Antivirus for Linux hosts

This howto shows how to install and configure the ClamAV® open source antivirus engine on a Linux host. There is a debate as to whether antivirus software is required on a Linux host at all or not. Notwithstanding that debate, this page is a resource for those who feel that hew would prefer to run antivirus software on their Linux host and for those whose organization insists that antivirus software is run on all their hosts.

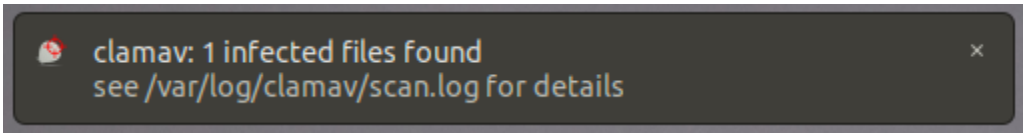
This HowTo was written on a Linux host running Ubuntu 18.04, feel free to adapt it to suit your environment.

In this HowTo we install three components of ClamAV:

- *clamav-daemon*, which runs the antivirus software in memory, checking incoming files and emails
- *clamav-freshclam*, which keeps the virus definitions up to date
- *clamtk*, a simple GUI for ClamAV that lets you carry out scans on demands or schedule your own scans

In addition, this HowTo sets up a daily scan under anacron that occurs at a set time every morning or the first time the host is turned on each morning. Note that daily scans are incremental. The first scan checks all files and directories that are not explicitly excluded. Subsequent scans only scan files and directories not scanned since the last scan. The scans run under nice and do not noticeably degrade the performance of the host.

If ClamAV detects a problem, a desktop notification appears:



The following log files are created:

- /var/log/clamav/clamav.log: log file for the *clamav-daemon* virus scanner
- /var/log/clamav/freshclam.log: log file for the *clamav-freshclam* daemon that keeps virus definitions up to date
- /var/log/clamav/scan.log: the log of the latest scheduled scan
- /var/log/clamav/error.log: log of any errors that occurred in the latest scheduled scan

Follow the steps below to install ClamAV.

Install the ClamAV software

1. Install the clamav software from the repository

```
sudo apt install clamav-daemon clamav-freshclam clamtk
```

2. Check the status of the *clamav-daemon* service

```
sudo service clamav-daemon status
 clamav-daemon.service - Clam AntiVirus userspace daemon
   Loaded: loaded (/lib/systemd/system/clamav-daemon.service; enabled; vendor preset: enabled)
  Drop-In: /etc/systemd/system/clamav-daemon.service.d
           extend.conf
   Active: active (running) since Mon 2019-05-13 11:02:24 IST; 23s ago
     Docs: man:clamd(8)
           man:clamd.conf(5)
           https://www.clamav.net/documents/
  Process: 24527 ExecStartPre=/bin/chown clamav /run/clamav (code=exited, status=0/SUCCESS)
  Process: 24526 ExecStartPre=/bin/mkdir /run/clamav (code=exited, status=0/SUCCESS)
 Main PID: 24535 (clamd)
    Tasks: 2 (limit: 4915)
   CGroup: /system.slice/clamav-daemon.service
           24535 /usr/sbin/clamd --foreground=true

May 13 11:02:40 saor clamd[24535]: Mon May 13 11:02:40 2019 -> Portable Executable support enabled.
May 13 11:02:40 saor clamd[24535]: Mon May 13 11:02:40 2019 -> ELF support enabled.
May 13 11:02:40 saor clamd[24535]: Mon May 13 11:02:40 2019 -> Mail files support enabled.
May 13 11:02:40 saor clamd[24535]: Mon May 13 11:02:40 2019 -> OLE2 support enabled.
May 13 11:02:40 saor clamd[24535]: Mon May 13 11:02:40 2019 -> PDF support enabled.
May 13 11:02:40 saor clamd[24535]: Mon May 13 11:02:40 2019 -> SWF support enabled.
May 13 11:02:40 saor clamd[24535]: Mon May 13 11:02:40 2019 -> HTML support enabled.
May 13 11:02:40 saor clamd[24535]: Mon May 13 11:02:40 2019 -> XMLDOCS support enabled.
May 13 11:02:40 saor clamd[24535]: Mon May 13 11:02:40 2019 -> HWP3 support enabled.
May 13 11:02:40 saor clamd[24535]: Mon May 13 11:02:40 2019 -> Self checking every 3600 seconds.
```

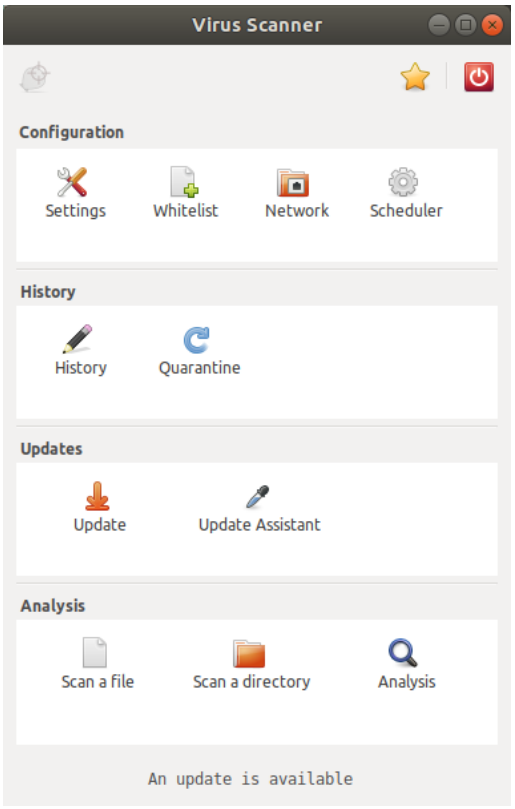
3. Check the status of the *clamav-freshclam* service

```
sudo service clamav-freshclam status
 clamav-freshclam.service - ClamAV virus database updater
   Loaded: loaded (/lib/systemd/system/clamav-freshclam.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2019-05-13 11:02:28 IST; 1min 51s ago
     Docs: man:freshclam(1)
           man:freshclam.conf(5)
           https://www.clamav.net/documents
 Main PID: 24570 (freshclam)
    Tasks: 1 (limit: 4915)
   CGroup: /system.slice/clamav-freshclam.service
           24570 /usr/bin/freshclam -d --foreground=true

May 13 11:02:28 saor systemd[1]: Started ClamAV virus database updater.
May 13 11:02:28 saor freshclam[24570]: Mon May 13 11:02:28 2019 -> ClamAV update process started at Mon
May 13 11:02:28 2019
May 13 11:02:28 saor freshclam[24570]: Mon May 13 11:02:28 2019 -> ^Your ClamAV installation is OUTDATED!
May 13 11:02:28 saor freshclam[24570]: Mon May 13 11:02:28 2019 -> ^Local version: 0.100.3 Recommended
version: 0.101.2
May 13 11:02:28 saor freshclam[24570]: Mon May 13 11:02:28 2019 -> DON'T PANIC! Read https://www.clamav.
net/documents/upgrading-clamav
May 13 11:02:28 saor freshclam[24570]: Mon May 13 11:02:28 2019 -> main.cvd is up to date (version: 58,
sigs: 4566249, f-level: 60, builder: sigmgr)
May 13 11:02:28 saor freshclam[24570]: Mon May 13 11:02:28 2019 -> daily.cld is up to date (version:
25448, sigs: 1568568, f-level: 63, builder: raynman)
May 13 11:02:28 saor freshclam[24570]: Mon May 13 11:02:28 2019 -> bytecode.cvd is up to date (version:
328, sigs: 94, f-level: 63, builder: neo)
```

4. Check that the *clamtk* client is working

```
clamtk
```



Configure ClamAV onAccess service for real-time protection

1. Update the clamav configuration file

```
sudo cat << EOF >> /etc/clamav/clamd.conf
OnAccessMountPath /
OnAccessIncludePath /
OnAccessPrevention yes
OnAccessExcludeUname clamav
OnAccessExcludeRootUID true
EOF
```

2. Create systemd file for clamonacc service

```
sudo cat << EOF > /etc/systemd/system/clamonacc.service

[Unit]
Description=ClamAV On Access Scanner
Requires=clamav-daemon.service
After=clamav-daemon.service syslog.target network.target

[Service]
Type=simple
User=root
ExecStartPre=/bin/bash -c "while [ ! -S /var/run/clamav/clamd.ctl ]; do sleep 1; done"
ExecStart=/usr/sbin/clamonacc -F --config-file=/etc/clamav/clamd.conf --log=/var/log/clamav/clamonacc.log

[Install]
WantedBy=multi-user.target
EOF
```

3. Reload the systemd configuration

```
sudo systemctl daemon-reload
```

4. Enable the clamonacc service to start at system boot

```
sudo systemctl enable clamonacc.service
sudo systemctl start clamonacc.service
```

Configure ClamAV daily scans

1. Check out the Nordix infra tools git repo

```
git clone https://gerrit.nordix.org/infra/tools
```

2. In the *tools/clamav* directory, run the *install.sh* script with root permissions

```
cd tools/clamav
sudo ./install.sh
```

3. Check the excluded files and directories in the */etc/clamav/clamscan_excludes.conf* file. This file provides a filter to a *find* command in the */etc /cron.daily/clamav* script. You can modify the filters by editing this file.

```
sudo vi /etc/clamav/clamscan_excludes.conf
```

4. Run the initial scan manually

```
sudo /etc/cron.daily/clamav
```

5. Check the results of the scan in the can log file

```
cat /var/log/clamav/scan.log
```