clamscan(1) - Linux man page

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.

--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).

-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.

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

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

--leave-temps
Do not remove temporary files.

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

-r, --recursive

Scan directories recursively. All the subdirectories in the given directory will be scanned.

--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.

--bell

Sound bell on virus detection.

--no-summary

Do not display summary at the end of scanning.

--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.

-i, --infected

Only print infected files.

--remove[=yes/no(*)]

Remove infected files. **Be careful.**

--move=DIRECTORY

Move infected files into DIRECTORY. Directory must be writable for the '' user or unprivileged user running clamscan.

--copy=DIRECTORY

Copy infected files into DIRECTORY. Directory must be writable for the '' user or unprivileged user running clamscan.

--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.

--bytecode-timeout=N

Set bytecode timeout in milliseconds (default: 60000 = 60s)

--detect-pua[=yes/no(*)]

Detect Possibly Unwanted Applications.

--exclude-pua=CATEGORY

Exclude a specific PUA category. This option can be used multiple times. See http://www.clamav.net/support/pua for the complete list of PUA

--include-pua=CATEGORY

Only include a specific PUA category. This option can be used multiple times. See http://www.clamav.net/support/pua 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]

Use the signature-based phishing detection.

--phishing-scan-urls[=yes(*)/no]

Use the url-based heuristic phishing detection (Phishing.Heuristics.Email.*)

--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.

--phishing-ssl[=yes/no(*)]

Block SSL mismatches in URLs (might lead to false positives!).

--phishing-cloak[=yes/no(*)]

Block cloaked URLs (might lead to some false positives).

--algorithmic-detection[=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.

--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-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-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.

--detect-broken[=yes/no(*)]

Mark broken executables as viruses (Broken.Executable).

--block-encrypted[=yes/no(*)]

Mark encrypted archives as viruses (Encrypted.Zip, Encrypted.RAR).

--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-filesize=#n

Extract and scan at most #n kilobytes from each archive. You may pass the value in megabytes in format xM or xm, where x is a number. This option protects your system against DoS attacks (default: 25 MB, max: <4 GB)

--max-scansize=#n

Extract and scan at most #n kilobytes from each scanned file. You may pass the value in megabytes in format xM or xm, where x is a number. This option protects your system against DoS attacks (default: 100 MB, max: <4 GB)

--max-recursion=#n

Set archive recursion level limit. This option protects your system against DoS attacks (default: 16).

--max-dir-recursion=#n

Maximum depth directories are scanned at (default: 15).

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) occured.

Credits

Please check the full documentation for credits.

Author

Tomasz Kojm <tkojm@clamav.net>

See Also

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

Referenced By

clamav-unofficial-sigs.sh(8), **clamfs**(1)