System Center Endpoint Protection

Manual de instalación y guía del usuario

Red Hat Enterprise Linux Server 5, 6
SUSE Linux Enterprise 10, 11
CentOS 5, 6
Debian Linux 5, 6
Ubuntu Linux 10.04, 12.04
Oracle Linux 5, 6

Microsoft

Microsoft® System Center Endpoint Protection

Contenido

Introducción

Gracias por utilizar System Center Endpoint Protection. El motor de análisis de última generación de Microsoft no tiene parangón en lo que a velocidad de análisis y tasas de detección se refiere; además, gracias a lo reducido de su impacto, es la opción ideal para cualquier servidor del sistema operativo Linux.

Funcionalidad principal

Análisis a petición

El análisis a petición lo puede iniciar un usuario con privilegios (por lo general un administrador del sistema) mediante la interfaz de la línea de comandos, la interfaz web o la herramienta de planificación automática del sistema operativo (p. ej., cron). El término *a petición* hace referencia a objetos del sistema de archivos que se estén analizando a petición del usuario o del sistema.

Protección en tiempo real

La protección en tiempo real se invoca siempre que un usuario y/o sistema operativo intente acceder a objetos del sistema de archivos. Esto también sirve para clarificar el término *al acceder*, el cual se refiere a un análisis que se activa ante cualquier intento de acceso a los objetos del sistema de archivos.

Características principales del sistema

Avanzados algoritmos del motor

Los algoritmos del motor de análisis antivirus de Microsoft proporcionan la máxima tasa de detección y los tiempos más rápidos de análisis.

Multiprocesamiento

System Center Endpoint Protection está desarrollado para ejecutarse el unidades con uno o varios procesadores.

Heurística avanzada

System Center Endpoint Protection incluye una heurística avanzada exclusiva para los gusanos Win32, las infecciones por la puerta trasera y otras formas de código malicioso.

Características integradas

Los archivadores integrados desempaquetan objetos de archivos comprimidos sin necesidad de ningún programa externo.

Velocidad y eficacia

Con el fin de aumentar la velocidad y la eficacia del sistema, la arquitectura de System Center Endpoint Protection se basa en el demonio en ejecución (programa residente) al que se envíen todas las solicitudes de análisis.

Seguridad mejorada

Todos los demonios ejecutables (excepto scep_dac) se ejecutan con una cuenta de usuario sin privilegios para, de este modo, mejorar la seguridad.

Configuración selectiva

El sistema es compatible con la configuración selectiva en función del usuario o del cliente/servidor.

Varios niveles de registro

Los distintos niveles de registro se pueden configurar para obtener información acerca de la actividad y las amenazas del sistema.

Interfaz web

La intuitiva interfaz web de fácil acceso pone la configuración y la administración en manos del usuario.

Sin bibliotecas externas

La instalación de System Center Endpoint Protection no necesita de bibliotecas ni programas externos, excepto la LIBC.

Notificación especificada por el usuario

El sistema se puede configurar para que notifique a determinados usuarios en el casos de detectarse un amenaza u otros sucesos importantes.

Requisitos del sistema reducidos

Para poderse ejecutar con eficacia, System Center Endpoint Protection solamente necesita 16 MB de espacio en el disco duro y 32 MB de RAM. Se ejecuta con fluidez en las versiones 2.2.x, 2.4.x y 2.6.x del kernel del sistema operativo Linux.

Rendimiento y escalabilidad

Desde los servidores de oficina, que requieren una baja alimentación, hasta los miles de usuarios de los servidores ISP empresariales, System Center Endpoint Protection proporciona el rendimiento y la escalabilidad que se esperan de una solución basada en UNIX, además de la seguridad sin parangón de los productos de seguridad de Microsoft.

Terminología y abreviaturas

En esta sección revisaremos los términos y abreviaturas que se utilizan en este documento. Tenga en cuenta que la letra en negrita se reserva para los nombres de componentes de productos, así como para los términos y abreviaturas recién definidos. Los términos y abreviaturas que se definen en este documento se amplían más adelante en este documento.

SCEP

SCEP es el acrónimo estándar para los productos de seguridad desarrollados por Microsoft para varios sistemas operativos Linux. A su vez, es el nombre del paquete de software que contiene los productos.

SCEP daemon

El control principal del sistema SCEP y el demonio de análisis: *scep_daemon*.

Directorio base de SCEP

El directorio en el que se guardan los módulos cargables de SCEP que contienen la base de firmas de virus. Para hacer referencia a este directorio de aquí en adelante, se utilizará la abreviatura *@BASEDIR@*. Se enumera a continuación el valor de *@BASEDIR@* (en función del sistema operativo):

```
Linux: /var/opt/microsoft/scep/lib
```

Directorio de configuración de SCEP

El directorio en el que se guardan todos los archivos relacionados con la configuración de System Center Endpoint Protection. Para hacer referencia a este directorio de aquí en adelante, se utilizará la abreviatura *@ETCDIR@*. Se enumera a continuación el valor de *@ETCDIR@* (en función del sistema operativo):

```
Linux: /etc/opt/microsoft/scep
```

Archivo de configuración de SCEP

Archivo de configuración principal de System Center Endpoint Protection. La ruta absoluta del archivo es la siguiente:

@ETCDIR@/scep.cfg

Directorio de archivos binarios de SCEP

El directorio en el que se guardan todos los archivos binarios relevantes de System Center Endpoint Protection. Para hacer referencia a este directorio de aquí en adelante, se utilizará la abreviatura *@BINDIR@*. Se enumera a continuación el valor de *@BINDIR@* (en función del sistema operativo):

```
Linux: /opt/microsoft/scep/bin
```

Directorio de archivos binarios del sistema de SCEP

El directorio en el que se guardan todos los archivos binarios relevantes del sistema de System Center Endpoint Protection. Para hacer referencia a este directorio de aquí en adelante, se utilizará la abreviatura *@SBINDIR@*. Se enumera a continuación el valor de *@SBINDIR@* (en función del sistema operativo):

```
Linux: /opt/microsoft/scep/sbin
```

Directorio de archivos de objetos de SCEP

El directorio en el que se guardan todos los archivos de objetos y las bibliotecas de System Center Endpoint Protection. Para hacer referencia a este directorio de aquí en adelante, se utilizará la abreviatura *@LIBDIR@*. Se enumera a continuación el valor de *@LIBDIR@* (en función del sistema operativo):

```
Linux: /opt/microsoft/scep/lib
```

Instalación

System Center Endpoint Protection se distribuye como un archivo binario:

```
scep.i386.ext.bin
```

En el archivo binario mostrado anteriormente, *'ext'* es un sufijo que depende de la distribución del sistema operativo Linux, es decir, 'deb' para Debian, 'rpm' para RedHat y SuSE y 'tgz' para otras distribuciones del sistema operativo Linux.

Para instalar o actualizar el producto, utilice el siguiente comando:

```
sh ./scep.i386.ext.bin
```

para ver el acuerdo de aceptación de licencia para el usuario del producto. Una vez que haya confirmado el acuerdo de aceptación, el paquete de instalación se colocará en el directorio de trabajo actual y se mostrará en pantalla la información relevante con relación a la instalación, desinstalación y actualización del paquete.

Una vez que se haya instalado el paquete, podrá utilizar el siguiente comando para verificar que el servicio principal de SCEP se esté ejecutando:

```
ps -C scep_daemon
```

Tras pulsar INTRO, debería ver el siguiente mensaje (o uno similar):

```
 PID TTY TIME CMD
2226 ? 00:00:00 scep_daemon
2229 ? 00:00:00 scep_daemon
```

Al menos dos procesos del demonio de SCEP se están ejecutando en segundo plano. El primer PID representa el administrador de procesos y subprocesos del sistema. El otro representa el proceso de análisis de SCEP.

Instalación de un paquete de idioma

Para instalar el paquete de idioma necesario para System Center Endpoint Protection, utilice el siguiente comando:

```
sh ./scep-lang.lng.bin
```

donde *'lng'* se debe sustituir por el código de idioma del archivo que desee importar.

Después de que aparezca la notificación *Installation completed successfully*, actualice la variable del sistema LANG como corresponda y, si es necesario, actualice el entorno. Con esto concluye la instalación del paquete de idioma.

Cada paquete de idioma contiene los siguientes elementos:

- Interfaz web localizada
- Salidas localizadas de los agentes y comandos SCEP de la consola
- Documentación en PDF localizada

Visión general acerca de la arquitectura

Una vez que System Center Endpoint Protection se haya instalado con éxito, habrá de familiarizarse con su arquitectura.

El sistema consta de las siguientes partes:

NÚCLEO

El núcleo de System Center Endpoint Protection es el demonio de SCEP (scep_daemon). El demonio utiliza el archivo libscep.so de la biblioteca de la API de SCEP y el archivo em00X_xx.dat de los módulos de carga de SCEP para proporcionar tareas básicas del sistema, tales como análisis, mantenimiento de los procesos del agente demonio, mantenimiento del sistema de envío de muestras, registros, notificaciones, etc. Consulte la página *scep_daemon(8)* del manual para obtener información detallada.

AGENTES

El objetivo de los módulos del agente de SCEP es integrar SCEP con el entorno del servidor del Linux.

UTILIDADES

Los módulos de utilidades proporcionan un sencilla y efectiva gestión del sistema. Son los responsables de tareas del sistema como la gestión de la cuarentena, así como de la configuración y actualización del sistema.

CONFIGURACIÓN

La correcta configuración es el aspecto más importante de un sistema de seguridad; el resto de este capítulo está dedicado a la explicación de todos los componentes relacionados. También se recomienda una comprensión exhaustiva del archivo *scep.cfg*, ya que contiene información que es esencial para la configuración de System Center Endpoint Protection.

Una vez que se haya instalado correctamente el producto, todos los componentes de su configuración se guardan en el directorio de configuración de SCEP. El directorio consta de los siguientes archivos:

@ETCDIR@/scep.cfg

Se trata del archivo de configuración más importante, ya que controla todos los aspectos principales de la funcionalidad del producto. El archivo scep.cfg se compone de varias secciones, cada una de las cuales contiene varios parámetros. El archivo contiene una sección global y varias «de agentes», con todos los nombres de secciones entre corchetes. Los parámetros de la sección global se utilizan para definir las opciones de configuración para el demonio de SCEP, así como los valores predeterminados para la configuración del motor de análisis de SCEP. Los parámetros de las secciones de agente permiten definir las opciones de configuración de los módulos utilizados para interceptar diferentes tipos de flujos de datos en el ordenador y/o en su entorno, así como para preparar este para el análisis. Tenga en cuenta que, además de los diversos parámetros que se utilizan para la configuración del sistema, también hay reglas que rigen la organización del archivo. Para obtener información detallada acerca del modo más eficaz de organizar este archivo, consulte las páginas *scep.cfg(5)* y *scep_daemon(8)* del manual, así como las páginas relevantes del manual de los agentes.

@ETCDIR@/certs

El directorio se utiliza para guardar los certificados que usa la interfaz web de SCEP para la autentificación. Consulte la página *scep_wwwi(8)* del manual para obtener información detallada.

@ETCDIR@/scripts/daemon_notification_script

Si lo ha activado el parámetro *'exec_script'* del archivo de configuración, este script se ejecuta cuando se da la condición de que el sistema antivirus detecte una amenaza. Se utiliza para enviar al administrador del sistema notificaciones por correo electrónico con relación al suceso.

Integración con los servicios del sistema de archivos

En este capítulo se describe la configuración de la protección a petición y en tiempo real, la cual supone la protección más eficaz frente a infecciones en el sistema de archivos a causa de virus y gusanos. La potencia de análisis de System Center Endpoint Protection procede del comando de análisis a petición *'scep_scan'* y del comando de análisis al acceder *'scep_dac'*. La versión Linux de System Center Endpoint Protection ofrece una técnica adicional de análisis a petición que hace uso del módulo de biblioteca precargado *libscep_pac.so*. Todos estos comandos se describen en las siguientes secciones.

Análisis a petición

El análisis a petición lo puede iniciar un usuario con privilegios (por lo general un administrador del sistema) mediante la interfaz de la línea de comandos, la interfaz web o la herramienta de planificación automática del sistema operativo (p. ej., cron). El término *a petición* hace referencia a objetos del sistema de archivos que se analizan a petición del usuario o del sistema.

El análisis a petición no necesita ninguna configuración especial para poder ejecutarse. Una vez que el paquete SCEP se ha instalado correctamente, el análisis a petición se puede ejecutar inmediatamente mediante la interfaz de línea de comandos o la herramienta Planificador de tareas. Para ejecutar el análisis a petición desde la línea de comandos, utilice la siguiente sintaxis:

```
@SBINDIR@/scep_scan [option(s)] FILES
```

donde FILES (archivos) es una lista de los directorios y/o archivos que se hayan de analizar.

El análisis a petición de SCEP cuenta con varias opciones para la línea de comandos. Si desea ver la lista completa de opciones, consulte la página *scep_scan(8)* del manual.

Protección en tiempo real proporcionada por Dazuko

La protección en tiempo real se invoca cuando un usuario y/o un sistema operativo accede a objetos del sistema de archivos. Esto también explica el término *al acceder*, el cual se refiere a un análisis que se activa ante cualquier intento de acceso a un objeto seleccionado del sistema de archivos.

Dazuko (pronunciado 'da-tzu-ko') proporciona la técnica que utiliza el análisis a petición de SCEP. El proyecto Dazuko es de código abierto, lo cual quiere decir que su código fuente se puede distribuir sin restricciones. Esto permite que los usuarios puedan compilar el módulo del kernel para sus propios kérneles personalizados. Tenga en cuenta que el módulo del kernel Dazuko no forma parte de ningún producto de SCEP y que se ha de compilar e instalar en el kernel antes de utilizar el comando al acceder *scep_dac*. La técnica Dazuko hace que el análisis al acceder sea independiente del tipo de sistema de archivos que se utilice. También es adecuado para el análisis de objetos del sistema de archivos vía Network File System (NFS), Nettalk y Samba.

Importante: antes de que se proporcione información detallada acerca de la configuración y el uso del análisis al acceder, debe señalarse que, en principio, el análisis se ha desarrollado y comprobado para proteger sistemas de archivos montados de manera externa. Si hay varios sistemas de archivos que no estén montados de este modo, habrá de excluirlos del control de acceso a archivos para evitar que el sistema se cuelgue. Entre los directorios que suelen deber excluirse está *'/dev'* y cualesquiera directorios que utilice SCEP.

Fundamento del funcionamiento

La protección en tiempo real *scep_dac* (SCEP Dazuko-powered file Access Controller) es un programa residente que proporciona supervisión y control continuos sobre el sistema de archivos. Cada objeto del sistema de archivos se analiza en función de tipos de sucesos personalizables de acceso a archivos. Los siguientes tipos de sucesos son compatibles en la versión actual:

Sucesos de abertura

Para activar este tipo de acceso a archivos, configure el valor del parámetro *'event_mask'* a abrir en la sección **[fac]** del archivo scep.cfg. Así se activará el bit ON_OPEN de la máscara de acceso de Dazuko.

Sucesos de cierre

Para activar este tipo de acceso a archivos, configure el valor del parámetro *'event_mask'* a cerrar en la sección **[fac]** del archivo scep.cfg. Así se activará el bit ON_OPEN de la máscara de acceso de Dazuko. Así se activarán los bits ON_OPEN y ON_CLOSE_MODIFIED de la máscara de acceso de Dazuko.

Nota: algunas versiones del kernel del sistema operativo no son compatibles con la interceptación de sucesos ON_CLOSE. En estos casos, *scep_dac* no supervisará los sucesos de cierre.

Sucesos de ejecución

Para activar este tipo de acceso a archivos, configure el valor del parámetro *'event_mask'* a ejecutar en la sección **[fac]** del archivo scep.cfg. Así se activará el bit ON_EXEC de la máscara de acceso de Dazuko.

La protección en tiempo real garantiza que *scep_daemon* analice primero todos los archivos que se abran, cierren o ejecuten con el fin de que no contengan virus. En función de los resultados del análisis, se denegará o permitirá el acceso a determinados archivos.

Instalación y configuración

Antes de inicializar *scep_dac*, se debe compilar e instalar el módulo del kernel Dazuko en el kernel que se esté ejecutando. Para obtener información detallada acerca de cómo compilar e instalar Dazuko, consulte:

http://www.dazuko.org

Una vez que Dazuko esté instalado, revise y modifique las secciones **[global]** y **[fac]** del archivo de configuración de SCEP (scep.cfg). Tenga en cuenta que el correcto funcionamiento de la protección en tiempo real depende de la configuración de la opción *'agent_type'* de la sección **[fac]** de este archivo. Además, ha de definir los objetos del sistema de archivos (es decir, los directorios y archivos) que la protección en tiempo real deba supervisar. Para llevar a cabo esta tarea, puede definir los parámetros de las opciones *'ctl_incl'* y *'ctl_excl'*, que también se encuentran en la sección **[fac]**. Una vez que haya efectuado cambios en el archivo scep.cfg, puede recargar el demonio de SCEP para, de este modo, forzar la relectura de la configuración recién creada.

Sugerencias

Con el fin de asegurarse de que el módulo de Dazuko se cargue antes de la inicialización del demonio de *scep_dac*, siga estos pasos:

Coloque una copia del módulo de Dazuko en cualquiera de los siguientes directorios reservados para los módulos del kernel:

```
/lib/modules
```

o

```
/modules
```

Haga uso de las utilidades 'depmod' y 'modprobe' del kernel (para el sistema operativo BSD use 'kldconfig' y 'kldload') con el fin de gestionar las dependencias e inicializar correctamente el módulo de Dazuko recién añadido.

En el script de inicialización '/etc/init.d/scep_daemon' de scep_daemon, añada la siguiente línea antes de la declaración de inicialización del demonio.

```
/sbin/modprobe dazuko
```

Para el sistema operativo BSD, se ha de introducir la línea

```
/sbin/kldconfig dazuko
```

en el script '/usr/local/etc/rc.d/scep_daemon.sh'.

Alerta Es de suma importancia que estos pasos se ejecuten en el orden preciso que se ha expuesto. Si el módulo del kernel no se encuentra en el directorio del módulos del kernel, no se cargará correctamente, lo que hará que el sistema se cuelgue.

Protección en tiempo real mediante la biblioteca LIBC de precarga

En las secciones anteriores se ha descrito la integración de la protección en tiempo real proporcionada por Dazuko con los servicios de sistema de archivos Linux/BSD. Puede que la utilización de Dazuko no sea factible en todas las situaciones, incluida la de los administradores de sistemas que mantengan sistemas críticos en los que:

- El código fuente y/o los archivos de configuración relacionados con el kernel en ejecución no estén disponibles
- El kernel sea más monolítico que modular
- El módulo de Dazuko simplemente no sea compatible con el sistema operativo en cuestión

En cualquiera de estos casos, se debe utilizar la técnica de análisis al acceder basada en la biblioteca LIBC de precarga. Consulte los siguientes temas de esta sección para obtener información detallada. Tenga en cuenta que esta sección solo es pertinente para los usuarios del sistema operativo Linux y que contiene información con relación al funcionamiento, instalación y configuración del análisis al acceder mediante la utilización de la biblioteca *'libscep_pac.so'* de precarga.

Fundamento del funcionamiento

La protección en tiempo real *libscep_pac.so* (SCEP Preload library based file Access Controller) es una biblioteca de objetos compartidos que se activa al inicio del sistema. Esta biblioteca se utiliza para las llamadas de LIBC que realizan los servidores del sistema, tales como el servidor FTP o el Samba. Cada objeto del sistema de archivos se analiza en función de tipos de sucesos personalizables de acceso a archivos. Los siguientes tipos de sucesos son compatibles en la versión actual:

Sucesos de abertura

Este tipo de acceso a archivos se activa si la palabra *'open'* está presente en el parámetro *'event_mask'* del archivo esest.cfg (sección **[fac]**).

Sucesos de cierre

Este tipo de acceso a archivos se activa si la palabra *'close'* está presente en el parámetro *'event_mask'* del archivo scep.cfg (sección **[fac]**). En este caso, se interceptan todos los descriptores de archivo y las funciones de cierre de FILE (archivo) de la LIBC.

Eventos de ejecución

Este tipo de acceso a archivos se activa si la palabra *'exec'* está presente en el parámetro *'event_mask'* del archivo scep.cfg (sección **[fac]**). En este caso, se interceptan todas las funciones de ejecución de la LIBC.

El demonio de SCEP analiza todos los archivos abiertos, cerrados y ejecutados para comprobar que no tengan virus. En función de los resultados de tales análisis, se denegará o permitirá el acceso a determinados archivos.

Instalación y configuración

El módulo de biblioteca *libscep_pac.so* se instala mediante un mecanismo de instalación estándar de las bibliotecas precargadas. Habrá de definir la variable de entorno *'LD_PRELOAD'* con la ruta absoluta a la biblioteca *libscep_pac.so*. Para obtener más información, consulte la página *ld.so(8)* del manual.

Nota: es importante que solo se defina la variable de entorno *'LD_PRELOAD'* para los procesos del demonio del servidor de red (FTP, Samba, etc.) que vayan a estar bajo control de la protección en tiempo real. Por lo general, no se recomienda la precarga de llamadas de LIBC de todos los procesos del sistema operativo, dado que puede ralentizar de forma espectacular el rendimiento del sistema e, incluso, hacer que este se cuelgue. En este sentido, no se debe utilizar el archivo '/etc/ld.so.preload' ni exportar de forma global la variable de entorno 'LD_PRELOAD'. Ambas acciones anularían todas las llamadas de LIBC relevantes, lo que podría provocar cuelgues del sistema durante la inicialización.

Para garantizar que solo se intercepten las llamadas de acceso a archivos relevantes en un sistema de archivos en cuestión, las declaraciones ejecutables se pueden anular mediante la siguiente línea:

```
LD_PRELOAD=@LIBDIR@/libscep_pac.so COMMAND COMMAND-ARGUMENTS
```

en la que 'COMMAND COMMAND-ARGUMENTS' es la declaración ejecutable original.

Revise y modifique las secciones **[global]** y **[fac]** del archivo de configuración de SCEP (scep.cfg). Con el fin de que el análisis al acceder funcione correctamente, habrá de definir los objetos del sistema de objetos (es decir, directorios y archivos) que deban estar bajo control de la biblioteca de precarga. Para ello, defina los parámetros de las opciones *'ctl_incl'* y *'ctl_excl'* en la sección **[fac]** del archivo de configuración de SCEP. Una vez que haya efectuado cambios en el archivo scep.cfg, puede recargar el demonio de SCEP para, de este modo, forzar la relectura de la configuración recién creada.

Sugerencias

Con el fin de activar la protección en tiempo real inmediatamente después de que se inicie el sistema, se ha de definir la variable de entorno *'LD_PRELOAD'* en el script de inicialización del servidor de archivos en red adecuado.

Ejemplo: supongamos que queremos realizar el análisis al acceder para supervisar todos los sucesos de acceso al sistema de archivos después de iniciar el servidor Samba. En el script de inicialización del demonio de Samba (/etc/init.d/smb), habremos de sustituir la declaración

```
daemon /usr/sbin/smbd $SMBDOPTIONS
```

por la siguiente línea:

```
LD_PRELOAD=@LIBDIR@/libscep_pac.so daemon /usr/sbin/smbd $SMBDOPTIONS
```

De este modo, al inicio del sistema se analizarán los objetos seleccionados del sistema de archivos que controle Samba.

Mecanismos importantes de SCEP

Directiva de gestión de objetos

El mecanismo de la directiva de gestión de archivos proporciona un filtro para el análisis de objetos en función de su estado. Esta funcionalidad se basa en el las siguientes opciones de configuración:

- action_av
- action_av_infected
- action_av_notscanned
- action_av_deleted

Para obtener información detallada acerca de estas opciones, consulte la página *scep.cfg(5)* del manual.

Todos los objetos procesados se gestionan primero según la configuración de la opción *'action_av'*. Si esta opción está configurada a *'accept'* (o a *'defer'*, *'discard'*, *'reject'*), el objeto se acepta (o se desplaza, descarta o rechaza). Si la opción está configurada a *'scan'*, el objeto se analiza para buscar amenazas de virus, y si la opción *'av_clean_mode'* está en *'yes'*, el objeto también se desinfecta. Además, las opciones de configuración *'action_av_infected'*, *'action_av_notscanned'* y *'action_av_deleted'* también se tienen en cuenta para evaluar con más profundidad la gestión del archivo. Si se ha adoptado la opción *'accept'* como resultado de estas tres opciones de acción, el objeto se acepta. De otro modo, el objeto se bloqueará.

Configuración específica del usuario

El mecanismo de configuración específica del usuario tiene como propósito proporcionar un mayor grado de personalización y funcionalidad. Permite que el administrador del sistema defina los parámetros de análisis del antivirus de SCEP en función del usuario que esté accediendo a los objetos del sistema de archivos.

En la página *scep.cfg(5)* del manual podrá encontrar una descripción detallada de esta funcionalidad. En esta sección solo se proporciona un breve ejemplo de una configuración específica del usuario.

En este ejemplo, el objetivo es utilizar el módulo de *scep_dac* para controlar los sucesos de acceso ON_OPEN y ON_EXEC para un disco externo que esté montado en el directorio /home. Este módulo se puede configurar en la sección **[fac]** del archivo de configuración de SCEP. Observe a continuación:

```
[fac]
agent_type = "dazuko"
event_mask = "open"
ctl_incl = "/home"
action_av = "scan"
```

Para determinar la configuración de análisis de un usuario individual, el parámetro *'user_config'* debe especificar el nombre de archivo de configuración especial en el que se guardarán las reglas de análisis individual. En el ejemplo que aquí se muestra, el archivo de configuración especial se llama *'scep_dac_spec.cfg'* y se encuentra en el directorio de configuración de SCEP. (Este directorio se determina en función del sistema operativo. Consulte la página Terminología y abreviaturas).

```
[fac]
agent_type = "dazuko"
event_mask = "open"
ctl_incl = "/home"
action_av = "scan"
user_config = "scep_dac_spec.cfg"
```

Una vez que se ha especificado el parámetro *'user_config'* del archivo en la sección **[fac]**, se debe crear el archivo *'scep_dac_spec.cfg'* en el directorio de configuración de SCEP. Por último, agregue las reglas de análisis que desee.

```
[username]
action_av = "reject"
```

En la parte superior de la sección especial, introduzca el nombre de usuario al cual se le aplicarán las reglas individuales. Esta configuración permitirá que todos los demás usuarios que intenten acceder al sistema de archivos se procesen con normalidad; es decir, todos los objetos del sistema de archivos a los que accedan otros usuarios se analizarán para comprobar las amenazas, excepto el del usuario *'username'*, cuyo acceso se rechazará (bloqueará).

Planificador de tareas

Entre las funciones del 'Planificador de tareas' se incluyen la ejecución de tareas programadas en un momento determinado o según un suceso específico y la gestión e inicio de tareas con una configuración y unas propiedades predefinidas. La configuración y las propiedades de las tareas se pueden utilizar para influir en las fechas y horas de inicio, pero también para ampliar la aplicación de las tareas mediante la introducción del uso de perfiles personalizados durante la ejecución de las mismas.

La opción *'scheduler_tasks'* está comentada de forma predeterminada, lo que hace que se aplique la configuración predeterminada del Planificador de tareas. En el archivo de configuración de SCEP, todos los parámetros y tareas están separados por puntos y comas. Los demás puntos y comas (y las barras invertidas) deben estar separados por barras invertidas. Cada tarea cuenta con 6 parámetros, y la sintaxis es la siguiente:

- id: número exclusivo
- name: descripción de la tarea
- flags: aquí se pueden configurar indicadores especiales para desactivar la tarea del planificador especificado
- failstart: indica qué se ha de hacer si la tarea no se puede ejecutar en la fecha programada
- datespec: una especificación de fecha periódica con 6 campos (crontab como ampliados por años), una fecha recurrente o una opción de nombre de evento.
- command: puede ser una ruta absoluta a un comando seguido de sus argumentos o un nombre de comando especial con el prefijo @ (p. ej., actualización de antivirus: *@update*).

```
#scheduler_tasks = "id;name;flags;failstart;datespec;command;id2;name2;...";
```

Los siguientes nombres de suceso se pueden utilizar en lugar de la opción datespec:

- start: inicio del demonio
- startonce: inicio del demonio, pero una vez al día a lo sumo
- engine: actualización correcta del motor
- login: inicio de sesión en la interfaz web
- threat: amenaza detectada
- notscanned: archivo no analizado.

Para ver la configuración actual del planificador de tareas, utilice la interfaz web o ejecute el siguiente comando:

```
cat @ETCDIR@/scep.cfg | grep scheduler_tasks
```

Para obtener una descripción completa del 'Planificador de tareas' y de sus parámetros, consulte la correspondiente sección de la página *scep_daemon(8)* del manual.

Interfaz web

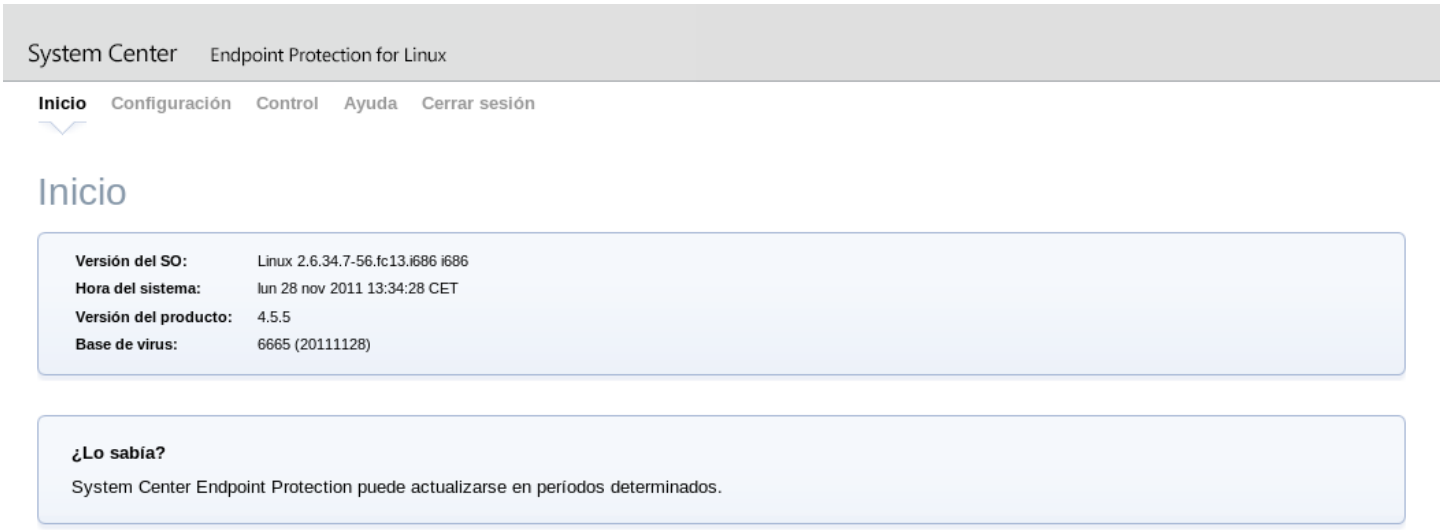
La interfaz web permite una configuración y administración de fácil uso para los sistemas de seguridad de SCEP. Este módulo es un agente independiente y se debe activar de forma explícita. Para configurar con rapidez la *interfaz web*, ajuste las siguientes opciones en el archivo de configuración de SCEP y reinicie el demonio de SCEP.

```
[wwwi]
agent_enabled = yes
listen_addr = address
listen_port = port
username = name
password = pass
```

Sustituya el texto en cursiva por sus propios valores y dirija el navegador hacia *'https://address:port'* (tenga en cuenta la indicación «https»). Inicie sesión con *'username/password'*. Las instrucciones de utilización básica se pueden encontrar en la página de ayuda, mientras que los detalles técnicos acerca de *scep_wwwi* se encuentran en la página *scep_wwwi(1)* del manual.

La interfaz web le permite acceder de forma remota al demonio de SCEP e implementarlo con facilidad. Esta potente utilidad facilita la escritura y la lectura de los valores de configuración.

Figura 6-1. System Center Endpoint Protection: pantalla de inicio.



La interfaz web de System Center Endpoint Protection se divide en dos secciones principales. La ventana principal, que sirve para ver el contenido de la opción del menú que se seleccione y el menú principal. La barra horizontal de la parte superior le permite navegar entre las siguientes opciones principales:

- **Inicio**: proporciona información básica acerca del sistema y del producto de Microsoft
- **Configuración**: aquí puede cambiar la configuración del sistema de System Center Endpoint Protection
- **Control**: le permite ejecutar tareas sencillas y ver las estadísticas globales acerca de los objetos procesados por scep_daemon
- **Ayuda**: proporciona instrucciones detalladas de uso de la interfaz web de System Center Endpoint Protection
- **Cerrar sesión**: se utiliza para finalizar la sesión actual

Importante: asegúrese de hacer clic en el botón **Guardar cambios** tras realizar cualquier cambio en la sección **Configuración** de la interfaz web para, de este modo, guardar la nueva configuración. Para aplicar su configuración, necesitará hacer clic en **Aplicar cambios** en el panel izquierdo para, de este modo, reiniciar el demonio de SCEP.

Ejemplo de configuración de protección en tiempo real

Hay dos formas de configurar SCEP. En nuestro ejemplo, demostraremos cómo usar cualquiera de ellos para configurar el módulo Access Controller, que se describe en el capítulo Protección en tiempo real mediante la biblioteca LIBC de precarga. Puede elegir la opción que más le plazca.

- Utilización del archivo de configuración de SCEP:

```
[fac]
agent_type = "preload"
event_mask = "open"
ctl_incl = "/home"
action_av_deleted = "reject"
action_av = "scan"
action_av_infected = "reject"
```

- Utilización de la interfaz web:

Figura 6-3. SCEP: Configuración > Análisis al acceder.

Cuando modifique la configuración de la interfaz web, acuérdese siempre de hacer clic en **Guardar cambios** para, de este modo, guardar su configuración. Para aplicar los nuevos cambios, haga clic en el botón **Aplicar cambios** del panel de las secciones **Configuración**.

Análisis a petición

Esta sección incluye un ejemplo de cómo ejecutar el análisis a petición para buscar virus.

- Desplácese a **Control > Análisis a petición**
- Introduzca la ruta del directorio que quiera analizar
- Ejecute el analizador de línea de comandos haciendo clic en el botón **Analizar archivos**.

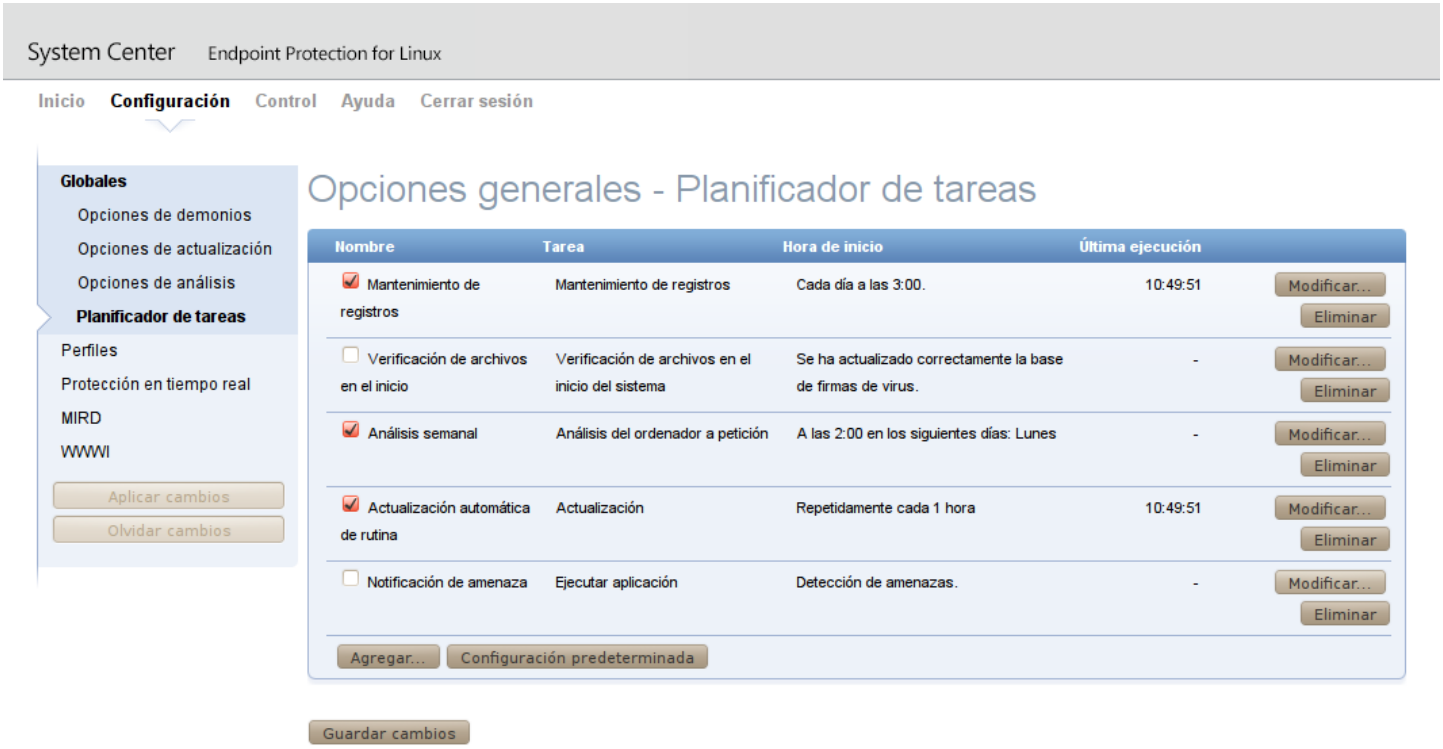
Figura 6-4. SCEP: Control > Análisis a petición.

El análisis de línea de comandos de Microsoft se ejecutará de forma automática en segundo plano. Haga clic en el vínculo **Ver** si desea ver el progreso del análisis. Se abrirá una nueva ventana del navegador.

Planificador de tareas

Puede gestionar las tareas del planificador mediante el archivo de configuración de SCEP (consulte el capítulo Planificador de tareas) o con la interfaz web.

Figura 6-5. SCEP: Global > Planificador de tareas.



Haga clic en la casilla de verificación para activar/desactivar una tarea programada. De forma predeterminada, se muestran las siguientes tareas programadas:

- **Mantenimiento de registros**: el programa elimina automáticamente los registros antiguos para ahorrar espacio en el disco duro. El 'Planificador de tareas' comenzará a desfragmentar los registros. Durante este proceso se eliminarán todas las entradas de registro vacías. De este modo se mejorará la velocidad a la hora de trabajar con registros. La mejora será más perceptible si los registros contienen un gran número de entradas.
- **Verificación de archivos en el inicio**: analiza la memoria y los servicios en ejecución tras la correcta actualización de la base de firmas de virus.
- **Análisis semanal**: analiza todo el sistema de archivos semanalmente (de forma predeterminada los lunes a las 2:00 a.m.). El usuario puede personalizar esta tarea.
- **Actualización automática periódica**: la mejor manera de disfrutar del máximo nivel de seguridad en el ordenador es actualizar System Center Endpoint Protection de forma periódica. Para obtener más información, consulte Utilidad de actualización de SCEP.
- **Notificaciones de amenaza**: de forma predeterminada, todas las amenazas se registrarán en syslog. Además, SCEP se puede configurar para que ejecute un script externo (una notificación) con el que notificar la detección de amenazas al administrador del sistema por correo electrónico.

Estadísticas

Aquí puede ver estadísticas para todos los agentes de SCEP activos. El resumen **Estadísticas** se actualiza cada 10 segundos.

Figura 6-6. SCEP: Control > Estadísticas.

Registro

SCEP proporciona registro del demonio del sistema mediante syslog. *Syslog* es un estándar para el registro de mensajes de programas que se puede utilizar para registrar sucesos del sistema, tales como los relacionados con la red o con la seguridad.

Los mensajes hacen referencia a una aplicación:

```
auth, authpriv, daemon, cron, ftp, lpr, kern, mail, ..., local0, ..., local7
```

El remitente de los mensajes les asigna una prioridad/nivel.

```
Error, Warning, Summall, Summ, Partall, Part, Info, Debug
```

En esta sección se describe cómo configurar y leer la salida de registro de syslog. La opción *'syslog_facility'* (cuyo valor predeterminado es *'daemon'*) define el programa Syslog que se utiliza para el registro. Para modificar la configuración de syslog, edite el archivo de configuración de SCEP o utilice la interfaz web. Modifique el valor del parámetro *'syslog_class'* para cambiar la clase del registro. Le recomendamos no modifique esta configuración a no ser que esté familiarizado con syslog. A continuación podrá ver un ejemplo de configuración de syslog:

```
syslog_facility = "daemon"
syslog_class = "error:warning:summall"
```

El nombre y la ubicación del archivo de registro dependen de la instalación y configuración de syslog (p. ej., rsyslog, syslog-ng, etc.). Los nombres de archivo estándares para los archivos de salida de syslog son, por ejemplo, *'syslog'*, *'daemon.log'*, etc. Para seguir la actividad de syslog, ejecute uno de los siguientes comandos desde la consola:

```
tail -f /var/log/syslog
tail -100 /var/log/syslog | less
cat /var/log/syslog | grep scep | less
```

Importante: debe habilitarse previamente la supervisión del producto SCEP para Linux mediante System Center Operations Manager en el archivo de configuración o mediante la interfaz web de SCEP para su correcto funcionamiento. Asegúrese de que el parámetro *'scom_enabled'* del archivo de configuración anteriormente mencionado esté configurado de la manera siguiente *'scom_enabled = yes'* o cambie el parámetro adecuado en la interfaz web en **Configuración** > **Global** > **Opciones de demonios** > **SCOM activado**.

Actualización del sistema de seguridad de SCEP

Utilidad de actualización de SCEP

Con el fin de mantener la efectividad de System Center Endpoint Protection, la base de firmas de virus debe estar actualizada. La utilidad *scep_update* se ha desarrollado específicamente con este propósito. Consulte la página *scep_update(8)* del manual para obtener información detallada. En el caso de que el servidor acceda a Internet mediante un Proxy HTTP, se deben definir las opciones de configuración adicionales *'proxy_addr'* y *'proxy_port'*. Si el acceso al Proxy HTTP requiere un nombre de usuario y una contraseña, también es preciso definir las opciones *'proxy_username'* y *'proxy_password'* en esta sección. Para iniciar una actualización, introduzca el siguiente comando:

@SBINDIR@/scep_update

Con el objetivo de proporcionar el máximo nivel de seguridad posible para el usuario final, el equipo de Microsoft recopila constantemente definiciones de virus procedentes de todo el mundo: se añaden nuevos patrones a la base de firmas de virus cada muy poco tiempo. Por ello, le recomendamos que inicie actualizaciones de forma periódica. Para poder especificar la frecuencia de las actualizaciones, necesita configurar la tarea *'@update'* en la opción *'scheduler_tasks'* de la sección **[global]** en el archivo de configuración de SCEP. También puede utilizar el Planificador de tareas para determinar la frecuencia de actualización. El demonio de SCEP debe estar activo y ejecutándose para que, de este modo, se pueda actualizar correctamente la base de firmas de virus.

Descripción del proceso de actualización de SCEP

El proceso de actualización consta de dos fases: En la primera se descargan del servidor de Microsoft los módulos de actualización precompilados.

La segunda fase del proceso de actualización es la compilación de módulos que pueda cargar el análisis de System Center Endpoint Protection desde aquellos que se encuentren guardados en el Mirror local. Por lo general, se crean los siguientes módulos de carga de SCEP: módulo de cargador (em000.dat), módulo de análisis (em001.dat), módulo de la base de firmas de virus (em002.dat), módulo de compatibilidad de archivos (em003.dat), módulo de heurística avanzada (em004.dat), etc. Los módulos se crean en el siguiente directorio:

@BASEDIR@

Háganos saber

Esperamos que esta guía le haya proporcionado una comprensión exhaustiva de los requisitos para instalar, configurar y mantener System Center Endpoint Protection. Sin embargo, nuestro objetivo es mejorar continuamente la calidad y la eficacia de nuestra documentación. Si considera que la guía tiene secciones que no están claras o que se han de completar, póngase en contacto con atención al cliente para, de este modo, hacérnoslo saber.

support.microsoft.com

Nos dedicamos a proporcionar el máximo nivel de asistencia: esperamos poder ayudarle en el caso de que tenga algún problema con relación a este producto.

Apéndice A. Licencia PHP

The PHP License, version 3.01 Copyright (c) 1999 - 2006 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.
4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"
5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes PHP software, freely available from <http://www.php.net/software/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.