Clam-antivirus

Virusdetectie in Linux

Ton Valkenburgh

Clam-antivirus is een open source-programma voor Unix. Er zijn echter ook implementaties voor Linux, Windows, Mac OS X, BSD en Solaris. Hier gaan we in op ClamAV voor Linux.

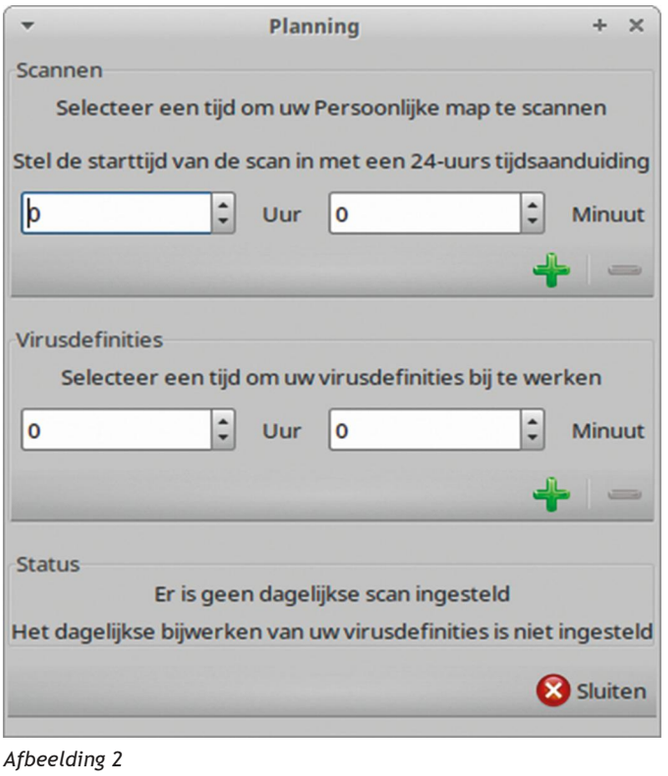
Inleiding

Er is veel discussie op internet over de vraag of bij Linux eigenlijk wel een antivirusprogramma nodig is. Linux zou zo inherent veilig zijn dat er geen behoefte aan is. Ook zou Windows door zijn groter aantal gebruikers veel interessanter zijn dan Linux voor malwareverspreiders. Linux komt echter voor in routers, servers, televisies, IoT en eigenlijk ook in Android. De verspreiding van Linux-desktops is weliswaar minder dan die met Windows, maar als doelwit is Linux echt wel interessant. Ook wordt in de Linux-desktop Wine gebruikt om Windows-programma's te kunnen gebruiken. Als je een Windows-virus op een Linux-pc hebt, zou je het kunnen verspreiden via de mail. Dus ook om die reden is het goed om onder Linux een antivirusprogramma te gebruiken. Er zijn niet veel antivirusprogramma's voor Linux. En die er zijn, zijn vaak verouderd of onhandig in gebruik. ClamAV zit standaard in de repositorie van Linux-distributies. Het is eenvoudig te installeren en configureren. ClamAV wordt gebruikt via een command-line interface. Gelukkig is er ook een grafische gebruikersinterface ClamTk.

ClamTk installeren en configureren

Start het Software Center en zoek naar *clamtk*. Na installatie vind je de grafische gebruikersinterface *ClamTk* bij *Hulpmiddelen* onder het *Startmenu*. Als je ClamTk start krijg je het openingsvenster uit afbeelding 1 te zien.

Afbeelding 1



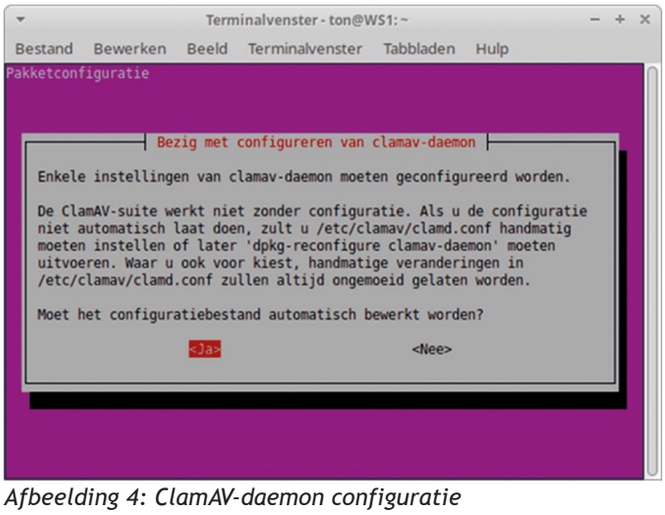
Afbeelding 2

Afbeelding 3

Dubbelklik op de *Updateassistent* en stel Ik wil zelf de virusdefinities bijwerken in. Klik daarna op *Toepassen*. Ga daarna terug. Dubbelklik nu op *Planner*. Stel nu de gewenste tijden voor Scannen en Virusdefinities in en klik op het bijbehorende plusteken (afbeelding 2). Klik daarna op *Sluiten*.

Bij *Instellingen* kun je instellen wat er moet worden gescand (afbeelding 3). Als je Wine gebruikt kun je beter bij *Op potentieel ongewenste toepassingen scannen* geen vinkje zetten. Je krijgt anders veel valse meldingen.
Standaard wordt de *Home map* van de gebruiker gescand, maar je kunt ook andere mappen instellen.

De Clam-daemon



Afbeelding 4: ClamAV-daemon configuratie

Standaard worden bestanden alleen gescand als je handmatig scant of de automatische dagelijkse scan gebruikt. Wil je al een scan doen bij het opslaan of openen van bestanden, dan moet je de Clam-deamon installeren en configureren. Ik neem aan dat je al eerder *Synaptic pakketbeheer* hebt geïnstalleerd. Met dit programma installeren we namelijk de daemon. Start *Synaptic* en zoek op clam-daemon. Vink deze aan en klik op Markeren voor installatie en daarna op Toepassen. Na installatie sluiten we *Synaptic* af.

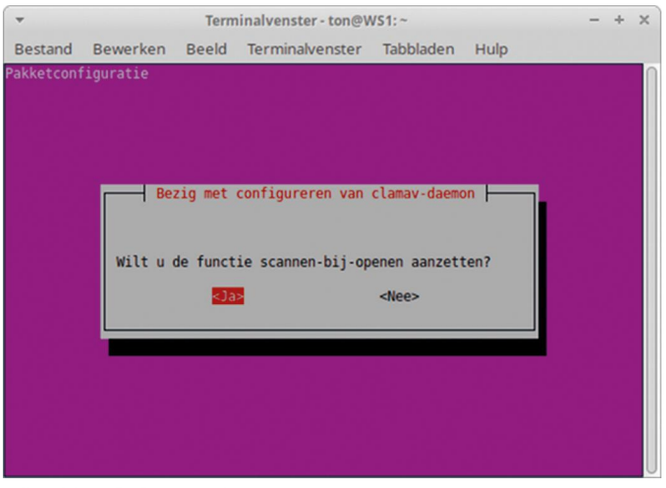
Nu moeten we de daemon nog configureren. Open een terminal en geef de opdracht:

```
sudo dpkg-reconfigure clamav-daemon
```

Geef nu *Enter* (afbeelding 4) en je gaat stap voor stap door het configureren heen. De standaardwaarden voldoen in het algemeen. Een belangrijke keuze is bij *Scannen bij openen* (afbeelding 5).

Standaard is *Nee*. Met Shift-Tab kun je het op *Ja* zetten.

Na het configureren is ClamAV gereed en actief.



Afbeelding 5: Scannen-bij-openen

Conclusie

Clam antivirus is een eenvoudig te gebruiken antivirusprogramma voor o.a. Linux pc's. Omdat het geheel automatisch kan functioneren heeft de gebruiker er geen omkijken naar. Standaard wordt de *Home map* van de gebruiker gescand.

Wil je ook andere mappen scannen dan zal dat helaas met de hand moeten worden gescand. Als de daemon echter is geïnstalleerd worden bestanden in ieder geval bij het opslaan gescand. Is ook het *Scannen-bij-operen* geactiveerd dan heb je zo goed mogelijke veiligheid.

Vergeet echter niet dat veiligheid niet alleen afhangt van technische oplossingen, maar ook sterk wordt bepaald door je eigen gedrag op internet.

Link

1. https://www.clamav.net/