clamd설치 / Sendmail 연동하기

clamav 설치

1.Sendmail과 연동하기 위한 패키지 설치

```
$> yum install -y sendmail-devel
```

1. clam바이너리 다운로드 - http://sourceforge.net/projects/clamav/files/clamav/0.97.8/clamav-0.97.8.tar.gz
2. 바이너리 컴파일 & 설치

```
$> tar -zxvf clamav-0.97.8.tar.gz
$> useradd -s /bin/false clamav
$> cd clamav-0.97.8
$> ./configure --prefix=/usr/ --sysconfdir=/etc/ --enable-milter
$> make;make install
```

3. 설정파일 변경 – Freshclam (엔진 업데이트)

```
$> $ vi /etc/freshclam.conf
#Example
...
UpdateLogFile /var/log/clamav/freshclam.log
LogTime yes
DatabaseMirror database.clamav.net
NotifyClamd /etc/clamd.conf
SubmitDetectionStats /etc/clamd.conf
...
```

4. 설정파일 변경 – Clamd (Clamav데몬)

```
$> vi /etc/clamd.conf
LogFile /var/log/clamav/clamd.log
LogTime yes
LogSyslog yes
PidFile /var/run/clamav/clamd.pid
LocalSocket /var/run/clamav/clamd.sock
FixStaleSocket yes
TCPSocket 3310
TCPAddr 127.0.0.1
StreamMaxLength 100M
User clamav
PhishingSignatures yes
PhishingScanURLs yes
MaxFileSize 30M
```

5. 설정파일 변경 – Milter(SMTP와 연동)

```
$> vi /etc/clamav-milter.conf
MilterSocket /var/run/clamav/clamav-milter.sock
MilterSocketMode 666
FixStaleSocket yes
User clamav
PidFile /var/run/clamav/clamav-milter.pid
ClamdSocket unix:/var/run/clamav/clamd.sock
OnClean Accept
OnInfected Quarantine
OnFail Defer
LogFile /var/log/clamav/clamav-milter.log
LogTime yes
```

6. 파일 생성 및 권한 변경

```
$> mkdir /usr/share/clamav
```

```
$> cd /var/log
$> mkdir clamav
$> cd clamav
$> touch clamav-milter.log
$> touch clamd.log
$> touch freshclam.log
$> cd /var/run
$> mkdir clamav
$> chown -R clamav.clamav /var/log/clamav
$> chown -R clamav.clamav /var/run/clamav
$> chown -R clamav.clamav /usr/share/clamav
```

7. 엔진 업데이트 & 프로세스 실행

```
$> freshclam
$> /usr/sbin/clamav-milter
```

8. 정상적으로 실행할 경우

```
$> ps -ef | grep clam
clamav 4242 1 0 15:37 ? 00:00:00 clamd
clamav 4251 1 0 15:37 ? 00:00:00 clamav-milter
```

Sendmail연동

1. /etc/mail/sendmail.mc 파일 열어서

```
$> vi /etc/mail/sendmail.mc
...
INPUT_MAIL_FILTER(`clamav`, `S=local:/var/run/clamav/clamav-milter.sock, F=, T=S:4m;R:4m`)
define(`confINPUT_MAIL_FILTERS`, `clamav`)
...
*따음표(‘) 와 역슬래쉬(`)와 구분해야 되요
```

2. sendmail 서비스는 freshclam 후에 구동되도록 설정이 필요.

```
$> chkconfig sendmail off
```

3. 자동으로 엔진업데이트를 하기 위해서는 freshclam 프로세스를 데몬형태로 띄우면 됨(conf파일 정책에 따라 2시간마다 한번씩 업데이트 시도함)

```
$> freshclam -d
```

4. /etc/rc.local에 아래 내용 추가

```
$> vi /etc/rc.local
/usr/sbin/clamd /usr/sbin/clamav-milter freshclam -d
$> /etc/init.d/sendmail start
```

Revision #1
★Created 8 June 2022 06:34:13 by artop0420
Updated 24 December 2023 02:31:41 by artop0420