NAME

clamd.conf − Configuration file for Clam AntiVirus Daemon

DESCRIPTION

clamd.conf configures the Clam AntiVirus daemon, clamd(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. To specify the size in bytes just don't use modifiers.

NUMBER
Unsigned integer.

DIRECTIVES

When some option is not used (commented out or not included in the configuration file at all) clamd takes a default action.

Example
If this option is set clamd will not run.

LogFile STRING
Save all reports to a log file.
Default: disabled

LogFileUnlock BOOL
By default the log file is locked for writing and only a single daemon process can write to it. This option disables the lock.
Default: no

LogFileMaxSize SIZE
Maximum size of the log file.
Value of 0 disables the limit.
Default: 1048576

LogTime BOOL
Log time for each message.
Default: no

LogClean BOOL
Log all clean files.
Useful in debugging but drastically increases the log size.
Default: no

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

LogFacility STRING
Type of syslog messages
Please refer to 'man syslog' for facility names.
Default: LOG_LOCAL6

LogVerbose BOOL
Enable verbose logging.
Default: no

LogRotate BOOL
Rotate log file. Requires LogFileMaxSize option set prior to this option.
Default: no

ExtendedDetectionInfo BOOL
Log additional information about the infected file, such as its size and hash, together with the virus name.
Default: no

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

TemporaryDirectory STRING
This option allows you to change the default temporary directory.
Default: system specific (usually /tmp or /var/tmp).

DatabaseDirectory STRING
This option allows you to change the default database directory. If you enable it, please make sure it points to the same directory in both clamd and freshclam.
Default: defined at configuration (/usr/local/share/clamav)

OfficialDatabaseOnly BOOL
Only load the official signatures published by the ClamAV project.
Default: no

FailIfCvdOlderThan NUMBER
Return with a nonzero error code if the virus database is older than the specified number of days.
Default: -1

LocalSocket STRING
Path to a local (Unix) socket the daemon will listen on.
Default: disabled

LocalSocketGroup STRING
Sets the group ownership on the unix socket.
Default: the primary group of the user running clamd

LocalSocketMode STRING
Sets the permissions on the unix socket to the specified mode.
Default: socket is world readable and writable

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

TCPSocket NUMBER
TCP port number the daemon will listen on.
Default: disabled

TCPAddr STRING
By default clamd binds to INADDR_ANY.
This option allows you to restrict the TCP address and provide some degree of protection from the outside world. This option can be specified multiple times in order to listen on multiple IPs. IPv6 is now supported.
Default: disabled

MaxConnectionQueueLength NUMBER
Maximum length the queue of pending connections may grow to.
Default: 200

StreamMaxLength SIZE
Close the STREAM session when the data size limit is exceeded.
The value should match your MTA's limit for the maximum attachment size.
Default: 100M

StreamMinPort NUMBER
The STREAM command uses an FTP-like protocol.
This option sets the lower boundary for the port range.
Default: 1024

StreamMaxPort NUMBER
This option sets the upper boundary for the port range.
Default: 2048

MaxThreads NUMBER
Maximum number of threads running at the same time.
Default: 10

ReadTimeout NUMBER
This option specifies the time (in seconds) after which clamd should timeout if a client doesn't provide any data.
Default: 120

CommandReadTimeout NUMBER
This option specifies the time (in seconds) after which clamd should timeout if a client doesn't provide any initial command after connecting. The default is set to 30 to avoid timeouts with TCP sockets when processing large messages. If using a Unix socket, the value can be changed to 5. Note: the timeout for subsequents commands, and/or data chunks is specified by ReadTimeout.
Default: 30

SendBufTimeout NUMBER
This option specifies how long to wait (in milliseconds) if the send buffer is full. Keep this value low to prevent clamd hanging.
Default: 500

MaxQueue NUMBER
Maximum number of queued items (including those being processed by MaxThreads threads). It is recommended to have this value at least twice MaxThreads if possible.
WARNING: you shouldn't increase this too much to avoid running out of file descriptors, the following condition should hold: MaxThreads*MaxRecursion + MaxQueue - MaxThreads + 6 < RLIMIT_NOFILE. RLIMIT_NOFILE is the maximum number of open file descriptors (usually 1024), set by **ulimit −n**.
Default: 100

IdleTimeout NUMBER
This option specifies how long (in seconds) the process should wait for a new job.
Default: 30

ExcludePath REGEX
Don't scan files and directories matching REGEX. This directive can be used multiple times.
Default: disabled

MaxDirectoryRecursion NUMBER
Maximum depth directories are scanned at.
Default: 15

FollowDirectorySymlinks BOOL
Follow directory symlinks.
Default: no

CrossFilesystems BOOL
Scan files and directories on other filesystems.
Default: yes

FollowFileSymlinks BOOL
Follow regular file symlinks.
Default: no

SelfCheck NUMBER
This option specifies the time intervals (in seconds) in which clamd should perform a database check.
Default: 600

ConcurrentDatabaseReload BOOL
Enable non-blocking (multi-threaded/concurrent) database reloads. This feature will temporarily load a second scanning engine while scanning continues using the first engine. Once loaded, the new engine takes over. The old engine is removed as soon as all scans using the old engine have completed. This feature requires more RAM, so this option is provided in case users are willing to block scans during reload in exchange for lower RAM requirements.
Default: yes

VirusEvent COMMAND
Execute a command when virus is found. Use the following environment variables to identify the file and virus names: - $CLAM_VIRUSEVENT_FILENAME - $CLAM_VIRUSEVENT_VIRUSNAME In the command string, '%v' will also be replaced with the virus name. Note: The '%f' filename format character has been disabled and will no longer be replaced with the file name, due to command injection security concerns. Use the 'CLAM_VIRUSEVENT_FILENAME' environment variable instead. For the same reason, you should NOT use the environment variables in the command directly, but should use it carefully from your executed script.
Default: disabled

ExitOnOOM BOOL
Stop daemon when libclamav reports out of memory condition.
Default: no

AllowAllMatchScan BOOL
Permit use of the ALLMATCHSCAN command.
Default: yes

Foreground BOOL
Don't fork into background.
Default: no

Debug BOOL
Enable debug messages from libclamav.
Default: no

LeaveTemporaryFiles BOOL
Do not remove temporary files (for debugging purpose).
Default: no

GenerateMetadataJson BOOL
Record metadata about the file being scanned. Scan metadata is useful for file analysis purposes and for debugging scan behavior. The JSON metadata will be printed after the scan is complete if Debug is enabled. A metadata.json file will be written to the scan temp directory if LeaveTemporaryFiles is enabled.
Default: no

User STRING
Run the daemon as a specified user (the process must be started by root).
Default: disabled

Bytecode BOOL
With this option enabled ClamAV will load bytecode from the database. It is highly recommended you keep this option turned on, otherwise you may miss detections for many new viruses.
Default: yes

BytecodeSecurity STRING
Set bytecode security level.

Possible values:
TrustSigned − trust bytecode loaded from signed .c[lv]d files and insert runtime safety checks for bytecode loaded from other sources,
Paranoid − don't trust any bytecode, insert runtime checks for all.
Recommended: **TrustSigned**, because bytecode in .cvd files already has these checks.
Default: TrustSigned

BytecodeTimeout NUMBER
Set bytecode timeout in milliseconds.
Default: 10000

BytecodeUnsigned BOOL
Allow loading bytecode from outside digitally signed .c[lv]d files. **Caution**: You should NEVER run bytecode signatures from untrusted sources. Doing so may result in arbitrary code execution.
Default: no

BytecodeMode STRING
Set bytecode execution mode.

Possible values:
Auto − automatically choose JIT if possible, fallback to interpreter
ForceJIT − always choose JIT, fail if not possible
ForceInterpreter − always choose interpreter
Test − run with both JIT and interpreter and compare results. Make all failures fatal.
Default: Auto

DetectPUA BOOL
Detect Possibly Unwanted Applications.
Default: No

ExcludePUA CATEGORY
Exclude a specific PUA category. This directive can be used multiple times. See https://docs.clamav.net/faq/faq-pua.html for the complete list of PUA categories.
Default: disabled

IncludePUA CATEGORY
Only include a specific PUA category. This directive can be used multiple times. See https://docs.clamav.net/faq/faq-pua.html for the complete list of PUA categories.
Default: disabled

HeuristicAlerts BOOL
In some cases (eg. complex malware, exploits in graphic files, and others), ClamAV uses special algorithms to provide accurate detection. This option controls the algorithmic detection.
Default: yes

HeuristicScanPrecedence BOOL

Allow heuristic match to take precedence. When enabled, if a heuristic scan (such as phishingScan) detects a possible virus/phishing it will stop scanning immediately. Recommended, saves CPU scan-time. When disabled, virus/phishing detected by heuristic scans will be reported only at the end of a scan. If an archive contains both a heuristically detected virus/phishing, and a real malware, the real malware will be reported. Keep this disabled if you intend to handle "*.Heuristics.*" viruses differently from "real" malware. If a non-heuristically-detected virus (signature-based) is found first, the scan is interrupted immediately, regardless of this config option.
Default: no

ScanPE BOOL

PE stands for Portable Executable − it's an executable file format used in all 32 and 64−bit versions of Windows operating systems. This option allows ClamAV to perform a deeper analysis of executable files and it's also required for decompression of popular executable packers such as UPX.
If you turn off this option, the original files will still be scanned, but without additional processing.
Default: yes

ScanELF BOOL

Executable and Linking Format is a standard format for UN*X executables. This option allows you to control the scanning of ELF files.
If you turn off this option, the original files will still be scanned, but without additional processing.
Default: yes

ScanMail BOOL

Enable scanning of mail files.
If you turn off this option, the original files will still be scanned, but without parsing individual messages/attachments.
Default: yes

ScanPartialMessages BOOL

Scan RFC1341 messages split over many emails. You will need to periodically clean up $TemporaryDirectory/clamav-partial directory. **WARNING: This option may open your system to a DoS attack. Never use it on loaded servers.**
Default: no

PhishingSignatures BOOL

Enable email signature-based phishing detection.
Default: yes

PhishingScanURLs BOOL

Enable URL signature-based phishing detection (Heuristics.Phishing.Email.*)
Default: yes

StructuredDataDetection BOOL

Enable the DLP module.
Default: no

StructuredMinCreditCardCount NUMBER

This option sets the lowest number of Credit Card numbers found in a file to generate a detect.
Default: 3

StructuredCCOnly BOOL
With this option enabled the DLP module will search for valid Credit Card0umbers only. Debit and Private Label cards will not be searched.
Default: No

StructuredMinSSNCount NUMBER
This option sets the lowest number of Social Security Numbers found in a file to generate a detect.
Default: 3

StructuredSSNFormatNormal BOOL
With this option enabled the DLP module will search for valid SSNs formatted as xxx-yy-zzzz.
Default: Yes

StructuredSSNFormatStripped BOOL
With this option enabled the DLP module will search for valid SSNs formatted as xxxyyzzzz.
Default: No

ScanHTML BOOL
Perform HTML/JavaScript/ScriptEncoder normalisation and decryption.
If you turn off this option, the original files will still be scanned, but without additional processing.
Default: yes

ScanOLE2 BOOL
This option enables scanning of OLE2 files, such as Microsoft Office documents and .msi files.
If you turn off this option, the original files will still be scanned, but without additional processing.
Default: yes

ScanPDF BOOL
This option enables scanning within PDF files.
If you turn off this option, the original files will still be scanned, but without additional processing.
Default: yes

ScanSWF BOOL
This option enables scanning within SWF files.
If you turn off this option, the original files will still be scanned, but without decoding and additional processing.
Default: yes

ScanXMLDOCS BOOL
This option enables scanning xml-based document files supported by libclamav.
If you turn off this option, the original files will still be scanned, but without additional processing.
Default: yes

ScanHWP3 BOOL
This option enables scanning HWP3 files.
If you turn off this option, the original files will still be scanned, but without additional processing.
Default: yes

ScanOneNote BOOL
This option enables scanning OneNote files.
If you turn off this option, the original files will still be scanned, but without additional processing.
Default: yes

ScanArchive BOOL
Scan within archives and compressed files.
If you turn off this option, the original files will still be scanned, but without unpacking and additional processing.
Default: yes

ScanImage BOOL
This option enables scanning of image (graphics).
If you turn off this option, the original files will still be scanned, but without unpacking and additional processing.
Default: yes

ScanImageFuzzyHash BOOL
This option enables detection by calculating a fuzzy hash of image (graphics) files. Signatures using image fuzzy hashes typically match files and documents by identifying images embedded or attached to those files.
If you turn off this option, then some files may no longer be detected.
Default: yes

AlertBrokenExecutables BOOL
Alert on broken executable files (PE & ELF).
Default: no

AlertBrokenMedia BOOL
Alert on broken graphics files (JPEG, TIFF, PNG, GIF).
Default: no

AlertEncrypted BOOL
Alert on encrypted archives and documents (encrypted .zip, .7zip, .rar, .pdf).
Default: no

AlertEncryptedArchive BOOL
Alert on encrypted archives (encrypted .zip, .7zip, .rar).
Default: no

AlertEncryptedDoc BOOL
Alert on encrypted documents (encrypted .pdf).
Default: no

AlertOLE2Macros BOOL
Alert on OLE2 files containing VBA macros (Heuristics.OLE2.ContainsMacros).
Default: no

AlertExceedsMax BOOL
When AlertExceedsMax is set, files exceeding the MaxFileSize, MaxScanSize, or MaxRecursion limit will be flagged with the virus name starting with "Heuristics.Limits.Exceeded".
Default: no

AlertPhishingSSLMismatch BOOL
Alert on emails containing SSL mismatches in URLs (might lead to false positives!).
Default: no

AlertPhishingCloak BOOL

Alert on emails containing cloaked URLs (might lead to some false positives).
Default: no

AlertPartitionIntersection BOOL

Alert on raw DMG image files containing partition intersections.
Default: no

DisableCache

This option allows you to disable the caching feature of the engine.
By default, the engine will store an MD5 in a cache of any files that are not flagged as virus or that hit limits checks. **Warning: Disabling the cache will have a negative performance impact on large scans.**
Default: no

CacheSize

This option allows you to set the number of entries the cache can store. The value should be a square number or will be rounded up to the nearest square number.
Default: 65536

ForceToDisk

This option causes memory or nested map scans to dump the content to disk.
If you turn on this option, more data is written to disk and is available when the leave-temps option is enabled at the cost of more disk writes.
Default: no

MaxScanTime SIZE

This option sets the maximum amount of time a scan may take to complete. The value is in milliseconds. The value of 0 disables the limit. **WARNING: disabling this limit or setting it too high may result allow scanning of certain files to lock up the scanning process/threads resulting in a Denial of Service.**
Default: 120000

MaxScanSize SIZE

Sets the maximum amount of data to be scanned for each input file. Archives and other containers are recursively extracted and scanned up to this value. The size of an archive plus the sum of the sizes of all files within archive count toward the scan size. For example, a 1M uncompressed archive containing a single 1M inner file counts as 2M toward the max scan size. **Warning: disabling this limit or setting it too high may result in severe damage to the system.**
Default: 400M

MaxFileSize SIZE

Files larger than this limit won't be scanned. Affects the input file itself as well as files contained inside it (when the input file is an archive, a document or some other kind of container). **Warning: disabling this limit or setting it too high may result in severe damage to the system. Technical design limitations prevent ClamAV from scanning files greater than 2 GB at this time.**
Default: 100M

MaxRecursion NUMBER

Nested archives are scanned recursively, e.g. if a Zip archive contains a RAR file, all files within it will also be scanned. This options specifies how deeply the process should be continued. **Warning: setting this limit too high may result in severe damage to the system.**
Default: 17

MaxFiles NUMBER
Number of files to be scanned within an archive, a document, or any other kind of container. **Warning: disabling this limit or setting it too high may result in severe damage to the system.**
Default: 10000

MaxEmbeddedPE SIZE
This option sets the maximum size of a file to check for embedded PE.
Files larger than this value will skip the additional analysis step.
Negative values are not allowed.
Default: 40M

MaxHTMLNormalize SIZE
This option sets the maximum size of a HTML file to normalize.
HTML files larger than this value will not be normalized or scanned.
Negative values are not allowed.
Default: 40M

MaxHTMLNoTags SIZE
This option sets the maximum size of a normalized HTML file to scan.
HTML files larger than this value after normalization will not be scanned.
Negative values are not allowed.
Default: 8M

MaxScriptNormalize SIZE
This option sets the maximum size of a script file to normalize.
Script content larger than this value will not be normalized or scanned.
Negative values are not allowed.
Default: 20M

MaxZipTypeRcg SIZE
This option sets the maximum size of a ZIP file to reanalyze type recognition.
ZIP files larger than this value will skip the step to potentially reanalyze as PE.
Negative values are not allowed.
WARNING: setting this limit too high may result in severe damage or impact performance.
Default: 1M

MaxPartitions SIZE
This option sets the maximum number of partitions of a raw disk image to be scanned.
Raw disk images with more partitions than this value will have up to the value partitions scanned.
Negative values are not allowed.
WARNING: setting this limit too high may result in severe damage or impact performance.
Default: 50

MaxIconsPE SIZE
This option sets the maximum number of icons within a PE to be scanned.
PE files with more icons than this value will have up to the value number icons scanned.
Negative values are not allowed.
WARNING: setting this limit too high may result in severe damage or impact performance.
Default: 100

MaxRecHWP3 NUMBER
This option sets the maximum recursive calls to HWP3 parsing function.
HWP3 files using more than this limit will be terminated and alert the user.
Scans will be unable to scan any HWP3 attachments if the recursive limit is reached.

Negative values are not allowed.
WARNING: setting this limit too high may result in severe damage or impact performance.
Default: 16

PCREMatchLimit NUMBER

This option sets the maximum calls to the PCRE match function during an instance of regex matching.
Instances using more than this limit will be terminated and alert the user but the scan will continue.
For more information on match_limit, see the PCRE documentation.
Negative values are not allowed.
WARNING: setting this limit too high may severely impact performance.
Default: 10000

PCRERecMatchLimit NUMBER

This option sets the maximum recursive calls to the PCRE match function during an instance of regex matching.
Instances using more than this limit will be terminated and alert the user but the scan will continue.
For more information on match_limit_recursion, see the PCRE documentation.
Negative values are not allowed and values > PCREMatchLimit are superfluous.
WARNING: setting this limit too high may severely impact performance.
Default: 2000

PCREMaxFileSize SIZE

This option sets the maximum filesize for which PCRE subsigs will be executed.
Files exceeding this limit will not have PCRE subsigs executed unless a subsig is encompassed to a smaller buffer.
Negative values are not allowed.
Setting this value to zero disables the limit.
WARNING: setting this limit too high or disabling it may severely impact performance.
Default: 100M

OnAccessIncludePath STRING

This option specifies a directory (including all files and directories inside it), which should be scanned on access. This option can be used multiple times.
Default: disabled

OnAccessExcludePath STRING

This option allows excluding directories from on-access scanning. It can be used multiple times.
Default: disabled

OnAccessExcludeRootUID BOOL

With this option you can exclude the root UID (0). Processes run under root will be able to access all files without triggering scans or permission denied events.
Note that if clamd cannot check the uid of the process that generated an on-access scan event (e.g., because **OnAccessPrevention** was not enabled, and the process already exited), clamd will perform a scan. Thus, setting **OnAccessExcludeRootUID** is not *guaranteed* to prevent every access by the root user from triggering a scan (unless **OnAccessPrevention** is enabled).
Default: no

OnAccessExcludeUID NUMBER

With this option you can exclude specific UIDs. Processes with these UIDs will be able to access all files without triggering scans or permission denied events.

This option can be used multiple times (one per line).
Note: using a value of 0 on any line will disable this option entirely. To exclude the root UID (0) please enable the OnAccessExcludeRootUID option.
Also note that if clamd cannot check the uid of the process that generated an on-access scan event (e.g., because **OnAccessPrevention** was not enabled, and the process already exited), clamd will perform a scan. Thus, setting **OnAccessExcludeUID** is not *guaranteed* to prevent every access by the specified uid from triggering a scan (unless **OnAccessPrevention** is enabled).
Default: disabled

OnAccessExcludeUname STRING

This option allows exclusions via user names when using the on-access scanning client. It can be used multiple times, and has the same potential race condition limitations of the OnAccessExcludeUID option.
Default: disabled

OnAccessMaxFileSize SIZE

Files larger than this value will not be scanned in on access.
Default: 5M

OnAccessMaxThreads NUMBER

Max number of scanning threads to allocate to the OnAccess thread pool at startup. These threads are the ones responsible for creating a connection with the daemon and kicking off scanning after an event has been processed. To prevent clamonacc from consuming all clamd's resources keep this lower than clamd's max threads.
Default: 5

OnAccessCurlTimeout NUMBER

Max amount of time (in milliseconds) that the OnAccess client should spend for every connect, send, and receive attempt when communicating with clamd via curl.
Default: 5000 (5 seconds)

OnAccessMountPath STRING

Specifies a mount point (including all files and directories under it), which should be scanned on access. This option can be used multiple times.
Default: disabled

OnAccessDisableDDD BOOL

Disables the dynamic directory determination system which allows for recursively watching include paths.
Default: no

OnAccessPrevention BOOL

Enables fanotify blocking when malicious files are found.
Default: disabled

OnAccessRetryAttempts NUMBER

Number of times the OnAccess client will retry a failed scan due to connection problems (or other issues).
Default: 0

OnAccessDenyOnError BOOL

When using prevention, if this option is turned on, any errors that occur during scanning will result in the event attempt being denied. This could potentially lead to unwanted system behaviour with certain configurations, so the client defaults this to off and prefers allowing access events in

case of scan or connection error.
Default: no

OnAccessExtraScanning BOOL
Toggles extra scanning and notifications when a file or directory is created or moved.
Requires the DDD system to kick-off extra scans.
Default: no

DisableCertCheck BOOL
Disable authenticode certificate chain verification in PE files.
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/clamd.conf

AUTHORS

Tomasz Kojm <tkojm@clamav.net>, Kevin Lin <klin@sourcefire.com>

SEE ALSO

clamd(8), clamdscan(1), clamav-milter(8), freshclam(1), freshclam.conf(5)