SOPHOS

Security made simple.

# Sophos for Virtual Environments

# Guía de inicio: edición Sophos Central

Versión: 1.0

# Contenido

# 1 Acerca de esta guía

En esta guía se explica cómo:

- Utilizar Sophos for Virtual Environments para proporcionar una protección centralizada contra amenazas para equipos virtuales en un entorno VMware ESXi o un entorno Microsoft Hyper-V.
- Utilizar Sophos Central para administrar Sophos for Virtual Environments.

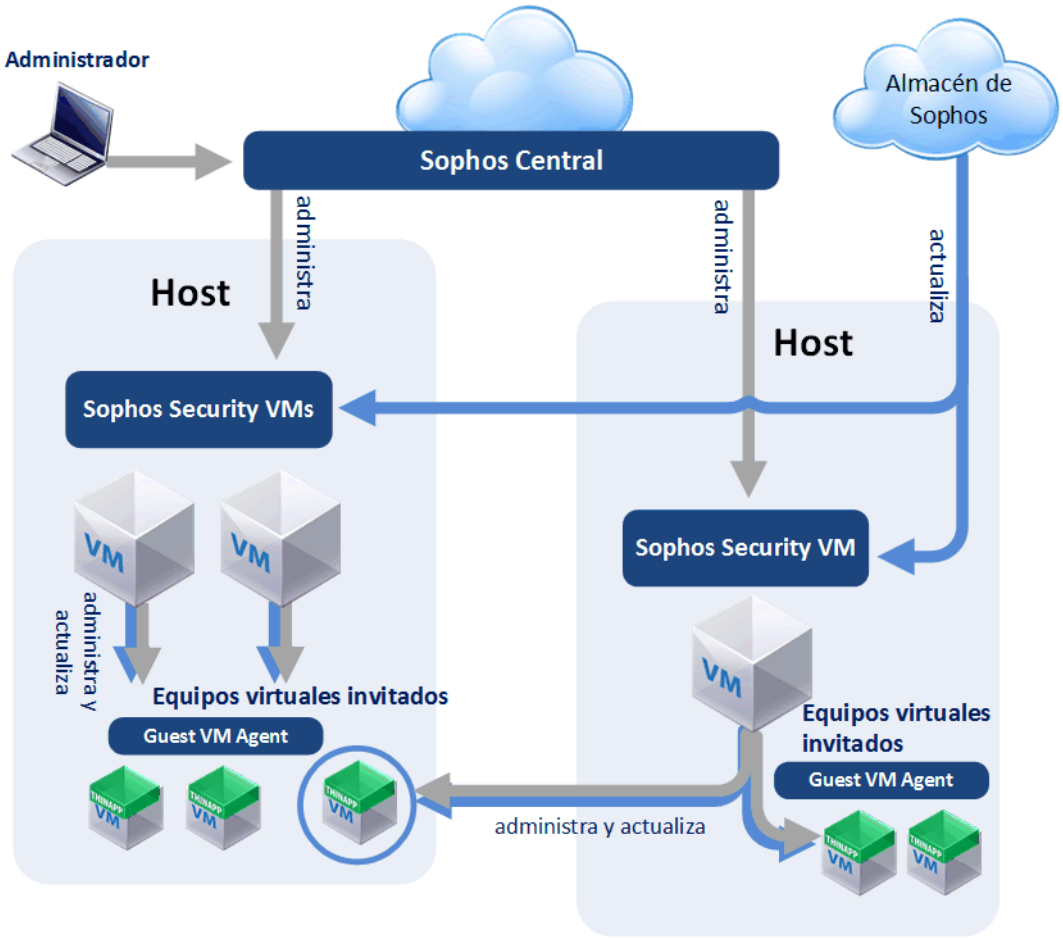
Si está migrando a Sophos for Virtual Environments, consulte Migrar a Sophos for Virtual Environments en la página 25.

Si desea utilizar Sophos Enterprise Console Central en lugar de Sophos Central, consulte la *Guía de inicio de Sophos for Virtual Environments: edición Enterprise Console*.

# 2 Acerca de Sophos for Virtual Environments

Sophos for Virtual Environments es un sistema de seguridad para la protección de equipos virtuales. El funcionamiento es el siguiente:

- Se realiza una o varias instalaciones de **Sophos Security VM** en cada host. Entonces el Sophos Security VM puede detectar y bloquear amenazas en los equipos virtuales invitados.
- Se debe instalar **Sophos Guest VM Agent** en cada equipo virtual invitado.
- Se utiliza **Sophos Central** para administrar los Sophos Security VM.




## ¿En qué entornos se puede utilizar Sophos?

Sophos for Virtual Environments puede proteger equipos virtuales en un entorno VMware EXSi o un entorno Microsoft Hyper-V.

## ¿Qué equipos virtuales invitados se pueden proteger?

El Sophos Security VM puede proteger equipos virtuales invitados que ejecutan sistemas operativos Windows. Para obtener más información, consulte Requisitos de los equipos virtuales invitados en la página 8.

**Nota:** el Sophos Security VM puede proteger equipos virtuales invitados que se encuentran en otro host.

## ¿Cómo funciona el escaneado?

Cuando un equipo virtual invitado intenta acceder a un archivo:

- Sophos Guest VM Agent en ejecución en el equipo virtual notifica al Sophos Security VM.
- El Sophos Security VM escanea el archivo.
- Si el Sophos Security VM detecta alguna amenaza, se bloquea el acceso al archivo y el Sophos Security VM envía una alerta a Sophos Central.

El Sophos Security VM también puede realizar un escaneado completo de los equipos virtuales invitados. Puede ejecutar este escaneado inmediatamente o programarlo.

El escáner de archivos utiliza el almacenamiento inteligente en caché para conservar los resultados de escaneados anteriores. Esto ayuda a mejorar el rendimiento general cuando hay demasiados equipos virtuales invitados conectados o cuando se accede al mismo archivo repetidamente.

## ¿Cómo se administra el Sophos Security VM?

Sophos Central muestra el estado del Sophos Security VM; por ejemplo, si se encuentra actualizado y si ha detectado alguna amenaza.

Sophos Central permite configurar el escaneado mediante políticas.

## Qué hacer ante una amenaza

El Sophos Security VM ofrece la posibilidad de limpiar las amenazas automáticamente. Para más información, consulte: Limpiar una amenaza en la página 21.

## ¿Cómo se actualiza el Sophos Security VM?

El Sophos Security VM recibe e instala las actualizaciones automáticamente desde Sophos.

## ¿Cómo se actualiza el Sophos Guest VM Agent?

Sophos Guest VM Agent se actualiza automáticamente.

El agente no escanea archivos, de modo que no necesita identidades de amenazas actualizadas. Sin embargo, sí que recibe actualizaciones cuando mejoramos el producto.

El Sophos Security VM recibe estas actualizaciones de producto de Sophos y las aplica a los equipos virtuales invitados.

Las actualizaciones se distribuyen de forma escalonada para minimizar la carga en el Sophos Security VM y el host del hipervisor subyacente.

# 3 Pasos clave para la instalación

Los pasos de instalación que se describen en las siguientes secciones son:

- Comprobar los requisitos del sistema.
- Desinstalar otros productos antivirus.
- Instalar el Sophos Security VM
- Instalar Sophos Guest VM Agent en los equipos virtuales invitados.
- Comprobar que los equipos virtuales invitados están protegidos.

# 4 Comprobar los requisitos del sistema

En esta sección se describen los requisitos del sistema necesarios y cómo comprobar que los cumple.

También se explica toda la información (como los datos de los ordenadores) que debe reunir ahora para tenerla a mano cuando vaya a instalar los Sophos Security VM.

Se cubren los requisitos tanto para entornos VMware EXSi como para entornos Microsoft Hyper-V.

## 4.1 Requisitos de VMware

En esta sección se indica el software que necesita en un entorno VMware.

### 4.1.1 Host VMware ESXi

Instale los siguientes componentes en todos los hosts que vayan a ejecutar un Sophos Security VM:

- Host VMware ESXi 5.5, 6.0 o 6.5.

**Nota:** se recomienda que configure el host de modo que reciba actualizaciones de VMware.

#### Requisitos de hardware

El host VMware ESXi debe ser capaz de asignar los recursos siguientes para el Sophos Security VM:

- 2 procesadores.
- 20 Gb de espacio en disco.
- 4 Gb de RAM.

**Notas**

No se debe imponer ningún límite de recursos de los procesadores en el Sophos Security VM.

Se asignan 2 procesadores de forma predeterminada. Si necesita proteger una gran cantidad de equipos virtuales invitados, puede configurar más procesadores después de instalar el Sophos Security VM. En esta guía se explica cómo hacerlo.

El Sophos Security VM reserva memoria. Los sistemas de alta disponibilidad y equilibrio de cargas eligen de forma automática según las reservas de recursos para los equipos virtuales del entorno VMware. No elimine la reserva de memoria del Sophos Security VM.

### 4.1.2 VMware vCenter y vSphere

Es necesario el software de vCenter y vSphere siguiente.

| Software | Versión | Notas |
|---|---|---|
| vCenter | Versión 5.5 o 6.5<br>Se requiere la versión 6.5 para administrar un host ESXi 6.0, pero también permite administrar versiones anteriores de ESXi. | También necesitará:<br>La dirección de red.<br>Una cuenta de administrador. |
| vSphere Client | Versión 5.5 o 6.5. | |

### 4.1.3 Herramientas de VMware

Estos componentes no son necesarios para utilizar Sophos for Virtual Environments. Sin embargo, recomendamos disponer de ellos porque pueden mejorar el rendimiento de la red.

## 4.2 Requisitos de Microsoft Hyper-V

En esta sección se indica el software que necesita en un entorno Microsoft Hyper-V.

El sistema Microsoft Hyper-V debe ser uno de los siguientes:

- Hyper-V en Windows Server 2012 (Core, completo)
- Hyper-V in Windows Server 2012 R2 (Core, completo)

### Componentes de integración de Microsoft Hyper-V

Los componentes de integración de Microsoft Hyper-V se instalarán automáticamente si la actualización de Windows está activada y funciona correctamente. Sin estas herramientas, el rendimiento de su equipo virtual podría verse reducido.

### Directrices sobre antivirus para Microsoft Hyper-V

Microsoft publica directrices sobre cómo proteger su servidor Hyper-V de la forma más efectiva. Consulte Microsoft KBA 3105657.

## 4.3 Requisitos de los equipos virtuales invitados

Los equipos virtuales invitados deben utilizar uno de los sistemas operativos indicados aquí.

| Sistema operativo | Service Packs | Comentarios |
|---|---|---|
| Windows 10 (32 y 64 bits). El artículo de la base de conocimiento 125679 incluye | | Los contenedores de Windows y Hyper-V no son compatibles. |

| Sistema operativo | Service Packs | Comentarios |
|---|---|---|
| una lista con todas las versiones compatibles. | | |
| Windows 8.1 (32 y 64 bits) | --- | |
| Windows 7 (32 y 64 bits) | SP1+ | |
| Windows Server 2016 (64 bits) | | Los contenedores de Windows y Hyper-V no son compatibles. |
| Windows Server 2012 R2 (64 bits) | --- | |
| Windows Server 2012 (64 bits) | --- | |
| Windows Server 2008 R2 (64 bits) | --- | |

## 4.4 Requisitos de red

Los requisitos de infraestructura son los siguientes:

- El Sophos Security VM y los equipos virtuales invitados deben compartir una conexión de red. Lo ideal es que sea una red de área local (LAN) de alta velocidad sin limitación de tráfico de red.
- El tráfico de red entre el Sophos Security VM y los equipos virtuales invitados no debe estar bloqueado por firewalls ni controladores de acceso a la red.

### 4.4.1 Requisitos de redes NAT

Si tiene un equipo virtual invitado dentro de una red NAT (traducción de direcciones de red), puede protegerlo con un Sophos Security VM dentro o fuera de esa red.

Durante la instalación, debe configurar el Sophos Security VM con lo siguiente:

- Una dirección IP principal fuera de la red NAT (esta dirección debe poder comunicarse con la consola de administración)
- Una dirección IP secundaria dentro de la red NAT

### 4.4.2 Subredes

Puede configurar el Sophos Security VM con hasta cinco direcciones IP. Cada dirección IP debe encontrarse en una subred diferente.

## 4.5 Requisitos de administración de Sophos

Antes de poder proteger y administrar sus equipos virtuales, necesita:

- Una cuenta de Sophos Central.

# 5 Desinstalar otros productos antivirus

Debe desinstalar todos los productos antivirus, **incluidos los productos de Sophos**, que ya estén instalados en sus equipos virtuales invitados.

Debe deshabilitar Windows Defender en las plataformas de servidor donde no esté presente el centro de seguridad. Se recomienda que lo haga mediante una política de grupo.

No puede utilizar Sophos for Virtual Environments para proteger equipos virtuales invitados que ejecutan otros productos antivirus. Si intenta hacerlo, es posible que el rendimiento se vea afectado o que se produzca un interbloqueo del sistema en que el equipo virtual invitado deja de responder.

Esta limitación también es aplicable a equipos virtuales con productos de servidor o puerta de enlace de Sophos que incluyan o requieran componentes antivirus.

Para más información, vea el artículo 125679 en la base de conocimiento.

# 6 Instalar el Sophos Security VM

Puede instalar uno o más Sophos Security VM en cada host en el que desee proteger equipos virtuales invitados.

Antes de empezar, asegúrese de que el host cumpla los requisitos del sistema. También se recomienda que configure el host de modo que reciba actualizaciones de VMware.

Los pasos necesarios para la instalación, que se describen en las secciones siguientes, son:

- Comprobar que dispone de las contraseñas necesarias.
- Comprobar que los sistemas están sincronizados.
- Descargar el programa de instalación.
- Instalar el Sophos Security VM
- Comprobar que el Sophos Security VM está instalado.

## 6.1 Comprobar que dispone de las contraseñas necesarias

Al ejecutar el programa de instalación de Sophos Security VM, es necesario introducir ciertas contraseñas. Asegúrese de que dispone de las contraseñas para las siguientes cuentas:

- La cuenta de Sophos Central.
- Si se encuentra en un entorno MVware, la cuenta de administrador de vCenter.

## 6.2 Comprobar que los sistemas están sincronizados

Asegúrese de que la hora esté sincronizada en el host en el que instala el Sophos Security VM y en los equipos virtuales invitados.

Puede utilizar la sincronización NTP (protocolo de tiempo de redes) para cada host.

**Aviso:** si la hora no está sincronizada, podrá instalar el Sophos Security VM pero no podrá administrarlo desde Sophos Central.

## 6.3 Comprobar los requisitos del programa de instalación

Compruebe que el ordenador y la cuenta de usuario que va a utilizar cumplan los requisitos.

- El programa de instalación debe encontrarse en un ordenador Windows que tenga acceso a su servidor VMware vCenter o Microsoft Hyper-V a través de la red.
- La instalación del Sophos Security VM debe realizarse en la red local. Actualmente el programa de instalación no admite el uso de un proxy.
- El programa de instalación no puede utilizarse en un ordenador con Windows XP o Windows Server 2003.
- Si utiliza Microsoft Hyper-V, debe ejecutar el programa de instalación como usuario con derechos para crear y controlar equipos virtuales en el servidor Hyper-V. Esto puede ser una cuenta de usuario local en el servidor Hyper-V o un usuario de dominio.

El ordenador donde se guarda el programa de instalación se utiliza solo para la instalación. No se usa para la administración ni la protección de su Sophos Security VM ni de equipos virtuales invitados tras la instalación.

## 6.4 Descargar el programa de instalación de Sophos Security VM.

Descargue el programa de instalación desde Sophos Central (si todavía no lo ha hecho).

Se asume que dispone de una cuenta de Sophos Central.

**Notas:**

- Puede descargar el programa de instalación desde cualquier ordenador y después copiarlo al ordenador donde desea utilizarlo.
- Las instrucciones de instalación de las secciones siguientes le indicarán en qué ordenador u ordenadores debe utilizar el programa de instalación.

Para descargar el programa de instalación:

1. Inicie sesión en Sophos Central.
2. Vaya a la página **Proteger dispositivos**.
3. En **Protección de entornos virtuales**, haga clic en el enlace para descargar el programa de instalación para su entorno (Hyper-V o ESXi).

Después de instalar el Sophos Security VM, podrá obtener Sophos Guest VM Agent desde una unidad compartida pública del Sophos Security VM.

## 6.5 Instalar el Sophos Security VM

Para instalar un Sophos Security VM, necesitará el programa de instalación de Sophos Security VM. Si aún no lo ha descargado, consulte Descargar el programa de instalación de Sophos Security VM. en la página 12.

Asegúrese de que el ordenador y la cuenta que utilice cumplan los requisitos en la página 11.

Algunos pasos de la instalación son aplicables solo a VMware ESXi o solo a Microsoft Hyper-V. Esto se indica al principio del paso.

1. Haga doble clic en el programa de instalación.

   Siga los pasos del asistente.

2. Acepte el acuerdo de licencia.
3. En la página de bienvenida, haga clic en **Install** para extraer los archivos de instalación a una carpeta en el equipo.
4. Compruebe que ha instalado todos los requisitos previos para la instalación que aparecen en **Prerequisites for installation**.
5. **Si se encuentra en un entorno VMware ESXi:**

   En **VMware vCenter credentials**, introduzca los detalles y un nombre para el Sophos Security VM.

   **Nota:** introduzca el nombre de usuario del administrador en el formulario que utiliza para iniciar sesión en vCenter usando vSphere Client. Es decir, con o sin el prefijo del dominio, según se requiera, y con las mismas mayúsculas y minúsculas.

6. En **ESXi host** o **Hyper-V host name**, especifique el host en el que desea instalar el Sophos Security VM.
7. En **Management console**, seleccione **Use Sophos Central**.
8. Introduzca sus datos de cuenta de Sophos Central en **Sophos Central account details**:
   a) Introduzca la dirección de correo electrónico y la contraseña que utilizó cuando se registró en Sophos Central.
   b) Introduzca los datos del servidor proxy que usó para conectarse a Sophos Central (si procede).
9. Cree una contraseña de acceso en **Password for access** para su Sophos Security VM.
   Esta contraseña es necesaria para ver los equipos virtuales invitados protegidos o si necesita que el soporte técnico de Sophos solucione algún problema en la instalación de forma remota. El equipo de soporte técnico la utiliza para obtener registros, que puede revisar y enviar a Sophos si es necesario.
10. En **Timezone**, seleccione la zona horaria que utilizará el Sophos Security VM para programar los escaneados.
11. **Solo si se encuentra en un entorno VMware ESXi**:
    En **Datastore for the Security VM**, seleccione el tipo de almacén de datos en el que desea instalar el Sophos Security VM.
    **Nota:** el Sophos Security VM protege los equipos virtuales invitados incluso si sus plantillas se guardan en distintos almacenes de datos.
12. En **IP settings for the Sophos Security VM**, introduzca la configuración de IP para todas las redes en las que desea proteger equipos virtuales invitados. Un Sophos Security VM puede proteger los equipos virtuales de varias redes.
    a) En **Select virtual LAN** (ESXi) o **Select vSwitch** (Hyper-V), seleccione de entre las opciones disponibles.
    b) Introduzca la dirección IPv4 estática en **Static IPv4 address**. Solo puede utilizar direcciones estáticas.
    c) Introduzca una máscara de subred en **Subnet mask**.
    d) Introduzca el sufijo del dominio en **Domain suffix**.
    e) Seleccione **Make Primary** si esta es la red que debe tener acceso a la consola de administración de Sophos. Solo puede tener una red principal.
       Puede utilizar el botón "+" que aparece sobre los campos para añadir otra red. El botón "-" sirve para eliminar una red. Los botones "<" y ">" le permiten desplazarse por las opciones de configuración de las distintas redes.
13. En **Gateway and DNS server details for the primary network card**, introduzca los datos que permitirán al Sophos Security VM comunicarse con la consola de administración y descargar las actualizaciones.
    **Nota:** puede introducir un servidor DNS o, si lo desea, dos.
14. **Si se encuentra en un entorno Microsoft Hyper-V:**
    En **Disk image location**, especifique una ubicación para la imagen de disco del Sophos Security VM. Puede ser una unidad compartida de red o una carpeta local en el host.
15. En la página **Summary of installation**, aparecen todos los datos de la instalación. Haga clic en **Install**.

16. En la página **Finished**, verá si la instalación del Sophos Security VM se ha realizado correctamente. Si se ha producido algún error, consulte el registro para más información.

    **Sugerencia:** Puede hacer clic en **Start Over** para ejecutar otra instalación o para volver a intentar la instalación si se han producido errores.

17. En la página **What to do next** se explica cómo configurar el Sophos Security VM y proteger los equipos virtuales invitados.

Siga las instrucciones de la siguiente sección para comprobar que puede ver el Sophos Security VM en Sophos Central.

**Aviso:** no "suspenda" el Sophos Security VM. Si lo hace, más tarde no se podrán reanudar las comunicaciones con el software de administración.

## 6.6 Comprobar que el Sophos Security VM está instalado

En esta sección se explica cómo comprobar si el Sophos Security VM está instalado y si dispone de los recursos que necesita.

### Comprobar que puede ver el Sophos Security VM

Cuando se haya instalado el Sophos Security VM, vaya a Sophos Central.

Los equipos virtuales de seguridad se incluyen en la página **Servidores** de Sophos Central. Busque "Sophos Security VM" en la columna "Nombre/SO".

Para ver solo el Sophos Security VM, seleccione **Servidores virtuales** en el filtro de lista.

### Comprobar si necesita configurar recursos

Normalmente, no es necesario configurar recursos para el Sophos Security VM. Tenga en cuenta que:

- **Si tiene una gran cantidad de equipos virtuales invitados** alojados en un único host, asegúrese de que el Sophos Security VM dispone de capacidad de procesamiento suficiente para el escaneado. Consulte Apéndice: Añadir procesadores al Sophos Security VM en la página 27.
- **El programa de instalación reserva memoria para el Sophos Security VM.** En un entorno VMware, los sistemas de alta disponibilidad y equilibrio de cargas eligen de forma automática según las reservas de recursos para los equipos virtuales y podrían hacer elecciones diferentes una vez instalado el Sophos Security VM. No elimine la reserva de memoria del Sophos Security VM.

# 7 Instalar Sophos Guest VM Agent

Sophos Guest VM Agent debe ejecutarse en todos los equipos virtuales invitados que desee proteger.

Compruebe en qué sistemas operativos puede instalar Sophos Guest VM Agent. Consulte Requisitos de los equipos virtuales invitados en la página 8.

1. En el equipo virtual invitado, desplácese hasta el host en que esté instalado el Sophos Security VM. Debe utilizar la dirección IP.
2. En la unidad compartida **Pública**, busque el programa de instalación **SVE-Guest-Installer.exe**
3. Haga doble clic en el programa de instalación para ejecutarlo o transfiéralo al equipo virtual invitado y ejecútelo. Siga las instrucciones en pantalla. Alternativamente puede:
   - Usar la línea de comandos. Puede optar por instalarlo con (IU limitada) o sin (sin IU) una barra de progreso para indicar el estado de la instalación. En los comandos se distingue entre mayúsculas y minúsculas. Introduzca la opción que corresponda:

     IU limitada: `SVE-Guest-Installer.exe SVMIPAddress=<IP Address of SVM> /install /passive`

     Sin IU: `SVE-Guest-Installer.exe SVMIPAddress=<IP Address of SVM> /install /quiet`

   - Utilice la implementación de política de grupo. Para más información, consulte este artículo de Microsoft: http://support.microsoft.com/kb/816102

Recomendamos que haga una instantánea del equipo virtual invitado antes de instalar el agente. Esto le permitirá revertir el equipo virtual invitado de forma segura posteriormente en caso de que sea necesario.

# 8 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 acceso en un equipo virtual invitado.
- Solucionar problemas del escaneado en acceso.

## 8.1 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** desde el menú 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 en la página 16.

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 en la página 17.

## 8.2 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. Visite eicar.org/86-0-Intended-use.html. 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. Iniciar 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 en la página 17. Si no se limpia EICAR, simplemente elimínelo.

## 8.3 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. Consulte Ver equipos virtuales protegidos en la página 18.
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.

# 9 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.

# 10 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.

## Escanear equipos virtuales invitados ahora

Para realizar un escaneado remoto de los equipos virtuales invitados de forma inmediata:

1. Iniciar sesión en Sophos Central.
2. Vaya a la página **Servidores**.
3. Busque el Sophos Security VM y haga clic en él para abrir la página de detalles.
4. En el panel de la izquierda, haga clic en **Escanear ahora**.

## Escanear equipos virtuales invitados de forma programada

Para realizar un escaneado remoto de los equipos virtuales invitados de forma programada:

1. Iniciar sesión en Sophos Central.
2. Vaya a la página **Servidores**.
3. Busque el Sophos Security VM y haga clic en él para ver la página de detalles.
4. En la ficha **Resumen**, localice la política de protección contra amenazas aplicable en la sección **Resumen**. Haga clic en ella para editarla.
5. En la política, vaya a la sección **Escaneado programado**. Active el escaneado y especifique los momentos en los que se ejecutará el escaneado.

# 11 Qué ocurre cuando se detecta una amenaza

Si el Sophos Security VM detecta alguna amenaza en algún equipo virtual invitado:

- 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 ve en Sophos Central

Sophos Central:

- Muestra que la amenaza ha sido bloqueada. Consulte la ficha **Eventos** de la página de detalles del 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 en la página 21.

## Lo que el usuario ve en el equipo virtual invitado

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

# 12 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, vaya a la página **Alertas** en Sophos Central, 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 perderá los datos al hacerlo.

Utilice uno de estos métodos:

- Eliminar el equipo virtual invitado afectado y volver a clonarlo a partir de una imagen de plantilla.
- Revertir el equipo virtual invitado afectado a un estado anterior limpio.

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

# 13 Mantener el Sophos Security VM

Esta sección ofrece consejos sobre las tareas de mantenimiento y posteriores a la instalación.

- **Debe encender el Sophos Security VM de forma manual cada vez que retire el host del modo de mantenimiento o espera.** Enciéndalo antes que los equipos virtuales invitados para que estén protegidos de forma inmediata.
- **No "suspenda" el Sophos Security VM.** Si lo hace, más tarde no se podrán reanudar las comunicaciones con el software de administración.
- **Verifique que el Sophos Security VM esté recibiendo actualizaciones de seguridad de Sophos.** Para hacerlo, revise su estado de actualización en Sophos Central.
- **Copias de seguridad.** Recomendamos que el Sophos Security VM se excluya de las tareas periódicas de copia de seguridad, ya que esto puede afectar al rendimiento. Si necesita recuperarse el Sophos Security VM debido a fallos en la infraestructura, le recomendamos que vuelva a desplegar el Sophos Security VM.

# 14 Desinstalar el Sophos Security VM

Para desinstalar un Sophos Security VM, debe eliminarlo.

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 en la página 18. A continuación, mueva los equipos virtuales invitados a otro Sophos Security VM con una configuración de políticas similar.

Para mover los equipos virtuales invitados:

1. Desinstale Sophos Guest VM Agent. Consulte Desinstalar Sophos Guest VM Agent en la página 24.
2. Vuelva a instalar Sophos Guest VM Agent con la dirección IP del nuevo Sophos Security VM. Consulte Instalar Sophos Guest VM Agent en la página 15.

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

1. Vaya a su hipervisor.
2. Apague el Sophos Security VM.
3. Elimine el equipo virtual.

# 15 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

# 16 Migrar a Sophos for Virtual Environments

## ¿Desde qué productos puedo realizar la migración?

Puede migrar a Sophos for Virtual Environments desde estos productos.

- Sophos Anti-Virus para vShield en un entorno VMWare ESXi
- Sophos Anti-Virus ejecutado localmente en cada equipo virtual invitado en un entorno VMware ESXi o un entorno Microsoft Hyper-V
- Productos antivirus de otros proveedores en un entorno VMware ESXi o un entorno Microsoft Hyper-V

**Nota:** Sophos for Virtual Environments protege equipos virtuales invitados en un host VMware ESXi incluso cuando se ejecuta en un entorno NSX. Sin embargo, Sophos for Virtual Environments no se integra con NSX Manager. No debe instalar ningún software antivirus para ejecutarse en NSX, ya que esto afectaría al rendimiento y provocaría interbloqueos.

**Nota:** Sophos for Virtual Environments utiliza un Security VM para ofrecer un escaneado de amenazas centralizado. Cuando lo haya instalado, los equipos virtuales invitados ya no necesitarán actualizaciones de datos de amenazas.

## ¿Cómo realizo la migración?

Siga los pasos que incluimos a continuación. Encontrará más información sobre cada paso en esta guía.

**Nota:** si está migrando desde un software antivirus de terceros, tenga en cuenta lo siguiente:

- Sophos for Virtual Environments requiere conectividad de red entre el Security VM y los equipos virtuales invitados.
- Sophos for Virtual Environments admite tecnologías de equilibrio de cargas de equipos virtuales dinámico como vMotion y Live Migration, pero el rendimiento es mejor si se mantiene la conectividad de red de alta velocidad entre el Security VM y los equipos virtuales invitados.

Para migrar:

1. Instale un Sophos Security VM.

   **Nota:** este nuevo Security VM puede estar en el mismo host que un Security VM existente que ejecute SAV para vShield.

2. Vaya a la consola de administración y verifique que el Sophos Security VM se esté actualizando correctamente.
3. Apague el Sophos Security VM anterior o desinstale el software antivirus anterior.

**Advertencia:** sus equipos virtuales invitados quedarán desprotegidos; asegúrese de garantizar su seguridad.

4. Instale el nuevo agente ligero Sophos Guest VM Agent.

5. Verifique, como se describe en esta guía, que todos los equipos virtuales invitados estén ahora protegidos.

# 17 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.

# 18 Soporte técnico

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

- Visitar el fórum 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/support/contact-support/support-query.aspx.

# 19 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.