ClamAV —— Linux 下的安全软件

作者：Complexity-Naughty
原文链接：https://ld246.com/article/1533785819461
来源网站：链滴

简介

官网的解释极其简单：

ClamAV的®registered是用于检测木马，病毒，恶意软件和其他恶意胁的一个开源杀毒引擎。(点击传送到官网)

今天跟小伙伴们吹牛，提到了安全问题，顺便就来为Linux安装一个杀毒引擎吧。（哈哈哈哈哈哈哈日常吹牛）

安装

1、安装clamav

```
$ yum -y install clamav
```

注：我的Linux版本：**Cent OS 7.3**， ClamAV版本：**ClamAV 0.100.1**

安装以前首先使用命令rpm -qa|grep epel-release检查是否安装epel-release。如果已安装，会出现：

```
[root@liaow0316 11:01:47 /]$ rpm -qa|grep epel-release
epel-release-7-11.noarch
[root@liaow0316 11:05:00 /]$
```

如果没有，使用yum -y install epel-release先安装epel-release，再安装clamav。

2、更新数据库

```
$ freshclam
```

配置

[注：yum安装有默认配置，可以跳过配置，试用后再配置]

以yum方式安装完成后，我并没有找到网上说的那些安装目录，所以我使用rpm -qla|grep clam命令自己找了一下他的相关目录：

```
[root@liaow0316 11:11:45 /]$ rpm -qla|grep clam
/etc/cron.d/clamav-update
/etc/freshclam.conf
/etc/logrotate.d/clamav-update
/etc/sysconfig/freshclam
/usr/bin/freshclam
/usr/share/clamav/freshclam-sleep
/usr/share/man/man1/freshclam.1.gz
/usr/share/man/man5/freshclam.conf.5.gz
/var/lib/clamav/bytecode.cld
/var/lib/clamav/daily.cld
/var/lib/clamav/main.cld
/var/lib/clamav/mirrors.dat
/var/log/freshclam.log
```

```
/etc/clamd.d
/usr/share/clamav
/var/lib/clamav
/usr/bin/clambc
/usr/bin/clamconf
/usr/bin/clamdscan
/usr/bin/clamdtop
/usr/bin/clamscan
/usr/bin/clamsubmit
/usr/share/doc/clamav-0.100.1
/usr/share/doc/clamav-0.100.1/clamdoc.pdf
/usr/share/doc/clamav-0.100.1/phishsigs_howto.pdf
/usr/share/doc/clamav-0.100.1/signatures.pdf
/usr/share/man/man1/clambc.1.gz
/usr/share/man/man1/clamconf.1.gz
/usr/share/man/man1/clamdscan.1.gz
/usr/share/man/man1/clamdtop.1.gz
/usr/share/man/man1/clamscan.1.gz
/usr/share/man/man1/clamsubmit.1.gz
/usr/share/man/man5/clamav-milter.conf.5.gz
[root@liaow0316 11:12:02 /]$
```

发现它的文件到处分布，目录并没有太大的实际参考价值。

所以，还是使用最下面的指令来查看帮助吧。

1、配置文件导出

```
$ clamconf -g clamd.conf > /home/clamscan/clamd.conf
```

将配置文件模板输出到/home/clamscan/目录下的clamd.conf文件中，这才有了网上说的配置文件。

2、未完待续。（吃饭去了）

使用

使用clamscan杀毒

clamscan是扫描病毒的命令，这里简单的列举一部分常用指令参数

```
$ clamscan  //不加参数的使用：扫描当前目录下的文件
$ clamscan -V  //查看clamAV的版本
$ clamscan -r  //递归扫描子文件夹
$ clamscan -i  //仅仅显示被感染的文件
$ clamscan -o  //跳过显示状态ok的文件
$ clamscan --remove  //检测到有病毒时，直接删除
$ clamscan --no-summary  //不显示统计信息
$ clamscan -l scan.log  //将扫描日志写入scan.log文件

//以上命令都可以在末尾添加文件夹，来扫描指定目录，如
$ clamscan --remove -rio /home/liaow0316  //扫描/home/liaow0316目录下的所有文件，只示病毒文件，并同时删除
```

示例：

```
[root@liaow0316 12:48:16 /home/clamscan]$ clamscan -l aa.log
/home/clamscan/clamd.conf: OK
/home/clamscan/aa.log: OK
/home/clamscan/clamscan.log: OK

----------- SCAN SUMMARY -----------
Known viruses: 6603127
Engine version: 0.100.1
Scanned directories: 1
Scanned files: 3
Infected files: 0
Data scanned: 0.04 MB
Data read: 0.02 MB (ratio 2.00:1)
Time: 13.739 sec (0 m 13 s)
[root@liaow0316 13:04:22 /home/clamscan]$
```

使用clamd杀毒

不知道是版本问题还是什么其他原因，我安装的clamav并没有clamd服务模块，所以也这一种杀毒方就没有尝试。我使用的版本：**ClamAV 0.100.1**（使用clamscan -V查看版本）

指令

[注：这些指令都是官方github上的说明，点击相关指令，跳转官方说明文档]

clamscan

一个命令行程序，用于扫描不需要clamd守护程序的文件和目录。

clamd

多线程守护程序。

当clamd运行时，使用这些工具来与它进行交互：

- clamdtop

要监视的命令行GUI clamd。

- clamdscan

通过命令行程序扫描文件和目录clamd。

freshclam

签名数据库（cvd）更新工具。

libclamav

clamav库 - 因此您可以将ClamAV引擎构建到您的程序中。

sigtool

一个签名数据库（cvd）操纵工具 - 用于恶意软件分析师和签名编写者。

clambc

另一种专门用于字节码签名的签名操作工具。

clamconf

用于检查或生成ClamAV配置文件并收集有助于远程调试问题所需的其他信息的工具。

clamav-config

用于检查ClamAV如何编译的附加工具。