System Center Módulo de supervisión para Endpoint Protection para Linux

Microsoft Corporation

Publicación: 10/26/2015

Envíe los comentarios o sugerencias acerca de este documento a mpgfeed@microsoft.com. Incluya el nombre de la guía del módulo de administración en su comentario.

El equipo de Operations Manager le invita a enviar comentarios acerca del módulo de supervisión y proporciona una revisión de la página del módulo de administración en el Catálogo de módulos de administración (http://go.microsoft.com/fwlink/?LinkID=82105).

Contenido

Guía del módulo de administración de SCEP

Este módulo de administración le permite administrar System Center Endpoint Protection (SCEP) desde System Center 2012 Operations Manager en un entorno de red, lo que incluye estaciones de trabajo y servidores, desde una ubicación central. Con el sistema de administración de tareas de Operations Manager, puede administrar SCEP en ordenadores remotos, ver alertas y estados, y dar respuesta de forma rápida a nuevos problemas y amenazas.

System Center 2012 Operations Manager no proporciona ninguna otra forma de protección contra el código malicioso. System Center 2012 Operations Manager depende de la presencia de una solución SCEP en ordenadores con el sistema operativo Linux instalado.

Esta guía se ha redactado basándose en la versión 4.5.10.1 del módulo de administración para SCEP.

Historial de guía

Versión	Fecha de lanzamiento	Cambios
4.5.9.1	05/16/2012	Publicación original de esta guía.
4.5.10.1	11/06/2012	Nuevas distribuciones de Linux admitidas. Mejor descripción de algunas herramientas del módulo de administración.

Cambios en la versión 4.5.10.1

La versión 4.5.10.1 del módulo de administración de System Center Endpoint Protection incluye los siguientes cambios:

- Nuevas distribuciones de Linux admitidas:
  - Red Hat Enterprise Linux Server 5
  - SUSE Linux Enterprise 10
  - CentOS 5, 6
  - Debian Linux 5, 6
  - Ubuntu Linux 10.04, 12.04
  - Oracle Linux 5, 6

  Nota: estas nuevas distribuciones solo se admiten con System Center 2012 Operations Manager Service Pack 1 y versiones superiores.
- Mejor descripción de:
  - Monitor de código malicioso activo
  - Alerta de código malicioso activo (de la regla)

Configuraciones compatibles

En general, las configuraciones compatibles se describen en Configuraciones compatibles de Operations Manager 2007 R2 (http://go.microsoft.com/fwlink/?LinkId=90676).

Este módulo de administración requiere System Center 2012 Operations Manager 2007 R2 o posterior. En la siguiente tabla se proporciona información detallada acerca de los sistemas operativos compatibles con este módulo de administración:

Nombre del sistema operativo	x86	x64
Red Hat Enterprise Linux Server 5, 6	Sí	Sí
SUSE Linux Enterprise 10, 11	Sí	Sí
CentOS 5, 6	Sí	Sí
Debian Linux 5, 6	Sí	Sí
Ubuntu Linux 10.04, 12.04	Sí	Sí
Oracle Linux 5, 6	Sí	Sí

Requisitos previos

Para ejecutar este módulo de administración son necesarios los siguientes requisitos:

- System Center Operations Manager 2007 R2 actualización acumulativa 5 (http://support.microsoft.com/kb/2449679)

Los módulos de administración para SCEP que aparecen a continuación se integran en System Center 2012 Operations Manager 2007 R2 o están disponibles para su descarga desde el catálogo en línea.

ID	Nombre	Versión

Microsoft.Linux.Library	Linux Operating System Library	6.1.7000.256
Microsoft.SystemCenter.InstanceGroup.Library	Instance Group Library	6.1.7221.0
Microsoft.SystemCenter.Library	System Center Core Library	6.1.7221.0
Microsoft.SystemCenter.WSManagement.Library	WS-Management Library	6.1.7221.0
Microsoft.SystemCenter.DataWarehouse.Library	Data Warehouse Library	6.1.7221.0
Microsoft.Unix.Library	Unix Core Library	6.1.7000.256
Microsoft.Unix.Service.Library	Unix Service Template Library	6.1.7221.0
Microsoft.Windows.Library	Windows Core Library	6.1.7221.0
System.Health.Library	Health Library	6.1.7221.0
System.Library	System Library	6.1.7221.0

Importante: debe habilitarse previamente la supervisión del producto SCEP para Linux mediante System Center 2012 Operations Manager en el archivo de configuración */etc/opt/microsoft/scep/scep.cfg* 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**.

Archivos incluidos en este módulo de administración

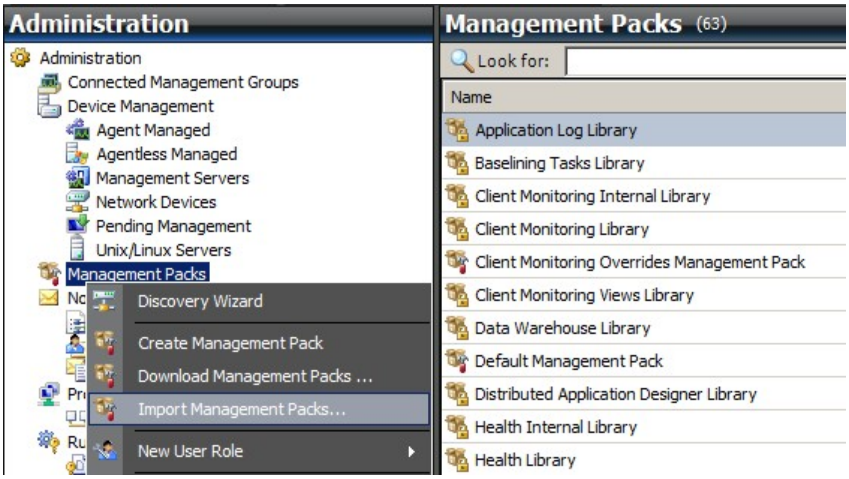
El módulo de administración para SCEP incluye los siguientes archivos:

Nombre de archivo	Descripción
Microsoft.SCEP.Linux.Library.mp	Contiene las definiciones de clase y sus relaciones mutuas, además de las definiciones de tipos de monitores y módulos.
Microsoft.SCEP.Linux.Application.mp	Implementa la supervisión y las alertas, además de las tareas y las vistas.

Inicio rápido

El requisito previo para iniciar la supervisión de SCEP es importar módulos de administración en Operations Manager e identificar los ordenadores que se van a supervisar (proceso conocido como "detección").

Importación de módulos de administración

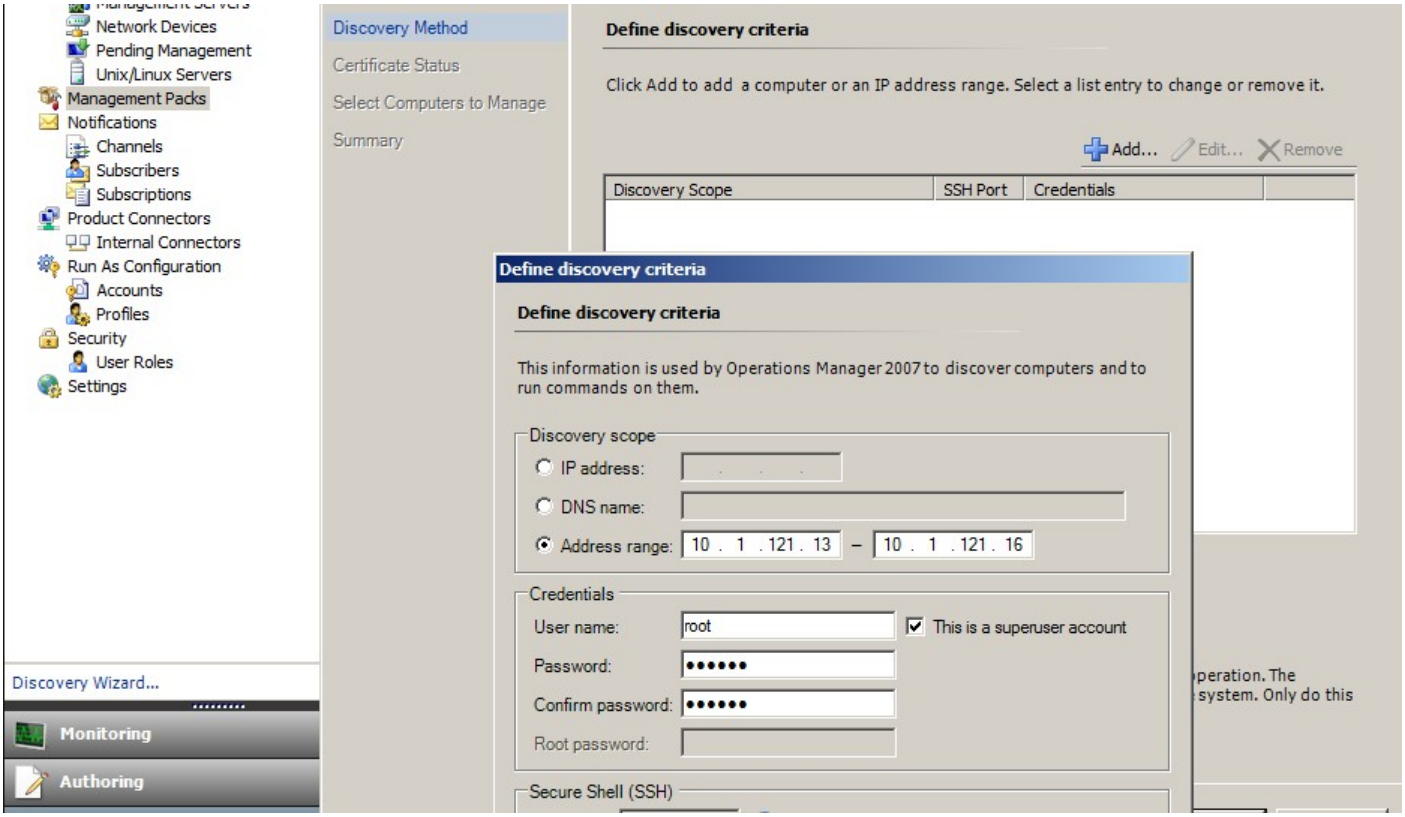


1. Haga clic en el espacio de trabajo **Administration** en el panel izquierdo de la ventana Consola de operaciones.
2. Haga clic con el botón derecho del ratón en **Management Packs** y seleccione **Import Management Packs...** en el menú contextual.
3. En la ventana Módulos de administración, haga clic en el botón **Add** y seleccione **Add from disk...** en el menú desplegable.
4. Confirme que desea que Operations Manager busque e instale también dependencias que no se encuentren en el disco local. Para ello, haga clic en **Yes** en la ventana emergente **Online Catalog Connection**.
5. Asegúrese de seleccionar ambos archivos de la lista (Microsoft.SCEP.Linux.Application.mp y Microsoft.SCEP.Linux.Library.mp) y haga clic en **Install**.

Nota: para obtener más instrucciones acerca de cómo importar un módulo de administración, consulte Importación de un módulo de administración en Operations Manager 2007 (http://go.microsoft.com/fwlink/?LinkId=142351).

Detección

Después de que los archivos *.mp se hayan importado correctamente, tiene que realizar una detección de ordenadores.



1. En el espacio de trabajo **Administration** (en el panel izquierdo de la ventana Consola de operaciones) haga clic en el vínculo **Discovery wizard…** (en la parte inferior del panel izquierdo).
2. En el Asistente de administración de dispositivos y ordenadores, seleccione la opción **Unix/Linux computers** y haga clic en **Next** para continuar.
3. En la sección Definir criterios de detección, haga clic en el botón **Add**.
4. Defina el **Address range** IP que se analizará y las **Credentials** de SSH aplicables a los ordenadores en los que System Center 2012 Operations Manager instalará su agente.
5. Confirme los criterios de ámbito y credenciales haciendo clic en **OK** y haga clic en el botón **Discover** para iniciar el proceso de detección.
6. Finalizada la operación, aparecerá una lista que le permite seleccionar los sistemas que desea supervisar o administrar.

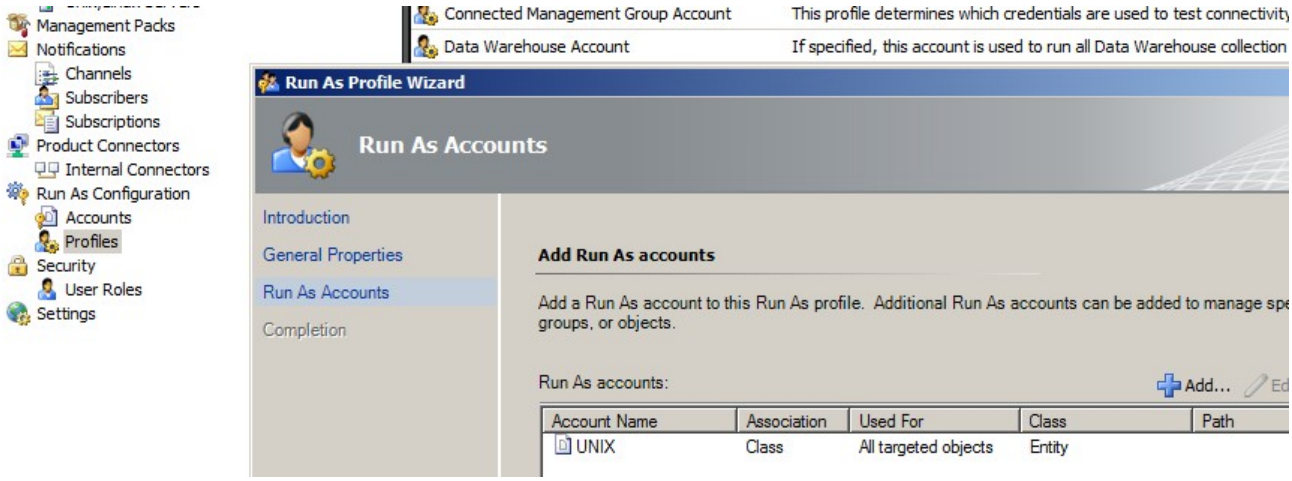
Nota: se puede realizar la instalación de un agente de Linux en las siguientes Distribuciones de Linux. Si el agente de Linux no se puede instalar mediante la detección, consulte las instrucciones de instalación manual en el siguiente artículo de Microsoft: Instalación manual de agentes multiplataforma (http://technet.microsoft.com/en-us/library/dd789016.aspx).

Nota: la detección de servidores Linux con una instalación SCEP se ejecuta automáticamente en intervalos de 8 horas en todos los ordenadores Linux administrados mediante Operations Manager (es decir, tienen el módulo de administración de Linux correspondiente instalado para distribución del sistema). La detección crea todas las entidades de módulo de servicio: servidor Linux protegido y entidades anidadas o servidor Linux no protegido (se pueden encontrar en las secciones correspondientes). La instalación de SCEP se puede considerar completa cuando aparece el servicio "scep_daemon" (detenido o en ejecución). De este modo, la primera detección se lleva a cabo cuando se instala un módulo de administración y la siguiente se realizará a las 8 horas, con respecto al ciclo de detección. Si un producto SCEP está desinstalado, el servidor correspondiente pasará automáticamente a No protegido (Servidores sin SCEP) y viceversa.

Configuración de cuentas de ejecución

Para crear una cuenta Unix, siga estas instrucciones:

1. En el espacio de trabajo **Administration** (panel izquierdo), desplácese a **Run As Configuration** > **Accounts**.
2. Para crear una nueva cuenta, abra la sección **Actions** del panel **Acciones** (panel derecho) y haga clic en **Crear cuenta de ejecución...**
3. En la ventana Propiedades generales, seleccione **Basic Authentication** en el menú desplegable **Run As Account type**.
4. Después de crear una cuenta, tiene que agregar la cuenta nueva a un perfil para que se produzca la distribución. Para ello, haga clic con el botón derecho del ratón en el perfil **Unix Privileged Account** debajo de **Run As Configuration** > **Profiles**, seleccione **Properties** y ejecute el asistente para asignar la cuenta recién creada.



Nota: para obtener más información acerca de la creación de una cuenta de ejecución, consulte el tema Configuración de una cuenta de ejecución multiplataforma (http://go.microsoft.com/fwlink/?LinkId=160348) en la biblioteca en línea de System Center 2012 Operations Manager 2007 R2.

Después de realizar todos los pasos mencionados anteriormente, los servidores Linux detectados recientemente estarán disponibles momentáneamente (durante unos minutos) en **Monitoring** > **System Center Endpoint Protection para Linux** > **Servidores con SCEP**.

Instalación de un paquete de idioma para SCEP

El formato de un paquete de idioma es el siguiente:
Microsoft.SCEP.Linux.Application.LNG.mp y Microsoft.SCEP.Linux.Library.LNG.mp

Para instalar el paquete de idioma, utilice los mismos pasos que se describen en la sección anterior **Importación de módulos de administración**. Para mostrar el idioma instalado en System Center 2012 Operations Manager, utilice las siguientes instrucciones:

1. Haga clic en el icono **Inicio** de Windows y desplácese al **Panel de control**.
2. En el Panel de control, haga clic en **Opciones regionales y de idioma**.
3. Cambie la configuración regional del sistema para los programas no Unicode en la pestaña **Administrativo**. En la pestaña **Ubicación**, cambie la ubicación actual de acuerdo con el paquete de idioma instalado.

Objetivo del módulo de administración

El módulo de administración para SCEP tiene las siguientes funcionalidades:

- Supervisión y alertas en tiempo real para incidencias de seguridad y estado de seguridad.
- Habilitación de los administradores de servidores para que realicen tareas relacionadas con la seguridad de forma remota en sus servidores. El objetivo principal de estas tareas es solucionar problemas de disponibilidad relacionados con la seguridad.

Vistas

El administrador del servidor puede supervisar, mediante la consola de Operations Manager, todos los ordenadores que tengan instalado SCEP. Para "System Center Endpoint Protection para Linux" están disponibles las siguientes vistas:

- **Alertas activas**: todas las alertas activas de SCEP de todos los niveles de gravedad. No se incluyen las alertas cerradas.
- **Panel**: muestra los espacios de trabajo Servidores con SCEP y Alertas activas.
- **Servidores con SCEP**: muestra todos los servidores Linux protegidos.
- **Servidores sin SCEP**: muestra todos los servidores Linux desprotegidos.
- **Estado de las tareas:** muestra una lista de todas las tareas ejecutadas.

Al supervisar el estado de SCEP con el módulo de administración System Center 2012 Operations Manager, puede obtener una

vista instantánea del estado de SCEP.

En lugar de esperar a que surja una alerta, puede visualizar el resumen de estado de los componentes de SCEP en cualquier momento. Para ello, haga clic en el panel **Monitoring** > **System Center Endpoint Protection para Linux** > **Servidores con SCEP** de la consola de supervisión de Operations Manager. El estado de un componente se indica en el campo Estado con iconos de colores:

Icono	Estado	Descripción
	Healthy	Un icono verde indica que el estado es correcto o que hay información disponible que no requiere ninguna acción.
	Warning	Un icono amarillo indica un error o una alerta.
	Critical	Un icono rojo puede indicar un error grave o un problema de seguridad, o que hay un servicio que no está disponible.
	Not monitored	Si no hay icono indica que no se han recopilado datos relacionados con el estado.

Es posible que en la vista aparezca una larga lista de objetos. Para encontrar un objeto determinado o un grupo de objetos específico, puede utilizar los botones de ámbito, búsqueda y buscar de la barra de herramientas de Operations Manager. Para obtener más información, consulte el tema Administración de datos de supervisión mediante las opciones de ámbito, búsqueda y buscar (http://go.microsoft.com/fwlink/?LinkId=91983).

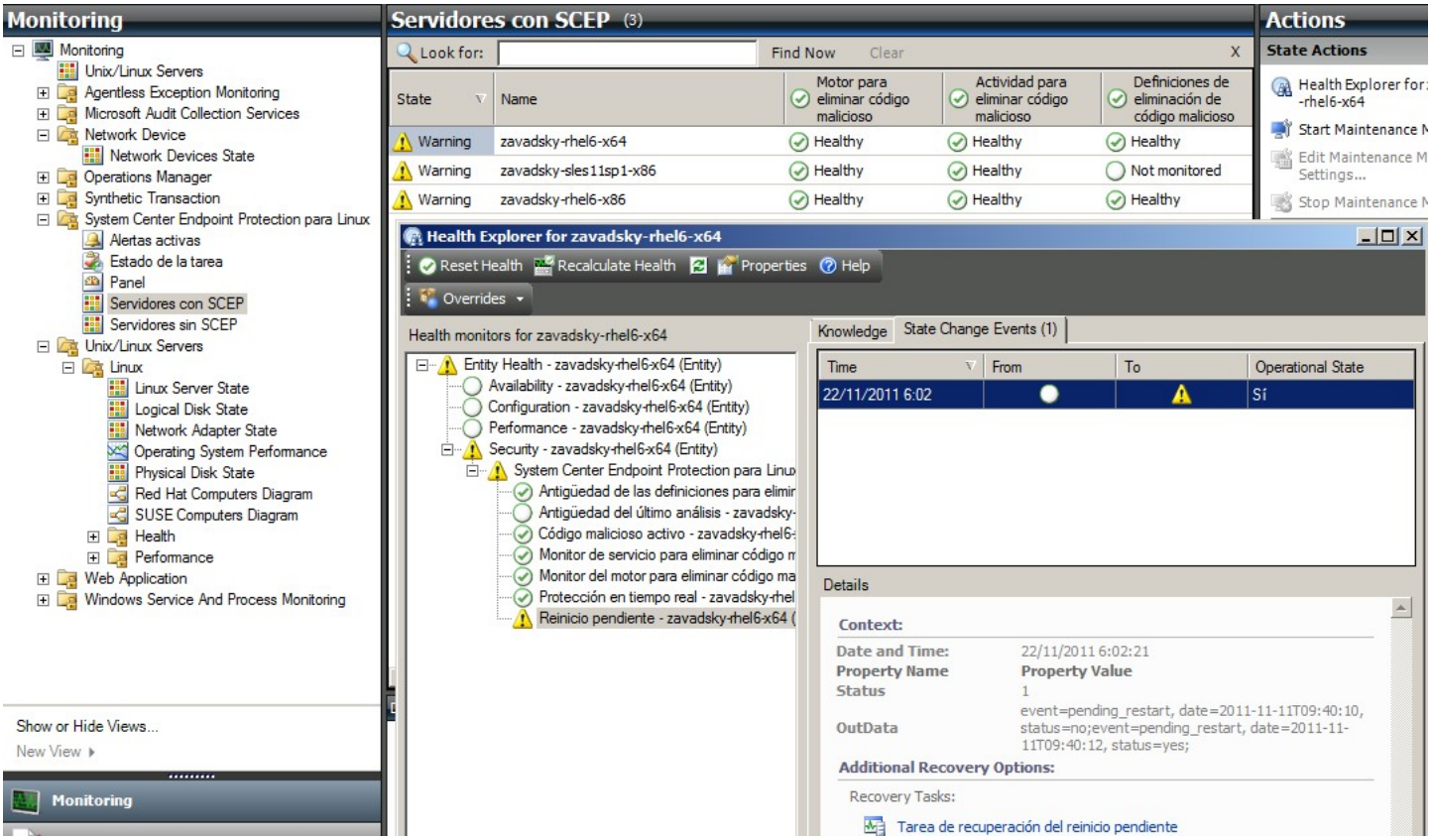
Monitores

En Operations Manager 2007, se pueden utilizar monitores para evaluar distintas condiciones que pueden darse en los objetos supervisados.

Hay un total de 17 monitores disponibles para SCEP:

- 9 monitores de unidad: los componentes de supervisión fundamentales, se utilizan para supervisar contadores, eventos, scripts y servicios específicos.
- 2 monitores de agregación: se utilizan para un resumen agregado que reúne a varios monitores en uno solo; a continuación, se utiliza ese monitor para establecer el estado correcto y generar una alerta.
- 6 monitores de dependencias : referencias que contienen datos sobre el estado de los monitores existentes.

Nota: para obtener más información acerca de los monitores, consulte la Ayuda de Operations Manager 2007 R2 (pulse la tecla F1 en System Center 2012 Operations Manager).



Los monitores de estado de SCEP tienen la estructura y las propiedades que se describen a continuación.

Código malicioso activo

Tipo de monitor	Monitor de unidad
Objeto	Servidor Linux protegido
Origen de datos	Supervisa el archivo de registro de texto: /var/log/scep/eventlog_scom.dat
Intervalo	Basado en eventos
Alerta	Sí. No se autorresuelve.
Comportamiento de reinicio	La vuelta al estado correcto es automática después de un periodo de 8 horas. La alerta permanece activa para conservar la información acerca del código malicioso no tratado.
Notas	Este monitor cambiará el estado a Grave cuando se detecte código malicioso que no se ha desinfectado. El estado cambiará automáticamente a Estado correcto tras 8 horas (esto se debe a que no es posible determinar con precisión si el código malicioso se desinfectó o eliminó). Se necesita la intervención del administrador para que valore las circunstancias y cierre la incidencia manualmente.
Estado	Estado correcto: Sin código malicioso Grave: Código malicioso activo
Activado	Verdadero
Tarea de recuperación	No

Este monitor rastrea las operaciones de desinfección de código malicioso que fallaron. Este monitor informa de un estado grave si el cliente informa de que no ha podido desinfectar el código malicioso.

Antigüedad de las definiciones para eliminar código malicioso

Tipo de monitor	Monitor de unidad
Objeto	Servidor Linux protegido
Origen de datos	Comando usado para obtener datos de supervisión: /opt/microsoft/scep/sbin/scep_daemon --status
Intervalo	Cada 8 horas
Alerta	Sí. Se autorresuelve.
Estado	Estado correcto - antigüedad <= 3 días Advertencia: antigüedad > 3 Y antigüedad <= 5 días Grave - antigüedad > 5 días
Activado	Verdadero
Tarea de recuperación	Sí, de forma manual (sin recuperación automática)

Las definiciones actualizadas ayudan a garantizar que el ordenador está protegido contra las amenazas más recientes de código malicioso.

Motor para eliminar código malicioso

Tipo de monitor	Monitor de unidad
Objeto	Servidor Linux protegido
Origen de datos	Supervisa el archivo de registro de texto: /var/log/scep/eventlog_scom.dat
Intervalo	Basado en eventos
Alerta	Sí. Se autorresuelve.
Estado	Estado correcto: Activado Desactivado: Alerta
Activado	Verdadero
Tarea de recuperación	Sí, de forma manual (sin recuperación automática)

Se recomienda que la protección para eliminar código malicioso esté siempre activada.
Nota: este monitor rastrea el estado de la protección antivirus, que no es el mismo que el de la protección en tiempo real. Con el motor para eliminar código malicioso desactivado, no se puede iniciar un análisis a petición.

Servicio para eliminar código malicioso

Tipo de monitor	Monitor de unidad
Objeto	Servidor Linux protegido
Origen de datos	Supervisa el estado del proceso: scep_daemon
Intervalo	Cada 10 minutos
Alerta	Sí. Se autorresuelve.
Estado	Estado correcto: En ejecución Grave: No en ejecución

Activado	Verdadero
Tarea de recuperación	Sí, de forma manual (sin recuperación automática)

El monitor informa de un estado grave cuando el servicio para eliminar código malicioso (scep_daemon) en el equipo cliente no se está ejecutando o no responde, o cuando el motor para eliminar el código malicioso no está funcionando correctamente.

Antigüedad del último análisis

Tipo de monitor	Monitor de unidad
Objeto	Servidor Linux protegido
Origen de datos	Comando usado para obtener datos de supervisión: /opt/microsoft/scep/sbin/scep_daemon --status
Intervalo	Cada 8 horas
Alerta	No
Estado	Estado correcto - antigüedad <= 7 Alerta - antigüedad > 7
Activado	Verdadero
Tarea de recuperación	Sí, de forma manual (sin recuperación automática)

Este monitor rastrea el tiempo desde el último análisis del ordenador (independientemente del tipo de análisis). Se recomienda programar la ejecución de un análisis cada semana.

Reinicio pendiente

Tipo de monitor	Monitor de unidad
Objeto	Servidor Linux protegido
Origen de datos	Supervisa el archivo de registro de texto: /var/log/scep/eventlog_scom.dat
Intervalo	Basado en eventos
Alerta	Sí. Se autorresuelve.
Estado	No: Estado correcto Sí: Alerta
Activado	Verdadero
Tarea de recuperación	Sí, de forma manual (sin recuperación automática)

Este monitor rastrea la necesidad de reiniciar el sistema para que los cambios en la configuración surtan efecto (normalmente cuando se activa/desactiva la protección en tiempo real). El monitor aplica la siguiente llamada para una actualización a petición de este estado: /opt/microsoft/scep/sbin/scep_daemon --status.

Protección en tiempo real

Tipo de monitor	Monitor de unidad
Objeto	Servidor Linux protegido
Origen de datos	Supervisa el archivo de registro de texto: /var/log/scep/eventlog_scom.dat El monitor también puede utilizar la siguiente llamada para una actualización de estado a petición: /opt/microsoft/scep/sbin/scep_daemon --status.
Intervalo	Basado en eventos
Alerta	Sí. Se autorresuelve.
Estado	Activado: Estado correcto Desactivado: Alerta
Activado	Verdadero
Tarea de recuperación	Sí, de forma manual (sin recuperación automática)

Supervisa el estado de la protección en tiempo real. La protección en tiempo real le alerta cuando un virus, spyware y otro software potencialmente no deseado intenta instalarse en su ordenador.

System Center Endpoint Protection para Linux

Tipo de monitor	Monitor de agregación
Objeto	Servidor Linux protegido
Condición	El peor
Alerta	No
Activado	Verdadero
Tarea de recuperación	No

Este monitor es el resumen del estado (peor estado) de todos los monitores de unidad de seguridad del servidor Linux protegido de

SCEP 7. Si el estado es de no inicializado, o no ha comenzado la supervisión del objeto o no se han definido monitores de seguridad para este objeto.

Motor para eliminar código malicioso

Tipo de monitor	Monitor de dependencias
Objeto	Motor para eliminar código malicioso
Alerta	No
Activado	Verdadero
Tarea de recuperación	No

Muestra el estado del monitor de unidad de motor para eliminar código malicioso/servidor Linux protegido en la lista de ordenadores supervisados.

Servicio para eliminar código malicioso

Tipo de monitor	Monitor de dependencias
Objeto	Motor para eliminar código malicioso
Alerta	No
Activado	Verdadero
Tarea de recuperación	No

Muestra el estado del monitor de unidad de servicio para eliminar código malicioso/servidor Linux protegido en la lista de ordenadores supervisados.

Definiciones de eliminación de código malicioso

Tipo de monitor	Monitor de dependencias
Objeto	Definiciones de eliminación de código malicioso
Alerta	No
Activado	Verdadero
Tarea de recuperación	No

Muestra el estado del monitor de antigüedad de definiciones para eliminar código malicioso/servidor Linux protegido en la lista de ordenadores supervisados.

Código malicioso activo

Tipo de monitor	Monitor de dependencias
Objeto	Actividad para eliminar código malicioso
Alerta	No
Activado	Verdadero
Tarea de recuperación	No

Muestra el estado del monitor de código malicioso activo/servidor Linux protegido en el explorador de estado de actividad para eliminar código malicioso.

Ping en el equipo

Tipo de monitor	Monitor de unidad
Objeto	Actividad para eliminar código malicioso
Intervalo	Cada 60 minutos
Alerta	No
Estado	Accesible: Estado correcto Inaccesible: Grave
Activado	Falso
Tarea de recuperación	No

Cambia el estado a Grave si no hay respuesta del servidor.

Actividad de código malicioso

Tipo de monitor	Monitor de unidad
Objeto	Actividad para eliminar código malicioso
Origen de datos	Supervisa el archivo de registro de texto: /var/log/scep/eventlog_scom.dat
Intervalo	Basado en eventos

Alerta	No
Estado	Sin código malicioso: Estado correcto Actividad de código malicioso detectada: Grave
Activado	Verdadero
Tarea de recuperación	No

Este monitor cambia a estado Grave a los 5 minutos de la detección de código malicioso (desinfectado o sin tratar) y permanece en estado Grave durante los siguientes 60 minutos. El estado Grave se renueva con cada nueva detección positiva y, con ella, la duración del periodo de alerta. Es decir, si no se detecta código malicioso en el sistema durante un periodo de 60 minutos, el monitor vuelve al Estado correcto.

Brote de código malicioso del servidor

Tipo de monitor	Monitor de agregación
Objeto	Actividad para eliminar código malicioso
Condición	El mejor
Alerta	No
Activado	Verdadero
Tarea de recuperación	No

Monitores agregados: Actividad de código malicioso y Ping en el equipo.
Cambia el estado a Grave si no hay respuesta del servidor durante los 60 minutos posteriores a la detección positiva de código malicioso (desinfectado o no tratado). El cambio de estado a Grave también se puede activar si, después de un periodo en el que no se recibe respuesta del servidor, se detecta código malicioso poco después de recuperar la conexión.

Brote de código malicioso

Tipo de monitor	Monitor de dependencias
Objeto	Monitor de servidores protegidos
Condición	Peor de 95%
Alerta	No
Activado	Verdadero
Tarea de recuperación	No

Muestra el estado del monitor de Actividad para eliminar código malicioso/Brote de código malicioso del servidor.
Si más del 5% de todos los ordenadores Linux (protegidos y no protegidos) registran una detección de código malicioso en los 60 minutos anteriores, este monitor cambia al estado Grave.

Resumen de estado del rol del ordenador de SCEP para Linux

Tipo de monitor	Monitor de dependencias
Objeto	Ordenador Linux
Alerta	No
Activado	Verdadero
Tarea de recuperación	No

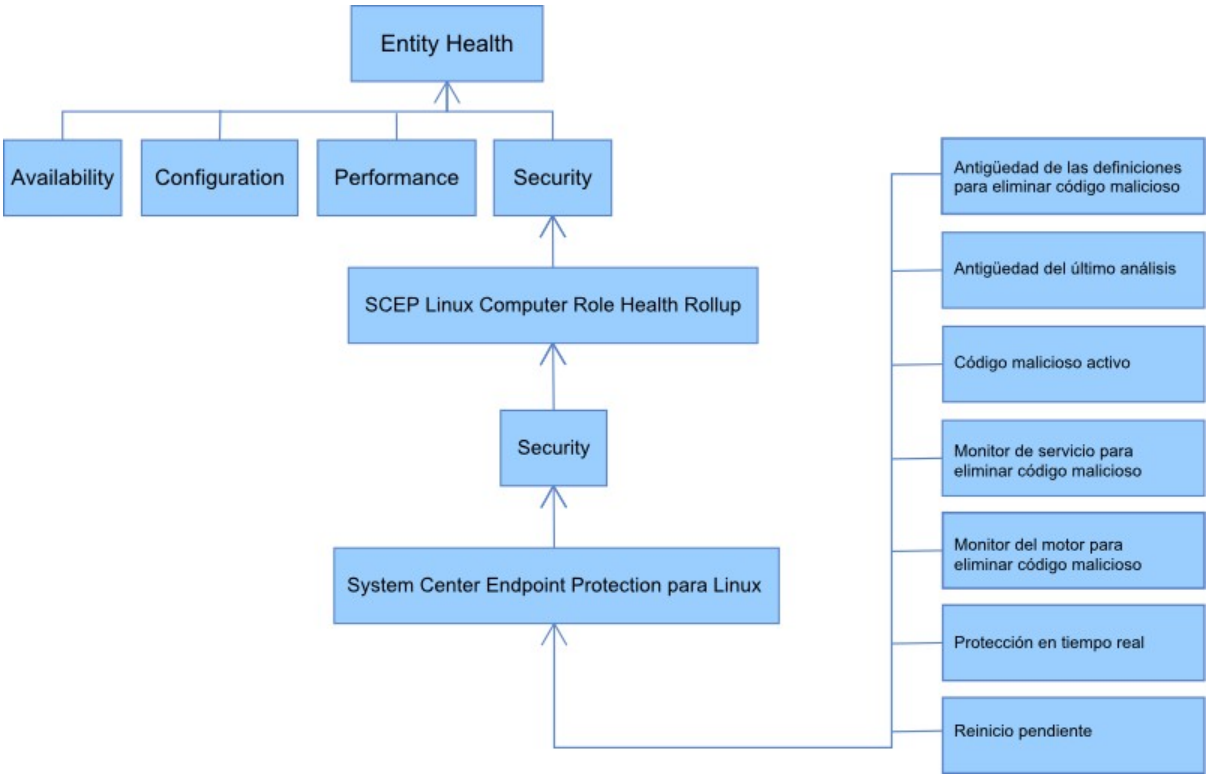
Propaga el estado de la entidad de ordenadores Linux protegidos al monitor principal de ordenadores Linux/seguridad.

Resumen de estado

Este módulo de administración expande la supervisión del sistema operativo Linux como estructura de capas, donde el buen estado de cada capa depende de la capa inferior. La parte superior de esta estructura es la totalidad del entorno del estado de la entidad, y el nivel más bajo de los entornos de seguridad es el de todos los monitores. Cuando el estado de una capa cambia, la capa que está por encima cambia al mismo estado. Esta acción se llama reproducción del estado.

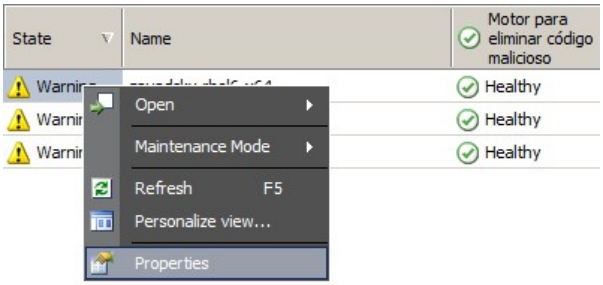
Por ejemplo, si la protección en tiempo real devuelve un estado de alerta y todos los demás componentes están en buen estado, el estado de alerta se transferirá a través de esta estructura de árbol hasta la raíz (Estado de la entidad), que también adquirirá el estado de alerta.

En el siguiente diagrama se muestra cómo los estados de los objetos se reproducen en este módulo de administración.



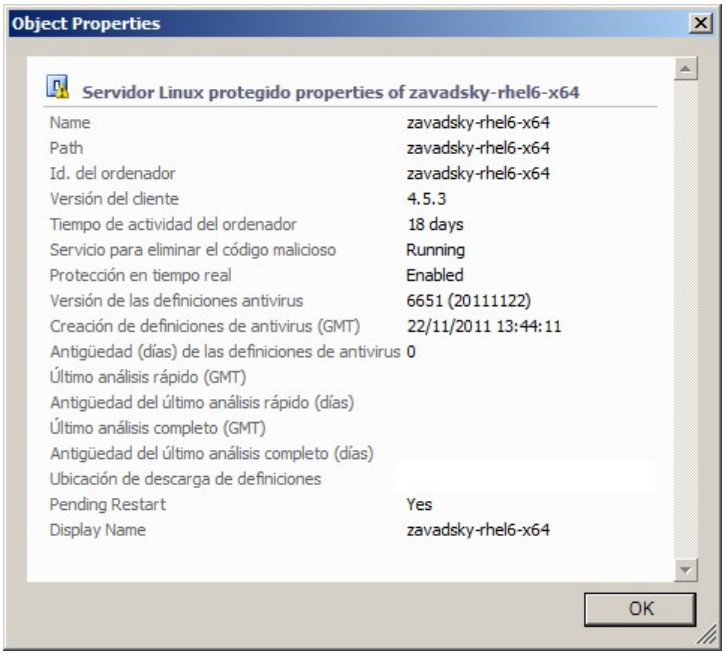
Propiedades de objetos

Para ver las propiedades de un objeto, haga clic con el botón derecho del ratón en el objeto y seleccione **Properties**.



Un objeto del servidor Linux protegido cuenta con las siguientes propiedades:

- **Id. del ordenador**: identificador del servidor, nombre del dominio.
- **Nombre de pantalla**: nombre del servidor, nombre del dominio.
- **Versión del cliente**: versión del producto SCEP instalado.
- **Tiempo de actividad del ordenador**: el tiempo de actividad del servidor (medida del tiempo que una máquina ha estado funcionando sin tiempo de inactividad) no es un dato esencial para el funcionamiento adecuado de un módulo de administración, por lo tanto, su ausencia podría indicar un error en dicho módulo.
- **Servicio para eliminar el código malicioso**: estado de protección para eliminar código malicioso (En ejecución/No en ejecución).
- **Protección en tiempo real**: estado de la protección en tiempo real; su ausencia indica problemas de SCEP.
- **Definiciones de antivirus:** datos de estado de la base de virus (versión, fecha de creación, antigüedad); la ausencia de datos indica problemas de SCEP.
- **Último análisis rápido/completo:**: datos acerca del último análisis del ordenador. Si aún no se ha realizado el análisis (Análisis rápido/Análisis completo), no aparecerán datos al respecto.
- **Ubicación de descarga de definiciones**: actualización de la dirección y el nombre del servidor. La información aparece después de que se haya realizado la primera actualización correctamente.
- **Reinicio pendiente:** información que indica que es necesario reiniciar para que se apliquen los cambios debido a que se ha llevado a cabo una nueva instalación o se han realizado cambios en la configuración de SCEP.



Alertas

Una alerta es un elemento que indica que una situación predefinida con una gravedad específica (seriedad) se ha producido en un objeto supervisado. Las alertas se definen mediante reglas. Existe una vista en la consola de Operations Manager a la que se puede acceder desde **Monitoring** > **System Center Endpoint Protection para Linux** > **Alertas activas** en la que se muestran las alertas, relativas a un objeto específico, que el usuario de la consola puede ver mediante los derechos correspondientes.

Nota: si se generan más alertas del mismo tipo de forma repetida (por ejemplo, Código malicioso activo) desde el mismo servidor, solo se muestra la primera de ellas (las alertas redundantes se ignoran).

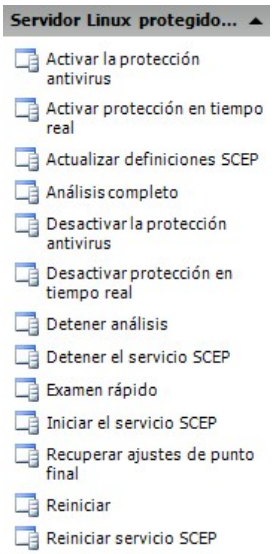
Alerta	Intervalo	Prioridad	Gravedad	Descripción
Infección por código malicioso repetido	Basado en eventos	Alta	Grave	La alerta se genera en caso de detecciones repetidas `por código malicioso (3 repeticiones) durante un intervalo de tiempo determinado (30 minutos). La alerta contiene datos acerca del servidor e información básica sobre el código malicioso.
Código malicioso desinfectado	Basado en eventos	Baja Media	Información: código malicioso desinfectado correctamente. Alerta: se requiere la intervención del usuario, por ejemplo, reiniciar el servidor.	Alertas que informan de que se ha desinfectado código malicioso correctamente. Contienen todos los datos disponibles acerca del código malicioso en cuestión. Cada código malicioso detectado genera un evento individual. SCEP para Linux asigna la prioridad y la gravedad en función de la eficiencia del proceso de desinfección: Desinfectado = Baja + Información. Desinfectado pero se requiere acción (por ejemplo, reinicio) = Media + Alerta.
Código malicioso activo (del monitor)	Basado en eventos	Alta	Grave	Alertas que informan de código malicioso que no se ha desinfectado. Contienen todos los datos disponibles acerca del código malicioso en cuestión.
Código malicioso activo (de la regla)	Basado en eventos	Alta/Media/ Baja	Grave/Media/Baja, según el tipo de código malicioso	Igual que antes. Se emplea en los conectores a otros sistemas de supervisión/creación de vales. **Nota:** esta regla (alerta) está desactivada de forma predeterminada.

El servicio para eliminar código malicioso de System Center Endpoint Protection está inactivo	300 segundos	Media	Grave	Alertas que informan sobre la no disponibilidad del servicio para eliminar código malicioso de SCEP (scep_daemon). Incluyen el nombre del servidor y la versión de SCEP correspondientes.
Protección para eliminar código malicioso desactivada	Basado en eventos	Media	Alerta	Alertas que informan de que la protección para eliminar código malicioso está desactivada. Incluyen el nombre del servidor correspondiente.
Protección en tiempo real desactivada	Basado en eventos	Media	Alerta	Alertas que informan de que la protección en tiempo real está desactivada. Incluyen el nombre del servidor correspondiente.
Las definiciones no están actualizadas	Cada 8 horas	Media	Advertencia (antigüedad <= 5 días Y antigüedad > 3 días) Grave (antigüedad > 5 días)	Alertas que informan de que la base de firmas de virus no se ha actualizado desde hace más de 3 días. Incluyen el nombre del servidor y la antigüedad de la base de firmas de virus correspondientes.
Brote de código malicioso	Basado en eventos	Alta	Grave	Forefront Endpoint Protection ha detectado más de un 5% de código malicioso activo en los ordenadores. Es posible que el código malicioso se esté propagando en los equipos. Se aconseja la actualización de todos los servidores para que usen las definiciones más recientes. Si necesita cambiar el número de amenazas activas que desencadenan esta alerta, invalide el parámetro del monitor Brote de código malicioso (consulte el capítulo Invalidaciones).

Tareas

El módulo de administración para SCEP implementa 13 tareas. La ejecución de estas tareas es inmediata. Se muestran los resultados inmediatamente después de la ejecución de las tareas. También es posible visualizarlos posteriormente en la ventana Estado de las tareas. El tiempo máximo requerido para la ejecución de una tarea es de 180 segundos. No se permiten invalidaciones. Todas las tareas son comandos BASH ejecutados mediante SSH.

Las tareas se pueden ejecutar en **Monitoring** > **System Center Endpoint Protection para Linux** > **Servidores con SCEP**, en el panel derecho de la ventana Consola de operaciones.



- **Desactivar la protección antivirus**: desactiva todos los componentes de la protección antivirus; desactiva el análisis a petición.
- **Activar la protección antivirus**: activa todos los componentes de la protección antivirus.
- **Desactivar protección en tiempo real**: desactiva la protección en tiempo real.
- **Activar protección en tiempo real**: activa la protección en tiempo real.
- **Análisis completo**: actualiza la base de firmas de virus y ejecuta un análisis completo del ordenador.
- **Análisis rápido**: actualiza la base de firmas de virus y ejecuta un análisis rápido del ordenador.
- **Detener análisis**: detiene todos los análisis del ordenador que se estén ejecutando.
- **Recuperar ajustes de servidor**: muestra el estado actual del producto SCEP; la lista de parámetros mostrados es idéntica a las propiedades de la entidad del servidor Linux protegido. Los datos mostrados no se transfieren al servidor Linux protegido.
- **Reiniciar servicio para eliminar código malicioso**: reinicia el servicio para eliminar código malicioso de SCEP (scep_daemon).
- **Detener el servicio para eliminar código malicioso**: detiene el servicio para eliminar código malicioso de SCEP (scep_daemon).
- **Iniciar el servicio para eliminar código malicioso**: inicia el servicio para eliminar código malicioso de SCEP (scep_daemon).
- **Actualizar definiciones Antimalware**: inicia la actualización de la base de firmas de virus.
- **Reiniciar:** reinicia el ordenador con Linux.

Configuración del módulo de administración para SCEP

Recomendación: crear un módulo de administración para personalizaciones

De forma predeterminada, Operations Manager guarda todas las personalizaciones como invalidaciones en el módulo de administración predeterminado. Se recomienda que, en su lugar, cree un módulo de administración para cada módulo de administración independiente que desee personalizar.

A la hora de crear un módulo de administración con el objetivo de guardar configuraciones personalizadas de un módulo de administración independiente, resulta útil especificar el nombre del módulo de administración nuevo basándose en el nombre del módulo de administración que se está personalizando, como "Personalizaciones de SCEP 2012".

Si se crea un módulo de administración nuevo para guardar las personalizaciones de cada módulo de administración independiente, resulta más sencillo exportar las personalizaciones desde un entorno de prueba a un entorno de producción. Además, también es más fácil eliminar un módulo de administración, puesto que antes de hacerlo se deben eliminar todas las dependencias. Si las personalizaciones de todos los módulos de administración se guardan en el módulo de administración predeterminado y tiene que eliminar un único módulo de administración, deberá primero eliminar el módulo de administración predeterminado, lo que también eliminará las personalizaciones del resto de módulos de administración.

Configuración de seguridad

El ordenador debe ejecutar el servicio SSHD y el puerto SSH (valor predeterminado 22) debe estar abierto. System Center 2012 Operations Manager se conecta a los ordenadores de Linux remotos a través del puerto mediante la Run As Account adecuada (situada en el panel **Administration** > **Run As Configuration** de la consola de supervisión de Operations Manager) con el tipo **Basic Authentication**.

Nombre de perfil de ejecución	Notas
Unix Privileged Account	Se utiliza para supervisar el servidor Unix de forma remota, y para reiniciar procesos en los que se exigen derechos con privilegios.

Este módulo de administración no utiliza la Unix Action Account.

Advertencia: la supervisión de ordenadores mediante la cuenta raíz conlleva un posible riesgo de seguridad en caso de que, por ejemplo, la contraseña se haya dañado.

Si no desea utilizar la cuenta raíz para la supervisión y la gestión, puede usar una cuenta de usuario estándar, pero esta cuenta deberá tener derechos para ejecutar comandos de *sudo*. Por lo tanto, la siguiente configuración debe estar presente en el archivo /etc/sudoers en cada estación de trabajo supervisada de SCEP de Linux para autorizar la elevación de privilegios en sudo para la cuenta de usuario seleccionada. Este es un ejemplo de configuración para el nombre de usuario user1:

```
#------------------------------------------------------------------------
# User configuration for SCEP monitoring - for a user with the name: user1

user1  ALL=(root)    NOPASSWD:     /opt/microsoft/scx/bin/scxlogfilereader -p
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /sbin/reboot
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep restart
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep start
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep stop
user1  ALL=(root)    NOPASSWD:     /bin/sh -c export LANG=C;if \[ -e /opt/microsoft/scep/sbin/
scep_daemon \] ; then echo scep_daemon installed; else echo scep_daemon unprotected; fi; kill -0
`cat /var/run/scep_daemon.pid 2>/dev/null` 2>/dev/null; if \[ $\? -eq 0 \] ; then echo scep_daemon
running; else echo scep_daemon stop;fi ; /opt/microsoft/scep/sbin/scep_daemon --status; uptime
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /opt/microsoft/scep/sbin/scep_daemon *
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /opt/microsoft/scep/lib/scep_sci --scom *
```

```
user1  ALL=(root)    NOPASSWD:     /bin/sh -c pkill scep_sci
user1  ALL=(root)    NOPASSWD:     /bin/sh -c export LANG=C; kill -0 `cat /var/run/scep_daemon.pid 2>/
dev/null` 2>/dev/null; if \[ $? -eq 0 \] ; then echo scep_daemon running; else echo scep_daemon
stop;fi ; /opt/microsoft/scep/sbin/scep_daemon --status; uptime

# End user configuration for SCEP monitoring
#--------------------------------------------------------------------------------
```

Ajuste de las reglas de umbral de rendimiento

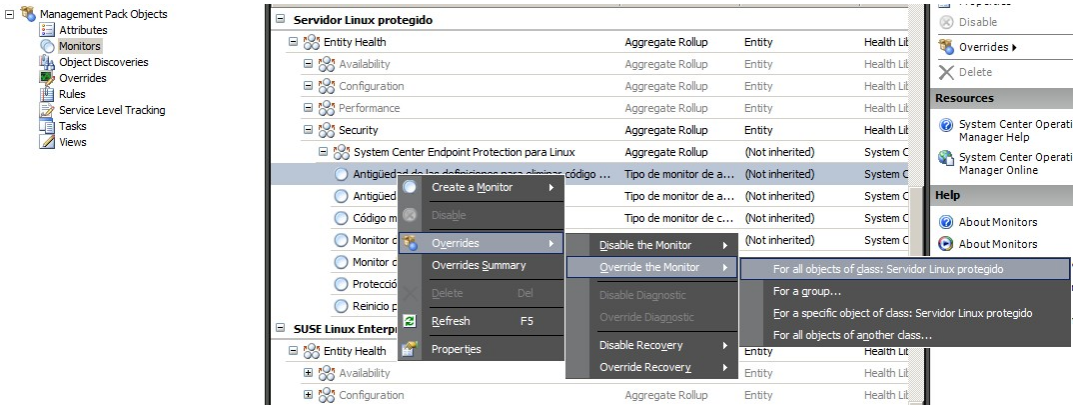
En la siguiente tabla figuran las reglas de umbral de rendimiento que tienen umbrales predeterminados y que podrían requerir un ajuste adicional para adecuarse a su entorno. Considere estas reglas para determinar si los umbrales predeterminados son apropiados para su entorno. Si un umbral predeterminado no fuese apropiado para su entorno, puede ajustarlo aplicándole una invalidación.

Nombre de la regla	Parámetro de invalidación	Umbral predeterminado	Limitaciones de ajuste
Regla de infección de código malicioso repetido	Umbral de recuento de infecciones repetidas	3 repeticiones	Si se configura un valor inferior a 2, la regla queda obsoleta.
Regla de infección de código malicioso repetido	Ventana de tiempo de infecciones repetidas	30 minutos	No se recomienda configurar un valor inferior a la duración del análisis a petición puesto que un solapamiento podría evitar que se generasen alertas.
Regla de alerta de código malicioso activo	Activada	Falso	Puede activar esta alerta si utiliza conectores a otros sistemas de supervisión/creación de vales.

Invalidaciones

Las invalidaciones se pueden utilizar para restringir la configuración de un objeto de supervisión en System Center 2012 Operations Manager. Se incluyen monitores, reglas, detecciones de objetos y atributos provenientes de módulos de administración importados.

Para invalidar un monitor, en la Consola de operaciones haga clic en el botón **Authoring** y expanda **Management Pack Objects** > **Monitors**. En el panel Monitores, busque y expanda un tipo de objeto completamente y, a continuación, haga clic en **Overrides**.



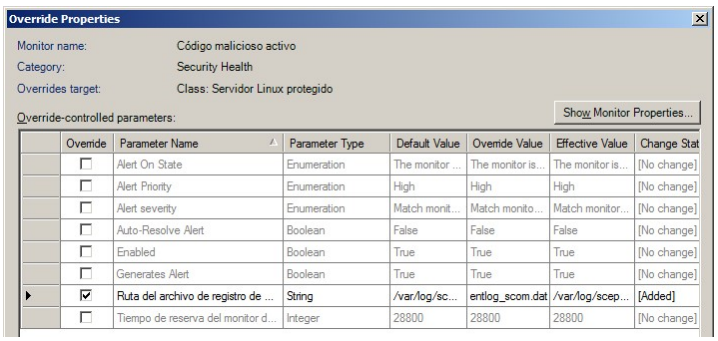
Utilice la ventana de invalidaciones para crear o modificar una invalidación de una ocurrencia de cualquiera de los siguientes parámetros:

- **Tiempo de reserva del monitor de código malicioso activo** (relacionado solo con el monitor de código malicioso activo)
- **Antigüedad de las definiciones para eliminar código malicioso** (relacionado solo con el monitor de antigüedad de las definiciones para eliminar código malicioso)
- **Intervalo de detección** (relacionado solo con el monitor de antigüedad del último análisis)
- **Estado de alerta**
- **Prioridad de la alerta**
- **Gravedad de la alerta**
- **Autorresolver alerta**
- **Activado**: determine si el monitor seleccionado está activado o desactivado.
- **Genera alerta**
- **Ruta de acceso del archivo de registro de SCEP**

Si una invalidación predeterminada no fuese apropiada para su entorno, puede ajustar los umbrales aplicándoles una invalidación:

Parámetro de invalidación	Nombre del monitor	Valor predeterminado	Notas de ajuste
Intervalo de ping	Ping en el equipo	3600 segundos	Un intervalo para comprobar la disponibilidad del servidor Linux protegido. Una duración más corta activa un estado de error en el monitor de brote de código malicioso del servidor más rápido, en caso de que el ordenador deje de responder debido a un ataque. Como consecuencia, se incrementa la carga en la red, el ordenador supervisado y el servidor System Center 2012 Operations Manager.
Ventana de tiempo del brote de código malicioso	Actividad de código malicioso	3600 segundos	Un intervalo requerido por el monitor para volver al estado correcto después de una actividad de código malicioso. El valor del monitor de la ventana de tiempo debe ser superior al intervalo de ping/ping del ordenador para que la combinación funcione apropiadamente. Si durante el intervalo de la ventana de tiempo del brote de código malicioso, un número de ordenadores con un porcentaje excesivo del brote de código malicioso establecido (consulte Brote de código malicioso) registra actividad de código malicioso, se genera una alerta de brote de código malicioso. Nota: esto es diferente del brote de código malicioso del servidor, que no genera alerta.
Tiempo de reserva del monitor de código malicioso activo	Código malicioso activo	28800 segundos	Intervalo de tiempo desde la detección de código malicioso, tras el cual el código malicioso se considera desinfectado.
Ruta de acceso del archivo de registro de SCEP	Código malicioso activo	/var/log/scep/ eventlog_scom.log	Ruta del archivo donde se registran los sucesos de System Center 2012 Operations Manager. No modifique este parámetro a menos que surjan problemas.
Antigüedad crítica de las definiciones de eliminación de código malicioso	Antigüedad de las definiciones para eliminar código malicioso	5 días	Después de este intervalo, se genera una alerta de error que indica un producto SCEP sin actualizar.
Antigüedad del estado correcto de las definiciones de eliminación de código malicioso	Antigüedad de las definiciones para eliminar código malicioso	3 días	Antigüedad máxima permitida de definiciones para eliminar código malicioso, tiempo durante el cual se consideran actualizadas. Este valor debe ser siempre inferior al valor de antigüedad crítica de las definiciones de eliminación de código malicioso.
Intervalo	Antigüedad de las definiciones para eliminar código malicioso	28800 segundos	Intervalo de comprobación de la antigüedad de las definiciones para eliminar código malicioso.
Intervalo	Servicio para eliminar código malicioso	300 segundos	Intervalo de comprobación de la disponibilidad del servicio para eliminar código malicioso.
Nombre del proceso	Servicio para eliminar código malicioso	scep_daemon	El nombre del servicio para eliminar código malicioso. No modifique este valor si el monitor está operativo.
Intervalo de detección	Antigüedad del último análisis	28800 segundos	Intervalo de comprobación de la ejecución del último análisis.
Antigüedad máxima del análisis	Antigüedad del último análisis	7 días	Se debe configurar de acuerdo con la configuración del producto SCEP. Si se programa un análisis cada 7 días, configure este valor en 7 días.
Ruta de acceso del archivo de registro	Reinicio pendiente	/var/log/scep/ eventlog_scom.log	Ruta del archivo donde se registran los sucesos de System Center 2012 Operations Manager. No modifique este parámetro a menos que surjan problemas.
Ruta de acceso del archivo de registro de SCEP	Protección en tiempo real	/var/log/scep/ eventlog_scom.log	Ruta del archivo donde se registran los sucesos de System Center 2012 Operations Manager. No modifique este parámetro a menos que surjan problemas.

Porcentaje	Brote de código malicioso	95%	Porcentaje de servidores Linux (protegidos y no protegidos) que se requiere que vuelvan al estado correcto, con respecto a todo el grupo supervisado que se considera que tienen un estado correcto. Si se detecta código malicioso en el 5% o más del total, se genera un brote de código malicioso.



Nota: Para obtener información acerca de las invalidaciones, consulte Supervisión con invalidaciones (http://go.microsoft.com/fwlink/?LinkID=117777).

Enlaces

Los siguientes enlaces le ofrecen información acerca de tareas comunes relacionadas con este módulo de administración:

- Administración del ciclo de vida de los módulos de administración (http://go.microsoft.com/fwlink/?LinkId=211463)
- Importación de un módulo de administración en Operations Manager 2007 (http://go.microsoft.com/fwlink/?LinkID=142351)
- Supervisión con invalidaciones (http://go.microsoft.com/fwlink/?LinkID=117777)
- Creación de una cuenta de ejecución en Operations Manager 2007 (http://go.microsoft.com/fwlink/?LinkID=165410)
- Configuración de una cuenta de ejecución multiplataforma (http://go.microsoft.com/fwlink/?LinkId=160348)
- Modificación de un perfil de ejecución existente (http://go.microsoft.com/fwlink/?LinkID=165412)
- Exportación de personalizaciones de los módulos de administración (http://go.microsoft.com/fwlink/?LinkId=209940)
- Eliminación de un módulo de administración (http://go.microsoft.com/fwlink/?LinkId=209941)
- Administración de datos de supervisión mediante las opciones de ámbito, búsqueda y buscar (http://go.microsoft.com/fwlink/?LinkId=91983)
- Supervisión de Linux mediante SCOM 2007 R2 (en inglés) (http://blogs.technet.com/b/birojitn/archive/2010/01/20/monitoring-linux-using-scom-2007-r2.aspx)
- Instalación manual de agentes multiplataforma (http://technet.microsoft.com/en-us/library/dd789016.aspx)
- Configuración de la elevación de privilegios en sudo para UNIX y supervisión de Linux con System Center 2012: Operations Manager (http://social.technet.microsoft.com/wiki/contents/articles/7375.configuring-sudo-elevation-for-unix-and-linux-monitoring-with-system-center-2012-operations-manager.aspx)

Para consultas acerca de Operations Manager y los módulos de supervisión, consulte el Foro de la comunidad de System Center Operations Manager (http://go.microsoft.com/fwlink/?LinkID=179635).
Un recurso que resulta útil es el blog System Center Operations Manager Unleashed (http://opsmgrunleashed.wordpress.com/), que contiene publicaciones de ejemplos de módulos de supervisión específicos.

Para obtener información adicional acerca de Operations Manager, consulte los siguientes blogs:

- Blog del equipo de Operations Manager (en inglés)
  (http://blogs.technet.com/momteam/default.aspx)
- Blog OpsMgr de Kevin Holman (en inglés)
  (http://blogs.technet.com/kevinholman/default.aspx)
- Blog Thoughts on OpsMgr (en inglés)
  (http://thoughtsonopsmgr.blogspot.com/)
- Blog de Raphael Burri (en inglés)
  (http://rburri.wordpress.com/)
- BWren's Management Space (en inglés)
  (http://blogs.technet.com/brianwren/default.aspx)
- Blog del equipo de soporte técnico de System Center Operations Manager (en inglés)
  (http://blogs.technet.com/operationsmgr/)
- Ops Mgr ++ (en inglés)
  (http://blogs.msdn.com/boris_yanushpolsky/default.aspx)
- Notas acerca de System Center Operations Manager (en inglés)
  (http://blogs.msdn.com/mariussutara/default.aspx)

Para obtener información acerca de la resolución de problemas, visite los siguientes hilos del foro:

- Falta Microsoft.Unix.Library (en inglés)
  (http://social.technet.microsoft.com/Forums/en-US/operationsmanagermgmtpacks/thread/8469d0ff-54d6-4cb4-9909-49ab62126b74/)