SOPHOS

Cybersecurity made simple.

Sophos for Virtual Environments

guía de configuración para usuarios con Sophos Central

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 Central para gestionar su software de seguridad.

Si usa Sophos Enterprise Console, consulte la guía de configuración para usuarios de Sophos Enterprise Console.

2 Configurar políticas

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

Solo se puede usar el tipo de política de protección contra amenazas, pero puede crear varias políticas si lo desea.

Por defecto, Sophos Central aplica una política base de protección contra amenazas a todos los Sophos Security VM. La configuración de esa política se utiliza después para los equipos virtuales invitados.

Esta configuración ofrece:

- Detección de programas maliciosos conocidos.
- Controles en la nube para permitir la detección de los últimos programas maliciosos conocidos por Sophos.
- Detección proactiva de programas maliciosos que no se conocían.
- Limpieza automática de programas maliciosos.

Tareas relacionadas

Crear o editar una política (página 2)
Para configurar Sophos for Virtual Environments, se utilizan las políticas de Sophos Central.

Referencia relacionada

Configuración de políticas (página 2)
Las opciones que puede usar para los Sophos Security VM

2.1 Crear o editar una política

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

Solo se puede usar el tipo de política de protección contra amenazas, pero puede crear varias políticas si lo desea.

Para crear o editar una política de protección contra amenazas:

1. Abra Sophos Central y vaya a **Server Protection > Políticas**.
2. Haga clic en una política de **Protección contra amenazas** o bien en **Añadir política** para crear una política nueva.
3. En la ficha **Servidores**, seleccione los Sophos Security VM a los que desea aplicar la política.
4. En la ficha **Configuración**, especifique las opciones que desee.

2.2 Configuración de políticas

Las opciones que puede usar para los Sophos Security VM

Live Protection

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

Opción	¿Compatible?
Utilizar protección activa	Sí
Enviar automáticamente muestras de archivos a SophosLabs	No

Escaneado en tiempo real

Las opciones del **Escaneado en tiempo real** son las siguientes:

Opción	¿Compatible?
Activar o desactivar	Sí
Escanear archivos locales o Escanear archivos locales y remotos	Sí
Leer	No
Escribir	No

Escaneado en tiempo real - Internet

Las opciones del **Escaneado en tiempo real - Internet** son las siguientes:

Opción	¿Compatible?
Escanear descargas en progreso	No
Bloquear el acceso a sitios web maliciosos	No
Detectar archivos de baja reputación	No

Remediación

Las opciones de la **Remediación** son las siguientes:

Opción	¿Compatible?
Limpieza automática de aplicaciones maliciosas	Sí

Escaneado en tiempo real - Opciones

Las opciones del **Escaneado en tiempo real - Opciones** son las siguientes:

Opción	¿Compatible?
Excluir automáticamente actividad de aplicaciones conocidas	No
Detectar comportamiento malicioso (HIPS)	No

Escaneado programado

Las opciones del **Escaneado programado** son las siguientes:

Opción	¿Compatible?
Activar escaneado programado	Sí

Protección en tiempo de ejecución

Las opciones de las **Protección en tiempo de ejecución** son las siguientes:

Opción	¿Compatible?
Detectar tráfico de red para gestionar y controlar servidores	No
Proteger archivos de documentos de ransomware (CryptoGuard)	No
Activar Sophos Security Heartbeat	No

Exclusiones de escaneado

Las opciones de las **Exclusiones de escaneado** son las siguientes:

Opción	¿Compatible?
Exclusiones de escaneado globales Para editarlas, vaya a **Configuración > Exclusiones de escaneado globales**.	Sí
Exclusiones de escaneado de políticas (Windows y Linux)	Sí
Exclusiones de Heartbeat de políticas (solo Windows)	No
Excluir servidor DNS (solo Windows)	No

Mensaje de escritorio

Las opciones del **Mensaje de escritorio** son las siguientes:

Opción	¿Compatible?
Activar los mensajes de escritorio para la protección contra amenazas	No

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 6).

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 Resolución de problemas de escaneado en tiempo real (página 7).

3.2 Probar el escaneado en tiempo real

Compruebe que el escaneado en tiempo real funciona en un Sophos Security VM.

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 Sophos Security VM realiza el escaneado en acceso de archivos:

1. Vaya a http://2016.eicar.org/86-0-Intended-use.html y utilice el archivo de prueba EICAR.

2. 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.
3. Pruebe a acceder al archivo desde el equipo virtual invitado.
4. Inicie sesión en Sophos Central.
    - Si tiene la limpieza automática activada, vaya a la página **Servidores** y haga clic en el Sophos Security VM para abrir la página de detalles. En su ficha **Eventos**, debe ver que se ha detectado y limpiado EICAR.
    - Si no tiene activada la limpieza automática, busque en la página **Alertas**. Debería ver una alerta en el Sophos Security VM. Se ha detectado EICAR, pero no se ha limpiado.

Si no se ha detectado EICAR, consulte Resolución de problemas de escaneado en tiempo real (página 7). Si no se limpia EICAR, simplemente elimínelo.

3.3 Resolución de problemas de escaneado en tiempo real

Si el escaneado en tiempo real no funciona:

1. Asegúrese de que el escaneado en tiempo real está activado en la política del servidor aplicada al Sophos Security VM:
    a) En Sophos Central, vaya a la página **Servidores**, busque el Sophos Security VM y haga clic en él para ver los detalles.
    b) En la ficha **Resumen**, verá la política de protección contra amenazas aplicada al servidor en la sección **Resumen**. Haga clic en el nombre de la política.
    c) En la política, vaya a la sección **Escaneado en tiempo real**. Asegúrese de que **Escanear** está activado.
    d) 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. Para más información, consulte Ver equipos virtuales protegidos (página 8).
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 invitados

Puede ver los datos de todos los equipos virtuales invitados de la siguiente manera:

- Ver equipos virtuales invitados conectados (página 8). Puede hacerlo en Sophos Central.
- Ver equipos virtuales protegidos (página 8).

Los equipos virtuales invitados "conectados" tienen instalado el agente de Sophos y pueden conectarse al Sophos Security VM.

Normalmente, un equipo virtual invitado conectado también está protegido. Sin embargo, si el agente está recién instalado, o si hay algún problema, es posible que todavía no sea haya iniciado el escaneado contra amenazas.

4.1 Ver equipos virtuales invitados conectados

Puede ver todos los equipos virtuales invitados que están conectados a un Sophos Security VM de la siguiente manera.

1. Inicie sesión en Sophos Central.
2. Vaya a **Server Protection > Servidores**.
3. Localice el Sophos Security VM en la lista y haga clic en él para ver los detalles.
4. En la ficha **Resumen**, en **Estado de entornos virtuales**, busque **Equipos virtuales invitados conectados**. Haga clic en el número que aparece.

   Nota
   Si no hay ningún equipo virtual invitado ejecutándose o si todavía está instalando los agentes, es posible que vea cero equipos virtuales invitados.

5. Verá una lista de nombres de equipos virtuales y direcciones IP.

   Puede buscar un equipo virtual invitado concreto en la lista o utilizar el filtro para mostrar los equipos virtuales de escritorio o servidor.

4.2 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

El Sophos Security VM siempre escanea los archivos en acceso, es decir, cuando se abren y cierran.

El Sophos Security VM también puede realizar un escaneado completo de los equipos virtuales invitados. 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 realiza los escaneados por fases para impedir la sobrecarga del host. Por defecto se escanean siempre dos equipos virtuales invitados a la vez. Por lo tanto, el escaneado de todos los equipos virtuales invitados administrados por el Sophos Security VM puede tardar algo más de tiempo.

- Para realizar un escaneado remoto de los equipos virtuales invitados de forma inmediata:
  a) Inicie sesión en Sophos Central.
  b) Vaya a la página **Servidores**.
  c) Busque el Sophos Security VM y haga clic en él para abrir la página de detalles.
  d) En el panel de la izquierda, haga clic en **Escanear ahora**.
- Para realizar un escaneado remoto de los equipos virtuales invitados de forma programada:
  a) Inicie sesión en Sophos Central.
  b) Vaya a la página **Servidores**.
  c) Busque el Sophos Security VM y haga clic en él para ver la página de detalles.
  d) En la ficha **Resumen**, localice la política de protección contra amenazas aplicable en la sección **Resumen**. Haga clic en ella para editarla.
  e) En la política, vaya a la sección **Escaneado programado**. Active el escaneado y especifique los momentos en los que se ejecutará el escaneado.

6 Qué ocurre cuando se detecta una amenaza

Si Sophos Security VM detecta alguna amenaza en algún equipo virtual invitado, hace lo siguiente:

- Bloquea la amenaza.
- Intenta eliminar la amenaza automáticamente.
- Envía una alerta a Sophos Central si necesita tomar alguna medida.

Nota
El Sophos Security VM no limpia automáticamente las amenazas durante un escaneado remoto completo de todos los equipos virtuales invitados.

Lo que se ve en Sophos Central

Sophos Central:

- Muestra que la amenaza ha sido bloqueada. Consulte la ficha **Eventos** de la página de detalles de Sophos Security VM.
- Muestra una alerta en la página **Alertas**. Esto muestra qué es la amenaza, en qué equipo virtual se encuentra y si es posible limpiarla.
- Elimina la alerta si se realiza correctamente la limpieza automática.

Si la limpieza automática no está disponible o no se realiza correctamente, aparece una alerta en la página **Alertas** que le solicita que la limpie manualmente.

Para obtener más información sobre la limpieza, consulte Limpiar una amenaza (página 12).

Lo que el usuario ve en el equipo virtual invitado

Si Sophos Security VM detecta una amenaza cuando un usuario intenta acceder a un archivo, bloquea el acceso a ese archivo desde el equipo virtual invitado. Si la aplicación utilizada para acceder al archivo puede hacerlo, informa al usuario de que el archivo ya no es accesible.

7 Limpiar una amenaza

En esta sección se describe la limpieza automática y la manual de amenazas.

Para obtener información sobre una amenaza y consejos para su limpieza, inicie sesión en Sophos Central, vaya a la página **Alertas**, busque la alerta de la amenaza y haga clic en el nombre de la amenaza.

Limpieza automática

El Sophos Security VM limpia automáticamente las amenazas que detecta.

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

Limpieza manual

Puede limpiar un equipo virtual invitado manualmente.

Para la limpieza manual, debe restaurar el equipo virtual invitado. Tenga en cuenta que es posible que se pierdan datos (vea información abajo).

Utilice uno de estos métodos:

- Eliminar el equipo virtual invitado y volver a crearlo. Los datos se perderán.
- Revertir el equipo virtual invitado a un estado anterior limpio. Se perderán los datos que se hayan añadido después de tomar la instantánea del sistema.

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

8 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 8). 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.

9 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

10 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.

11 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.

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.

12 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.

13 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.