Clamav

# Clamav简介

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，可以出可疑文件以及病毒，并删除威胁文件.

# Clamav安装

第一步：Clamav下载：<http://www.clamav.net/downloads>

第二步，创建clamav用户和组

# groupadd clamav && useradd -g clamav clamav

第三部，解压编译安装

# yum install gcc openssl openssl-devel  -y

# tar -xf /data/install/clamav-0.101.2.tar.gz

# cd /data/install/clamav-0.101.2

# ./configure --prefix=/data/server/clamav && make && make install

第四部，配置配置文件

# mkdir /data/server/clamav/logs (日志存放目录)

# touch /data/server/clamav/logs/clamd.log

# touch /data/server/clamav/logs/freshclam.log

# mkdir /data/server/clamav/update (病毒库目录)

# chown clamav. –R /data/server/clamav

现在开始修改配置文件

# cd /data/server/clamav/etc

# cp clamd.conf.sample clamd.conf

# cp freshclam.conf.sample freshclam.conf

然后编辑clamav.conf文件：

#Example    （注释掉这一行）

LogFile /data/server/clamav/logs/clamd.log     （这里和下面去掉注释并修改内容）  
PidFile /data/server/clamav/updata/clamd.pid       
DatabaseDirectory /data/server/clamav/updata

开始编辑freshclam.conf文件：

#Example    （注释掉这一行    
DatabaseDirectory /data/server/clamav/updata （这里和下面去掉注释并修改内容）  
UpdateLogFile /data/server/clamav/logs/freshclam.log  
PidFile /data/server/clamav/updata/freshclam.pid

# Clamav使用

开始升级病毒库

# /data/server/clamav/bin/freshclam

开始查杀：

# /data/server/clamav/bin/clamscan /home --remove （查杀指定目录并删除感染的文件）

放入定时任务定期更新并杀毒

0 1 \* \* \* /data/server/clamav/bin/freshclam

0 30 \* \* \* /data/server/clamav/bin/clamscan --infected  -r /  --remove -l /data/server/clamav/logs/clamscan.log