Guía de actualización de Symantec AntiVirus Corporate Edition™

Guía de actualización de Symantec AntiVirus™ Corporate Edition

Versión de la documentación: 8.1

Información de copyright

Marcas comerciales

Impreso en Irlanda.

10 9 8 7 6 5 4 3 2 1

Contenido

Capítulo 1 Actualizaciones de la Guía de instalación de Symantec AntiVirus Corporate Edition

Capítulo 1

Actualizaciones de la Guía de instalación de Symantec AntiVirus Corporate Edition

Acerca de las actualizaciones de la Guía de instalación de Symantec AntiVirus Corporate Edition

El propósito de este capítulo es explicar los cambios aplicados a la *Guía de instalación de Symantec AntiVirus Corporate Edition* entre las versiones 8.0 y 8.1 de Symantec AntiVirus Corporate Edition.

Compatibilidad con Windows 3.x/DOS

El producto Symantec AntiVirus Corporate Edition 8.1 ya no incluye clientes de versiones anteriores para Windows 3.x y DOS en el CD de soluciones anteriores de Symantec AntiVirus. Las referencias de la documentación a clientes Windows 3.x y DOS podrán aplicarse sólo a los clientes instalados como parte de Norton AntiVirus Corporate Edition 7.6x y Symantec AntiVirus Corporate Edition 8.0.

Novedades de esta versión

Symantec AntiVirus Corporate Edition incorpora nuevas funciones, además de mejoras en las ya existentes. La Tabla 1-1 recoge y describe las novedades de esta versión.

Tabla 1-1 Nuevas características de Symantec AntiVirus Corporate Edition

Función	Descripción
Seguridad mejorada en los grupos de servidores	Una manera de mejorar la seguridad proporcionada por las contraseñas para los grupos de servidores consiste en crear listas de acceso para restringir la comunicación entrante de modo que sólo puedan acceder las direcciones IP e IPX especificadas en dicha lista de acceso. Por ejemplo, podrá evitar que un agresor con acceso a la consola de Symantec System Center y contraseña válida para un grupo de servidores pueda realizar cambios no autorizados en los siguientes elementos: ■ Valores de protección antivirus de servidores y clientes ■ Valores de protección en tiempo real del sistema de archivos ■ Asignaciones de pertenencia a grupos de clientes ■ Asignaciones de servidores principales ■ Distribución del archivo Grc.dat ■ Recuperación de archivos de definiciones de virus

Tabla 1-1 Nuevas características de Symantec AntiVirus Corporate Edition

Función	Descripción
Auditoría de redes	Los equipos de la red que no estén protegidos contra virus pueden abrir agujeros de seguridad en la red. Puede realizar auditorías de seguridad de la red en los equipos remotos para determinar: ■ si hay un client de Symantec AntiVirus Corporate Edition instalado y ejecutándose; ■ el tipo de protección instalada, como por ejemplo un cliente no administrado, un cliente o servidor antivirus; ■ si el equipo tiene instalado algún software antivirus de Symantec (como por ejemplo una versión de Symantec AntiVirus para consumidores) o de otro fabricante. Esta información incluye el tipo y la versión del software.
Compatibilidad con equipos de 64 bits	El client de Symantec AntiVirus Corporate Edition proporciona protección antivirus a los clientes y servidores compatibles de 64 bits. Si desea obtener más información acerca de los requisitos del sistema, consulte "El client de Symantec AntiVirus Corporate Edition en equipos de 64 bits" en la página 15.
Compatibilidad con Windows Server 2003	Podrá instalar los siguientes componentes en equipos que ejecuten Windows Server 2003: ■ El servidor de Symantec AntiVirus Corporate Edition (de 32 bits) ■ El servidor de cuarentena (de 32 bits) ■ El client de Symantec AntiVirus Corporate Edition (de 32 y 64 bits)
Compatibilidad con Secure Console de NetWare	Symantec AntiVirus Corporate Edition puede instalarse en servidores NetWare mientras se ejecuta Secure Console de NetWare.

Funcionamiento de la instalación de Symantec AntiVirus Corporate Edition

Symantec AntiVirus Corporate Edition ofrece varios métodos para instalar servidores, que se muestran en la Tabla 1-2.

Tabla 1-2 Orígenes de instalación de servidores de Symantec AntiVirus Corporate Edition

Origen	Descripción
Paquete	Si desea instalar un servidor de Symantec AntiVirus Corporate Edition, puede utilizar el paquete preconfigurado de instalación del servidor. Los paquetes se pueden distribuir por medio de Symantec Packager, por una instalación basada en Web, por una secuencia de comandos de inicio de sesión o con herramientas de terceros.
Herramienta de distribución del servidor antivirus	Es posible transferir una instalación de servidor a equipos en los que se ejecuten sistemas operativos Microsoft Windows y NetWare 5.x o superior desde Symantec System Center o desde el CD de Symantec AntiVirus Corporate Edition.
Symantec Packager	Se puede crear un paquete personalizado que contenga una instalación del servidor.
Basada en Web	Se puede crear una instalación basada en Web para un servidor Web compatible. Los administradores también pueden crear un sitio para descargar la instalación del servidor, si así lo desean.

En la Tabla 1-3 se muestran y describen los métodos de instalación del cliente de Symantec AntiVirus Corporate Edition y se resumen las tareas previas que es preciso realizar antes de la distribución.

Tabla 1-3 Métodos de instalación de clientes de Symantec AntiVirus Corporate Edition

Método	Descripción
Herramienta de instalación de clientes de NT	Se pueden transferir instalaciones de clientes a equipos con sistemas operativos compatibles Microsoft Windows desde Symantec System Center o desde el CD de Symantec AntiVirus Corporate Edition.
Symantec Packager	Puede utilizar Symantec Packager para crear un paquete que contenga una instalación de cliente personalizada para equipos de 32 bits. Los paquetes se pueden distribuir por medio de Symantec Packager, por una instalación basada en Web, por una secuencia de comandos de inicio de sesión o con herramientas de terceros. Symantec Packager no es compatible con equipos de 64 bits.
CD o imagen de disco	Es posible instalar clientes desde una imagen de disco basada en un servidor o desde el CD de instalación.
Instalación basada en Web	Se puede crear una instalación basada en Web para un servidor Web compatible. Existen instalaciones de clientes basadas en Web disponibles para equipos que ejecuten sistemas operativos compatibles Microsoft Windows. Tras configurar el servidor Web, se puede proporcionar a los usuarios una URL para acceder a la ubicación de la instalación.
Secuencia de comandos de inicio de sesión	Si se utilizan secuencias de comandos de inicio de sesión en las redes de Windows o NetWare, se puede agregar un componente a la secuencia de comandos que compruebe la existencia del cliente y lo instale. El programa de instalación del servidor crea automáticamente un grupo de inicio de sesión de NetWare. Mediante las herramientas de administración de la red habituales se pueden agregar usuarios a ese grupo.
Herramientas de terceros	Se pueden distribuir clientes utilizando herramientas de otros fabricantes, como Microsoft Systems Management Server.

Cómo se realiza la actualización de la protección

Las políticas de firewall de Symantec AntiVirus Corporate Edition ofrece cuatro métodos para actualizar los archivos de definiciones de virus, que se describen en la Tabla 1-4.

Tabla 1-4 Métodos de actualización de los archivos de definiciones de virus

Método	Descripción
Método de transporte de definiciones de virus	Operación de transferencia que se inicia cuando un servidor primario de la red recibe nuevas definiciones de virus de Symantec o de un servidor de LiveUpdate interno. El servidor primario transfiere un paquete con las definiciones de virus a todos los servidores secundarios. Los servidores secundarios extraen automáticamente las definiciones de virus, las colocan en el directorio adecuado y las transfieren a cada client de 32 bits de Symantec AntiVirus Corporate Edition que administre. Esta función no es compatible con equipos de 64 bits. Los clientes extraen las definiciones de virus y las colocan en el directorio correspondiente.
LiveUpdate	Operación de obtención que comienza cuando un client o un servidor de Symantec AntiVirus Corporate Edition solicita nuevas definiciones de virus. Es posible configurar LiveUpdate para que se ejecute de forma planificada o tras un número de días determinado cuando se detecte una conexión a Internet. Esta utilidad puede configurarse en cada equipo para solicitar la actualización desde un servidor de LiveUpdate interno designado o directamente desde el servidor LiveUpdate de Symantec. Además, la función LiveUpdate continuo permite a los clientes con conexión intermitente iniciar LiveUpdate de forma automática cuando se conecten a Internet y haya transcurrido un número determinado de días. LiveUpdate es el único método de actualización de archivos de definiciones de virus compatible con equipos de 64 bits.

Tabla 1-4 Métodos de actualización de los archivos de definiciones de virus

Método	Descripción
Sondeo de Cuarentena central	Se puede configurar el servidor de Cuarentena central para averiguar si existen actualizaciones de archivos de definiciones de virus en Symantec y transferirlas automáticamente a los equipos de la red.
Intelligent Updater	Archivo ejecutable autoextraíble que contiene archivos de definiciones de virus. Este tipo de archivos puede descargarse del sitio Web de Symantec.

Preparación del Método de transporte de definiciones de virus

El Método de transporte de definiciones de virus constituye una operación de transferencia que se inicia desde Symantec System Center. Este método no es compatible con equipos de 64 bits.

Preparación de LiveUpdate

Mediante LiveUpdate, los servidores y clientes de Symantec AntiVirus Corporate Edition obtienen los archivos de definiciones de virus desde Symantec o desde un servidor interno de LiveUpdate.

Nota: LiveUpdate es el único método de actualización de archivos de definiciones de virus compatible con equipos de 64 bits.

Preparación del sondeo de Cuarentena central

Mediante el sondeo de Cuarentena central, el servidor de Cuarentena central sondea periódicamente la pasarela de Symantec Digital Immune System en busca de nuevos archivos de definiciones de virus. Cuando haya nuevas definiciones disponibles, el servidor de Cuarentena central puede transmitirlas automáticamente a los equipos que las necesiten, utilizando para ello el Método de transporte de definiciones de virus. Este método no es compatible con equipos de 64 bits.

Preparación de Intelligent Updater

Los archivos de Intelligent Updater son archivos ejecutables autoextraíbles que contienen definiciones de virus. Están disponibles para ser descargados desde el sitio Web de Symantec Security Response. Este método no es compatible con equipos de 64 bits.

Al planificar la actualización de las definiciones de virus mediante Intelligent Updater, debe determinar las formas en las que se podrán distribuir los archivos de Intelligent Updater. Por ejemplo, si todos los usuarios de equipos portátiles de su organización disponen de unidad de CD-ROM, podría crear un CD que contuviera el archivo de Intelligent Updater y enviárselo a los usuarios que tengan una conexión lenta a Internet.

Protección de volúmenes y agrupaciones de servidores de NetWare

Symantec AntiVirus Corporate Edition protege los volúmenes y agrupaciones de servidores de NetWare proporcionando funciones de análisis manuales y en tiempo real para todos los servidores de la agrupación. Los servidores propietarios de los volúmenes gestionarán los análisis antivirus de los volúmenes de las agrupaciones correspondientes. En caso de fallo de un servidor con propiedad sobre un volumen de agrupación, NetWare transferirá la propiedad sobre el volumen a otro servidor de la agrupación, el cual asumirá automáticamente las tareas de análisis antivirus.

Para proteger volúmenes y agrupaciones de servidores de NetWare

- Ejecute Symantec AntiVirus Corporate Edition después de que todos los volúmenes se hayan montado y los servicios de la agrupación se hayan iniciado en el archivo Autoexec.ncf.

  La ejecución de Symantec AntiVirus Corporate Edition una vez que se han completado estas tareas garantiza que se detecten todos los volúmenes.

Instalación en una agrupación de NetWare

Para instalar Symantec AntiVirus Corporate Edition en una agrupación de NetWare, deberá instalar primero Symantec AntiVirus Corporate Edition en todos los servidores de NetWare que haya en la agrupación siguiendo el procedimiento de instalación estándar para servidores de NetWare. No instale Symantec AntiVirus Corporate Edition en los volúmenes.

Acerca de los requisitos de instalación

Symantec AntiVirus Corporate Edition requiere protocolos, software, hardware, sistemas operativos y versiones de Service Pack específicos.

Todos los requisitos de los componentes de Symantec AntiVirus Corporate Edition se han diseñado para funcionar junto con las recomendaciones de hardware y software para los equipos compatibles con Microsoft Windows y NetWare.

Requisitos de instalación del servidor de Symantec AntiVirus Corporate Edition

Sistemas operativos de Microsoft Windows

El servidor de Symantec AntiVirus Corporate Edition presenta los siguientes requisitos para poder utilizarse en sistemas operativos de Windows:

- Windows NT 4.0 Workstation, Server y Terminal Server Edition con Service Pack 6a o posterior; Windows 2000 Professional, Server, Advanced Server; Windows XP Professional; Windows Server 2003 Web, Standard, Enterprise y Datacenter
- 32 MB de RAM (se recomiendan 64 MB o más)
- 111 MB de espacio en el disco (65 MB para los archivos de servidor de Symantec AntiVirus Corporate Edition y 46 MB para la imagen de disco del client de Symantec AntiVirus Corporate Edition)
- 15 MB de espacio disponible en disco para los archivos del servidor de AMS^2 (si decide instalar el servidor de AMS^2)
- Procesador Intel Pentium (se recomienda Pentium II o superior)
- Dirección IP fija (se recomienda)

Requisitos para versiones anteriores de NetWare

Symantec AntiVirus Corporate Edition es compatible con NetWare 3.12, 3.2, 4.11, 4.2 y 5.x (sin necesidad de Support Pack) con el servidor de Norton AntiVirus Corporate Edition 7.6.

Si desea más información, consulte la *Guía de implementación de Norton AntiVirus Corporate Edition,* situada en la carpeta de documentos del CD de soluciones anteriores de Symantec AntiVirus.

Requisitos del servidor de cuarentena

El servidor de cuarentena presenta los siguientes requisitos:

- Windows NT 4.0 Workstation y Server con Service Pack 6a; Windows 2000 Professional, Server, Advanced Server; Windows XP Professional; Windows Server 2003 Web, Standard, Enterprise y Datacenter
- 128 MB de RAM
- Un archivo de intercambio de un tamaño mínimo de 250 MB
- 40 MB de espacio disponible en disco; se recomienda disponer de entre 500 MB y 4 GB de espacio disponible en disco para los elementos en cuarentena
- Internet Explorer 5.5 con Service Pack 2
- Procesador Intel Pentium (se recomienda Pentium II o superior)

Requisitos de instalación del cliente de Symantec AntiVirus Corporate Edition

El client de Symantec AntiVirus Corporate Edition en equipos de 32 bits

El client de Symantec AntiVirus Corporate Edition para equipos de 32 bits precisa los siguientes requisitos:

- Windows 98/98 SE/ME; Windows NT 4.0 Workstation/Server/Terminal Server Edition con Service Pack 6a; Windows 2000 Professional/Server/ Advanced Server; Windows XP Home/Professional o Windows Server 2003 Web/Standard/Enterprise/Datacenter
- 32 MB de RAM como mínimo
- 46 MB de espacio disponible en disco
- Procesador Intel Pentium (se recomienda Pentium II o superior)

El client de Symantec AntiVirus Corporate Edition en equipos de 64 bits

El client de Symantec AntiVirus Corporate Edition para equipos de 64 bits precisa los siguientes requisitos:

- Edición de 64 bits de Windows XP versión 2003; ediciones de 64 bits de Windows Server 2003 Enterprise/Datacenter
- 32 MB de RAM como mínimo
- 80 MB de espacio disponible en disco
- Procesador Itanium 2

Requisitos de Symantec Packager

Symantec Packager funciona sólo en sistemas operativos Microsoft de 32 bits y precisa los siguientes requisitos de sistema:

- Sistemas operativos admitidos:
  - Windows NT Workstation 4.0 o Server 4.0, con Service Pack 6a
  - Windows 2000 Professional o Server, con Service Pack 2
  - Windows XP Professional
- Microsoft Internet Explorer 5.5 o posterior
- Windows Installer 2.0
  Si Windows Installer 2.0 no está instalado, el programa de instalación de Symantec Packager se encargará de instalarlo.
- Procesador Pentium II a 300 MHz (o superior)
- 64 MB de RAM (128 MB recomendados)
- 60 MB de espacio disponible en disco
- Unidad de CD-ROM o de DVD-ROM

Requisitos de los paquetes de instalación

Aunque Symantec Packager funciona sólo en los sistemas operativos Windows NT, 2000 y XP, los paquetes que se creen utilizando Symantec Packager se pueden instalar en los siguientes sistemas operativos:

- Windows 98
- Windows Millennium Edition (ME)
- Windows NT 4.0 con Service Pack 6a
- Windows 2000
- Windows XP Home Edition o Professional Edition

Los paquetes que contengan sólo comandos personalizados pueden funcionar en otros sistemas operativos. No obstante, los paquetes instalados sólo funcionarán en sistemas Microsoft de 32 bits.

Los requisitos de sistema específicos para los paquetes dependen del contenido y de las opciones de cada paquete en concreto. Los requisitos de hardware para los paquetes de instalación varían dependiendo del contenido de cada paquete.

Requisitos de derechos de usuario

Symantec Packager precisa derechos de administrador para poder instalarse en Windows NT/2000/XP/2003.

Windows XP impide a los usuarios que tengan asignadas cuentas de usuario limitado o de invitado que instalen o desinstalen software, que cambien las opciones de configuración que afectan a todo el sistema o que agreguen, modifiquen o eliminen cuentas de usuario. Para obtener un rendimiento óptimo, inicie sesión como usuario con derechos de administrador cuando ejecute Symantec Packager en Windows XP.

Instalación de Symantec System Center

Symantec System Center se instala directamente desde el CD de Symantec AntiVirus Corporate Edition.

Instale Symantec System Center en los equipos desde los que desee administrar la protección antivirus.

Además de Symantec System Center, se instalan de forma predeterminada los siguientes componentes de administración:

- Consola de Alert Management System^2 (AMS^2): necesaria si se quiere utilizar el sistema de alertas mejorado que incorpora AMS^2.
- Módulo integrable de Symantec AntiVirus: necesario en caso de que se quiera administrar la protección antivirus de forma centralizada.
- Módulo integrable de Symantec Client Firewall: necesario si se desean distribuir de forma centralizada las políticas de firewall y de detección de intrusiones.
- Herramienta de distribución del servidor antivirus: hace que sea posible transferir la instalación del server a los equipos remotos. Esta herramienta también se encuentra disponible en el CD de Symantec AntiVirus Corporate Edition.
- Herramienta de instalación de cliente de NT: permite transferir la instalación del client de Symantec AntiVirus Corporate Edition en equipos remotos con sistemas operativos Microsoft Windows. Esta herramienta también se encuentra disponible en el CD de Symantec AntiVirus Corporate Edition.

Inicio de la instalación del servidor

Para iniciar la instalación desde Symantec System Center

1. En el panel izquierdo de Symantec System Center, haga clic en **Jerarquía del sistema** o en cualquiera de los objetos situados debajo.
2. En el menú Herramientas, haga clic en **Distribución de servidores de AV**.

   La distribución de servidores sólo estará disponible si el componente de distribución del servidor se selecciona durante la instalación de Symantec System Center. Este componente está seleccionado para instalarse de forma predeterminada.
3. Continúe con la instalación.

Finalización de la instalación del servidor

En caso de realizar la instalación desde un servidor de NetWare, el nombre de la carpeta nueva quedará restringido a 8 caracteres.

Instalación de Symantec AntiVirus Corporate Edition con Secure Console de NetWare activado

Si utiliza Secure Console de NetWare, podrá instalar Symantec AntiVirus Corporate Edition mientras Secure Console se esté ejecutando. Tras realizar una instalación estándar de Symantec AntiVirus Corporate Edition, deberá copiar el NLM en el directorio correspondiente y después ejecutar el NLM en cada uno de los servidores de NetWare para completar el proceso de instalación. Esto se puede realizar desde la consola del servidor si se cuenta con los derechos necesarios, o utilizando Rconsole (NetWare 5.x) en redes que empleen el protocolo IPX, o RConsoleJ (NetWare 5.x o 6) en redes que empleen el protocolo IP.

Cargue manualmente los NLM de Symantec AntiVirus Corporate Edition mientras esté ejecutando Secure Console

Tras terminar con el proceso de instalación, deberá copiar el archivo Vpstart.nlm que hay en el directorio de instalación a Sys:\System y después cargar el archivo Vpstart.nlm por primera vez mediante el parámetro /Install. Si elige el inicio automático durante la instalación, los NLM se cargarán automáticamente cuando se reinicie el servidor, mientras que, si elige el inicio manual, deberá cargar Vpstart.nlm manualmente cada vez que reinicie el servidor.

Nota: No añada la ruta a los comandos especificados en la consola de NetWare. Escriba cada comando tal y como aparezca. Estos comandos de NetWare distinguen entre mayúsculas y minúsculas.

Para cargar los NLM de Symantec AntiVirus Corporate Edition manualmente por primera vez al ejecutar Secure Console

1. Copie el archivo **Vpstart.nlm** que hay en el directorio de instalación predeterminado, Sys:\Sav (o el directorio que se especificase durante la instalación) al directorio Sys:\System.
2. En la consola del servidor, escriba lo siguiente:
   Vpstart /install /SECURE_CONSOLE SYS:\SAV\VPSTART.NLM

Advertencia: Sólo tendrá que realizar este procedimiento una vez después de instalar el software. Si vuelve a utilizar el parámetro /Install, sobrescribirá cualquier configuración establecida.

Para cargar los NLM de Symantec AntiVirus Corporate Edition manualmente tras la instalación de los NLM y mientras se ejecuta Secure Console

- En la consola del servidor, escriba lo siguiente:
  Vpstart.nlm

Instalación manual del servidor de AMS

Se puede instalar el servidor de AMS^2 manualmente en equipos en los que ya se haya instalado el servidor de Symantec AntiVirus Corporate Edition.

Instale manualmente el servidor de AMS

El método de instalación de AMS^2 es distinto en equipos con Windows NT, 2000 o XP y en servidores de NetWare.

Nota: Para evitar la pérdida de información importante al desinstalar Symantec AntiVirus Corporate Edition de un servidor primario en un equipo con NetWare, debe primero convertir ese servidor en secundario y otro servidor distinto en primario. Para obtener más información acerca de la selección de servidores primarios, consulte la *Guía del administrador de Symantec AntiVirus Corporate Edition*.

Para instalar manualmente el servidor de AMS^2 en servidores de NetWare

1. Desinstale el servidor antivirus de Symantec AntiVirus Corporate Edition.
2. Ejecute el programa de instalación del servidor.
   Cuando así se le solicite, asegúrese de que tiene marcada la opción Alert Management System^2 (AMS^2).

Inicio de la instalación del client

Puede instalar el client de Symantec AntiVirus Corporate Edition mediante la herramienta Instalación de cliente de NT.

Para iniciar la instalación del client desde Symantec System Center

1. En el panel izquierdo de Symantec System Center, haga clic en **Jerarquía del sistema** o en cualquiera de los objetos situados debajo.
2. En el menú Herramientas, haga clic en **Instalación de cliente de NT.**
   Esta opción sólo estará disponible si la herramienta Instalación de cliente de NT se seleccionó al instalar Symantec System Center. Este componente está seleccionado para instalarse de forma predeterminada.
3. Continúe con la instalación.
   Vea "Ejecución del programa de instalación del cliente antivirus" en la página 20.

Ejecución del programa de instalación del cliente antivirus

Para ejecutar el programa de instalación del client

1. En la ventana de bienvenida de la utilidad de instalación de clientes, haga clic en **Siguiente.**
2. En la sección Equipos disponibles del cuadro de diálogo Selección de equipos, haga doble clic en **Red de Microsoft Windows.**
3. Lleve a cabo los siguientes pasos:
   - En la sección Equipos disponibles, seleccione un equipo.
   - En la sección Servidores de Symantec AntiVirus, seleccione un equipo.
4. Haga clic en **Agregar.**
5. Repita los pasos 3 y 4 hasta agregar todos los clientes que desee administrar.
   Puede volver a realizar la instalación en equipos en los que ya se ejecute Symantec AntiVirus Corporate Edition, o importar un archivo de texto para agregar clientes de Windows NT, 2000, 2003 o XP.

Asocie los usuarios con la secuencia de comandos de inicio de sesión

El recurso compartido de inicio de sesión para Windows Server 2003 se encuentra de forma predeterminada en C:\Winnt\Sysvol\Sysvol\Domainname\Scripts.

Instale localmente los clientes de Symantec AntiVirus Corporate Edition

Al instalar el client de Symantec AntiVirus Corporate Edition, se inicia la instalación, se selecciona si se debe realizar una instalación administrada o no del cliente y se finaliza la instalación.

Para iniciar la instalación

1. Si los usuarios van a ejecutar el cliente en modo administrado, infórmeles del servidor de Symantec AntiVirus Corporate Edition al que deberán conectarse.

   El programa de instalación les pedirá esta información.

2. Otorgue acceso a los usuarios al CD de Symantec AntiVirus Corporate Edition.

3. En el caso de instalación en equipos de 32 bits, pida a los usuarios que ejecuten el archivo Setup.exe que hay en el directorio raíz del CD. En el caso de instalación en equipos de 64 bits, deberá ejecutarse el archivo Setup.exe localizado en la carpeta D:\SAVWIN64.

Advertencia: Si la versión de Setup.exe para 32 bits se ejecutase en un equipo de 64 bits, la instalación resultaría fallida y ni siquiera se notificaría el fallo. En el caso de instalaciones en equipos de 64 bits, los usuarios deberán ejecutar el archivo Setup.exe que hay en la carpeta \SAVWIN64 del directorio raíz del CD.

Capítulo 2

Actualizaciones de la Guía del administrador de Symantec AntiVirus Corporate Edition

Acerca de las actualizaciones de la Guía del administrador de Symantec AntiVirus Corporate Edition

El propósito de este capítulo es explicar los cambios aplicados a la *Guía del administrador de Symantec AntiVirus Corporate Edition* entre las versiones 8.0 y 8.1 de Symantec AntiVirus Corporate Edition.

Compatibilidad con Windows 3.x/DOS

El producto Symantec AntiVirus Corporate Edition 8.1 ya no incluye clientes de versiones anteriores para Windows 3.x y DOS en el CD de soluciones anteriores de Symantec AntiVirus. Las referencias de la documentación a clientes Windows 3.x y DOS podrán aplicarse sólo a los clientes instalados como parte de Norton AntiVirus Corporate Edition 7.6x y Symantec AntiVirus Corporate Edition 8.0.

Requisito de WINS o Active Directory para el servicio de reconocimiento

El servicio de reconocimiento precisa utilizar la resolución de nombres WINS (Windows Internet Naming Service) o Active Directory. Al intentar ejecutar el servicio de reconocimiento en un entorno en el que no se disponga de WINS o Active Directory, primero se deberá localizar en la red al menos un equipo en el que se ejecute un servidor de Symantec AntiVirus Corporate Edition. Para buscar el equipo, puede utilizar la función Buscar equipo o la herramienta Importer.

Auditoría de equipos

Los equipos de la red en los que no se esté ejecutando Symantec AntiVirus Corporate Edition pueden abrir agujeros de seguridad en la red. Puede realizar auditorías de seguridad de la red en los equipos remotos para determinar:

- si hay un componente antivirus de Symantec instalado y ejecutándose;
- el tipo de protección instalada, como por ejemplo un cliente no administrado, un cliente o servidor antivirus;
- si hay instalado en el equipo algún software antivirus de otro fabricante o de Symantec (como una versión de Symantec AntiVirus para consumidores), incluido el tipo y la versión del software.

Deberá poder iniciar la sesión como administrador en los equipos remotos que vaya a auditar.

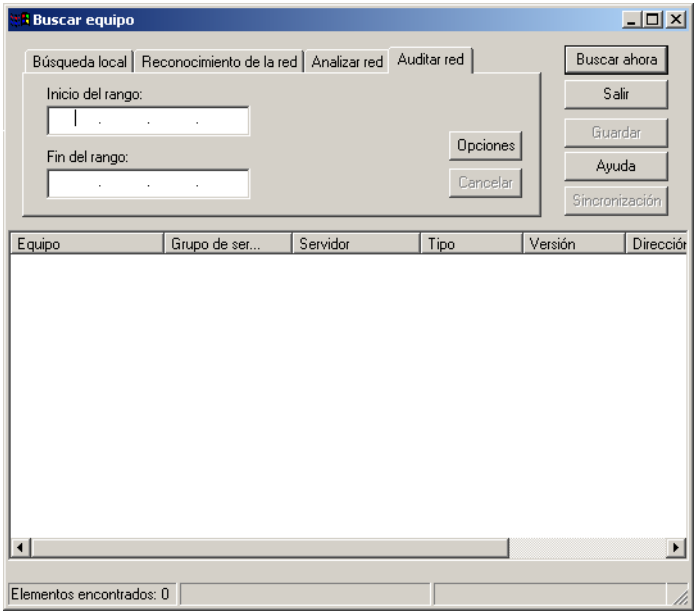
Nota: Si en el equipo remoto se está ejecutando un firewall, es posible que la operación de auditoría de red no consiga recopilar información.

Realización de auditorías de red y sincronización

Las auditorías de red sirven para determinar el estado de protección antivirus en los equipos que se administren. Una vez identificado el estado de los equipos dentro del intervalo examinado, podrá localizar los equipos que seleccione sincronizándose con ellos.

Para realizar una auditoría de red

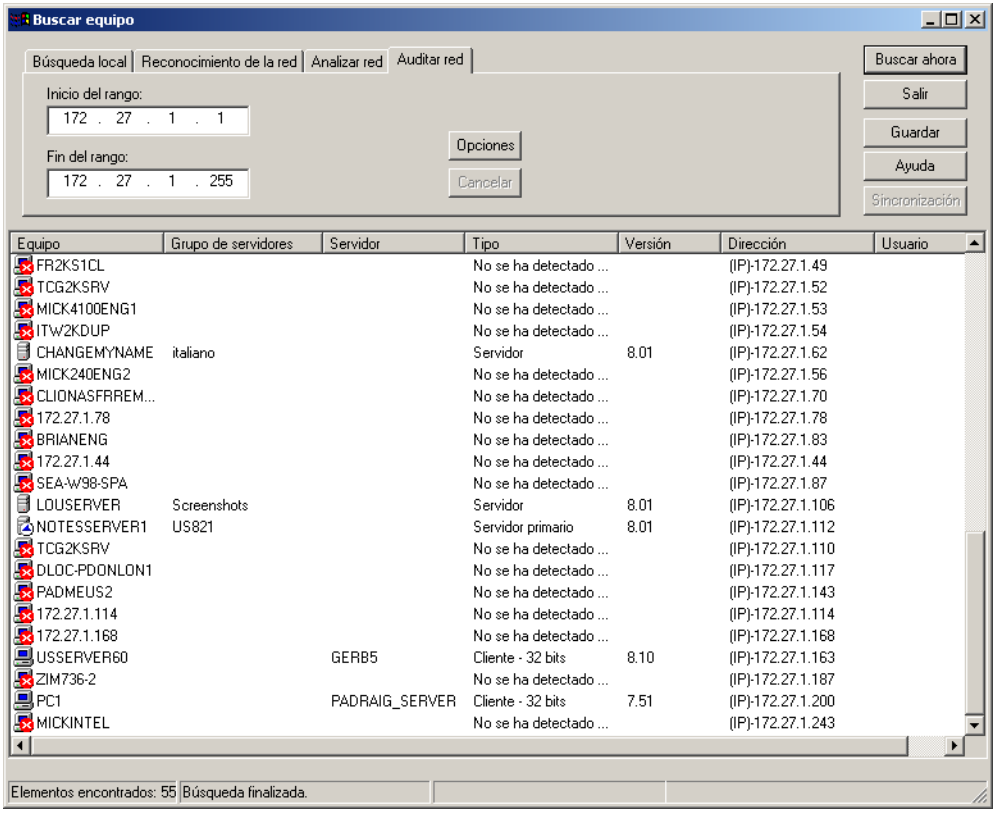
1 Haga clic en **Buscar equipo** en el menú Herramientas de la consola de Symantec System Center.



2 En el cuadro de diálogo Buscar equipo, escriba el principio y el final del intervalo de direcciones IP en la ficha Auditar red.

3 Para cambiar las opciones predeterminadas, haga clic en **Opciones.**
Vea "Configuración de las opciones de auditoría de red" en la página 28.

4 Haga clic en **Buscar ahora** para iniciar la auditoría.



Podrá ver cómo avanza el proceso de auditoría en la parte inferior del cuadro de diálogo Buscar equipo.

Una vez terminado el proceso de auditoría, aparecerá la siguiente información:

Nombre de equipo	Indica el nombre del equipo remoto.
Grupo de servidores	Muestra el nombre del grupo de servidores al que pertenece el equipo remoto.
Servidor	Indica el nombre del servidor que controla al equipo remoto.
Tipo	Señala el tipo de servidor o de cliente. Los errores de inicio de sesión aparecerán también indicados en esta columna.
Versión	Muestra la versión del producto antivirus que se está ejecutando en el equipo.
Dirección	Indica la dirección IP del equipo.
Usuario	Muestra el nombre de usuario asociado al equipo.

Para sincronizar elementos

1. En el cuadro de diálogo Buscar equipo, haga clic en **Sincronización** para localizar un equipo seleccionado que ejecute el cliente antivirus de Symantec AntiVirus Corporate Edition.
2. Escriba la contraseña para el grupo de servidores al que pertenezca el elemento.

Etiquetado de elementos y repetición de auditorías

Los siguientes son ejemplos de elementos que conviene etiquetar:

- Equipos que no puedan localizarse o con los que no se pueda establecer conexión
- Enrutadores y unidades de red
- Equipos que no tengan instalado software antivirus de Symantec

Para etiquetar un elemento y repetir la auditoría

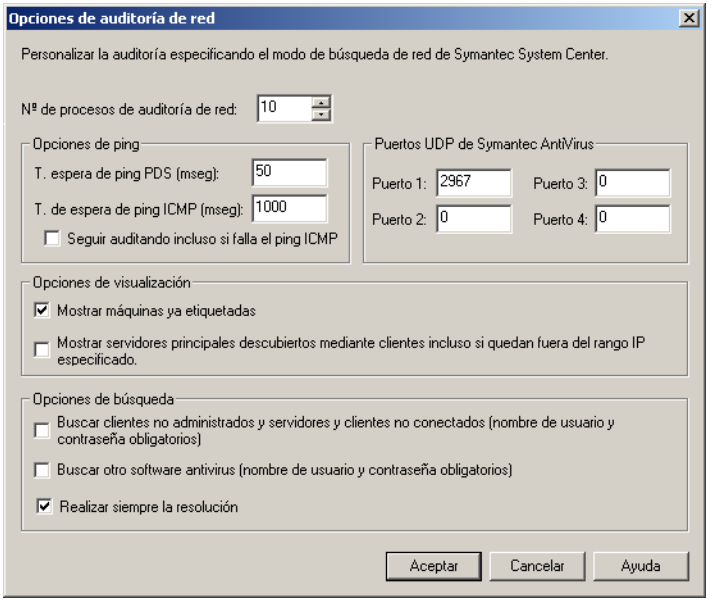
1. En el cuadro de diálogo Buscar equipo, en la columna Equipo, haga clic con el botón derecho en un elemento y, a continuación, haga clic en **Etiquetar**.
2. En el cuadro de diálogo Editar la descripción de, escriba la nueva etiqueta que quiera aplicar al equipo.
3. Haga clic en **Aceptar**.
4. Vuelva a hacer clic con el botón derecho en el elemento y, después, haga clic en **Volver a auditar**.

Configuración de las opciones de auditoría de red

Las opciones de auditoría de red pueden personalizarse. Por ejemplo, puede activar una opción para localizar equipos remotos en los que se esté ejecutando un cliente antivirus no administrado.

Para establecer opciones de auditoría de red

1 En el cuadro de diálogo Buscar equipo, en la ficha Auditar red, haga clic en **Opciones**.



2 En el cuadro de diálogo Opciones de auditoría de red, especifique el número de procesos de auditoría de red que desee utilizar.

Cuanto mayor sea el número, más rápida será la obtención de resultados, si bien se usarán más recursos de la red.

3 En Opciones de ping, especifique el tiempo de espera en milisegundos para un ping Windows ICMP o un ping Symantec PDS.

4 Marque **Seguir auditando incluso si falla el ping ICMP** si prefiere que el proceso de auditoría continúe en caso de que falle el ping ICMP.

Por ejemplo, si sabe que hay un firewall configurado con una norma para bloquear pings ICMP, podrá seguir auditando los equipos en los que se esté ejecutando Symantec AntiVirus Corporate Edition.

5 En Opciones de visualización, marque la casilla **Mostrar máquinas ya etiquetadas** si ya etiquetó equipos durante otra auditoría anterior y desea que éstos aparezcan en los resultados tal y como se etiquetaron anteriormente.

6 Marque **Mostrar servidores principales descubiertos mediante clientes incluso si quedan fuera del rango IP especificado** para que aparezcan también en los resultados los servidores principales de los equipos que queden fuera del rango indicado y en los que se esté ejecutando el client o el server de Symantec AntiVirus Corporate Edition.

7 En Puertos UDP de Symantec AntiVirus, escriba hasta cuatro números de puerto para los puertos a los que quiera hacer ping.

El valor predeterminado para el puerto 1 es 2967, que es el número de puerto predeterminado para RTVScan.

8 En Opciones de búsqueda, marque las casillas correspondientes para localizar equipos en los que se esté ejecutando software antivirus no administrado de Symantec AntiVirus Corporate Edition, servidores y clientes desconectados, o equipos en los que se esté ejecutando software antivirus de otro fabricante.

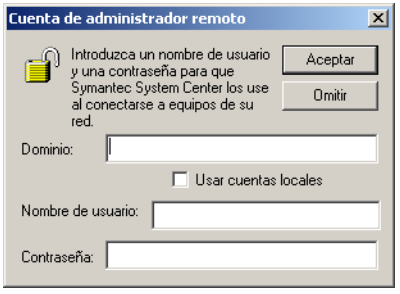
Debe proporcionar información válida de cuenta de administrador.

Vea "Configuración de las opciones de la cuenta de administrador" en la página 29.

Configuración de las opciones de la cuenta de administrador

Si opta por buscar equipos en los que se esté ejecutando software antivirus no administrado de Symantec AntiVirus Corporate Edition, servidores desconectados o equipos en los que se ejecute software antivirus de otro fabricante, aparecerá el cuadro de diálogo Cuenta de administrador remoto.

Figura 2-1 Cuadro de diálogo Cuenta de administrador remoto



Para establecer las opciones de la cuenta de administrador

1. En el cuadro de diálogo Cuenta de administrador remoto, realice una de las siguientes acciones:
   - Escriba el nombre del dominio que contenga los equipos que desee localizar seguido de la información correcta de la cuenta del administrador del dominio.
   - Marque la casilla **Usar cuentas locales** para acceder a un equipo concreto y, a continuación, escriba el nombre de usuario y la contraseña de administrador.
2. Haga clic en **Aceptar**.

Mejora de la seguridad en los grupos de servidores

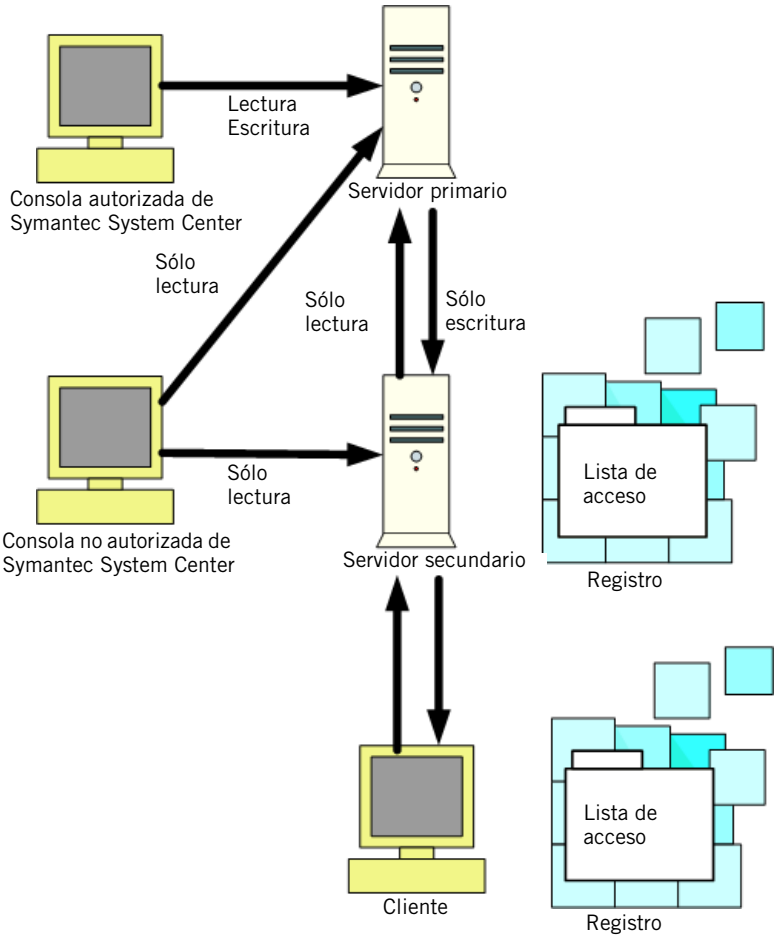
Una manera de mejorar la seguridad proporcionada por las contraseñas para los grupos de servidores consiste en crear listas de acceso para restringir la comunicación entrante de modo que sólo puedan acceder las direcciones IP e IPX especificadas en dicha lista de acceso. Por ejemplo, podrá evitar que un agresor con acceso a la consola de Symantec System Center y contraseña válida para un grupo de servidores pueda realizar cambios no autorizados en los siguientes elementos:

- Valores de protección antivirus de servidores y clientes
- Valores de protección en tiempo real del sistema de archivos
- Asignaciones de pertenencia a grupos de clientes
- Asignaciones de servidores principales
- Distribución del archivo Grc.dat
- Recuperación de archivos de definiciones de virus

Funcionamiento de la lista de acceso

La lista de acceso se almacena en el registro de Windows de todos los equipos protegidos y comprueba si las direcciones de las consolas de Symantec System Center que intentan comunicarse con el equipo están en la lista de acceso. Las consolas de Symantec System Center cuyas direcciones IP o IPX no estén en la lista de acceso sólo podrán acceder en modo de lectura a los valores de protección antivirus y a otros valores (consulte la Figura 2-2).

Figura 2-2 Seguridad mejorada en los grupos de servidores



Aplicación de mayor seguridad en los grupos de servidores

Debe realizar las siguientes operaciones para ampliar la protección y controlar posibles cambios de configuración no autorizados:

- Seleccione los equipos que desee proteger.
- Cree una lista de acceso.
- Distribuya la lista de acceso.
- Registre los intentos de cambios de configuración no autorizados.

Selección de equipos que proteger

La dirección IP del equipo en el que se esté ejecutando la consola de Symantec System Center deberá incluirse en las listas de acceso de todos los servidores que formen parte de un grupo de servidores. En caso de cambiar sólo los valores de configuración de los grupos de clientes, únicamente necesitará incluir la dirección del servidor principal.

No es necesario que incluya la lista de acceso en todos los clientes. Si crea una lista de acceso en todos los servidores de un grupo y la deja vacía, conseguirá bloquear eficazmente el grupo de servidores y evitar la simulación de las direcciones IP. Añada las direcciones IP e IPX a la lista de acceso sólo cuando necesite que Symantec System Center pueda acceder al servidor. Borre el valor de dirección cuando ya no sea necesario acceder al servidor.

Creación de una lista de acceso

Para crear una lista de acceso, es necesario crear primero una subclave de registro y especificar las direcciones IP e IPX autorizadas.

Para crear una lista de acceso

1. Inicie un editor de registro, como por ejemplo Regedt32.
2. Abra la clave HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion.
3. Escriba **AccessList** como nueva subclave.

4 En la subclave AccessList, añada los valores de cadena para las direcciones IP e IPX y las direcciones de subred de los equipos que vaya a incluir en la lista de acceso. Utilice los siguientes formatos:

IP	Escriba **(IP)-<0.0.0.0>** donde <0.0.0.0> será la dirección numérica del equipo.
Subred IP	Escriba **(IP)-<0.0.0.0>/<n>** donde <0.0.0.0> será la dirección numérica del equipo y <n> será la anotación de subred (por ejemplo, 16 o 24).
IPX	Escriba **(IPX)-<0000000:0000000000000>** donde <0000000:0000000000000> será la dirección numérica del equipo.
Subred IPX	Escriba **(IPX)-<0000000>:<FFFFFFFFFFFFFF>** donde <0000000> será la dirección numérica del equipo y <FFFFFFFFFFFFFF> será la anotación de subred.

5 Cierre el editor del registro.

Recarga forzosa de la lista de acceso

La lista de acceso se actualiza de manera predeterminada cada cinco minutos, si bien es posible forzar el proceso de recarga para aplicar de manera inmediata cualquier cambio realizado.

Para forzar la lista de acceso a fin de que vuelva a cargarse

1 Inicie un editor de registro, como por ejemplo Regedt32.

2 Abra la clave HKEY_LOCAL_MACHINE\SOFTWARE \INTEL\LANDesk\ VirusProtect6\CurrentVersion\ProductControl.

3 Escriba **ReadAccessList** como nuevo valor de DWORD.

4 Escriba **1** como dato binario asociado al valor de DWORD de ReadAccessList.

5 Cierre el editor del registro.

Distribución de la lista de acceso

Para distribuir la lista de acceso puede:

- crear una secuencia de comandos de registro con la información que quiera añadir a la lista de acceso, como, por ejemplo, valores nuevos para autorizar a más equipos;
- distribuir la lista mediante su herramienta de distribución preferida;
- forzar el componente de antivirus de Symantec AntiVirus Corporate Edition para que importe la lista de acceso de manera inmediata.
  Vea "Recarga forzosa de la lista de acceso" en la página 33.

Registro de intentos de cambios de configuración no autorizados

Cuando el componente de antivirus de Symantec AntiVirus Corporate Edition recibe comunicación desde una dirección no incluida en la lista de acceso, este componente de antivirus de Symantec AntiVirus Corporate Edition puede escribir el correspondiente suceso en el registro de sucesos. Cuando se produzca un error en un equipo que esté ejecutando un software de cliente de Symantec AntiVirus Corporate Edition, el registro de sucesos pasará a remitirse al servidor principal.

Nota: De forma predeterminada, los registros no incluyen información relativa a cambios de configuración no autorizados.

Registro de cambios y definición de la frecuencia de registro

Si lo desea, podrá modificar el registro para que deje constancia de cambios no autorizados. También es posible especificar la frecuencia de registro de este tipo de elementos.

Para registrar los cambios de configuración no autorizados

1. Inicie un editor de registro, como por ejemplo Regedt32.
2. Abra la clave HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\AccessList.
3. Escriba **LogAccessDenied** como nuevo valor de DWORD.
4. Escriba **1** como dato binario asociado al valor de DWORD de LogAccessDenied para activar el proceso registro.
5. Cierre el editor del registro.

Para definir la frecuencia de registro de intentos de cambios de configuración no autorizados

1. Inicie un editor de registro, como por ejemplo Regedt32.
2. Abra la clave HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\AccessList.
3. Escriba **LogAccessDeniedWindowMinutes** como nuevo valor de DWORD.
4. Realice una de las acciones siguientes:
   - Para registrar todos los incidentes, escriba **0** como dato binario asociado al valor de DWORD para LogAccessDeniedWindowMinutes.

     En caso de que se produzca un suceso no autorizado, aparecerá el siguiente mensaje:

     Acceso denegado a la comunicación por red desde dirección no autorizada: <dirección IP o IPX> <puerto>

     donde <dirección IP o IPX > será la dirección IP o IPX del equipo al que se le haya denegado el acceso y <puerto> será el número del puerto que el equipo haya intentado utilizar.
   - Para registrar incidentes según una frecuencia determinada en minutos, escriba un número (minutos) como dato binario asociado al valor de DWORD para LogAccessDeniedWindowMinutes.

     En caso de que se produzca un suceso no autorizado, aparecerá el siguiente mensaje:

     Acceso denegado a la comunicación por red desde direcciones no autorizadas <N> veces en los últimos <N> minutos. Dirección más reciente: <dirección IP o IPX> <puerto>

     donde <N> será la frecuencia y el número de minutos, <dirección IP o IPX> será la dirección IP o IPX del equipo al que se le haya denegado el acceso, y <puerto> será el número de puerto que el equipo haya intentado utilizar.
5. Cierre el editor del registro.

Aceleración de la configuración de alerta

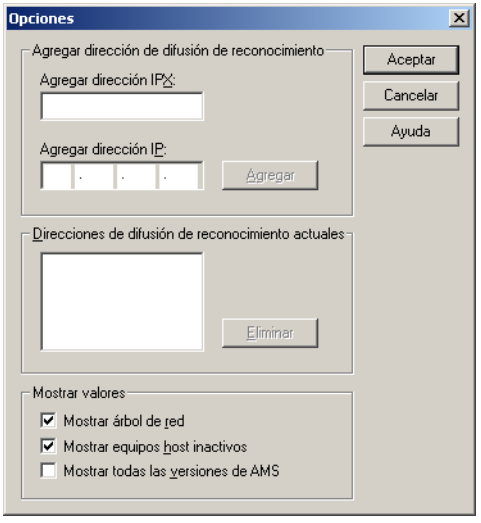
En una red de gran tamaño, se puede acelerar y simplificar la configuración de AMS^2 mediante la delimitación de la búsqueda de equipos con AMS^2 a un determinado segmento de la red.

Esta función es especialmente útil si se administra una red grande con muchos servidores diferentes y se desea reducir la búsqueda a una sección específica de la red o a una máscara de subred en concreto. El proceso es más rápido cuando se limita la búsqueda y las alertas se limitan a un segmento determinado de la red.

Se puede conseguir una respuesta más rápida en una red de gran tamaño si se limitan los segmentos de la red. Se puede usar esta opción con protocolos de red IPX o TCP/IP. Se puede especificar si AMS^2 debe reconocer sólo los clientes de un segmento o máscara de subred determinados.

Para acelerar la configuración de alerta

1. En la consola de Symantec System Center, haga clic con el botón derecho en el grupo de servidores y, a continuación, haga clic en **Todas las tareas** > **AMS** > **Configurar**.
2. Haga clic en **Opciones**.



3 En el cuadro de diálogo Opciones, realice una de las acciones siguientes:

- Si usa una red IPX, introduzca en el cuadro Agregar dirección IPX la dirección de difusión de la red IPX en la que desee buscar equipos con AMS^2.
- Si utiliza una red TCP/IP, escriba en el cuadro Agregar dirección IP la dirección de difusión de la red TCP/IP en la que desee buscar equipos con AMS^2.

  Esto es, los tres primeros segmentos de la dirección IP del equipo seguidos de un segmento de inclusión general. Por ejemplo, si introduce 192.168.0.255 como dirección de difusión de la búsqueda, las 256 computadoras con AMS^2 de la subred recibirán la difusión. Por lo tanto, si la dirección IP del equipo con AMS^2 que está buscando es 192.168.0.50, la encontrará.

4 Haga clic en **Agregar** para agregar esta dirección de red a la lista Direcciones de difusión del reconocimiento actual.

Sólo se realizará la búsqueda de nuevas computadoras con AMS^2 en las redes de difusión que se detallan aquí. Si no ha especificado ninguna red de difusión, se realizará la búsqueda sobre toda la red cada vez que inicie un reconocimiento.

5 Para suprimir una dirección de red que ya no sea necesaria de la lista Direcciones de difusión del reconocimiento actual, seleccione la dirección y haga clic en **Eliminar**.

Cuando se suprime una dirección de red de esta lista no se inhabilita la sección correspondiente de la red. Cuando se suprime una dirección de red sólo se evita que AMS^2 busque computadoras con AMS^2 en esa sección de la red.

6 Haga clic en **OK** para guardar la lista y volver al cuadro de diálogo Alert Actions.

Configuración del análisis en tiempo real del correo electrónico

Mediante el análisis en tiempo real se pueden analizar archivos adjuntos de correo electrónico de las siguiente aplicaciones:

- Lotus Notes 4.5x y 4.6 y 5.0
- Microsoft Exchange 5.0 y 5.5
- Microsoft Outlook 97, 98, 2000 y 2002 (sólo MAPI, no Internet)

Si se ha activado la protección en tiempo real para el correo electrónico, los datos adjuntos se descargarán de forma inmediata en el equipo que ejecute el cliente de correo electrónico y se analizarán cuando el usuario abra el correspondiente mensaje. Esta operación ralentiza el funcionamiento del cliente de correo electrónico cuando la conexión es lenta y se reciben datos adjuntos de gran tamaño. En el caso de usuarios que reciban con regularidad datos adjuntos extensos, tal vez prefiera desactivar esta función.

Permiso para que los usuarios interrumpan, pospongan o detengan análisis

Para permitir a los usuarios interrumpir o posponer análisis

En el cuadro de diálogo Opciones de pausa del análisis, realice una de las siguientes acciones:

- Limite el número de minutos que el análisis puede estar interrumpido: marque la casilla **Limitar el tiempo que el análisis puede estar interrumpido** y escriba el número de minutos.
- Limite el número de veces que se puede interrumpir un análisis: escriba un número en el cuadro **Número de veces que se puede posponer**.
- Haga que aparezca el botón Posponer 3 horas: marque la casilla **Activar el botón para posponer durante 3 horas**.

  De forma predeterminada, el usuario puede interrumpir un análisis durante una hora. Deberá activar esta opción para permitir que el usuario pueda interrumpir un análisis durante tres horas.

La mejor opción: usar LiveUpdate continuo en equipos de 64 bits

Para garantizar que todos los equipos de 64 bits administrados cuenten con las últimas definiciones de virus, puede usar LiveUpdate continuo con objeto de obligar a todos los equipos a comprobar la existencia de actualizaciones transcurrido un intervalo de tiempo concreto. Si hay más de un equipo de 64 bits en la red y utiliza la consola Symantec System Center, podrá agrupar estos equipos dentro de un grupo de clientes o de servidores y administrar las definiciones de virus desde la consola. Si no usa la consola, puede optar por activar esta función y definir el intervalo correspondiente en el equipo cliente.

Capítulo 3

Actualizaciones de la Guía del cliente de Symantec AntiVirus Corporate Edition

Acerca de las actualizaciones de la Guía del cliente de Symantec AntiVirus Corporate Edition

El propósito de este capítulo es explicar los cambios aplicados a la *Guía del cliente de Symantec AntiVirus Corporate Edition* entre las versiones 8.0 y 8.1 de Symantec AntiVirus Corporate Edition.

Realización de análisis manuales

Los análisis manuales se pueden llevar a cabo en cualquier momento, tanto en un único archivo como en un disquete o en todo el sistema.

Inicio de análisis manuales

Los análisis los puede iniciar desde Mi PC, desde la ventana del Explorador de Windows o desde la ventana principal de Symantec AntiVirus Corporate Edition.

Para iniciar un análisis manual desde Windows

- Desde Mi PC o desde el Explorador de Windows, haga clic con el botón derecho en un archivo, carpeta o unidad y, a continuación, haga clic en **Analizar en busca de virus**.

Nota: Esta función no es compatible con los sistemas operativos de 64 bits.

Índice

M

P

R

S

T

W