SOPHOS

Cybersecurity made simple.

Sophos Anti-Virus para Linux

Guía de configuración

Contenido

1 Acerca de esta guía

En este 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 está disponible en http://www.sophos.com/es-es/support/documentation.aspx.

Instalaciones administradas por Sophos Central

Si utiliza servidores Linux de 32 bits administrados mediante Sophos Central consulte la Guía de inicio de Sophos Anti-Virus para Linux.

Si utiliza servidores Linux de 64 bits administrados mediante Sophos Central consulte la Guía de inicio de Sophos Anti-Virus para Linux 10.

Atención
La información de configuración de esta guía también es aplicable a Sophos Anti-Virus para Linux 10.

2 Acerca de Sophos Anti-Virus para Linux

2.1 Funciones de Sophos Anti-Virus para Linux

Sophos Anti-Virus para Linux 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.

Sophos Anti-Virus permite ejecutar escaneados 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.

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 para Linux

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

Equipos administrados por Sophos Enterprise Console o Sophos Central

Si sus equipos Linux se administran con Sophos Enterprise Console o Sophos Central, configure Sophos Anti-Virus para Linux 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 UNIX 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 Anti-Virus para Linux, versión 10.

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

Equipos en red no administrados por Sophos Enterprise Console o Sophos Central

Si dispone de una red de equipos Linux no administrados por Sophos Enterprise Console o Sophos Central, el escaneado en demanda se configura desde la línea de comandos de Sophos Anti-Virus para Linux en cada ordenador de forma local.

Equipo independiente no administrado por Sophos Enterprise Console o Sophos Central

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

Por defecto, el escaneado en acceso se encuentra activado. Si es necesario, puede comprobar que se encuentra activo o iniciarlo.

Nota
Para utilizar los comandos en esta sección debe disponer de derechos de root.

En este documento se asume que ha instalado Sophos Anti-Virus para Linux en la ubicación predeterminada, `/opt/sophos-av`. De lo contrario, utilice el directorio de instalación correspondiente.

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 inicia 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 /`.

Nota
También puede utilizar Sophos Enterprise Console para realizar el escaneado remoto de estaciones de la red. Para obtener más información, consulte la Ayuda de Sophos Enterprise Console.

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 -vvsweep -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 -vvsweep -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 (página 15)).
- Se envía una alerta a Sophos Enterprise Console si el equipo se administra desde Sophos Enterprise Console.
- Se envía una alerta a root@localhost.

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 (página 12).

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 or email support@sophos.com
End of Scan.
```

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 (página 13)) 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 archivo.

  Nota
  La desinfección de documentos infectados no puede deshacer el daño que el virus haya podido causar. Vea Información de limpieza (página 12) 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 archivo.

  Nota
  La desinfección de documentos infectados no puede deshacer el daño que el virus haya podido causar. Vea Información de limpieza (página 12) 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 archivo.

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 Sophos Anti-Virus 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 obtener más información, consulte Cambiar el método de intercepción del escaneado en acceso (página 31).

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 Apéndice: Configurar escaneados programados

Sophos Anti-Virus programar los escaneados.

Nota
Los escaneados programados desde Sophos Enterprise Console tienen el prefijo “SEC:” y sólo se pueden actualizar o eliminar desde Sophos 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 una fetcha 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 Daily /home/fred/DailyScan`.

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 Sophos 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 Sophos 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 Sophos 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 Sophos Enterprise Console.

10.7 Actualizar un escaneado programado desde un archivo

Nota
No es posible actualizar escaneados programados creados desde Sophos 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 (página 19).
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 Sophos 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 Daily -`.
   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 una fetcha y una hora.
3. 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 una fetcha y una hora.

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 Sophos 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 Sophos Enterprise Console.

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

11 Apéndice: Configurar alertas

Nota
Si modifica la configuración de un ordenador en la red, puede perder dicha configuración al actualizarse desde Enterprise Console.

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.

Nota
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 'Póngase en contacto con el departamento informático'`.

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.

Nota
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 'Póngase en contacto con el departamento informático'`.

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 'Póngase en contacto con el departamento informático'`.

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 'Póngase en contacto con el departamento informático'`.

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 Apéndice: Configurar el registro

Nota
Si modifica la configuración de un ordenador en la red, puede perder dicha configuración al actualizarse desde Sophos Enterprise Console.

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 Apéndice: Configurar la actualización

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

13.1 Conceptos básicos

Servidor de actualización

Un servidor de actualización es 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.

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 como un servidor de actualización para otros ordenadores en la red.

Nota
El servidor de actualización debe ser un ordenador de 64 bits si se utiliza para mantener cualquier cliente de 64 bit actualizado. Si el servidor de actualización es un ordenador de 32 bits, no descargará actualizaciones para equipos de 64 bits, y por tanto no actualizará a los clientes.

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) Copie el directorio de caché local (/opt/sophos-av/update/cache/) a otro directorio. Puede automatizar esta tarea mediante un script.
   b) 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 una estación para utilizar un servidor de actualización

Para configurar una estación para utilizar un servidor de actualización:

1. En el ordenador que desea configurar, 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 la opción para configurar la fuente primaria (o secundaria) de actualización.
   `savsetup` le pedirá los datos de la fuente de actualización.
4. Introduzca la dirección del servidor, y las credenciales de acceso si es necesario.

Utilice la dirección HTTP o ruta UNC, según su servidor.

`savsetup` le preguntará si accede al servidor a través de un proxy.

5. Si es así, pulse Y e introduzca los datos necesarios.

14 Apéndice: Configurar Sophos Live Protection

Nota
Si modifica la configuración de un ordenador en la red, puede perder dicha configuración al actualizarse desde Sophos Enterprise Console.

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 Apéndice: Configurar el escaneado en acceso

Nota
Si modifica la configuración de un ordenador en la red, puede perder dicha configuración al actualizarse desde Sophos Enterprise Console.

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 (página 32).

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 Sophos Enterprise Console.

- 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/report`.
  a) Para añadir el directorio `/tmp/informe/` a la lista de exclusiones, escriba: `/opt/sophos-av/bin/savconfig add ExcludeFilePaths /tmp/report/`.

- 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 Sophos Enterprise Console.

- 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 "al abrir" (cuando los archivos se copian, se mueven o se abren). No puede hacerlo al escanear "al cerrar" (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 (página 12) 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 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 Apéndice: Códigos de retorno del escaneado en demanda (página 41).

16.1 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.

16.2 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`.

16.3 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.

16.4 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*.

16.5 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 obtener más información, consulte Escanear un directorio o archivo (página 6).

16.6 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.

16.7 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.

16.8 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 (página 13).
3. Si se siguen detectando fragmentos de virus, póngase en contacto con el soporte técnico de Sophos.

16.9 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.

17 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.

17.1 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
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

18 Apéndice: Configurar la función «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 installa 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`.

19 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`.

20 Glosario

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.
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.
desinfección	Eliminación de virus en archivos o sectores de arranque.
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.
fuente primaria de actualización	Ubicación desde la que se actualizan las estaciones. Puede que necesite credenciales de acceso.
escaneado programado	Escaneado del ordenador, o parte, que se ejecuta a las horas establecidas.
fuente secundaria de actualización	Ubicación de actualización alternativa que se utiliza cuando la fuente primaria no está disponible. Puede que necesite credenciales de acceso.
Sophos Live Protection	Función que utiliza la conexión a Internet para comprobar archivos sospechosos.
estación	Ordenador en el que ha instalado Sophos Anti-Virus y que no actúa como fuente de actualización para otros ordenadores.
servidor de actualización	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.

21 Soporte

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

- Visitar el foro Sophos Community en community.sophos.com/ para consultar casos similares.
- 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/es-es/support/contact-support/support-query.aspx.

22 Aviso legal

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

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

Some software programs are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or similar Free Software licenses which, among other rights, permit the user to copy, modify, and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires for any software licensed under the GPL, which is distributed to a user in an executable binary format, that the source code also be made available to those users. For any such software which is distributed along with this Sophos product, the source code is available by submitting a request to Sophos via email to savlinuxgpl@sophos.com. A copy of the GPL terms can be found at www.gnu.org/copyleft/gpl.html

libcap

Unless otherwise *explicitly* stated, the following text describes the licensed conditions under which the contents of this libcap release may be used and distributed:

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

1. Redistributions of source code must retain any existing copyright notice, and this entire permission notice in its entirety, including the disclaimer of warranties.
2. Redistributions in binary form must reproduce all prior and current copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of any author may not be used to endorse or promote products derived from this software without their specific prior written permission.

ALTERNATIVELY, this product may be distributed under the terms of the GNU General Public License (v2.0 - see below), in which case the provisions of the GNU GPL are required INSTEAD OF the above restrictions. (This clause is necessary due to a potential conflict between the GNU GPL and the restrictions contained in a BSD-style copyright.)

THIS SOFTWARE IS PROVIDED "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(S) 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.

OpenSSL

OpenSSL copyright

LICENSE ISSUES

==========

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 © 1998–2017 The OpenSSL Project. All rights reserved.

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 (C) 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 Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared 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

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 rouines 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 licence 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 licence [including the GNU Public Licence.]

protobuf

This license applies to all parts of Protocol Buffers except the following:

- Atomicops support for generic gcc, located in src/google/protobuf/stubs/atomicops_internals_generic_gcc.h. This file is copyrighted by Red Hat Inc.

- Atomicops support for AIX/POWER, located in src/google/protobuf/stubs/atomicops_internals_power.h. This file is copyrighted by Bloomberg Finance LP.

Copyright 2014, 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)

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

Copyright (C) 1995-2017 Jean-loup Gailly and Mark Adler

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.

Jean-loup Gailly Mark Adler

jloup@gzip.org madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files http://tools.ietf.org/html/rfc1950 (zlib format), rfc1951 (deflate format) and rfc1952 (gzip format).