NAME

clamscan − scan files and directories for viruses

SYNOPSIS

clamscan [options] [file/directory/−]

DESCRIPTION

clamscan is a command line anti−virus scanner.

OPTIONS

Most of the options are simple switches which enable or disable some features. Options marked with [=yes/no(*)] can be optionally followed by =yes/=no; if they get called without the boolean argument the scanner will assume 'yes'. The asterisk marks the default internal setting for a given option.

−h, −−help
Print help information and exit.

−V, −−version
Print version number and exit.

−v, −−verbose
Be verbose.

−a, −−archive−verbose
Show filenames inside scanned archives

−−debug
Display debug messages from libclamav.

−−quiet
Be quiet (only print error messages).

−−stdout
Write all messages (except for libclamav output) to the standard output (stdout).

−−no−summary
Do not display summary at the end of scanning.

−i, −−infected
Only print infected files.

−o, −−suppress−ok−results
Skip printing OK files

−−bell Sound bell on virus detection.

−−tempdir=DIRECTORY
Create temporary files in DIRECTORY. Directory must be writable for the 'clamav' user or unprivileged user running clamscan.

−−leave−temps
Do not remove temporary files.

−−force−to−disk
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 LeaveTemporaryFiles option is enabled.

−−gen−json
Generate JSON description of scanned file(s). JSON will be printed and also dropped to the temp directory if --leave-temps is enabled.

−d FILE/DIR, −−database=FILE/DIR
Load virus database from FILE or load all virus database files from DIR.

−−official−db−only=[yes/no(*)]
Only load the official signatures published by the ClamAV project.

−−fail−if−cvd−older−than=days
Return with a nonzero error code if the virus database is older than the specified number of days.

−l FILE, −−log=FILE
Save scan report to FILE.

−r, −−recursive
Scan directories recursively. All the subdirectories in the given directory will be scanned.

−z, −−allmatch
After a match, continue scanning within the file for additional matches.

−−cross−fs=[yes(*)/no]
Scan files and directories on other filesystems.

−−follow−dir−symlinks=[0/1(*)/2]
Follow directory symlinks. There are 3 options: 0 - never follow directory symlinks, 1 (default) - only follow directory symlinks, which are passed as direct arguments to clamscan. 2 - always follow directory symlinks.

−−follow−file−symlinks=[0/1(*)/2]
Follow file symlinks. There are 3 options: 0 - never follow file symlinks, 1 (default) - only follow file symlinks, which are passed as direct arguments to clamscan. 2 - always follow file symlinks.

−f FILE, −−file−list=FILE
Scan files listed line by line in FILE.

−−remove[=yes/no(*)]
Remove infected files. **Be careful!**

−−move=DIRECTORY
Move infected files into DIRECTORY. Directory must be writable for the ’clamav’ user or unprivileged user running clamscan.

−−copy=DIRECTORY
Copy infected files into DIRECTORY. Directory must be writable for the ’clamav’ user or unprivileged user running clamscan.

−−exclude=REGEX, −−exclude−dir=REGEX
Don’t scan file/directory names matching regular expression. These options can be used multiple times.

−−include=REGEX, −−include−dir=REGEX
Only scan file/directory matching regular expression. These options can be used multiple times.

−−bytecode[=yes(*)/no]
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.

−−bytecode−unsigned[=yes/no(*)]
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.

−−bytecode−timeout=N
Set bytecode timeout in milliseconds (default: 10000 = 10s)

−−statistics[=none(*)/bytecode/pcre]
Collect and print execution statistics.

−−detect−pua[=yes/no(*)]
Detect Possibly Unwanted Applications.

−−exclude−pua=CATEGORY
Exclude a specific PUA category. This option can be used multiple times. See https://docs.clamav.net/faq/faq-pua.html for the complete list of PUA

−−include−pua=CATEGORY
Only include a specific PUA category. This option can be used multiple times. See https://docs.clamav.net/faq/faq-pua.html for the complete list of PUA

−−detect−structured[=yes/no(*)]
Use the DLP (Data Loss Prevention) module to detect SSN and Credit Card numbers inside documents/text files.

−−structured−ssn−format=X
X=0: search for valid SSNs formatted as xxx-yy-zzzz (normal); X=1: search for valid SSNs formatted as xxxyyzzzz (stripped); X=2: search for both formats. Default is 0.

−−structured−ssn−count=#n
This option sets the lowest number of Social Security Numbers found in a file to generate a detect (default: 3).

−−structured−cc−count=#n
This option sets the lowest number of Credit Card numbers found in a file to generate a detect (default: 3).

−−scan−mail[=yes(*)/no]
Scan mail files. If you turn off this option, the original files will still be scanned, but without parsing individual messages/attachments.

−−phishing−sigs[=yes(*)/no]
Enable email signature-based phishing detection.

−−phishing−scan−urls[=yes(*)/no]
Enable URL signature-based phishing detection (Heuristics.Phishing.Email.*)

−−heuristic−alerts[=yes(*)/no]
In some cases (eg. complex malware, exploits in graphic files, and others), ClamAV uses special algorithms to provide accurate detection. This option can be used to control the algorithmic detection.

−−heuristic−scan−precedence[=yes/no(*)]
Allow heuristic match to take precedence. When enabled, if a heuristic scan (such as phishingScan) detects a possible virus/phish it will stop scan immediately. Recommended, saves CPU scan-time. When disabled, virus/phish detected by heuristic scans will be reported only at the end of a scan. If an archive contains both a heuristically detected virus/phish, 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.

−−normalize[=yes(*)/no]
Normalize (compress whitespace, downcase, etc.) html, script, and text files. Use normalize=no for yara compatibility.

−−scan−pe[=yes(*)/no]
PE stands for Portable Executable − it's an executable file format used in all 32−bit versions of Windows operating systems. By default ClamAV performs deeper analysis of executable files and attempts to decompress popular executable packers such as UPX, Petite, and FSG. If you turn off this option, the original files will still be scanned but without additional processing.

−−scan−elf[=yes(*)/no]
Executable and Linking Format is a standard format for UN*X executables. This option controls the ELF support. If you turn it off, the original files will still be scanned but without additional processing.

−−scan−ole2[=yes(*)/no]
Scan Microsoft Office documents and .msi files. If you turn off this option, the original files will still be scanned but without additional processing.

−−scan−pdf[=yes(*)/no]
Scan within PDF files. If you turn off this option, the original files will still be scanned, but without decoding and additional processing.

−−scan−swf[=yes(*)/no]
Scan SWF files. If you turn off this option, the original files will still be scanned but without additional processing.

−−scan−html[=yes(*)/no]
Detect, normalize/decrypt and scan HTML files and embedded scripts. If you turn off this option, the original files will still be scanned, but without additional processing.

−−scan−xmldocs[=yes(*)/no]
Scan xml-based document files supported by libclamav. If you turn off this option, the original files will still be scanned, but without additional processing.

−−scan−hwp3[=yes(*)/no]
Scan HWP3 files. If you turn off this option, the original files will still be scanned, but without additional processing.

−−scan−archive[=yes(*)/no]
Scan archives supported by libclamav. If you turn off this option, the original files will still be scanned, but without unpacking and additional processing.

−−scan−image[=yes(*)/no]
This option enables scanning of image (graphics). If you turn off this option, the original files will still be scanned, but without additional processing.

−−scan−image−fuzzy−hash[=yes(*)/no]
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.

−−alert−broken[=yes/no(*)]
Alert on broken executable files (PE & ELF).

−−alert−encrypted[=yes/no(*)]
Alert on encrypted archives and documents (encrypted .zip, .7zip, .rar, .pdf).

−−alert−encrypted-archive[=yes/no(*)]
Alert on encrypted archives (encrypted .zip, .7zip, .rar, .pdf).

−−alert−encrypted-doc[=yes/no(*)]
Alert on encrypted documents (encrypted .zip, .7zip, .rar, .pdf).

−−alert−macros[=yes/no(*)]
Alert on OLE2 files containing VBA macros (Heuristics.OLE2.ContainsMacros).

−−alert−exceeds−max[=yes/no(*)]
Alert on files that exceed max file size, max scan size, or max recursion limit (Heuristics.Limits.Exceeded).

−−alert−phishing−ssl[=yes/no(*)]
Alert on emails containing SSL mismatches in URLs (might lead to false positives!).

--alert-phishing-cloak[=yes/no(*)]
Alert on emails containing cloaked URLs (might lead to some false positives).

--alert-partition-intersection[=yes/no(*)]
Detect partition intersections in raw disk images using heuristics.

--nocerts
Disable authenticode certificate chain verification in PE files.

--dumpcerts
Dump authenticode certificate chain in PE files.

--max-scantime=#n
The maximum time to scan before giving up. The value is in milliseconds. The value of 0 disables the limit. This option protects your system against DoS attacks (default: 120000 = 120s or 2min)

--max-filesize=#n
Extract and scan at most #n bytes from each archive. You may pass the value in kilobytes in format xK or xk, or megabytes in format xM or xm, where x is a number. This option protects your system against DoS attacks (default: 100 MB, max: 2 GB)

--max-scansize=#n
Extract and scan at most #n bytes from each archive. The size the 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 max-scansize. You may pass the value in kilobytes in format xK or xk, or megabytes in format xM or xm, where x is a number. This option protects your system against DoS attacks (default: 400 MB)

--max-files=#n
Extract at most #n files from each scanned file (when this is an archive, a document or another kind of container). This option protects your system against DoS attacks (default: 10000)

--max-recursion=#n
Set archive recursion level limit. This option protects your system against DoS attacks (default: 17).

--max-dir-recursion=#n
Maximum depth directories are scanned at (default: 15).

--max-embeddedpe=#n
Maximum size file to check for embedded PE. You may pass the value in kilobytes in format xK or xk, or megabytes in format xM or xm, where x is a number (default: 40 MB).

--max-htmlnormalize=#n
Maximum size of HTML file to normalize. You may pass the value in kilobytes in format xK or xk, or megabytes in format xM or xm, where x is a number (default: 40 MB).

--max-htmlnotags=#n
Maximum size of normalized HTML file to scan. You may pass the value in kilobytes in format xK or xk, or megabytes in format xM or xm, where x is a number (default: 8 MB).

--max-scriptnormalize=#n
Maximum size of script file to normalize. You may pass the value in kilobytes in format xK or xk, or megabytes in format xM or xm, where x is a number (default: 20 MB).

--max-ziptypercg=#n
Maximum size zip to type reanalyze. You may pass the value in kilobytes in format xK or xk, or megabytes in format xM or xm, where x is a number (default: 1 MB).

--max-partitions=#n
This option sets the maximum number of partitions of a raw disk image to be scanned. This must be a positive integer (default: 50).

−−max−iconspe=#n
This option sets the maximum number of icons within a PE to be scanned. This must be a positive integer (default: 100).

−−max−rechwp3=#n
This option sets the maximum recursive calls to HWP3 parsing function (default: 16).

−−pcre-match-limit=#n
Maximum calls to the PCRE match function (default: 100000).

−−pcre-recmatch-limit=#n
Maximum recursive calls to the PCRE match function (default: 2000).

−−pcre-max-filesize=#n
Maximum size file to perform PCRE subsig matching (default: 100 MB).

−−disable−cache
Disable caching and cache checks for hash sums of scanned files.

ENVIRONMENT VARIABLES

clamscan uses the following environment variables:

LD_LIBRARY_PATH - May be used on startup to find the libclamunrar_iface shared library module to enable RAR archive support.

EXAMPLES

(0) Scan a single file:

clamscan file

(1) Scan a current working directory:

clamscan

(2) Scan all files (and subdirectories) in /home:

clamscan −r /home

(3) Load database from a file:

clamscan −d /tmp/newclamdb −r /tmp

(4) Scan a data stream:

cat testfile | clamscan −

(5) Scan a mail spool directory:

clamscan −r /var/spool/mail

RETURN CODES

0 : No virus found.

1 : Virus(es) found.

2 : Some error(s) occurred.

CREDITS

Please check the full documentation for credits.

AUTHOR

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

SEE ALSO

clamdscan(1), freshclam(1), freshclam.conf(5)