NAME

clamav-milter.conf − Configuration file for clamav-milter

DESCRIPTION

clamav-milter.conf contains the configuration options for clamav-milter(8).

FILE FORMAT

The file consists of comments and options with arguments. Each line which starts with a hash (#) symbol is ignored by the parser. Options and arguments are case sensitive and of the form **Option Argument**. The arguments are of the following types:

BOOL Boolean value (yes/no or true/false or 1/0).

STRING
String without blank characters.

SIZE Size in bytes. You can use 'M' or 'm' modifiers for megabytes and 'K' or 'k' for kilobytes.

NUMBER
Unsigned integer.

MAIN OPTIONS

Example
If this option is set clamav-milter will not run.

MilterSocket STRING
Define the interface through which we communicate with sendmail. This option is mandatory!
Possible formats are:
[[unix|local]:]/path/to/file - to specify a unix domain socket
inet:port@[hostname|ip-address] - to specify an ipv4 socket
inet6:port@[hostname|ip-address] - to specify an ipv6 socket
Default: unset

MilterSocketGroup STRING
Define the group ownership for the (unix) milter socket.
Default: disabled (the primary group of the user running clamd)

MilterSocketMode STRING
Sets the permissions on the (unix) milter socket to the specified mode.
Default: disabled (obey umask)

FixStaleSocket BOOL
Remove stale socket after unclean shutdown.
Default: yes

User STRING
Run as another user (clamav-milter must be started by root for this option to work)
Default: unset (don´t drop privileges)

ReadTimeout NUMBER
Waiting for data from clamd will timeout after this time (seconds).
Default: 120

Foreground BOOL
Don´t fork into background.
Default: no

Chroot STRING
Chroot to the specified directory. Chrooting is performed just after reading the config file and before dropping privileges.
Default: unset (don´t chroot)

PidFile STRING

Write the daemon's pid to the specified file.
Default: disabled

TemporaryDirectory STRING

Optional path to the global temporary directory.
Default: system specific (usually /tmp or /var/tmp).

CLAMD OPTIONS

ClamdSocket STRING

Define the clamd socket to connect to for scanning. This option is mandatory! Syntax:
ClamdSocket unix:path
ClamdSocket tcp:host:port
The first syntax specifies a local unix socket (needs an absolute path) e.g.:
ClamdSocket unix:/run/clamav/clamd.sock
The second syntax specifies a tcp local or remote tcp socket: the host can be a hostname or an ip address; the ":port" field is only required for IPv6 addresses, otherwise it defaults to 3310 e.g.:
ClamdSocket tcp:192.168.0.1
This option can be repeated several times with different sockets or even with the same socket: clamd servers will be selected in a round-robin fashion.
Default: no default

EXCLUSIONS

LocalNet STRING

Messages originating from these hosts/networks will not be scanned. This option takes a host(name)/mask pair in CIRD notation and can be repeated several times. If "/mask" is omitted, a host is assumed. To specify a locally originated, non-smtp, email use the keyword "local"
Default: unset (scan everything regardless of the origin)

AllowList STRING

This option specifies a file which contains a list of basic POSIX regular expressions. Addresses (sent to or from - see below) matching these regexes will not be scanned. Optionally each line can start with the string "From:" or "To:" (note: no whitespace after the colon) indicating if it is, respectively, the sender or recipient that is to be allowed. If the field is missing, "To:" is assumed. Lines starting with #, : or ! are ignored.
Default: unset (no exclusion applied)

SkipAuthenticated STRING

Messages from authenticated SMTP users matching this extended POSIX regular expression (egrep-like) will not be scanned. As an alternative, a file containing a plain (not regex) list of names (one per line) can be specified using the prefix "file:". e.g. SkipAuthenticated file:/etc/good_guys. Note: this is the AUTH login name!
Default: unset (no allowing based on SMTP auth)

MaxFileSize SIZE

Messages larger than this value won´t be scanned. Make sure this value is lower or equal than StreamMaxLength in clamd.conf
Default: 100M

ACTIONS

The following group of options controls the delivery process under different circumstances. The following actions are available:
- Accept: The message is accepted for delivery
- Reject: Immediately refuse delivery (a 5xx error is returned to the peer)
- Defer: Return a temporary failure message (4xx) to the peer
- Blackhole (not available for OnFail): Like Accept but the message is sent to oblivion
- Quarantine (not available for OnFail): Like Accept but message is quarantined instead of being delivered.

NOTE: In Sendmail the quarantine queue can be examined via mailq −qQ. For Postfix this causes the message to be placed on hold.

OnClean STRING
Action to be performed on clean messages (mostly useful for testing)
Default: Accept

OnInfected STRING
Action to be performed on infected messages
Default: Quarantine

OnFail STRING
Action to be performed on error conditions (this includes failure to allocate data structures, no scanners available, network timeouts, unknown scanner replies and the like)
Default: Defer

RejectMsg STRING
This option allows you to set a specific rejection reason for infected messages and it´s therefore only useful together with "OnInfected Reject". The string "%v", if present, will be replaced with the virus name.
Default: MTA specific

AddHeader STRING
If this option is set to "Replace" (or "Yes"), an "X-Virus-Scanned" and an "X-Virus-Status" headers will be attached to each processed message, possibly replacing existing headers. If it is set to Add, the X-Virus headers are added possibly on top of the existing ones. Note that while "Replace" can potentially break DKIM signatures, "Add" may confuse procmail and similar filters.
Default: no

ReportHostname STRING
When AddHeader is in use, this option allows you to set the reported hostname. This may be desirable in order to avoid leaking internal names. If unset the real machine name is used.
Default: disabled

VirusAction STRING
Execute a command (possibly searching PATH) when an infected message is found. The following parameters are passed to the invoked program in this order: virus name, queue id, sender, destination, subject, message id, message date. Note #1: this requires MTA macroes to be available (see LogInfected below). Note #2: the process is invoked in the context of clamav-milter. Note #3: clamav-milter will wait for the process to exit. Be quick or fork to avoid unnecessary delays in email delivery.
Default: disabled

LOGGING OPTIONS

LogFile STRING
Enable logging to selected file.
Default: no

LogFileUnlock BOOL
Disable a system lock that protects against running clamd with the same configuration file multiple times.
Default: no

LogFileMaxSize SIZE
Limit the size of the log file. The logger will be automatically disabled if the file is greater than SIZE. Value of 0 disables the limit.
Default: 1M

LogTime BOOL
Log time for each message.
Default: no

LogSyslog BOOL
Use system logger (can work together with LogFile).
Default: no

LogFacility STRING
Specify the type of syslog messages − please refer to 'man syslog' for facility names.
Default: LOG_LOCAL6

LogVerbose BOOL
Enable verbose logging.
Default: no

LogInfected STRING
This option allows you to tune what is logged when a message is infected. Possible values are Off (the default − nothing is logged), Basic (minimal info logged), Full (verbose info logged)
Note: For this to work properly in sendmail, make sure the msg_id, mail_addr, rcpt_addr and i macroes are available in eom. In other words add a line like: Milter.macros.eom={msg_id}, {mail_addr}, {rcpt_addr}, i to your .cf file. Alternatively use the macro: define('confMILTER_MACROS_EOM', '{msg_id}, {mail_addr}, {rcpt_addr}, i')
Postfix should be working fine with the default settings.
Default: disabled

LogClean STRING
This option allows you to tune what is logged when no threat is found in a scanned message.
See LogInfected for possible values and caveats.
Useful in debugging but drastically increases the log size.
Default: disabled

SupportMultipleRecipients BOOL
This option affects the behaviour of LogInfected, LogClean and VirusAction when a message with multiple recipients is scanned:
If SupportMultipleRecipients is off (the default) then one single log entry is generated for the message and, in case the message is determined to be malicious, the command indicated by VirusAction is executed just once. In both cases only the last recipient is reported.
If SupportMultipleRecipients is on then one line is logged for each recipient and the command indicated by VirusAction is also executed once for each recipient.
Note: although it's probably a good idea to enable this option, the default value is currently set to off for legacy reasons.
Default: no

NOTES

All options expressing a size are limited to max 4GB. Values in excess will be reset to the maximum.

FILES

/etc/clamav/clamav-milter.conf

AUTHOR

aCaB <acab@clamav.net>

SEE ALSO

clamav-milter(8), clamd(8), clamd.conf(5)