Guía del cliente de Symantec™ Endpoint Protection 14.3 RU3 para Linux - Spanish - Spain

September 2021

Table of Contents

Protección de dispositivos de Linux con Symantec Endpoint Protection

Acerca del Agente de Symantec para Linux

El Agente de Symantec para Linux protege los dispositivos de Linux contra amenazas de software malicioso, riesgos y vulnerabilidades. Protege proactivamente los dispositivos de Linux contra software malicioso conocido y desconocido.

Las funciones de protección contra software malicioso incluyen la **Protección contra software malicioso** (AMD) que protege los dispositivos de Linux contra software malicioso como, por ejemplo, virus, spyware, ransomware, etc. y **Auto-Protect** (AP), que detecta las amenazas maliciosas cuando se inicia una aplicación.

Symantec recomienda tener Auto-Protect habilitado para garantizar la protección en tiempo real. Cualquier software malicioso que se detecte se pone en cuarentena de forma inmediata. Si deshabilita Auto-Protect, aún podrá detectar software malicioso usando un análisis a petición.

Guía de inicio sobre el Agente de Linux

Requisitos del sistema del Agente de Symantec para Linux

Esta sección incluye los requisitos del sistema para la versión más actual.

Para conocer los requisitos del sistema para las versiones anteriores de Symantec Endpoint Protection o la versión más actual de estos requisitos del sistema, consulte la siguiente página web:

Notas de la versión, nuevas correcciones y requisitos del sistema para todas las versiones de Endpoint Protection

Table 1: Requisitos del sistema del Agente de Symantec para Linux

Componente	Requisitos
Hardware	• Intel Pentium 4 (2 GHz) o un procesador posterior • 500 MB de RAM libre (se recomiendan 4 GB de RAM) • 2 GB de espacio libre en disco si `/var`, `/opt` y `/tmp` comparten el mismo sistema de archivos o volumen • 500 MB de espacio libre en disco en cada `/var`, `/opt` y `/tmp` si están en volúmenes diferentes
Sistemas operativos	• Amazon Linux 2 • CentOS 6, 7 y 8 • Debian 9, 10 • Oracle Enterprise Linux 6, 7 y 8 • Red Hat Enterprise Linux 6, 7 y 8 • SuSE Linux Enterprise Server 12.x, 15.x • Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS Para obtener una lista de los kernel de sistemas operativos compatibles, consulte Kernel de Linux compatibles para Symantec Endpoint Protection.

Componente	Requisitos
Otros requisitos del entorno	• Glibc No se admiten sistemas operativos que ejecuten una versión de Glibc anterior a 2.6. • net-tools o iproute2 Symantec Endpoint Protection usa una de estas dos herramientas, dependiendo de cuál está instalada en el equipo. • OpenSSL 1.0.2k-fips o versiones posteriores

Instalación del Agente de Symantec para Linux o del cliente de Symantec Endpoint Protection para Linux

(Para la versión 14.3 RU1 y posteriores)

El Agente de Symantec para Linux se instala directamente en un dispositivo con Linux. No es posible implementar el Agente de Linux desde Symantec Endpoint Protection Manager remotamente.

Para instalar el Agente de Symantec para Linux, cree un paquete de instalación en Symantec Endpoint Protection Manager, transfiera el paquete de instalación a un dispositivo con Linux y, a continuación, ejecute el instalador. El instalador configurará el nuevo agente y lo registrará con Symantec Endpoint Protection Manager.

> **NOTE**
> El Agente de Symantec para Linux 14.3 RU1 y versiones posteriores no pueden ejecutarse como cliente no administrado.Todas las tareas de administración se deben realizar en Symantec Endpoint Protection Manager o en la consola en la nube.

Para la versión 14.3 RU1 y versiones posteriores: Para instalar el Agente de Symantec para Linux

1. Haga clic en Symantec Endpoint Protection Manager, cree y descargue el paquete de instalación.
2. Ponga el paquete en un recurso compartido de la red, un dispositivo USB u otro mecanismo de uso compartido.
   Si los dispositivos donde se desea instalar el Agente de Linux están en una red aislada o no tienen acceso a Internet, configure un repositorio local.Consulte:
   Creación de un repositorio local
3. Instale el Agente de Linux de una de las siguientes formas:

Si se ha transferido el paquete al dispositivo con Linux	1. Vaya a la ubicación de la carpeta y ejecute el siguiente comando para hacer que el archivo **LinuxInstaller** sea ejecutable:
	`chmod u+x LinuxInstaller`
	2. Ejecute el siguiente comando para instalar el agente:
	`./LinuxInstaller`

Si se ha configurado un repositorio local	1. Ejecute el siguiente comando:
	`./LinuxInstaller – --local-repo <URL del repositorio LOCAL>`
	Por ejemplo:
	`./LinuxInstaller – --local-repo https://your-domain.com/sep_linux_agent/14_3RU3`

   Se debe ejecutar el comando como raíz.
   Para ver la lista de opciones de la instalación, ejecute `./LinuxInstaller -h`.
4. Para verificar la instalación, vaya a `/usr/lib/symantec` y ejecute `./status.sh` para confirmar que se han cargado los módulos y que se están ejecutando los daemons:

```
./status.sh
Versión del Agente de Symantec para Linux: 14.3.450.1000
Comprobando el estado del Agente de Symantec para Linux (SEPM)..
Estado de daemon:
```

```
cafagent en ejecución
sisamdagent en ejecución
sisidsagent en ejecución
sisipsagent en ejecución
Estado del módulo:
sisevt cargado
sisap cargado
```

Tenga en cuenta que el `estado de comunicación` solo está disponible para los clientes administrados en la nube.

Para la versión 14.3 MP1 y versiones anteriores

Se instala un cliente de Symantec Endpoint Protection administrado o no administrado directamente en un equipo con Linux. No es posible implementar el cliente de Linux desde Symantec Endpoint Protection Manager remotamente. Los pasos de instalación son similares si es un cliente administrado o no administrado.

La única forma de instalar un cliente administrado es con un paquete de instalación que se crea en Symantec Endpoint Protection Manager. Es posible convertir un cliente no administrado en un cliente administrado en cualquier momento importando la configuración de comunicación entre el cliente y el servidor en el cliente de Linux.

Si el núcleo del sistema operativo Linux no es compatible con el módulo precompilado del núcleo de Auto-Protect, el instalador intenta compilar un módulo compatible del núcleo de Auto-Protect. El proceso de compilación automática se inicia de forma automática si es necesario. Sin embargo, el instalador tal vez no pueda compilar un módulo del núcleo de Auto-Protect compatible. En este caso, Auto-Protect se instala, pero se deshabilita. Para obtener más información, consulte:

Kernels de Linux admitidos para Symantec Endpoint Protection

> **NOTE**
>
> Es necesario tener privilegios de superusuario para instalar el cliente de Symantec Endpoint Protection en el equipo con Linux. El procedimiento usa `sudo` para demostrar esta elevación del privilegio.

Para la versión 14.3 MP1 y anteriores: Para instalar el cliente de Symantec Endpoint Protection para Linux:

1. Copie el paquete de instalación que creó en el equipo con Linux. El paquete es un archivo .zip.
2. En el equipo con Linux, abra una ventana de terminal de la aplicación.
3. Navegue al directorio de instalación con el comando siguiente:

   ```
   cd /directory/
   ```

   Donde directory es el nombre del directorio en el cual se ha copiado el archivo .zip.
4. Extraiga el contenido del archivo .zip en un directorio denominado `tmp` con el comando siguiente:

   ```
   unzip "InstallPackage" -d sepfiles
   ```

   Donde `InstallPackage` es el nombre completo del archivo .zip y `sepfiles` representa una carpeta de destino en la cual el proceso de extracción coloca los archivos de instalación.

   Si no existe la carpeta de destino, el proceso de la extracción la crea.
5. Vaya a `sepfiles` con el comando siguiente:

   ```
   cd sepfiles
   ```
6. Para configurar correctamente los permisos del archivo de ejecución en `install.sh`, use el siguiente comando:

   ```
   chmod u+x install.sh
   ```
7. Use el script integrado para instalar Symantec Endpoint Protection con el comando siguiente:

   ```
   sudo ./install.sh -i
   ```

Si se le solicita, escriba la contraseña.

Este script inicia la instalación de los componentes de Symantec Endpoint Protection. El directorio de instalación predeterminado es el siguiente:

`/opt/Symantec/symantec_antivirus`

El directorio de trabajo predeterminado para LiveUpdate es el siguiente:

`/opt/Symantec/LiveUpdate/tmp`

La instalación se completa cuando la línea de comandos devuelve. No es necesario reiniciar el equipo para completar la instalación.

Para la versión 14.3 MP1 y versiones anteriores

Para verificar la instalación del cliente, haga clic o haga clic con el botón secundario en el escudo amarillo de Symantec Endpoint Protection y después haga clic en **Abrir Symantec Endpoint Protection**. La ubicación del escudo amarillo varía según la versión de Linux. La interfaz de usuario del cliente muestra información sobre la versión del programa, las definiciones de virus, el estado de conexión del servidor y la administración.

Más información

- Acerca de la compilación automática para el cliente de Symantec Endpoint Protection para Linux
- Acerca de la interfaz gráfica de usuario del cliente Linux
- Cómo importar la configuración de comunicación entre el cliente y el servidor en el cliente de Linux
- Cómo prepararse para la instalación de clientes
- Instalación de Symantec Endpoint Protection 14.x para distribuciones basadas en RedHat

Guía de inicio sobre el Agente de Linux

Es posible que el administrador de Symantec Endpoint Protection Manager haya permitido configurar los valores de configuración en el Agente de Linux.

Table 2: Pasos de inicio en el Agente de Linux (para la versión 14.3 RU1 y posteriores)

Paso	Tarea	Descripción
Paso 1	Instale el Agente de Symantec para Linux.	El administrador de proporciona el paquete de instalación para un cliente administrado o envía un vínculo por correo electrónico para descargarlo.Consulte: Instalación del Agente de Symantec para Linux o del cliente de Symantec Endpoint Protection para Linux
Paso 2	Compruebe que el Agente de Linux se comunica con Symantec Endpoint Protection Manager o con la consola en la nube.	Para confirmar la conexión con Symantec Endpoint Protection Manager o con la consola en la nube, se puede ejecutar el siguiente comando: `/usr/lib/symantec/status.sh`
Paso 3	Verifique que Auto-Protect está en ejecución.	Para comprobar el estado de Auto-Protect, ejecute el siguiente comando: `cat /proc/sisap/status`
Paso 4	Compruebe que las definiciones estén actualizadas.	Las definiciones de LiveUpdate están disponibles en la siguiente ubicación: `/opt/Symantec/sdcssagent/AMD/sef/definitions/`

Table 3: Pasos de inicio en el cliente de Linux (versión 14.3 MP1 y anteriores)

Paso	Tarea	Descripción
Paso 1	Instale el cliente Linux.	El administrador de Symantec Endpoint Protection Manager proporciona el paquete de instalación para un cliente administrado o envía un vínculo por correo electrónico para descargarlo. También puede desinstalar un cliente no administrado, que no se comunica con Symantec Endpoint Protection Manager de ninguna manera. El usuario del equipo principal debe administrar el equipo cliente, actualizar el software y actualizar las definiciones. Puede convertir un cliente no administrado en un cliente administrado. Consulte: Instalación del Agente de Symantec para Linux o del cliente de Symantec Endpoint Protection para Linux
Paso 2	Compruebe que el cliente Linux se comunica con Symantec Endpoint Protection Manager.	Haga doble clic en el escudo de Symantec Endpoint Protection. Si el cliente se comunica correctamente con Symantec Endpoint Protection Manager, la información del servidor se mostrará en **Administración** , junto a **Servidor**. Si ve **Sin conexión**, póngase en contacto con el administrador de Symantec Endpoint Protection Manager. Si ve **Autoadministrado**, el cliente no está administrado. El icono del escudo también indica tanto la administración como el estado de la comunicación.
Paso 3	Verifique que Auto-Protect está en ejecución.	Haga doble clic en el escudo de Symantec Endpoint Protection. El estado de Auto-Protect aparece en **Estado**, junto a **Auto-Protect**. También puede comprobar el estado de Auto-Protect a través de la interfaz de línea de comandos: `sav info -a`
Paso 4	Compruebe que las definiciones estén actualizadas.	LiveUpdate se inicia automáticamente una vez finalizada la instalación. Se puede verificar que las definiciones están actualizadas haciendo doble clic en el escudo de Symantec Endpoint Protection. La fecha de las definiciones se muestra en **Definiciones**. De forma predeterminada, LiveUpdate para el cliente Linux se ejecuta cada cuatro horas. Si las definiciones no están actualizadas, puede hacer clic en **LiveUpdate** para ejecutar LiveUpdate de forma manual. También puede utilizar la interfaz de línea de comandos para ejecutar LiveUpdate: `sav liveupdate -u`
Paso 5	Ejecute un análisis.	De forma predeterminada, el cliente administrado de Linux analiza todos los archivos y carpetas diariamente a las 00:30. Sin embargo, se puede iniciar un análisis manual usando la interfaz de la línea de comandos: sav manualscan -s pathname **Note:** El comando para iniciar un análisis manual requiere privilegios de superusuario.

Más información

Preguntas más frecuentes de Symantec Endpoint Protection para Linux (preguntas frecuentes de SEP para Linux)

Actualización del Agente de Symantec para Linux

(Para la versión 14.3 RU1 y posteriores)

A partir de la versión 14.3 RU1, el instalador del cliente de Linux detecta y desinstala el cliente de Linux heredado (anterior a la versión 14.3 RU1) y, a continuación, realiza una nueva instalación. Las configuraciones antiguas no se conservarán.

Para actualizar el Agente de Symantec para Linux

1. Haga clic en Symantec Endpoint Protection Manager, cree y descargue el paquete de instalación.
   Exportación de paquetes de instalación de clientes
2. Copie el paquete descargado en el dispositivo con Linux.
3. Vaya a la ubicación de la carpeta y ejecute el siguiente comando para hacer que el archivo **LinuxInstaller** sea ejecutable:

   ```
   chmod u+x LinuxInstaller
   ```
4. Ejecute el siguiente comando para desinstalar el agente existente y volver a instalar el Agente de Symantec para Linux:

   ```
   ./LinuxInstaller
   ```

   Ejecute el comando como raíz.
5. Para verificar la instalación, vaya a `/usr/lib/symantec` y ejecute el script `./status.sh` para confirmar que se han cargado los módulos y que se están ejecutando los daemons:

   ```
   ./status.sh
   Versión del Agente de Symantec para Linux: 14.3.450.1000
   Comprobando el estado del Agente de Symantec para Linux (SEPM)..
   Estado de daemon:
   cafagent en ejecución
   sisamdagent en ejecución
   sisidsagent en ejecución
   sisipsagent en ejecución
   Estado del módulo:
   sisevt cargado
   sisap cargado
   ```

Actualización de los módulos de kernel para el Agente de Symantec para Linux

El Agente de Symantec para Linux es el mismo cliente, ya se administre desde Symantec Endpoint Protection Manager o desde la consola en la nube.

(Para la versión 14.3 RU1 y posteriores)

Siempre que se lanza una nueva actualización del kernel de Linux, se debe actualizar el Agente de Symantec para Linux para esa plataforma para admitir el nuevo kernel. Para hacer que el proceso sea más eficaz, los módulos de kernel del Agente de Linux se pueden actualizar ahora usando el repositorio de Linux.

> **NOTE**
> Asegúrese de que los agentes puedan conectarse al servidor de repositorio de Symantec (https://linux-repo.us.securitycloud.symantec.com/) para descargar las actualizaciones del módulo de kernel.

Siempre que se ejecuta el comando `yum update` en un sistema RHEL, Amazon Linux, Oracle Linux o CentOS, el comando también busca nuevos paquetes de agente. Si una actualización está disponible, se descargará el módulo de kernel más reciente y el agente se actualizará automáticamente. Una vez actualizado el módulo de kernel, se debe reiniciar la instancia para que la actualización surta efecto.

Alternativamente, se puede actualizar el módulo de kernel del agente ejecutando el siguiente comando en la instancia. Abra una ventana de terminal con privilegios de raíz, vaya a `/usr/lib/symantec/` y ejecute el siguiente comando:

```
/usr/lib/symantec/installagent.sh --update-kmod
```

Para actualizar los módulos de kernel en sistemas Ubuntu

1. Para actualizar la base de datos de paquetes local, escriba los comandos siguientes:
   ```
   sudo apt-get clean
   sudo apt-get update
   ```
2. Para actualizar al último módulo del kernel, escriba los siguientes comandos:
   ```
   /usr/lib/symantec/installagent.sh --update-kmod
   ```
   Se requieren privilegios de superusuario para realizar esta acción.

Para actualizar los módulos de kernel en un entorno restringido sin conexión a Internet

1. Método 1: Transfiera manualmente el último paquete KMOD a un sistema que no tenga ninguna conexión a Internet, adjunte el paquete KMOD a LinuxInstaller y, a continuación, ejecute LinuxInstaller.
   1. En un sistema que tenga conexión a Internet, descargue el paquete KMOD.
      ```
      ./LinuxInstaller -d
      ```
   2. Copie y pegue manualmente el paquete KMOD en el agente que desea actualizar.
   3. Enumere los paquetes adjuntos.
      ```
      ./LinuxInstaller -l
      ```
   4. Adjunte el nuevo paquete KMOD a LinuxInstaller.
      ```
      tar czf - [KMOD-package-name] >> LinuxInstaller
      ```
   5. Asegúrese de que el nuevo paquete KMOD esté incluido en la lista de paquetes adjuntos.
      ```
      ./LinuxInstaller -l
      ```
   6. Ejecute el instalador para actualizar los módulos de kernel.
      ```
      ./LinuxInstaller -- --update-kmod
      ```
2. Método 2: Configure un repositorio local y edite la configuración del repositorio de modo que el agente use el repositorio local en vez del repositorio predeterminado de Symantec.
   1. Configure el repositorio local que aloja los paquetes KMOD.
      Para obtener información sobre cómo crear un repositorio local, consulte la documentación de la distribución de Linux correspondiente que se está utilizando.
   2. En el equipo cliente, ejecute el siguiente comando para redirigirlo para usar el repositorio local:
      ```
      ./LinuxInstaller --local-repo <URL_repositorio_local>
      ```
      Ejemplo de dirección URL: `--local-repo 'http://<IP_o_nombrehost_repositorio>:<puerto_opcional>/sep_linux'`
   3. Para actualizar KMOD, ejecute:
      ```
      ./LinuxInstaller -- --update-kmod
      ```

Si actualiza los módulos de kernel del sistema operativo, también debe actualizar la actualización del módulo de kernel correspondiente para el cliente de Symantec Endpoint Protection. Sin los módulos de kernel compatibles, es posible que el cliente de Symantec Endpoint Protection no funcione correctamente y que algunas funciones estén deshabilitadas.

Más información

Creación e instalación de un paquete de instalación del Agente de Linux de Symantec

Administración del cliente de Linux usando la herramienta de línea de comandos (sav)

La herramienta de la línea de comandos del cliente de Linux le permite controlar y comprobar el cliente de Linux.

Para administrar el cliente de Linux usando la herramienta de la línea de comandos, consulte:

(Para la versión 14.3 RU2 y posteriores)

La herramienta de la línea de comandos del cliente de Linux le permite controlar y comprobar el cliente de Linux.

Para administrar el cliente de Linux usando la herramienta de la línea de comandos

1. En un equipo cliente de Linux, navegue a la siguiente ubicación:
   `/opt/Symantec/sdcssagent/AMD/tools`
2. Ejecute el comando sav de la siguiente manera:
   `Comando ./sav [opciones]`

Table 4: Opciones para sav

Opción	Descripción	Se aplica a
`-q`	Silencioso	A partir de la versión 14.3 RU2
`-h`	Muestra las opciones y los comandos disponibles para sav.	A partir de la versión 14.3 RU2

Table 5: Comandos para sav

Opción	Descripción	Se aplica a
`autoprotect -e`	Habilita Auto-Protect. Para comprobar el estado de Auto-Protect, ejecute el siguiente comando: `[root@localhost tools]# cat /proc/sisap/status | grep -i MODE` La respuesta puede ser una de las siguientes: • `mode=ENA` (si está habilitado) • `mode=DIS` (si está deshabilitado)	A partir de la versión 14.3 RU2
`autoprotect -d`	Deshabilita Auto-Protect.	A partir de la versión 14.3 RU2
`info -d`	Muestra la versión y la fecha de las definiciones actuales de virus y riesgos para la seguridad en uso en el dispositivo.	A partir de la versión 14.3 RU3
`info -e`	Muestra la versión del motor de análisis en uso en el dispositivo.	A partir de la versión 14.3 RU3
`info -p`	Muestra la versión del Agente de Symantec en uso en el dispositivo.	A partir de la versión 14.3 RU3
`info -a`	Muestra el estado de Auto-Protect en el dispositivo.	A partir de la versión 14.3 RU3
`liveupdate -u`	Ejecuta LiveUpdate de forma inmediata.	A partir de la versión 14.3 RU3
`manage -i <archivo>`	Importa el archivo *sylink.xml* en la ubicación especificada.	A partir de la versión 14.3 RU2

Opción	Descripción	Se aplica a
`manualscan -s <lista de archivos>`	Inicia un análisis manual. <lista de archivos> especifica la lista de archivos y directorios que se desea analizar. Para especificar esta lista, escriba una lista de archivos y directorios separados por avances de línea y que terminen con una señal de fin de archivo, por ejemplo, CTRL-D. Si se especifica un directorio, también se analizarán todos los subdirectorios. Se admiten caracteres comodín. De forma predeterminada, el número máximo de elementos que se pueden agregar a un análisis manual que se ha iniciado desde la interfaz de línea de comandos es 100. Es posible usar **symcfg** para cambiar el valor DWORD de VirusProtect6MaxInput para aumentar este límite. Para eliminar el límite totalmente, configure el valor de VirusProtect6MaxInput en 0. Si especifica un guion (-) en vez de una lista de archivos y directorios, la lista de nombres de ruta se lee desde la entrada estándar. Es posible usar comandos que produzcan una lista de archivos o nombres de ruta separados por avances de línea.Enviar una lista de elementos muy larga a este comando puede afectar negativamente el rendimiento. Symantec recomienda limitar las listas a un máximo de unos pocos miles de elementos.	A partir de la versión 14.3 RU3
`manualscan -t`	Detiene un análisis manual que esté en curso.	A partir de la versión 14.3 RU3

Más información

Solución de problemas del Agente de Symantec para Linux

Solución de problemas del Agente de Symantec para Linux

La tabla siguiente muestra los recursos para solucionar problemas del Agente de Symantec para Linux (a partir de la versión 14.3 RU1).

Table 6: Recursos para solución de problemas del Agente de Symantec para Linux

Acción	Descripción
Comprobar el estado del agente.	Para comprobar la versión y el estado de conexión del agente, para confirmar que los módulos están cargados y para comprobar que los daemons están en ejecución, vaya a `/usr/lib/symantec` y ejecute el comando siguiente: `./status.sh`
Comprobar las versiones de los paquetes del agente.	Vaya a `/usr/lib/symantec` y ejecute el siguiente comando: `./version.sh`

Visualizar los registros.	Se encuentran los registros del Agente de Symantec para Linux en las siguientes ubicaciones:
	• Registro de AMD: proporciona información relacionada con el análisis.
	`/var/log/sdcsslog/amdlog`
	• Registro de CAF: proporciona información relacionada con actividades del agente como, por ejemplo, comunicación con el servidor, inscripción, comandos, eventos, etc.
	`/var/log/sdcss-caflog/`
	• Registro del agente: proporciona información relacionada con las actividades del agente.
	`/var/log/sdcsslog/SISIDSEvents*.csv`
	• Registro de CVE: proporciona información relacionada con la comunicación entre Symantec Endpoint Protection Manager y el agente.
	`/var/log/sdcss-caflog/cve.log`

Acción	Descripción
Recopilar los registros en un archivo ZIP.	Se puede utilizar el script `GetAgentInfo` para recopilar todos los archivos del registro en un archivo ZIP que se puede enviar al departamento de soporte al cliente. 1. Inicie sesión en el sistema del Agente de Symantec para Linux. 2. Vaya a `/opt/Symantec/sdcssagent/IPS/tools/`. 3. Ejecute `./getagentinfo.sh` como raíz. 4. Se creará un archivo ZIP en el directorio `/tmp/`. El nombre del archivo será similar a `20201208_184935_0001_CU_mihsan-rhel8.zip` `-out <directorio>` permite cambiar la ubicación y el nombre del archivo ZIP generado.
Cambiar el nivel de registro de CVE.	De forma predeterminada, el nivel de registro de CVE es `info`. Se puede cambiar el nivel de registro a `debug` en el archivo `/opt/Symantec/cafagent/bin/log4j.properties`. Después de cambiar el archivo, se debe reiniciar el servicio `cafagent`.

Cambiar el nivel de registro de AMD.	De forma predeterminada, el nivel de registro de AMD es `info`.
	Se puede cambiar el nivel de registro a `trace`, `warning` o a `error` en el archivo `/opt/Symantec/sdcssagent/AMD/system/AntiMalware.ini`.
	Note: Antes de modificar el archivo AntiMalware.ini, detenga sisamdagent:
	`service sisamdagent stop`
	Note: Una vez que se modifique el archivo, reinicie el servicio:
	`service sisamdagent start`

Desinstalación del Agente de Symantec para Linux o del cliente de Symantec Endpoint Protection para Linux

Se desinstala el cliente de Symantec Endpoint Protection para Linux con el script que la instalación proporciona.

> **NOTE**
>
> Es necesario tener privilegios de superusuario para desinstalar el cliente de Symantec Endpoint Protection en el equipo con Linux. El procedimiento usa `sudo` para demostrar esta elevación del privilegio.

Para la versión 14.3 RU1 y versiones posteriores: Para desinstalar el Agente de Symantec para Linux

1. En el equipo con Linux, abra una ventana de terminal de la aplicación.
2. Vaya al siguiente directorio:
   `/usr/lib/symantec/`
3. Ejecute el siguiente script integrado para desinstalar el Agente de Symantec para Linux:
   `./uninstall.sh`
4. Reinicie el equipo después de que finalice la desinstalación y aparezca la solicitud de reinicio.
   Tenga en cuenta que el script `uninstall.sh` eliminará todos los componentes del Agente de Symantec para Linux (`sdcss-caf`, `sdcss-sepagent` y `sdcss-kmod`).

```
[root@localhost symantec]# ./uninstall.sh
Running ./uninstall.sh (PWD /usr/lib/symantec; version 2.2.4.41)
Uninstalling Symantec Agent for Linux (SEPM) ...
Removing packages sdcss-caf sdcss-sepagent sdcss-kmod sdcss-scripts
Symantec Agent for Linux (SEPM) uninstalled successfully.
A reboot is required to complete uninstallation.
Please reboot your machine at the earliest convenience.
```

Para la versión 14.3 MP1 y anteriores: Para desinstalar el cliente de Symantec Endpoint Protection para Linux:

1. En el equipo con Linux, abra una ventana de terminal de la aplicación.
2. Vaya a la carpeta de instalación de Symantec Endpoint Protection con el comando siguiente:

   `cd /opt/Symantec/symantec_antivirus`

   La ruta es la ruta de instalación predeterminada.
3. Use el script integrado para desinstalar Symantec Endpoint Protection con el comando siguiente:

   `sudo ./uninstall.sh`

   Si se le solicita, escriba la contraseña.

   Este script inicia la desinstalación de los componentes de Symantec Endpoint Protection.
4. En la ventana emergente, escriba `Y` y después presione **Intro**.

   La desinstalación se completa cuando la línea de comandos devuelve.

   NOTE

   En algunos sistemas operativos, si el único contenido de la carpeta `/opt` son los archivos del cliente de Symantec Endpoint Protection, el script de desinstalación además elimina `/opt`. Para volver a crear esta carpeta, escriba el siguiente comando: `sudo mkdir /opt`

Para desinstalar usando un administrador de paquetes o un administrador del software, consulte la documentación específica de su distribución de Linux.


Symantec
A Division of Broadcom