magic-smtpd User’s Manual

Josh Wilsdon <josh@wizard.ca>

23rd April 2004

Contents

Chapter 1

Introduction

The MagicMail Server is an Internet email transport software package developed by LinuxMagic Inc. With all of the optional features disabled, magic-smtpd acts as a drop in replacement for the qmail-smtpd daemon that is included with Qmail. This means that any system currently running Qmail should be able to install magic-smtpd in place of qmail-smtpd without any problems. This document describes the installation and configuration of the magic-smtpd program.

1.1 Features

The main advantages of using magic-smtpd over the SMTP daemon that comes with qmail (qmail-smtpd), are that magic-smtpd has:

1. The ability to check the validity of users before accepting mail destined to them, in order to reduce the number of bounced messages. [Chapter 3]
2. The ability to do SMTP authentication to allow users with dynamic addresses the ability to relay through your server. [Chapter 4]
3. The ability to limit the rate/amount of email coming in on a given SMTP session in order to discourage spamming and reduce server resource usage. [Chapter 7.4]
4. The ability to do basic spam checking at the SMTP level. [Chapter 5]

The commercial version of magic-smtpd also integrates with magic-local, and other proprietary tools to provide additional features such as more advanced spam checking, and virus checking at the delivery level.

Chapter 2

Installation

2.1 Introduction and Prerequisites

Currently, the only supported method for installation is via source code. In order to do a source install you will need the following:

- Linux (see NOTES section below)
- the GNU C compiler + standard C development libraries and headers
- Berkeley DB development files version 2 or greater (see NOTES section below)
- the magic-smtpd-X.X.X.tar.gz tarball (see NOTES section below, X.X.X will be the version number)
- Qmail must already be installed and running with qmail-smtpd running under tcpserver

If you have compiled other software on your machine in the past, you most likely have the minimum requirements to build this package.

2.2 Build Process

Building the magic-smtpd binary should be mostly straightforward if you have built other software packages in the past. Please read this entire section before beginning. The process should progress as follows (each step is annotated below):

1. tar zxfv magic-smtpd-<version>.tar.gz
2. cd magic-smtpd-<version>
3. make

4. mkdir -p /etc/magic-mail/control
5. magic-smtpd -s

Step 1 uses the "tar" command to both uncompress and un-archive the tarball. The "<version>" string should be replaced with the actual version (so that it matches the file you actually have). This will create a directory "magic-smtpd-<version>" in the current directory. Steps 2 and 3 change the working directory to the magic-smtpd source directory and begin the build process respectively. If you receive errors when compiling, you will need to resolve these before continuing. If you need refer to the mailing lists (see Chapter 10.1). Step 4 will create an empty control directory, and step 5 should produce output consisting of the current magic-smtpd configuration if the magic-smtpd binary has been properly built.

2.3 Installation

This section will guide you through the installation of the new binary you have built in Chapter 2.2. Please read this entire section before beginning. The process should progress as follows (each step is annotated below):

1. cp magic-smtpd /var/qmail/bin/magic-smtpd
2. chown root.qmail /var/qmail/bin/magic-smtpd
3. mv -i /var/qmail/bin/qmail-smtpd /var/qmail/bin/qmail-smtpd.old
4. ln -s /var/qmail/bin/magic-smtpd /var/qmail/bin/qmail-smtpd
5. test that your email is working correctly

Steps 1 and 2 place the magic-smtpd binary in the proper location with the proper permissions. If your qmail installation is in a directory other than /var/qmail, you will need to alter the commands accordingly. Steps 3 and 4 are very critical. If they are not performed properly, the SMTP service could be left in a non-functional state. During the time between execution of step 3 and execution of step 4, your SMTP server will be rejecting new connections. Once you have created the link for the magic-smtpd daemon (step 4) you should begin testing your new configuration (this is step 5). To do this, you can use any mail client which connects to your SMTP server, and attempt to send an email. If the mail is successfully sent, you have successfully installed the magic-smtpd daemon. Once you have verified that your configuration is functioning properly, you can begin to configure the additional features provided by magic-smtpd which are described in the rest of this document.

2.4 NOTES

- This software may work on other UNIX-like operating systems, but this has not been tested, nor can it be supported at this time. If you need help with this, please refer to the mailing lists.
- You only need the Berkeley DB development files if you are going to be compiling in DBFILE support. As this is not currently recommended it is not enabled by default.
- The latest tarball can be found on the LinuxMagic website at the URL: http://www.linuxmagic.com/opensource/magicmail/magic-smtpd/
- If you are not running qmail-smtpd under tcpserver, you will need to adjust the instructions in this section accordingly.

Chapter 3

Valid-User Checking

3.1 Description

Valid-User Checking is used to reject mail at the SMTP level destined to email addresses which do not exist on the server. Using this feature decreases the number of messages your server needs to queue for bounces. In many cases this offers a significant savings in terms of server resources. To begin using magic-smtpd for Valid-User Checking, you should look over the next 3 sections and configure one of the 3 methods. Once you have configured the system for your chosen method, refer to Chapter 3.5 for details on activating your configuration. After activating your configuration you can refer to Chapter 3.6 for instructions on testing your configuration.

3.2 External Program

This is the currently recommended method for the OpenSource version. To use this method, you will need an executable program or script with the following characteristics:

- takes an email address in user@domain format as its only command line argument
- exits with value 0 (user exists) or 1 (user does not exist)

This program can also optionally (required if you want to use spam checking without either the dbfile or database backends) print to stdout (descriptor 1) the directory which holds the spam rules for the email address which was passed as the command line argument (see Chapter 5 for information on spam checking). The absolute path to this program should be placed in the control file “ext_check_user_prog”. There is a sample script included in the magic-smtpd distribution tarball “scripts/vpopmail-check-user.sh” which should work for most vpopmail installations.

3.3 Berkeley DB file

When a server is configured to use this method, all spam rules and user information are stored in Berkeley DB database files. This allows very fast access with a very small i/o load. The format of the DB file is documented in the file builddb/doc/KEY_FORMAT. The builddb tool (see Chapter 9) can be used to build this file if an appropriate module is available. To use this method, support must be compiled into your binary, and you must have the “user_info_dbfile” and “spam_rule_dbfile” control files set with the location of your DB files. You must also set the control file “use_dbfile” to a boolean true value.

NOTE: As of this writing there are no builddb modules available in the OpenSource package. This means that unless you either build the dbfile manually or write your own module, you will be unable to use the dbfile method at this time.

3.4 Magicmail Database

This method is only available in the commercial version of MagicMail. With this method, the magic-smtpd daemon gets all spam and user information from the MagicMail database.

3.5 Enabling Valid-User Checking

To enable valid user checking you must first have configured one of the mechanisms detailed in the previous 3 sections. After configuring the appropriate method, you must activate this feature by specifying a boolean true value in the control file "check_valid_users" (see Chapter 7.1 for details on using control files).

3.6 Testing Valid-User Checking

In order to verify that Valid-User checking is working, you will need to have 2 email addresses handy: one which you know is an existing user and one that you know is not. In the following examples the addresses “validuser@wizard.ca” and “invaliduser@wizard.ca” will be used for the valid and invalid addresses respectively. Once you have these email addresses you can test as follows (the *italicized* portions indicate your input):

```
./magic-smtpd
220 wizard.ca ESMTP
MAIL FROM: josh@wizard.ca
250 ok
```

```
RCPT TO: invaliduser@wizard.ca
550 User does not exist
QUIT
221 wizard.ca
```

this was a test with a user known to not be valid. If you receive a “250 ok” message rather than the “550 User does not exist” message in response to your “RCPT TO:” command, the system thinks that the user does exist. If this works properly, you should also test with a known-valid user:

```
./magic-smtpd
220 wizard.ca ESMTP
MAIL FROM: josh@wizard.ca
250 ok
RCPT TO: validuser@wizard.ca
250 ok
QUIT
221 wizard.ca
```

If you receive a “550 User does not exist” rather than the “250 ok” in response to your “RCPT TO:” command, this means that your configuration is incorrect. If it does not work for you, please recheck your configuration and try again. If it works properly and you get the proper response to both of these test cases: congratulations, you have successfully configured Valid-User checking.

Chapter 4

SMTP Authentication

4.1 Introduction

The magic-smtpd daemon supports SMTP Authentication (As described in RFC2554). After authenticating themselves, users are allowed to relay mail to remote servers. This allows clients that have dynamic addresses to use the server running magic-smtpd as their outgoing mail-server without much work on the part of the administrator. To enable SMTP authentication you will need to set a boolean "true" value in the file:

/etc/magic-mail/control/auth_enable

Doing this will turn on support for the SMTP AUTH command. The authentication can be done either against an external program, against a Berkeley DB file or (in the commercial version only) against the MagicMail database. Chapters 4.3, 4.4 and 4.5 give more information on configuring each of these authentication types.

4.2 Support AUTH types

Currently magic-smtpd only supports the "LOGIN" AUTH type. This is the type that is used by Microsoft's Outlook and Outlook Express and the most commonly used by mail clients. In the future we plan to add support for at least the "PLAIN" and "CRAM-MD5" types. We may add support for more types if there is sufficient demand and time permits.

4.3 External Program

This is the currently recommended method for the OpenSource version. In order to use this method for SMTP authentication you must specify the external program to use for authentication (including the absolute path) in the control file “ext_check_passwd_prog”. This program must be compatible with Dan Bernstein’s checkpassword program interface. More information on this interface is available at the following URL:

http://cr.yp.to/checkpwd/interface.html

Being that the program only needs to be compatible with the checkpassword program, almost any program which is being used with an existing Qmail installation for POP3 authentication (assuming you are using the included qmail-popup and qmail-pop3d programs) can be used directly for SMTP authentication, including the vchkpw program included in the vpopmail package.

4.4 Berkeley DB file

With this method, SMTP authentication will be done against a Berkeley DB file. To use this method, you must set the boolean control option “use_dbfile” to a boolean “true” value. With this method usernames and encrypted passwords are stored in a Berkeley DB file. When a user attempts authentication, magic-smtpd will access the file and compare the password the user has sent with their authentication request with the password in the file. The file used for this authentication can be specified using the “user_info_dbfile” control file. The format of the records read from this file must match that generated by the builddb program which is included in the source distribution.

NOTES:

- Berkeley DB versions 2, 3 and 4 are supported.
- If an external program is also specified for authentication, the external program will be run first and the Berkeley DB file will only be used if the specified program has an error.
- In the commercial version, if the use_database option is selected, the database will also take precedence over the Berkeley DB file and the external program. Processing will only continue to the next method if there is an error reading from the MagicMail database.
- As of this writing there are no builddb modules available in the OpenSource package. This means that unless you either build the dbfile manually or write your own module, you will be unable to use the dbfile method at this time.

4.5 MagicMail Database

This method is only available in the commercial version of MagicMail. With this method, the magic-smtpd daemon does user authentication against the MagicMail database.

4.6 Enabling SMTP Authentication

Once you have selected one of the authentication backend types from the preceding 3 sections, you will still need to activate SMTP authentication before it can be used on your server. In order to do this, you must set a boolean true value in the control file “auth_enable”. After doing this, you can test that SMTP authentication is working by following the instructions in the next section.

4.7 Testing SMTP Authentication

In order to test SMTP Authentication, you will need to know the base64 encoded value of a valid username and password for your mailserver. To find these, you can run the following commands on the command-line (after replacing the strings *username* and *password* with the actual username and password):

```
perl -e "use MIME::Base64; print encode_base64(’username’)"
perl -e "use MIME::Base64; print encode_base64(’password’)"
```

The resulting strings were: *dXNlcm5hbWU=* and *cGFzc3dvcmQ=* in this example. After you have the base64 encoded strings, you can make a telnet connection to the localhost (these commands should be run on the machine running magic-smtpd) and do a test of the SMTP Authentication feature (the italicized portions *indicate* your input):

```
telnet localhost 25
Trying 127.0.0.1....
Connected to localhost.
Escape character is ’^]’.
220 wizard.ca ESMTP
EHLO wizard.ca
250-wizard.ca
250-AUTH LOGIN
250-AUTH=LOGIN
250-PIPELINING
250 8BITMIME
AUTH LOGIN dXNlcm5hbWU=
334 UGFzc3dvcmQ6
```

```
cGFzc3dvcmQ=
235 ok, go ahead (#2.0.0)
```

If you do not see the “AUTH LOGIN” lines as part of the response to your “EHLO” command, this means that the SMTP Authentication has not been properly enabled. Please double check your settings and try again. The “AUTH LOGIN” command’s argument is the base64 encoded username. The subsequent “334 UGFzc3dvcmQ6” prompt actually says “334 Password:” as this string is base64 encoded, so your response should be the base64 encoded version of your password. If something is misconfigured, or your password or username are incorrect you will instead see either “454 problems performing authorization (#4.3.0)” or “535 authorization failed (#5.7.0)”. If you receive either of these messages, you will need to doublecheck your settings and the username and password you are using. If you receive the “235 ok, go ahead (#2.0.0)” message as above: congratulations, you now have your server configured for SMTP Authentication and should be able to configure your mail client to use this.

Chapter 5

Spam Checking

5.1 How spam rules are loaded

5.1.1 External Program

This is the currently recommended method for the OpenSource version. In order to use this method, you will also need to be using an external program for Valid-User checking which writes a directory out to stdout for each user. Once you have this configured, the spam rules will be loaded from the directory specified by the Valid-User program. The directory is assumed to have all spam rules in separate files similar to qmail control files. This means you would have one file named “spam_check” which would contain the value “true” and one file named “smtp_check” which contains the value “true”. For options which take multiple values (such as whitelists and blacklists) you must specify these values on multiple lines, with one value per line. A list of spam rules that can be configured is included in Appendix A, and a detailed description of each rule is included in Chapter 5.3.

5.1.2 Berkeley DB File

With this method, spam rules will be loaded from a Berkeley DB file. To use this method, you must set the boolean control option “use_dbfile” to a boolean “true” value. When email comes in the user’s email_id will be looked up from the user_info_dbfile and the rules from that id will be looked up in the dbfile containing the spam rules. The file which contains these spam rules can be specified using the “spam_rule_dbfile” control file. The format of the records read from this file must match that generated by the builddb program which is included in the source distribution.

NOTES:

- Berkeley DB versions 2, 3 and 4 are supported.
- If an external program is also specified for authentication, the external program will be run first and the Berkeley DB file will only be used if the specified program has an error.
- In the commercial version, if the use_database option is selected, the database will also take precedence over the Berkeley DB file and the external program. Processing will only continue to the next method if there is an error reading from the MagicMail database.
- As of this writing there are no builddb modules available in the open-source package. This means that unless you either build the dbfile manually or write your own module, you will be unable to use the dbfile method at this time.

5.1.3 PostgreSQL database

This method is only available in the commercial version of MagicMail. With this method, the magic-smtpd daemon loads users' spam rules from the MagicMail database.

5.2 Global Rules

5.2.1 With DBFile and Database

With either the database or dbfile methods for loading spam rules, there is a special email_id (id 0) which will be used (if they exist) as the "global rules". These rules can be set by the administrator in the commercial version using the MagicMail web interface. Chapter 5.3.19 explains some more about including these global rules conditionally for users.

5.2.2 With External Program

In contrast to the database and dbfile methods, when using an external program for spam rule loading there is no special id (in fact there are no id's at all) which can be used for global rules. Because of this there is no way currently to implement global rules when using the external program method for spam rule loading.

5.3 SMTP Spam Checking

5.3.1 NOTES

- See Chapter 5.1 for details on enabling the spam rules listed here with your chosen method.

- With the OpenSource version, you will always need to enable to three rules “spam_check”, “smtp_check” and “smtp_blocking” in order to be able to utilize any of the other spam checking options.
- With the OpenSource version, you must always use the values “true” or “false” for boolean spam controls. Do not use “1” or “0” or any other values.
- Whitelists always take precedence over blacklists and other rules. This means that if a message is on a whitelist, it will not be marked as spam no matter which blacklists or other rules determine it to be spam.

5.3.2 spam_check

This option must be set to “true” in order for any spam checking to be done. If this option is not set, or is set to “false”, none of the other checks will be done.

5.3.3 smtp_check

This enables checks in the magic-smtpd daemon. In the OpenSource version this should always be set to “true” as without this none of the other checks will be done.

5.3.4 smtp_blocking

With the commercial version of MagicMail, when spam is detected at the SMTP level there are two things which can be done:

1. the message can be refused
2. the message can be marked to go into the quarantine

This option is used to select between them. If this is set to “true” the message will be refused if it is detected to be spam. If this option is set to “false” (the default) the message will be marked so that when magic-local receives the message, it will be placed in the quarantine folder.

NOTE: With the OpenSource version this rule must always be set “true” in order to do any spam checking.

5.3.5 valid_from_domain

If this rule is set, the domain of the email address set as the SMTP “MAIL FROM” address will be checked. Thus if the remote uses the command “MAIL FROM: josh@wizard.ca”, the domain that will be checked will be wizard.ca. If the domain has neither an A record nor an MX record available via DNS, this rule will mark the message as spam.

5.3.6 check_dynamic_reverse_dns

If this rule is set and tcpserver has set the TCPREMOTEHOST variable, the TCPREMOTEHOST is checked to see if it is a host in the form X-X-X-X.domain.com (where the X's are numbers which could be IP address octets). If the hostname is found to match this pattern, this rule will mark the message as spam.

5.3.7 require_full_addr

This rule will mark the message as spam if the “RCPT TO:” recipient address does not include an @ character and at least one character before and after it.

5.3.8 block_mail_from_self

This rule will mark the message as spam if the “RCPT TO:” recipient address is exactly the same as the “MAIL FROM:” sender address.

5.3.9 block_ip_in_addr

This rule will mark the message as spam if the email address in either the “MAIL FROM:” or “RCPT TO:” is in the form user@X.X.X.X where X.X.X.X is an IP Address.

5.3.10 valid_bounce

This rule will mark the message as spam if the magic-smtpd daemon cannot connect to tcp port 25 on a mail exchange (as specified in DNS by an MX record) for the domain of the email address included with the “MAIL FROM:” command.

5.3.11 require_helo

This rule will mark the message as spam if the remote SMTP client does not send either a HELO or an EHLO command at the beginning of their SMTP transaction.

5.3.12 valid_helo_domain

This rule will mark the message as spam if the hostname given in the “HELO” or “EHLO” command does not have either an A record or an MX record available via DNS.

5.3.13 mail_from_strict_addr_parse

This rule will mark the message as spam if the address given in the "MAIL FROM:" command is not in the format:

> <user@domain>

where "user" and "domain" are at least 1 character and the <,@ and > characters are all present.

5.3.14 check_ip_reverse_dns

This rule will mark the message as spam if the IP address of the SMTP client that is connecting to the magic-smtpd server does not have a reverse DNS record (a PTR record).

5.3.15 from_blacklist, from_whitelist

The from_whitelist and from_blacklist rules are lists of regular expressions that will be run on the email address passed as an argument to "MAIL FROM:" by the connecting SMTP client. If the address is matched by an entry in the from_whitelist the message will not be marked as spam regardless of whether other rules have marked it as spam or not. If the message is matched by an entry in the from_blacklist it will be marked as spam. As always, the whitelist takes precedence in the case where an entry is both whitelisted and blacklisted. Entries on both lists should be valid extended POSIX regular expressions. An example would be:

> ^j.*@wizard.ca$

which would match "josh@wizard.ca", "joe@wizard.ca" and any other email address with a name that starts with j and whose domain is wizard.ca. If you use a simple substring like:

> wizard

this would match "josh@wizard.ca" or "wizard@domain.com" or any other address which contains the string "wizard".

NOTE: These regular expressions can be fairly complicated. Please make sure you know what you are doing if you use more complicated forms.

5.3.16 helo_blacklist, helo_whitelist

The helo_whitelist and helo_blacklist rules are lists of regular expressions that will be run on the hostname passed as an argument to the "HELO" or "EHLO" by the connecting SMTP client. If the hostname is matched by an entry in the helo_whitelist the message will not be marked as spam regardless of whether other rules have marked it as spam or not. If the message is matched by the helo_blacklist it will be marked as spam. As always, the whitelist takes precedence in the case where an entry is both whitelisted and blacklisted. Entries on both lists should be valid extended POSIX regular expressions. An example would be:

```
^m.*wizard.ca$
```

which would match "mail.wizard.ca", "mx.wizard.ca" and any other address with a name that starts with m and whose domain is wizard.ca. If you use a simple substring like:

```
wizard
```

this would match "mail.wizard.ca" or "wizard.domain.com" or any other hostname which contains the string "wizard".

NOTE: These regular expressions can be fairly complicated. Please make sure you know what you are doing if you use more complicated forms.

5.3.17 country_blacklist, country_whitelist

The country_whitelist and country_blacklist define lists of country codes. These country codes must be the 2 letter country codes as defined by IANA. A list of these country codes can be found at:

http://www.iana.org/cctld/cctld-whois.htm

Each entry in this list should consist only of the two letters of the country code. No other characters should be present. The connecting IP address will be checked against a database in order to determine which country the client is connected from. If the country that the client connects from is found on the country_whitelist, the message will not be marked as spam regardless of what other rules determine the message is spam. If the country is on the country_blacklist, the message will be marked as spam. If a country is both whitelisted and blacklisted, the whitelist will take precedence.

NOTE: please see Chapter 5.5 for some special information pertaining to country code based rules.

5.3.18 ip_blacklist, ip_whitelist

The ip_whitelist and ip_blacklist define lists IP addresses which should never or always be treated as sending spam respectively. If a message comes from an IP address on the ip_whitelist, it will never be marked as spam regardless of which other rules determine it to be spam. If the IP address of the connecting client is on the ip_blacklist the message will be marked as spam. The whitelists always take precedence over blacklists, so if a message is both whitelisted and blacklisted it will not be marked as spam.

5.3.19 all_global_rules, use_global_*

The all_global_rules rule, and all of the spam rules which begin with use_global_ will function correctly only for the DBFile and Database spam rule loading mechanisms. When available, the use_global* rules simply state for each global list, whether or not that list should be used for the user for whom they are set. The all_global_rules option changes the spam rule defaults, so that rather than the system defaults, the global user's rules are used as the defaults.

5.4 Delivery Level Spam Checking

Spam checks which are done at the delivery level are done by the magic-local program. This program is available only with the commercial version of MagicMail Server.

5.5 Special Considerations for Country Rules

In order to do lookups to match IP addresses to country codes, magic-smtpd utilizes the database that comes with the perl IP::Country module. There are two files included with this module named "ip.gif" and "cc.gif". The directory in which both of these files exist should be specified in the "ip2country_datadir" MagicMail control file.

Chapter 6

FAQ - Frequently Asked Questions

6.1 Does magic-smtpd support TLS?

No. Currently there is no support for TLS in magic-smtpd. This will be added eventually, but there is no schedule yet as to when it will be available.

6.2 Does magic-smtpd work on FreeBSD/OpenBSD/Solaris?

Previous versions have been reported to work on FreeBSD with some small patches to the build process. We have developed MagicMail on Linux running on the x86 architecture and do not currently have the resources to test on other operating systems or architectures. In theory it should work fine on any Unix-like system. Hopefully at some point in the future we will have the resources available to test each release on several combinations of operating system and hardware.

6.3 Can magic-smtpd do virus checking?

No. Virus scanning is supported in the commercial version of MagicMail, but that checking is done at the magic-local (delivery) level, not at the SMTP level.

6.4 Can magic-smtpd block attachments?

No. As magic-smtpd does not scan the body or headers of the message, it has no way to determine the type of attachments, or even whether there are attachments at all.

Chapter 7

Configuration

7.1 Using Control Files

Configuration of the magic-smtpd daemon is done through Qmail style control files. These files exist in the directory specified at compile time which by default is "/etc/magic-mail/control". Each file is named after the option for which it holds values. The content of each file will be treated by magic-smtpd as the value(s) of that option. Each control file is expected to have a specific type of values. These types are described in detail in Chapter 7.2. You can refer to [Appendix B] for a list of available control files and the type of data they expect. If any of these files do not exist, the default value for that option will be used.

7.2 Control File Types

When magic-smtpd reads it's control files, it has a specific type of value that it expects in each control file. You can find out which type is expected in a given control file by looking at the output of the "magic-smtpd -s" command, or by looking at the table in Appendix B. The next sections describe each of these types in detail.

7.2.1 Integer

Control options which expect integer values are expected to have the following properties:

- less than 2147483647
- greater than -2147483647
- contains only the digits 0-9 and optionally prefixed with - or + sign

7.2.2 Program

Control options which are listed as type “program” are expected to have a single executable binary as their value. This program should be specified with an absolute path such as:

```
/var/qmail/bin/qmail-queue
```

7.2.3 Boolean

Control options which are listed as type “boolean” are expected to have either a “true” or “false” value. Several different forms are accepted (case insensitive):

true	false
true	false
on	off
yes	no
1	0

7.2.4 String

Control files listed as having the “string” type are expected to have a single line string value. This can be an arbitrary length string but must consist of only one line. It is expected that this line be composed of ASCII characters only. Foreign character sets and Unicode are not supported at this time.

7.2.5 Directory

Control options which are listed as type "directory" are expected to have a single directory (readable to the user magic-smtpd runs as) as their value. This directory must exist, and should be specified with an absolute path such as:

```
/var/qmail/queue/
```

NOTE: currently it is required to place a trailing “/” character on the directory specified by this option.

7.2.6 Filename

Control options which are listed as type "filename" are expected to have a single file (readable to the user magic-smtpd runs as) as their value. This file must exist, and should be specified with an absolute path such as:

```
/var/qmail/control/defaultdomain
```

7.3 Logging

Magic-smtpd uses syslog to log information about its execution. The logs will go to the syslog “mail” facility with appropriate priorities. For logs to be written out to disk, a syslog daemon must be running. On most machines this daemon is called syslogd and the configuration file is in /etc/syslogd.conf. The configuration of this daemon is outside the scope of this document, but it must be configured properly before log messages will be received from magic-smtpd. After a syslog daemon has been configured, the user may also want to adjust the level of output which magic-smtpd produces. This can be done with the control file “log_level”. The value set by this control file determines the minimum priority messages that will be written to syslog. Messages at and above (on the chart below) the value specified for “log_level” will be written to syslog.

Value	Syslog Priority	Description
0	LOG_EMERG	system is unusable
1	LOG_ALERT	action must be taken immediately
2	LOG_CRIT	critical conditions
3	LOG_ERR	error conditions
4	LOG_WARNING	warning conditions
5	LOG_NOTICE	normal but significant condition
6	LOG_INFO	informational
7	LOG_DEBUG	debug-level messages

For example: if the log_level control indicates a log_level of 4, warning conditions (4), error conditions (3), critical conditions (2), alerts (1) and emergency messages (0) will be printed, but notice (5), informational (6) and debug (7) messages will not.

7.4 Limits

This section describes those control files which can be used to put limits on resource usage.

7.4.1 max_hops

This option specifies the maximum number of “Received:” and “Delivered-To:” headers allowed in a message before flagging a message as being in a mail delivery loop. (default is 100)

7.4.2 max_invalid_rcpt

This option specifies the maximum number of “RCPT” commands which contain non-existent users that will be accepted per connection before printing a 550 message and exiting. If this value is set to “0” there will be no limit. (this the default)

7.4.3 max_line_length

This option specifies the maximum length of a command string or message line that will be read before returning an error message to the sending client. (the default is 1024)

7.4.4 max_rcpt

This option specifies the maximum number of “RCPT” commands allowed per client connection. If this value is set to “0” there will be no limit. (this the default)

7.4.5 max_smtp_cmds

This is the maximum number of SMTP commands that will be processed per individual connection. Exceeding this amount will return a 552 error code to the client and disconnect. If this value is set to “0” there will be no limit. (this the default)

7.4.6 rcpt_delay_at

The number of “RCPT” commands to allow before imposing the RCPT delay penalty for a client. If this value is set to “0” there will be no limit. (this the default)

7.4.7 rcpt_delay_inc

The number of seconds to increment the value of RCPT delay for each “RCPT” command after the rcpt_delay_at threshold is exceeded. If this value is set to “0” there will be no limit. (this the default)

7.4.8 rcpt_delay_max

The maximum number of seconds to raise RCPT delay to. If this value is set to “0” there will be no limit. (this the default)

7.5 Other Controls

This section describes those control files which are not related to Logging (Chapter 7.3) or Limits (Chapter 7.4).

7.5.1 add_check_flags

This option is only used by the commercial version of MagicMail and should always be disabled in the OpenSource version.

7.5.2 always_virus_check

This option is only used by the commercial version of MagicMail and should be ignored in the OpenSource version.

7.5.3 auth_enable

This option can be used to enable or disable SMTP Authentication. If this option is set to a boolean true value, SMTP Authentication will be available. See Chapter 4 for more information about SMTP Authentication.

7.5.4 check_valid_users

This option can be used to enable or disable Valid User Checking. If this option is set to a boolean true value, The recipients specified in by the RCPT command will be checked before being accepted. If the user does not exist using your configured Valid User Checking mechanism, the remote server will receive a “550 User does not exist” message. See Chapter 3 for more information on Valid User Checking.

7.5.5 dbname, dbhost, dbport, dbuser, dbpwd, fallback_db, spam_log_db, spam_table

These options are only used by the commercial version of MagicMail and should be ignored in the OpenSource version.

7.5.6 defaultdomain

This option can be used to specify a domain to be assumed when an RCPT command does not include the domain. If the defaultdomain is set to “domain.com” then issuing the command “RCPT TO: joe” will cause magic-smtpd to treat this RCPT as though it had been sent as “RCPT TO: joe@domain.com”.

7.5.7 dump_core

If this option is enabled, the server will write a core dump file to /var/cores/magic-smtpd/PID/core if a segmentation violation signal is received (segfault). If you are having problems with magic-smtpd segfaulting, turning this option on is a good idea as these core dumps will be helpful to developers trying to track down your problem.

7.5.8 ext_check_passwd_prog

When using SMTP Authentication with the External Program method, the program specified by this control file will be used for the authentication. The program must operate with the interface of Dan Bernstein's check-password program, and must be executable by the user who is running magic-smtpd. See Chapter 4.3 for more details on SMTP Authentication with this method.

7.5.9 ext_check_user_prog

When using Valid User Checking with the External Program method, the program specified by this control file will be run for each RCPT recipient in order to determine whether that recipient is valid or not. This program can also output a directory to stdout (descriptor 1) for valid users in order to have spam rules loaded from that directory. See Chapter 3.2 for more details.

7.5.10 ip2country_datadir

This option specifies the directory containing the ip and countrycode databases from the perl IP::Country module. See Chapter 5.5 for more details.

7.5.11 qmail_local

This option is used by magic-local to determine the path of qmail's version of qmail-local. It is only used by the commercial version of MagicMail and should be ignored in the OpenSource version.

7.5.12 qmail_queue

This option can be used to specify an alternate qmail-queue binary. This can be especially useful for running programs like qmail-scanner to do virus and spam checking. This option works in quite the same manner as the QMAILQUEUE environment variable does with the QMAILQUEUE patch applied to qmail. magic-smtpd also supports the QMAILQUEUE environment variable for compatibility.

7.5.13 qmailcontroldir

This option specifies the directory which contains the qmail control files. These are loaded by magic-smtpd for compatibility purposes. The default value is "/var/qmail/control/" and this should only be changed if you have installed qmail elsewhere. Please note that this option currently requires a trailing '/' character in order for it to function properly.

7.5.14 rfc_addr_only

If this option is enabled (it is disabled by default), the magic-smtpd daemon will reject and RCPT commands which do not include the “<” and “>” brackets. This can prevent some spam from even needing to be scanned. It can also prevent legitimate mail from misconfigured or poorly designed software, so one must take care when enabling this option.

7.5.15 stray_newline_detection

By default qmail is very strict about stray newlines in messages, as these are forbidden by RFC2821. Unfortunately several mailservers and many client applications are not well behaved. This option can be set to “false” in order to allow the magic-smtpd daemon to be less strict about checking for stray newlines. The default is to do the stray newline detection in the same manner as qmail-smtpd.

7.5.16 spam_check_enable

This option turns on or off spam checking. If this option is set to a boolean true value (by default this is disabled), spam rules will be checked on a per user basis in a manner determined by the method that is being used for loading users’ rules. See Chapter 5 for more information on spam checking.

7.5.17 use_database

This option is used to enable support for the MagicMail database as a backend for SMTP Authentication, Valid User Checking and loading spam rules. It is only available in the commercial version of MagicMail and should be ignored in the OpenSource version.

7.5.18 use_dbfile

This option is used to enable support for using Berkeley DB files for SMTP Authentication, Valid User Checking and loading of spam rules. If support for Berkeley DB has been compiled in to magic-smtpd, you can set this option to a boolean true value in order to enable this method.

7.5.19 user_info_dbfile, spam_rule_dbfile

When Berkeley DB files are being used for SMTP Authentication, Valid User Checking and/or loading of spam rules, these options can be used to specify the location of the DB files to use. The user_info_dbfile should specify the DB file which contains user information such as directories, passwords and quotas. The spam_rule_dbfile should contain the spam rules.

See Chapter 9 for more information on these DB files, and the program which can build them for you.

7.5.20 virus_local

This option is not used by magic-smtpd. It is used by magic-local to determine the version of qmail-local to use which supports virus checking. It can only be used by the commercial version of MagicMail and should be ignored in the OpenSource version.

7.5.21 welcome_message

This option specifies the location of the file which will be linked to all new users directories. It should always be read only and must be on the same partition as the mail files. This option is not used by magic-smtpd and is only used by the commercial version of MagicMail. It should be ignored in the OpenSource version.

7.6 Troubleshooting

One of the first things you should do when troubleshooting problems with the magic-smtpd daemon is to run the daemon with the “-s” command line option. This will print out a list of the settings that the daemon is configured to use. If any settings in this list seem incorrect, you should ensure that you have set values for all control files appropriate for the feature which is not functioning correctly. If you come across an issue that you are unable to resolve your next resort should be to ask for help on the mailing list (Chapter 10.1).

Chapter 8

Versions

8.1 How to determine which version you have

In order to determine which version of magic-smtpd you have you can simply run the command “magic-smtpd -v”. This will generate a string such as the following:

```
OpenSource 0.8.1 (compiled: Mar 29 2004) +EXTPROG +DBFILE
```

Which will tell you which version you are running (in this case “OpenSource 0.8.1”), the date it was compiled, and which extensions are enabled (in this case EXTPROG and DBFILE).

8.2 Differences between Commercial and OpenSource versions

The main differences between the commercial and the OpenSource versions of MagicMail are: the MagicMail database (which isn’t available in the Opensource version), the administration interface, and the available support. For more information about the commercial version please visit:

http://magicmail.linuxmagic.com/

Chapter 9

builddb program

The builddb program can be used to build a database suitable for use with the magic-smtpd daemon. Currently however we do not have an OpenSource module for this program and thus it is not able to build a file except for the commercial version.

Chapter 10

Where to get help

10.1 Mailing Lists

The “magicmail-users” mailing list has been created for discussion of issues related to the Magicmail system. You can subscribe to this list by sending an empty email message to “magicmail-users-subscribe@linuxmagic.com”.

10.2 Commercial Support

If you are unable to resolve your problems on your own, Wizard IT Services can provide support. Support is done on an hourly rate with 15 minute increments. For more details on this support service please contact Wizard IT by telephone at (604) 589-0037 or by email at <sales@wizard.ca>. You can also check out their website at http://www.wizard.ca/.

Appendix A

Spam Rules

Rule Name	Value Type	SMTP
spam_check	boolean	Yes
smtp_blocking	boolean	Yes
valid_from_domain	boolean	Yes
virus_check	boolean	No
block_non_printable	boolean	No
use_spamassassin	boolean	No
required_header_list	string	No
subject_whitelist	string	No
subject_blacklist	string	No
header_from_whitelist	string	No
header_from_blacklist	string	No
all_global_rules	boolean	Yes
smtp_check	boolean	Yes
delivery_check	boolean	No
check_dynamic_reverse_dns	boolean	Yes
require_full_addr	boolean	Yes
block_mail_from_self	boolean	Yes
block_ip_in_addr	boolean	Yes
require_me_in_dest	boolean	No
valid_bounce	boolean	Yes
require_helo	boolean	Yes
valid_helo_domain	boolean	Yes
mail_from_strict_addr_parse	boolean	Yes
check_ip_reverse_dns	boolean	Yes
use_global_from_blacklist	boolean	Yes
use_global_from_whitelist	boolean	Yes
from_blacklist	list	Yes
from_whitelist	list	Yes
helo_blacklist	list	Yes
helo_whitelist	list	Yes
use_global_helo_blacklist	boolean	Yes
use_global_helo_whitelist	boolean	Yes
use_global_country_blacklist	boolean	Yes
country_blacklist	list	Yes
country_whitelist	list	Yes
use_global_ip_blacklist	boolean	Yes
use_global_ip_whitelist	boolean	Yes
ip_blacklist	list	Yes
ip_whitelist	list	Yes

Appendix B

Configuration Options

Filename	Value Type	Default Value	Relevance
add_check_flags	boolean	0	Commercial
always_virus_check	boolean	0	Commercial
auth_enable	boolean	0	Both
check_valid_users	boolean	0	Both
dbname	string		Commercial
dbhost	string		Commercial
dbport	string		Commercial
dbuser	string		Commercial
dbpwd	string		Commercial
defaultdomain	string		Both
dump_core	boolean	0	Both
ext_check_passwd_prog	program		OpenSource
ext_check_user_prog	program		OpenSource
fallback_db	boolean	1	Commercial
ip2country_datadir	directory	/usr/local/share/perl/5.6.1/IP/Country/Fast	Both
log_level	integer	ountry/Fast	Both
max_hops	integer	100	Both
max_invalid_rcpt	integer	0	Both
max_line_length	integer	1024	Both
max_rcpt	integer	0	Both
max_smtp_cmds	integer	0	Both
qmail_local	program	/var/qmail/bin/qmail-local-real	Both
qmail_queue	program	/var/qmail/bin/qmail-queue	Both
qmailcontroldir	directory	/var/qmail/control/	Both
rcpt_delay_at	integer	0	Both
rcpt_delay_inc	integer	0	Both
rcpt_delay_max	integer	0	Both
rfc_addr_only	boolean	0	Both
stray_newline_detection	boolean	1	Both
spam_check_enable	boolean	0	Both
spam_log_db	boolean	0	Commercial
spam_rule_dbfile	filename	/var/qmail/bin/qmail-local-real	Both
spam_table	string		Commercial
use_database	boolean	1	Commercial
use_dbfile	boolean	0	Both
user_info_dbfile	filename	/var/qmail/bin/qmail-local-real	Both
virus_local	program	/var/qmail/bin/qmail-local-real	Commercial
welcome_message	filename		Commercial