SOPHOS

Cybersecurity made simple.

Sophos for Virtual Environments

guía de configuración para usuarios con Enterprise Console

Contenido

1 Acerca de esta guía

En esta guía se explica cómo configurar Sophos for Virtual Environments.

Esta guía parte de la base que utiliza Sophos Enterprise Console para gestionar su software de seguridad.

Nota
Si utiliza Sophos Central, consulte la edición Sophos Central de esta guía de configuración.

2 Configurar políticas

Para configurar Sophos for Virtual Environments, se utilizan las políticas de Sophos Enterprise Console.

Al incluir su Sophos Security VM en un grupo de Sophos Enterprise Console, se aplican políticas que protegen y actualizan los equipos virtuales invitados.

Recomendamos que utilice la configuración predeterminada, ya que ofrece un equilibrio óptimo entre protección y rendimiento del sistema. No obstante, puede cambiar la configuración en estas políticas:

- Antivirus y HIPS
- Actualización

Las demás políticas de Sophos Enterprise Console no son aplicables al Sophos Security VM.

Nota
Todos los equipos virtuales invitados protegidos por un Sophos Security VM utilizan las mismas políticas que el Sophos Security VM. Para aplicar una política distinta a algunos equipos virtuales invitados, muévalos a otro Sophos Security VM de otro grupo de Sophos Enterprise Console. Después aplique una política diferente a este grupo. Para obtener instrucciones sobre cómo mover equipos virtuales invitados, consulte la Guía de inicio de Sophos for Virtual Environments para usuarios de Enterprise Console.

Para ver la lista de todos los equipos virtuales invitados administrados por un Sophos Security VM, consulte Ver equipos virtuales protegidos (página 10).

2.1 Política antivirus y HIPS

Por defecto, Sophos Security VM hace lo siguiente:

- Escanea los archivos cuando se accede a ellos en los equipos virtuales invitados.
- Bloquea el acceso a los archivos infectados.
- Limpia automáticamente las amenazas detectadas.

Las opciones de configuración de la política antivirus y HIPS no son todas aplicables al Sophos Security VM. En esta sección se describe qué opciones de escaneado se aplican y pueden configurarse de forma centralizada.

Para obtener más información sobre la configuración, consulte la ayuda de Sophos Enterprise Console.

Escaneado en acceso

Las opciones del escaneado en acceso son compatibles según se detalla a continuación. El control de comportamiento no es compatible.

Para abrir las páginas de configuración del escaneado en acceso en Sophos Enterprise Console:

1. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
2. Haga doble clic en la política que desee modificar.

3. En el cuadro de diálogo **Política antivirus y HIPS**, busque el panel **Escaneado en acceso**. Junto a **Activar el escaneado en acceso**, haga clic en **Configurar**.

   Aparece el cuadro de diálogo **Configuración del escaneado en acceso**.

Las opciones de cada ficha se muestran a continuación.

Escaneado	¿Compat	Notas
Comprobar archivos al leer/cambiar el nombre/escribir	No	Si están activadas una o varias de las opciones, el Sophos Security VM realiza el escaneado en las tres situaciones. Si las tres opciones están desactivadas, el sistema no está protegido.
Detectar adware y aplicaciones potencialmente no deseadas/archivos sospechosos	No	
Permitir el acceso a unidades con sectores de arranque infectados	No	
Escanear dentro de archivos comprimidos (no recomendado)	Sí	
Escanear memoria del sistema	No	

Extensiones	¿Compatible?
Escanear todos los archivos (no recomendado)	Sí
Escanear sólo los archivos ejecutables o vulnerables	Sí
Extensiones adicionales a escanear	Sí
Escanear archivos sin extensión	Sí
Excluir tipos de archivo del escaneado	Sí

Exclusiones	¿Compat	Notas
Ficha **Exclusiones de Windows**	Sí	Para excluir una carpeta, se debe especificar la ruta completa, incluida la letra de la unidad o el nombre del recurso compartido de red, por ejemplo, `"C:\Herramientas\registros\»` o `"\\Servidor\Herramientas\registros\»`. Para obtener más información, consulte el apartado sobre la configuración de la política antivirus y HIPS de la ayuda de Sophos Enterprise Console.
Ficha **Exclusiones de Mac**	No	

Exclusiones	¿Compat	Notas
Ficha **Exclusiones de Linux/UNIX**	No	

Limpieza	¿Compat ?	Notas
Limpieza de virus/programas espía	Sí	Las acciones alternativas que deben aplicarse no tienen efecto si la limpieza falla. El Sophos Security VM siempre deniega el acceso a los elementos infectados.
Limpieza de archivos sospechosos	No	

Para más información sobre la configuración y qué opciones escoger, consulte la ayuda de Sophos Enterprise Console.

Escaneado programado

Para configurar o editar un escaneado programado:

- En el cuadro de diálogo **Política antivirus y HIPS**, busque el panel **Escaneado programado**.
- Haga clic en **Añadir** o **Editar**.

También puede especificar tipos de archivo adicionales que quiera incluir o excluir del escaneado haciendo clic en **Extensiones y exclusiones**.

Las opciones del escaneado programado son compatibles según se detalla a continuación. **Añadir/editarConfiguración del escaneado programado**.

Configuración del escaneado programado	¿Compatib	Notas
Discos duros locales	Sí	
Disquetes y unidades extraíbles	Sí	
Unidades de CD-ROM	Sí	
Horario de escaneado	Sí	El Sophos Security VM inicia el escaneado a la hora programada, pero por defecto solo escanea dos equipos virtuales invitados a la vez, para limitar el efecto sobre el rendimiento del sistema.

Añadir/editarConfiguración del escaneado programadoConfigurarConfiguración de escaneado y limpieza

Escaneado y limpieza	¿Compat	Notas
Ficha **Escaneado**		

Escaneado y limpieza	¿Compat	Notas
Detectar adware y aplicaciones potencialmente no deseadas/archivos sospechosos/rootkits	No	
Escanear archivos comprimidos	Sí	
Escanear memoria del sistema	No	Por defecto, se escanea la memoria del sistema. Esta opción no puede configurarse.
Ejecutar escaneado con baja prioridad	No	
Ficha **Limpiar**		
Limpieza de virus/programas espía	Sí	El Sophos Security VM no limpia automáticamente disquetes, unidades de CD ni ubicaciones de red. Las acciones para los elementos infectados no tienen efecto si no se ha ejecutado la limpieza. El Sophos Security VM siempre registrará el evento si la limpieza no se ha ejecutado.
Limpieza de adware y aplicaciones potencialmente no deseadas	No	
Limpieza de archivos sospechosos	No	

Extensiones y exclusionesExtensiones y exclusiones del escaneado programado.

Extensiones y exclusiones	¿Compat	Notas
Ficha **Extensiones**		
Escanear todos los archivos (no recomendado)	Sí	
Escanear sólo los archivos ejecutables o vulnerables	Sí	
Extensiones adicionales a escanear	Sí	
Escanear archivos sin extensión	Sí	
Excluir tipos de archivo del escaneado	Sí	
Ficha **Exclusiones**		

Extensiones y exclusiones	¿Compat	Notas
Ficha **Exclusiones de Windows**	Sí	Para excluir una carpeta del escaneado, se debe especificar la ruta completa, incluida la letra de la unidad o el nombre del recurso compartido de red, por ejemplo, `C:\Herramientas\registros\` o `\\Servidor\Herramientas\registros\`. Para más información, consulte la ayuda de Sophos Enterprise Console.
Ficha **Exclusiones de Mac**	No	
Ficha **Exclusiones de Linux/UNIX**	No	

Protección activa de Sophos

Live Protection compara los archivos sospechosos con la información de malware más reciente de la base de datos de SophosLabs.

Opción	¿Compatible?
Activar protección activa	Sí
Activar protección activa para el escaneado en demanda	Sí
Enviar automáticamente muestras de archivos a Sophos	No

Protección web

Incompatible.

Autorización

La autorización, así como la detección, de adware y otras aplicaciones potencialmente no deseadas (PUA) no es compatible.

Notificación

Solo es compatible la notificación por correo electrónico.

2.1.1 Extensiones de archivos escaneados

Los archivos con las extensiones siguientes se escanean por defecto.

386 3gr add ani asp aspx asx bat cab chm class cmd com cpl dbx dex dll dmd doc docm	docx dot drv eml exe fas flt fon fot hlp ht? hta html i13 ifs inf ini jar jpeg jpg	jpz js jse lnk lsp mnl mod mpd mpp mpt mso mui nws o ocx ov? pdf pdr php pif	pl pot pps ppt pptm pptx prc ps1 psm1 rtf scr sh shb shs src swf sys tif tiff vb?	vlx vs? vxd wbk wma wmf wsf xl? xlsm xlsx xsn zip zipx

Las siguientes extensiones adicionales se escanean por defecto si la opción **Escanear dentro de archivos comprimidos** de la política antivirus y HIPS aplicada al Sophos Security VM está activada.

7z 7zip ??_ a arj bin bz2 gz hqx hxs	lha lzh rar rpm tar taz tbz tbz2 tgz uue z

Puede añadir extensiones específicas para que sean escaneadas o excluir extensiones del escaneado según se describe en la ayuda de Sophos Enterprise Console en la sección de configuración de la política antivirus y HIPS.

2.2 Política de actualización

Todas las opciones de configuración de la política de actualización de Sophos Enterprise Console son aplicables al Sophos Security VM.

Para obtener más información, consulte el apartado **Actualizar ordenadores > Configurar la política de actualización** de la ayuda de Sophos Enterprise Console.

3 Comprobar que los equipos virtuales invitados están protegidos

En esta sección se explica cómo puede comprobar si sus equipos virtuales invitados están protegidos. Puede:

- Comprobar la configuración de protección en un equipo virtual invitado.
- Probar el escaneado en tiempo real en un equipo virtual invitado.
- Solucionar problemas del escaneado en tiempo real.

3.1 Comprobar la configuración de protección

Para comprobar si un equipo virtual invitado está protegido:

1. Vaya al equipo virtual invitado y busque **Seguridad y mantenimiento** en el menú de inicio. Si no encuentra esta opción, busque **Centro de actividades**.

   Atención
   Si no encuentra ninguna de estas dos opciones, significa que el equipo virtual invitado no ofrece el Centro de seguridad de Windows. Debe comprobar si el equipo virtual invitado está protegido siguiendo los pasos que se indican en Probar el escaneado en tiempo real (página 8).

2. Haga clic en la flecha desplegable junto a **Seguridad**. Debería ver que Sophos for Virtual Environments está habilitado.

   Nota
   Si no lo está, consulte Solución de problemas del escaneado en acceso (página 9).

3.2 Probar el escaneado en tiempo real

El escaneado en tiempo real es el principal método de protección contra amenazas. Al abrir, escribir, mover o cambiar de nombre un archivo, el Sophos Security VM escanea el archivo y concede acceso al mismo solo si no supone una amenaza. Al ejecutar un programa, el Sophos Security VM escanea el archivo ejecutable y cualquier otro archivo que cargue.

Importante
Asegúrese de que Sophos Endpoint para Windows no esté instalado en ninguno de los equipos virtuales invitados que están protegidos con un Sophos Security VM.

Para comprobar que el equipo virtual de seguridad realiza el escaneado en acceso de archivos:

1. Vaya a http://2016.eicar.org/86-0-Intended-use.html y utilice el texto de prueba EICAR. Copie el texto de prueba EICAR en un archivo nuevo. Asigne un nombre al archivo con la extensión .com y guárdelo en uno de los equipos virtuales invitados.
2. Pruebe a acceder al archivo desde el equipo virtual invitado.
3. En Sophos Enterprise Console, en la lista de ordenadores en la parte inferior, haga clic en **Estado**.
4. En la lista de ordenadores, busque el Sophos Security VM.
   - Si tiene activada la limpieza automática, haga doble clic en el Sophos Security VM para abrir **Detalles del ordenador**. En la sección "Historial", debe ver que se ha detectado y limpiado EICAR.
   - Si no tiene activada la limpieza automática, debe ver una alerta en la columna **Alertas y errores**. Haga clic con el botón derecho del ratón en el Sophos Security VM. En **Resolver alertas y errores**, debería ver que se ha detectado EICAR, pero que no se ha limpiado.

Si no se ha detectado EICAR, consulte Solución de problemas del escaneado en acceso (página 9). Si no se limpia EICAR, simplemente elimínelo.

3.3 Solución de problemas del escaneado en acceso

Si el escaneado en acceso no funciona:

1. Asegúrese de que el Sophos Security VM esté en un grupo cuya política antivirus especifique que el escaneado en acceso debe estar activado:
   a) En Sophos Enterprise Console, en **Grupos**, haga clic con el botón derecho en el grupo que contiene el Sophos Security VM y seleccione **Ver/editar políticas del grupo**. Compruebe qué política antivirus y HIPS usan.
   b) En **Políticas**, haga doble clic en **Antivirus y HIPS**.
   c) Haga doble clic en la política que usa el grupo que contiene el Sophos Security VM.
   d) En **Escaneado en acceso**, asegúrese de que la opción **Activar el escaneado en acceso** se encuentra activada. Haga clic en **Aceptar**.
   e) En la lista de ordenadores, haga clic con el botón derecho en el Sophos Security VM y seleccione **Cumplir con**. Seleccione **Política antivirus y HIPS del grupo**.
   f) Compruebe que el Sophos Security VM cumpla con la política.
2. Asegúrese de que el equipo virtual invitado esté protegido. Vaya al host del Sophos Security VM y consulte el archivo de registro.
3. Asegúrese de que el Centro de seguridad de Windows muestre el equipo virtual invitado como protegido por Sophos for Virtual Environments.
4. Compruebe que no haya reinicios pendientes solicitados por las actualizaciones de Microsoft, ya que pueden impedir que se complete la instalación de Sophos Guest VM Agent.
5. Compruebe que no haya otros productos antivirus instalados. En las plataformas de servidor en que no está presente el centro de seguridad, compruebe que Windows Defender no esté activo. Recuerde que no puede utilizar Sophos for Virtual Environments para proteger equipos virtuales invitados que ejecutan otros productos antivirus.
6. Si el problema persiste, póngase en contacto con soporte técnico de Sophos.

4 Ver equipos virtuales protegidos

Puede ver todos los equipos virtuales invitados que están protegidos por un Sophos Security VM.

1. Desplácese hasta el Sophos Security VM. Debe utilizar el Explorador de Windows y la dirección IP.
2. Haga doble clic en la unidad compartida **Registros**.
3. Cuando se le solicite, introduzca sus credenciales.
   - El nombre de usuario es "sophos".
   - La contraseña es la contraseña de acceso que estableció cuando instaló el Sophos Security VM.
4. Abra **ProtectedGVMs.log** para ver los equipos virtuales invitados protegidos.

> **Nota**
> El archivo ProtectedGVMs.log solo aparece cuando el Sophos Security VM empieza a proteger los equipos virtuales invitados.

5 Escanear equipos virtuales invitados

Sophos for Virtual Environments escanea los archivos en acceso, es decir, cuando se abren y se cierran (si tiene activado el escaneado en acceso en su política).

Un Sophos Security VM también puede realizar un escaneado completo de todos los equipos virtuales invitados que administra. Puede realizar el escaneado de forma inmediata o de forma programada.

El escaneado remoto puede detectar amenazas, pero no limpiarlas.

Nota
El Sophos Security VM no puede ejecutar un escaneado si todavía está en el grupo **No asignados** de Sophos Enterprise Console. Debe estar en un grupo en el que haya aplicado políticas.

Nota
El Sophos Security VM realiza los escaneados por fases para impedir la sobrecarga del hipervisor. De forma predeterminada, se escanean siempre dos equipos virtuales invitados a la vez. Escanear un gran número de equipos virtuales invitados puede tardar bastante tiempo.

- Para realizar un escaneado remoto de todos los equipos virtuales invitados de forma inmediata:
  a) Vaya a Sophos Enterprise Console y localice el Sophos Security VM en la lista de ordenadores.
  b) Haga clic con el botón derecho sobre Sophos Security VM y seleccione **Escaneado remoto**.

  Sugerencia
  Si lo prefiere, en el menú **Acciones**, seleccione **Escaneado remoto**.

- Para realizar un escaneado remoto de todos los equipos virtuales invitados de forma programada:
  a) Vaya a Sophos Enterprise Console.
  b) Cree un escaneado programado, como se describe en la ayuda de Sophos Enterprise Console en la sección sobre la configuración de la política antivirus y HIPS.
- Para ver el resultado de los escaneados completados:
  a) En Sophos Enterprise Console, en la lista de ordenadores de la parte inferior derecha de la ventana, haga doble clic en el Sophos Security VM para abrir **Detalles del ordenador**.

6 Información sobre una amenaza

Para obtener información sobre una amenaza y cómo limpiarla:

1. En Sophos Enterprise Console, en la lista de ordenadores de la parte inferior derecha de la ventana, haga doble clic en el Sophos Security VM para abrir **Detalles del ordenador**.
   En la sección **Historial**, se enumeran los **Elementos detectados**. El nombre de la amenaza se muestra en **Nombre** y el nombre del equipo virtual afectado y el nombre del archivo detectado se muestran en **Detalles**.
2. Haga clic en el nombre de la amenaza.
   Se abrirá el sitio web de Sophos, donde encontrará una descripción del elemento y qué hacer para solucionar el problema.

7 Limpiar una amenaza

Sophos Security VM puede limpiar amenazas automáticamente y también puede limpiarlas usted manualmente.

7.1 Limpieza automática

El Sophos Security VM puede limpiar automáticamente las amenazas que detecta.

Nota
La limpieza automática no está disponible en el caso de CD u otros sistemas de archivos o medios de solo lectura, ni en sistemas de archivos remotos.

¿Qué sucede cuando se produce una limpieza automática?

Cuando se detecta una amenaza y se limpia automáticamente, Sophos Enterprise Console hace lo siguiente:

- Muestra que se ha bloqueado la amenaza (véase la sección "Historial" de **Detalles del ordenador**).
- Muestra una alerta que indica cuál es la amenaza y si se puede limpiar.
- Elimina la alerta si la limpieza se realiza correctamente y la marca como "Imposible limpiar" si la limpieza falla.

A veces puede ser necesario reiniciar un equipo virtual invitado para que se complete la limpieza. En este caso, se muestra la alerta "Es necesario reiniciar" para el Sophos Security VM. Para comprobar a qué equipo virtual invitado corresponde la alerta, haga doble clic en el Sophos Security VM para abrir **Detalles del ordenador** y ver la descripción de la alerta en **Alertas y errores pendientes**.

7.2 Limpieza manual

Las amenazas pueden limpiarse de forma manual.

Una vez haya eliminado la amenaza, debe borrar la alerta de Sophos Enterprise Console.

7.2.1 Limpiar el equipo virtual afectado

Para la limpieza manual, debe restaurar el equipo virtual invitado. Tenga en cuenta que perderá los datos al hacerlo. Utilice uno de estos métodos:

- Revertir el equipo virtual afectado a un estado anterior limpio.
- Eliminar el equipo virtual afectado y volver a crearlo.

Asegúrese de que la imagen de plantilla tenga las herramientas de Sophos necesarias instaladas (consulte la Guía de inicio de Sophos for Virtual Environments para usuarios de Enterprise Console).

Independientemente del método usado, ejecute un escaneado completo del equipo virtual posteriormente para asegurarse de que está limpio.

7.2.2 Quitar una alerta en Sophos Enterprise Console

Tras limpiar el equipo virtual afectado, quite la alerta en Sophos Enterprise Console:

1. En Sophos Enterprise Console, en la lista de ordenadores, haga clic con el botón derecho en el Sophos Security VM y seleccione **Resolver alertas y errores**.
2. En **Resolver alertas y errores**, en la ficha **Alertas**, seleccione la alerta y haga clic en **Quitar**.

La alerta desaparecerá de Sophos Enterprise Console.

8 Alertas

En esta sección se describen las alertas que envía el Sophos Security VM cuando se detectan y se limpian amenazas.

Alertas de amenazas

Si Sophos Security VM detecta alguna amenaza en un equipo virtual invitado, verá estas alertas en Sophos Enterprise Console:

- Se muestra una alerta en el panel de control.
- Aparece un icono rojo de alerta en la lista de ordenadores, en la ficha **Estado**, junto al Sophos Security VM en **Alertas y errores**.

Si la amenaza se limpia automáticamente, la alerta relativa a la amenaza se quita de Sophos Enterprise Console.

Para saber a qué equipo virtual invitado es aplicable la alerta, haga doble clic en el Sophos Security VM en la lista de ordenadores. En **Detalles del ordenador**, en **Alertas y errores pendientes**, busque la descripción de la alerta. Se muestran los detalles del equipo virtual invitado, seguidos de la ruta de la amenaza, del siguiente modo:

```
NombreEquipo(dirección IP)/C:\amenaza.exe
```

Si el Sophos Security VM detecta una amenaza cuando el usuario intenta acceder a un archivo, también puede aparecer un mensaje en el equipo virtual invitado indicando al usuario que no se puede acceder al archivo. Aunque este depende de la aplicación usada para acceder al archivo.

Alertas después de la limpieza

Si la amenaza se limpia, la alerta se quita de Sophos Enterprise Console.

También se informa de la limpieza en Sophos Enterprise Console. Para ver el informe, haga doble clic en el Sophos Security VM en la lista de ordenadores para abrir **Detalles del ordenador** y busque **Historial**.

Si la amenaza se ha eliminado parcialmente, pero es necesario reiniciar el equipo virtual para completar la limpieza, se mostrará la alerta "Requiere reinicio".

9 Registros

Puede consultar los registros en un equipo virtual invitado.

En los equipos virtuales, los registros se escriben en el registro de eventos de aplicación de Windows. Encontrará el registro en **Registros de aplicaciones y servicios > Sophos > SVE**.

En un Sophos Security VM, puede recopilar los registros y recuperarlos desde el directorio de registros compartidos. Para ello:

1. Abra una consola en el Sophos Security VM.
2. Inicie sesión:
   - El nombre de usuario es "sophos".
   - La contraseña es la contraseña de acceso que estableció cuando instaló el Sophos Security VM.
3. Introduzca el siguiente comando: `sudo /opt/sophox/logcollector/diagnose`.
4. Introduzca su contraseña de acceso cuando se le solicite. (Esto puede tardar un minuto en completarse).
5. En el Explorador de Windows, ya puede acceder a los registros recopilados en `\\<SVM-IP-Address>\logs\logs.tgz`. Introduzca sus credenciales cuando se le solicite.
   - El nombre de usuario es "sophos".
   - La contraseña es la contraseña de acceso que estableció cuando instaló el Sophos Security VM.

Para información sobre el registro en Sophos Enterprise Console, consulte la ayuda de Sophos Enterprise Console.

10 Desinstalar Sophos Security VM

Antes de comenzar, asegúrese de que los equipos virtuales invitados vayan a seguir protegidos. Vaya al Sophos Security VM y siga los pasos de Ver equipos virtuales protegidos (página 10). A continuación, mueva los equipos virtuales invitados a otro Sophos Security VM con una configuración de políticas similar.

Para desinstalar un Sophos Security VM, debe eliminarlo.

Para mover los equipos virtuales invitados:

1. Desinstale Sophos Guest VM Agent. Consulte Desinstalar Sophos Guest VM Agent.
2. Vuelva a instalar Sophos Guest VM Agent con la dirección IP del nuevo Sophos Security VM.

Una vez que haya movido los equipos virtuales invitados, puede eliminar el Sophos Security VM. Para ello:

3. Vaya a su hipervisor.
4. Apague el Sophos Security VM.
5. Elimine el equipo virtual.

11 Desinstalar Sophos Guest VM Agent

Puede desinstalar Sophos Guest VM Agent desde el Panel de control.

1. En el equipo virtual invitado, abra el **Panel de control**.
2. Haga clic en **Programas y características**.
3. Seleccione estas funciones y haga clic en **Desinstalar**:
   - Sophos for Virtual Environments
   - Sophos Guest VM Scanning Service
   - Sophos Virus Removal Tool

12 Apéndice: Añadir Sophos Security VM para la migración de equipos virtuales invitados

En cualquier momento se pueden añadir más Sophos Security VM que estarán disponibles para proteger la migración de equipos virtuales invitados.

Si tiene previsto crear más Sophos Security VM en el futuro, debe reservar direcciones IP para los Sophos Security VM que probablemente vaya a añadir. Para ello, cree una versión maestra rellenada previamente de este archivo. Este archivo debe contener todas las direcciones IP de los Sophos Security VM que tiene y que tendrá en el futuro. Puede copiar este archivo en cada Sophos Security VM a medida que se cree.

Importante
Debe seguir estos pasos en el Sophos Security VM que quiera añadir y en los Sophos Security VM existentes.

1. Abra una consola en el Sophos Security VM.
2. Inicie sesión:

   El nombre de usuario es "sophos".

   La contraseña es la contraseña de acceso que estableció cuando instaló el Sophos Security VM.
3. Abra el archivo de configuración additional_svms.txt para editarlo ejecutando el siguiente comando: `sudo vi /opt/sophos-svms/etc/additional_svms.txt`
4. Edite el archivo para añadir o eliminar direcciones IP de los Sophos Security VM que están disponibles para proteger la migración de equipos virtuales invitados, con una dirección IP por línea y sin caracteres de separación adicionales.

   a) Pulse `i` para abrir el modo edición en vi.

   b) Especifique una dirección IP por línea sin caracteres de separación adicionales. Por ejemplo:

   ```
   1.2.3.4
   5.6.7.8
   ```

   c) No es necesario que incluya la dirección IP para el Sophos Security VM en el que haya iniciado sesión.

   d) Pulse `Esc` para salir del modo edición en vi.

   e) Para guardar los cambios, introduzca `:wq`.
5. Consulte el registro de Sophos Security VM (`/var/log/ssvm.log`) para comprobar si se han producido errores al procesar la lista de Sophos Security VM adicionales.

   Si no hay errores, la lista actualizada se envía a todos los equipos virtuales invitados conectados para que puedan obtener protección de los nuevos Sophos Security VM.

13 Apéndice: Añadir procesadores al Sophos Security VM

Si tiene una muchos equipos virtuales invitados en un host, asegúrese de que el Sophos Security VM dispone de capacidad de procesamiento suficiente para escanear los archivos que utilizan al iniciarse.

Para ello, añada más procesadores al Sophos Security VM. Puede hacerlo en cualquier momento.

Nota
Si añade procesadores después de incluir el Sophos Security VM en un grupo de ordenadores en Sophos Enterprise Console, debe esperar hasta que el Sophos Security VM cumpla la política de grupo.

En función del tipo de carga, añadir procesadores también puede mejorar el rendimiento general del sistema.

Añadir procesadores en VMware ESXi

Añada procesadores del siguiente modo:

1. Apague el Sophos Security VM.
2. En vSphere Client, seleccione el Sophos Security VM.
3. Seleccione **Edit Settings > Hardware > CPUs.** A continuación, especifique el número de procesadores o CPU.

Añadir procesadores en Microsoft Hyper-V

Añada procesadores del siguiente modo:

1. Haga clic en **Inicio**, seleccione **Herramientas administrativas** y haga clic en **Administrador de Hyper-V**.
2. En el panel de resultados, en **Máquinas virtuales**, seleccione el Sophos Security VM.
3. En el panel **Acción**, debajo del nombre del equipo virtual, haga clic en **Configuración**.
4. Haga clic en **Procesador** y especifique el número de procesadores.

14 Soporte técnico

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

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

15 Aviso legal

Licencias de terceros

Para las licencias de terceros aplicables a su uso de este producto, consulte la siguiente carpeta del Sophos Security VM: `/usr/share/doc`.

Algunos programas de software se ofrecen al usuario bajo licencias de público general (GPL) o licencias similares de software gratuito que, entre otros derechos, permiten copiar, modificar y redistribuir ciertos programas o partes de los mismos, y tener acceso al código fuente. Las licencias de dichos programas, que se distribuyen al usuario en formato binario ejecutable, exigen que el código fuente esté disponible. Para cualquiera de tales programas que se distribuya junto con el producto de Sophos, se puede obtener el código fuente siguiendo las instrucciones que se incluyen en el artículo de la base de conocimiento 124427.