

Maildrop-Extension

Philipp Haefelfinger <philipp.haefelfinger@syscp.org>
Ron Brand <ron.brand@syscp.org>
Florian Aders <florian.aders@syscp.org>

Maildrop-Extension

by Philipp Haefelfinger, Ron Brand, and Florian Aders
Copyright © 2005, 2006 SysCP

This work is licensed under the Creative Commons Attribution-Noncommercial-Share Alike 2.0 Germany License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/2.0/de/> or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

Table of Contents

Introduction	v
1. Installation	6
1. Get the Sources	6
2. Apply the Patch	6
2.1. maildrop_mysql-sarge.patch	6
2.2. maildrop-sarge.patch	6
3. Compile Maildrop	6
4. Install Maildrop	7
2. Configuration	8
1. Maildrop configurationfile	8
2. Maildropsript	8
3. Postfix - adjustments	9
4. Spamassassin	10
5. ClamAV	10
3. SysCP-Modules for Maildrop and Spamassassin	12
1. SysCP-Module Maildrop	12
2. SysCP-Module SA-Settings	12
A. The last words	13
1. Credits	13
2. Disclaimer	13

Introduction

Maildrop is being used for filtering purposes and automated delivery in the appropriate directories. To guarantee a smooth operation with *SysCP* there must be a small change of code in Maildrop.

Even though the man page of maildrop is quite informative, there might be a misunderstanding when it comes to connection with MySQL. The Author likes to give a brief explanation thereof:

The user-data is stored in a MySQL-Database. maildrop fetches these data (homedir and maildir) out of the database, however, before the execution takes place (in delivery-mode, Option -d), all data that was taken from MySQL (homedir, maildir, etc.) will be deleted and replaced with default values.

On that point the question might raise what is going on here: We have a MySQL-Database where all data of the mailaccount are present, but maildrop simply refuse to use them? Does that make sense? A definite answer is not possible. It could be happening that some of the environment-variables are declared wrong, and therefore cause errors or (worse) could be used to manipulate the entire system. But this can only happen if data are retrieved not from the database but from those environment-variables.

Thinking that over we might come to this conclusion: We only verify, if all data were taken correctly from the database. If data were not completely fetched error free then default values must be used. If all data were fetched they can be used, since manipulation of the database hopefully should not be possible.

Not only because of this kind of "bug", but more because of the non present MySQL-support, we will do a new compile of maildrop. The following instructions will show you how to do this.

If you prefer not to compile it by yourself you may freely use the precompiled package of the author. The package was compiled on a Debian-Sarge Installation. You can get the latest file from chimera.ch [<http://www.chimera.ch>] too, where a amd64 package is also available.

Chapter 1. Installation

1. Get the Sources

Eventually your `sources.list` needs to be updated according to your needs. When done go the directory `/usr/src` and run the following commands. To make sure your package list has the latest information:

```
syscp ~ # apt-get update
```

When updated you can get the sources by running:

```
syscp ~ # apt-get source courier-maildrop
```

```
syscp ~ # apt-get build-dep courier-maildrop
```

First command gets the source of maildrop being stored in the directory `/usr/src/courier-<version>`. Second command makes sure all packages needed to compile maildrop will be installed and configured.

2. Apply the Patch

Its time to copy the patch into the directory `/usr/src`. The patch changes two elementary settings in the Courier-Maildrop-Package.

- Activation of MySQL support
- Removal of Code which prevents an error free operation with postfix

You can find the patch here [<http://www.syscp.org/wiki/docs/Installation/config>]. To apply the patch run the following command in the directory `/usr/src`

```
syscp ~ # patch -p0 < maildrop_mysql-sarge.patch
```

There are two different patch files we might need.

2.1. maildrop_mysql-sarge.patch

This patch eliminates the problem with the environment-variables and also adjusts the rules-file for the compile. The rule says that MySQL should be used and that users vmail and postfix must be accepted as a trusted user. Otherwise maildrop will be ignoring all inputs from postfix. This patch is for all who don't want to adjust the build-option manually.

2.2. maildrop-sarge.patch

This patch only changes the source of maildrop. Problems with environment-variables are not involved. The rules-files for the build are not going to be changed. If you use this patch, all build-options must be done manually, or maildrop will not function properly. This patch is for all who have a deeper knowledge and who are able to adjust the build-options according to their needs.

3. Compile Maildrop

Maidrop is now patched and ready to compile. To compile Courier-Maidrop run the following command in `/usr/src`:

```
syscp ~ # apt-get source courier-maidrop -b
```

Since the sources are already present and unpacked, Debian will skip this step and starts with configure followed by a compile. Unfortunately the whole Courier-system is compiled, not only maidrop. Therefore we get more than one `.deb`-Files at the end.

4. Install Maidrop

Of course our maidrop also has to be installed. In the same directory as before `/usr/src` run the following command:

```
syscp ~ # dpkg -i courier-maidrop<version>.deb
```

Additionally, after installation the system has to be informed not to upgrade in case of a **apt-get** upgrade since we are using a patched package

```
syscp ~ # echo courier-maidrop hold | dpkg --set-selections
```

The hold-status can be switched by

```
syscp ~ # echo courier-maidrop install | dpkg --set-selections
```

To verify your settings use

```
syscp ~ # dpkg -l courier-maidrop
```

Below is an example for an output, given by the above verification-command

```
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Installed/Config-files/Unpacked/Failed-config/Half-installed
| / Err?=====(none)/Hold/Reinst-required/X=both-problems (Status,Err: uppercase=)
||/ Name          Version          Description
++-+-----+-----+-----+
hi courier-maldr 0.47-4          Courier Mail Server - Mail delivery agent
```

Reading the first character will inform you about the status. Character `h` stands for hold and confirms that this package is not being upgraded automatically.

Chapter 2. Configuration

1. Maildrop configurationfile

To avoid a termination with error code Signal 0x0B the configuration-file must be created now. Here you find an example of a typical configuration file.

```
/etc/courier/maildropmysql.config
```

```
hostname                localhost
socket                  /var/run/mysqld/mysqld.sock
port                    3306
database                syscp
dbuser                  syscp
dbpw                    SYSCPPASSWD
dbtable                 mail_users
default_uidnumber       2000
default_gid             2000
uid_field               email
uidnumber_field         uid
gidnumber_field         gid
maildir_field           maildir
homedirectory_field     homedir
quota_field             100000000
#quota_field            quota
# unused for now, but needs to be a valid field.
mailstatus_field        postfix
where_clause            AND postfix = 'Y'
```

The privileges of this files are recommended as 600. Keep in mind that it contains the password for syscp.

2. Maildropscrip

In order to give a detailed instruction of operation for maildrop we need the file `/etc/courier/maildroprc` which contains these instructions. This script forwards the mail to the virus-scanner or spam-filter and checks for results. Use the script from here [<http://www.syscp.de/wiki/docs/Installation/config/maildroprc>] and adapt the configuration of it to your needs:

```
/etc/courier/maildroprc
```

```
[...]
#Configuration
#####
# set this to 1 if you want to log the usersettings vor vscan, etc.
LOGUSERSETTINGS=0

# Full path to the maildrop log of each user
LOGFILEPATH=$HOME$DEFAULT/maildrop.log

# Setting for SysCP maildrop module
USESYSCPSETTINGS=0

# Basedir of your syscp installation
SYSCPBASEDIR="/var/www/syscp"
```

```
# Default setting for the spamfilter
SPAMFILTER=0

# use spamc instead of the direct call to spamassassin
USESPAMC=1

# Default setting for the virusscan
VSCAN=0

# include userdefined filters into maildrop
USERFILTER=0

# basedir of your userdefined filterfiles
MAILFILTERDIR="/var/kunden/mailfilter"

# Only scan mails smaller than SCANSPAMSIZE for spam
SCANSPAMSIZE="2000000"

# Only scan mails smaller than VSCANSIZE for a virus
VSCANSIZE="2000000"
[...]
```

You may use the variable `SPAMFILTER` for a default activity of the spam-filter, where a value of 1 activates and a value of 0 deactivates the filter. Likewise the same applies to `VSCAN` which controls the behaviour of the virus-scanner. In case the `SysCP`-module for maildrop is installed, the value of `USESYSYSCPSETTINGS` can be set to 1 to engage a retrieval for virus-scanner / spamfilter from the `SysCP` database.

3. Postfix - adjustments

To let postfix know, that mails are forwarded to maildrop instead of using the own virtual-daemon the adjustments below need to be done. The value of the variable `virtual_transport` will be switched from virtual into maildrop

```
/etc/postfix/main.cf
```

```
[...]
virtual_gid_maps = mysql:/etc/postfix/mysql-virtual_gid_maps.cf
#virtual_gid_maps = static:2000

# use this for virtual delivery
#virtual_transport = virtual
# use this for maildrop-delivery
virtual_transport = maildrop

#Maildrop-Options for usage with maildrop
maildrop_destination_recipient_limit = 1
maildrop_destination_concurrency_limit = 1
[...]
```

Postfix also needs to know where exactly the target maildrop is located. It will be done by an adjustment of the file `/etc/postfix/master.cf`. The original file should already contain an commented out line for maildrop.

Please note the whitespaces in the second line. Postfix is quite sensitive regarding the syntax of `master.cf`

Once again we also like to point out: Don't use Windows - Editors (e.g. Notepad.exe)

```
/etc/postfix/master.cf
```

```
[...]
maildrop    unix    -    n    n    -    -    pipe
           flags=R  user=vmail argv=/usr/bin/maildrop -d ${recipient}
[...]
```

4. Spamassassin

For installation and configuration of Spamassassin please refer to the countless HowTos you can find on the Internet. For an operation with maildrop a default installation is sufficient. It is up to you, if you prefer further filter, rules and plugins.

The current configuration here [<http://www.syscp.org/wiki/docs/Installation/config/spamassassin>] can be chosen to operate either with spamc or spamassassin. If you have a close look into `/etc/courier/maildroprc` you'll find `xfilter-lines`. Some users have reported that `spamd` will not start. By default `spamd` is deactivated. Therefore it has to be activated. Once again a small change to a configuration-file must be done.

In case you want to use maildrop in conjunction with spamc, the options have to be adjusted as well, because `spamd` must run as user `vmail`, otherwise no access to the settings in `/var/kunden/mail` is possible.

`/etc/default/spamassassin`

```
[...]
# Change to one to enable spamd
ENABLED=1
[...]
```

```
[...]
# Default options for use with spamassassin
#OPTIONS="--create-prefs --max-children 5 --helper-home-dir"

# My options for use with spamc and maildrop
OPTIONS="--create-prefs --max-children 5 -q -x -u vmail"
```

5. ClamAV

The only needed shell script for a cooperation with maildrop is as follows:

`/usr/bin/clamscan.sh`

```
#!/bin/bash
# Created by Tom Walsh, slim at ala.net
# slightly modified by Wolfgang Ziegler, nuppla at gmx.at

RUN=clamscan
# Enable this line, if you are using the clamav-daemon.
# RUN=clamdscan

#start
MSG=$(cat /proc/self/fd/0) # stdin -> $MSG
SCAN=$(echo "$MSG" | $RUN --stdout --disable-summary)
EXIT="$?"
VIRUS=$(echo "$SCAN" | awk '{print $2}')
SUBJECT=$(echo "$MSG" | reformail -x Subject:)

if [ "$EXIT" == "1" ]; then
    SUBJECT="''VIRUS'' [$VIRUS] $SUBJECT"
    MSG=$(echo "$MSG" | reformail -i"X-Virus-Status: INFECTED")
```

```
MSG=$(echo "$MSG" | reformail -i"Subject: $(echo "$SUBJECT)")")
else
MSG=$(echo "$MSG" | reformail -i"X-Virus-Status: CLEAN")
fi

echo "$MSG"
exit 0
```

Chapter 3. SysCP-Modules for Maildrop and Spamassassin

For being able to use the option "USESYSACPSETTINGS" in the file maildroprc, at least the *SysCP* Module for maildrop needs to be installed. If you would like to adjust the settings of spamassassin on your *SysCP* frontend, the module SA-Settings can be recommended. You can find it in our contribution - forum [<http://syscp-forum.org/index.php?board=35.0>].

Although both modules are optimized for a dual operation, they can work separately of course.

Basically just follow the install-instruction for both modules.

1. SysCP-Module Maildrop

Using this *SysCP*-module users can decide, if mails will be routed through the virus-scanner or the spam-filter. Due to the law in some countries, which forbids any filtering without confirmation of the user, it is advisable to switch the filter off by default and leave it to the customer itself.

2. SysCP-Module SA-Settings

This module is used to enable any adjustment of the Spamassassin-settings directly through the *SysCP* Frontend. Spamassassin gets all settings from the *SysCP*-database. This is helpful, as you don't have to change the configfile each time you want to adjust something. Furthermore all settings are possible for each individual domains, and are not only available as a global context

Appendix A. The last words

1. Credits

This HowTo was originally written by Philipp Haefelfinger and might be maintained by himself most probably.

His "thanks a lot" goes to some persons:

- Ron Brand for joining many times into discussions, and the English translation of this HowTo.
- Martin Burchert for countless assistance on many topics

2. Disclaimer

This HowTo was written to the best of the authors knowledge. Although it will be maintained carefully, the author cannot guarantee a 100% error free work. Use it at your own risc. The author can not be held responsible for damage on hard/software due to the usage of this document. Feel free to distribute this HowTo as long as the Credits and Disclaimer will remain untouched.