**Linux 杀毒软件 ClamAV 安装教程**

------安装ClamAV 0.104.2 版本rpm 安装方法

环境:centos7+/ClamAV0.104.2

ClamAV介绍

Clam AntiVirus是一个类UNIX系统上使用的反病毒软件包。主要应用于邮件服务器，采用多线程后台操作，可以自动升级病毒库。ClamAV是一个在命令行下查毒软件，因为它不将杀毒作为主要功能，默认只能查出您计算机内的病毒，但是无法清除。ClamAV可以工作很多的平台上，但是有少数无法支持，这就要取决您所使用的平台的流行程度了。

二、 下载安装  
ClamAV的官方下载地址：<http://www.clamav.net/download.html>

以下载 clamav-0.104.2.linux.x86\_64.rpm 为例

三、输入命令安装

rpm -ivh clamav-0.104.2.linux.x86\_64.rpm

四、安装完成后的配置

1、创建用户组和组成员

groupadd clamav

useradd -g clamav clamav

2、创建日志目录和病毒库目录

mkdir -p /usr/local/clamav/logs

mkdir -p /usr/local/clamav/updata

3、创建日志文件

touch /usr/local/clamav/logs/clamd.log

touch /usr/local/clamav/logs/freshclam.log

4、文件授权

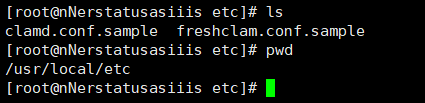
chown clamav:clamav /usr/local/clamav/logs/clamd.log

chown clamav:clamav /usr/local/clamav/logs/freshclam.log

chown clamav:clamav /usr/local/clamav/updata

5、编辑更新配置文件

cd /usr/local/etc



先从模板复制出一个配置文件：cp freshclam.conf.sample freshclam.conf



5.1、编辑这个配置文件：

Vim freshclam.conf

#Example　　//删除这一行，并添加以下内容：

UpdateLogFile /usr/local/clamav/logs/freshclam.log

PidFile /usr/local/clamav/updata/freshclam.pid

DatabaseDirectory /usr/local/clamav/updata

6、更新病毒库：freshclam

7、开始杀毒

输入命令：clamscan --help，查看帮忙信息，显示命令行参数解释和示例

输入命令：clamscan -ir /，全盘查病毒并显示结果，其中：-r 表示递归扫描子目录，-i 表示只显示发现的病毒文件。

参考地址

<https://baijiahao.baidu.com/s?id=1724801266971166972&wfr=spider&for=pc>

8、配置邮件告警

8.1、安装mail邮件工具

首先安装 mail

在CentOS 操作系统上安装mail

yum install mailx -y

8.2、配置邮箱登录发件信息

vi /etc/mail.rc

set smtp=smtp.163.com

set smtp-auth=login

set [smtp-auth-user=WYH17609972212@163.com](mailto:smtp-auth-user=WYH17609972212@163.com)

set smtp-auth-password=邮箱授权码

set [from=WYH17609972212@163.com](mailto:from=WYH17609972212@163.com)

163邮箱需要手动开启SMTP服务，并获取授权码，获取到的授权码代替163邮箱密码

测试发邮件是否正常

Echo “测试正文” | mail -s “测试标题” WYH17609972212@163.com

9、配置定时扫描和邮件告警

9.1、编辑脚本

新建sh 文件

vi /root/scan.sh

#!/bin/bash

freshclam

date=`date +%Y%m%d\_%H%M%S`

clamscan -r -i / -1 /var/log/clamav.$date.log

ip=$(ip addr | awk ‘/^[0-9]+: / {}; /inet.\*global/ {print gensub(/(.\*)\/(.\*)/,”\\1”,”g”, $2)}’)

data\_log=””

while read line

do

data\_log+=$line”<br>”

done < /var/log/clamav/clamav.$date.log

infected\_files=`echo $data\_log | sed ‘s/.\*\(Infected files: \(.\*\)<br>Data scanned.\*\?\)/\2/’`)

scan time=`echo $data log | sed ‘s/.\*\(start Date: \(.\*\)<br>End Date.\*\?\)/\2/’`

if [ $infected\_files -gt 0 ]

then

data\_log=${data\_log/SCAN SUMMARY/扫描结果}

data\_log=${data\_log/Known viruses/病毒库数量}

data\_log=${data\_log/Engine version/引擎版本}

data\_log=${data\_log/Scanned directories/已扫描目录}

data\_log=${data\_log/Scanned files/已扫描文件}

data\_log=${data\_log/Infected files/已发现病毒文件}

data\_log=${data\_log/Data Scanned/已扫描数据}

data\_log=${data\_log/Data read/读取数据}

data\_log=${data\_log/Time/扫描时长}

data\_log=${data\_log/Start Data/开始时间}

data\_log=${data\_log/End Data/结束时间}

body=”杀毒软件ClamAv于$scan\_time对您服务器$ip进行了扫描，发现有$infected\_files个高危病毒:

$data\_log<br>

请立即登录服务器处理。”

Echo $body |mail -s “$(echo -e “$ip 服务器病毒处理通知-$data\nContent-Type: text/html; charset=utf-8”)” [WYH17609972212@163.com](mailto:WYH17609972212@163.com)

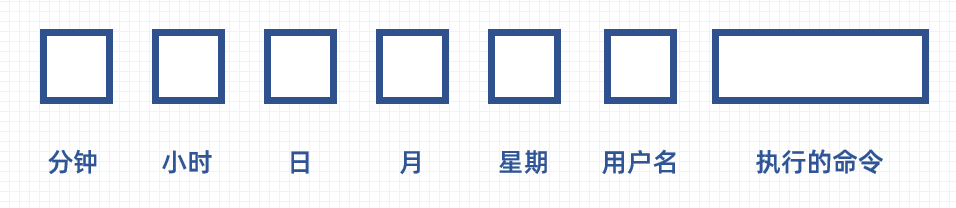
fi

9.2、配置定时计划

随后我们要编辑系统的定时计划任务，定时执行上述脚本。

cron是linux用来定时执行任务的工具，配置文件路径为。

crontab格式如下：



编辑/etc/crontab

0 4 \* \* \* root root/scan.sh

上述内容表示每天凌晨4点，以用户root身份定时执行脚本，/root/scan.sh为脚本路径。

添加完成后，请执行下方命令，启动cron，并设置开机自动启动cron。

service crond start

chkconfig crond on



到此，杀毒软件ClamAV的安装及邮件告警功能配置完成。

------安装ClamAV 0.104.2 版本rpm 安装方法

------安装Sophus 安装方法

模板类安装

sudo git clone https://github.com/strasdat/Sophus.git

cd Sophus

sudo mkdir build && cd build

sudo cmake .. && sudo make install

非模板类安装

git clone https://github.com/strasdat/Sophus.git Sophus\_no\_template

cd Sophus\_no\_template

git checkout a621ff

sudo mkdir build && cd build

sudo cmake -D CMAKE\_INSTALL\_PREFIX=/usr/local/include/sophus\_no\_template ..

sudo make install

模板类的安装没有指定安装目录，默认会在/usr/local/include/sophus