

**ÍNDICE DE CONTENIDO**

<b>Tema 11. Instalacion de Antivirus ClamAV.....</b>	<b>3</b>
<b>11.1 Sobre ClamAV.....</b>	<b>5</b>
<b>11.2 Instalacion ClamAV.....</b>	<b>5</b>
<b>11.3 Configuracion de ClamAV.....</b>	<b>9</b>
11.3.1 Fichero /etc/freshclam.conf.....	9
11.3.1.1 Definiendo la cantidad de actualizaciones que se buscan por dia.....	9
11.3.2 Fichero /etc/clamd.conf.....	9
11.3.2.1 Busqueda de fraude mediante firmas.....	11
11.3.2.2 Busqueda de fraude mediante analisis de direcciones.....	11
11.3.2.3 Busqueda de fraude haciendo uso de una base de datos.....	11
11.3.2.4 Analizar el contenido HTML.....	11
11.3.2.5 Analisis a Ficheros.....	11
11.3.2.6 Tamaño maximo de archivos a analizar.....	11
11.3.2.7 Tamaño maximo de subcarpetas a analizar.....	13
11.3.2.8 Tamaño maximo de archivos a analizar.....	13
<b>11.4 Activando ClamAV.....</b>	<b>13</b>

# Información de Derechos reservados de esta publicación.

## Reconocimiento-NoComercial-CompartirIgual 2.1

Usted es libre de:

- Copiar, Distribuir y Comunicar públicamente la obra

**Bajo las condiciones siguientes:**



**Reconocimiento.** Debe reconocer y citar al autor original.



**No comercial.** No puede utilizar esta obra para fines comerciales.



**Compartir bajo la misma licencia.** Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta.

- Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.
- alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor

**Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior.**

Reconocimiento-NoComercial-CompartirIgual 2.1

# Tema 11. Instalacion de Antivirus ClamAV





## 11.1 Sobre ClamAV

El proyecto ClamAv Antivirus fue fundado en el año 2001 por Tomasz Kojm. Actualmente tiene una implementación superior a los 500 000 servidores en todo el mundo. Así mismo ClamAV nació como un proyecto Open Source que pretende identificar y bloquear virus en el sistema. El primer objetivo de ClamAv fue combatir el Spam. Como consecuencia de ello ClamAv se está usando en un número elevado de servidores de correo.

Gracias a la colaboración de varias compañías, universidades y otras organizaciones ha posibilitado al proyecto ClamAV poseer una red extensa de distribución rápida y fiable en todo el mundo.

Algunas de las características de ClamAV son las siguientes:

- Licenciado bajo GNU General Public License 2
- Detecta alrededor de 320.000 virus, gusanos, troyanos, incluyendo virus programados como macros de Microsoft Office.
- Escaneo de archivos y ficheros comprimidos:
  - ZIP
  - RAR
  - ARJ
  - TAR
  - Gzip
  - Bzip2
  - MS OLE2
  - MS Cabinet File
  - MS CHM
  - MS SZDD
  - BinHex
  - SIS
  - Autolt
- Soporta formatos especiales como:
  - HTML
  - RTF
  - PDF
  - CryptFF
  - SCREnc
  - uuencode
  - TNEF

## 11.2 Instalacion ClamAV

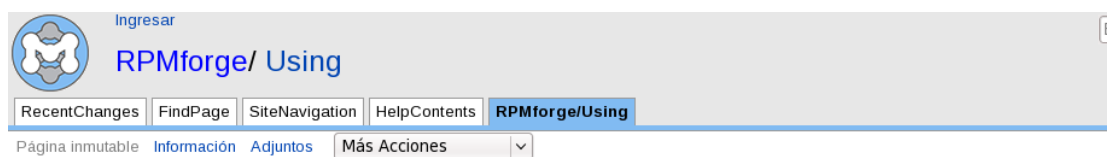
Para poder llevar a cabo la instalacion de ClamAV se deben agregar los repositorios de rpmforge, ya que ClamAV no esta contenido en los repositorios originales de Centos

Los repositorios RMPforge se agregaran de la siguiente manera.

Acceda al portal web de RMPforge -->

<https://rpmrepo.org/RPMforge/Using>

La pagina debe lucir muy parecida a esta



### Using RPMforge

To enable RPMforge you can install the rpmforge-release package for your distribution.

#### Installing the rpmforge-release package

Download the correct package below and install the package by doing:

```
wget http://packages.sw.be/rpmforge-release/rpmforge-release-0.3.6-1.$dist.rf.$arch.rpm
rpm -Uvh rpmforge-release-0.3.6-1.$dist.rf.$arch.rpm
```

⚠ **WARNING** Substitute the URL in the example with the exact one from below, else it will not work.

This will install the repository for smart, apt and yum. For up2date a manual intervention is required.

#### Distributions

##### RHEL / CentOS

💡 **TIP** For CentOS Yum users there is a very good document on [how to enable RPMforge safely using the Yum priorities plugin](#)

- RHEL5 / CentOS-5
  - i386: <http://packages.sw.be/rpmforge-release/rpmforge-release-0.3.6-1.el5.rf.i386.rpm>
  - x86\_64: [http://packages.sw.be/rpmforge-release/rpmforge-release-0.3.6-1.el5.rf.x86\\_64.rpm](http://packages.sw.be/rpmforge-release/rpmforge-release-0.3.6-1.el5.rf.x86_64.rpm)
- RHEL4 / CentOS-4
  - i386: <http://packages.sw.be/rpmforge-release/rpmforge-release-0.3.6-1.el4.rf.i386.rpm>
  - x86\_64: [http://packages.sw.be/rpmforge-release/rpmforge-release-0.3.6-1.el4.rf.x86\\_64.rpm](http://packages.sw.be/rpmforge-release/rpmforge-release-0.3.6-1.el4.rf.x86_64.rpm)
- RHEL3 / CentOS-3
  - i386: <http://packages.sw.be/rpmforge-release/rpmforge-release-0.3.6-1.el3.rf.i386.rpm>
  - x86\_64: [http://packages.sw.be/rpmforge-release/rpmforge-release-0.3.6-1.el3.rf.x86\\_64.rpm](http://packages.sw.be/rpmforge-release/rpmforge-release-0.3.6-1.el3.rf.x86_64.rpm)

Descarge el paquete enmarcado en el recuadro negro, en particular la version para 32 bits (i386).

La razon del porque descargamos este paquete y no los demas es porque nosotros tenemos instalada la version de Centos 5.3.

Al finalizar la descarga abra una terminal, vaya a donde descargo el paquete y posteriormente instale de la siguiente manera:

```
[BASH]# rpm -ivh rpmforge-release-0.3.6-1.$dist.rf.$arch.rpm
```

Una vez concluida esta accion podremos empezar a instalar ClamAV.

Los paquetes que instalaremos seran los siguientes:

● clamav	<b>El paquete antivirus</b>
● libclamav	<b>La API para integrar mas modulos</b>
● clamtk	<b>interfaz gráfica basada en GTK</b>
● clamd	<b>Métodos para ejecutar el motor en segundo plano (demonio del sistema)</b>

Instale estos paquetes tecleando en consola lo siguiente:

```
[BASH]# sudo yum install clamav libclamav clamtk clamd
```

## 11.3 Configuracion de ClamAV

Al concluir la instalacion deberan ser editados los siguientes ficheros:

- /etc/freshclam.conf
- /etc/clamd.conf

### 11.3.1 Fichero /etc/freshclam.conf

Con la ayuda de algun editor de textos agregue o comente las siguientes lineas.

#### 11.3.1.1 Definiendo la cantidad de actualizaciones que se buscan por dia

Con la ayuda de algun editor de textos edite, busque y agregue la siguiente linea

```
Checks 12
```

El comando

```
Cheks
```

define el intervalo de tiempo en el que ClamAV buscara y descargara las actualizaciones de los virus mas actuales. El numero

```
12
```

Nos indica que cada 2 horas ClamAV buscara y descargara las actualizaciones

## 11.3.2 Fichero /etc/clamd.conf

Con la ayuda de algun editor de textos agregue o comente las siguientes lineas.

### 11.3.2.1 Búsqueda de fraude mediante firmas

Para habilitar la búsqueda de fraude mediante firmas solo debe agregar la siguiente linea

```
PhishingSignatures yes
```

En caso de que el valor tenga asignada la sentencia “no” solo habra que cambiarla por “yes”

### 11.3.2.2 Búsqueda de fraude mediante analisis de direcciones

Para habilitar la búsqueda de fraude mediante analisis de direcciones solo debe agregar la siguiente linea

```
PhishingURLs yes
```

En caso de que el valor tenga asignada la sentencia “no” solo habra que cambiarla por “yes”

### 11.3.2.3 Búsqueda de fraude haciendo uso de una base de datos

Para habilitar la búsqueda de fraudes haciendo uso de una base de datos solo debe agregar la siguiente linea

```
PhishingRestrictedScan yes
```

En caso de que el valor tenga asignada la sentencia “no” solo habra que cambiarla por “yes”

### 11.3.2.4 Analizar el contenido HTML

Para habilitar el analisis al contenido HTML solo debe agregar la siguiente linea

```
ScanHTML yes
```

En caso de que el valor tenga asignada la sentencia “no” solo habra que cambiarla por “yes”

### 11.3.2.5 Analisis a Ficheros

Para habilitar el analisis a los ficheros solo debe agregar la siguiente linea

```
ScanArchive yes
```

En caso de que el valor tenga asignada la sentencia “no” solo habra que cambiarla por “yes”

### 11.3.2.6 Tamaño maximo de archivos a analizar

Para definir el tamaño maximo de archivos a analizar solo debe agregar la siguiente linea



```
ArchiveMaxFileSize 5M
```

Así mismo, puede definir una cantidad mayor de bytes a analizar, solo debe usar la siguiente nomenclatura

```
(m, M = megabytes)
(k, K = kilobytes)
```

### 11.3.2.7 Tamaño máximo de subcarpetas a analizar

Para definir el tamaño máximo de subcarpetas a analizar solo debe agregar la siguiente línea

```
ArchiveMaxRecursion 10
```

El número "10" se refiere a la cantidad de recursiones que hará sobre cada carpeta, usted puede cambiar este valor a su conveniencia

### 11.3.2.8 Tamaño máximo de archivos a analizar

Para definir el tamaño máximo de archivos a analizar solo debe agregar la siguiente línea

```
ArchiveMaxFiles 1000
```

El número "1000" se refiere a la cantidad de archivos que analizará ClamAV, usted puede cambiar este valor a su conveniencia

## 11.4 Activando ClamAV

Para iniciar el Antivirus ClamAV por primera vez solo deberá teclear en terminal el siguiente comando:

```
[root@ localhost ~]# /etc/init.d/clamd start
```

Igualmente existen opciones ya sea para reiniciar, detener, recargar o conocer el status en el que se encuentra el Antivirus ClamAV. Estas opciones pueden ser consultadas en la siguiente tabla:

<b>start</b>	Inicia el servicio
<b>stop</b>	Detiene el servicio
<b>restart</b>	Reinicia el servicio.-La diferencia con reload radica en que al ejecutar un restart este mata todos los procesos relacionado con el servicio y los vuelve a generar de nueva cuenta
<b>reload</b>	Recarga el servicio.-La diferencia con restart radica en que al ejecutar un reload este solamente carga las actualizaciones hechas al fichero de configuración del servicio sin necesidad de matar los procesos relacionados con el mismo, por lo que podría entenderse que hace el cambio en caliente.
<b>condrestart</b>	Reinicio Condicional.- Solamente se inicia si el servicio se encuentra ejecutándose.
<b>status</b>	Da a conocer el estado en el que se encuentra el servicio

Como alternativa también podemos ocupar el siguiente comando para iniciar el Antivirus ClamAV

```
[root@ localhost ~]# service clamd start
```

Y de igual manera podemos usar las opciones antes descritas en la tabla anterior.

Recuerde que estos comandos se ejecutan como root.