

SOPHOS



sophos **anti-virus**

Guía de inicio

UNIX y Linux

Documento versión 1.0



Acerca de esta guía

En esta guía encontrará información sobre cómo:

- instalar Sophos Anti-Virus en un ordenador UNIX
- añadir las últimas identidades de virus
- escanear el ordenador
- eliminar virus
- actualizar Sophos Anti-Virus
- desinstalar Sophos Anti-Virus.

También le indicará cómo:

- instalar Sophos Anti-Virus en varios ordenadores UNIX
- configurar la notificación centralizada desde estaciones no UNIX
- especificar otras opciones de instalación.

Podrá obtener más información sobre otras opciones de configuración en el *Manual de usuario de Sophos Anti-Virus para UNIX*.

- ❗ Si desea instalar y actualizar Sophos Anti-Virus de forma automática mediante EM Library, consulte la *Guía de inicio de Sophos Anti-Virus* en el CD-ROM de instalación en red de Sophos Anti-Virus.

La documentación de los productos de Sophos está disponible en www.esp.sophos.com/support/docs/ y en los CD-ROM de Sophos.

Contenido

1 Instalar Sophos Anti-Virus	3
2 Añadir los últimos archivos de identidad de virus	7
3 Escanear el ordenador	9
4 Eliminar virus	10
5 Mantener actualizado Sophos Anti-Virus	11
6 Desinstalar Sophos Anti-Virus	14

Apéndices

Apéndice 1 Instalación en múltiples equipos UNIX	16
Apéndice 2 Instalar la notificación centralizada	17
Apéndice 3 Otras opciones de instalación	18

1 Instalar Sophos Anti-Virus

Si dispone de varios ordenadores UNIX en red y desea instalar y actualizar Sophos Anti-Virus desde un directorio central, en vez de realizar la instalación de forma individual, vaya al [apéndice 1](#).

- ❗ El Servidor InterCheck es un daemon que se ejecuta en un servidor UNIX y procesa alertas de virus desde estaciones Windows, Macintosh y OS/2. No es indispensable para que Sophos Anti-Virus funcione y se actualice. Para utilizarlo, deberá determinar un usuario y grupo para el daemon y establecer permisos en un directorio común. Consulte el [apéndice 2](#).

El proceso de instalación de Sophos Anti-Virus consta de tres pasos:

- Extraer los archivos de instalación (apartado 1.1).
- Instalar Sophos Anti-Virus (apartado 1.2).
- Comprobar la configuración del sistema (apartado 1.3).

1.1 Extraer los archivos de instalación

Extraiga los archivos de instalación del CD-ROM suplementario de Sophos Anti-Virus de la siguiente manera:

1. Inicie la sesión con privilegios de root o cambie a "super usuario" e inserte el CD-ROM suplementario de Sophos Anti-Virus.
2. Monte el CD-ROM suplementario de Sophos Anti-Virus y enumere los elementos del subdirectorio `unix`.
3. Seleccione el archivo comprimido para su versión de UNIX.

Para Linux en usuarios Intel:

Si tiene un sistema libc6 más reciente con glibc 2.2 o posterior, como RedHat 7 o posterior, necesitará

```
linux.intel.libc6.glibc.2.2.tar
```

Si tiene un sistema libc6 más antiguo, como RedHat 6, SUSE 6, o Slackware 7, necesitará

```
linux.intel.libc6.tar
```

Si no tiene un sistema libc6, necesitará

```
linux.intel.libc5.tar
```

- ❗ Para comprobar de qué tipo de sistema dispone, vaya al directorio `/lib` y busque un archivo o enlace llamado `libc.so.6` o similar. Si se encuentra presente, significa que tiene un sistema libc6.

Para Linux en usuarios Alpha:

Necesitará

```
linux.alpha.tar
```

4. Copie el archivo comprimido en el directorio `/tmp`.

5. Descomprima el archivo en /tmp de la siguiente forma:

```
cd /tmp
tar xvf linux.intel.libc6.glibc.2.2.tar
```

o

```
cd /tmp
tar xvf linux.intel.libc6.tar
```

o

```
cd /tmp
tar xvf linux.intel.libc5.tar
```

o

```
cd /tmp
tar xvf linux.alpha.tar
```

Se creará un directorio `sav-install` en el directorio /tmp, que contiene los archivos de instalación descomprimidos.

Ahora ya puede instalar Sophos Anti-Virus (apartado 1.2).

1.2 Instalar Sophos Anti-Virus

Para instalar Sophos Anti-Virus **sin** el Servidor InterCheck (recomendado), ejecute el script de instalación:

```
cd sav-install
./install.sh
```

Para instalar Sophos Anti-Virus **con** el Servidor InterCheck, ejecute el script de instalación con la opción `-i` (debe haber seguido las instrucciones en el [apéndice 2.1](#)):

```
cd sav-install
./install.sh -i
```

Para más información sobre todas las opciones con las que puede ejecutar el script de instalación, consulte el [apéndice 3](#).

Es posible que aparezca un aviso sobre la variable de entorno `MANPATH`. Sin embargo, la instalación se llevará a cabo correctamente.

Durante la instalación se copiarán:

- los archivos binarios en `/usr/local/bin`
- las bibliotecas compartidas en `/usr/local/lib`
- los datos de virus en `/usr/local/sav`
- las páginas de manual en `/usr/local/man`

A continuación, compruebe la configuración del sistema (apartado 1.3).

1.3 Comprobar la configuración del sistema

Asegúrese de que las variables de entorno en su archivo de inicio de sesión o su perfil de usuario incluyen los directorios que utiliza Sophos Anti-Virus.

`PATH` debe incluir `/usr/local/bin`

`MANPATH` debe incluir `/usr/local/man`

Si no aparece alguno de estos valores, deberá añadirlos como se muestra a continuación. No modifique ninguno de los valores ya existentes.

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

```
PATH=$PATH:/usr/local/bin
export PATH
```

Si trabaja en el entorno `csh` o `tcsh`, escriba

```
setenv PATH <valores>:/usr/local/bin
```

donde `<valores>` son los valores ya existentes para esta variable.

Debería hacer que estas variables sean de uso general en el sistema. Para ello, modifique `/etc/login` o `/etc/profile`.

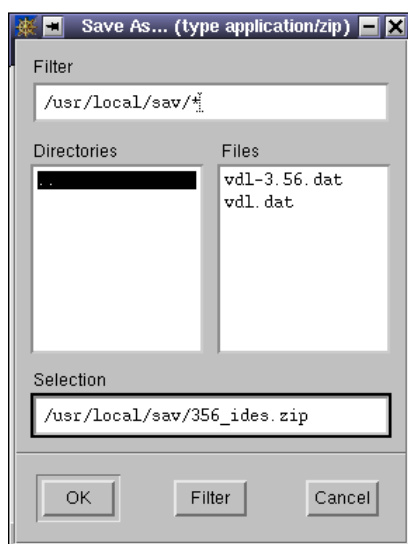
- ❗ **Si no dispone de un archivo de inicio de sesión, deberá establecer estos valores cada vez que inicie la sesión.**

Ahora puede añadir las últimas identidades de virus (apartado 2).

2 Añadir los últimos archivos de identidad de virus

❓ Los archivos de **identidad (IDE) de virus** permiten a Sophos Anti-Virus detectar nuevos virus. Necesitará los archivos IDE para proteger su ordenador contra los virus que han aparecido desde la última actualización de su versión de Sophos Anti-Virus.

1. Inicie su navegador de Internet y abra la página Web de Sophos (www.esp.sophos.com/downloads/ide).
2. Descargue el archivo comprimido con las últimas identidades de virus.
3. Extraiga el contenido del archivo en el directorio `usr/local/sav`.



💡 También es posible descargar las IDE de forma individual.

💡 En la base de conocimiento de Sophos (www.esp.sophos.com/support/knowledgebase) encontrará más información sobre la descarga e instalación de archivos IDE. Si utiliza Internet Explorer 5.0, lea el artículo acerca de la razón por la que los archivos IDE adquieren una extensión adicional al descargarlos.

Si necesita más ayuda sobre la descarga de IDE, póngase en contacto con el equipo de soporte técnico de Sophos.

Ya ha terminado la instalación de Sophos Anti-Virus.

Si *instala* Sophos Anti-Virus con notificación centralizada, ahora puede activar el Servidor InterCheck ([apéndice 2.2](#)). Si *actualiza* Sophos Anti-Virus con notificación centralizada, ya ha finalizado la actualización.

Para obtener más información, consulte los siguientes apartados de esta guía:

- El [apartado 3](#) describe cómo escanear el ordenador.
- El [apartado 4](#) describe cómo eliminar virus.
- El [apartado 5](#) describe cómo actualizar Sophos Anti-Virus.
- El [apartado 6](#) describe cómo desinstalar Sophos Anti-Virus.

3 Escanear el ordenador

Para escanear el equipo local, escriba

```
sweep /
```

Para escanear un directorio o archivo, indique la ruta de acceso, como por ejemplo

```
sweep /usr/mydirectorio/archivo
```

Tras un escaneado, verá un mensaje similar al siguiente.

Si Sophos Anti-Virus detecta algún virus, lo indicará en una línea que empieza por los caracteres >>> seguidos por Virus o Virus Fragment:

```
SWEEP virus detection utility
Version 3.90.0 [Linux/Intel]
Virus data version 3.90, February 2005
Includes detection for 99603 viruses, trojans and worms
Copyright (c) 1989-2005 Sophos Plc, www.sophos.com

System time 09:35:55, System date 16 February 2005

Quick Sweeping

>>> Virus 'EICAR-AV-Test' found in file /home/source/eicar.src

33 files swept 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, email support@sophos.com
or telephone +44 1235 559933
End of Sweep.
```

Para mostrar la ayuda de Sophos Anti-Virus, escriba

```
sweep -h
```

4 Eliminar virus

El método de desinfección de virus con Sophos Anti-Virus depende del tipo de elemento infectado: un programa o un documento.

4.1 Para desinfectar un documento

Para desinfectar un documento específico, escriba

```
sweep <archivo> -di
```

donde <archivo> es la ruta al documento infectado.

También es posible realizar un escaneo genérico del equipo con la desinfección de documentos activada:

```
sweep / -di
```

En cualquier caso, Sophos Anti-Virus solicitará confirmación antes de llevar a cabo la desinfección de cualquier documento.

- ❗ Debería comprobar cada archivo tras la desinfección. Sophos Anti-Virus puede eliminar el virus pero no sus efectos secundarios. Consulte la descripción del virus en la Web de Sophos.

4.2 Para desinfectar un programa

Para desinfectar un programa, desinstale el programa y sustitúyalo con una copia de seguridad o con el original.

Para desinfectar un programa específico, escriba

```
sweep <archivo> -remove
```

donde <archivo> es el programa infectado.

También es posible realizar un escaneo genérico del sistema con la opción de eliminar archivos infectados activada:

```
sweep / -remove
```

En cualquier caso, Sophos Anti-Virus solicitará confirmación antes de llevar a cabo la desinfección de cualquier programa.

5 Mantener actualizado Sophos Anti-Virus

Debe actualizar Sophos Anti-Virus a menudo para permitir que detecte los últimos virus. Actualícelo

- cada mes, cuando se publica la nueva versión de Sophos Anti-Virus (apartado 5.1)
- siempre que aparezca un virus que suponga un riesgo importante para su ordenador (apartado 5.2).

5.1 Para actualizar Sophos Anti-Virus cada mes

Cada mes se publica una nueva versión de Sophos Anti-Virus. Para saber cuándo, consulte la página de fechas de lanzamiento de Sophos Anti-Virus en la Web de Sophos (www.esp.sophos.com/downloads/release_dates/).

Tan pronto como se haya publicado la nueva versión, siga los siguientes pasos:

- Descargar y extraer los archivos de instalación (apartado 5.1.1).
- Actualizar Sophos Anti-Virus (apartado 5.1.2).
- Descargar los últimos archivos IDE (apartado 2).

5.1.1 Descargar y extraer los archivos de instalación

Descargue y extraiga los archivos de instalación desde la Web de Sophos de la siguiente manera:

1. Borre todos los archivos *.ide de `/usr/local/sav`.
2. Inicie la sesión con privilegios de root o cambie a "super usuario".

3. Vaya a la página de descarga de productos de Sophos (www.esp.sophos.com/support/updates). Guarde el archivo comprimido para su versión de UNIX en el directorio `/tmp`.

Para Linux en usuarios Intel:

Si tiene un sistema libc6 más reciente con glibc 2.2 o posterior, como RedHat 7 o posterior, necesitará


Linux en Intel con libc6 (glibc 2.2)

Si tiene un sistema libc6 más antiguo, como RedHat 6, SUSE 6, o Slackware 7, necesitará

Linux en Intel con libc6

Si no tiene un sistema libc6, necesitará

Linux en Intel con libc5

-  Para comprobar de qué tipo de sistema dispone, vaya al directorio `/lib` y busque un archivo o enlace llamado `libc.so.6` o similar. Si se encuentra presente, significa que tiene un sistema libc6.

Para Linux en usuarios Alpha:

Necesitará

Linux en Alpha

4. Descomprima el archivo en `/tmp` de la siguiente forma:

```
cd /tmp
uncompress linux.intel.libc6.glibc.2.2.tar.Z
tar xvf linux.intel.libc6.glibc.2.2.tar
```

o

```
cd /tmp
uncompress linux.intel.libc6.tar.Z
tar xvf linux.intel.libc6.tar
```

o

```
cd /tmp
uncompress linux.intel.libc5.tar.Z
tar xvf linux.intel.libc5.tar
```

o

```
cd /tmp
uncompress linux.alpha.tar.Z
tar xvf linux.alpha.tar
```

Se creará un directorio `sav-install` en el directorio `/tmp`, que contiene los archivos de instalación descomprimidos.

Ahora ya puede actualizar Sophos Anti-Virus (apartado 5.1.2).

5.1.2 Actualizar Sophos Anti-Virus

Para actualizar Sophos Anti-Virus **sin** el Servidor InterCheck (recomendado), ejecute el script de instalación:

```
cd sav-install
./install.sh
```

Para actualizar Sophos Anti-Virus **con** el Servidor InterCheck, ejecute el script de instalación con la opción `-i`:

```
cd sav-install
./install.sh -i
```

Para más información sobre todas las opciones con las que puede ejecutar el script de instalación, consulte el [apéndice 3](#).

Es posible que aparezca un aviso sobre la variable de entorno `MANPATH`. Sin embargo, la actualización se llevará a cabo correctamente.

Durante la instalación se copiarán:

- los archivos binarios en `/usr/local/bin`
- las bibliotecas compartidas en `/usr/local/lib`
- los datos de virus en `/usr/local/sav`
- las páginas de manual en `/usr/local/man`

Ahora puede descargar el último archivo IDE ([apartado 2](#)). De este modo, su ordenador estará protegido contra los virus que han aparecido después de que se publicara la última versión de Sophos Anti-Virus.

5.2 Para actualizar cuando se detecta un virus importante

Este tipo de actualización se lleva a cabo entre actualizaciones mensuales de Sophos Anti-Virus.

Cuando aparezca un virus que suponga un riesgo importante para su equipo, vaya a la página de descargas de IDE de la Web de Sophos (www.esp.sophos.com/downloads/ide) y descargue la IDE del virus en `usr/local/sav`.

- 🔔 Para recibir notificaciones por email sobre IDE y otras alertas, puede registrarse en www.esp.sophos.com/virusinfo/notifications.

6 Desinstalar Sophos Anti-Virus

1. Desinstale el programa `sweep` de `/usr/local/bin`.
2. Desinstale las bibliotecas de Sophos Anti-Virus (`libsavi.*`) de `/usr/local/lib`.
3. Desinstale el directorio de datos de Sophos Anti-Virus `/usr/local/sav` y su contenido.
4. Desinstale el archivo de configuración `/etc/sav.conf`.
5. Desinstale la página de manual `/usr/local/man/man1/sweep.1`.

Ya ha desinstalado Sophos Anti-Virus del ordenador.

Apéndices

Instalación en múltiples equipos UNIX

Activar la notificación centralizada

Otras opciones de instalación

Apéndice 1 Instalación en múltiples equipos UNIX

Si dispone de varios ordenadores UNIX en red, es posible instalar y actualizar Sophos Anti-Virus en todos ellos desde un directorio central.

❗ Para este proceso se parte de la base de una relación de confianza entre equipos.

1. En un equipo UNIX, cree un archivo compartido al que tengan acceso el resto de ordenadores.
2. Descomprima en este directorio los archivos de la distribución de Sophos Anti-Virus para UNIX.

Si existen equipos en la red con diferentes sistemas UNIX (por ejemplo, Linux y FreeBSD), descomprima los archivos correspondientes en diferentes directorios.

3. Utilice ssh para ejecutar el script install.sh en los equipos UNIX desde el directorio compartido. Por ejemplo, escriba:

```
ssh -l [usuario] [host] / .install.sh
```

donde [usuario] es su nombre de usuario y [host] es el equipo en el que desea instalar Sophos Anti-Virus.

En cada caso, asegúrese de ejecutar el archivo install.sh correspondiente a su sistema operativo.

- ❗ En distribuciones antiguas de UNIX, es posible que ssh no esté incluido. Puede utilizar rsh, aunque es menos seguro.
- ❗ Puede incluir el paso 3 en un script que se ejecute desde uno de sus equipos UNIX.

Apéndice 2 Instalar la notificación centralizada

El Servidor InterCheck es un daemon que se ejecuta en servidores UNIX y recibe las alertas de virus procedentes de equipos Windows, Macintosh y OS/2. Para utilizarlo, debe crear un usuario y un grupo para este daemon y establecer permisos en un directorio común.

Para instalar Sophos Anti-Virus con el Servidor InterCheck, tendrá que realizar los siguientes pasos:

- Preparar la instalación (apéndice 2.1).
- Extraer los archivos de instalación (apartado 1.1).
- Instalar Sophos Anti-Virus (apartado 1.2).
- Comprobar la configuración del sistema (apartado 1.3).
- Añadir las últimas identidades de virus (apartado 2).
- Activar la notificación centralizada (apéndice 2.2).

Apéndice 2.1 Preparar la instalación

Antes de iniciar la instalación, debe

- crear un grupo de usuarios con el nombre 'sweep'
- crear un usuario con el nombre 'sweep'. El grupo primario de este usuario debe ser 'sweep', y el usuario no podrá iniciar la sesión en una terminal. Puede establecer la shell como `/bin/false`. Consulte la documentación de su sistema UNIX.

Ahora puede proceder a extraer los archivos de instalación (apartado 1.1).

Apéndice 2.2 Activar la notificación centralizada

Para utilizar el Servidor InterCheck:

1. Exporte el directorio `/var/spool/intercheck` de manera que sea visible desde equipos no UNIX.
2. Para activar el Servidor InterCheck, escriba:

```
icheckd
```

Para más información sobre cómo controlar y configurar la notificación centralizada, vea el *Manual de usuario de Sophos Anti-Virus para UNIX*.

Apéndice 3 Otras opciones de instalación

Es posible especificar el directorio de instalación y los archivos de Sophos Anti-Virus que se instalan.

Para realizar una instalación no predeterminada, ejecute el script de instalación `install.sh` con las siguientes opciones.

-d [prefijo]

Instala el programa, las bibliotecas, la información de virus y las páginas de manual en `[prefijo]/bin`, `[prefijo]/lib`, `[prefijo]/sav` y `[prefijo]/man`.

Vea las opciones `-b`, `-l`, `-m` y `-s` para especificar diferentes directorios.

-b [directorio]

Instala el programa de escaneo en `[directorio]`.

Los otros archivos se instalarán en el directorio predeterminado, a menos que utilice las opciones `-l`, `-m` o `-s`.

-l [directorio]

Instala la biblioteca de Sophos Anti-Virus en `[directorio]`.

Los otros archivos se instalarán en el directorio predeterminado, a menos que utilice las opciones `-b`, `-m` o `-s`.

-m [directorio]

Instala las páginas `man` en `[directorio]`.

Los otros archivos se instalarán en el directorio predeterminado, a menos que utilice las opciones `-b`, `-l` o `-s`.

-s [directorio]

Instala la información de virus en `[directorio]`.

Los otros archivos se instalarán en el directorio predeterminado, a menos que utilice las opciones `-b`, `-l` o `-m`.

-i [directorio]

Instala los archivos del Servidor InterCheck en `[directorio]`. Si no especifica ningún directorio, se utilizará el valor en `/etc/ichckd.conf` o el predeterminado `/var/spool/intercheck`. También se copiarán las páginas `man` e `ichckd` binary.

-ni

No instala el Servidor InterCheck.

-ssi

Detiene e inicia el Servidor InterCheck tras la instalación (por defecto implica `-i`).

-nssi

No detiene e inicia el Servidor InterCheck tras la instalación.

-h

Muestra la ayuda en pantalla.

-v

Operación recursiva, Muestra la ubicación de cada archivo que se instala.

Soporte técnico

Si necesita soporte técnico, diríjase a

www.esp.sophos.com/support

Si se pone en contacto con soporte técnico, intente aportar toda la información posible, incluyendo el número de versión del programa de Sophos, sistemas operativos y niveles de actualización y el texto exacto de los mensajes de error.

Copyright © 2005 Sophos Plc

Reservados todos los derechos. Ninguna parte de esta publicación puede ser reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea éste electrónico, químico, mecánico, electro-óptico, grabación, fotocopia o cualquier otro, a menos que disponga de una licencia válida, en cuyo caso puede reproducirse según los términos del acuerdo de licencia, o con la previa autorización escrita por parte del propietario.

Todos los nombres son marcas registradas de sus propietarios a menos que se especifique lo contrario. *InterCheck* y *Sophos* son marcas registradas de Sophos Plc.