# Linux环境中Clamav杀毒软件详细使用步骤

1.Clamav介绍

Clam AntiVirus 是一款 UNIX 下开源的 (GPL) 反病毒工具包，专为邮件网关上的电子邮件扫描而设计。该工具包提供了包含灵活且可伸缩的监控程序、命令行扫描程序以及用于自动更新数据库的高级工具在内的大量实用程序。该工具包的核心在于可用于各类场合的反病毒引擎共享库。

主要使用ClamAV开源杀毒引擎检测木马、病毒、恶意软件和其他恶意的威胁

## 2.部署Clamav杀毒软件

### 2.1.安装依赖软件

1.安装依赖软件

yum -y install gcc gcc-c++ openssl openssl-devel libcurl-devel

### 2.2.安装clamav

<https://www.clamav.net/downloads>

wget https://www.clamav.net/downloads/production/clamav-0.105.1-2.linux.x86\_64.rpm

1.创建管理用户  
groupadd clamav   
useradd -g clamav -s /bin/false -c "Clam AntiVirus" clamav  
  
2.安装clamav  
rpm -ivh clamav-0.105.1-2.linux.x86\_64.rpm

### 2.3.配置clamav

1.创建clamav所在的日志目录和更新病毒库的目录  
# mkdir /usr/local/clamav/logs -p  
# mkdir /usr/local/clamav/updata -p  
# touch /usr/local/clamav/logs/clamd.log  
# touch /usr/local/clamav/logs/freshclam.log  
  
2.修改目录属性  
# chown clamav:clamav /usr/local/clamav/logs/clamd.log  
# chown clamav:clamav /usr/local/clamav/logs/freshclam.log  
# chown clamav:clamav /usr/local/clamav/updata  
  
3.准备clamav配置文件  
# cd /usr/local/etc/  
# cp clamd.conf.sample clamd.conf  
# cp freshclam.conf.sample freshclam.conf  
4.配置clamav  
# vim /usr/local/etc/clamd.conf  
#Example　　//注释掉这一行  
#添加以下内容  
LogFile /usr/local/clamav/logs/clamd.log  
PidFile /usr/local/clamav/updata/clamd.pid  
DatabaseDirectory /usr/local/clamav/updata  
  
# vim /usr/local/etc/freshclam.conf  
#Example　　//注释掉这一行  
#添加以下内容  
DatabaseDirectory /usr/local/clamav/updata  
UpdateLogFile /usr/local/clamav/logs/freshclam.log  
PidFile /usr/local/clamav/updata/freshclam.pid

## 3.更新病毒库

# freshclam  
ClamAV update process started at Mon Nov 14 10:02:26 2022  
daily database available for download (remote version: 26719)  
Time: 22.5s, ETA: 0.0s [========================>] 57.41MiB/57.41MiB  
Testing database: '/usr/local/clamav/updata/tmp.9f6f2d7a7d/clamav-61931e20c8e0f80a3c63e6aa848e94b6.tmp-daily.cvd' ...  
Database test passed.  
daily.cvd updated (version: 26719, sigs: 2010711, f-level: 90, builder: raynman)  
main database available for download (remote version: 62)  
Time: 1m 04s, ETA: 0.0s [========================>] 162.58MiB/162.58MiB  
Testing database: '/usr/local/clamav/updata/tmp.9f6f2d7a7d/clamav-eca021361ed82d6cd4327ae96b774ac0.tmp-main.cvd' ...  
Database test passed.  
main.cvd updated (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)  
bytecode database available for download (remote version: 333)  
Time: 1.7s, ETA: 0.0s [========================>] 286.79KiB/286.79KiB  
Testing database: '/usr/local/clamav/updata/tmp.9f6f2d7a7d/clamav-e149b18323ee83a80329254f1d9047bf.tmp-bytecode.cvd' ...  
Database test passed.  
bytecode.cvd updated (version: 333, sigs: 92, f-level: 63, builder: awillia2)

## 4.Clamav常用命令参数

全盘扫描：# clamscan -r /  
扫描到病毒后立即删除（慎用）：# clamscan -r / --remove  
扫描到病毒后立即移动到/tmp目录：# clamscan -r / --move=/tmp  
  
clamscan --查杀当前目录下的文件  
clamscan -r --查杀当前目录的所有文件及目录   
clamscan dir --查杀dir目录   
clamscan -r dir --查杀目录dir下的所有文件及目录  
  
  
clamscan -r -i /home --remove -l /var/log/clamscan.log #递归扫描home目录，将病毒文件删除，并且记录日志，将有问题的文件都会进行记录  
clamscan -r -i /home --move=/opt/infected -l /var/log/clamscan.log #扫描指定目录，然后将感染文件移动到指定目录，并记录日志

## 5.杀毒扫描报告说明

----------- SCAN SUMMARY -----------  
Known viruses: 9141451 #已知病毒  
Engine version: 0.102.4 #软件版本  
Scanned directories: 498 #扫描目录  
Scanned files: 738 #扫描文件  
Infected files: 4 #感染文件!!!  
Data scanned: 530.25 MB #扫描数据  
Data read: 14131.60 MB (ratio 0.04:1) #数据读取  
Time: 203.805 sec (3 m 23 s) #扫描用时

<https://blog.csdn.net/weixin_44953658/article/details/122446768>

<https://blog.csdn.net/mr_wanter/article/details/124679908>