Install and Configure Antiviruses (ClamAV and LMD)

Agenda

- Why use Antivirus in Linux?
- Install Linux Malware Detect
- Install ClamAV
- Using LMD & ClamAV

Why use Antiviruses in Linux?

A process is a program that has been loaded from a long-term storage device, usually a hard disk drive, into system RAM and is currently being processed by the CPU on the motherboard.

Install Linux Malware Detect

Install Linux Malware Detect from the official website.

wget http://www.rfxn.com/downloads/maldetect-current.tar.gz
tar -xvf maldetect-current.tar.gz
cd maldetect-x.y.z
./install.sh

Once the installation finishes, Linux Malware Detect will automatically create a daily cronjob task.

Install Linux Malware Detect

All configuration settings of Linux Malware Detect are stored in the file /usr/local/maldetect/conf.maldet. Configure the following subset of options:

email_alert=1
email_addr=youremail@localhost
email_subj="Malware alerts for $HOSTNAME - $(date +%Y-%m-%d)"
quar_hits=1
quar_clean=1
clam_av=1
For the values below, 1=true and 0=false.

email_alert=1: If you want to receive notifications via email.
email_addr=youremail@localhost: Enter your email address.
email_subj="Malware alerts for $HOSTNAME - $(date +%Y-%m-%d)" : Email subject of the notification.
quar_hits=1: Move the malware to quarantine.
quar_clean=1: Delete any malware detected.
clamav_scan=1: Use ClamAV's malware library to scan.

Install ClamAV

Installing ClamAV helps Linux Malware Detect to scan processes faster and more effectively. First, we need to install the EPEL repo:

yum install epel-release

Then, we install ClamAV with the following command:

yum update && yum install clamd

Using LMD & ClamAV

To scan a folder, use this command:
maldet --scan-all /home/domain.com/public_html

If you only want to scan some specified file types (.php for example), you can use the following command:
maldet --scan-all /home/domain.com/public_html/*.php

To view a scanning report, use the following command. Replace 14715-1421.3219 with the scan ID.
maldet --report 14715-1421.3219

You can update Linux Malware Detect by running:
maldet -u

To delete all quarantined files:
rm -rf /usr/local/maldetect/quarantine/*

Thank You

Email us – support@intellipaat.com

Visit us - https://intellipaat.com