ClamAV

Documentation home > Workflows / guidelines / tools > DR Utilities

Last updated: Sep 5, 2024

ClamAV is an open-source antivirus engine that scans files for viruses and malware.

The Archives uses ClamAV in the digital transfer workflow to check transfer packages and remove infected files before ingest to the repository. If you find infected files in a given transfer, you should contact the producer to advise them of the situation.

Installation

Install ClamAV with homebrew (Mac users).

- You will need administrator access to your computer to install the software.

Open Terminal and enter the following command:

```
brew install clamav
```

Configuration

You will need to create and edit configuration files to run the software. In order to access these files, set your Mac to view hidden files:

```
shift + command + .
```

Navigate to **/usr/local/etc/clamav**

Create copies of the sample config files **clam.conf.sample** and **freshclam.conf.sample**; save these as **clam.conf** and **freshclam.conf**

Use a text editor (e.g BBEdit) to find and comment out (add # to) these lines in both files:

```
# Comment or remove the line below.
# Example
```

Usage

Run ClamAV in a Terminal window.

Always update the virus definitions database before running a scan.

```
freshclam
```

There are many variables that can be adjusted. The Archives' standard scan uses the following:

```
clamscan -ri --log=/path/to/log.txt /path/to/transfer/folder
```

Flags:

- -r = recursive: scan all sub-folders and items.
- -i = infected: print only names of infected files.

- --log = output the scan results to a separate log file; give the full path + file name and extension (e.g. --**log=/Users/home/Desktop/Clamscan/log.txt**)

- transfer folder = the folder's file path; you can get this by simply dragging the folder into your Terminal window.

Links

ClamAV website: https://clamav.net