Índice de contenido

Información de Derechos reservados de esta publicación.

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 implementacion superior a los 500 000 servidores en todo el mundo. Asi 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 caracteristicas 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
    - AutoIt
- Soporta formatos especiales como:
    - HTML
    - RTF
    - PDF
    - CryptFF
    - SCREnc
    - uuencode
    - TNEF

11.2 Instalacion ClamAV

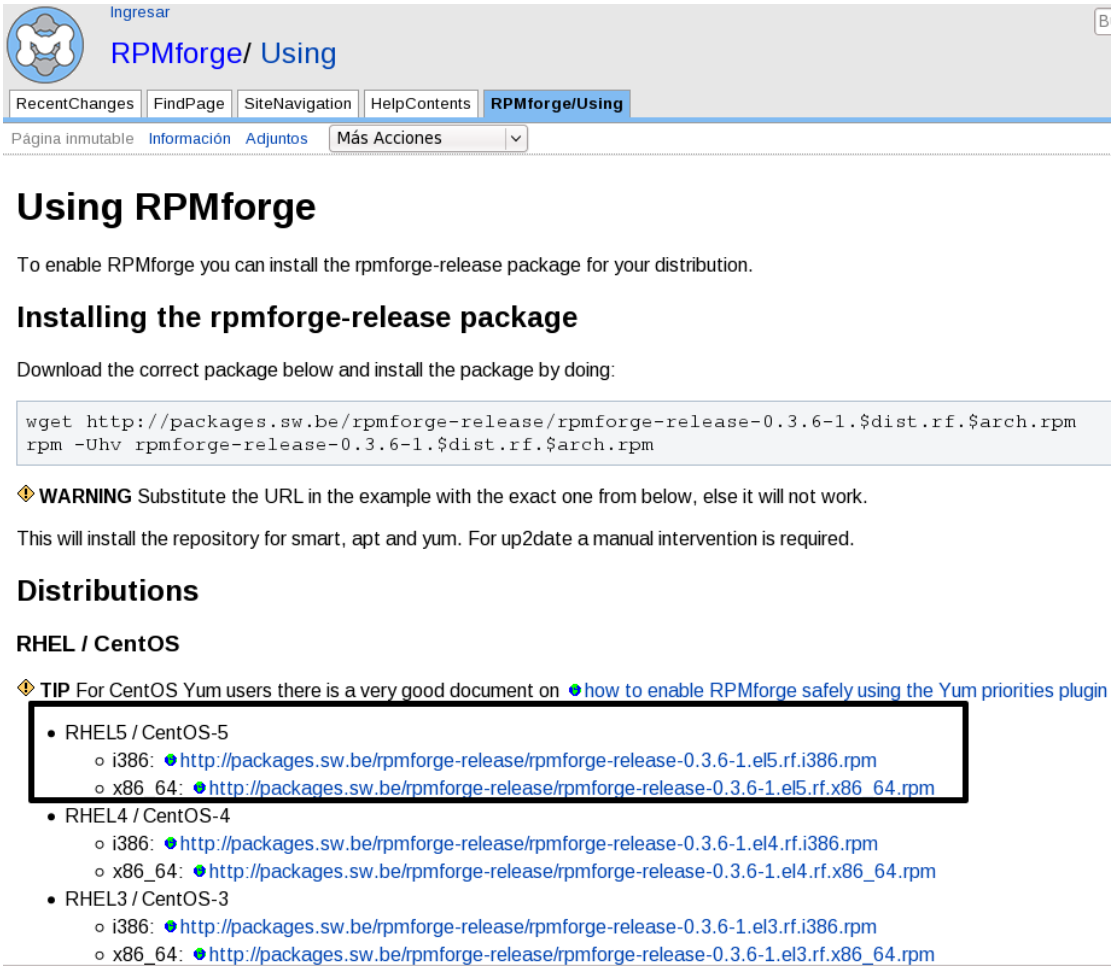
Para poder llevar a cabo la instalacion de ClamAV se deben agregar los repositorios de rpmforge, ya que ClamAV no esta contenido en los repositorios originales de Centos

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



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

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 agrege 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 agrege 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 agrege o comente las siguientes lineas.

11.3.2.1 Busqueda de fraude mediante firmas

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

```
PhisingSignatures yes
```

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

11.3.2.2 Busqueda de fraude mediante analisis de direcciones

Para habilitar la busqueda 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 Busqueda de fraude haciendo uso de una base de datos

Para habilitar la busqueda 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

```
ArchiveMaxiFileSize 5M
```

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

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

11.3.2.7 Tamaño maximo de subcarpetas a analizar

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

```
ArchiveMaxRecursion 10
```

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

11.3.2.8 Tamaño maximo de archivos a analizar

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

```
ArchiveMaxFiles 1000
```

El numero **"1000"** se refiere a la cantidad de archivos que analizara 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 el Antivirus ClamAV. Estas opciones pueden ser consultadas en la siguiente tabla:

start	Inicia el servicio
stop	Detiene el servicio
restart	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
reload	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.
condrestart	Reinicio Condicional.- Solamente se inicia si el servicio se encuentra ejecutándose.
status	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.