SOPHOS

Security made simple.

Sophos Anti-Virus para Linux

Guía de configuración

Versión: 9

Contenido

1 Acerca de esta guía....5
2 Acerca de Sophos Anti-Virus para Linux....6
2.1 Función de Sophos Anti-Virus....6
2.2 Protección de Sophos Anti-Virus....6
2.3 Uso de Sophos Anti-Virus....6
2.4 Configurar Sophos Anti-Virus....6
3 Escaneado en acceso....8
3.1 Comprobar que el escaneado en acceso se encuentra activo....8
3.2 Comprobar que el escaneado en acceso se inicia de forma automática al arrancar....8
3.3 Iniciar el escaneado en acceso....8
3.4 Detener el escaneado en acceso....9
4 Escaneado en demanda....10
4.1 Ejecutar un escaneado en demanda....10
4.2 Configurar el escaneado en demanda....11
5 Qué ocurre si se detecta algún virus....14
6 Limpiar virus....16
6.1 Información de limpieza....16
6.2 Poner en cuarentena los archivos infectados....16
6.3 Limpiar archivos infectados....17
6.4 Recuperación tras una infección....18
7 Ver el registro de Sophos Anti-Virus....19
8 Actualizar Sophos Anti-Virus de forma inmediata....20
9 Acerca de la compatibilidad del kernel....21
9.1 Acerca de la compatibilidad con kernel nuevos....21
9.2 Acerca de la compatibilidad con kernel personalizados....21
10 Configurar escaneados programados....22
10.1 Añadir un escaneado programado desde un archivo....22
10.2 Añadir un escaneado programado de forma manual....22
10.3 Exportar un escaneado programado a un archivo....23
10.4 Exportar los nombres de todos los escaneados programados a un archivo....23
10.5 Exportar un escaneado programado a la salida estándar....23
10.6 Exportar los nombres de todos los escaneados programados a la salida estándar....23
10.7 Actualizar un escaneado programado desde un archivo....24

10.8 Actualizar un escaneado programado de forma manual....24
10.9 Ver el registro de un escaneado programado....24
10.10 Eliminar un escaneado programado....25
10.11 Eliminar todos los escaneados programados....25
11 Configurar alertas....26
11.1 Configurar alertas de escritorio....26
11.2 Configurar alertas en la línea de comandos....26
11.3 Configurar alertas por email....27
12 Configurar registro....30
13 Configurar la actualización....31
13.1 Conceptos básicos....31
13.2 Comando de configuración savsetup....31
13.3 Ver la configuración de actualización en un ordenador....31
13.4 Configurar un servidor de actualización....32
13.5 Configurar la actualización de varias estaciones....32
13.6 Configurar la actualización de una estación....33
14 Configurar Sophos Live Protection....35
14.1 Comprobar la configuración de la protección activa de Sophos....35
14.2 Activar o desactivar la protección activa de Sophos....35
15 Configurar el escaneado en acceso....36
15.1 Cambiar el método de intercepción del escaneado en acceso....36
15.2 Excluir archivos y directorios del escaneado....36
15.3 Excluir un sistema de archivos del escaneado....37
15.4 Escanear archivos comprimidos....38
15.5 Limpiar archivos infectados....38
16 configuración mediante archivos extra....40
16.1 Acerca de los archivos extra de configuración....40
16.2 Cómo usar los archivos extra de configuración....40
16.3 Actualizar los archivos extra de configuración....43
16.4 Capas de configuración....43
16.5 Comando de configuración savconfig....44
17 Solución de problemas....46
17.1 No se puede ejecutar un comando....46
17.2 No se aplican las exclusiones correctamente....46
17.3 No se encuentra la página man....47
17.4 Se queda sin espacio en disco....47
17.5 El escaneado en demanda es muy lento....48
17.6 El programa de copias de seguridad copia todos los archivos que han sido escaneados....49

17.7 No se limpian los virus....49
17.8 Fragmento de virus detectado....50
17.9 No se puede acceder a un disco....50
18 Apéndice: Códigos de retorno del escaneado en demanda....52
18.1 Códigos de retorno extendido....52
19 Apéndice: Configuración de la función de llamada a casa....54
20 Apéndice: Configuración de los reinicios en RMS....55
21 Glosario....56
22 Soporte técnico....58
23 Aviso legal....59

1 Acerca de esta guía

En esta guía encontrará información sobre cómo utilizar y configurar Sophos Anti-Virus para Linux.

Puede encontrar información sobre la instalación de las siguientes formas:

Para instalar Sophos Anti-Virus de modo que pueda administrarse con Sophos Central, inicie sesión en Sophos Central, vaya a la página Descargas y siga las instrucciones que encontrará allí.

Para instalar Sophos Anti-Virus de modo que pueda administrarse con Sophos Enterprise Console, consulte la *Guía de inicio de Sophos Enterprise Console para Linux y UNIX*.

Para instalar o desinstalar Sophos Anti-Virus no administrado en red o en ordenadores independientes Linux, consulte la *Guía de inicio de Sophos Anti-Virus para Linux.*

La documentación de Sophos se encuentra en http://www.sophos.com/es-es/support/documentation.aspx.

Importante: la información de configuración de esta guía también es aplicable a Sophos Linux Security.

2 Acerca de Sophos Anti-Virus para Linux

2.1 Función de Sophos Anti-Virus

Sophos Anti-Virus permite proteger ordenadores Linux contra virus, gusanos y troyanos. Además de amenazas para Linux , también puede detectar amenazas que afectan a otras plataformas. Esto se consigue mediante el escaneado.

2.2 Protección de Sophos Anti-Virus

El escaneado en acceso es la principal forma de protección contra virus. Siempre que abre, guarda o copia un archivo, Sophos Anti-Virus lo escanea y permite el acceso al mismo solo si es seguro.

Sophos Anti-Virus también le permite ejecutar un análisis en demanda para ofrecerle una protección adicional. Los escaneados en demanda son escaneados iniciados por el usuario. Puede escanear desde un solo archivo a todo el contenido del equipo con permiso de lectura: Los escaneados en demanda se pueden ejecutar de forma manual o programarse para que se ejecuten automáticamente.

2.3 Uso de Sophos Anti-Virus

Todas las tareas se realizan desde la línea de comandos.

Debe utilizar una sesión root para ejecutar todos los comandos menos **savscan**, que se emplea para el escaneado en demanda.

En este documento se asume que ha instalado Sophos Anti-Virus en la ubicación predeterminada, `/opt/sophos-av`. Los comandos y ejemplos descritos se refieren a esta ubicación.

2.4 Configurar Sophos Anti-Virus

Los métodos que se emplean para configurar Sophos Anti-Virus dependen de si se utiliza el software de administración de Sophos (Sophos Enterprise Console o Sophos Central) o no.

Equipos administrados por Enterprise Console o Sophos Central

Si sus equipos Linux se administran con Enterprise Console o Sophos Central, configure Sophos Anti-Virus del siguiente modo:

- Configure **el escaneado en acceso, el escaneado programado, las alertas, el registro y la actualización** de forma centralizada desde su consola de administración. Para obtener información, consulte la Ayuda en la consola de administración.

  Nota: ciertos parámetros de estas funciones no se pueden configurar de forma centralizada desde la consola de administración. Utilice la línea de comandos de Sophos Anti-Virus en cada estación Linux para configurar estos parámetros de forma local. La consola de administración los ignora.

Nota: si utiliza servidores Linux de 64 bits administrados mediante Sophos Central, consulte la Guía de inicio de Sophos Linux Security.

- El **escaneado en demanda** se configura desde la línea de comandos de Sophos Anti-Virus en cada ordenador Linux de forma local.

Equipos en red no administrados por Enterprise Console o Sophos Central

Si dispone de una red de equipos Linux no administrados por Enterprise Console o Sophos Central, configure Sophos Anti-Virus de la siguiente manera:

- El **escaneado en acceso, los escaneados programados, las alertas, el registro y la actualización** se configuran de forma centralizada mediante un archivo de configuración desde el que se actualizan los ordenadores. Consulte el Apéndice: Configuración mediante archivos extra en la página 40.
- El **escaneado en demanda** se configura desde la línea de comandos de Sophos Anti-Virus en cada estación.

Nota: no debería emplear esta configuración a menos que se le indique desde soporte técnico o si no es posible el uso de una consola de administración de Sophos. No es posible utilizar la consola de administración junto con la configuración mediante archivos extra.

Equipos en red no administrados por Enterprise Console o Sophos Central

Si dispone de un equipo Linux independiente *no* administrado por Enterprise Console o Sophos Central, configure todas las funciones de Sophos Anti-Virus desde la línea de comandos.

3 Escaneado en acceso

El escaneado en acceso es la principal forma de protección contra virus. Siempre que abre, guarda o copia un archivo, Sophos Anti-Virus lo escanea y permite el acceso al mismo solo si es seguro.

3.1 Comprobar que el escaneado en acceso se encuentra activo

- Para comprobar si el escaneado en acceso se encuentra activo, escriba:
  `/opt/sophos-av/bin/savdstatus`

3.2 Comprobar que el escaneado en acceso se inicia de forma automática al arrancar

Para realizar este procedimiento necesita derechos de root.

1. Compruebe que **`savd`** se inicia de forma automática al iniciarse el sistema:
   `chkconfig --list`

   Nota: si este comando no está disponible en su distribución Linux, utilice la herramienta correspondiente para comprobar los servicios que se inician de forma automática al iniciarse el sistema.

   Si el resultado muestra la entrada sav-protect con 2:on, 3:on, 4:on y 5:on, el escaneado en acceso se iniciará de forma automática al iniciarse el sistema.

   De lo contrario, escriba:

   `/opt/sophos-av/bin/savdctl enableOnBoot savd`

2. Compruebe que el escaneado en acceso se inicia de forma automática con **`savd`**:
   `/opt/sophos-av/bin/savconfig query EnableOnStart`

   Si el resultado es `true`, el escaneado en acceso se inicia de forma automática con **`savd`** al iniciarse el sistema.

   De lo contrario, escriba:

   `/opt/sophos-av/bin/savconfig set EnableOnStart true`

3.3 Iniciar el escaneado en acceso

Para iniciar el escaneado en acceso:

- Escriba:
  `/opt/sophos-av/bin/savdctl enable`

- Utilice la herramienta apropiada para iniciar el servicio sav-protect. Por ejemplo, escriba:
  `/etc/init.d/sav-protect start`

o

```
service sav-protect start
```

3.4 Detener el escaneado en acceso

Importante: si detiene el escaneado en acceso, Sophos Anti-Virus no escaneará los archivos que utiliza. Pondrá en riesgo ese equipo y los equipos conectados.

- Para detener el escaneado en acceso, escriba:
  `/opt/sophos-av/bin/savdctl disable`

4 Escaneado en demanda

Los *escaneados en demanda* son escaneados iniciados por el usuario. Puede escanear desde un solo archivo a todo el contenido del equipo con permiso de lectura: Los escaneados en demanda se pueden ejecutar de forma manual o programarse para que se ejecuten automáticamente.

Para programar un escaneado en demanda, utilice el comando **`crontab`**. Para más información, vea el artículo 12176 en la base de conocimiento de Sophos.

4.1 Ejecutar un escaneado en demanda

Para ejecutar un escaneado en demanda utilice el comando **`savscan`**.

4.1.1 Escanear el ordenador

- Para escanear el ordenador, escriba:
  `savscan /`

4.1.2 Escanear un directorio o archivo

- Para escanear un directorio o archivo, indique la ruta de acceso. Por ejemplo, escriba:
  `savscan /usr/mydirectory/myfile`

  Puede indicar más de un directorio o archivo a la vez.

4.1.3 Escanear el sistema de archivos

- Para escanear un sistema de archivos, indique su nombre. Por ejemplo, escriba:
  `savscan /home`

  Puede indicar más de un sistema de archivos a la vez.

4.1.4 Escanear el sector de arranque

Nota: sólo se aplica a Linux y FreeBSD.

Para escanear el sector de arranque, inicie la sesión como superusuario. De esta forma tendrá acceso a los dispositivos de disco.

Puede escanear el sector de arranque de unidades lógicas o físicas.

- Para escanear el sector de arranque de unidades lógicas, escriba:
  `savscan -bs=`*`unidad, unidad, ...`*

  donde *unidad* es el nombre de la unidad, por ejemplo`/dev/fd0` o `/dev/hda1`.

- Para escanear el sector de arranque de todas las unidades lógicas, escriba:
  `savscan -bs`

- Para escanear el sector de arranque maestro de todas las unidades físicas fijas del sistema, escriba:
  savscan -mbr

4.2 Configurar el escaneado en demanda

En esta sección, *ruta* hace referencia a la ruta de acceso a escanear.

Para ver la lista completa de opciones para el escaneado en demanda, escriba:

man savscan

4.2.1 Escanear todos los tipos de archivo

Por defecto, Sophos Anti-Virus escanea sólo archivos ejecutables. Para ver la lista de los tipos de archivo que Sophos Anti-Virus escanea por defecto, escriba **savscan -vv**.

- Para escanear todos los tipos de archivo, utilice la opción **-all**. Escriba:
  savscan *ruta* **-all**

  Nota: el escaneado de todos los tipos de archivo tardará más, puede afectar al rendimiento y causar falsos positivos.

4.2.2 Escanear un tipo de archivo

Por defecto, Sophos Anti-Virus escanea sólo archivos ejecutables. Para ver la lista de los tipos de archivo que Sophos Anti-Virus escanea por defecto, escriba **savscan -vv**.

- Para escanear un tipo de archivo, utilice la opción **-ext** e indique la extensión del tipo de archivo que desee escanear. Por ejemplo, para escanear archivos `.txt`, escriba:
  savscan *ruta* **-ext=txt**

- Para no escanear un tipo de archivo, utilice la opción **-ext** e indique la extensión del tipo de archivo que no desee escanear.

Nota: puede especificar más de un tipo de archivo separados por coma.

4.2.3 Escanear dentro de archivos comprimidos

Puede configurar Sophos Anti-Virus para escanear dentro de archivos comprimidos. Para ver la lista de archivos comprimidos, escriba **savscan -vv**.

Nota: el motor de detección de amenazas solo escanea los archivos comprimidos que tienen más de 8 GB (una vez descomprimidos). Esto se debe a que funciona con el formato comprimido POSIX ustar, que no admite archivos más grandes.

- Para escanear dentro de archivos comprimidos, utilice la opción **-archive**. Escriba:
  savscan *ruta* **-archive**

  Los archivos comprimidos anidados (por ejemplo, un archivo TAR dentro de un archivo ZIP) se escanean de forma recursiva.

  El escaneado se puede ralentizar si dispone de gran cantidad de archivos comprimidos complejos. Tenga esto en cuenta a la hora de programar el escaneado.

4.2.4 Escanear dentro de un tipo de archivo comprimido

Puede configurar Sophos Anti-Virus para escanear dentro de un tipo de archivo comprimido. Para ver la lista de archivos comprimidos, escriba **`savscan -vv`**.

Nota: el motor de detección de amenazas solo escanea los archivos comprimidos que tienen más de 8 GB (una vez descomprimidos). Esto se debe a que funciona con el formato comprimido POSIX ustar, que no admite archivos más grandes.

- Para escanear dentro de un tipo de archivo comprimido, utilice la opción que se muestra en la lista de tipos de archivos. Por ejemplo, para escanear archivos TAR y ZIP, escriba:
  `savscan` *`ruta`* **`-tar -zip`**

  Los archivos comprimidos anidados (por ejemplo, un archivo TAR dentro de un archivo ZIP) se escanean de forma recursiva.

  El escaneado se puede ralentizar si dispone de gran cantidad de archivos comprimidos complejos. Tenga esto en cuenta a la hora de programar el escaneado.

4.2.5 Escanear ordenadores remotos

Por defecto, Sophos Anti-Virus no escanea elementos en ordenadores remotos (es decir, no cruza puntos de montaje remotos).

- Para escanear ordenadores remotos, utilice **--no-stay-on-machine**. Escriba:
  `savscan` *`ruta`* **`--no-stay-on-machine`**

4.2.6 Desactivar el escaneado de elementos con enlace simbólico

Por defecto, Sophos Anti-Virus escaneará los elementos con enlace simbólico.

- Para desactivar este tipo de escaneado, utilice la opción **--no-follow-symlinks**. Escriba:
  `savscan` *`ruta`* **`--no-follow-symlinks`**

  Para evitar escanear elementos más de una vez, utilice la opción **--backtrack-protection**.

4.2.7 Escanear el sistema de archivos inicial

Sophos Anti-Virus se puede configurar para no escanear elementos fuera del sistema de archivos inicial (es decir, no cruzar puntos de montaje).

- Para escanear sólo el sistema de archivos inicial, utilice la opción **--stay-on-filesystem**. Escriba:
  `savscan` *`ruta`* **`--stay-on-filesystem`**

4.2.8 Excluir elementos del escaneado

Puede configurar Sophos Anti-Virus para excluir elementos (archivos, directorios o sistemas de archivos) del escaneado mediante la opción **-exclude**. Sophos Anti-Virus excluirá los elementos indicados. Por ejemplo, para escanear los elementos `fred` y `harry`, pero no `tom` ni `peter`, escriba:

```
savscan fred harry -exclude tom peter
```

Puede excluir directorios y archivos *dentro* de un directorio.. Por ejemplo, para escanear el directorio personal de Fred excluyendo el directorio `juegos` (y todo su contenido), escriba:

```
savscan /home/fred -exclude /home/fred/games
```

También puede configurar Sophos Anti-Virus para *incluir* elementos mediante la opción **-include**. Por ejemplo, para escanear los elementos `fred`, `harry` y `bill`, pero no `tom` ni `peter`, escriba:

```
savscan fred harry -exclude tom peter -include bill
```

4.2.9 Escanear archivos que UNIX define como ejecutables

Por defecto, Sophos Anti-Virus no escanea archivos que UNIX define como ejecutables.

- Para escanear los archivos que UNIX define como ejecutables, utilice la opción **--examine-x-bit**. Escriba:
  savscan *ruta* **--examine-x-bit**

  Sophos Anti-Virus también escaneará archivos con extensiones incluidas en la lista. Para ver la lista de extensiones, escriba **savscan -vv**.

5 Qué ocurre si se detecta algún virus

Por defecto, si Sophos Anti-Virus detecta un virus durante el escaneado en acceso o en demanda:

- Se crea una entrada en el registro del sistema y en el registro de Sophos Anti-Virus (consulte Ver el registro de Sophos Anti-Virus en la página 19).
- Se envía una alerta a Enterprise Console si el equipo se administra desde Enterprise Console.
- Se envía una alerta a root@localhost.

Por defecto, Sophos Anti-Virus también muestra una alerta, según se describe a continuación.

Escaneado en acceso

Sophos Anti-Virus deniega el acceso al archivo infectado y muestra una alerta de escritorio como la siguiente.

Si no se puede mostrar el mensaje, se mostrará una alerta en la línea de comandos.

Para más información sobre la limpieza de virus, consulte Limpiar virus en la página 16.

Escaneados en demanda

Sophos Anti-Virus muestra una alerta en la línea de comandos. El nombre del virus se muestra en una línea que comienza con >>> seguido de `Virus` o `Fragmento de virus`:

```
SAVScan virus detection utility
Version 4.69.0 [Linux/Intel]
Virus data version 4.69
Includes detection for 2871136 viruses, Trojans and worms
Copyright (c) 1989-2012 Sophos Limited. All rights reserved.
System time 13:43:32, System date 22 September 2012
IDE directory is: /opt/sophos-av/lib/sav
Using IDE file nyrate-d.ide
```

```
. . . . . .
Using IDE file injec-lz.ide
Quick Scanning
>>> Virus 'EICAR-AV-Test' found in file /usr/mydirectory/eicar.src
33 files scanned in 2 seconds.
1 virus was discovered.
1 file out of 33 was infected.
Please send infected samples to Sophos for analysis.
For advice consult www.sophos.com/es-es or email soporte@sophos.com
End of Scan.
```

Para más información sobre la limpieza de virus, consulte Limpiar virus en la página 16.

6 Limpiar virus

6.1 Información de limpieza

Cuando se notifica un virus, se puede obtener información y consejos de limpieza desde la web de Sophos.

Para obtener información de limpieza:

1. Visite la página de análisis de Sophos (http://www.sophos.com/es-es/threat-center/threat-analyses/viruses-and-spyware.aspx).
2. Haga una búsqueda con el término utilizado por Sophos Anti-Virus en la detección.

6.2 Poner en cuarentena los archivos infectados

Puede configurar el escaneado en demanda para colocar los archivos infectados en el área de cuarentena y evitar así el acceso. Para ello, se cambiará el propietario y los permisos del archivo.

Nota: si activa la desinfección (consulte Limpiar archivos infectados en la página 17) además de la cuarentena, Sophos Anti-Virus intentará primero la desinfección y, si no es posible, se utilizará la cuarentena.

En esta sección, *ruta* hace referencia a la ruta de acceso a escanear.

6.2.1 Hacer uso de la cuarentena

- Para hacer uso de la cuarentena, utilice la opción **--quarantine**. Escriba:
  `savscan` *`ruta`* **`--quarantine`**

6.2.2 Especificar el propietario y los permisos que se aplican

Por defecto, Sophos Anti-Virus cambia:

- El propietario de los archivos infectados al usuario que ejecuta Sophos Anti-Virus.
- El grupo al que pertenecen los archivos al grupo del usuario.
- Los permisos de los archivos a `-r--------` (0400).

Si lo desea, puede modificar el usuario, grupo y permisos que Sophos Anti-Virus aplica a los archivos infectados. Para hacerlo, utilice los siguientes parámetros:

```
uid=nnn
user=usuario
gid=nnn
group=grupo
mode=ppp
```

No puede especificar más de un parámetro de cada tipo. Por ejemplo, no puede especificar el **uid** y **user**.

Para cada parámetro que no especifique, se usará la configuración predeterminada, tal como se ha mostrado anteriormente.

Por ejemplo:

```
savscan fred --quarantine:user=virus,group=virus,mode=0400
```

modificará el propietario de los archivos infectados a "virus", el grupo a "virus" y los permisos a `-r---------`. Esto significa que el archivo es propiedad del usuario "virus" y pertenece al grupo "virus", pero sólo el usuario "virus" puede acceder al archivo (y solamente con permiso de lectura) Nadie podrá manipular este archivo aparte del usuario root.

Es posible que necesite ser un usuario especial o un "super usuario" para configurar el propietario y los permisos del archivo.

6.3 Limpiar archivos infectados

Puede configurar los escaneado en demanda para que limpien (desinfectar o borrar) archivos infectados. Las acciones llevadas a cabo por Sophos Anti-Virus se muestran en el resumen del escaneado y se anotan en el registro de Sophos Anti-Virus. Por defecto, la limpieza se encuentra desactivada.

En esta sección, *ruta* hace referencia a la ruta de acceso a escanear.

6.3.1 Desinfectar un archivo

- Para desinfectar un archivo, utilice la opción **-di**. Escriba:
  savscan *ruta* **-di**

  Sophos Anti-Virus pedirá confirmación antes de desinfectar el sector de arranque.

  Nota: la desinfección de documentos infectados no puede deshacer el daño que el virus haya podido causar. (Vea Información de limpieza en la página 16 para obtener desde la web de Sophos información sobre cada virus.)

6.3.2 Desinfectar todos los archivos

- Para desinfectar todos los archivos infectados, escriba:
  savscan / -di

  Sophos Anti-Virus pedirá confirmación antes de desinfectar el sector de arranque.

  Nota: la desinfección de documentos infectados no puede deshacer el daño que el virus haya podido causar. (Vea Información de limpieza en la página 16 para obtener desde la web de Sophos información sobre cada virus.)

6.3.3 Eliminar un archivo infectado

- Para eliminar un archivo infectado, utilice la opción **-remove**. Escriba:
  savscan *ruta* **-remove**

  Sophos Anti-Virus pedirá confirmación antes de eliminar el archivo.

6.3.4 Eliminar todos los archivos infectados

- Para eliminar todos los archivos infectados, escriba:
  `savscan / -remove`

  Sophos Anti-Virus pedirá confirmación antes de eliminar el archivo.

6.3.5 Desinfectar el sector de arranque

Nota: sólo se aplica a Linux y FreeBSD.

- Para desinfectar el sector de arranque, utilice la opción de desinfección **-di** y la opción del sector de arranque **-bs**. Por ejemplo, escriba:
  `savscan -bs=/dev/fd0 -di`

  donde **`/dev/fd0`** es la unidad con el sector de arranque infectado.

  Sophos Anti-Virus pedirá confirmación antes de desinfectar el sector de arranque.

6.4 Recuperación tras una infección

La recuperación tras el ataque de un virus depende del tipo de infección. Algunos virus no provocan efectos secundarios, mientras que otros pueden destruir todos los datos del disco duro.

Algunos virus realizan pequeños cambios de forma gradual en documentos. Este tipo de daño es difícil de detectar y corregir. Es importante que lea la descripción ofrecida sobre cada virus en la web de Sophos y que compruebe sus documentos detenidamente tras la desinfección.

Siempre debe disponer de copias de seguridad. Si no dispone de copias de seguridad, comience a crearlas para minimizar el impacto de una posible infección.

A veces es posible recuperar datos en discos dañados por un virus. Sophos proporciona herramientas para reparar el daño creado por ciertos virus. Póngase en contacto con el soporte técnico de Sophos si necesita ayuda.

7 Ver el registro de Sophos Anti-Virus

Sophos Anti-Virus utiliza el registro de Sophos Anti-Virus y syslog para detallar su actividad. En el registro de Sophos Anti-Virus también se incluyen errores y la detección de virus.

- Para ver el registro de Sophos Anti-Virus, utilice el comando **`savlog`**. El comando cuenta con diferentes opciones.

  Por ejemplo, para mostrar los mensajes de las últimas 24 horas en el registro de Sophos Anti-Virus con la fecha en formato UTC/ISO 8601, escriba:

  ```
  /opt/sophos-av/bin/savlog --today --utc
  ```

- Para ver la lista completa de opciones de **`savlog`**, escriba:

  ```
  man savlog
  ```

8 Actualizar Sophos Anti-Virus de forma inmediata

Si tiene activada la opción de actualización automática, Sophos Anti-Virus se actualiza a intervalos regulares. También es posible actualizar las estaciones de forma inmediata.

- Para actualizar Sophos Anti-Virus de forma inmediata, en el equipo que desee realizar la actualización, escriba:
  `/opt/sophos-av/bin/savupdate`

Nota: también puede actualizar las estaciones de forma inmediata desde Sophos Enterprise Console.

9 Acerca de la compatibilidad del kernel

Nota: esta sección sólo se aplica si utiliza el módulo Talpa para el escaneado en acceso. Para más información, consulte Cambiar el método de intercepción del escaneado en acceso en la página 36.

9.1 Acerca de la compatibilidad con kernel nuevos

Cuando un fabricante de Linux compatible con Sophos Anti-Virus actualiza el kernel, Sophos publica el modulo Talpa compatible con dicho kernel. Si aplica la actualización del kernel antes de disponer del módulo Talpa correspondiente, Sophos Anti-Virus iniciará la compilación automática del módulo. Si el proceso falla, Sophos Anti-Virus intentará utilizar Fanotify para el escaneado en acceso. Si Fanotify no se encuentra disponible, el escaneado en acceso se detendrá con un error.

Para evitar este problema, asegúrese de que dispone del módulo Talpa correspondiente antes de aplicar la actualización del kernel. En el artículo 14377 de la base de conocimiento de Sophos encontrará la lista de distribuciones Linux compatibles (http://www.sophos.com/es-es/support/knowledgebase/14377.aspx). Las actualizaciones del módulo Talpa se muestran cuando están disponibles. Si tiene activada la opción de actualización automática, Sophos Anti-Virus se actualiza a intervalos regulares. Si lo desea, puede actualizar Sophos Anti-Virus de forma inmediata con el siguiente comando:

```
/opt/sophos-av/bin/savupdate
```

A continuación podrá aplicar la actualización del kernel.

9.2 Acerca de la compatibilidad con kernel personalizados

Si dispone de un kernel personalizado, en este manual no se describe cómo configurar la actualización para mantener la compatibilidad. Consulte el artículo 13503 de la base de conocimiento de Sophos (http://www.sophos.com/es-es/support/knowledgebase/13503.aspx).

10 Configurar escaneados programados

Sophos Anti-Virus programar los escaneados.

Nota: los escaneados programados desde Enterprise Console tienen el prefijo “SEC:” y sólo se pueden actualizar o eliminar desde Enterprise Console.

10.1 Añadir un escaneado programado desde un archivo

1. Para utilizar una plantilla de escaneado como guía, abra `/opt/sophos-av/doc/namedscan.example.en`.

   Para empezar de cero necesitará un archivo de texto vacío.

2. Indique los elementos a escanear, las horas de escaneado y cualquier otra opción utilizando los parámetros que aparecen en la plantilla.

   Para programar el escaneado debe especificar al menos un día y una hora.

3. Guarde el archivo, sin sobrescribir la plantilla.
4. Añada el escaneado programado a Sophos Anti-Virus mediante el comando **`savconfig`** con la operación **add** y el parámetro **NamedScans**. Indique el nombre del escaneado y la ruta al archivo con la configuración.

   Por ejemplo, para añadir el escaneado Diario, que se encuentra en `/home/fred/EscanDiario`, escriba:

   `/opt/sophos-av/bin/savconfig add NamedScans Diario /home/fred/EscanDiario`

10.2 Añadir un escaneado programado de forma manual

1. Añada el escaneado programado a Sophos Anti-Virus mediante el comando **`savconfig`** con la operación **add** y el parámetro **NamedScans**. Indique el nombre del escaneado y añada un guión para establecer que la configuración se establecerá de forma manual.

   Por ejemplo, para añadir el escaneado Diario, escriba:

   `/opt/sophos-av/bin/savconfig add NamedScans Diario -`

   Al pulsar Intro, Sophos Anti-Virus pedirá la configuración del escaneado.

2. Indique los elementos a escanear, las horas de escaneado y cualquier otra opción utilizando los parámetros que aparecen en la plantilla `/opt/sophos-av/doc/namedscan.example.en` Tras introducir cada parámetro y su valor, pulse Intro.

   Para programar el escaneado debe especificar al menos un día y una hora.

3. Para terminar, pulse CTRL+D.

10.3 Exportar un escaneado programado a un archivo

- Para exportar un escaneado programado desde Sophos Anti-Virus a un archivo, utilice el comando **savconfig** con la operación **query** y el parámetro **NamedScans**. Debe indicar el nombre del escaneado y la ruta del archivo que desea crear.

  Por ejemplo, para exportar el escaneado Diario al archivo `/home/fred/EscanDiario`, escriba::

  ```
  /opt/sophos-av/bin/savconfig query NamedScans Diario
  /home/fred/EscanDiario
  ```

10.4 Exportar los nombres de todos los escaneados programados a un archivo

- Para exportar los nombres de todos los escaneados programados (incluyendo los creados en Enterprise Console) desde Sophos Anti-Virus a un archivo, utilice el comando **savconfig** con la operación **query** y el parámetro **NamedScans**. Debe indicar la ruta del archivo que desea crear.

  Por ejemplo, para exportar los nombres de todos los escaneados programados al archivo `/home/fred/EscanTodos`, escriba::

  ```
  /opt/sophos-av/bin/savconfig query NamedScans >
  /home/fred/EscanTodos
  ```

  Nota: `SEC:FullSystemScan` es un escaneado que siempre se encuentra presente si el equipo se encuentra administrado desde Enterprise Console.

10.5 Exportar un escaneado programado a la salida estándar

- Para exportar un escaneado programado desde Sophos Anti-Virus a la salida estándar, utilice el comando **savconfig** con la operación **query** y el parámetro **NamedScans**. Debe especificar el nombre del escaneado.

  Por ejemplo, para exportar el escaneado Diario, escriba:

  ```
  /opt/sophos-av/bin/savconfig query NamedScans Diario
  ```

10.6 Exportar los nombres de todos los escaneados programados a la salida estándar

- Para exportar los nombres de todos los escaneados programados (incluyendo los creados en Enterprise Console) desde Sophos Anti-Virus a la salida estándar, utilice el comando **savconfig** con la operación **query** y el parámetro **NamedScans**.

  Por ejemplo, para exportar los nombres de todos los escaneados programados a la salida estándar, escriba::

  ```
  /opt/sophos-av/bin/savconfig query NamedScans
  ```

Nota: `SEC:FullSystemScan` es un escaneado que siempre se encuentra presente si el equipo se encuentra administrado desde Enterprise Console.

10.7 Actualizar un escaneado programado desde un archivo

Nota: no es posible actualizar escaneados programados creados desde Enterprise Console.

1. Abra el archivo con la configuración del escaneado programado que desea actualizar.

   Si no dispone del archivo de configuración del escaneado, puede crearlo como se describe en Exportar un escaneado programado a un archivo en la página 23.

2. Realice los cambios necesarios utilizando los parámetros indicados en la plantilla de escaneado: `/opt/sophos-av/doc/namedscan.example.en`. Debe definir el escaneado en su totalidad, no sólo especificar los cambios.
3. Guarde el archivo.
4. Actualice el escaneado programado en Sophos Anti-Virus mediante el comando **`savconfig`** con la operación **update** y el parámetro **NamedScans**. Indique el nombre del escaneado y la ruta al archivo con la configuración.

   Por ejemplo, para actualizar el escaneado Diario, que se encuentra en `/home/fred/EscanDiario`, escriba:

   `/opt/sophos-av/bin/savconfig update NamedScans Diario /home/fred/EscanDiario`

10.8 Actualizar un escaneado programado de forma manual

Nota: no es posible actualizar escaneados programados creados desde Enterprise Console.

1. Actualice el escaneado programado en Sophos Anti-Virus mediante el comando **`savconfig`** con la operación **update** y el parámetro **NamedScans**. Indique el nombre del escaneado y añada un guión para establecer que la configuración se establecerá de forma manual.

   Por ejemplo, para actualizar el escaneado Diario, escriba:

   `/opt/sophos-av/bin/savconfig update NamedScans Diario -`

   Al pulsar Intro, Sophos Anti-Virus pedirá la configuración del escaneado.

2. Indique los elementos a escanear, las horas de escaneado y cualquier otra opción utilizando los parámetros que aparecen en la plantilla `/opt/sophos-av/doc/namedscan.example.en` Tras introducir cada parámetro y su valor, pulse Intro. Debe definir el escaneado en su totalidad, no sólo especificar los cambios.

   Para programar el escaneado debe especificar al menos un día y una hora.

3. Para terminar, pulse CTRL+D.

10.9 Ver el registro de un escaneado programado

- Para ver el registro de un escaneado programado, utilice el comando **`savlog`** con la opción **namedscan**. Debe especificar el nombre del escaneado.

  Por ejemplo, para ver el registro del escaneado Diario, escriba:

```
/opt/sophos-av/bin/savlog --namedscan=Diario
```

10.10 Eliminar un escaneado programado

Nota: no es posible eliminar escaneados programados creados desde Enterprise Console.

- Para eliminar un escaneado programado desde Sophos Anti-Virus, utilice el comando **savconfig** con la operación **remove** y el parámetro **NamedScans**. Debe especificar el nombre del escaneado.

  Por ejemplo, para eliminar el escaneado Diario, escriba:

  ```
  /opt/sophos-av/bin/savconfig remove NamedScans Diario
  ```

10.11 Eliminar todos los escaneados programados

Nota: no es posible eliminar escaneados programados creados desde Enterprise Console.

- Para eliminar todos los escaneados programados desde Sophos Anti-Virus, escriba: **/opt/sophos-av/bin/savconfig delete NamedScans**

11 Configurar alertas

Nota: si modifica la configuración de un ordenador en la red, puede perder dicha configuración al actualizarse desde Enterprise Console o mediante un archivo de configuración.

Puede configurar Sophos Anti-Virus para enviar alertas cuando se detecte algún virus o se produzca algún error. Las alertas se pueden hacer llegar al usuario mediante:

- Mensajes de escritorio (sólo escaneado en acceso)
- Línea de comandos (sólo escaneado en acceso)
- Email (escaneado en acceso y escaneado en demanda)

Los mensajes de escritorio y de la línea de comandos se muestran en el idioma del sistema. Los mensajes de alerta se pueden enviar en inglés o japonés.

11.1 Configurar alertas de escritorio

11.1.1 Desactivar las alertas de escritorio

Por defecto, las alertas de escritorio se encuentran activadas.

- Para desactivar las alertas de escritorio, escriba:
  `/opt/sophos-av/bin/savconfig set UIpopupNotification disabled`
- Para desactivar las alertas de escritorio y las de línea de comandos, escriba:
  `/opt/sophos-av/bin/savconfig set UINotifier disabled`

11.1.2 Mensaje personalizado

Puede especificar un mensaje personalizado que se añadirá a todas las alertas de la línea de comandos y a las alertas de escritorio.

Recuerde: el principal mensaje de alerta puede mostrarse en distintos idiomas (en función de la configuración del sistema), pero el texto personalizado seguirá estando en el idioma que haya utilizado al especificarlo.

- Para especificar el mensaje, utilice el parámetro **UIContactMessage**. Por ejemplo, escriba:
  `/opt/sophos-av/bin/savconfig set UIContactMessage 'Contact IT'`

11.2 Configurar alertas en la línea de comandos

11.2.1 Desactivar las alertas de la línea de comandos

Por defecto, las alertas de la línea de comandos se encuentran activadas.

- Para desactivar las alertas de la línea de comandos, escriba:
  `/opt/sophos-av/bin/savconfig set UIttyNotification disabled`

- Para desactivar las alertas de escritorio y las de línea de comandos, escriba:
  `/opt/sophos-av/bin/savconfig set UINotifier disabled`

11.2.2 Mensaje personalizado

Puede especificar un mensaje personalizado que se añadirá a todas las alertas de la línea de comandos y a las alertas de escritorio.

👉 **Recuerde:** el principal mensaje de alerta puede mostrarse en distintos idiomas (en función de la configuración del sistema), pero el texto personalizado seguirá estando en el idioma que haya utilizado al especificarlo.

- Para especificar el mensaje, utilice el parámetro **UIContactMessage**. Por ejemplo, escriba:
  `/opt/sophos-av/bin/savconfig set UIContactMessage 'Contact IT'`

11.3 Configurar alertas por email

11.3.1 Desactivar las alertas por email

Por defecto, las alertas por email se encuentran activadas.

- Para desactivar las alertas por email, escriba:
  `/opt/sophos-av/bin/savconfig set EmailNotifier disabled`

11.3.2 Especificar el nombre o la dirección IP del servidor SMTP

La configuración predeterminada del servidor SMTP es localhost:25.

- Para especificar el nombre o la dirección IP del servidor SMTP, utilice el parámetro **EmailServer**. Por ejemplo, escriba:
  `/opt/sophos-av/bin/savconfig set EmailServer 171.17.31.184`

11.3.3 Especificar el idioma

El idioma predeterminado del sistema de alerta es inglés.

- Para especificar el idioma del sistema de alerta, utilice el parámetro **EmailLanguage**. De momento, los únicos valores disponibles son **`English`** y **`Japanese`**. Por ejemplo, escriba:
  `/opt/sophos-av/bin/savconfig set EmailLanguage Japanese`

  Nota: la selección de idioma sólo se aplica al mensaje de alerta, no a los mensajes personalizados que se pueden incluir.

11.3.4 Especificar los destinatarios

Por defecto, las alertas por email se envían a root@localhost.

- Para añadir destinatarios, utilice el parámetro **Email** con la operación **add**. Por ejemplo, escriba:
  `/opt/sophos-av/bin/savconfig add Email admin@localhost`

Nota: puede especificar más de un destinatario. Deje un espacio entre cada destinatario.

- Para eliminar destinatarios, utilice el parámetro **Email** con la operación **remove**. Por ejemplo, escriba:
  `/opt/sophos-av/bin/savconfig remove Email admin@localhost`

  Importante: no puede eliminar **root@localhost** con este comando. Para hacerlo, debe sobrescribir toda la lista con el siguiente comando:
  `/opt/sophos-av/bin/savconfig set Email <direcciones de correo electrónico>`

11.3.5 Especificar la dirección remitente

Por defecto, el remitente de las alertas es root@localhost.

- Para especificar la dirección remitente, utilice el parámetro **EmailSender**. Por ejemplo, escriba:
  `/opt/sophos-av/bin/savconfig set EmailSender admin@localhost`

11.3.6 Especificar la dirección de respuesta

- Para especificar la dirección de respuesta, utilice el parámetro **EmailReplyTo**. Por ejemplo, escriba:
  `/opt/sophos-av/bin/savconfig set EmailReplyTo admin@localhost`

11.3.7 Qué ocurre si se detecta algún virus en el escaneado en acceso

Por defecto, Sophos Anti-Virus envía una alerta por email si se detecta algún virus en el escaneado en acceso. Se incluye un mensaje en inglés personalizado con cada alerta, además del mensaje de alerta en sí. Puede cambiar el texto de este mensaje personalizado, pero no se traduce.

- Para desactivar el envío de alertas por email cuando se detectan virus en el escaneado en acceso, escriba:
  `/opt/sophos-av/bin/savconfig set SendThreatEmail disabled`

- Para especificar el mensaje, utilice el parámetro **ThreatMessage**. Por ejemplo, escriba:
  `/opt/sophos-av/bin/savconfig set ThreatMessage 'Contact IT'`

11.3.8 Especificar el comportamiento ante un error del escaneado en acceso

Por defecto, Sophos Anti-Virus envía una alerta por email si se produce algún error del escaneado en acceso. Se incluye un mensaje en inglés personalizado con cada alerta, además del mensaje de alerta en sí. Puede cambiar el texto de este mensaje personalizado, pero no se traduce.

- Para desactivar el envío de alertas por email cuando se produce un error del escaneado en acceso, escriba:

  `/opt/sophos-av/bin/savconfig set SendErrorEmail disabled`

- Para especificar el mensaje, utilice el parámetro **ScanErrorMessage**. Por ejemplo, escriba:
  `/opt/sophos-av/bin/savconfig set ScanErrorMessage 'Contact IT'`

11.3.9 Desactivar las alertas por email para el escaneado en demanda

Por defecto, Sophos Anti-Virus envía un email con el resumen de los escaneados en demanda sólo si se detecta algún virus.

- Para desactivar este tipo de mensajes, escriba:
  `/opt/sophos-av/bin/savconfig set EmailDemandSummaryIfThreat disabled`

11.3.10 Especificar el comportamiento ante un evento del registro

Por defecto, Sophos Anti-Virus envía un mensaje de alerta cuando se guarda un evento en el registro de Sophos Anti-Virus. Un mensaje predefinido se incluye en cada alerta junto con el mensaje de la alerta. Este mensaje se puede modificar.

- Para especificar el mensaje, utilice el parámetro **LogMessage**. Por ejemplo, escriba:
  `/opt/sophos-av/bin/savconfig set LogMessage 'Póngase en contacto con el departamento informático'`

12 Configurar registro

Nota: si modifica la configuración de un ordenador en la red, puede perder dicha configuración al actualizarse desde Enterprise Console o mediante un archivo de configuración.

Por defecto, la actividad del escaneado se guarda en el registro de Sophos Anti-Virus: `/opt/sophos-av/log/savd.log`. Al alcanzar el tamaño de 1 MB, se crea una copia de seguridad y se inicia un nuevo archivo de registro.

- Para ver el número de archivos que se guardan, escriba:
  `/opt/sophos-av/bin/savconfig -s query LogMaxSizeMB`

- Para especificar el tamaño máximo del registro, utilice el parámetro **LogMaxSizeMB**. Por ejemplo, para establecer el límite del registro en 50, escriba:
  `/opt/sophos-av/bin/savconfig set LogMaxSizeMB 50`

13 Configurar la actualización

Importante: si administra Sophos Anti-Virus mediante Sophos Enterprise Console, debe configurar la actualización desde Enterprise Console. Para más información, consulte la Ayuda de Enterprise Console.

13.1 Conceptos básicos

Servidor de actualización

Un *servidor de actualización* es un ordenador en el que ha instalado Sophos Anti-Virus para Linux y que actúa como fuente de actualización para otros ordenadores. Estos ordenadores pueden ser estaciones u otros servidores de actualización, según el modo en el que haya distribuido Sophos Anti-Virus en la red.

Estación

Una *estación* es un ordenador en el que ha instalado Sophos Anti-Virus y que no actúa como fuente de actualización para otros ordenadores.

Fuente primaria de actualización

La *fuente primaria de actualización* es la ubicación desde la que se actualizan las estaciones. Puede que necesite credenciales de acceso.

Fuente secundaria de actualización

La *fuente secundaria de actualización* es la ubicación de actualización alternativa que se utiliza cuando la fuente primaria no está disponible. Puede que necesite credenciales de acceso.

13.2 Comando de configuración savsetup

`savsetup` es el comando que se usa para configurar los parámetros de actualización. Sólo debe utilizarse para tareas específicas, como se describe en las siguientes secciones.

Aunque permite acceder sólo a algunos de los parámetros que se pueden configurar con **`savconfig`**, es más fácil de usar; bastará con seleccionar o escribir los valores deseados cuando se le pida. Para iniciar **`savsetup`**, escriba:

```
/opt/sophos-av/bin/savsetup
```

13.3 Ver la configuración de actualización en un ordenador

1. En el ordenador en el que desea ver la configuración, escriba:
   `/opt/sophos-av/bin/savsetup`

   `savsetup` le preguntará qué desea hacer.

2. Seleccione **Auto-updating configuration**.

   savsetup le preguntará qué desea hacer.

3. Seleccione **Display update configuration** para mostrar la configuración de actualización.

13.4 Configurar un servidor de actualización

Puede utilizar cualquier instalación independiente de Sophos Anti-Virus para Linux como un servidor de actualización para otros ordenadores en la red.

1. En el servidor de actualización, escriba:
   /opt/sophos-av/bin/savsetup

   savsetup le preguntará qué desea hacer.

2. Seleccione una opción y siga las instrucciones.

   Al configurar la actualización, si se actualiza desde Sophos, introduzca el nombre de usuario y la contraseña que se incluye en su licencia. Si se actualiza desde un servidor de actualización, utilice la dirección HTTP o ruta UNC, según su servidor.

3. Para ofrecer actualizaciones de Sophos Anti-Virus a otras estaciones:

   a) Configure el servidor de actualización para que descargue archivos adicionales que clientes de actualización podrían necesitar. En el servidor de actualización, escriba:
   /opt/sophos-av/bin/savconfig set PrimaryUpdateAllDistros true

   b) Fuerce la actualización del servidor de actualización para garantizar que los archivos adicionales se hayan descargado. En el servidor de actualización, escriba:
   /opt/sophos-av/bin/savupdate --force

   c) Copie el directorio de caché local (/opt/sophos-av/update/cache/) a otro directorio.

   Puede automatizar esta tarea mediante un script.

   d) Comparta este directorio con el resto de estaciones, por ejemplo mediante HTTP, SMB o NFS.

   Esta es la ubicación del directorio de instalación central (CID) para el resto de estaciones.

13.5 Configurar la actualización de varias estaciones

A continuación se describe cómo modificar los parámetros de actualización en los archivos extra de configuración. Las estaciones descargan esta configuración durante las actualizaciones.

En esta sección se asume que ya ha creado los archivos extra de configuración. Si no sea crea, consulte el Apéndice: Configuración mediante archivos extra en la página 40.

Nota: aquí se describe cómo configurar la actualización de varias estaciones desde la fuente de actualización *primaria*. Utilice el mismo procedimiento para la fuente de actualización *secundaria* sustituyendo *Primary* por *Secondary*. Por ejemplo, en vez de **PrimaryUpdateSourcePath**, utilice **SecondaryUpdateSourcePath**.

Para configurar la actualización de varias estaciones:

1. En el equipo donde almacena los archivos extra de configuración, establezca la fuente de actualización desde **sophos:** o desde el directorio de instalación central (CID) mediante el parámetro **PrimaryUpdateSourcePath**.

   Para la actualización desde el CID, utilice la dirección HTTP o ruta UNC, según su servidor. Por ejemplo, escriba:

   /opt/sophos-av/bin/savconfig -f *archivo-conf-prueba* **-c set PrimaryUpdateSourcePath 'http://www.mywebcid.com/cid'**

   Para la actualización desde **sophos:**, escriba:

   /opt/sophos-av/bin/savconfig -f *archivo-conf-prueba* **-c set PrimaryUpdateSourcePath 'sophos:'**

2. Si se requiere autenticación, indique el nombre de usuario y la contraseña con los parámetros **PrimaryUpdateUsername** y **PrimaryUpdatePassword**, respectivamente. Por ejemplo, escriba:
   /opt/sophos-av/bin/savconfig -f *archivo-conf-prueba* **-c set PrimaryUpdateUsername 'fred'**

   /opt/sophos-av/bin/savconfig -f *archivo-conf-prueba* **-c set PrimaryUpdatePassword 'j23rjjfwj'**

3. Si accede al servidor de actualización a través de un proxy, debe indicar su dirección y las credenciales de acceso mediante los parámetros **PrimaryUpdateProxyAddress**, **PrimaryUpdateProxyUsername** y **PrimaryUpdateProxyPassword**. Por ejemplo, escriba:
   /opt/sophos-av/bin/savconfig -f *archivo-conf-prueba* **-c set PrimaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'**

   /opt/sophos-av/bin/savconfig -f *archivo-conf-prueba* **-c set PrimaryUpdateProxyUsername 'penelope'**

   /opt/sophos-av/bin/savconfig -f *archivo-conf-prueba* **-c set PrimaryUpdateProxyPassword 'fj202jrjf'**

4. Tras establecer los parámetros en el archivo de configuración de prueba, aplique los cambios en el archivo de configuración mediante el comando **addextra**. La sintaxis es la siguiente:

   /opt/sophos-av/update/addextra
   offline-config-file-pathlive-config-file-path
   --signing-key=*signing-key-file-path*
   --signing-certificate=*signing-certificate-file-path*

   Por ejemplo:

   /opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg /var/www/extrafiles/ --signing-key= /root/certificates/extrafiles-signing.key --signing-certificate=/root/certificates/extrafiles-signing.crt

La nueva configuración se aplicará en las estaciones la próxima vez que se actualicen.

13.6 Configurar la actualización de una estación

1. En el ordenador que desea configurar, escriba:
   /opt/sophos-av/bin/savsetup

   savsetup le preguntará qué desea hacer.

2. Seleccione una opción y siga las instrucciones.

   Al configurar la actualización, si se actualiza desde Sophos, introduzca el nombre de usuario y la contraseña que se incluye en su licencia. Si está realizando la actualización desde un CID, puede especificar una dirección HTTP o una ruta UNC, en función de cómo haya configurado el servidor de actualización.

14 Configurar Sophos Live Protection

Nota: si modifica la configuración de un ordenador en la red, puede perder dicha configuración al actualizarse desde Enterprise Console o mediante un archivo de configuración.

La protección activa de Sophos determina si los archivos sospechosos suponen una amenaza y, en caso afirmativo, se llevan a cabo de inmediato las acciones especificadas en la configuración para la limpieza de virus de Sophos Anti-Virus.

La protección activa mejora de forma significativa la detección de nuevas amenazas sin el riesgo de falsos positivos. La comprobación se realiza con los datos de los programas maliciosos más recientes. Cuando se detecte una nueva amenaza, Sophos enviará la actualización de forma inmediata.

Si en un escaneado se detecta algún archivo sospechoso pero no se consigue su identificación con los datos de detección en dicho ordenador, se enviarán a Sophos ciertos datos del archivo (como la suma de verificación y otros atributos) para su verificación.

Para la comprobación se utilizan las bases de datos de SophosLabs. La respuesta se envía al ordenador, donde se actualiza de forma automática el estado del archivo afectado.

14.1 Comprobar la configuración de la protección activa de Sophos

La protección activa de Sophos se encuentra activada por defecto en cada instalación nueva de Sophos Anti-Virus. Se encontrará desactivada si ha realizado una actualización desde una versión anterior de Sophos Anti-Virus.

- Para comprobar la configuración de la protección activa, escriba:
  `/opt/sophos-av/bin/savconfig query LiveProtection`

14.2 Activar o desactivar la protección activa de Sophos

- Para activar la protección activa, escriba:

  `/opt/sophos-av/bin/savconfig set LiveProtection true`

- Para desactivar la protección activa, escriba:

  `/opt/sophos-av/bin/savconfig set LiveProtection false`

15 Configurar el escaneado en acceso

Nota: si modifica la configuración de un ordenador en la red, puede perder dicha configuración al actualizarse desde Enterprise Console o mediante un archivo de configuración.

15.1 Cambiar el método de intercepción del escaneado en acceso

Si se actualiza a una versión del kernel de Linux que no es compatible con Talpa, puede utilizar Fanotify para la intercepción de archivos.

Importante: el uso de Fanotify en Sophos Anti-Virus se encuentra en fase beta.

- Para utilizar Fanotify, escriba:
  `/opt/sophos-av/bin/savconfig set DisableFanotify false`

15.2 Excluir archivos y directorios del escaneado

Puede excluir archivos y directorios del escaneado de dos formas:

- Especificando el nombre del archivo o el directorio
- Mediante caracteres comodín

Si desea excluir archivos o directorios no UTF-8, consulte Especificar la codificación de caracteres de nombres de directorios y archivos en la página 37.

15.2.1 Especificar el nombre del archivo o el directorio

Nota: si modifica la configuración de un ordenador en la red, puede perder dicha configuración al actualizarse desde Enterprise Console o mediante un archivo de configuración.

- Para excluir algún archivo o directorio, utilice el parámetro **ExcludeFilePaths** con la operación **add**. Especifique un directorio con una barra inclinada al final. Por ejemplo, para añadir el archivo `/tmp/informe` a la lista de exclusiones, escriba:
  `/opt/sophos-av/bin/savconfig add ExcludeFilePaths /tmp/informe`

  Para añadir el directorio `/tmp/informe/` a la lista de exclusiones, escriba:

  `/opt/sophos-av/bin/savconfig add ExcludeFilePaths /tmp/informe/`

- Para eliminar una exclusión de la lista, utilice el parámetro **ExcludeFilePaths** con la operación **remove**. Por ejemplo, escriba:

  `/opt/sophos-av/bin/savconfig remove ExcludeFilePaths /tmp/report`

15.2.2 Utilizar caracteres comodín

Nota: si modifica la configuración de un ordenador en la red, puede perder dicha configuración al actualizarse desde Enterprise Console o mediante un archivo de configuración.

- Para excluir algún archivo o directorio con caracteres comodín, utilice el parámetro **ExcludeFileOnGlob** con la operación **add**. Los caracteres comodín permitidos son *****, que representa cualquier número de caracteres, y **?**, que represente un carácter. Por ejemplo, para excluir todos los archivos de texto en el directorio `/tmp/`, escriba:
  `/opt/sophos-av/bin/savconfig add ExcludeFileOnGlob '/tmp/*.txt'`

  Nota: si utiliza **ExcludeFileOnGlob** para excluir **un directorio**, debe añadir el comodín * al final de la ruta. Por ejemplo:

  `/opt/sophos-av/bin/savconfig add ExcludeFileOnGlob '/tmp/report/*'`

- Si no utiliza comillas, Linux aplica la expresión y pasa la lista de archivos a Sophos Anti-Virus. Esto puede ser útil para excluir los archivos existentes, pero no los que se añadan en el futuro. Por ejemplo, para excluir sólo los archivos actuales de texto en el directorio `/tmp`, escriba:
  `/opt/sophos-av/bin/savconfig add ExcludeFileOnGlob /tmp/*.txt`

- Para eliminar una exclusión de la lista, utilice el parámetro **ExcludeFileOnGlob** con la operación **remove**. Por ejemplo, escriba:
  `/opt/sophos-av/bin/savconfig remove ExcludeFileOnGlob '/tmp/notes.txt'`

15.2.3 Especificar la codificación de caracteres de nombres de directorios y archivos

Linux permite permite el uso de diferentes codificaciones para los nombres de directorios y archivos (por ejemplo, UTF-8, EUC_jp). Sin embargo, Sophos Anti-Virus almacena las exclusiones en UTF-8. Si desea excluir directorios o archivos cuya codificación no es UTF-8, debe utilizar el parámetro **ExclusionEncodings**. De esta forma, las exclusiones se aplicarán con la codificación especificada. Esto se aplica a las exclusiones definidas mediante los parámetros **ExcludeFilePaths** y **ExcludeFileOnGlob**. Por defecto, se emplean las codificaciones UTF-8, EUC_jp e ISO-8859-1 (Latin-1).

Por ejemplo, si desea excluir directorios y archivos con nombres en codificación EUC_cn, debe especificar las exclusiones mediante **ExcludeFilePaths** o **ExcludeFileOnGlob**. A continuación, añada EUC_cn a la lista de codificaciones:

`/opt/sophos-av/bin/savconfig add ExclusionEncodings EUC_cn`

Ahora Sophos Anti-Virus empleará las codificaciones UTF-8, EUC_jp, ISO-8859-1 (Latin-1) y EUC_cn para determinar las exclusiones. Las exclusiones se aplicarán durante el escaneado.

15.3 Excluir un sistema de archivos del escaneado

Por defecto, se escanean todos los sistemas de archivos.

- Para excluir algún sistema de archivos, utilice el parámetro **ExcludeFilesystems** con la operación **add**. Los tipos de sistemas de archivos aparecen en el archivo **/proc/filesystems**. Por ejemplo, para añadir nfs a la lista de sistemas de archivos a excluir, escriba:

```
/opt/sophos-av/bin/savconfig add ExcludeFilesystems nfs
```

- Para eliminar una exclusión de la lista, utilice el parámetro **ExcludeFilesystems** con la operación **remove**. Por ejemplo, escriba:
  ```
  /opt/sophos-av/bin/savconfig remove ExcludeFilesystems nfs
  ```

15.4 Escanear archivos comprimidos

Por defecto, el escaneado en acceso no comprueba archivos comprimidos. Si lo desea, puede activar el escaneado dentro de archivos comprimidos. Por ejemplo, para escanear archivos comprimidos antes de enviarlos por email.

Nota: no se recomienda activar esta opción por las siguientes razones:

- El escaneado de archivos comprimidos es bastante más lento.
- El contenido de los archivos comprimidos se escanea cuando se realiza la extracción.

Nota: el motor de detección de amenazas solo escanea los archivos comprimidos que tienen más de 8 GB (una vez descomprimidos). Esto se debe a que funciona con el formato comprimido POSIX ustar, que no admite archivos más grandes.

- Para *activar* el escaneado de archivos comprimidos, escriba:
  ```
  /opt/sophos-av/bin/savconfig set ScanArchives enabled
  ```
- Para *desactivar* el escaneado de archivos comprimidos, escriba:
  ```
  /opt/sophos-av/bin/savconfig set ScanArchives disabled
  ```

15.5 Limpiar archivos infectados

Puede configurar el escaneado en acceso para que limpie (desinfectar o borrar) archivos infectados. Por defecto, la limpieza se encuentra desactivada.

Las acciones que Sophos Anti-Virus lleva a cabo con los archivos infectados se recogen en el registro de Sophos Anti-Virus.

Nota: puede activar tanto la desinfección como la eliminación, aunque no se recomienda. Si activa ambas, Sophos Anti-Virus primero intentará la desinfección. Si falla, realizará la eliminación.

Nota: Sophos Anti-Virus puede desinfectar o eliminar archivos al escanear escanear "al abrir" (es decir, cuando los archivos se copian, se mueven o se abren). No puede hacerlo al escanear "al cerrar" (es decir, cuando los archivos se guardan o se crean). Esto no supone un problema en condiciones de uso normales, ya que el escaneado "al abrir" no se puede desactivar de forma centralizada en ordenadores Linux, y desinfectará o eliminará archivos durante el siguiente acceso.

15.5.1 Disinfectar archivos y sectores de arranque

- Para *activar* la desinfección de archivos y sectores de arranque infectados en el escaneado en acceso, escriba:
  ```
  /opt/sophos-av/bin/savconfig add AutomaticAction disinfect
  ```
  Importante: Sophos Anti-Virus no pedirá confirmación antes de la desinfección.

Nota: la desinfección de documentos infectados no puede deshacer el daño que el virus haya podido causar. (Vea Información de limpieza en la página 16 para obtener desde la web de Sophos información sobre cada virus.)

- Para *desactivar* la desinfección de archivos y sectores de arranque infectados en el escaneado en acceso, escriba:
  `/opt/sophos-av/bin/savconfig remove AutomaticAction disinfect`

15.5.2 Eliminar archivos infectados

Importante: sólo debería utilizar esta opción bajo las indicaciones del soporte técnico de Sophos. Si el archivo infectado es un buzón de correo, Sophos Anti-Virus podría borrar el buzón entero.

- Para *activar* la eliminación de archivos infectados en el escaneado en acceso, escriba:
  `/opt/sophos-av/bin/savconfig add AutomaticAction delete`

  Importante: Sophos Anti-Virus no pedirá confirmación antes de eliminar archivos.

- Para *desactivar* la eliminación de archivos infectados en el escaneado en acceso, escriba:
  `/opt/sophos-av/bin/savconfig remove AutomaticAction delete`

16 configuración mediante archivos extra

En esta sección se describe cómo configurar Sophos Anti-Virus con archivos extra de configuración.

16.1 Acerca de los archivos extra de configuración

En esta sección se describen los archivos extra de configuración.

16.1.1 ¿Qué es la configuración mediante archivos extra?

La configuración mediante archivos extra es un método de configuración de Sophos Anti-Virus. Es una alternativa al uso de Sophos Enterprise Console y no requiere un equipo con Windows.

Debe utilizar este método sólo si no puede utilizar Enterprise Console.

Nota: No es posible utilizar Enterprise Console junto con la configuración mediante archivos extra.

Puede utilizar este método para todas las opciones de Sophos Anti-Virus excepto el escaneado en demanda, para el que debe consultar Configurar el escaneado en demanda en la página 11.

16.1.2 ¿Cómo se utiliza la configuración mediante archivos extra?

Se crea un archivo que contiene los valores de los archivos extra de configuración. Este archivo no está en línea, por lo que otros equipos no pueden acceder a él.

Cuando esté listo para configurar los equipos, se copia el archivo sin conexión a un archivo de configuración en vivo, que se encuentra en una ubicación a la que pueden acceder los equipos. Las estaciones obtienen esta configuración del archivo en vivo cuando cuando se actualizan.

Para volver a configurar los equipos de los usuarios, se actualiza el archivo de configuración que está sin conexión, y se copiar en el archivo de configuración en vivo de nuevo.

Notas:

- Para asegurarse de que el archivo de configuración es seguro, debe crear y utilizar certificados de seguridad, tal como se describe en las siguientes secciones.
- Es posible bloquear la configuración para que los usuarios finales individuales no puedan modificarla en sus equipos.

Las siguientes secciones explican cómo crear y utilizar archivos extra de configuración.

16.2 Cómo usar los archivos extra de configuración

Para utilizar archivos extra, debe:

- Crear certificados de seguridad en el servidor.
- Crear un archivo extra de configuración.

- Instalar el certificado raíz en las estaciones.
- Permitir a las estaciones de trabajo de los usuarios utilizar archivos extra de configuración.

16.2.1 Crear certificados de seguridad en el servidor

Para crear los certificados de seguridad proceda de la siguiente manera:

Nota: si utiliza OpenSSL para generar certificados, debe ejecutar OpenSSL 0.9.8 o posterior.

1. Busque el script que vaya a utilizar para crear los certificados. El script está disponible en el artículo de la base de conocimiento de soporte de Sophos 119602.
2. Ejecute el script para crear un conjunto de certificados. Por ejemplo, escriba:

   ```
   ./create_certificates.sh /root/certificates
   ```

   Puede especificar un directorio diferente en el que colocar los certificados. Sin embargo, debe asegurarse de que los certificados se encuentran en un lugar seguro.
3. Cuando se le solicite, introduzca y confirme la contraseña de la clave raíz.
4. Cuando se le solicite, introduzca y confirme la contraseña de la clave de firma.
5. Compruebe que los certificados se encuentran en el directorio. Escriba:

   ```
   ls /root/certificates/
   ```

   Debe ver estos archivos:

   ```
   extrafiles-root-ca.crt extrafiles-root-ca.key extrafiles-signing.cnf
   extrafiles-signing.crt extrafiles-signing.key
   ```

16.2.2 Crear archivos extra de configuración

1. En el equipo donde desee almacenar los archivos extra de configuración, utilice el comando **savconfig** para crear el archivo de configuración de prueba.

   La sintaxis es la siguiente:

   /opt/sophos-av/bin/savconfig -f *archivo-conf-prueba* **-c** *operación parámetro valor*

   donde:

   - -f *archivo-conf-prueba* indica la ruta y nombre del archivo de configuración de prueba. **savconfig** creará el archivo.
   - **-c** especifica el acceso a la capa corporativa (para más información sobre las capas, consulte Capas de configuración en la página 43).
   - *operation* será **set**, **update**, **add**, **remove** o **delete**.
   - *parámetro* es la opción que desea configurar.
   - *valor* es el valor que desea establecer.

   Por ejemplo, para crear un archivo con el nombre `OfflineConfig.cfg` en el directorio `/rootconfig/` y desactivar las alertas por email, escriba:

   ```
   /opt/sophos-av/bin/savconfig -f /root/config/OfflineConfig.cfg -c
   set EmailNotifier Disabled
   ```

   Para más información sobre el uso de **savconfig**, consulte Comando de configuración savconfig en la página 44.

2. Para ver los valores de cada parámetro, utilice la opción **query**. Puede ver el valor de algún parámetro en particular o de todos los parámetros. Por ejemplo, para ver los valores de todos los parámetros, escriba:
   /opt/sophos-av/bin/savconfig -f /root/config/OfflineConfig.cfg -c query
3. Tras establecer los parámetros en el archivo de configuración de prueba, cree una unidad compartida web o de red para ofrecer el archivo de configuración.
4. Cree el archivo de configuración mediante el comando **addextra**. La sintaxis es la siguiente:

   /opt/sophos-av/update/addextra
   offline-config-file-pathlive-config-file-path
   --signing-key=*signing-key-file-path*
   --signing-certificate=*signing-certificate-file-path*

   Por ejemplo:

   /opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg /var/www/extrafiles/ --signing-key= /root/certificates/extrafiles-signing.key --signing-certificate=/root/certificates/extrafiles-signing.crt

16.2.3 Instalar el certificado raíz en las estaciones

Debe instalar el certificado raíz en cada estación de trabajo.

1. En el equipo en el que ha creado los certificados (o el equipo al que los ha copiado), cree un nuevo directorio para el certificado raíz. Escriba:

   mkdir rootcert
   cd rootcert/
2. Copie el certificado raíz en el nuevo directorio. Escriba:

   cp /root/certificates/extrafiles-root-ca.crt .
3. Copie el nuevo directorio en un directorio compartido.
4. Vaya a cada equipo y monte el directorio compartido.
5. Instale el certificado. La sintaxis es la siguiente:

   /opt/sophos-av/update/addextra_certs --install= *shared-rootcert-directory*

   Por ejemplo:

   /opt/sophos-av/update/addextra_certs --install= /mnt/rootcert/

16.2.4 Permitir a las estaciones de trabajo de los usuarios utilizar archivos extra de configuración

Puede permitir que las estaciones de los usuarios puedan descargar y utilizar archivos extra de configuración de la siguiente manera.

1. Si el archivo de configuración se encuentra en una unidad compartida de red, monte dicho directorio en las estaciones.

2. En las estaciones, especifique la ruta de acceso al archivo de configuración. Por ejemplo:

   `/opt/sophos-av/bin/savconfig set ExtraFilesSourcePath http://www.example.com/extrafiles`

   La nueva configuración se aplicará en las estaciones la próxima vez que se actualicen.

3. Para ejecutar una actualización ahora, escriba:

   `/opt/sophos-av/bin/savupdate`

16.3 Actualizar los archivos extra de configuración

1. En el equipo donde almacena los archivos extra de configuración, utilice el comando **`savconfig`** para actualizar el archivo de configuración de prueba.

   Utilice la misma sintaxis que empleó al crear el archivo de configuración de prueba.

   Por ejemplo, para actualizar un archivo con el nombre `OfflineConfig.cfg` en el directorio `/opt/sophos-av` y activar las alertas por email, escriba:

   `opt/sophos-av/bin/savconfig -f /opt/sophos-av/OfflineConfig.cfg -c set EmailNotifier Disabled`

2. Para ver los valores de cada parámetro, utilice la opción **query**. Puede ver el valor de algún parámetro en particular o de todos los parámetros. Por ejemplo, para ver los valores de todos los parámetros, escriba:
   `/opt/sophos-av/bin/savconfig -f /opt/sophos-av/OfflineConfig.cfg -c query`

3. Tras establecer los parámetros en el archivo de configuración de prueba, aplique los cambios en el archivo de configuración mediante el comando **`addextra`**. La sintaxis es la siguiente:

   `/opt/sophos-av/update/addextra` *`offline-config-file-pathlive-config-file-path`*
   `--signing-key=`*`signing-key-file-path`*
   `--signing-certificate=`*`signing-certificate-file-path`*

   Por ejemplo:

   `/opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg /var/www/extrafiles/ --signing-key= /root/certificates/extrafiles-signing.key --signing-certificate=/root/certificates/extrafiles-signing.crt`

   La nueva configuración se aplicará en las estaciones la próxima vez que se actualicen.

4. Para ejecutar una actualización ahora, escriba:

   `/opt/sophos-av/bin/savupdate`

16.4 Capas de configuración

La instalación de Sophos Anti-Virus incluye un archivo local de configuración con las opciones de Sophos Anti-Virus, aparte de los escaneados en demanda.

Cada archivo de configuración local contiene varias capas:

- Sophos: Siempre presente en el archivo. Incluye la configuración predeterminada que sólo Sophos puede modificar.
- Corporativa: Capa que se configura mediante archivos extra.
- Usuario: Presente si se realiza configuración local. Incluye la configuración personalizada del equipo.

Cada capa incluye los mismos parámetros, por lo que se pueden configurar independientemente. Sin embargo, cuando Sophos Anti-Virus lee los parámetros de configuración, los aplicará de forma jerárquica:

- Por defecto, la capa corporativa tiene preferencia sobre la de usuario.
- Tanto la capa corporativa como la de usuario están por encima de la capa de Sophos.

Por ejemplo, si alguna opción se configura en la capa de usuario y en la capa corporativa, se utilizará el valor de la capa corporativa. Sin embargo, puede desbloquear los valores en la capa corporativa que desee configurar de forma local.

Cuando se actualiza el archivo de configuración local mediante un archivo extra de configuración, se sustituirá la capa corporativa.

16.5 Comando de configuración savconfig

`savconfig` es el comando que se usa para configurar los parámetros de Sophos Anti-Virus menos el escaneado en demanda. La ruta del comando es `/opt/sophos-av/bin`. El uso de este comando se explica en los restantes capítulos de este manual. En el resto de esta sección se describe su sintaxis.

La sintaxis de **`savconfig`** es:

`savconfig [`*`opción`***`] ... [`***`operación`***`] [`***`parámetro`***`] [`***`valor`***`] ...`**

Para ver la lista completa de opciones, operaciones y parámetros, escriba:

```
man savconfig
```

16.5.1 *opción*

Puede especificar más de una opción. Las opciones están principalmente asociadas con las *capas* en los archivos de configuración local en cada instalación Por defecto, el comando accede a la capa de usuario. Si desea acceder a otra capa, por ejemplo la capa de empresa, utilice la opción **-c** o **--corporate**.

Por defecto, los valores de los parámetros en la capa de empresa están bloqueados, de modo que anulan los valores de la capa de usuario. Si desea que un parámetro de empresa sea anulado por los usuarios, utilice la opción **--nolock**. Por ejemplo, para configurar el valor de **LogMaxSizeMB** y permitir que sea anulado, escriba:

```
/opt/sophos-av/bin/savconfig --nolock -f corpconfig.cfg -c
LogMaxSizeMB 50
```

Si utiliza Enterprise Console, puede mostrar los valores de los parámetros antivirus mediante la opción **--consoleav**. Escriba:

```
/opt/sophos-av/bin/savconfig --consoleav query
```

También puede mostrar los parámetros de actualización de Enterprise Console mediante la opción **--consoleupdate**. Escriba:

```
/opt/sophos-av/bin/savconfig --consoleupdate query
```

16.5.2 *operación*

Puede especificar una operación. Las operaciones especifican cómo desea acceder a un parámetro. Algunos parámetros sólo pueden tener un valor, mientras que otros tienen una lista de valores. Las operaciones permiten añadir o eliminar valores de la lista. Por ejemplo, el parámetro **Email** es una *lista* de direcciones de correo electrónico.

Para mostrar los valores de los parámetros, utilice la operación **query**. Por ejemplo, para mostrar el valor del parámetro **EmailNotifier**, escriba:

```
/opt/sophos-av/bin/savconfig query EmailNotifier
```

Si utiliza Enterprise Console, cuando **savconfig** devuelve los valores de los parámetros, los que entren en conflicto con la política de Enterprise Console se marcarán con la palabra “Conflict”.

16.5.3 *parámetro*

Puede especificar un parámetro. Para enumerar todos los parámetros básicos, escriba:

```
/opt/sophos-av/bin/savconfig -v
```

Algunos parámetros requieren parámetros secundarios que también deben especificarse.

16.5.4 *valor*

Puede especificar los valores que desee asignar a un parámetro. Si algún valor contiene espacios, deberá incluirlo entre comillas simples.

17 Solución de problemas

En esta sección se describe cómo solucionar posibles problemas con Sophos Anti-Virus.

Para más información sobre los códigos de error del escaneado en demanda de Sophos Anti-Virus consulte el Apéndice: Códigos de error del escaneado en demanda en la página 52.

17.1 No se puede ejecutar un comando

Síntomas

El sistema no permite ejecutar comandos de Sophos Anti-Virus.

Causa

Puede que no disponga de los permisos necesarios.

Solución

Inicie la sesión con un usuario que disponga de más premisos o como root.

17.2 No se aplican las exclusiones correctamente

Síntomas

En ocasiones, al configurar Sophos Anti-Virus para incluir archivos previamente excluidos del escaneado en acceso, los archivos siguen excluidos.

Causa

Esto se puede deber a que la caché de archivos escaneados todavía incluye las exclusiones.

Solución

Según el tipo de intercepción de archivos que utilice, siga los pasos siguientes:

- Si utiliza Talpa, vacíe la caché. Escriba:

  ```
  echo 'disable' > /proc/sys/talpa/intercept-filters/Cache/status
  echo 'enable' > /proc/sys/talpa/intercept-filters/Cache/status
  ```

- Si utiliza Fanotify, reinicie el servicio sav-protect. Escriba:

  ```
  /etc/init.d/sav-protect restart
  ```

17.3 No se encuentra la página man

Síntomas

Al intentar ver alguna página man de Sophos Anti-Virus, puede que se muestre un mensaje del tipo `No manual entry for ...`.

Causa

Probablemente se debe a que la variable de entorno MANPATH no incluye la ruta a dichas páginas man.

Solución

1. Si trabaja en el entorno sh, ksh o bash, debe editar el archivo `/etc/profile`.

   Si trabaja en el entorno csh o tcsh, debe editar el archivo `/etc/login`.

   Nota: si no dispone de un script de inicio de sesión o perfil, realice los siguientes pasos desde la línea de comandos. Debe realizar estos pasos cada vez que reinicie el sistema.

2. Compruebe que la variable de estado MANPATH incluye el directorio `/usr/local/man`.
3. Si MANPATH no incluye dicho directorio, haga lo siguiente. No modifique los valores existentes.

   Si trabaja en el entorno sh, ksh o bash, escriba:

   `MANPATH=$MANPATH:/usr/local/man`

   `export MANPATH`

   Si trabaja en el entorno csh o tcsh, escriba:

   `setenv MANPATH` *`valores`***`:/usr/local/man`**

   donde *valores* son los valores existentes.

4. Guarde el script de inicio de sesión o perfil.

17.4 Se queda sin espacio en disco

Síntomas

Sophos Anti-Virus se queda sin espacio en disco, posiblemente al escanear archivos comprimidos complejos.

Causa

Esto puede ocurrir por alguna de las siguientes razones:

- Al descomprimir los archivos comprimidos, Sophos Anti-Virus utiliza el directorio `/tmp` para guardar sus archivos de trabajo. Si este directorio no es suficientemente grande, es posible que Sophos Anti-Virus se quede sin espacio.
- Sophos Anti-Virus ha excedido la cuota de usuario.

Solución

Escoja una de las siguientes opciones:

- Amplíe el directorio `/tmp`.
- Incremente la cuota de usuario.
- Cambie el directorio de trabajo de Sophos Anti-Virus. Para ello, cambie el valor de la variable de entorno SAV_TMP.

17.5 El escaneado en demanda es muy lento

Esto puede ocurrir por alguna de las siguientes razones:

Síntomas

Sophos Anti-Virus tarda demasiado al realizar un escaneado en demanda.

Causa

Esto puede ocurrir por alguna de las siguientes razones:

- Por defecto, Sophos Anti-Virus realiza el escaneado rápido, que comprueba sólo las partes de los archivos que pueden contener virus. Si utiliza el escaneado exhaustivo (mediante la opción **-f**), se comprobará el contenido completo del archivo.
- Por defecto, Sophos Anti-Virus sólo escanea determinados tipos de archivo. Si se configura para escanear *todos* los archivos, el proceso requerirá más tiempo.

Solución

Pruebe las siguientes opciones:

- No utilice el escaneado exhaustivo a menos que se lo recomiende el equipo de soporte técnico de Sophos.
- Para escanear archivos con una extensión específica, añádala a la lista de extensiones que Sophos Anti-Virus escanéa por defecto. Para más información, consulte Escanear un tipo de archivo en la página 11.

17.6 El programa de copias de seguridad copia todos los archivos que han sido escaneados

Síntomas

El programa de copias de seguridad copia todos los archivos que Sophos Anti-Virus haya escaneado.

Causa

Esto se debe a que Sophos Anti-Virus modifica la hora de cambio de estado en los archivos escaneados. Por defecto, Sophos Anti-Virus restaura la hora de acceso (**atime**) tras escanear los archivos. Esto produce el cambio en la hora de cambio de estado (**ctime**). Si su programa de copias de seguridad comprueba el estado de **ctime**, copiará todos los archivos escaneados por Sophos Anti-Virus.

Solución

Ejecute **savscan** con la opción **--no-reset-atime**.

17.7 No se limpian los virus

Síntomas

- Sophos Anti-Virus no realiza la limpieza de los virus detectados.
- Sophos Anti-Virus muestra el mensaje de error `Disinfection failed`.

Causa

Esto puede ocurrir por alguna de las siguientes razones:

- No tiene activada la limpieza automática.
- Sophos Anti-Virus no puede desinfectar el tipo de virus detectado.
- Los archivos detectados se encuentran en una unidad extraíble, por ejemplo disquete o CD-ROM, protegido contra escritura.
- Los archivos detectados se encuentran en un sistema de archivos NTFS.
- Sophos Anti-Virus no limpia fragmentos de virus ya que no se dispone una correspondencia exacta.

Solución

Pruebe las siguientes opciones:

- Active la desinfección automática para ese tipo de escaneado.

- Si es posible, quite la protección contra escritura.
- Desinfecte los archivos en sistemas de archivos NTFS de forma local.

17.8 Fragmento de virus detectado

Síntomas

Sophos Anti-Virus informa de la detección de un fragmento de virus.

Causa

Esto indica que parte de un archivo coincide de forma parcial con algún virus. Esto puede ocurrir por alguna de las siguientes razones:

- Muchos de los nuevos virus están basados en otros anteriores. Así, las nuevas variantes comparten parte del código con sus predecesores.
- A menudo, los virus contienen errores por lo que su rutina de replicado podría fallar, creando archivos corruptos. Sophos Anti-Virus podría detectar el archivo que el virus intentaba crear o infectar.
- Al realizar escaneados exhaustivos, Sophos Anti-Virus podría notificar la existencia de un fragmento de virus en una base de datos.

Solución

1. Actualice Sophos Anti-Virus con la detección más reciente.
2. Para desinfectar el archivo, consulte Desinfectar un archivo en la página 17.
3. Si se siguen detectando fragmentos de virus, póngase en contacto con el soporte técnico de Sophos.

17.9 No se puede acceder a un disco

Síntomas

No es posible acceder a los archivos en un disco extraíble.

Causa

Por defecto, Sophos Anti-Virus bloqueará el acceso a unidades extraíbles con sectores de arranque infectados.

Solución

Si necesita acceso a la unidad (por ejemplo, para copiar los archivos), haga lo siguiente:

1. Escriba:

   ```
   /opt/sophos-av/bin/savconfig set AllowIfBootSectorThreat enabled
   ```

2. Cuando haya terminado, escriba:

   `/opt/sophos-av/bin/savconfig set AllowIfBootSectorThreat disabled`

3. Retire el disco del equipo para que no pueda intentar infectarlo de nuevo durante el reinicio.

18 Apéndice: Códigos de retorno del escaneado en demanda

savscan devolverá un código diferente según el resultado del escaneado.. Puede ver el código de retorno tras concluir el escaneado mediante el sigueinte comando:

echo $?

Código de retorno	Descripción
0	No se produjo ningún error ni se detectó ningún virus
1	El usuario interrumpió el escaneado mediante CTRL+C
2	Se produjo algún error que interrumpió el escaneado
3	Se detectó algún virus

18.1 Códigos de retorno extendido

savscan devuelve códigos de retorno más detallados si se ejecuta con la opción **-eec**. Puede ver el código de retorno tras concluir el escaneado mediante el sigueinte comando:

echo $?

Código de retorno extendido	Descripción
0	No se produjo ningún error ni se detectó ningún virus
8	Se produjo algún error pero se pudo continuar
16	Se encontró algún archivo protegido con contraseña (no se escanea)
20	Se ha detectado y desinfectado algún virus

Código de retorno extendido	Descripción
24	Se ha detectado algún virus, pero no se ha desinfectado
28	Se ha detectado algún virus en la memoria
32	Falló la verificación de integridad
36	Se produjo algún error y no se pudo continuar
40	Se interrumpió el escaneado

19 Apéndice: Configuración de la función de llamada a casa

Sophos Anti-Virus puede contactar con Sophos a fin de enviarnos algunos datos sobre el producto y la plataforma. La función "llamada a casa" nos ayuda a mejorar el producto y la experiencia del usuario.

Cuando instala Sophos Anti-Virus, se activa de forma predeterminada la función llamada a casa. Le agradeceríamos que la dejara activada. No afecta a su seguridad ni al rendimiento de su ordenador.

- Sus datos se envían encriptados a una ubicación segura y los guardamos durante un máximo de 3 meses.
- El producto únicamente envía 2 KB de datos una vez a la semana. Básicamente llama al domicilio a intervalos aleatorios para evitar que diversos ordenadores contacten con el hogar a la vez.

Una vez instalada, puede desinstalarla cuando desee.

Para desactivar la función de llamada a casa, escriba:

```
/opt/sophos-av/bin/savconfig set DisableFeedback true
```

Para activar la función de llamada a casa, escriba:

```
/opt/sophos-av/bin/savconfig set DisableFeedback false
```

20 Apéndice: Configuración de los reinicios en RMS

Si RMS (Remote Management System), que se encarga de gestionar las comunicaciones con el servidor, se bloquea o no se inicia correctamente, un adaptador reiniciará los componentes de RMS, mrouter y magent.

Si desea reinicie el RMS periódicamente, agregue

`RestartIntervalHours=<Horas>`

a $INST/etc/sophosmgmtd.conf.

21 Glosario

archivos extra	Archivos de configuración centralizada de Sophos Anti-Virus. Las estaciones se actualizan con estos archivos desde la ubicación especificada.
desinfección	Eliminación de virus en archivos o sectores de arranque.
directorio de instalación central (CID)	Directorio en el que se copia el software de Sophos y las actualizaciones. Las estaciones de la red se actualizan desde este directorio.
escaneado en acceso	Es la principal forma de protección contra virus. Al acceder (copiar, guardar, mover o abrir) un archivo, Sophos Anti-Virus lo escanea y permite el acceso sólo si no supone una amenaza para el equipo.
escaneado en demanda	Escaneado iniciado por el usuario. Puede escanear desde un solo archivo a todo el contenido del equipo con permiso de lectura.
escaneado programado	Escaneado del ordenador, o parte, que se ejecuta a las horas establecidas.
estación	Ordenador en el que ha instalado Sophos Anti-Virus y que no actúa como fuente de actualización para otros ordenadores.
fuente primaria de actualización	Ubicación desde la que se actualizan las estaciones. Puede que necesite credenciales de acceso.
fuente secundaria de actualización	Ubicación de actualización alternativa que se utiliza cuando la fuente primaria no está disponible. Puede que necesite credenciales de acceso.
Protección activa de Sophos	Función que utiliza la conexión a Internet para comprobar archivos sospechosos.
servidor de actualización	Un ordenador en el que ha instalado Sophos Anti-Virus y que actúa como fuente de actualización para otros ordenadores. Estos ordenadores pueden ser estaciones u otros servidores de actualización, según el modo en el que haya distribuido Sophos Anti-Virus en la red.

virus	Programa informático que se copia a sí mismo. Los virus pueden alterar el funcionamiento del sistema o dañar datos. Los virus se extienden ocultos en otros programas desde donde se ejecutan. Algunos virus se propagan a través de redes o enviándose por email. El término “virus” se utiliza a menudo para referirse a virus, gusanos y troyanos.
virus de sector de arranque	Virus que altera el proceso de arranque del equipo. Puede afectar al sector de arranque maestro o al sector de arranque de particiones.

22 Soporte técnico

Para obtener asistencia técnica sobre cualquier producto de Sophos, puede:

- Visitar la comunidad de Sophos en community.sophos.com/ para consultar casos de otros usuarios con el mismo problema.
- Visitar la base de conocimiento de Sophos en www.sophos.com/es-es/support.aspx.
- Descargar la documentación correspondiente desde www.sophos.com/es-es/support/documentation.aspx.
- Abrir un ticket de incidencia con nuestro equipo de soporte en https://secure2.sophos.com/support/contact-support/support-query.aspx.

23 Aviso legal

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

the underlying OS platform is Y2K-compliant. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, CoSMIC™, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. Schmidt

GNU General Public License

Algunos programas de software se ofrecen al usuario bajo licencias de público general (GPL) o licencias similares de software gratuito que, entre otros derechos, permiten copiar, modificar y redistribuir ciertos programas o partes de los mismos, y tener acceso al código fuente. Las licencias de dichos programas, que se distribuyen al usuario en formato binario ejecutable, exigen que el código fuente esté disponible. Para cualquiera de tales programas que se distribuya junto con el producto de Sophos, el código fuente está disponible mediante solicitudes por correo electrónico a savlinuxgpl@sophos.com. Para ver los términos de la licencia GPL, visite www.gnu.org/copyleft/gpl.html

libmagic – file type detection

Copyright © Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.

Software written by Ian F. Darwin and others; maintained 1994–2004 Christos Zoulas.

This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice immediately at the beginning of the file, without modification, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)

ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Medusa web server

Medusa was once distributed under a 'free for non-commercial use' license, but in May of 2000 Sam Rushing changed the license to be identical to the standard Python license at the time. The standard Python license has always applied to the core components of Medusa, this change just frees up the rest of the system, including the http server, ftp server, utilities, etc. Medusa is therefore under the following license:

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Sam Rushing not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

SAM RUSHING DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL SAM RUSHING BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Sam would like to take this opportunity to thank all of the folks who supported Medusa over the years by purchasing commercial licenses.

OpenSSL Cryptography and SSL/TLS Toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998-2016 The OpenSSL Project. Todos los derechos reservados.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

   The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

Protocol Buffers (libprotobuf)

Copyright 2008, Google Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

pycrypto

Distribute and use freely; there are no restrictions on further dissemination and usage except those imposed by the laws of your country of residence. This software is provided “as is” without warranty of fitness for use or suitability for any purpose, express or implied. Use at your own risk or not at all.

Incorporating the code into commercial products is permitted; you do not have to make source available or contribute your changes back (though that would be nice).

– –amk (www.amk.ca)

Python

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

1. This LICENSE AGREEMENT is between the Python Software Foundation (“PSF”), and the Individual or Organization (“Licensee”) accessing and otherwise using this software (“Python”) in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, worldwide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF’s License Agreement and PSF’s notice of copyright, i.e., “Copyright © 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009 Python Software Foundation; All Rights Reserved” are retained in Python alone or in any derivative version prepared by Licensee.
3. In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.
4. PSF is making Python available to Licensee on an “AS IS” basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.
8. By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

TinyXML XML parser

www.sourceforge.net/projects/tinyxml

Original code by Lee Thomason (www.grinninglizard.com)

This software is provided ‘as-is’, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

zlib data compression library

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

20161125

Índice

A

acceso a discos 50
actualización 20–21, 31
  compatibilidad con kernel nuevos 21
  compatibilidad con kernel personalizados 21
  configurar 31
  inmediata 20
alertas 14, 26–27
  correo electrónico 27
  línea de comandos 14, 26
  mensajes de escritorio 14, 26
alertas de escritorio 14, 26
alertas en la línea de comandos 14, 26
alertas por email 27
análisis de virus 16
archivos comprimidos 11–12
  escaneados en demanda 11–12
archivos infectados 16–18, 38
  cuarentena 16
  desinfectar 17
  eliminar 17–18
  limpieza 17, 38
archivos, escaneado en demanda 10

C

capas, en archivo de configuración 43
codificación de caracteres 37
códigos de error 52
códigos de retorno 52
configurar Sophos Anti-Virus. 6
copia de seguridad de archivos escaneados 49

D

desinfectar 17–18
  archivos infectados 17
  sectores de arranque 18
directorios, escaneado en demanda 10
discos, acceso 50

E

efectos secundarios de los virus 18
ejecutables UNIX, escaneados en demanda 13
elementos con enlace simbólico, escaneados en demanda 12
eliminar archivos infectados. 17–18
Enterprise Console 6
escaneado en acceso 8, 36
  excluir elementos 36
  Fanotify 36
escaneado en demanda lento 48
escaneados en demanda 10–13, 22
  archivos 10
  archivos comprimidos 11–12
escaneados en demanda *(continuación)*
  directorios 10
  ejecutables UNIX 13
  elementos con enlace simbólico 12
  escaneados programados 22
  excluir elementos 12
  ordenador 10
  ordenadores remotos 12
  sectores de arranque 10
  sistema de archivos 10, 12
  tipos de archivo 11, 13
escaneados programados 22
espacio en disco insuficiente 47
excluir elementos 12, 36–37
  codificación de caracteres 37
  escaneado en acceso 36
  escaneados en demanda 12

F

fragmento detectado, virus 50

I

información de limpieza 16

K

kernel 21
  nuevas ediciones 21
  personalizados 21
kernel personalizados 21

L

limpiar archivos infectados 17, 38
Live Protection 35

N

No manual entry for … 47
no se encuentra la página man 47

O

ordenador, escaneado en demanda 10
ordenadores remotos, escaneado en demanda 12

P

poner en cuarentena los archivos infectados 16

R

registro de Sophos Anti-Virus 30
  configurar 30

Registro, Sophos Anti-Virus 30
    configurar 30

S

savconfig 44
savsetup 31
sector de arranque infectado 50
sectores de arranque 10, 18, 50
    desinfectar 18
    escaneados en demanda 10
    infectado 50
sistema de archivos, escaneado en demanda 10, 12

T

tipos de archivo, escaneado en demanda 11, 13

V

virus 14, 16, 18, 29, 49–50
    análisis 16
    detectado 14, 29
    efectos secundarios 18
    fragmento detectado 50
    no se limpian 49