpenPGP
IgnoreHeader Organization
IgnoreHeader Originator
IgnoreHeader PGP-ID
IgnoreHeader Path
IgnoreHeader Received
IgnoreHeader Received-SPF
IgnoreHeader References
IgnoreHeader Reply-To
IgnoreHeader Resent-Date
IgnoreHeader Resent-From
IgnoreHeader Resent-Message-ID
IgnoreHeader Thread-Index
IgnoreHeader Thread-Topic
IgnoreHeader User-Agent
IgnoreHeader X--MailScanner-SpamCheck
IgnoreHeader X-AV-Scanned
IgnoreHeader X-AVAS-Spam-Level
IgnoreHeader X-AVAS-Spam-Score
IgnoreHeader X-AVAS-Spam-Status
IgnoreHeader X-AVAS-Spam-Symbols
```

```
IgnoreHeader X-AVAS-Virus-Status
IgnoreHeader X-AVK-Virus-Check
IgnoreHeader X-Abuse
IgnoreHeader X-Abuse-Contact
IgnoreHeader X-Abuse-Info
IgnoreHeader X-Abuse-Management
IgnoreHeader X-Abuse-To
IgnoreHeader X-Abuse-and-DMCA-Info
IgnoreHeader X-Accept-Language
IgnoreHeader X-Admission-MailScanner-SpamCheck
IgnoreHeader X-Admission-MailScanner-SpamScore
IgnoreHeader X-Amavis-Alert
IgnoreHeader X-Amavis-Hold
IgnoreHeader X-Amavis-Modified
IgnoreHeader X-Amavis-OS-Fingerprint
IgnoreHeader X-Amavis-PenPals
IgnoreHeader X-Amavis-PolicyBank
IgnoreHeader X-AntiVirus
IgnoreHeader X-Antispam
IgnoreHeader X-Antivirus
IgnoreHeader X-Antivirus-Scanner
IgnoreHeader X-Antivirus-Status
IgnoreHeader X-Archive
IgnoreHeader X-Assp-Spam-Prob
IgnoreHeader X-Attention
IgnoreHeader X-BTI-AntiSpam
IgnoreHeader X-Barracuda
IgnoreHeader X-Barracuda-Bayes
IgnoreHeader X-Barracuda-Spam-Flag
IgnoreHeader X-Barracuda-Spam-Report
IgnoreHeader X-Barracuda-Spam-Score
IgnoreHeader X-Barracuda-Spam-Status
IgnoreHeader X-Barracuda-Virus-Scanned
IgnoreHeader X-Bogosity
IgnoreHeader X-Brightmail-Tracker
IgnoreHeader X-CRM114-CacheID
IgnoreHeader X-CRM114-Status
IgnoreHeader X-CRM114-Version
IgnoreHeader X-CTASD-IP
IgnoreHeader X-CTASD-RefID
IgnoreHeader X-CTASD-Sender
IgnoreHeader X-Cache
IgnoreHeader X-ClamAntiVirus-Scanner
IgnoreHeader X-Comment-To
IgnoreHeader X-Comments
IgnoreHeader X-Complaints
IgnoreHeader X-Complaints-Info
IgnoreHeader X-Complaints-To
IgnoreHeader X-DKIM
IgnoreHeader X-DMCA-Complaints-To
IgnoreHeader X-DMCA-Notifications
IgnoreHeader X-Despammed-Tracer
IgnoreHeader X-ELTE-SpamCheck
IgnoreHeader X-ELTE-SpamCheck-Details
IgnoreHeader X-ELTE-SpamScore
IgnoreHeader X-ELTE-SpamVersion
IgnoreHeader X-ELTE-VirusStatus
IgnoreHeader X-Enigmail-Supports
IgnoreHeader X-Enigmail-Version
IgnoreHeader X-Extra-Info
IgnoreHeader X-Face
IgnoreHeader X-Forwarded
IgnoreHeader X-GMX-Antispam
IgnoreHeader X-GMX-Antivirus
IgnoreHeader X-GPG-Fingerprint
IgnoreHeader X-GPG-Key-ID
IgnoreHeader X-GPS-DegDec
IgnoreHeader X-GPS-MGRS
IgnoreHeader X-GWSPAM
IgnoreHeader X-Gateway
IgnoreHeader X-Greylist
```

```
IgnoreHeader X-HTMLM
IgnoreHeader X-HTMLM-Info
IgnoreHeader X-HTMLM-Score
IgnoreHeader X-HTTP-Posting-Host
IgnoreHeader X-HTTP-UserAgent
IgnoreHeader X-HTTP-Via
IgnoreHeader X-ID
IgnoreHeader X-IMAIL-SPAM-STATISTICS
IgnoreHeader X-IMAIL-SPAM-URL-DBL
IgnoreHeader X-IMAIL-SPAM-VALFROM
IgnoreHeader X-IMAIL-SPAM-VALHELO
IgnoreHeader X-IMAIL-SPAM-VALREVDNS
IgnoreHeader X-Info
IgnoreHeader X-IronPort-Anti-Spam-Filtered
IgnoreHeader X-IronPort-Anti-Spam-Result
IgnoreHeader X-KSV-Antispam
IgnoreHeader X-Kaspersky-Antivirus
IgnoreHeader X-MDAV-Processed
IgnoreHeader X-MDRemoteIP
IgnoreHeader X-MDaemon-Deliver-To
IgnoreHeader X-MIE-MailScanner-SpamCheck
IgnoreHeader X-MIMEOLE
IgnoreHeader X-MIMETrack
IgnoreHeader X-MMS-Spam-Filter-ID
IgnoreHeader X-MS-Has-Attach
IgnoreHeader X-MS-TNEF-Correlator
IgnoreHeader X-MSMail-Priority
IgnoreHeader X-MailScanner
IgnoreHeader X-MailScanner-Information
IgnoreHeader X-MailScanner-SpamCheck
IgnoreHeader X-Mailer
IgnoreHeader X-Mlf-Spam-Status
IgnoreHeader X-NAI-Spam-Checker-Version
IgnoreHeader X-NAI-Spam-Flag
IgnoreHeader X-NAI-Spam-Level
IgnoreHeader X-NAI-Spam-Report
IgnoreHeader X-NAI-Spam-Route
IgnoreHeader X-NAI-Spam-Rules
IgnoreHeader X-NAI-Spam-Score
IgnoreHeader X-NAI-Spam-Threshold
IgnoreHeader X-NEWT-spamscore
IgnoreHeader X-NNTP-Posting-Date
IgnoreHeader X-NNTP-Posting-Host
IgnoreHeader X-NetcoreISpam1-ECMScanner
IgnoreHeader X-NetcoreISpam1-ECMScanner-From
IgnoreHeader X-NetcoreISpam1-ECMScanner-Information
IgnoreHeader X-NetcoreISpam1-ECMScanner-SpamCheck
IgnoreHeader X-NetcoreISpam1-ECMScanner-SpamScore
IgnoreHeader X-Newsreader
IgnoreHeader X-Newsserver
IgnoreHeader X-No-Archive
IgnoreHeader X-No-Spam
IgnoreHeader X-OSBF-Lua-Score
IgnoreHeader X-OWM-SpamCheck
IgnoreHeader X-OWM-VirusCheck
IgnoreHeader X-Olypen-Virus
IgnoreHeader X-Orig-Path
IgnoreHeader X-OriginalArrivalTime
IgnoreHeader X-Originating-IP
IgnoreHeader X-PAA-AntiVirus
IgnoreHeader X-PAA-AntiVirus-Message
IgnoreHeader X-PGP-Fingerprint
IgnoreHeader X-PGP-Hash
IgnoreHeader X-PGP-ID
IgnoreHeader X-PGP-Key
IgnoreHeader X-PGP-Key-Fingerprint
IgnoreHeader X-PGP-KeyID
IgnoreHeader X-PGP-Sig
IgnoreHeader X-PIRONET-NDH-MailScanner-SpamCheck
IgnoreHeader X-PIRONET-NDH-MailScanner-SpamScore
IgnoreHeader X-PMX
```

```
IgnoreHeader X-PMX-Version
IgnoreHeader X-PN-SPAMFiltered
IgnoreHeader X-Posting-Agent
IgnoreHeader X-Posting-ID
IgnoreHeader X-Posting-IP
IgnoreHeader X-Priority
IgnoreHeader X-Proofpoint-Spam-Details
IgnoreHeader X-Qmail-Scanner-1.25st
IgnoreHeader X-Quarantine-ID
IgnoreHeader X-RAV-AntiVirus
IgnoreHeader X-RITmySpam
IgnoreHeader X-RITmySpam-IP
IgnoreHeader X-RITmySpam-Spam
IgnoreHeader X-Rc-Spam
IgnoreHeader X-Rc-Virus
IgnoreHeader X-Received-Date
IgnoreHeader X-RedHat-Spam-Score
IgnoreHeader X-RedHat-Spam-Warning
IgnoreHeader X-RegEx
IgnoreHeader X-RegEx-Score
IgnoreHeader X-Rocket-Spam
IgnoreHeader X-SA-GROUP
IgnoreHeader X-SA-RECEIPTSTATUS
IgnoreHeader X-STA-NotSpam
IgnoreHeader X-STA-Spam
IgnoreHeader X-Scam-grey
IgnoreHeader X-Scanned-By
IgnoreHeader X-SenderID
IgnoreHeader X-Sohu-Antivirus
IgnoreHeader X-Spam
IgnoreHeader X-Spam-ASN
IgnoreHeader X-Spam-Check
IgnoreHeader X-Spam-Checked-By
IgnoreHeader X-Spam-Checker
IgnoreHeader X-Spam-Checker-Version
IgnoreHeader X-Spam-Clean
IgnoreHeader X-Spam-DCC
IgnoreHeader X-Spam-Details
IgnoreHeader X-Spam-Filter
IgnoreHeader X-Spam-Filtered
IgnoreHeader X-Spam-Flag
IgnoreHeader X-Spam-Level
IgnoreHeader X-Spam-OrigSender
IgnoreHeader X-Spam-Pct
IgnoreHeader X-Spam-Prev-Subject
IgnoreHeader X-Spam-Processed
IgnoreHeader X-Spam-Pyzor
IgnoreHeader X-Spam-Rating
IgnoreHeader X-Spam-Report
IgnoreHeader X-Spam-Scanned
IgnoreHeader X-Spam-Score
IgnoreHeader X-Spam-Status
IgnoreHeader X-Spam-Tagged
IgnoreHeader X-Spam-Tests
IgnoreHeader X-Spam-Tests-Failed
IgnoreHeader X-Spam-Virus
IgnoreHeader X-Spam-Warning
IgnoreHeader X-Spam-detection-level
IgnoreHeader X-SpamAssassin-Clean
IgnoreHeader X-SpamAssassin-Warning
IgnoreHeader X-SpamBouncer
IgnoreHeader X-SpamCatcher-Score
IgnoreHeader X-SpamCop-Checked
IgnoreHeader X-SpamCop-Disposition
IgnoreHeader X-SpamCop-Whitelisted
IgnoreHeader X-SpamDetected
IgnoreHeader X-SpamInfo
IgnoreHeader X-SpamPal
IgnoreHeader X-SpamPal-Timeout
IgnoreHeader X-SpamReason
IgnoreHeader X-SpamScore
```

```
IgnoreHeader X-SpamTest-Categories
IgnoreHeader X-SpamTest-Info
IgnoreHeader X-SpamTest-Method
IgnoreHeader X-SpamTest-Status
IgnoreHeader X-SpamTest-Version
IgnoreHeader X-Spamadvice
IgnoreHeader X-Spamarrest-noauth
IgnoreHeader X-Spamarrest-speedcode
IgnoreHeader X-Spambayes-Classification
IgnoreHeader X-Spamcount
IgnoreHeader X-Spamsensitivity
IgnoreHeader X-TERRACE-SPAMMARK
IgnoreHeader X-TERRACE-SPAMRATE
IgnoreHeader X-TM-AS-Category-Info
IgnoreHeader X-TM-AS-MatchedID
IgnoreHeader X-TM-AS-Product-Ver
IgnoreHeader X-TM-AS-Result
IgnoreHeader X-TMWD-Spam-Summary
IgnoreHeader X-TNEFEvaluated
IgnoreHeader X-Text-Classification
IgnoreHeader X-Text-Classification-Data
IgnoreHeader X-Trace
IgnoreHeader X-UCD-Spam-Score
IgnoreHeader X-User-Agent
IgnoreHeader X-User-ID
IgnoreHeader X-User-System
IgnoreHeader X-Virus-Check
IgnoreHeader X-Virus-Checked
IgnoreHeader X-Virus-Checker-Version
IgnoreHeader X-Virus-Scan
IgnoreHeader X-Virus-Scanned
IgnoreHeader X-Virus-Scanner
IgnoreHeader X-Virus-Scanner-Result
IgnoreHeader X-Virus-Status
IgnoreHeader X-VirusChecked
IgnoreHeader X-Virusscan
IgnoreHeader X-WSS-ID
IgnoreHeader X-WinProxy-AntiVirus
IgnoreHeader X-WinProxy-AntiVirus-Message
IgnoreHeader X-cid
IgnoreHeader X-iHateSpam-Checked
IgnoreHeader X-iHateSpam-Quarantined
IgnoreHeader X-policyd-weight
IgnoreHeader X-purgate
IgnoreHeader X-purgate-Ad
IgnoreHeader X-purgate-ID
IgnoreHeader X-sgxh1
IgnoreHeader X-to-viruscore
IgnoreHeader Xref
IgnoreHeader acceptlanguage
IgnoreHeader thread-index
IgnoreHeader x-uscspam
IgnoreHeader X-Paranoid-Spam
IgnoreHeader X-Paranoid-Prob
IgnoreHeader X-Paranoid-Report
IgnoreHeader X-ArGoMail-Read

Notifications   off
LocalMX 127.0.0.1 10.1.50.191 # <your mta here>

SystemLog on
UserLog   on
Opt out

ParseToHeaders on
ChangeModeOnParse on
ChangeUserOnParse full

Broken case

ClamAVPort      3310
```

```
ClamAVHost      127.0.0.1
ClamAVResponse  spam

ServerQueueSize 32
ServerPID               /var/run/dspam/dspam.pid
ServerMode auto
ServerParameters "--deliver=innocent -d %u"
ServerIdent "localhost"

ServerDomainSocketPath  "/var/run/dspam/dspam.sock"

ClientHost "/var/run/dspam/dspam.sock"
ClientIdent "secret@Relay1"

ProcessorBias on

Include /etc/dspam/dspam.d/
```

/var/spool/dspam/group

```
dspam:shared:*
```

/etc/postfix/dspam_filter_access

```
# Everything beginning with either ham or spam avoids the filter
/^(spam|ham)@.*$/ OK

# The rest is redirected to be filtered
/./ FILTER dspam:dspam
```

Webaccess DSpam Integration

First get the plugin from the community page. Unzip it directly into the webaccess/plugins folder, adjust the config a little and fix some permissions on the dspam config files (dspam complains otherwise). To activate the plugin's debug log, set the parameter 'dspam_log' to a path instead of 'false'.

install plugin

```
~# tar xzvf plugin.tar.gz -C /usr/shares/zarafa-webaccess/plugins/
~# chown -R root: /usr/shares/zarafa-webaccess/plugins/dspam
```

configure plugin

```
~# vim /usr/shares/zarafa-webaccess/plugins/dspam/config.php
```

config.php

```
<?php
/**
 * DSPAM training plugin

$GLOBALS['pluginconfig']['dspam']['defaults'] = array(
        // path to the dspam command (must be executable by the httpd user)
        'dspam_cmd' => '/usr/bin/dspam',
        // name of dspam user to collect date for or false for the current user
        'dspam_user' => 'dspam',
        // path to log file for error debugging or false for no logging
        //'dspam_log' => '/tmp/dspam-plugin.log'
          'dspam_log' => false
)
?>
```

fix dspam config permissions

```
~# chmod o+r /etc/dspam/dspam.conf
~# chmod o+r /etc/dspam/dspam.d/mysql.conf
```

Now purge your browser cache. A new 'Junk/No Junk' item should appear in the right-click menu. Marking elements as junk will move them into the 'Trash' folder and inject them into dspam, training it as spam. Unmarking will leave the message as it is, but train it as ham. Check if the plugin is working correctly in the debug log.

ClamAV

/etc/clamav.clamd.cfg

```
LocalSocket /var/run/clamav/clamd.ctl
FixStaleSocket true
LocalSocketGroup clamav
LocalSocketMode 666
User clamav
AllowSupplementaryGroups true
ScanMail true
ScanArchive true
ArchiveBlockEncrypted false
MaxDirectoryRecursion 15
FollowDirectorySymlinks false
FollowFileSymlinks false
ReadTimeout 180
MaxThreads 12
MaxConnectionQueueLength 15
LogSyslog true
LogFacility LOG_LOCAL6
LogClean false
LogVerbose false
PidFile /var/run/clamav/clamd.pid
DatabaseDirectory /var/lib/clamav
SelfCheck 3600
Foreground false
Debug false
ScanPE true
ScanOLE2 true
ScanHTML true
DetectBrokenExecutables false
ExitOnOOM false
LeaveTemporaryFiles false
AlgorithmicDetection true
ScanELF true
IdleTimeout 30
PhishingSignatures true
PhishingScanURLs true
PhishingAlwaysBlockSSLMismatch false
PhishingAlwaysBlockCloak false
DetectPUA false
ScanPartialMessages false
HeuristicScanPrecedence false
StructuredDataDetection false
CommandReadTimeout 5
SendBufTimeout 200
MaxQueue 100
ExtendedDetectionInfo true
OLE2BlockMacros false
StreamMaxLength 25M
Bytecode true
BytecodeSecurity TrustSigned
BytecodeTimeout 60000
OfficialDatabaseOnly false
CrossFilesystems true
TCPSocket 3310
```

Regular Maintenance

Drop this file into '/etc/cron.d'. It's pretty self-explanatory, however you might want adjust the values and/or intervals.

/etc/cron.d/zarafa-jobs

```
# minute (0-59),
# |     hour (0-23),
# |     |       day of the month (1-31),
# |     |       |       month of the year (1-12),
# |     |       |       |       day of the week (0-7 with 0=7=Sunday).
# |     |       |       |       |       user
# |     |       |       |       |       |       command

# sync LDAP to Zarafa regularly
*/15    *       *       *       *       root    /usr/bin/zarafa-admin --sync

# purge soft-deleted items after 30 days
3       30      *       *       *       root    /usr/bin/zarafa-admin --purge-softdelete 30
```

Testing / Verifying the setup

- Send Mails via
  - WebAccess
  - pop/pops
  - imap/imaps
- Deliver mails
  - check MTA logs
  - check dspam information in mailhaeders
  - check dspam mail (dspam_stats -H)

Thanks

Various readers for proofreading and pointing out errors and/or ambiguous statements.

Contact

Additions, comments, critisicm? mail to: b2c[at]dest-unreachable.net