Clam AntiVirus

Masterschool

Open-Source Antivirus Scan

Clam AntiVirus Scan

By **Babatunde Ojo**

September 02, 2023

Table of Contents

About ClamAV

ClamAV is an open-source (GPL) antivirus engine designed for detecting Trojans, viruses, malware, and other malicious threats on all the major operating systems. It was initially developed for **Unix**, but now it also runs on **Windows**, **macOS**, and other systems.

What sets ClamAV apart is that it's standard for mail gateway scanning software and supports a wide array of file formats, including executable files and archives, as well as multiple signature languages.

Being open-source, ClamAV benefits from a community of developers and contributors who continually update the malware signature database and improve the software's detection capabilities. This makes it a valuable tool for enhancing the security of various systems and networks.

Overall, ClamAV is a reliable and widely-used antivirus solution in the open-source and security communities, especially for systems that require command-line or server-side malware scanning and protection.

One of the notable features of ClamAV is its ability to integrate with email servers and file servers, providing real-time scanning and protection against malware in email attachments and files. Many mail servers and network security appliances use ClamAV to filter out potentially harmful email attachments and prevent malware from spreading through email.

ClamAV Installation Guide for Windows

Step 1: Download ClamAV for Windows

Visit the ClamAV's download page: ClamAV Downloads

Scroll down and find the latest version of ClamAV. Click on the download link beside it. This will download a .msi file to your system.

Step 2: Install clamav-X.X.X.win.x64.msi

Navigate to the location where you downloaded clamav-X.X.X.win.x64.msi and proceed with the installation process.

Step 3: Configuration Files

Navigate to the location where you installed ClamAV (`C:\Program Files\ClamAV`) Create two .conf files:

clamd.conf22.0KB

freshclam.conf6.9KB

Step 4: Update the Virus Definitions Database

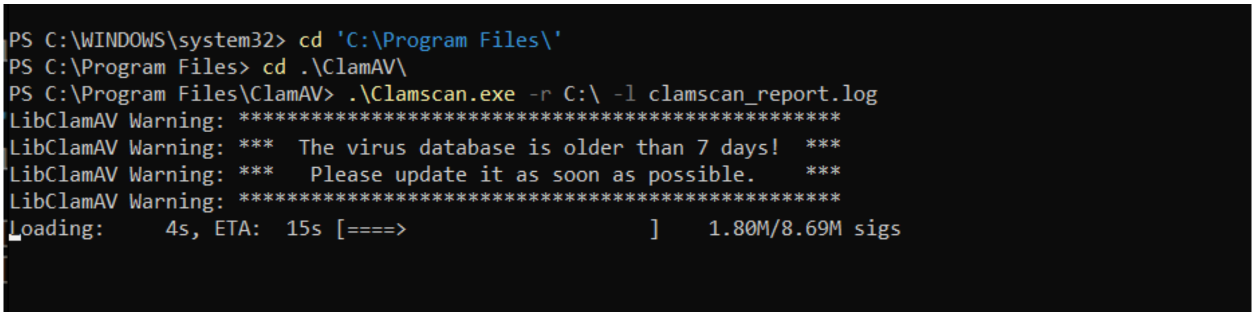
Before you run ClamAV, you need to update the virus definitions database. Open PowerShell as Administrator and navigate to the location where you installed ClamAV (`C:\Program Files\ClamAV`) Run the following command:

```
.\freshclam.exe --config-file=freshclam.conf
.\clamd.exe --config-file=clamd.conf
```

Step 5: Run a Manual Scan with ClamAV

To run a manual scan of your drive, execute the following command:

```
.\clamscan.exe -r C:\ -l <report_name.log>
```

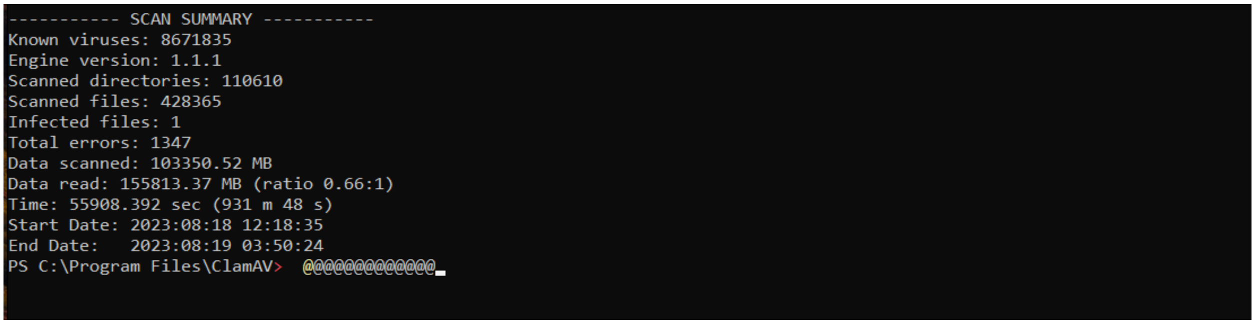


```
PS C:\WINDOWS\system32> cd 'C:\Program Files\'
PS C:\Program Files> cd .\ClamAV\
PS C:\Program Files\ClamAV> .\Clamscan.exe -r C:\ -l clamscan_report.log
LibClamAV Warning: **************************************************
LibClamAV Warning: ***  The virus database is older than 7 days!  ***
LibClamAV Warning: ***   Please update it as soon as possible.    ***
LibClamAV Warning: **************************************************
Loading:     4s, ETA:  15s [====>                    ]    1.80M/8.69M sigs
```

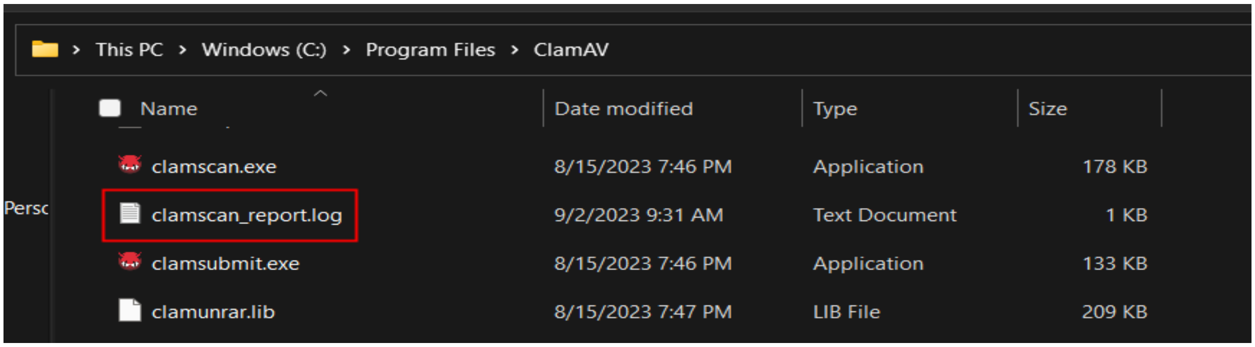
This will take a while; it depends on how much files you have in your drive.

Step 6: Analyze your report log

When clamAV gets done running, it will show a scan summary to indicate any infected files found. Take necessary steps to remediate this. Similarly, your report log can be found in ClamAV directory:



```
----------- SCAN SUMMARY -----------
Known viruses: 8671835
Engine version: 1.1.1
Scanned directories: 110610
Scanned files: 428365
Infected files: 1
Total errors: 1347
Data scanned: 103350.52 MB
Data read: 155813.37 MB (ratio 0.66:1)
Time: 55908.392 sec (931 m 48 s)
Start Date: 2023:08:18 12:18:35
End Date:   2023:08:19 03:50:24
PS C:\Program Files\ClamAV>  @@@@@@@@@@@@@
```

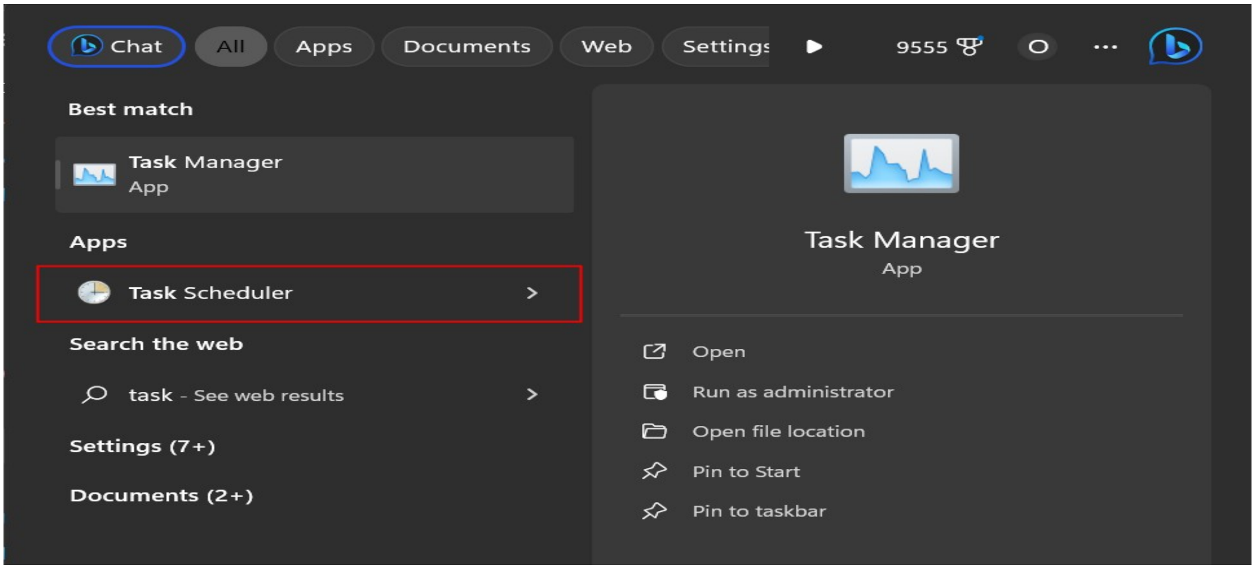


Name	Date modified	Type	Size
clamscan.exe	8/15/2023 7:46 PM	Application	178 KB
clamscan_report.log	9/2/2023 9:31 AM	Text Document	1 KB
clamsubmit.exe	8/15/2023 7:46 PM	Application	133 KB
clamunrar.lib	8/15/2023 7:47 PM	LIB File	209 KB

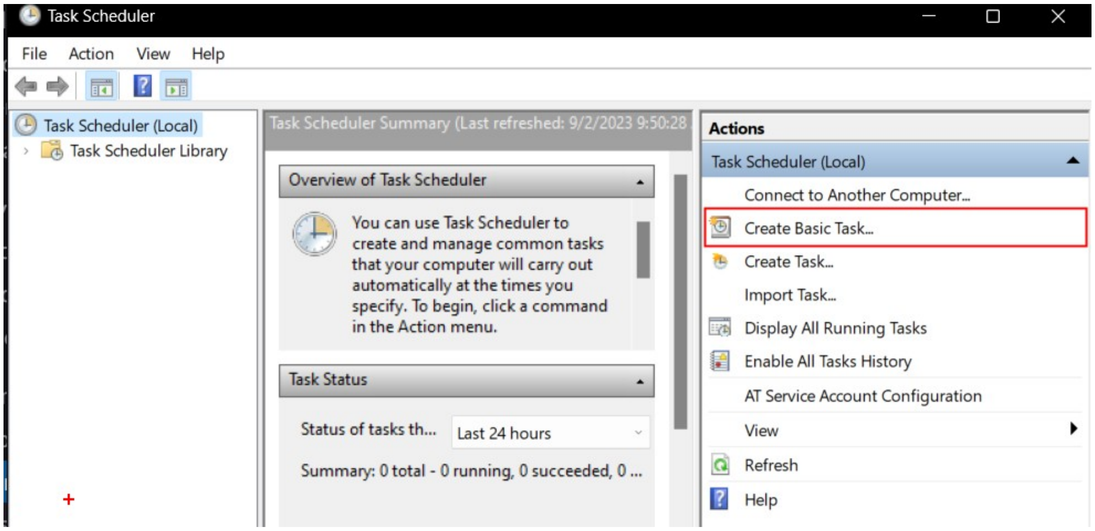
Step 7: Automate Scanning

To automate the scanning process, you can use the Task Scheduler in Windows to set up a task that runs ClamAV at a specific time.

1. Open the Task Scheduler (you can search for it in the Start Menu).



2. Click on "Create Basic Task..."



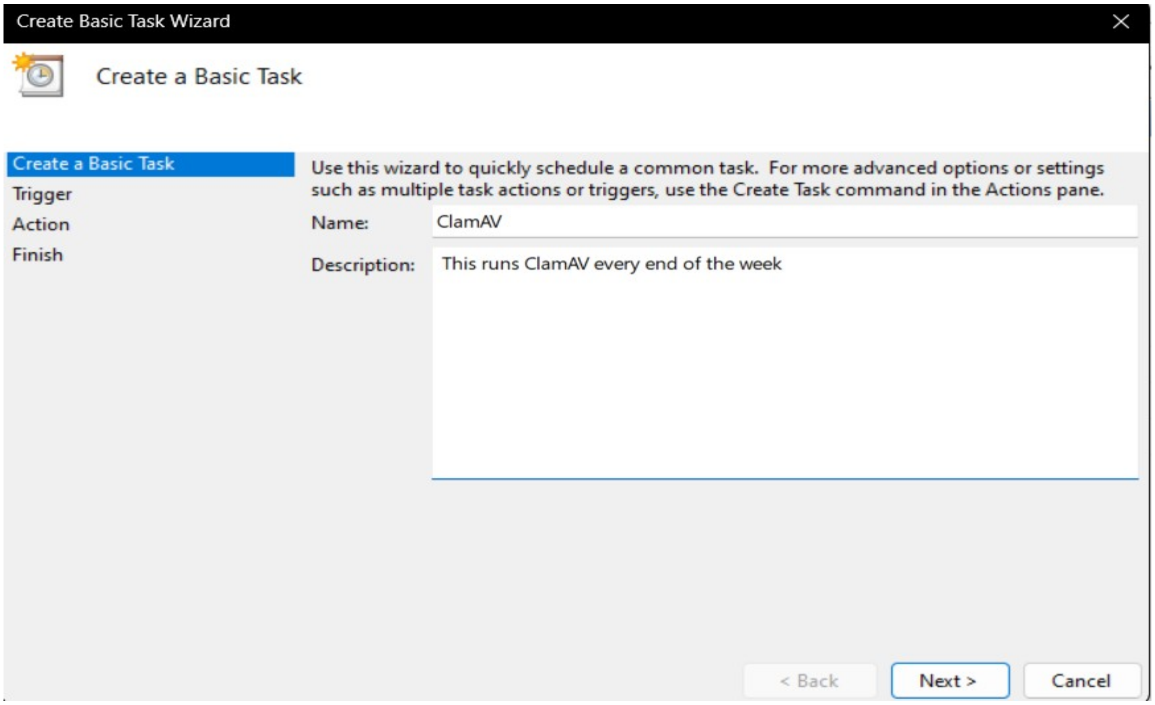
Task Scheduler Summary (Last refreshed: 9/2/2023 9:50:28

You can use Task Scheduler to create and manage common tasks that your computer will carry out automatically at the times you specify. To begin, click a command in the Action menu.

Status of tasks th... Last 24 hours

Summary: 0 total - 0 running, 0 succeeded, 0 ...

3. Name the task and add a description.



Create Basic Task Wizard

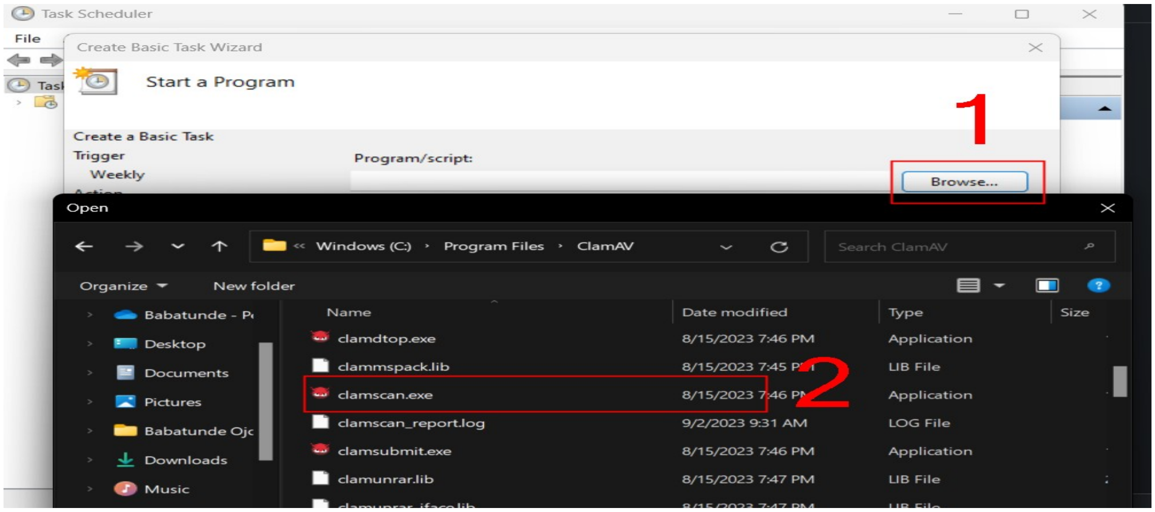
Create a Basic Task

Use this wizard to quickly schedule a common task. For more advanced options or settings such as multiple task actions or triggers, use the Create Task command in the Actions pane.

Name: ClamAV

Description: This runs ClamAV every end of the week

4. Choose when you want the task to start and how often it should run.
5. Select "Start a program" and browse to the `clamscan.exe` file in your ClamAV folder.



Create Basic Task Wizard

Start a Program

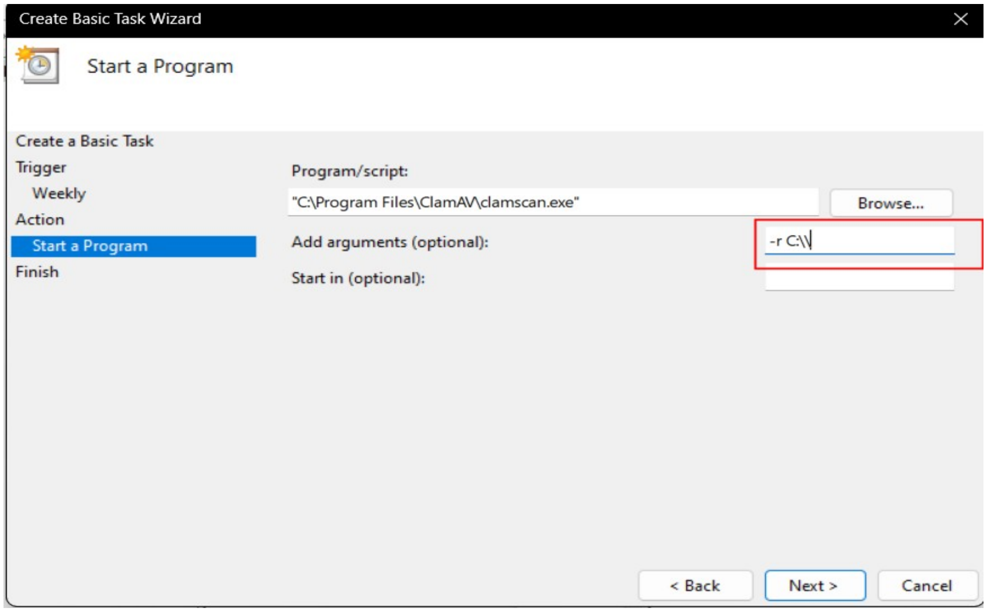
Program/script:

Open

Windows (C:) › Program Files › ClamAV

Name	Date modified	Type	Size
clamdtop.exe	8/15/2023 7:46 PM	Application	
clammspack.lib	8/15/2023 7:45 PM	LIB File	
clamscan.exe	8/15/2023 7:46 PM	Application	
clamscan_report.log	9/2/2023 9:31 AM	LOG File	
clamsubmit.exe	8/15/2023 7:46 PM	Application	
clamunrar.lib	8/15/2023 7:47 PM	LIB File	
clamunrar_iface.lib	8/15/2023 7:47 PM	LIB File	

6. In the "Add arguments" field, type `-r C:\\` to scan the entire C: drive. Adjust this as needed to specify other directories.



Create Basic Task Wizard

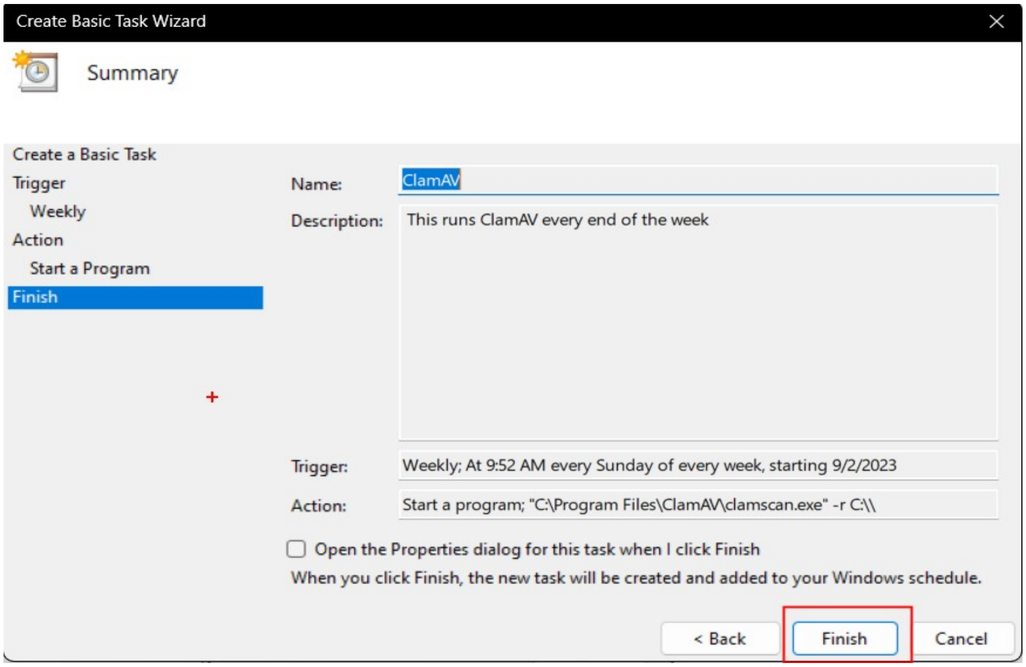
Start a Program

Program/script: "C:\Program Files\ClamAV\clamscan.exe"

Add arguments (optional): -r C:\\

Start in (optional):

7. Finish the wizard to create the task.



Create Basic Task Wizard

Summary

Name: ClamAV

Description: This runs ClamAV every end of the week

Trigger: Weekly; At 9:52 AM every Sunday of every week, starting 9/2/2023

Action: Start a program; "C:\Program Files\ClamAV\clamscan.exe" -r C:\\

☐ Open the Properties dialog for this task when I click Finish

When you click Finish, the new task will be created and added to your Windows schedule.

ClamAV Installation Guide for Ubuntu / Kali Linux

Step 1: Update Your System

Before installing any new software, it's a good practice to ensure your system is up-to-date. Open the Terminal and execute the following command:

```
sudo apt update
```

Step 2: Install ClamAV

After your system is updated, you can install ClamAV by running:

```
sudo apt install clamav clamav-daemon -y
```

This will install the ClamAV engine and the ClamAV Daemon, which you can use to set up automatic scanning.

Step 3: Check ClamAV Version

Once the installation is complete, check the ClamAV version to ensure that it is installed correctly:

```
clamscan --version
```

You should see output similar to:

```
ClamAV 1.0.1/26854/Sat Mar 25 03:22:39 2023
```

Step 4: Update ClamAV Virus Definitions Database

The next step is to update the ClamAV virus definitions database. Run the freshclam command as follows:

```
sudo freshclam
```

This command will output some information on your Terminal, including the version of the virus definitions database.

Step 5: Run a Manual Scan with ClamAV

To run a manual scan of your home directory, execute the following command:

```
clamscan -r /home
```

This command will recursively scan the `/home` directory and print the results to the Terminal.

Step 6: Automate ClamAV Scanning

If you want to automate the scanning process, you can set up a cron job that will run a scan at a specific time. For example, to run a full system scan every day at 1 am, open your crontab file by typing:

```
sudo crontab -e
```

Then, add the following line to the file:

```
0 1 * * * clamscan -r / | mail -s "ClamAV scan report" your-email@example.com
```

Make sure to replace `your-email@example.com` with your actual email address. This command will send a scan report to your email every day.

Step 7: Start and Enable ClamAV Service

Finally, to ensure ClamAV is running and starts at boot, run:

```
sudo systemctl start clamav-daemon
sudo systemctl enable clamav-daemon
```