

```
/******\
* Gökhan ALKAN
* gokhan [at] enderunix [dot] org
* EnderUNIX Yazılım Gelistirme Takımı
* http://www.enderunix.org
*
* Sürüm : 1.0
* Tarih : 25.05.2007
*****/
```

<u>1 CLAMAV KURULUMU.....</u>	<u>1</u>
<u>1.1 Kaynak Koddan Kurulum.....</u>	<u>1</u>
<u>1.2 FreeBSD Port Ağacından Kurulum.....</u>	<u>1</u>
<u>2 CLAMAV YAPILANDIRMASI.....</u>	<u>2</u>

## 1 CLAMAV KURULUMU

### 1.1 Kaynak Koddan Kurulum

Öncelikle gerekli paketler teminedilmelidir. <http://www.clamav.net> ana sayfasından temin edilebilir. Clamav'ın çalışması için gerekli grup ve kullanıcı oluşturulmalıdır.

Linux için

```
# groupadd clamav
# useradd -g clamav -s /bin/false -c "Clam AntiVirus" clamav
```

FreeBSD için

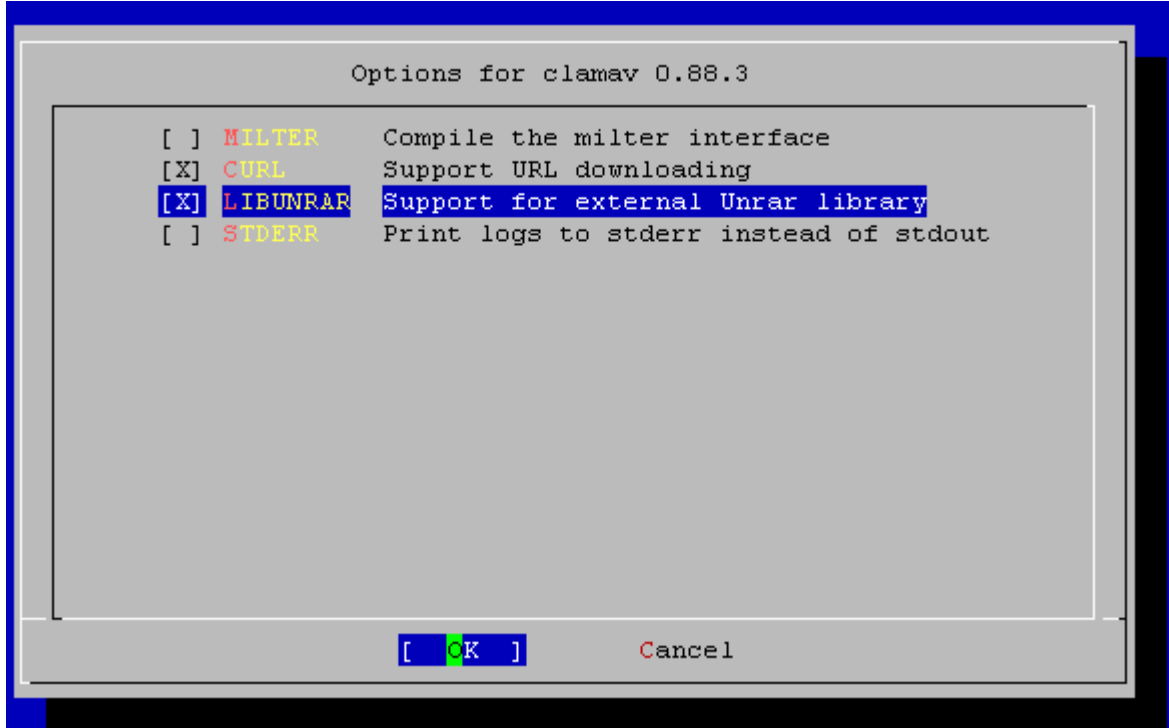
```
# pw groupadd clamav
# pw useradd clamav -g clamav -s /usr/sbin/nologin -c "Clam AntiVirus" -d /tmp
```

```
# tar -zxvf clamav-0.90.2.tar.gz
# cd clamav-0.90.2
# ./configure --prefix=/usr/local/clamav
# make
# make install
```

### 1.2 FreeBSD Port Ağacından Kurulum

```
# cd /usr/ports/security/clamav
# make install clean
```

Ekranı gelen ncurses tabanlı menüden istenilen özellikler seçilebilir.



Clamav ile beraber veritabanını otomatik olarak güncelleştirmek için freshclam adından araç gelmektedir. Bu sayede veritabanı sürekli güncel kalmaktadır. Clamav ile beraber freshclam'ı açılışta aktif hale getirmek için `/etc/rc.conf` dosyasına aşağıdaki satırlar yazılmalıdır.

```
# vi /etc/rc.conf
clamav_clamd_enable="YES"
clamav_freshclam_enable="YES"
#
```

Clamd başlatıldığında `/var/run/clamav/clamd` unix-domain soketi oluşturur. İstenirse `clamd.conf` yapılandırma dosyası içeririnden değiştirilebilir yada `/etc/rc.conf` dosyasında `clamav_clamd_socket` ile belirtilebilir ön tanımlı değeri `/var/run/clamav/clamd` dir.

## 2 CLAMAV YAPILANDIRMASI

Clamav yapılandırması `clamd.conf` dosyasıdır. Clamav'ın çalıştırılmasından önce freshclam çalıştırılıp veritabanının güncellenmesi gerekmektedir Freshclam için yapılandırma dosyası ise `freshclam.conf` dosyasıdır

```
# vi /usr/local/etc/freshclam.conf
```

```
UpdateLogFile /var/log/clamav/freshclam.log
```

Freshclam'ın log dosyalarını nereye yazacağını gösterir.

İstenirse gerekli Proxy bilgileri gerekli alanlara girilerek proxy kullanılabilir.Ön tanımlı olarak aktif değildir. Proxy kullanılabilmesi için yapılandırma dosyasının izini 0700 olmalıdır

```
# chmod 0700 /usr/local/etc/freshclam.conf
```

```
HTTPProxyServer myproxy.com
HTTPProxyPort 1234
HTTPProxyUsername myusername
HTTPProxyPassword mypass
```

#Example satırının basındaki # işareti olmalıdır.

Freshclam clamav için hazırlanmış ön tanımlı veritabanı güncelleştirme aracıdır. Komut satırı ve daemon olarak iki modda çalışmaktadır Alabileceği bazı parametreler aşağıda belirtilmiştir.

```
--config-file= : yapılandırma dosyasının yerini belirtir.
--log= yada -l : log dosyasının yeri belirtilir.
--daemon yada -d : daemon olarak çalışır.
--quiet : sadece hata mesajlarını basar
--debug: debug moda çalışır.
```

Yada cron işi girilerek freshclam çalıştırılabilir.

```
X * * * * /usr/local/bin/freshclam --quiet
```

Burada belirtilmek istenen zaman dilimi için önerilen X zaman diliminin 3 ile 57 arasında olmasıdır. 10'un katlarının olmasıda önerilmiyor çünkü çok fazla tercih edilen bir zaman dilimi.

Clamd için yapılandırma dosyası ise clamd.conf dosyasıdır.

```
# vi /usr/local/etc/clamd.conf
```

LogFile /var/log/clamav/clamd.log  
Log dosyasını yerini belirtir.

LocalSocket /var/run/clamav/clamd  
Clamd çalıştığında unix-domain soketi oluşturur. netstat ile görülebilir.

```
# netstat -na | grep 'clamd'
ce4f53d4 stream 0 0 cdf8b660 0 0 0 /var/run/clamav/clamd
#
```

User clamav  
Hangi kullanıcı ile çalışacağını belirtir.

#Example satırının başındaki # işareti olmalıdır.

```
# clamd ile yada freebsd port ağacından kurulum yapıldıysa hazır betiklerle başlatılabilir.
```

```
# /usr/local/etc/rc.d/clamav-clamd start
```