

SOPHOS

Sophos Anti-Virus para Unix Manual de usuario

Versión: 7

Edición: enero de 2011



Contenido

- 1 Acerca de este manual.....3
- 2 Acerca de Sophos Anti-Virus para UNIX4
- 3 Escaneado en demanda.....6
- 4 Qué ocurre si se detecta algún virus.....10
- 5 Limpiar virus.....11
- 6 Ver el registro de Sophos Anti-Virus14
- 7 Actualización inmediata de Sophos Anti-Virus15
- 8 Apéndice A: Códigos de retorno del escaneado en demanda.....16
- 9 Apéndice B: Configuración desde el CID.....18
- 10 Apéndice C: Configurar el escaneado programado.....23
- 11 Apéndice D: Configurar las alertas por email.....27
- 12 Apéndice E: Configurar el registro.....29
- 13 Apéndice F: Configurar la actualización.....30
- 14 Solución de problemas.....33
- 15 Glosario.....37
- 16 Soporte técnico.....38
- 17 Aviso legal.....39

1 Acerca de este manual

En este manual encontrará información sobre cómo utilizar y configurar Sophos Anti-Virus para UNIX.

Aquí se asume que instala y actualiza Sophos Anti-Virus desde una unidad compartida creada por Sophos Enterprise Console.

Para *instalar* Sophos Anti-Virus, consulte la Guía de inicio de *Sophos Endpoint Security and Control para Linux, NetWare y UNIX*.

La documentación de Sophos se encuentra en <http://esp.sophos.com/support/docs/>.

2 Acerca de Sophos Anti-Virus para UNIX

2.1 Función de Sophos Anti-Virus

Sophos Anti-Virus permite proteger ordenadores UNIX contra virus, gusanos y troyanos. Además de amenazas para UNIX, también puede detectar amenazas que afectan a otras plataformas. It does this by scanning your computer.

2.2 Cómo protege Sophos Anti-Virus el sistema

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

Sophos Anti-Virus dispone de una interfaz de línea de comandos. A través de esta interfaz puede utilizar y configurar Sophos Anti-Virus.

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

En este manual 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 Cómo se configura Sophos Anti-Virus

Si utiliza Sophos Enterprise Console para administrar las estaciones UNIX, configure Sophos Anti-Virus de la siguiente manera:

- El **escaneado programado, las alertas, el registro y la actualización** de forma centralizada desde Enterprise Console. Para más información, consulte la Ayuda de Enterprise Console.

Nota: ciertos parámetros no se pueden configurar desde Enterprise Console. Utilice la línea de comandos de Sophos Anti-Virus en cada estación UNIX para configurar estos parámetros de forma local. Enterprise Console ignora estos parámetros.

- El **escaneado en demanda** se configura desde la línea de comandos de Sophos Anti-Virus en cada estación UNIX.

Si dispone de una red de estaciones UNIX *no* administradas desde Enterprise Console, configure Sophos Anti-Virus de la siguiente manera:

- El **escaneado programado, las alertas, el registro y la actualización** de forma centralizada mediante un archivo de configuración en el directorio de instalación central (CID). Esta es la configuración desde el CID.

- El **escaneado en demanda** se configura desde la línea de comandos de Sophos Anti-Virus en cada estación.

Nota: sólo debería utilizar la configuración desde el CID si el equipo de soporte técnico lo aconseja o si no es posible el uso de Enterprise Console. No es posible realizar la configuración desde Enterprise Console y desde el CID de forma simultánea.

Si dispone de alguna estación UNIX independiente que *no* está administrada desde Enterprise Console, configure todas las funciones de Sophos Anti-Virus desde la línea de comandos de Sophos Anti-Virus.

3 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, consulte [Apéndice C: Configurar un escaneado programado](#) en la página 23.

3.1 Ejecutar un escaneado en demanda

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

3.1.1 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 más información, consulte la Ayuda de Enterprise Console.

3.1.2 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.

3.1.3 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.

3.2 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
```

3.2.1 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.

3.2.2 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.

3.2.3 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**.

- ❖ 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.

3.2.4 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**.

- ❖ 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.

3.2.5 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`

3.2.6 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**.

3.2.7 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`

3.2.8 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/juegos
```

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
```

3.2.9 Escanear los 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**.

4 Qué ocurre si se detecta algún virus

Si se detecta algún virus durante un escaneado en demanda, por defecto Sophos Anti-Virus:

- 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 14).
- Se envía una alerta a Enterprise Console si el equipo se administra desde Enterprise Console.
- Se envía una alerta a root@localhost.
- Se 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 utilidad de detección de virus
Versión 4.50.0 [Linux/Intel]
Versión de datos de virus 4.50, Febrero 2010
Incluye detección de 1375239 virus, troyanos y gusanos
Copyright (c) 1989-2010 Sophos Group. Todos los derechos
reservados.

Hora del sistema 13:43:32, Fecha del sistema 02 marzo 2010

El directorio IDE es: /opt/sophos-av/lib/sav

Usando archivo nystate-d.ide
. . . . .
Usando archivo injec-lz.ide

Escaneado rápido

>>> Virus 'EICAR-AV-Test' encontrado en el archivo
/usr/mydirectory/eicar.src

33 archivos escaneados en 2 segundos.
1 virus detectado.
1 archivo de 33 estaba infectado.
Envíe muestras de archivos infectados a Sophos para su
análisis.
Más información en http://esp.sophos.com, email
support@sophos.com
Fin del escaneado.
```

Para más información sobre la limpieza de virus, consulte [Limpiar virus](#) en la página 11.

5 Limpiar virus

5.1 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 (www.esp.sophos.com/security/analyses).
2. Haga una búsqueda con el término utilizado por Sophos Anti-Virus en la detección.

5.2 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 12) 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.

5.2.1 Hacer uso de la cuarentena

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

5.2.2 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.

5.3 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.

5.3.1 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](#) en la página 11 para obtener desde la web de Sophos información sobre cada virus.

5.3.2 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](#) en la página 11 para obtener desde la web de Sophos información sobre cada virus.

5.3.3 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.

5.3.4 Eliminar todos los archivos infectados

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

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

5.4 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: [Soporte técnico](#) en la página 38.

6 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

7 Actualización inmediata de Sophos Anti-Virus

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.

8 Apéndice A: 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 siguiente 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 |

8.1 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 siguiente 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 |

| Código de retorno extendido | Descripción |
|------------------------------------|---|
| 36 | Se produjo algún error y no se pudo continuar |
| 40 | Se interrumpió el escaneado |

9 Apéndice B: Configuración desde el CID

La configuración desde el directorio de instalación central (CID) es una alternativa a la configuración desde Sophos Enterprise Console. Puede utilizar este método para todas las opciones excepto el escaneado en demanda, para el que debe consultar [Configurar el escaneado en demanda](#) en la página 6.

Nota: Sólo debería utilizar la configuración desde el CID si el equipo de soporte técnico lo aconseja o si no es posible el uso de Enterprise Console. No es posible realizar la configuración desde Enterprise Console y desde el CID de forma simultánea.

Para la configuración desde el CID no se requiere ningún ordenador con Windows. Será necesario realizar cambios en un archivo de configuración presente en el CID mediante el comando **savconfig** (consulte [Comando de configuración savconfig](#) en la página 21). Posteriormente, las estaciones que se actualicen desde dicho CID utilizarán esta configuración.

Durante la configuración, es posible bloquear los parámetros para que no se puedan modificar en las estaciones. De esta forma el usuario no podrá cambiar la configuración de Sophos Anti-Virus.

Existen dos archivos de configuración: el que se encuentra en uso desde el CID y el que se utiliza para probar los cambios. Para realizar cambios de configuración, primero debe probar los cambios en un archivo que después transfiere al archivo de configuración en uso. El proceso se detalla a continuación.

9.1 Crear un archivo de configuración CID

1. Utilice el comando **savconfig** para establecer el valor de cada parámetro en el archivo de configuración.

La sintaxis es la siguiente:

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

donde:

- **-f** especifica el uso del archivo de prueba.
- *archivo-conf* es la ruta al archivo de prueba, en cualquier directorio menos el CID. **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 21).
- *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 CIDconfig.cfg en el directorio ./config y desactivar las alertas por email, escriba:

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

Para más información sobre el uso de **savconfig**, consulte [Comando de configuración savconfig](#) en la página 21.

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 ./config/CIDconfig.cfg -c query
```
3. Cuando haya terminado con la configuración, actualice Sophos Anti-Virus:

```
/opt/sophos-av/bin/savupdate
```
4. Ejecute **addcfg** con la opción **-f** y la ruta al archivo de configuración de prueba:

```
/opt/sophos-av/update/cache/Primary-unpacked/addcfg.sh -f archivo-conf
```
5. Copie el directorio `/opt/sophos-av/update/cache/Primary-unpacked/config` al directorio de instalación central.

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

9.2 Actualizar el archivo de configuración CID

1. Utilice el comando **savconfig** para establecer el valor de cada parámetro en el archivo de configuración.

La sintaxis es la siguiente:

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

donde:

- **-f** especifica el uso del archivo de prueba.
- *archivo-conf* es la ruta al archivo de prueba.
- **-c** especifica el acceso a la capa corporativa (para más información sobre las capas, consulte [Capas de configuración](#) en la página 21).
- *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 actualizar un archivo con el nombre CIDconfig.cfg en el directorio ./config y desactivar las alertas por email, escriba:

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

Nota: debe establecer *todos* los parámetros que desea tener en la capa corporativa, no sólo aquellos que desea actualizar. Para utilizar el archivo de configuración en el CID como archivo de pruebas, copie el archivo CorporateLayer.cfg en cualquier otro directorio. CorporateLayer.cfg se encuentra en el directorio config del CID.

Para más información sobre el uso de **savconfig**, consulte [Comando de configuración savconfig](#) en la página 21.

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 ./config/CIDconfig.cfg -c query
```

3. Cuando haya terminado con la configuración, actualice Sophos Anti-Virus:
/opt/sophos-av/bin/savupdate
4. Ejecute **addcfg** con la opción **-f** y la ruta al archivo de configuración de prueba:
/opt/sophos-av/update/cache/Primary-unpacked/addcfg.sh -f archivo-conf
5. Copie el directorio /opt/sophos-av/update/cache/Primary-unpacked/config al directorio de instalación central.

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

9.3 Capas de configuración

La instalación de Sophos Anti-Virus incluye un archivo local de configuración, con las opciones de Sophos Anti-Virus aparte del escaneo en acceso.

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 usa en la configuración desde un CID.
- **Usuario:** Presente si se realiza configuración local. Incluye la configuración personalizada del equipo.

Cada capa dispone de los mismos parámetros. Sin embargo, cuando Sophos Anti-Virus 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 desde el CID, se sustituirá la capa corporativa.

9.4 Comando de configuración `savconfig`

`savconfig` es el comando que se usa para configurar los parámetros de Sophos Anti-Virus menos el escaneo 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
```

9.4.1 *opción*

Puede especificar más de una opción. Las opciones están principalmente asociadas con las *capas* en los archivos de configuración local en cada instalación. Para más información sobre las capas, consulte [Capas de configuración](#) en la página 21. 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
```

9.4.2 *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".

9.4.3 *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.

9.4.4 *valor*

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

10 Apéndice C: Configurar el escaneado programado

Sophos Anti-Virus puede almacenar diferentes escaneados programados.

Nota: También puede utilizar Enterprise Console o el comando **crontab** para escanear los ordenadores a las horas deseadas. Para más información, consulte la Ayuda de Enterprise Console o el [artículo 12176 en la base de conocimiento de Sophos](#), respectivamente. 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 escaneo que siempre se encuentra presente si el equipo se encuentra administrado desde Enterprise Console.

10.7 Actualizar un escaneo programado desde un archivo

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

1. Abra el archivo con la configuración del escaneo programado que desea actualizar.
Si no dispone del archivo de configuración del escaneo, puede crearlo como se describe en [Exportar un escaneo programado a un archivo](#) en la página 24.
2. Realice los cambios necesarios utilizando los parámetros indicados en la plantilla de escaneo: `/opt/sophos-av/doc/namedscan.example.en`. Debe definir el escaneo en su totalidad, no sólo especificar los cambios.
3. Guarde el archivo.
4. Actualice el escaneo programado en Sophos Anti-Virus mediante el comando **savconfig** con la operación **update** y el parámetro **NamedScans**. Indique el nombre del escaneo y la ruta al archivo con la configuración.

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

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

10.8 Actualizar un escaneo programado de forma manual

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

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

Por ejemplo, para actualizar el escaneo Diario, escriba:

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

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

2. Indique los elementos a escanear, las horas de escaneo 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 escaneo en su totalidad, no sólo especificar los cambios.

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

3. Para terminar, pulse CTRL+D.

10.9 Eliminar un escaneo programado

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

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

Por ejemplo, para eliminar el escaneo Diario, escriba:

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

10.10 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 Apéndice D: Configurar las alertas por email

Nota: si modifica las opciones de un ordenador en la red, es posible que pierda la configuración al actualizarse desde el CID.

Puede configurar Sophos Anti-Virus para enviar alertas por email cuando se detecte algún virus o se produzca algún error. Los mensajes de alerta se pueden enviar en inglés o japonés.

11.1 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`

11.2 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 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.

11.4 Especificar los destinatarios

Por defecto, Sophos Anti-Virus envía los mensajes de alerta 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`

11.5 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`

11.6 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. Dicho mensaje incluye un mensaje predefinido junto con el mensaje de 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 E: Configurar el registro

Nota: Si modifica las opciones de un ordenador en la red, es posible que pierda la configuración al actualizarse desde el CID.

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 F: 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 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 *fuentes primaria de actualización* es la ubicación desde la que se actualizan las estaciones. Puede que necesite credenciales de acceso.

Fuente secundaria de actualización

La *fuentes 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 **Display update configuration** para mostrar la configuración de actualización.

13.4 Configurar las estaciones para utilizar un servidor de actualización

Nota: si desea modificar la configuración de una estación en particular, consulte [Configurar una estación para utilizar un servidor de actualización](#) en la página 32.

En el servidor de actualización deberá actualizar el archivo de configuración de prueba y, posteriormente, aplicar los cambios en el archivo de configuración que las estaciones descargarán en su actualización. En los pasos siguientes, *archivo-conf* representa la ruta de acceso al archivo de configuración de prueba..

En esta sección se describe cómo configurar la fuente *primaria* de actualización. Si desea configurar una fuente *secundaria* de actualización, utilice el parámetro correspondiente. Es decir, **SecondaryUpdateSourcePath** en vez de **PrimaryUpdateSourcePath**.

Para configurar las estaciones para utilizar un servidor de actualización:

1. Establezca la dirección de la fuente primaria de actualización al directorio de actualización central (CID) mediante el parámetro **PrimaryUpdateSourcePath**. Utilice la dirección HTTP o ruta UNC, según su servidor. Por ejemplo, escriba:

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

```
/opt/sophos-av/bin/savconfig -f archivo-conf -c set PrimaryUpdatePassword 'j23rjfwj'
```
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 -c set PrimaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'
```

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

```
/opt/sophos-av/bin/savconfig -f archivo-conf -c set PrimaryUpdateProxyPassword 'fj202jrjf'
```
4. Cuando haya terminado con la configuración, actualice Sophos Anti-Virus:

```
/opt/sophos-av/bin/savupdate
```
5. Ejecute **addcfg** con la opción **-f** y la ruta al archivo de configuración de prueba:

```
/opt/sophos-av/update/cache/Primary-unpacked/addcfg.sh -f archivo-conf
```
6. Copie el directorio `/opt/sophos-av/update/cache/Primary-unpacked/config` al directorio de instalación central.

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

13.5 Configurar una estación para utilizar un servidor de actualización

Nota: si desea modificar la configuración de un grupo de estaciones, consulte [Configurar las estaciones para utilizar un servidor de actualización](#) en la página 31.

1. En el ordenador que desea configurar, escriba:
/opt/sophos-av/bin/savsetup
savsetup le preguntará qué desea hacer.
2. Seleccione la opción para configurar la fuente primaria (o secundaria) de actualización.
savsetup le pedirá los datos de la fuente de actualización.
3. 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.
4. Si es así, pulse Y e introduzca los datos necesarios.

14 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 A: Códigos de retorno del escaneado en demanda](#) en la página 16.

14.1 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 permisos o como root.

14.2 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.

14.3 Sophos Anti-Virus 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.

14.4 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 escanea por defecto. Para más información, consulte [Escanear un tipo de archivo](#) en la página 7.

14.5 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**.

14.6 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.

14.7 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 12.
3. Si se siguen detectando fragmentos de virus, póngase en contacto con soporte técnico de Sophos, vea [Soporte técnico](#) en la página 38.

15 Glosario

| | |
|--|---|
| capa | Cada una de las secciones en el archivo de configuración local con diferentes niveles de prioridad. La configuración en la capa corporativa tiene prioridad sobre la capa de usuario. La configuración en la capa de usuario tiene prioridad sobre la capa de Sophos. |
| CID | Vea "directorio de instalación central" |
| configuración desde el CID | Configuración que se realiza en un archivo del CID mediante savconfig . Cuando las estaciones se actualicen desde el CID, aplicarán la nueva configuración. Este método antes se denominaba "archivo central de configuración". |
| 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 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 y que no actúa como fuente de actualización para otros ordenadores. |
| fuelle primaria de actualización | Ubicación desde la que se actualizan las estaciones. Puede que necesite credenciales de acceso. |
| fuelle secundaria de actualización | Ubicación de actualización alternativa que se utiliza cuando la fuente primaria no está disponible. Puede que necesite credenciales de acceso. |
| servidor de actualización | Componente que descarga las actualizaciones desde Sophos y actualiza las carpetas compartidas de actualización en la red. Sophos Update Manager and EM Library are update servers. |
| 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. |

16 Soporte técnico

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

- Visitar el fórum SophosTalk en <http://community.sophos.com/> para consultar casos similares.
- Visitar la base de conocimiento de Sophos en <http://www.sophos.com/support/>.
- Descargar la documentación correspondiente desde <http://www.sophos.com/support/docs/>.
- Enviar un email a support@sophos.com indicando la versión del producto de Sophos, el sistema operativo y parches aplicados, y el texto exacto de cualquier mensaje de error.

17 Aviso legal

Copyright © 2008-2011 Sophos Limited. Todos los derechos reservados. Ninguna parte de esta publicación puede ser reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea éste electrónico, mecánico, grabación, fotocopia o cualquier otro sin la correspondiente licencia del producto, bajo dichos términos, o sin la previa autorización escrita por parte del propietario.

Sophos y Sophos Anti-Virus son marcas registradas de Sophos Limited. Otros productos y empresas mencionados son marcas registradas de sus propietarios.

ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us¹⁰ know so we can promote your project in the DOC software success stories¹¹.

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies¹² around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE¹³, TAO¹⁴, CIAO¹⁵, and CoSMIC¹⁶ web sites are maintained by the DOC Group¹⁷ at the Institute for Software Integrated Systems (ISIS)¹⁸ and the Center for Distributed Object Computing of Washington University, St. Louis¹⁹ for the development of open-source software as part of the open-source software community²⁰. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters

acknowledgethat any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, WashingtonUniversity, 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. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me²¹ know.

Douglas C. Schmidt²²

References

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. mailto:doc_group@cs.wustl.edu
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>
16. <http://www.dre.vanderbilt.edu/cosmic/>
17. <http://www.dre.vanderbilt.edu/>
18. <http://www.isis.vanderbilt.edu/>
19. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
20. <http://www.opensource.org/>
21. <mailto:d.schmidt@vanderbilt.edu>
22. <http://www.dre.vanderbilt.edu/~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

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.

OpenSSL cryptographic 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 © 1998–2006 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 (ey@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

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

This package is an SSL implementation written by Eric Young (ey@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 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.]

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

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 compression tools

© 1995–2002 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 jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate **not** receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes.

Índice

A

- actualización
 - inmediata 15
- actualizar
 - configurar 30
- alertas
 - correo electrónico 27
 - línea de comandos 10
- alertas en la línea de comandos 10
- alertas por email 27
- análisis de virus 11
- archivos comprimidos
 - escaneados en demanda 7
- archivos infectados
 - desinfectar 12
 - eliminar 12, 13
 - limpieza 12
 - poner en cuarentena 11
- archivos, escaneado en demanda 6

C

- capas, en archivo de configuración 21
- CLI (interfaz de línea de comandos) 4
- códigos de error 16
- códigos de retorno 16
- configuración desde el CID 4, 18
- configurar Sophos Anti-Virus. 4, 18
- copia de seguridad de archivos escaneados 35

D

- desinfectar
 - archivos infectados 12
- directorios, escaneado en demanda 6

E

- efectos secundarios de los virus 13
- ejecutables UNIX, escaneados en demanda 8
- elementos con enlace simbólico, escaneados en demanda 8
- eliminar archivos infectados. 12, 13
- Enterprise Console 4
- escaneado en demanda lento 34

- escaneados en demanda 6
 - archivos 6
 - archivos comprimidos 7
 - directorios 6
 - ejecutables UNIX 8
 - elementos con enlace simbólico 8
 - escaneados programados 23
 - excluir elementos
 - ordenador 6
 - ordenadores remotos 8
 - sistema de archivos 6, 8
 - tipos de archivo 6, 7, 8
- escaneados programados 23
- espacio en disco insuficiente 34
- excluir elementos
 - escaneados en demanda 8

F

- fragmento detectado, virus 36

I

- información de limpieza 11
- interfaz de línea de comandos 4

L

- limpiar archivos infectados 12

N

- No manual entry for ... 33
- no se encuentra la página man 33

O

- ordenador, escaneado en demanda 6
- ordenadores remotos, escaneado en demanda 8

P

- poner en cuarentena los archivos infectados 11

R

- registro de Sophos Anti-Virus
 - configurar 29
 - visualizar 14

registro, Sophos Anti-Virus
 configurar 29
 visualizar 14

S

savconfig 21
savsetup 30
sistema de archivos, escaneado en demanda 6, 8

T

tipos de archivo, escaneado en demanda 6, 7, 8

V

virus
 análisis 11
 detectado 10, 28
 efectos secundarios 13
 fragmento detectado 36
 no se limpian 35