Guía del administrador de Symantec AntiVirus™ Corporate Edition

Guía del administrador de Symantec AntiVirus™ Corporate Edition

El software descrito en la presente guía está sujeto a un acuerdo de licencia y sólo podrá ser utilizado según los términos de ese acuerdo.

Nota de copyright

Documentación, versión 1a.

Marcas comerciales

Impreso en Irlanda.

10 9 8 7 6 5 4 3 2 1

Contenido

Sección 1 Administración de Symantec AntiVirus Corporate Edition

Capítulo 1 Administración de Symantec AntiVirus Corporate Edition

Acerca de la administración de Symantec AntiVirus Corporate Edition 12
Administración mediante Symantec System Center 12
Uso de las vistas de la consola 13
Almacenamiento de los valores de la consola 15
Descripción de los iconos de Symantec System Center 15
Reconocimiento de equipos y actualización de la consola 17
Acerca de los servidores y clientes 30
Acerca de los servidores primarios 30
Acerca de los servidores secundarios 31
Acerca de los servidores principales 31
Acerca de los grupos de servidores y de clientes 32
Administración con grupos de servidores o con grupos de clientes 32
Ejemplo de grupos de clientes y servidores 35
Administración mediante grupos de servidores 35
Creación de grupos de servidores 35
Bloqueo y desbloqueo de grupos de servidores 36
Utilización de contraseñas de grupos de servidores 37
Cambio de nombre de los grupos de servidores 39
Selección de un servidor primario para un grupo de servidores 40
Cambio de servidores primarios y principales 41
Traslado de un servidor a otro grupo de servidores 42
Visualización de los grupos de servidores 42
Supresión de grupos de servidores 43

Administración mediante grupos de clientes 44
Creación de un nuevo grupo de clientes 44
Adición de clientes a un grupo de clientes 45
Configuración de opciones y ejecución de tareas en el nivel de grupo de clientes 45
Búsqueda de opciones de grupos de clientes 46
Desplazamiento de clientes entre grupos de clientes 46
Visualización de grupos de clientes 46
Filtrado de la vista de grupos de clientes 47
Cambio de nombre de los grupos de clientes 49
Supresión de grupos de clientes 49
Conversión de cliente no administrado en cliente administrado (y viceversa) 50

Capítulo 2 Configuración de Alert Management System

Acerca de Alert Management System 54
Funcionamiento de Alert Management System 55
Configuración de las acciones de alerta 56
Tareas de configuración de alertas 56
Configuración de los mensajes de las acciones de alerta 57
Cómo acelerar la configuración de las alertas con un reconocimiento avanzado 59
Configuración de la acción de alerta de aparición de un cuadro de mensaje 61
Configuración de la acción de alerta de envío de un mensaje de difusión general 62
Configuración de la acción de alerta de ejecución de un programa 62
Configuración de la acción de alerta de carga de un NLM 63
Configuración de la acción de alerta de envío de un mensaje de correo por Internet 64
Configuración de la acción de alerta de envío de un mensaje a buscapersonas 65
Configuración de la acción de alerta de envío de capturas SNMP 69
Configuración de la acción de alerta de inclusión en el registro de sucesos 72
Utilización de las alertas configuradas 72
Cómo probar las acciones de alerta configuradas 73
Eliminación de una acción de alerta 73
Cómo exportar acciones de alerta a otros equipos 73

Utilización del registro de alertas deAlert Management System 75
Visualización de información más detallada acerca de las alertas 77
Cómo filtrar la lista del registro de alertas 79
Cómo enviar alertas desde los clientes no administrados 80

Sección 2 Configuración de Symantec AntiVirus Corporate Edition

Capítulo 3 Análisis de virus

Acerca de los análisis en Symantec AntiVirus Corporate Edition 84
Descripción de los análisis en tiempo real 84
Descripción de los análisis planificados 85
Descripción de los análisis manuales 85
Selección de equipos para analizar 86
Configuración de análisis en tiempo real 89
Configuración de la protección en tiempo real para archivos. 89
Configuración del análisis en tiempo real del correo electrónico 94
Determinación de exclusiones 95
Definición y restablecimiento de las opciones de protección en tiempo real 96
Bloqueo y desbloqueo de opciones de protección en tiempo real 97
Configuración de análisis manuales 98
Configuración de análisis planificados 100
Planificación de análisis para grupos de servidores o servidores individuales de Symantec AntiVirus Corporate Edition 100
Planificación de análisis para clientes de Symantec AntiVirus Corporate Edition 103
Establecimiento de opciones para análisis planificados no realizados 105
Modificación, supresión o desactivación de análisis planificados 106
Ejecución manual de un análisis planificado 107
Gestión de clientes de Symantec AntiVirus Corporate Edition que se conectan de forma intermitente 108

Configuración de opciones de análisis 110
Asignación de acciones primarias y secundarias para los virus detectados 110
Control de las posibilidades del usuario 111
Exclusión de archivos en los análisis 120
Selección de tipos y extensiones de archivos para el análisis 122
Definición de opciones para el análisis de archivos comprimidos 127
Configuración de las opciones de HSM 128
Omisión de la protección en tiempo real de archivos de los que se esté realizando copia de respaldo 132
Establecimiento del uso de la CPU 132

Capítulo 4 Actualización de las definiciones de virus

Acerca de los archivos de definiciones de virus 134
Métodos de actualización de los archivos de definiciones de virus 135
La mejor opción: utilización del método de transporte de definiciones de virus combinado con LiveUpdate 136
Actualización de los archivos de definiciones de virus en servidores de Symantec AntiVirus Corporate Edition 137
Actualización y configuración de servidores de Symantec AntiVirus Corporate Edition mediante el método de transporte de definiciones de virus 137
Actualización de servidores mediante LiveUpdate 143
Actualización de servidores mediante Intelligent Updater 146
Actualización de servidores mediante el sondeo de Cuarentena central 147
Reducción del tráfico en la red y gestión de actualizaciones no realizadas 148
Actualización de los archivos de definiciones de virus en clientes de Symantec AntiVirus Corporate Edition 151
Configuración de clientes administrados para que utilicen un servidor de LiveUpdate interno 153
Activación y configuración de LiveUpdate continuo para clientes administrados 154
Configuración de las políticas de uso de LiveUpdate 156
Control de los archivos de definiciones de virus 157
Comprobación del número de versión de los archivos de definiciones de virus 158
Visualización de la lista de virus 158
Uso de versiones anteriores de los archivos de definiciones de virus 158
Prueba de los archivos de definiciones de virus 159
Situaciones posibles de actualización 160

Capítulo 5 Respuesta ainfecciones víricas

Acerca de la respuesta a infecciones víricas 162
Preparación para responder a una infección vírica 162
Creación de un plan de respuesta a infecciones víricas 163
Definición de acciones de Symantec AntiVirus Corporate Edition para gestionar los archivos sospechosos 165
Depuración automática de archivos sospechosos del área de cuarentena local 166
Tratamiento de una infección vírica en la red 167
Uso de mensajes y alertas de virus 167
Ejecución de barridos de virus 168
Seguimiento de alertas de virus mediante registros de sucesos e historias 169
Seguimiento de envíos a Symantec Security Response con la consola de Cuarentena central 169

Capítulo 6 Administración de clientes de uso móvil

Acerca de los clientes de uso móvil 172
Componentes de los clientes de uso móvil 173
Funcionamiento del soporte para clientes de uso móvil 174
Implantación del soporte para clientes de uso móvil 175
Análisis de la red de Symantec AntiVirus Corporate Edition y elaboración de un mapa 175
Identificación de los servidores de cada nivel jerárquico 176
Creación de una lista de servidores de Symantec AntiVirus Corporate Edition del nivel 0 177
Creación de una lista jerárquica de servidores de Symantec AntiVirus Corporate Edition 177
Configuración del soporte para clientes de uso móvil en los clientes 178
Configuración del soporte para clientes de uso móvil en servidores de uso móvil 181
Configuración de las opciones de clientes de uso móvil 182
Opciones de la línea de comandos 184
Valores del registro 186

Capítulo 7 Trabajo con historias y registros de sucesos

Acerca de las historias y los registros de sucesos 190
Ordenación y filtrado de los datos de las historias y los registros de sucesos 191
Visualización de historias 193
Utilización de las historias de virus 194
Utilización de las historias de análisis 197
Descripción de los iconos de la ventana Registro de sucesos 199
Supresión de historias y registros de sucesos 200

Índice

Soluciones de Servicio y Soporte

Sección 1

Administración de Symantec AntiVirus Corporate Edition

- Administración de Symantec AntiVirus Corporate Edition
- Configuración de Alert Management System

Capítulo 1

Administración de Symantec AntiVirus Corporate Edition

En este capítulo se tratan los temas siguientes:

- Acerca de la administración de Symantec AntiVirus Corporate Edition
- Administración mediante Symantec System Center
- Acerca de los servidores y clientes
- Acerca de los grupos de servidores y de clientes
- Administración mediante grupos de servidores
- Administración mediante grupos de clientes
- Conversión de cliente no administrado en cliente administrado (y viceversa)

Acerca de la administración de Symantec AntiVirus Corporate Edition

Mediante Symantec System Center, es posible realizar operaciones de administración de Symantec AntiVirus Corporate Edition, tales como instalar la protección antivirus en estaciones de trabajo y servidores de red, actualizar definiciones de virus y administrar los servidores y clientes de Symantec AntiVirus Corporate Edition. Además de Symantec System Center, se pueden utilizar los archivos de configuración (Grc.dat) para configurar los clientes de Symantec AntiVirus Corporate Edition. Haga uso de los archivos de configuración en caso de que desee emplear una herramienta de otro fabricante para realizar la configuración de la red interna de forma remota.

Consulte la *Guía de referencia de Symantec AntiVirus Corporate Edition* si desea obtener información adicional sobre el uso de los archivos de configuración.

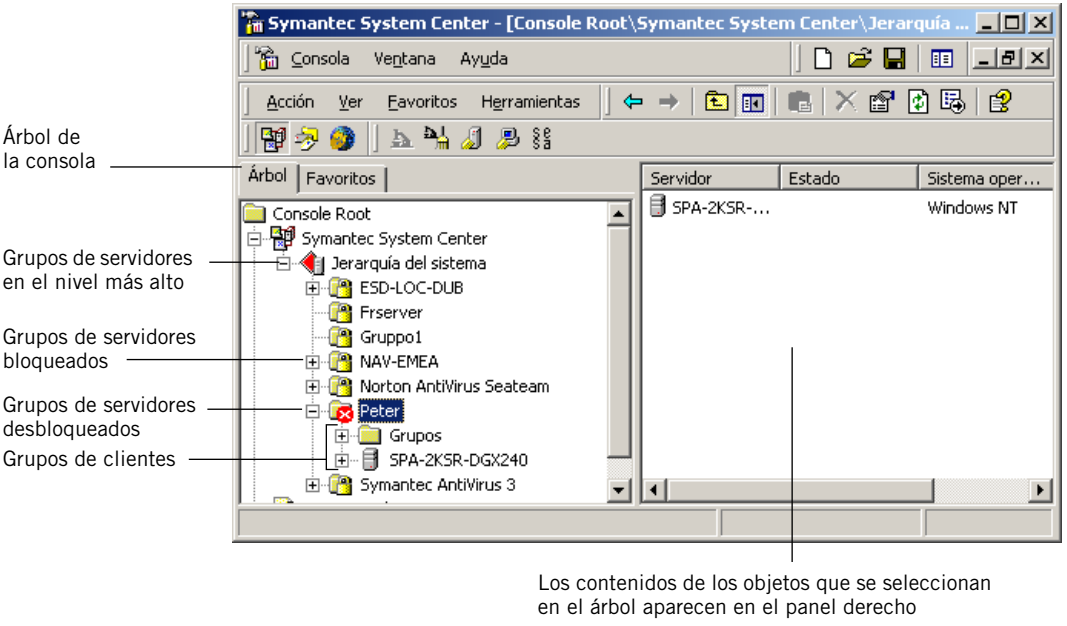
Administración mediante Symantec System Center

Cuando se ejecuta Symantec System Center, se muestra una jerarquía de sistema con los grupos de servidores, los grupos de clientes y los servidores en forma de árbol que se puede expandir o contraer. La jerarquía del sistema es el nivel más alto y contiene todos los grupos de servidores y de clientes.

Nota: La jerarquía del sistema no contiene ningún elemento hasta que no se instala al menos un servidor de Symantec AntiVirus Corporate Edition.

Para iniciar Symantec System Center

- En la barra de tareas de Windows, haga clic en **Inicio** > **Programas** > **Consola de Symantec System Center** > **Consola de Symantec System Center**.



Uso de las vistas de la consola

Con cada módulo integrable de administración se añade una nueva vista de producto a Symantec System Center. Por ejemplo, cuando se instala el módulo integrable de administración de Symantec AntiVirus Corporate Edition, se agrega la vista Symantec AntiVirus, que incluye campos relacionados con Symantec AntiVirus Corporate Edition, como Último análisis y Definiciones.

Las columnas que aparecen en el panel derecho cambian en función de la vista seleccionada. Cuando se selecciona Jerarquía del sistema, la vista predeterminada de la consola muestra las siguientes columnas de datos:

- Nombre
- Estado
- Servidor primario
- Estado de validez

La Tabla 1-1 recoge las columnas de datos de la vista Symantec AntiVirus.

Tabla 1-1 Columnas de datos de la vista Symantec AntiVirus

Objeto seleccionado en el panel de la izquierda	Columnas de datos que aparecen en el panel de la derecha
Icono de Jerarquía del sistema	■ Grupo de servidores ■ Estado ■ Definiciones compartidas ■ Definiciones más recientes ■ Estado de actualizaciones de servidor
Icono de Grupo de servidores	■ Servidor ■ Tipo ■ Estado ■ Último análisis ■ Definiciones ■ Versiones ■ Motor de análisis ■ Dirección ■ Estado de actualizaciones de cliente
Icono de Grupos (para grupos de clientes)	■ Nombre del grupo ■ Fecha de modificación de la configuración ■ Número de clientes
Icono de Grupo de clientes o icono de Servidor	■ Cliente ■ Usuario ■ Estado ■ Último análisis ■ Definiciones ■ Versión ■ Motor de análisis ■ Dirección ■ Grupo ■ Servidor

Modificación de las vistas de la consola

A menos que se cambie la vista, la consola de Symantec System Center muestra la vista predeterminada de la consola. La existencia de otras vistas depende de los productos de Symantec AntiVirus Corporate Edition que se hayan instalado.

Para cambiar las vistas de la consola

1. En el panel izquierdo de la consola de Symantec System Center, expanda **Jerarquía del sistema**.
2. Seleccione una vista en la lista que aparece en la parte inferior del menú Ver.

Almacenamiento de los valores de la consola

Cuando se cierra la consola, el programa pregunta si se debe guardar la configuración de la consola de Symantec System Center.

Para guardar los valores de la consola

- Realice una de las acciones siguientes:
  - Haga clic en **Sí** si desea mantener la misma vista de la consola la próxima vez que ejecute Symantec System Center.
  - Haga clic en **No** si desea volver a la última vista guardada la próxima vez que ejecute Symantec System Center.

    Si selecciona No, se pueden perder los cambios de los valores. Por ejemplo, si cambia la configuración de un servidor de cuarentena asociado y después selecciona **No** al salir de la consola, no se guardarán los cambios efectuados en el servidor de cuarentena.

Nota: Si el sistema dispone de una versión más reciente de MMC, es posible que tenga que actualizar a la nueva versión con el fin de guardar los cambios antes de salir de la consola de Symantec System Center.

Descripción de los iconos de Symantec System Center

Symantec System Center utiliza iconos para representar los diferentes estados de los equipos que tienen instalados los productos de Symantec administrados. Por ejemplo, si el icono de un grupo de servidores muestra un candado, dicho grupo de servidores debe desbloquearse mediante una contraseña para poder configurarlo o ejecutar análisis en los equipos que lo integran. La Tabla 1-2 recoge los iconos de Symantec System Center.

Tabla 1-2 Iconos de Symantec System Center

Icono	Descripción del icono
	Objeto del nivel más alto que representa la jerarquía del sistema y contiene todos los grupos de servidores.
	Grupo de servidores o de clientes desbloqueado. Compare este icono con el icono asociado al grupo de servidores bloqueado. Por razones de seguridad, todos los servidores están bloqueados de forma predeterminada cuando se inicia Symantec System Center.
	Grupo de servidores bloqueado. Se debe introducir una contraseña para poder ver los equipos de estos grupos de servidores, configurarlos o ejecutar análisis y actualizaciones.
	Existe algún conflicto que se debe resolver en este grupo de servidores. Por ejemplo, puede que no haya ningún servidor primario asignado al grupo de servidores o que uno de los servidores esté infectado por un virus.
	Servidor de Symantec AntiVirus Corporate Edition. Puede ser un servidor de Windows NT, de Windows 2000 o de NetWare. Compare este icono con el siguiente, que corresponde al servidor primario del grupo de servidores.
	Servidor primario de Symantec AntiVirus Corporate Edition. Puede ser un servidor de Windows NT, de Windows 2000 o de NetWare.
	Servidor de Symantec AntiVirus Corporate Edition no disponible. Este icono aparece cuando se corta la comunicación entre el servidor de Symantec AntiVirus Corporate Edition y la consola de Symantec System Center. El error en la comunicación puede deberse a diferentes causas. Por ejemplo, puede que el sistema del servidor no se esté ejecutando, que se haya desinstalado el software de Symantec o que exista un fallo en la red entre la consola y el sistema.
	Se ha detectado un virus en el equipo en el que se está ejecutando el servidor de Symantec AntiVirus Corporate Edition.
	Cliente de Symantec AntiVirus Corporate Edition en un equipo con Windows 95/98/ME o Windows NT/2000/XP Home Edition o Professional. Los clientes de Windows 95 ejecutan la versión anterior de Symantec AntiVirus. Cuando se selecciona este equipo, se ven únicamente las opciones correspondientes a él.

Tabla 1-2 Iconos de Symantec System Center

Icono	Descripción del icono
	Equipo con Windows 3.1. Los equipos con Windows 3.1 utilizan el cliente de la versión anterior de Symantec AntiVirus. Cuando se lleve a cabo un barrido de virus en un grupo de servidores o en un servidor que contenga esos clientes, los clientes se incluirán en el barrido. Desde la consola de Symantec System Center, es posible configurar estos equipos sólo en el nivel de grupo de servidores.
	Se ha detectado un virus en el equipo en el que se está ejecutando el cliente de Symantec AntiVirus Corporate Edition.
	Existe algún conflicto que se debe resolver en este cliente. Por ejemplo, puede que los archivos de definiciones de virus no estén al día o que el grupo de clientes al que pertenece el cliente ya no sea válido. En el campo de estado de la consola de Symantec System Center se indica cuál es realmente el problema.

Reconocimiento de equipos y actualización de la consola

Durante la ejecución inicial de la consola de Symantec System Center, ésta establece una comunicación ping con la red para localizar todos los equipos disponibles en los que se ejecuten servidores de Symantec AntiVirus Corporate Edition. A medida que dichos servidores responden, se van añadiendo a la consola. Las estaciones de trabajo conectadas que tengan instalado un producto cliente administrado de Symantec también se añadirán cuando su *servidor principal* se seleccione en el árbol de la consola.

Si se inicia algún servidor que esté ejecutando algún producto administrable de Symantec mientras Symantec System Center ya se esté ejecutando, puede que sea necesario localizar dicho servidor mediante la función de búsqueda o el servicio de reconocimiento para que se muestre en la vista de grupos de servidores.

Uso del servicio de reconocimiento

La consola de Symantec System Center ejecuta un único servicio de Windows NT, el servicio de reconocimiento de Symantec System Center (Nsctop.exe). Este servicio es el encargado de reconocer los equipos en los que se ejecuta el servidor de Symantec AntiVirus Corporate Edition que aparecen en la consola de Symantec System Center. Asimismo, el servicio de reconocimiento llena de objetos la consola de Symantec System Center.

Se puede elegir uno de los siguientes tipos de reconocimiento:

- Cargar sólo desde antememoria
- Reconocimiento local
- Reconocimiento intensivo

Vea "Descripción del tipo de reconocimiento Cargar sólo desde antememoria" en la página 20.

Vea "Descripción del reconocimiento local" en la página 20.

Vea "Descripción del reconocimiento intenso" en la página 21.

Cómo funciona el reconocimiento de los equipos de la red

Para reconocer los equipos de la red, un equipo en el que se ejecute un servidor de Symantec AntiVirus Corporate Edition envía un paquete ping a otro equipo que tenga instalado un cliente de Symantec AntiVirus Corporate Edition. El programa ping comprueba que el equipo remoto existe y que puede aceptar solicitudes. Cuando el servicio de reconocimiento mediante ping (Intel PDS) detecta un ping, responde a él con un paquete pong. Los paquetes ping y pong tienen un tamaño aproximado de 1 KB. Un reconocimiento mediante ping y pong llevado a cabo con éxito permite asegurar que el equipo funciona correctamente.

El paquete pong también proporciona información valiosa, como:

- La fecha de los archivos de definiciones de virus del equipo
- La fecha en la que el equipo sufrió la última infección

Se envían paquetes ping tanto a través de IP como a través de IPX al equipo remoto en el que se ejecute el servidor de Symantec AntiVirus Corporate Edition para determinar qué tipo de protocolo usa la máquina remota.

También se envían paquetes ping compatibles con Norton AntiVirus Corporate Edition y LANDesk Virus Protect, las versiones anteriores de Symantec AntiVirus Corporate Edition.

Los datos del equipo en el que se esté ejecutando el cliente de Symantec AntiVirus Corporate Edition se almacenan en la máquina que tenga instalado el servidor de Symantec AntiVirus Corporate Edition y que sea el servidor principal del cliente.

La consola de Symantec System Center lee el registro de cada servidor principal para obtener los datos que se muestran en ella.

Una vez que este proceso finaliza, se ejecuta el reconocimiento normal.

Reconocimiento normal

Tras efectuar todos los tipos de reconocimiento, se ejecuta un reconocimiento normal. En un reconocimiento normal, la consola de Symantec System Center difunde mensajes a todos los servidores que se encuentren en grupos de servidores desbloqueados. Este reconocimiento adicional solicita al servidor primario del grupo de servidores la lista de servidores secundarios en la antememoria de direcciones.

La antememoria de direcciones de la consola de Symantec System Center guarda información de todos los servidores que en algún momento le hayan enviado informes. La antememoria de direcciones del servidor primario contiene información de cada servidor del grupo de servidores, así como los nombres de todos los servidores secundarios y sus direcciones IP.

La consola de Symantec System Center compara su propia antememoria de direcciones con la enviada por el servidor primario. Si se detecta alguna diferencia entre ellas, la consola establece una comunicación ping con el servidor asociado. Cuando los datos pong son devueltos, se agregan a todos los demás servidores de la lista.

De este modo, el reconocimiento normal puede identificar cada servidor del grupo de servidores e intentar solucionar conflictos de información entre servidores principales.

Utilización de WINS en el servicio de reconocimiento

El servicio de reconocimiento precisa utilizar la resolución de nombres WINS (Windows Internet Naming Service). Si intenta efectuar un reconocimiento en un entorno que no disponga de WINS, como una red original de Windows 2000, deberá localizar antes al menos un equipo de la red interna que tenga instalado el servidor de Symantec AntiVirus Corporate Edition. Para buscar el equipo, puede utilizar la función Buscar equipo o la herramienta Importer.

Vea "Uso de la función Buscar equipo" en la página 26.

Consulte la *Guía de referencia de Symantec AntiVirus Corporate Edition* si desea obtener información sobre la herramienta Importer.

Búsqueda de equipos con NetWare

Es posible que el servicio de reconocimiento no encuentre los equipos con NetWare que sólo dispongan del protocolo IP. Para localizar los equipos que no es posible detectar mediante el servicio de reconocimiento, se puede utilizar la función de búsqueda de equipos.

Vea "Uso de la función Buscar equipo" en la página 26.

Descripción de la configuración del ciclo de reconocimiento

Se puede configurar el intervalo de tiempo de un ciclo de reconocimiento. En función de cómo se configure el servicio de reconocimiento, se puede fijar el intervalo desde 1 a 1.440 minutos entre intentos de reconocimiento. De forma predeterminada, el intervalo es de 480 minutos (cada 8 horas).

No será posible ejecutar un nuevo proceso de reconocimiento mientras aún esté ejecutándose uno anterior. Por ejemplo, si se configura el reconocimiento para que se ejecute una vez por minuto y el primer proceso dura 20 minutos, no se podrán completar con éxito los 19 intentos de reconocimiento restantes.

Cómo cambiar el intervalo del ciclo de reconocimiento

Aunque se puede cambiar el intervalo del ciclo de reconocimiento, se debe tener en cuenta que, si se aumenta el intervalo, puede que la consola de Symantec System Center muestre información obsoleta.

Para cambiar el intervalo del ciclo de reconocimiento

1. Haga clic en **Servicio de reconocimiento** en el menú Herramientas de Symantec System Center.
2. Cambie el valor **Intervalo en minutos** como sea necesario.

Descripción del tipo de reconocimiento Cargar sólo desde antememoria

El reconocimiento Cargar sólo desde antememoria constituye el tipo de reconocimiento más básico. Su finalidad es actualizar todos aquellos servidores cuya información relacionada se encuentre en la antememoria de direcciones de Symantec System Center. Se envía a cada servidor una serie de paquetes ping para comprobar si responde y actualizar así la información de la consola.

Tras la operación Cargar sólo desde antememoria, se ejecuta el reconocimiento normal.

Vea "Reconocimiento normal" en la página 19.

El reconocimiento Cargar sólo desde antememoria es el método de reconocimiento predeterminado y reduce el tráfico de red no deseado cuando se ejecuta Symantec System Center. Comprobará que, en la mayoría de los casos, este tipo de reconocimiento basta para encontrar todos los servidores que es necesario agregar a la consola de Symantec System Center.

Descripción del reconocimiento local

Durante un reconocimiento local, se difunde un paquete ping a través de la subred local del equipo en el que se encuentre la consola de Symantec System Center. Los servicios Intel PDS instalados en los servidores de la subred local responden con un paquete pong.

Un reconocimiento local genera menos tráfico, pero su utilidad se limita al ámbito de una subred local. Los reconocimientos locales funcionan especialmente bien en subredes pequeñas. En subredes muy grandes se consiguen mejores resultados con el reconocimiento intenso.

Tras un reconocimiento local, se ejecutan los siguientes tipos de reconocimiento:

- Cargar sólo desde antememoria
- Reconocimiento normal

Vea "Reconocimiento normal" en la página 19.

Descripción del reconocimiento intenso

El reconocimiento intenso se centra en Mis sitios de red en el caso de equipos locales con Windows 2000 y en Entorno de red si se trata de equipos locales con Windows NT, e intenta comunicarse con todos los equipos que encuentra en una dirección de red. Una vez que obtiene una dirección de la red, intenta enviar solicitudes ping. Se puede elegir si el reconocimiento intenso debe explorar las ramificaciones del árbol de red de NetWare, de Microsoft o ambas.

Desde la consola de Symantec System Center se puede seleccionar cualquier nodo que esté en la raíz de la consola y seleccionar Servicio de reconocimiento en el menú Herramientas para ejecutar un nuevo reconocimiento de los servidores.

Tras un reconocimiento intenso, se ejecutan los siguientes tipos de reconocimiento:

- Reconocimiento local
- Cargar sólo desde antememoria
- Reconocimiento normal

Vea "Reconocimiento normal" en la página 19.

Nota: Existen varios factores que limitan la posibilidad de localizar equipos mediante el reconocimiento intenso: la disponibilidad de un servidor WINS, la configuración de la subred y del enrutador de la red, la configuración DNS y la configuración del grupo de trabajo y del dominio de Microsoft. En general, la búsqueda por el intervalo de direcciones IP no se ve afectada por estos factores, razón por la cual es conveniente utilizar el reconocimiento de IP.

Descripción del reconocimiento de IP

El reconocimiento de IP permite localizar equipos en un intervalo de direcciones IP o en el intervalo IP de una subred.

Es posible que sólo necesite utilizar la función de reconocimiento de IP periódicamente. Esta función puede emplearse para localizar los equipos de una red.

Una vez que los equipos se encuentren en la antememoria de direcciones, podrá aplicar el método Cargar sólo desde antememoria.

Ejecución del servicio de reconocimiento

Todos los tipos de reconocimiento se ejecutan de forma manual desde la consola de Symantec System Center directamente.

Nota: El servicio de reconocimiento utiliza el servicio WINS (Windows Internet Naming Service) cuando se buscan nuevos equipos que estén ejecutando Symantec AntiVirus Corporate Edition. Si está intentando reconocer nuevos equipos en un entorno donde WINS no esté disponible, como una red original de Windows 2000, es conveniente utilizar antes la función Buscar equipo o la herramienta Importer. Vea "Uso de la función Buscar equipo" en la página 26. Consulte la *Guía de referencia de Symantec AntiVirus Corporate Edition* si desea obtener información sobre la herramienta Importer.

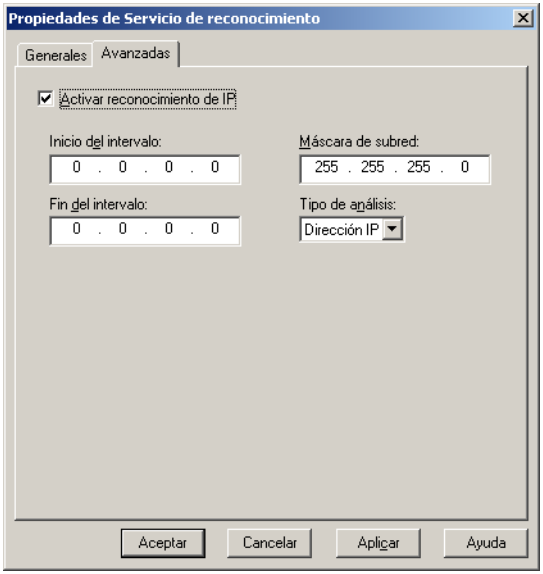
Ejecución del servicio de reconocimiento

Se puede ejecutar el servicio de reconocimiento para localizar servidores incluyendo o no direcciones y subredes IP.

Para ejecutar el reconocimiento de IP

1. En el panel izquierdo de la consola de Symantec System Center, seleccione cualquier nodo situado por debajo de la raíz de la consola.
2. En el menú Herramientas, haga clic en **Servicio de reconocimiento**.

3 En la ficha Avanzadas de la ventana de propiedades del servicio de reconocimiento, haga clic en **Activar reconocimiento de IP**.



Cuando la casilla se encuentre seleccionada, cada vez que ejecute un reconocimiento intenso se iniciará una sesión de reconocimiento de IP. Deje sin marcar esta casilla si desea ejecutar el reconocimiento intenso sin efectuar el reconocimiento de IP.

4 En la lista Tipo de análisis, seleccione una de las siguientes opciones:

- Subred IP: la consola difunde un mensaje en cada subred.
- Dirección IP: la consola envía un paquete ping a todos los equipos del intervalo de direcciones IP.

5 Escriba las direcciones en los cuadros Inicio del intervalo y Fin del intervalo.

6 Si ha seleccionado la opción Subred IP, escriba la máscara de la subred para ajustar la búsqueda.

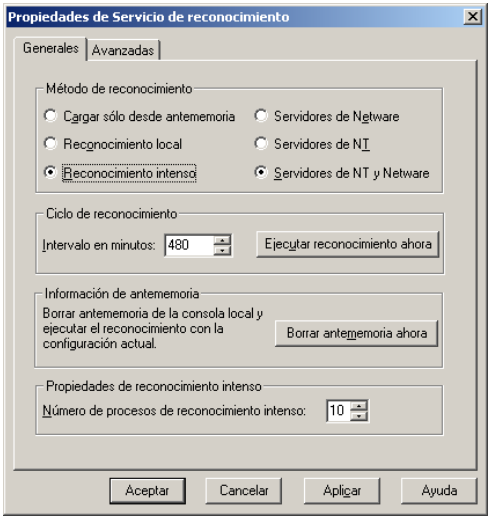
Los resultados de la búsqueda de direcciones IP aparecerán en el cuadro de lista de equipos. Los resultados de la búsqueda de subred IP aparecerán en la barra de estado de la consola de Symantec System Center.

También puede acceder al reconocimiento de IP desde el cuadro de diálogo Buscar equipo.

Vea "Uso de la función Buscar equipo" en la página 26.

Para efectuar el reconocimiento sin incluir direcciones IP

1 Haga clic en **Servicio de reconocimiento** en el menú Herramientas de la consola de Symantec System Center.



2 En la ficha Generales de la ventana de propiedades del servicio de reconocimiento, seleccione una de las opciones siguientes:

- Cargar sólo desde antememoria: éste es el método más rápido. Symantec System Center lee la lista de los servidores y los clientes almacenada en la antememoria local.

  Vea "Descripción del tipo de reconocimiento Cargar sólo desde antememoria" en la página 20.

- Reconocimiento local: envía mensajes de difusión a la subred local de la consola de Symantec System Center. Los servidores responden de inmediato con información acerca de ellos mismos y de sus clientes. En la consola aparece el grupo de servidores al que pertenece cada servidor (a menos que se filtre mediante el menú Ver). Se ejecutará asimismo el reconocimiento Cargar sólo desde antememoria.

  Vea "Descripción del reconocimiento local" en la página 20.

- Reconocimiento intenso: éste es el método más fiable. En el caso de que la red sea muy grande, el proceso puede prolongarse durante bastante tiempo. Symantec System Center envía paquetes ping sistemáticamente a cada servidor del entorno de red. Los nombres de los servidores aparecen en el área de mensajes de la consola de Symantec System Center al tiempo que se van encontrando durante el proceso de reconocimiento. En el reconocimiento intenso se realiza el mismo proceso de difusión de mensajes a través de la subred local que en el reconocimiento local. Se ejecutarán también el reconocimiento Cargar sólo desde antememoria y el reconocimiento local.

  En el caso del reconocimiento intenso, se puede limitar la búsqueda a los servidores de NetWare o a los de Windows NT, o incluir ambos en ella.

  Vea "Descripción del reconocimiento intenso" en la página 21.

3. En Ciclo de reconocimiento, seleccione la opción de Intervalo en minutos oportuna.
4. Para ejecutar un reconocimiento de inmediato, haga clic en **Ejecutar reconocimiento ahora** y después haga clic en **Cerrar**.

   Sólo se puede ejecutar un único reconocimiento al mismo tiempo.
5. En Propiedades de reconocimiento intenso, seleccione el número de procesos de reconocimiento intenso.

   Este valor afecta sólo a las sesiones de reconocimiento intenso. Cada proceso de reconocimiento es una búsqueda independiente de servidores y clientes. Para mantener la información lo más actualizada posible, se debe seleccionar un intervalo bajo de reconocimiento y un número mayor de procesos de reconocimiento.
6. Si desea suprimir toda la información acerca de los clientes y los servidores de la memoria activa y la antememoria de direcciones, así como ejecutar inmediatamente un reconocimiento basado en la configuración en uso, haga clic en **Borrar antememoria ahora**.

   Al suprimir la información de la antememoria, los grupos de servidores desbloqueados volverán a estar bloqueados a menos que se haya guardado la contraseña para el grupo de servidores.

Nota: La regeneración de la lista de servidores de una red grande puede llevar bastante tiempo.

Uso de la función Buscar equipo

Para encontrar rápidamente un servidor sin tener que expandir y explorar el árbol, se puede usar la función Buscar equipo. La búsqueda se puede realizar mediante las direcciones TCP/IP o IPX, o bien a través de los nombres de los equipos.

La función de búsqueda de equipos también es útil si se ha instalado un servidor y no es posible verlo en el árbol al expandir un grupo de servidores o un servidor. Esto puede ocurrir por las siguientes razones:

- Puede que Symantec System Center no reconozca automáticamente servidores o zonas de una red LAN separados por enrutadores.
- Los servidores pueden no estar visibles en el entorno de red. Por ejemplo, puede que los servidores de WINS (Windows Internet Naming Service) no hayan sido replicados a través de los segmentos de la red.

Los servidores de los segmentos que sólo usen el protocolo IPX también corren el riesgo de ser omitidos en el proceso de reconocimiento. En caso de que no se puedan localizar algunos servidores de la LAN, es posible encontrarlos manualmente mediante la función Buscar equipo de Symantec System Center. Una vez que se ha utilizado esta función de búsqueda para encontrar un servidor, éste se puede administrar desde la consola de Symantec System Center.

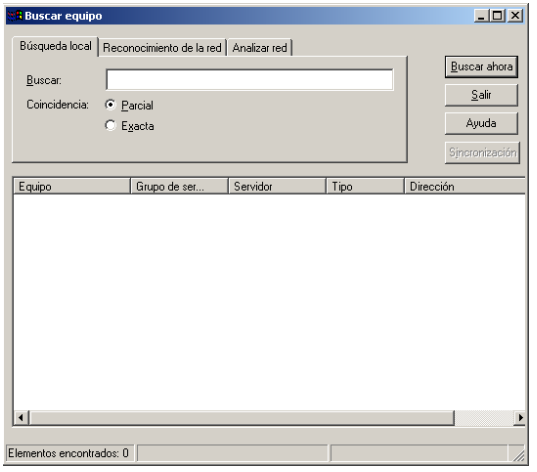
Nota: Si IPX no está instalado, puede que no se vean en la consola todos los equipos con NetWare. Aunque es posible encontrar los equipos mediante la función Buscar equipo, la instalación de IPX y TCP/IP garantiza que todos ellos sean reconocidos.

Localización de equipos mediante la búsqueda en la antememoria local

En lugar de analizar toda la red para localizar los equipos, es posible restringir la búsqueda a aquellos de los que con seguridad se sabe que están almacenados en la antememoria local.

Para localizar equipos mediante la búsqueda en la antememoria local

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



2. En la ficha Búsqueda local de la ventana Buscar equipo, escriba el nombre de red del servidor que desee buscar.
3. En el campo Coincidencia seleccione una de las siguientes opciones:
   - Exacta: busca un nombre de servidor que coincida exactamente con el especificado.
   - Parcial: busca un nombre de servidor que coincida de forma parcial con el especificado.

   Si deja vacío el cuadro Buscar y utiliza la opción Parcial en el campo Coincidencia, aparecerán todos los equipos de la antememoria local al ejecutar la búsqueda.

Localización de equipos mediante la búsqueda en red

Se puede utilizar la búsqueda en red para localizar equipos por separado en los que se ejecute el servidor de Symantec AntiVirus Corporate Edition.

Búsqueda de equipos

Se pueden localizar equipos mediante la búsqueda en red o especificando una dirección IP o un intervalo de subred.

Para localizar equipos mediante la búsqueda en red

1. Haga clic en **Buscar equipo** en el menú Herramientas de la consola de Symantec System Center.
2. En la ficha Reconocimiento de la red de la ventana Buscar equipo, especifique si desea utilizar una dirección TCP/IP, una dirección IPX o un nombre de equipo como criterio de búsqueda.
3. Escriba la dirección del servidor o el nombre del equipo.
4. Haga clic en **Buscar ahora**.

Para utilizar las direcciones IP para localizar un grupo de equipos que actúen como servidores de Symantec AntiVirus Corporate Edition

1. Haga clic en **Buscar equipo** en el menú Herramientas de la consola de Symantec System Center.
2. En la ficha Analizar red de la ventana Buscar equipo, seleccione una de las siguientes opciones:
   - Subred IP: envía un mensaje de difusión a cada subred.
   - Dirección IP: manda una señal ping a todos los equipos del intervalo de direcciones IP.
3. Escriba las direcciones en los cuadros Inicio del intervalo y Fin del intervalo.
4. Si ha seleccionado Subred IP en el paso 2, introduzca la máscara de subred para ajustar la búsqueda.
5. Haga clic en **Buscar ahora**.

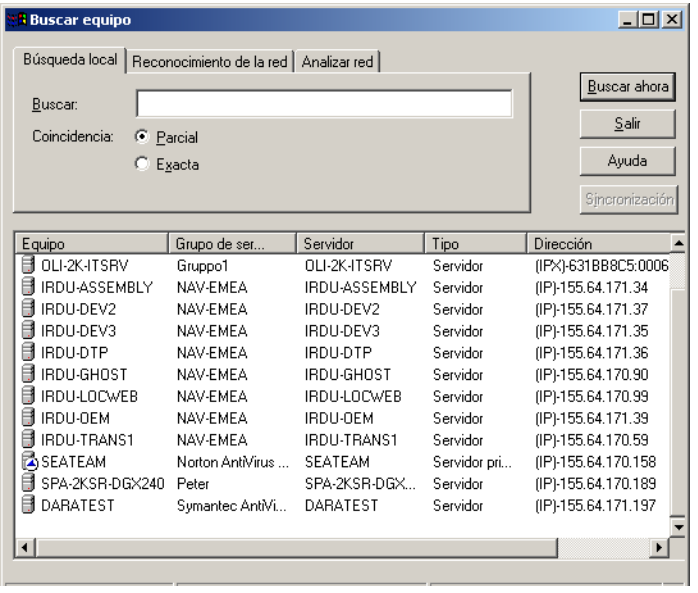
   Los resultados de la búsqueda de direcciones IP aparecerán en el cuadro de lista de equipos. Los resultados de la búsqueda de subredes IP aparecerán en la barra de estado de la consola de Symantec System Center.

Localización de los elementos encontrados en la consola de Symantec System Center

Es posible relacionar un elemento de una lista de búsqueda de equipos con su equivalente en el árbol de la consola de Symantec System Center. Para hacerlo, el grupo de servidores al que pertenece el elemento debe estar desbloqueado.

Para localizar los elementos encontrados en la consola de Symantec System Center

1 Seleccione el sistema que desee en la ventana Buscar equipo.



2 Haga clic en **Sincronización** para buscar el elemento seleccionado.

Uso de la función de actualización

Desde la consola de Symantec System Center, se puede actualizar la información en el nivel de la jerarquía de sistema, del grupo de servidores o del servidor para confirmar que la comunicación sigue activa con la lista de servidores que se muestra en cada momento. Sin embargo, la función de actualización no permite buscar servidores ni grupos de servidores que hayan sido añadidos después de iniciarse la sesión de Symantec System Center. Si la actualización determina que se ha perdido la comunicación con un servidor que antes se mostraba en el grupo de servidores, aparecerá el icono que indica que el servidor no está disponible.

Para utilizar la función de actualización

- En el panel izquierdo de la consola de Symantec System Center, haga clic con el botón derecho en la jerarquía del sistema, en el grupo de servidores desbloqueado, en el servidor o en el grupo de clientes y, a continuación, haga clic en **Actualizar**.

Acerca de los servidores y clientes

El programa cliente de Symantec AntiVirus Corporate Edition ofrece protección antivirus para equipos que estén o no conectados a una red. El cliente de Symantec AntiVirus Corporate Edition protege los equipos con Windows 98, ME, NT, 2000 y XP.

Los equipos con Windows 95, 3.1 y DOS utilizan el cliente de la versión anterior, Norton AntiVirus Corporate Edition 7.6.

El programa servidor de Symantec AntiVirus Corporate Edition administra otros equipos que dispongan de Symantec AntiVirus Corporate Edition y puede enviar actualizaciones de configuración y de archivos de definiciones de virus a los clientes de Symantec AntiVirus Corporate Edition. Además, el programa Symantec AntiVirus Corporate Edition proporciona protección antivirus a los equipos en los que se encuentra instalado. Los clientes de Symantec AntiVirus Corporate Edition son siempre administrados por un servidor.

Cuando se emplea Symantec System Center en tareas de administración, los equipos en los que se encuentre instalado el servidor de Symantec AntiVirus Corporate Edition pueden actuar como:

- Servidor primario
- Servidor secundario
- Servidor principal

Acerca de los servidores primarios

Cada grupo de servidores tiene un *servidor primario* designado por el administrador. Este servidor primario es el responsable de las funciones de configuración del grupo de servidores y, a su vez, puede ser el responsable de las actualizaciones de los archivos de definiciones de virus.

Cuando se inicia una tarea en el nivel de grupo de servidores desde la consola de Symantec System Center, esta tarea se ejecuta en el servidor primario del grupo de servidores. El servidor primario también envía la tarea al resto de servidores del grupo.

Si está utilizando Alert Management System (AMS)^2, el servidor primario se encargará además de procesar todas las notificaciones.

Los equipos que dispongan de alguno de los siguientes sistemas operativos pueden actuar como servidores primarios:

- Windows 2000 Server, Advanced Server o Professional
- Windows NT 4.0 Server o Windows NT 4.0 WorkstationNetWare 3.x, 4.x, 5.x o 6

Modificaciones en el registro

Al modificar las opciones de los servidores, se modifica directamente el registro de los servidores seleccionados. El cambio se realiza por medio del administrador de transporte, que se encarga de las comunicaciones.

El servidor primario almacena todas las opciones de los servidores en un grupo. Si se realizan cambios en un grupo, las modificaciones se guardan primero en el registro del servidor primario correspondiente a ese grupo en la clave

HKLM\Software\Intel\LANDesk\VirusProtect6\CurrentVersion\DomainData.

Posteriormente se almacenan en el resto de los servidores.

Acerca de los servidores secundarios

Los *servidores secundarios* son aquellos que no tienen asignado el estado de servidor primario y que dependen de un servidor primario. Reciben la información del servidor primario y la comparten con los clientes.

Todos los servidores de un mismo grupo son servidores secundarios hasta que se asigna a uno de ellos el estado de primario. Es necesario designar el servidor primario para poder realizar la mayor parte de las tareas en el nivel de grupo de servidores.

Nota: Los cambios que se produzcan en la configuración de los productos de Symantec no pueden administrarse en un nivel superior al de grupo de servidores.

Acerca de los servidores principales

Un servidor principal es un equipo en el que se ejecuta el servidor de Symantec AntiVirus Corporate Edition y con el que se comunica un equipo conectado en el que se ejecuta el cliente de Symantec AntiVirus Corporate Edition para obtener actualizaciones de configuración y enviar alertas. Algunos servidores pueden actuar como servidores principales y otros como servidores primarios y, como ambas funciones no se excluyen mutuamente, un servidor primario puede actuar también como servidor principal.

Acerca de los grupos de servidores y de clientes

Los miembros de un *grupo de servidores* pueden compartir una única configuración de Symantec AntiVirus Corporate Edition y es posible ejecutar en todos ellos una operación de Symantec AntiVirus Corporate Edition. La consola de Symantec System Center permite la creación de nuevos grupos de servidores y la administración de sus miembros. Los grupos de servidores no dependen de los dominios de Windows NT o 2000 ni de otros productos. Es posible incluir servidores de NetWare, de Windows NT y de Windows 2000 en un mismo grupo de servidores, lo que permite configurar simultáneamente y de forma remota estos sistemas.

Los *grupos de clientes* son agrupaciones lógicas de equipos. Aunque los grupos de clientes siempre están asociados a un grupo de servidores, se puede administrar cada grupo de clientes por separado. Cuando se configuran los grupos de clientes, se pueden establecer y administrar políticas diferentes bajo un mismo servidor principal.

- Se conoce como *clientes asignados* a los clientes de Symantec que han sido asignados a un grupo de clientes. Estos clientes reciben archivos de definiciones de virus del servidor al que se encuentran asociados físicamente, pero obtienen valores de configuración y actualizaciones en función del grupo de clientes en el que se aplican las políticas de Symantec AntiVirus Corporate Edition.
- Se denominan *clientes no asignados* los clientes de Symantec que no tienen asignado ningún grupo de clientes. Estos clientes reciben valores de configuración y actualizaciones de su servidor principal.

Administración con grupos de servidores o con grupos de clientes

Cada grupo de servidores de Symantec AntiVirus Corporate Edition admite una única configuración para todos los clientes que administra. Si se quiere utilizar una configuración adicional, es necesario agregar otro servidor al grupo de servidores. Es posible adaptar la configuración de los grupos de servidores a las necesidades del usuario siempre y cuando todos los clientes requieran las mismas opciones de configuración. Si se precisa una configuración más flexible, conviene aprovechar las ventajas que ofrece el uso de los grupos de clientes. Cuando las tareas de administración se realizan mediante grupos de clientes, no es necesario que la configuración de los clientes pertenecientes al mismo servidor sea idéntica, como sí sucede con los clientes de un mismo grupo de servidores. Además, mediante los grupos de clientes se puede reducir el número de servidores que se necesitan para administrar Symantec AntiVirus Corporate Edition. Aunque cada grupo de servidores requiere al menos un servidor por cada configuración única, puede contener, sin embargo, un número indefinido de grupos de clientes, cada uno con su propia configuración.

Nota: Si desea utilizar grupos de clientes, Symantec le recomienda que administre todos los clientes mediante grupos. Si bien es posible efectuar las tareas de administración en un entorno mixto, es decir, con algunos clientes asignados a un grupo y con otros no asignados a ninguno, esto supone mayor complejidad y puede provocar resultados inesperados.

Grupos de clientes y prioridad de configuración

Cuando se emplean grupos de clientes en la administración, los clientes asignados a un grupo obtienen la configuración de ese grupo, en lugar de recibirla del servidor principal asociado. Los cambios de configuración realizados en el nivel del servidor se ignoran y sólo se aplican a los clientes no asignados. Los cambios de configuración que se realicen en el nivel del grupo de servidores o de la jerarquía del sistema tienen prioridad sobre la configuración del grupo de clientes y anulan cualquier modificación realizada en este nivel.

La Tabla 1-3 recoge los distintos contextos que es posible seleccionar en Symantec System Center, así como lo que cada uno permite configurar.

Tabla 1-3 Prioridad de configuración

Contexto	Qué permite configurar
Jerarquía del sistema	Todos los grupos de servidores no bloqueados y los clientes que administran (independientemente del grupo de clientes al que pertenezcan)
Grupo de servidores	Todos los servidores y los clientes del grupo de servidores (independientemente del grupo de clientes al que pertenezcan)

Tabla 1-3 Prioridad de configuración

Contexto	Qué permite configurar
Servidor	El servidor y sus clientes (independientemente del grupo de clientes al que pertenezcan): ■ Barrido de virus ■ Actualización de definiciones de virus ■ Configuración del historial El servidor y sus clientes no asignados: ■ Análisis planificados y manuales ■ Actualización de definiciones de virus ■ Opciones de cuarentena ■ Opciones de protección en tiempo real para clientes y servidores ■ Opciones exclusivas para administradores de clientes ■ LiveUpdate ■ Estado de la protección en tiempo real del sistema de archivos ■ Visualización de la lista de virus ■ Supresión del estado de virus
Grupo de clientes	Clientes asignados al grupo de clientes: ■ Análisis planificados ■ Actualización de definiciones de virus ■ Opciones de cuarentena ■ Configuración del historial ■ Opciones de protección en tiempo real para clientes ■ Opciones exclusivas para administradores de clientes ■ LiveUpdate
Cliente	Sólo lectura

Ejemplo de grupos de clientes y servidores

Una empresa cuenta con departamentos de telemarketing y contabilidad y estos departamentos cuentan con personal en las oficinas de la empresa ubicadas en Boston, Nueva York y Newark. A todos los equipos de ambos departamentos se les ha asignado el mismo grupo de servidores, de modo que reciben las actualizaciones de las definiciones de virus de la misma fuente. Sin embargo, los informes de TI indican que el departamento de telemarketing es más vulnerable a los virus que el de contabilidad. Como resultado, el administrador del sistema crea los grupos de clientes Telemarketing y Contabilidad. Los clientes de Telemarketing comparten opciones de configuración que establecen de forma estricta el modo en que los usuarios pueden interactuar con su protección antivirus.

Administración mediante grupos de servidores

Pueden crearse tantos grupos de servidores como sea necesario con el fin de administrar los servidores y los clientes de forma eficiente.

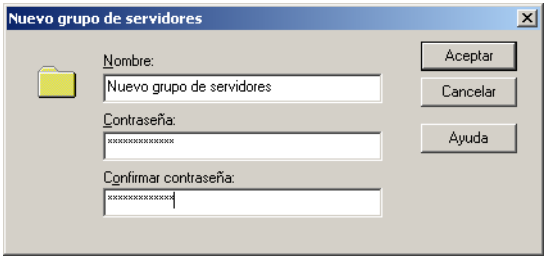
Creación de grupos de servidores

El programa de instalación agrupa todos los servidores seleccionados en un mismo grupo de servidores. Esto resulta apropiado si se quiere que todos los equipos administrados que tengan instalado Symantec AntiVirus Corporate Edition utilicen la misma configuración. Sin embargo, si desea realizar cambios de configuración globales en grupos de servidores, puede crear nuevos grupos de servidores y desplazar servidores fácilmente de un grupo a otro mediante el método de arrastrar y colocar (o cortar y pegar). Cuando se desplaza un servidor, todos los equipos clientes conectados se trasladan con él.

Por ejemplo, si cuenta con servidores que requieran niveles de protección más altos, puede incluirlos todos en el mismo grupo de servidores y establecer opciones especiales para protegerlo. (Recuerde que también es posible definir un nuevo grupo de clientes con este mismo fin. Consulte "Acerca de los grupos de servidores y de clientes" en la página 32.)

Para crear un grupo de servidores

1. En el panel izquierdo de la consola de Symantec System Center, haga clic con el botón derecho en **Jerarquía del sistema** y, a continuación, haga clic en **Nuevo** > **Grupo de servidores**.



2. En el cuadro de diálogo Nuevo grupo de servidores, escriba el nombre del grupo.
   El nombre no puede exceder los 47 caracteres.
3. Escriba una contraseña para el grupo de servidores en el cuadro de texto Contraseña.
4. Vuelva a escribir la contraseña en el cuadro Confirmar contraseña.
5. Haga clic en **Aceptar**.

Cada grupo de servidores requiere un servidor primario.

Vea "Selección de un servidor primario para un grupo de servidores" en la página 40.

Bloqueo y desbloqueo de grupos de servidores

Es posible bloquear un grupo de servidores mediante una contraseña para impedir que los administradores no autorizados efectúen cambios de configuración. Las contraseñas pueden añadirse o cambiarse en cualquier momento. La contraseña predeterminada del grupo de servidores que se creó durante la instalación es:

symantec

Las mayúsculas y minúsculas no son intercambiables en las contraseñas.

Bloqueo y desbloqueo de grupos de servidores

Los grupos de servidores se pueden bloquear y desbloquear tan a menudo como sea necesario. Para desbloquear un grupo de servidores, se debe escribir correctamente la contraseña correspondiente. Las mayúsculas y minúsculas no son intercambiables en las contraseñas. Por otra parte, es posible impedir que los grupos de servidores se bloqueen al salir de la consola.

Para bloquear un grupo de servidores

- En el panel izquierdo de la consola de Symantec System Center, haga clic con el botón derecho en el grupo de servidores que desee bloquear y seguidamente haga clic en **Bloquear grupo de servidores**.

Para desbloquear un grupo de servidores

1. En el panel izquierdo de la consola de Symantec System Center, haga clic con el botón derecho en el grupo de servidores y, a continuación, haga clic en **Desbloquear grupo de servidores**.
2. Escriba la contraseña para desbloquear el grupo de servidores.
3. Marque **Guardar esta contraseña** si no desea volver a escribirla en futuras sesiones ni para acceder a otros grupos de servidores que utilicen la misma contraseña.

   Si la contraseña es correcta, se guardará.

Para impedir que los servidores no bloqueados se bloqueen cuando el usuario salga de la consola

1. En el panel izquierdo de la consola de Symantec System Center, haga clic con el botón derecho en **Jerarquía del sistema** y después haga clic en **Propiedades**.
2. Deje sin marcar la opción **Bloquear todos los grupos de servidores al salir de la consola**.

Utilización de contraseñas de grupos de servidores

Es posible guardar, no guardar y modificar la contraseña de un grupo de servidores como sea necesario. Para ello, el grupo de servidores debe tener asignado un servidor primario. Las contraseñas se pueden dejar en blanco.

Almacenamiento de contraseñas de grupos de servidores

Puede guardar las contraseñas si no desea volver a escribirlas en futuras sesiones. Una vez guardada una contraseña, no será preciso introducirla cada vez que se abra un grupo de servidores que la utilice. Las contraseñas guardadas se codifican mediante el estándar de codificación de datos DES y se almacenan en el registro de la computadora local. Cuando intente desbloquear un grupo de servidores, Symantec System Center probará todas las contraseñas guardadas. Sólo tendrá que introducir la contraseña en caso de que ninguna de las contraseñas guardadas funcione.

Almacenamiento de contraseñas de grupos de servidores

La casilla de verificación Guardar esta contraseña sirve para almacenar la contraseña de modo que no sea necesario volver a introducirla la siguiente vez que se abra el grupo de servidores.

Cuando se guarda la contraseña, todos los grupos de servidores a los que se haya accedido con anterioridad quedan desbloqueados o no se le pide al usuario la contraseña cada vez que éste intenta desbloquearlos.

Si la casilla de verificación Bloquear todos los grupos de servidores al salir de la consola de la página de propiedades de la jerarquía del sistema no está marcada, el grupo de servidores permanecerá desbloqueado cuando se vuelva a abrir la consola de Symantec System Center.

Si no se guardan las contraseñas, todos los grupos de servidores se bloquearán automáticamente de forma predeterminada cada vez que se ejecute Symantec System Center, aunque se hayan desbloqueado la última vez que se haya ejecutado el programa.

Para guardar la contraseña de un grupo de servidores

1. En el panel izquierdo de la consola de Symantec System Center, haga clic con el botón derecho en un grupo de servidores bloqueado y, a continuación, haga clic en **Desbloquear grupo de servidores**.
2. Escriba la contraseña del grupo de servidores.

   Si ya existe una contraseña para el servidor y se marcó previamente la casilla de verificación **Guardar esta contraseña**, el cuadro de diálogo correspondiente a la contraseña no aparecerá. Puede crear una nueva contraseña con el fin de utilizar esta función.
3. Marque **Guardar esta contraseña**.
4. Haga clic en **Aceptar**.

Vea "Modificación de contraseñas de grupos de servidores" en la página 39.

Para no seguir guardando la contraseña del grupo de servidores

1. En el panel izquierdo de la consola de Symantec System Center, haga clic con el botón derecho en un grupo de servidores desbloqueado y, a continuación, haga clic en **Bloquear grupo de servidores**.
2. Escriba la contraseña anterior.
3. Pulse la tecla **Tabulador** y después escriba la nueva contraseña.
4. Pulse la tecla **Tabulador** y, a continuación, vuelva a escribir la contraseña.
5. Haga clic en **Aceptar**.
6. Cierre la consola de Symantec System Center.
7. Cuando se le pregunte si desea guardar los cambios, haga clic en **No**.

Modificación de contraseñas de grupos de servidores

Las contraseñas de los grupos de servidores se pueden modificar. Por ejemplo, puede que le interese cambiar las contraseñas de forma regular por motivos de seguridad.

Para cambiar la contraseña de un grupo de servidores

1. En el panel izquierdo de la consola de Symantec System Center, haga clic con el botón derecho en el grupo de servidores y, a continuación, haga clic en **Configurar contraseña del grupo de servidores**.
2. Escriba la contraseña anterior.
3. Pulse la tecla **Tabulador** y después escriba la nueva contraseña.
4. Pulse la tecla **Tabulador** y vuelva a escribir la contraseña.
5. Haga clic en **Aceptar**.

Cambio de nombre de los grupos de servidores

Puede cambiar el nombre de los grupos de servidores como considere necesario.

Para cambiar el nombre de un grupo de servidores

1. En el panel izquierdo de la consola de Symantec System Center, desbloquee el grupo de servidores cuyo nombre desee cambiar.
2. Haga clic con el botón derecho en el grupo de servidores y, a continuación, en **Cambiar nombre**.
3. Escriba el nuevo nombre para el grupo.

Selección de un servidor primario para un grupo de servidores

Cuando se selecciona un objeto correspondiente a un grupo de servidores en la consola de Symantec System Center y se configura, las opciones se guardan en el servidor primario del grupo seleccionado. La nueva configuración se aplica también a los restantes servidores del grupo.

Es preciso especificar cuál de los servidores del grupo es el servidor primario, ya que no se especifica ninguno de forma predeterminada. Hasta que no se designe un servidor primario, no se podrán realizar determinadas tareas de administración relacionadas con los productos de Symantec.

Los equipos que tengan instalado uno de los siguientes sistemas operativos podrán designarse como servidores primarios:

- Windows 2000 Server, Advanced Server o Professional
- Windows XP Professional
- Windows NT 4.0 Server o Workstation
- Novell NetWare Server

El servidor primario desempeña un papel importante, por lo que es preferible seleccionar un servidor estable que se encuentre en funcionamiento permanentemente.

Para seleccionar el servidor primario de un grupo de servidores

- En el panel izquierdo de la consola de Symantec System Center, haga clic con el botón derecho en el servidor que funcionará como servidor primario y a continuación haga clic en **Convertir servidor en primario**.

Nota: Al cambiar de servidor primario, se pueden perder las alertas de AMS^2 que se hayan configurado. Podrá configurarlas de nuevo en el nuevo servidor primario o exportarlas a éste antes de cambiar de servidor primario.

Cambio de servidores primarios y principales

Es posible cambiar fácilmente los servidores primarios y principales.

Cambio de servidores primarios

Puede degradar los servidores primarios y promover los servidores secundarios como considere oportuno.

Para cambiar un servidor primario

1. En el panel izquierdo de la consola de Symantec System Center, haga doble clic en el icono correspondiente al grupo de servidores.
2. Haga clic con el botón derecho en el servidor secundario que desee designar como servidor primario y, a continuación, en **Convertir en servidor primario**.

Cambio del servidor principal de los clientes

Para cambiar un servidor principal, debe copiar un archivo de configuración (Grc.dat) del nuevo servidor principal en el cliente y después reiniciar el cliente.

El archivo de configuración es un archivo de texto que actúa como depósito de los cambios efectuados en un grupo de clientes. Los archivos de configuración constituyen la base de la comunicación entre los equipos que cuentan con el servidor de Symantec AntiVirus Corporate Edition y aquellos que tienen instalado el cliente de Symantec AntiVirus Corporate Edition. En estos archivos se guarda información importante, como la identidad del servidor principal y los valores de configuración del producto Symantec AntiVirus Corporate Edition.

Para cambiar el servidor principal de un cliente

1. Copie el archivo de configuración (Grc.dat) del servidor que pretenda establecer como principal de la ubicación \Archivos de programa\SAV\.
2. Pegue el archivo de configuración en una de las siguientes carpetas del cliente:
   - En Windows 98 o ME: C:\Archivos de programa\Norton AntiVirus
   - En Windows NT: C:\Winnt\Profiles\All Users\Datos de programa\Symantec\Norton AntiVirus Corporate Edition\7.5
   - En Windows 2000 o XP: C:\Documents and Settings\All Users\Datos de programa\Symantec\Norton AntiVirus Corporate Edition\7.5
3. Reinicie el cliente.

Traslado de un servidor a otro grupo de servidores

Es posible desplazar servidores de un grupo a otro utilizando el método de arrastrar y colocar.

Cuando se traslada un servidor, se crea automáticamente en él un archivo de configuración (Grcsrv.dat), que transfiere la configuración del nuevo grupo de servidores al servidor. El nuevo grupo de servidores debe disponer de un servidor primario.

El archivo de configuración del servidor está ubicado en el mismo directorio del servidor en el que se instaló Symantec AntiVirus Corporate Edition y tiene el mismo formato que el archivo de configuración del cliente (Grc.dat). Sólo se crea cuando se sincroniza un servidor con la configuración de un nuevo grupo de servidores.

El archivo de configuración del servidor sólo funciona con servidores que tengan instalado tanto Norton AntiVirus Corporate Edition versión 7.5 o posterior como el servidor de Symantec AntiVirus Corporate Edition. En el caso de servidores más antiguos, el servicio de topología se encarga de copiar la configuración del registro del servidor primario en el servidor que se va a mover.

Visualización de los grupos de servidores

Cada vez que ejecute la consola de Symantec System Center, verá en formato de árbol los servidores en los que se ejecuten productos de Symantec AntiVirus Corporate Edition administrados. Los servidores se unen en grupos de servidores.

Visualización de un único grupo de servidores

Se puede ver sólo un grupo de servidores y su contenido.

Para ver un único grupo de servidores

- En el árbol de la consola de Symantec System Center, haga clic con el botón derecho en el grupo de servidores y, a continuación, en **Nueva ventana desde aquí**.

Filtrado de la vista de los grupos de servidores

Existe la posibilidad de filtrar los grupos de servidores que se muestran en la lista de Symantec System Center. Sólo los grupos de servidores que se muestran en ella son susceptibles de supervisión y administración. De forma predeterminada, la consola de Symantec System Center muestra todos los grupos de servidores. Para suprimir grupos de servidores que aparecen en la consola, debe filtrar la vista.

Sólo se reciben las notificaciones relacionadas con los grupos de servidores mostrados. Si filtra un grupo de servidores, dejará de recibir notificaciones relacionadas con él.

Para filtrar la vista de los grupos de servidores

1. En el panel izquierdo de la consola de Symantec System Center, haga clic con el botón derecho en **Jerarquía del sistema** y, a continuación, haga clic en **Ver** > **Filtrar vista del grupo de servidores**.
2. Deje sin marcar los grupos que desee filtrar de la lista de grupos de servidores.

   Todos los grupos de servidores se muestran de forma predeterminada.
3. Haga clic en **Aceptar**.

Supresión de grupos de servidores

Para poder suprimir un grupo de servidores, es necesario trasladar antes sus miembros a un grupo de servidores nuevo o ya existente.

Para suprimir un grupo de servidores

1. En el panel izquierdo de la consola de Symantec System Center, haga clic con el botón derecho en el grupo de servidores que desee suprimir y después haga clic en **Desbloquear grupo de servidores**, si es necesario.
2. Traslade los servidores existentes en el grupo de servidores que vaya a suprimir a otro grupo de servidores utilizando el método de arrastrar y colocar.

   Sólo es posible suprimir un grupo de servidores si se encuentra vacío.
3. Haga clic con el botón derecho en el grupo de servidores vacío y, a continuación, en **Suprimir**.
4. Haga clic con el botón derecho en **Jerarquía del sistema** y, a continuación, en **Actualizar**.

Administración mediante grupos de clientes

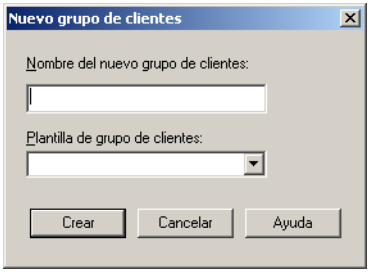
Pueden crearse tantos grupos de servidores como sea necesario para administrar los clientes de forma eficaz.

Creación de un nuevo grupo de clientes

Cada grupo de servidores contiene una única carpeta llamada Grupos en la que se guardan todos los grupos correspondientes a ese grupo de servidores en concreto. Cuando se crea un nuevo grupo de clientes, éste se incluye en la carpeta Grupos.

Para crear un nuevo grupo de clientes

1. En el panel izquierdo de la consola de Symantec System Center, haga clic con el botón derecho en el grupo de servidores al que desee agregar el grupo de clientes y, a continuación, haga clic en **Desbloquear grupo de servidores**.
2. Haga clic con el botón derecho en la carpeta Grupos y después haga clic en **Nuevo grupo**.



3. Escriba un nombre para el grupo en el cuadro de texto Nombre del nuevo grupo de clientes del cuadro de diálogo Nuevo grupo de clientes.
   El nombre no puede exceder los 15 caracteres.
4. Si desea aplicar la configuración de un grupo de clientes existente al nuevo grupo de clientes, seleccione el nombre del grupo que prefiera de la lista desplegable.
5. Haga clic en **Crear**.

Adición de clientes a un grupo de clientes

Se pueden agregar a los grupos de clientes los equipos que tengan instalado el servidor, el cliente o una versión anterior de Symantec AntiVirus Corporate Edition. Todos los clientes reciben el mismo tratamiento. Si un cliente de una versión anterior de Norton AntiVirus no dispone de una función para la cual existe un valor de configuración establecido, esta opción se ignora.

Nota: Sólo los servidores de Symantec AntiVirus Corporate Edition admiten grupos de clientes; las versiones anteriores de Norton AntiVirus Corporate Edition no.

Cada cliente sólo puede pertenecer a un grupo de clientes.

Para agregar un cliente a un grupo de clientes

1. En el panel izquierdo de la consola de Symantec System Center, haga clic en el servidor que contenga el cliente.
2. En el panel derecho, desplace el cliente hasta el grupo de clientes mediante el método de arrastrar y colocar.

Configuración de opciones y ejecución de tareas en el nivel de grupo de clientes

Se pueden establecer opciones de configuración y ejecutar tareas en el nivel de grupo de clientes. Estos valores de configuración se aplicarán a todos los clientes del grupo y cada tarea se ejecutará igualmente en todos los miembros del grupo de clientes.

Para configurar opciones y ejecutar tareas en el nivel de grupo de clientes

1. En el panel izquierdo de la consola de Symantec System Center, haga clic con el botón derecho en el grupo de clientes oportuno.
2. Haga clic en **Todas las tareas**.
3. Haga clic en el producto cuyas opciones desee configurar.
4. Haga clic en el tipo de opciones que quiera establecer o en la tarea que desee ejecutar.

Búsqueda de opciones de grupos de clientes

Los valores de configuración de los grupos de clientes se almacenan en el registro del servidor primario y se distribuyen a los distintos servidores por medio del archivo de configuración de grupo de clientes (Grcgrp.dat). El servidor primario reúne todas las opciones de configuración del grupo de clientes en el archivo de configuración correspondiente y lo copia en cada servidor secundario del grupo de servidores. Después, el servidor secundario distribuye la configuración a los clientes que administra.

Consulte la *Guía de referencia de Symantec AntiVirus Corporate Edition* si desea obtener información sobre los archivos de configuración.

Desplazamiento de clientes entre grupos de clientes

Es posible mover clientes de un grupo de clientes a otro utilizando el método de arrastrar y colocar. Cuando se desplaza un cliente, se le aplica la configuración del nuevo grupo de clientes.

Visualización de grupos de clientes

En el caso de los grupos de clientes, es posible:

- Ver un único grupo de clientes.
- Ver información sobre grupos de clientes.
- Filtrar la vista del grupo de clientes para que muestre sólo la información que le interese.

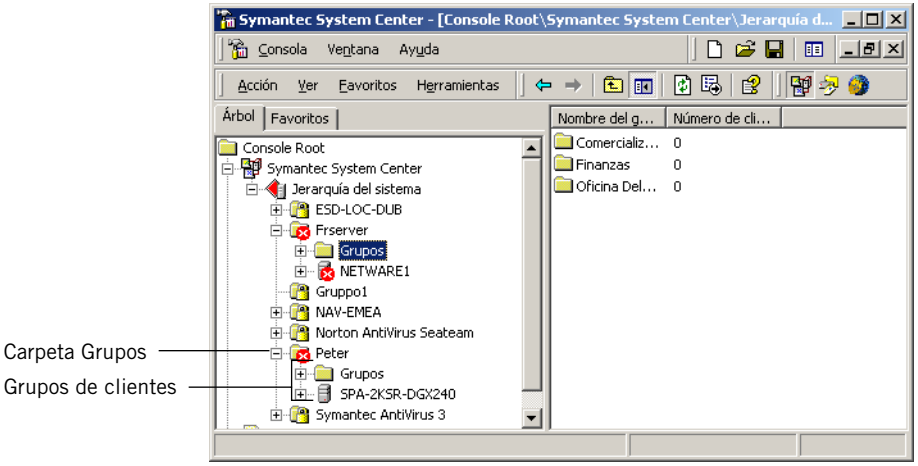
Visualización de un único grupo de clientes

Se puede seleccionar un único grupo de clientes cada vez con el fin de ver su contenido.

Para ver un único grupo de clientes

1. En el panel izquierdo de la consola de Symantec System Center, haga clic con el botón derecho en el grupo de servidores que contiene el grupo de clientes en cuestión y después haga clic en **Desbloquear grupo de servidores**.
2. Haga doble clic en el grupo de servidores.

3 Haga doble clic en la carpeta **Grupos**.



Los grupos de clientes aparecen organizados bajo la carpeta Grupos.

Visualización de información sobre grupos de clientes

Cuando la carpeta Grupos está seleccionada en el panel izquierdo y se selecciona la vista de consola predeterminada o la vista de un producto de Symantec en el menú Ver, los grupos de clientes aparecen en el panel de la derecha junto con información específica de esa vista. Por ejemplo, si la vista de consola predeterminada está activa, se puede ver el número de clientes contenidos en cada grupo de clientes.

Debe estar activado el filtro de grupo de clientes para poder determinar el número de clientes. Cuando se selecciona la carpeta Grupos, no es posible establecer el número de clientes de un grupo de clientes hasta que no se selecciona el grupo en cuestión.

Vea "Filtrado de la vista de grupos de clientes" en la página 47.

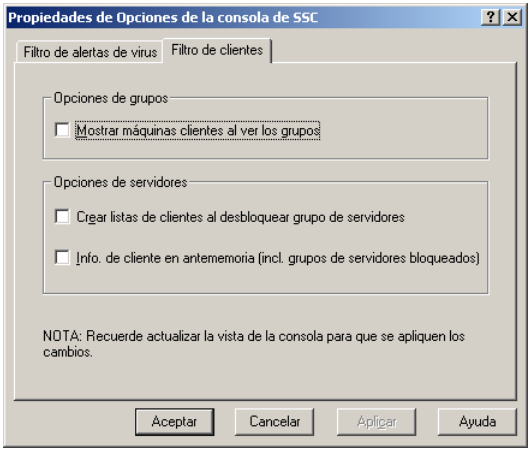
Filtrado de la vista de grupos de clientes

Al seleccionar un grupo de clientes en el panel de la izquierda, se muestran en el panel de la derecha todos los clientes que tiene asignados.

Los filtros mejoran la visualización de los clientes en la consola de Symantec System Center. No obstante, si hay muchos clientes y servidores en el grupo de servidores, los filtros pueden afectar al rendimiento. Los clientes deben enumerarse para poder mostrar los grupos de clientes de forma adecuada. Los filtros están desactivados de forma predeterminada.

Para filtrar la vista del grupo de clientes

1 En el menú Herramientas de la consola de Symantec System Center, haga clic en **Opciones de la consola de SSC**.



2 En el campo Opciones de grupos de la ficha Filtro de clientes del cuadro de diálogo de propiedades de Opciones de la consola de SSC, haga clic en **Mostrar máquinas clientes al ver los grupos**.

3 En Opciones de servidores, haga clic en las opciones siguientes que prefiera:

- Crear listas de clientes al desbloquear grupo de servidores: enumera todos los clientes del grupo de servidores cuando éste se desbloquea.

  Si esta opción no está marcada, los clientes no se agregarán a sus grupos de clientes hasta que se seleccione el servidor. El número de clientes de un grupo de clientes no se ajusta hasta que no se seleccionan todos los servidores del grupo de servidores.
- Info. de cliente en antememoria (incl. grupos de servidores bloqueados): enumera los clientes en los grupos de servidores, tanto bloqueados como desbloqueados, que reconoce el servicio de topología.

Estas opciones pueden afectar al rendimiento cuando el grupo de servidores contiene muchos clientes y servidores.

4 Haga clic en **Aceptar**.

5 En el menú Acción, haga clic en **Actualizar**.

Cambio de nombre de los grupos de clientes

Symantec System Center no permite cambiar el nombre de los grupos de clientes directamente. Si necesita cambiar el nombre de un grupo de clientes, deberá efectuar las siguientes tareas:

- Crear un nuevo grupo de clientes e importar, si lo desea, la configuración de otro grupo de clientes.
  Vea "Creación de un nuevo grupo de clientes" en la página 44.
- Trasladar los clientes del grupo de clientes antiguo al nuevo por medio del método de arrastrar y colocar.
- Suprimir el grupo de clientes antiguo.
  Vea "Supresión de grupos de clientes" en la página 49.

Supresión de grupos de clientes

Antes de suprimir un grupo de clientes, es conveniente asignar los clientes a otro grupo de clientes.

Cuando se suprime un grupo de clientes, los clientes pertenecientes a él conservan la configuración del grupo de clientes eliminado. No se aplicarán nuevos valores de configuración a los clientes hasta que no se produzca una de las acciones siguientes:

- El cliente realice la verificación con su servidor principal. Al cliente se le aplica, entonces, la configuración predeterminada del servidor para clientes no asignados.
- El cliente se asigne a otro grupo de clientes. Al cliente se le aplica, entonces, la configuración del nuevo grupo de clientes.

Si suprime un grupo de clientes y lo vuelve a crear antes de que los clientes realicen la verificación con sus servidores principales o sean asignados a otro grupo, los clientes recuperan automáticamente la pertenencia al grupo original y conservan la configuración de ese grupo.

Para suprimir un grupo de clientes

1. En el panel izquierdo de la consola de Symantec System Center, desbloquee el grupo de servidores en el que se encuentre el grupo de clientes que quiera suprimir.
2. Haga doble clic en el grupo de servidores.
3. Haga doble clic en la carpeta **Grupos**.

4. Haga clic con el botón derecho en el grupo que desee eliminar y, a continuación, en **Suprimir grupo**.
5. Haga clic en **Sí**.
6. Haga clic en **Suprimir**.

Conversión de cliente no administrado en cliente administrado (y viceversa)

Es posible convertir un cliente no administrado en cliente administrado y viceversa.

Cambio del modo de administración de un cliente

Cuando un cliente no administrado se convierte en cliente administrado, el cliente aparece en Symantec System Center y se configura desde aquí. Del mismo modo, cuando un cliente administrado se convierte en cliente no administrado, desaparece de Symantec System Center.

Para convertir un cliente no administrado en cliente administrado

1. Decida qué servidor va a funcionar como servidor principal del cliente.
2. Abra el Entorno de red o Mis sitios de red.
3. Localice y haga doble clic en el equipo que desee que actúe como servidor principal.
   El servidor de Symantec AntiVirus Corporate Edition debe estar instalado en el equipo que seleccione.
4. Abra la carpeta **VPHOME\Clt-inst\Win32.**
5. Copie el archivo Grc.dat en la ubicación que desee.
6. Pegue el archivo Grc.dat en una de las siguientes carpetas del cliente no administrado:
   - Windows 98 o ME: C:\Archivos de programa\Norton AntiVirus
   - Windows NT 4.0: C:\Winnt\Profiles\All Users\Datos de programa\Symantec\Norton AntiVirus Corporate Edition\7.5
   - Windows 2000 o XP: C:\Documents and Settings\All Users\Datos de programa\Symantec\Norton AntiVirus Corporate Edition\7.5
7. Reinicie el cliente.

Para convertir un cliente administrado en cliente no administrado

1. Desinstale Symantec AntiVirus Corporate Edition de la estación de trabajo del cliente.
2. Mediante el editor del registro, borre la siguiente subclave:
   HKEY_LOCAL_MACHINE\Software\Intel\LANDesk\VirusProtect6
3. Vuelva a instalar Symantec AntiVirus Corporate Edition.
4. Cuando se le pregunte si desea que el cliente sea administrado o no administrado, seleccione no administrado.

Capítulo 2

Configuración de Alert Management System

En este capítulo se tratan los temas siguientes:

- Acerca de Alert Management System
- Funcionamiento de Alert Management System
- Configuración de las acciones de alerta
- Utilización de las alertas configuradas
- Utilización del registro de alertas de Alert Management System
- Cómo enviar alertas desde los clientes no administrados

Acerca de Alert Management System

Alert Management System^2 (AMS^2) proporciona funciones de administración de emergencias. AMS^2 admite alertas de servidores de NetWare compatibles, de servidores y estaciones de trabajo Windows NT y 2000, de Windows XP Home Edition o Professional y de estaciones de trabajo Windows 98 y ME.

AMS^2 puede generar alertas a través de los siguientes medios:

- Cuadro de mensaje
- Mensaje de difusión general
- Mensaje de correo por Internet
- Mensaje a buscapersonas
- Ejecución de un programa
- Inclusión en el Registro de sucesos de Windows NT
- Envío de capturas SNMP
- Carga de un NLM

Nota: Las alertas generadas mediante una captura SNMP se pueden enviar a una consola de administración SNMP de cualquier otro fabricante. Para recibir capturas SNMP de Symantec AntiVirus Corporate Edition, debe tener instalado Symantec System Center y AMS^2. (AMS^2 sólo puede ejecutarse en un servidor primario. Se debe usar Symantec System Center para designar el servidor primario.)

Vea "Configuración de la acción de alerta de envío de capturas SNMP" en la página 69.

Funcionamiento de Alert Management System

Las alertas de AMS^2 se transfieren desde Symantec AntiVirus Corporate Edition a AMS^2 a través del servicio Symantec AntiVirus Corporate Edition. En los equipos en los que se esté ejecutando el cliente de Symantec AntiVirus Corporate Edition, el servicio Symantec AntiVirus Corporate Edition espera a que se dé un subproceso de suceso que requiera una alerta.

Estos subprocesos pueden ser generados por los siguientes sucesos:

- Cambio de configuración
- Alerta predeterminada
- Error en suma de control
- Inicio/cierre de Symantec AntiVirus Corporate Edition
- Inicio o fin de un análisis
- Actualización del archivo de definiciones de virus
- Detección de un virus

Si ha configurado una alerta para cualquiera de estos sucesos, se generará un subproceso cuando el suceso se produzca. El subproceso solicitará al servicio Symantec AntiVirus Corporate Edition que cree un bloqueo de información acerca de virus, que se enviará al servidor principal del cliente. Cuando el servidor principal reciba el bloqueo de información sobre virus, lo introducirá en su registro de AMS^2. La información sobre virus se enviará, entonces, al servidor primario, que realizará una llamada a AMS^2. AMS^2 introducirá la información en la base de datos de AMS^2 y actuará sobre ella. La acción que se lleve a cabo dependerá del modo en que se haya configurado la alerta.

La comunicación en AMS se realiza a través de CBA, que forma parte del método de comunicación de Intel.

Configuración de las acciones de alerta

AMS^2 permite configurar muchos métodos diferentes de notificación para los virus detectados y los cambios en la configuración, como el envío de mensajes a buscapersonas, las capturas SNMP y el correo electrónico.

Tareas de configuración de alertas

La configuración de las alertas de AMS^2 requiere que se ejecuten tres procedimientos:

- Selección de una alerta en el cuadro de diálogo Acciones de alerta.
- Selección de la acción que desee asignar a esa alerta. Esta acción es la que ejecutará AMS^2 como respuesta a la detección de un parámetro de la alerta.
- Configuración de la acción de alerta seleccionada.

Por ejemplo, es posible configurar la acción de envío de mensajes a buscapersonas para que cuando se detecte un virus en un servidor protegido se notifique. El mensaje al buscapersonas también puede incluir información adicional, como el nombre y el tipo de virus y las acciones que se han llevado a cabo sobre el archivo infectado.

No hay acciones de alerta predeterminadas para ninguna de las alertas. Hasta que no se configure AMS^2, no se generará ninguna alerta, aunque los sucesos de virus se almacenen en el archivo de registro de AMS^2.

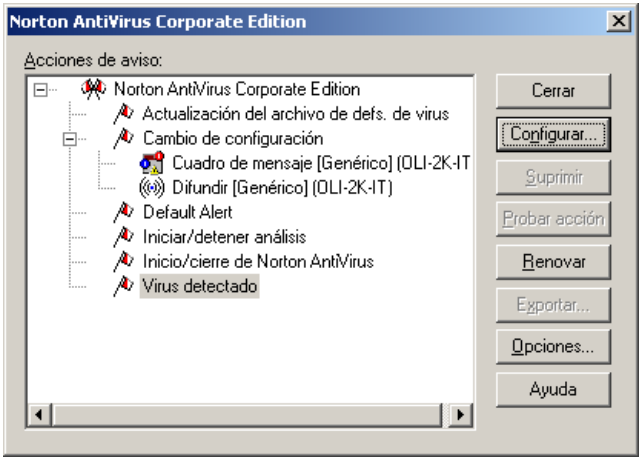
Se puede configurar más de una acción para cada alerta. Una vez configuradas las acciones de alerta para una alerta, aparecerá un signo más (+) o menos (-) junto a cada alerta configurada, dependiendo de si la entrada está contraída o expandida.

Cada acción de alerta de AMS^2 tiene su propio asistente de configuración. Una vez configurada la acción de alerta, dicha acción aparecerá en el cuadro de diálogo Acciones de alerta bajo la alerta para la que se haya configurado la acción.

Todas las acciones de alerta se ejecutarán en el equipo que se seleccione al configurar la acción. Las acciones no se ejecutarán si se han configurado en un equipo que no admita esas acciones concretas. Por ejemplo, los equipos en los que se haya configurado la acción de envío de mensajes a buscapersonas deben tener un módem.

Para configurar una alerta

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



2 Seleccione una alerta y haga clic en **Configurar** para definir una acción de alerta.

Configuración de los mensajes de las acciones de alerta

En las acciones de alerta que generan mensajes (por ejemplo, la aparición de cuadros de mensaje, el envío de mensajes de difusión general, el envío de mensajes a buscapersonas y el envío de mensajes de correo por Internet), se puede incluir información adicional acerca de la alerta que haya generado el mensaje. Los tipos de información adicional se recogen en la Tabla 2-1.

Tabla 2-1 Parámetros de alerta

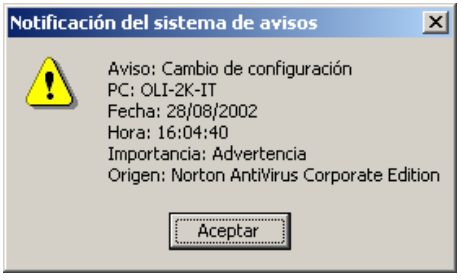
Parámetro de alerta	Descripción
<Equipo>	El nombre del equipo en el que se ha originado la alerta
<Fecha>	La fecha en la que se ha originado la notificación
<Descripción>	Más información acerca de la naturaleza de la notificación; por ejemplo, "Los servicios de Symantec AntiVirus Corporate Edition se han cerrado correctamente."
<Gravedad>	El nivel de gravedad asignado a la alerta; por ejemplo, si es muy grave o no lo es.

Tabla 2-1 Parámetros de alerta

Parámetro de alerta	Descripción
<Hora>	La hora en la que se ha originado la notificación
<Nombre de la alerta>	El nombre de la alerta; por ejemplo, Inicio/cierre de Symantec AntiVirus Corporate Edition
<Nombre del host>	Nombre del servidor de alertas
<Origen>	El producto que ha originado la notificación; por ejemplo, Symantec AntiVirus Corporate Edition

El cuadro de diálogo Mensaje incluye un cuadro de texto en el que se pueden introducir hasta 256 caracteres para utilizarlos como texto del mensaje que se desee enviar. Se pueden utilizar las variables de parámetros de alerta para insertar la información generada por la alerta. Los parámetros están delimitados por los caracteres < y >. Cada parámetro que se añade al cuadro de texto Mensaje se sustituye por la información de alerta correspondiente cuando se produce una alerta, como en la Figura 2-1.

Figura 2-1 Notificación del sistema de alertas



Vea "Cómo probar las acciones de alerta configuradas" en la página 73.

Si el sistema de alertas de AMS^2 detecta un mensaje de un tamaño mayor de 1 KB, no lo enviará. Si se ha configurado un mensaje de alerta predeterminado, se enviará éste en su lugar. Es posible configurar esta alerta predeterminada para que si un mensaje tiene un tamaño mayor de 1 KB lo notifique al administrador.

Para configurar un mensaje de alerta predeterminado

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

3. Haga clic en **Cuadro de mensaje** y, a continuación en **Siguiente**.
4. Seleccione el equipo en el que se debe ejecutar la acción y haga clic en **Siguiente**.
5. Seleccione si desea que se emita un sonido de error y si desea que el cuadro de diálogo permanezca siempre visible hasta que se solucione el suceso.
6. Haga clic en **Siguiente**.
7. Escriba el nombre de la acción que describirá el mensaje que se está configurando.

   El nombre de la acción y el del equipo que la ejecuta aparecerán en el cuadro de diálogo Acciones de alerta junto a esta acción.
8. En el cuadro Mensaje realice una de las acciones siguientes:
   - Escriba el mensaje personalizado que desee mostrar y mueva los valores disponibles que desee desde Parámetros de alerta hasta el cuadro Mensaje.
   - Haga clic en **Predeterminado** para usar la información correspondiente al mensaje predeterminado para esta acción de alerta y escriba el mensaje personalizado que desee que se muestre.

     Tenga en cuenta que el mensaje predeterminado incluye la siguiente información:

     Equipo: <Nombre del host>

     <Nombre del host> es el nombre del servidor de alertas. Para incluir el nombre del equipo en el que se ha originado la notificación, se debe añadir el parámetro <Equipo> al mensaje.
9. Haga clic en **Finalizar**.

Cómo acelerar la configuración de las alertas con un reconocimiento avanzado

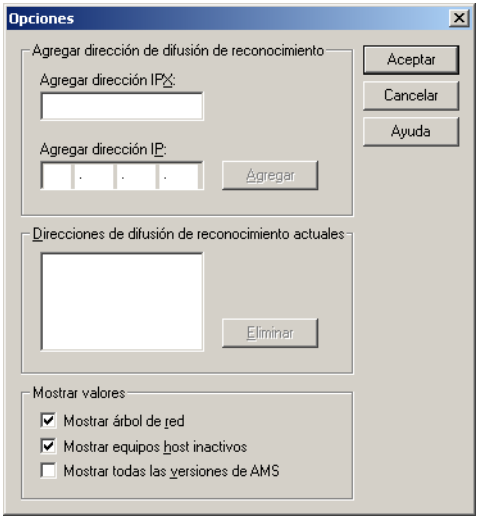
En una red de gran tamaño, se puede acelerar y simplificar la configuración de AMS^2 mediante el uso de la opción de reconocimiento avanzado para buscar equipos con AMS^2 sólo en una zona determinada de la red.

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 de reconocimiento 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 a un reconocimiento de AMS^2 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 configurar las opciones de reconocimiento avanzado

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.

     Es decir, 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 máquinas 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 nuevos equipos con AMS^2 en las redes de difusión que se detallen 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 es 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. Tan sólo se evita que AMS^2 busque equipos con AMS^2 en esa sección de la red.

6 Haga clic en **Aceptar** para guardar la lista y volver al cuadro de diálogo Acciones de alerta.

Configuración de la acción de alerta de aparición de un cuadro de mensaje

La acción de alerta de aparición de un cuadro de mensaje muestra un cuadro de mensaje en el equipo para el que se ha configurado la alerta. Se puede seleccionar si el cuadro de mensaje debe emitir un sonido y si debe permanecer siempre visible hasta que se solucione el problema.

Para configurar la acción de alerta de aparición de un cuadro de mensaje

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

2 Seleccione la alerta para la que desee configurar las acciones de alerta.

3 Haga clic en **Configurar**.

4 Haga clic en **Cuadro de mensaje** y luego en **Siguiente**.

5 Seleccione un equipo en el que ejecutar la acción y haga clic en **Siguiente**.

6 Seleccione si desea que se emita un sonido de error y si desea que el cuadro de diálogo permanezca siempre visible hasta que se solucione el problema.

7 Haga clic en **Siguiente**.

8 Escriba un nombre para la acción.

El nombre de la acción y el nombre del equipo que la ejecuta aparecerán en el cuadro de diálogo Acciones de alerta junto a esta acción.

9 En el campo Mensaje, escriba cualquier mensaje de texto que desee que se muestre y mueva los parámetros disponibles desde Parámetros de alerta hasta el cuadro Mensaje.

10 Haga clic en **Finalizar**.

Configuración de la acción de alerta de envío de un mensaje de difusión general

La acción de alerta de envío de un mensaje de difusión general envía un mensaje a todos los equipos que hayan iniciado una sesión en el servidor en el que se ha generado la alerta.

Para configurar la acción de alerta de envío de un mensaje de difusión general

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. Seleccione la alerta para la que desee configurar las acciones de alerta.
3. Haga clic en **Configurar**.
4. Haga clic en **Difusión** y luego haga clic en **Siguiente**.
5. Seleccione un equipo en el que ejecutar la acción y haga clic en **Siguiente**.
6. En el campo Mensaje, escriba cualquier mensaje de texto que desee que se muestre y mueva los parámetros disponibles desde Parámetros de alerta hasta el cuadro Mensaje.
7. Escriba un nombre para la acción.
   El nombre de la acción y el nombre del equipo que la ejecuta aparecerán en el cuadro de diálogo Acciones de alerta junto a esta acción.
8. Haga clic en **Finalizar**.

Configuración de la acción de alerta de ejecución de un programa

La acción de alerta de ejecución de un programa ejecuta un programa en el equipo para el que se ha configurado la acción. Se deben rellenar dos campos en el cuadro de diálogo Ejecución de programa.

El campo Programa debe incluir la ruta completa al programa que se debe ejecutar. El campo Línea de comandos debe contener cualquier opción de línea de comandos para dicho programa. El programa seleccionado debe estar en la unidad local del equipo para garantizar que AMS^2 pueda encontrarlo.

Si el programa está en un equipo remoto, debe introducir la ruta completa hacia el programa desde ese equipo.

Si se trata de un programa de Windows, se puede seleccionar si se debe ejecutar en una ventana normal, minimizada o maximizada. Está opción no surte ningún efecto en los programas para DOS.

Para configurar la acción de alerta de ejecución de un programa

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. Seleccione la alerta para la que desee configurar las acciones de alerta.
3. Haga clic en **Configurar**.
4. Haga clic en **Ejecución de programa** y luego en **Siguiente**.
5. Seleccione un equipo en el que ejecutar la acción y haga clic en **Siguiente**.
6. Escriba la ruta completa del programa que desee que se ejecute, incluido el nombre del programa.
7. Introduzca las opciones de línea de comandos que desee que use el programa.
8. Seleccione si el estado de ejecución debe ser normal, minimizado o maximizado.
9. Haga clic en **Finalizar**.

Configuración de la acción de alerta de carga de un NLM

La acción de alerta de carga de un NLM carga un módulo cargable de NetWare (NLM) en un servidor de NetWare seleccionado cuando se genera una alerta de AMS^2. Es preciso configurar esta alerta para determinar qué NLM se carga y el servidor que realiza la acción. Esta acción de alerta es similar a la alerta de ejecución de un programa de equipos con Windows NT.

Por ejemplo, si tiene instalado el módulo integrable de administración de Symantec AntiVirus Corporate Edition, puede configurar la acción de alerta de carga de un NLM para que se cargue un NLM creado por el usuario o por otro fabricante en un servidor de NetWare seleccionado cuando Symantec AntiVirus Corporate Edition detecte un virus. Este NLM permitiría supervisar quién accede al servidor y quién utiliza el archivo infectado, además de realizar copias de respaldo de los archivos por si se diera el caso de que el servidor se bloqueara debido al virus.

Para configurar la acción de alerta de carga de un NLM

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. Seleccione la alerta para la que desea configurar las acciones de alerta.
3. Haga clic en **Configurar**.
4. Haga clic en **Carga de un NLM** y luego en **Siguiente**.
   La primera vez que se configura esta acción, AMS^2 debe buscar en la red los equipos que pueden llevar a cabo esta acción.
   Cuando se complete la búsqueda, aparecerán los equipos con NetWare en forma de árbol.
5. Si el equipo que está buscando no aparece en la lista, haga clic en **Reconocimiento** para buscar todos los equipos de nuevo y encontrarlo.
6. Seleccione el equipo donde se deba cargar el NLM y haga clic en **Siguiente**.
7. Escriba o seleccione el NLM que se deba cargar.
   Los NLM se almacenan normalmente en el directorio SYS:SYSTEM de los servidores de NetWare.
8. Introduzca las opciones de línea de comandos que desee que use el programa.
9. Haga clic en **Finalizar**.

Configuración de la acción de alerta de envío de un mensaje de correo por Internet

La acción de alerta de envío de un mensaje de correo por Internet envía un mensaje de correo electrónico por Internet al usuario que se indique. Al utilizar esta acción de alerta, también es necesario especificar el servidor SMTP a través del cual la acción de alerta enviará el mensaje. Si se especifica el servidor de correo por su nombre, será necesario tener un servidor DNS configurado para que la acción de alerta pueda entender la dirección IP del servidor. Si no se dispone de un servidor DNS, se puede introducir la dirección IP del servidor directamente.

Si no tiene acceso a una cuenta de correo SMTP en las instalaciones, esta acción de alerta no funcionará.

Para configurar la acción de alerta de envío de un mensaje de correo por Internet

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. Seleccione la alerta para la que desee configurar las acciones de alerta.
3. Haga clic en **Configurar**.
4. Haga clic en **Envío de correo de Internet** y luego en **Siguiente**.
5. Seleccione el equipo en el que ejecutar la acción y haga clic en **Siguiente**.
6. En los cuadros Dirección de Internet, Remitente, Tema y Servidor de correo, escriba o seleccione la información adecuada.

   Es preferible introducir la dirección IP del servidor de correo en lugar del nombre.

   El cuadro Remitente debe contener una dirección de correo electrónico válida. La mayoría de los servidores de correo electrónico no enviarán los mensajes si el servidor no puede verificar la dirección de correo electrónico de quien lo envía.
7. Haga clic en **Siguiente**.
8. En el campo Mensaje escriba cualquier mensaje de texto que desee que se muestre y mueva los parámetros disponibles desde Parámetros de alerta al cuadro Mensaje.
9. Escriba un nombre para la acción.

   El nombre de la acción y el del equipo que la ejecuta aparecerán en el cuadro de diálogo Acciones de alerta junto a esta acción.
10. Haga clic en **Finalizar**.

Configuración de la acción de alerta de envío de un mensaje a buscapersonas

La acción de alerta de envío de mensajes a buscapersonas enviará un mensaje de buscapersonas al número que se indique. Para hacerlo, el equipo en el que se configure esta acción deberá tener un módem.

Vea "Cómo probar las acciones de alerta configuradas" en la página 73.

La configuración de la acción de alerta de envío de mensajes a buscapersonas se compone de los tres pasos siguientes:

- Configuración de un módem para su uso por parte de AMS[2.]
- Configuración del servicio de envío de mensajes a buscapersonas.
- Introducción de un mensaje de buscapersonas.

Para configurar la acción de alerta de envío de mensajes a buscapersonas

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. Seleccione la alerta para la que desee configurar las acciones de alerta.
3. Haga clic en **Configurar**.
4. Haga clic en **Envío a buscapersonas** y luego en **Siguiente**.
5. Seleccione un equipo en el que ejecutar la acción y haga clic en **Siguiente**.
6. Escriba el número de teléfono de acceso al que se deba llamar para acceder al servicio de envío de mensajes a buscapersonas.

   Debe asegurarse de que se incluyan todos los números necesarios para obtener línea con el exterior desde las instalaciones de su empresa.
7. Escriba el número de identificación y la contraseña del buscapersonas que utilice para acceder a la red del servicio de envío de mensajes a buscapersonas.

   Si su servicio de buscapersonas no utiliza contraseña, deje el cuadro correspondiente en blanco.
8. Seleccione el tipo de servicio.

   Si no aparece su servicio de envío de mensajes a buscapersonas, pruebe con uno de los tipos genéricos.

   Vea "Configuración del servicio de envío de mensajes a buscapersonas" en la página 67.
9. Haga clic en **Siguiente**.

   Si está creando un mensaje para un servicio de envío de mensajes a buscapersonas alfanumérico, en el cuadro Mensaje escriba el texto que desea mostrar y mueva los valores disponibles desde Parámetros de alerta al cuadro Mensaje.

   Si está creando un mensaje para un servicio de envío de mensajes a buscapersonas numérico, únicamente podrá escribir números en el cuadro Mensaje.
10. Escriba un nombre para la acción.

    El nombre de la acción y el del equipo que la ejecuta aparecerán en el cuadro de diálogo Acciones de alerta junto a esta acción.
11. Haga clic en **Finalizar**.

Configuración de un módem para su uso con AMS

Es preciso configurar un módem si se pretende que AMS^2 lo utilice para ponerse en contacto con el servicio de envío de mensajes a buscapersonas. Para que la acción de alerta de envío de mensajes a buscapersonas funcione correctamente, es necesario ejecutar la utilidad de configuración del módem y seleccionar el puerto COM adecuado y los valores correspondientes al tipo de módem que se vaya a utilizar.

Para configurar un módem para su uso con AMS

1. En el Explorador de Windows, haga doble clic en el archivo **Modemcfg.exe** para ejecutar la utilidad.

   Esta utilidad se instala en el equipo que ejecuta la acción en la carpeta Winnt\System32\AMS_ii.

2. Seleccione el puerto COM que utilice el módem.

3. Seleccione el tipo de módem adecuado.

4. Haga clic en **Aceptar** para guardar estos valores y el módem ya estará configurado para su correcto funcionamiento con el sistema de alertas AMS^2.

Configuración del servicio de envío de mensajes a buscapersonas

Se puede acceder a un servicio de envío de mensajes a buscapersonas directa o indirectamente. Con el método de envío directo, se marca el número de acceso de red del proveedor del servicio y se accede a su red de equipos directamente para introducir el número de identificación del buscapersonas. Posteriormente, la red del servicio de buscapersonas envía el mensaje al buscapersonas.

El sistema de alertas AMS^2 no funciona con el envío indirecto de mensajes a buscapersonas. En este tipo de envío es preciso llamar a un servicio de envío de mensajes a buscapersonas y proporcionarle a un operador el número de identificación del buscapersonas. El operador introduce la información en la red del servicio para que se pueda enviar el mensaje al buscapersonas. El método indirecto se suele usar cuando se debe realizar una llamada de pago para contactar con la red y el servicio de envío de mensajes ofrece llamadas gratuitas para contactar con sus operadores.

Deberá configurar la acción de alerta para su servicio de envío de mensajes. Como mínimo, esta información debe incluir el número de teléfono del servicio de buscapersonas y el nombre de dicho servicio.

Siempre se debe incluir el número de teléfono del servicio de envío de mensajes a buscapersonas en el cuadro Proveedor de servicios del cuadro de diálogo Envío a buscapersonas. Si su servicio de envío de mensajes no está incluido en la lista desplegable de servicios del cuadro de diálogo Envío a buscapersonas, puede intentar utilizar los servicios Buscapersonas genérico o Alfanumérico genérico (seleccione el que corresponda al tipo de servicio que utiliza). Escriba la contraseña que utilice para acceder a la red del servicio de envío de mensajes a buscapersonas en el cuadro Contraseña.

Si el servicio genérico seleccionado no funciona con su buscapersonas, deberá configurar los parámetros de comunicación que deba usar la acción de alerta de envío de mensajes a buscapersonas. Esta información incluye la velocidad en baudios, los bits de datos y de parada, la paridad y el protocolo de buscapersonas que usa su servicio. Si su servicio de buscapersonas está incluido en la lista desplegable, estos parámetros se configurarán automáticamente al seleccionar el servicio.

Para configurar la acción de alerta de envío de mensajes a buscapersonas para un servicio de buscapersonas que no se encuentra en la lista

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. Seleccione la alerta para la que desee configurar las acciones de alerta.
3. Haga clic en **Configurar**.
4. Haga clic en **Envío a buscapersonas** y luego en **Siguiente**.
5. Seleccione un equipo en el que ejecutar la acción y haga clic en **Siguiente**.
6. Haga clic en **Configuración**.
7. Introduzca los valores correspondientes al protocolo, la longitud máxima del mensaje, la velocidad en baudios, los bits de datos, los bits de parada y la paridad que utiliza el servicio de buscapersonas.

   Se puede conseguir esta información consultando al servicio de envío de mensajes a buscapersonas.
8. Haga clic en **Aceptar** y continúe configurando la acción de alerta de envío de mensajes a buscapersonas siguiendo el paso 6 de "Para configurar la acción de alerta de envío de mensajes a buscapersonas" en la página 66.

Introducción de un mensaje de buscapersonas

La acción de alerta de envío de mensajes a buscapersonas es compatible con los buscapersonas alfanuméricos y numéricos (los buscapersonas numéricos se llaman a veces beepers).

Si se envía el mensaje a un buscapersonas alfanumérico, el mensaje puede incluir cualquier texto escrito o información acerca de la alerta que ha generado el mensaje. Este mensaje no debe exceder el número máximo de caracteres que proporcione el servicio de envío de mensajes a buscapersonas; de lo contrario, se obtendrían mensajes truncados.

Si se van a enviar mensajes a un buscapersonas numérico, puede ser útil crear un sistema de números de servidor y de códigos de error numéricos que correspondan a las alertas que se configuren. Por ejemplo, se puede crear un sistema en el que "1" signifique el servidor principal y el número "101" que ha ocurrido algún suceso en concreto. Si el administrador recibe el mensaje "1 101", sabrá que el suceso ha ocurrido en el servidor principal.

Configuración de la acción de alerta de envío de capturas SNMP

El protocolo Simple Network Management Protocol (SNMP) es un protocolo de mensajes basado en un modelo de administrador y agentes que consiste en mensajes y respuestas del tipo Get, GetNext y Set. SNMP utiliza capturas para informar acerca de condiciones excepcionales como fallos en los componentes o violaciones del umbral.

AMS^2 puede generar capturas SNMP cuando se produce una alerta.
El administrador puede configurar las alertas generadas por el sistema para que se envíen las capturas a una consola de administración, como HP OpenView, Tivoli Enterprise Console o Computer Associates Unicenter.

Debe especificar la dirección (IP o IPX) de los equipos a los que desee enviar las capturas SNMP.

Para configurar la acción de alerta de envío de capturas SNMP

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. Seleccione la alerta para la que desee configurar las acciones de alerta.
3. Haga clic en **Configurar**.
4. Haga clic en **Envío de captura SNMP** y después en **Siguiente**.
5. Seleccione un equipo en el que ejecutar la acción y haga clic en **Siguiente**.

6 En el campo Captura SNMP, escriba cualquier mensaje de texto que desee que se muestre y mueva los parámetros disponibles de Parámetros de alerta al cuadro Mensaje.

7 Escriba un nombre para la acción.

El nombre de la acción y el del equipo que la ejecuta aparecerán en el cuadro de diálogo Acciones de alerta junto a esta acción.

8 Haga clic en **Finalizar**.

Configuración de los destinos de las capturas en Windows NT 4.0

Es posible configurar las capturas SNMP en el caso de Windows NT 4.0.

Para configurar los destinos de las capturas en Windows NT 4.0

1 En el Panel de control de Windows NT, haga doble clic en **Red**.

2 Haga clic en **Servicios**.

3 Haga clic en **Servicio SNMP** y luego en **Propiedades**.

4 Haga clic en **Capturas**.

5 En el cuadro Nombre de comunidad, haga clic en **Público**.

6 Si no existe una entrada pública en la lista, escríbala y después haga clic en **Agregar**.

7 En el campo Destinos de capturas, haga clic en **Agregar**.

8 Introduzca las direcciones de los equipos a los que desee enviar las capturas y haga clic en **Agregar**.

9 Haga clic en **Aceptar** y, a continuación, en **Cerrar**.

Configuración de los destinos de las capturas en Windows 2000 Server

Es posible configurar las capturas SNMP en Windows 2000 Server.

Para configurar los destinos de las capturas en Windows 2000 Server

1 En la barra de tareas de Windows, haga clic en **Inicio** > **Configuración** > **Panel de control**.

2 Haga doble clic en **Herramientas de administración**.

3 Haga doble clic en **Administración de equipos**.

4 Haga clic en **Servicios y Aplicaciones**.

5 Haga clic en **Servicios**.

6 En el panel derecho, haga clic en **Servicio SNMP**.

7 En el menú Acción, haga clic en **Propiedades**.

8 En la ficha Capturas, bajo Comunidad, escriba utilizando mayúsculas y minúsculas el nombre de la comunidad a la que este equipo enviará los mensajes de captura y, después, haga clic en **Agregar a la lista**.

9 En el campo Destinos de capturas, haga clic en **Agregar**.

10 En Nombre, dirección IP o IPX del host, escriba la información relativa al host y haga clic en **Agregar**.

11 Repita los pasos del 8 al 10 hasta que haya agregado todas las comunidades y los destinos de las capturas que desee.

Configuración de los destinos de las capturas en NetWare

Es posible configurar las capturas SNMP en servidores NetWare 4.1x, 5.x y 6.x.

Para configurar los destinos de las capturas en NetWare

1 En la consola del servidor de NetWare, escriba:
load inetcfg

2 Seleccione **Protocolos** y presione la tecla **Entrar**.

3 Seleccione **TCP/IP** y presione **Entrar**.

4 Seleccione **Tabla de administración de SNMP** y después presione **Entrar** para mostrar la tabla de administración de SNMP.

5 Realice una de las acciones siguientes:

- Para modificar una dirección existente, selecciónela y presione **Entrar**.
- Para agregar una nueva dirección, presione la tecla **Insert**, escriba una dirección IP y luego presione **Entrar**.
- Para suprimir una dirección, selecciónela, presione la tecla **Supr** y luego presione **Entrar** para confirmar la eliminación.

6 Presione la tecla **Esc** para cerrar el cuadro de diálogo.

7 Presione **Entrar** para confirmar el cambio en la base de datos.

Configuración de la acción de alerta de inclusión en el registro de sucesos

La acción de alerta de inclusión en el registro de sucesos crea una entrada en el registro de aplicaciones de Windows NT, 2000 y XP, que se almacena en el servidor del que procede la alerta. Sólo está disponible en equipos con Windows NT, 2000 y XP.

Para configurar la acción de alerta de inclusión en el registro de sucesos

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. Seleccione la alerta para la que desee configurar las acciones de alerta.
3. Haga clic en **Configurar**.
4. Haga clic en **Escritura en el Registro de sucesos** y luego en **Siguiente**.
5. Seleccione un equipo en el que ejecutar la acción y haga clic en **Siguiente**.
6. En el cuadro Mensaje, escriba cualquier mensaje que desee que se muestre y mueva los parámetros que prefiera desde Parámetros de alerta hasta el cuadro Mensaje.
7. Escriba un nombre para la acción.
   El nombre de la acción y el del equipo que la ejecuta aparecerán en el cuadro de diálogo Acciones de alerta junto a esta acción.
8. Haga clic en **Finalizar**.

Utilización de las alertas configuradas

Una vez que haya configurado las acciones de alerta, podrá:

- Probarlas para asegurarse de que funcionan del modo previsto.
- Suprimirlas.
- Exportarlas a otros equipos.

Cómo probar las acciones de alerta configuradas

Tras haber configurado las acciones de alerta, se puede comprobar su funcionamiento mediante el cuadro de diálogo Acciones de alerta. Al seleccionar una alerta y hacer clic en Probar acción, se ejecutan todas las acciones de alerta correspondientes a dicha alerta. Si sólo se selecciona una acción de alerta y se hace clic en Probar acción, se ejecutará únicamente la acción correspondiente.

Para probar una alerta

- En el cuadro de diálogo Acciones de alerta, seleccione una alerta y haga clic en **Probar acción**.

Eliminación de una acción de alerta

Se pueden suprimir las acciones asociadas a las alertas según sea necesario.

Para suprimir una acción de alerta de una 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. Seleccione la acción de alerta que desee suprimir y presione **Supr**.

Cómo exportar acciones de alerta a otros equipos

Cada equipo que genera alertas de AMS^2 almacena la información acerca de éstas en una base de datos local de AMS^2. Normalmente, las alertas y acciones que se almacenan en una base de datos no son visibles desde las bases de datos de AMS^2 de otros equipos.

Puede ocurrir que sea necesario trasladar directamente la configuración de las acciones de alerta de AMS^2 de un equipo a otros equipos para no tener que repetir el mismo trabajo. La opción de exportación de AMS^2 permite exportar acciones de alerta a otros equipos que generen alertas de AMS^2.

Las acciones de alerta, como la configuración de una acción de alerta de envío de mensajes a buscapersonas o la aparición de un cuadro de mensaje, sólo se exportarán si la alerta para la que se ha configurado la acción existe en ambos equipos. En la mayoría de los casos, se puede garantizar que se cumpla esta condición instalando la misma aplicación en ambos equipos. De este modo, ambas copias de la aplicación registrarán sus alertas en sus respectivas bases de datos de AMS^2.

Cuando se exportan las acciones de alerta de un equipo a otro, se puede elegir si se desea exportar una única acción de alerta o todas. Una vez que AMS^2 haya exportado las acciones de alerta a un equipo, AMS^2 mostrará el cuadro de diálogo Estado de la exportación que informará de los resultados de la exportación.

Si la opción de exportación no puede exportar una acción de alerta porque la alerta para la que está configurada la acción no existe en el equipo de destino (o por cualquier otra razón), el cuadro de diálogo Estado de la exportación indicará que la acción de alerta no se pudo exportar con éxito. La exportación de las acciones de alerta también puede fallar debido a que AMS^2 no esté funcionando correctamente en el equipo de destino.

Para exportar acciones de alerta a otros equipos

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. Realice una de las acciones siguientes:
   - Haga clic en la carpeta **Norton AntiVirus Corporate Edition** si desea exportar todas las alertas asociadas con Symantec AntiVirus Corporate Edition.
   - Seleccione una alerta (si desea exportar todas las acciones correspondientes a dicha alerta) o una acción de alerta específica (si sólo desea exportar la acción de alerta seleccionada).
3. Haga clic en **Exportar**.
4. En la lista de equipos disponibles, haga doble clic en los equipos que desee que reciban las acciones de alerta seleccionadas.

   Dichos equipos se agregarán a la lista de equipos seleccionados.

   Si AMS^2 está activo en el equipo seleccionado y éste no se muestra en la lista de equipos disponibles, haga clic en **Reconocimiento** para volver a buscar equipos mediante AMS^2.
5. Haga clic en **Exportar**.
6. Haga clic en **Sí** como respuesta al mensaje de confirmación.
7. En el cuadro de diálogo Estado de la exportación, compruebe que las acciones de alerta se han exportado con éxito.

Visualización del estado de la exportación

Cuando AMS^2 haya terminado de exportar las acciones de alerta a los equipos seleccionados en el cuadro de diálogo Selección de equipos, AMS^2 mostrará los resultados de la exportación en el cuadro de diálogo Estado de la exportación.

Este cuadro de diálogo muestra las acciones de alerta que no se han podido exportar con éxito. El hecho de que las alertas no se exporten correctamente puede deberse a las razones siguientes:

- AMS^2 no está activado o no funciona correctamente en el equipo de destino. Compruebe el funcionamiento de AMS^2 probando una acción de alerta configurada en ese equipo desde el cuadro de diálogo Acciones de alerta.
- La alerta para la que se ha configurado la acción no existe en el equipo de destino. Asegúrese de que la aplicación que ha registrado los datos con AMS^2 en el equipo de origen está instalada en el equipo de destino.

Utilización del registro de alertas de Alert Management System

El registro de alertas permite mostrar una lista de todas las alertas generadas por los equipos de la red en los que se ejecute Symantec AntiVirus Corporate Edition.

Es posible configurar el registro de alertas para que realice una de las acciones siguientes:

- Mostrar sólo las alertas que cumplan las condiciones especificadas.
- Mostrar un número concreto de entradas.

El registro de alertas muestra una lista de las alertas con la siguiente información acerca de cada una:

- Nombre de la alerta
- Origen
- Equipo
- Fecha
- Hora
- Gravedad

Además de la información básica que muestra el registro de alertas, se puede acceder a una información más detallada acerca de cada alerta en el cuadro de diálogo Información de alerta.

Cada servidor almacena su propia copia local del registro de alertas. Cuando se selecciona un servidor y se visualiza su registro de alertas, se almacena una copia del registro de alertas correspondiente a dicho servidor en la consola local. Por lo tanto, si dicho servidor no está encendido o no está disponible, no será posible obtener su registro de alertas para visualizarlo.

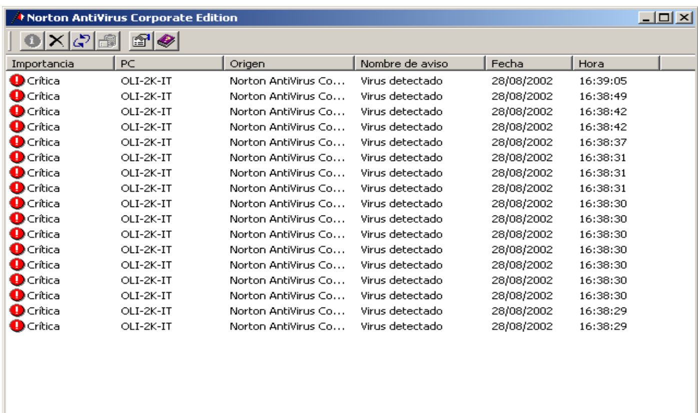
Visualización del registro de alertas e interacción con él

A continuación se indican las diversas formas en que es posible visualizar el registro de alertas e interactuar con él:

- Cambiando el número de entradas que aparecen en el registro.
- Eliminando entradas.
- Copiando los contenidos en el Portapapeles.

Para ver el registro de alertas

◆ Haga clic con el botón derecho en el grupo de servidores y luego haga clic en **Todas las tareas** > **AMS** > **Ver registro**.



Para cambiar el número de entradas que se muestran en el registro de alertas

1. En la ventana Registro de alertas, haga clic con el botón derecho y seleccione a continuación **Opciones**.
2. Especifique el número de entradas que desea que mantenga el registro.

Nota: Se puede configurar de modo independiente el número de entradas del registro de alertas para cada servidor.

Para eliminar una entrada en concreto

- Haga clic con el botón derecho en la entrada correspondiente y luego haga clic en **Suprimir** > **Entradas seleccionadas**.

Para suprimir varias entradas del registro

1. Presione **Ctrl** y seleccione las entradas del registro que desee suprimir.
2. En la ventana del registro de alertas, haga clic con el botón derecho y seleccione **Suprimir** > **Entradas seleccionadas**.

   Para seleccionar un intervalo, haga clic en la primera entrada, mantenga presionada la tecla **Mayús** y haga clic en la última entrada.

Para suprimir todas las entradas visibles del registro

- En la ventana del registro de alertas, haga clic con el botón derecho y, a continuación, haga clic en **Suprimir** > **Entradas filtradas**.

Para copiar el contenido del registro de alertas en el Portapapeles

1. Mantenga presionada la tecla **Ctrl** y seleccione las entradas del registro.
2. En la ventana del registro de alertas, haga clic con el botón derecho y, a continuación haga clic en **Copiar**.

   Sólo se copiarán las alertas visibles del registro. Para limitar el número de entradas del registro que se copian en el Portapapeles, aplique filtros que limiten el número de entradas del registro visibles.

Visualización de información más detallada acerca de las alertas

Puede visualizar información más detallada acerca de cada alerta en el registro de alertas. El cuadro de diálogo Información de alerta mostrará la información detallada e incluirá las alertas, sus valores y el estado de la acción correspondiente a cada alerta.

Igualmente, mostrará una serie de parámetros como el nombre de la alerta, su origen, su fecha, su gravedad y una descripción, así como los valores configurados para la acción de alerta seleccionada.

Este cuadro de diálogo también muestra los tipos de estado que se incluyen en la Tabla 2-2.

Tabla 2-2 Tipos de estado de la acción

Estado de la acción	Descripción
Equipo	El nombre del equipo que ha generado la alerta.
Estado	El estado de la alerta. El campo Estado puede indicar lo siguiente: que la acción está pendiente, en proceso, ha provocado un error, ha finalizado satisfactoriamente o no ha podido finalizar correctamente.
Nombre de la acción	Un nombre otorgado a la acción específica.
Tipo de acción	El tipo de acción generada por la alerta, por ejemplo, la aparición de un cuadro de mensaje, el envío de un mensaje de buscapersonas, de un mensaje de correo por Internet, de un mensaje de difusión general o la ejecución de programas.

Para ver la información acerca de la alerta y el estado de la acción

1. En la ventana del registro de alertas, haga doble clic en la alerta acerca de la cual desea que se muestre una información detallada.
2. Cuando termine de ver la información acerca de la alerta, haga clic **Cerrar**.

   El equipo que se muestra en el registro de alertas es el servidor primario que registró la acción, ya que éste es el que registra todos los sucesos de su grupo de servidores de Symantec. Para saber qué equipo generó realmente la alerta, haga doble clic en la entrada del registro de alertas sobre la que desea obtener más información. El cuadro de diálogo Información de alerta le proporcionará detalles adicionales acerca de la alerta, incluido el nombre del equipo que la generó.

Cómo filtrar la lista del registro de alertas

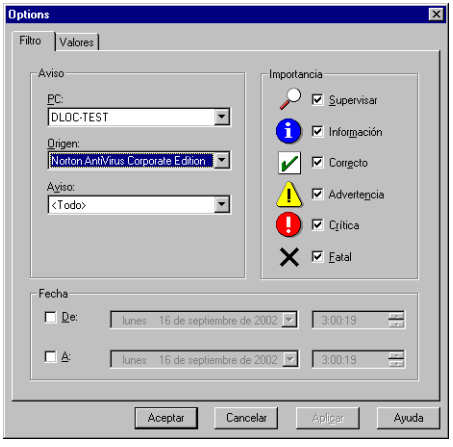
Es posible configurar el registro de alertas para que sólo muestre las alertas que cumplan determinados criterios. Puede filtrar las alertas que se mostrarán de acuerdo con los parámetros que aparecen en la Tabla 2-3.

Tabla 2-3 Filtros del registro de alertas

Filtro	Descripción
Equipo	Muestra las alertas de un equipo en concreto.
Origen	Muestra las alertas provocadas por el mismo suceso en uno o varios equipos.
Alerta	Muestra todas las alertas con un nombre de alerta específico.
Gravedad	Muestra sólo los equipos que cumplan el nivel de gravedad indicado. El administrador puede especificar los siguientes niveles de gravedad: Supervisión, Información, Aceptar, No grave, Muy grave y No recuperable.

Para especificar qué alertas se muestran en el registro de alertas

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** > **Ver registro**.
2. En la ventana Registro de alertas, haga clic con el botón derecho y seleccione a continuación **Opciones**.



3. Seleccione los filtros que desea aplicar a la lista del registro de alertas.
4. Haga clic en **Aceptar**.

Cómo enviar alertas desde los clientes no administrados

Es posible configurar los clientes de Symantec AntiVirus Corporate Edition no administrados para que envíen sus alertas a un servidor de AMS^2.

Para que la alerta se envíe, el equipo cliente debe estar conectado a la red y ser capaz de conectarse con el servidor de AMS.

Para enviar las alertas a un servidor de AMS

1. Utilice un programa de edición de texto, por ejemplo Bloc de notas, para crear un archivo de texto.
2. Copie las siguientes líneas:

```
[KEYS]
!KEY!=$REGROOT$\Common
AMSServer=S<NombredelservidordeAMS>
AMS=D1
!KEY!=$REGROOT$\ProductControl
LoadAMS=D1
```

3. En la línea <NombredelservidordeAMS,> efectúe una de las siguientes acciones:
   - Escriba la dirección IP o IPX del servidor de AMS^2 deseado.
   - Escriba el nombre del servidor de AMS^2 deseado (asegúrese primero de que el cliente puede interpretar el nombre del servidor).

     Asegúrese de mantener la S que precede a <NombredelservidordeAMS.> No incluya los corchetes angulares.
4. Guarde el archivo como Grc.dat en una de las siguientes carpetas del cliente:
   - Para Windows 98 o ME: C:\Archivos de programa\Norton AntiVirus.
   - Para Windows NT: C:\Winnt\Profiles\All Users\Datos de programa\Symantec\Norton AntiVirus Corporate Edition\7.5.
   - Para Windows 2000 o XP: C:\Documents and Settings\All Users\Datos de programa\Symantec\Norton AntiVirus Corporate Edition\7.5.

Una vez creado el archivo de configuración (Grc.dat), se puede copiar a cualquier otro cliente no administrado. Los clientes no administrados enviarán desde ese momento las alertas al mismo servidor de AMS^2.

Sección 2

Configuración de Symantec AntiVirus Corporate Edition

- Análisis de virus
- Actualización de las definiciones de virus
- Respuesta a infecciones víricas
- Administración de clientes de uso móvil
- Trabajo con historias y registros de sucesos

Capítulo 3

Análisis de virus

En este capítulo se tratan los temas siguientes:

- Acerca de los análisis en Symantec AntiVirus Corporate Edition
- Configuración de análisis en tiempo real
- Configuración de análisis manuales
- Configuración de análisis planificados
- Gestión de clientes de Symantec AntiVirus Corporate Edition que se conectan de forma intermitente
- Configuración de opciones de análisis

Acerca de los análisis en Symantec AntiVirus Corporate Edition

Es posible configurar cuatro tipos de análisis desde la consola de Symantec System Center:

- Análisis en tiempo real
- Análisis planificados
- Análisis manuales
- Análisis de archivos adjuntos de correo electrónico para Lotus Notes, Microsoft Exchange y Outlook (MAPI)

Se pueden realizar análisis de los siguientes elementos:

- Uno o varios servidores y clientes de Symantec AntiVirus Corporate Edition
- Grupos de servidores y clientes de Symantec AntiVirus Corporate Edition, mediante la utilización de grupos de servidores

Descripción de los análisis en tiempo real

En los análisis en tiempo real se inspeccionan de forma continua los archivos y los datos de correo electrónico a medida que se leen o se escriben en un equipo. La protección en tiempo real está activada de forma predeterminada. Es posible configurar valores de protección en tiempo real para servidores en grupos de servidores o servidores individuales, y en los clientes de grupos de servidores, de servidores particulares o de grupos de clientes. Cuando se configura la protección en tiempo real, el aspecto de las páginas de configuración varía ligeramente dependiendo de si se están estableciendo opciones para servidores o para clientes. Asimismo se puede bloquear la configuración de la protección en tiempo real en los clientes si se desea implantar una política antivirus determinada. Los usuarios no podrán modificar las opciones que se bloqueen.

Symantec AntiVirus Corporate Edition analiza los datos del correo electrónico sólo en clientes de Symantec AntiVirus Corporate Edition.

Descripción de los análisis planificados

Desde la consola de Symantec System Center, se pueden planificar análisis para servidores o clientes de Symantec AntiVirus Corporate Edition. Los usuarios pueden, asimismo, planificar análisis en sus equipos desde los clientes de Symantec AntiVirus Corporate Edition, pero no pueden cambiar o desactivar análisis que el administrador haya definido para esos equipos. Symantec AntiVirus Corporate Edition ejecuta un análisis planificado cada vez. Si hay más de un análisis planificado al mismo tiempo, se ejecutará uno y después otro.

Cuando se crea y se guarda un análisis planificado, Symantec AntiVirus Corporate Edition almacena el grupo de servidores, el servidor o el equipo en el que se debe ejecutar y todas las opciones seleccionadas para el análisis.

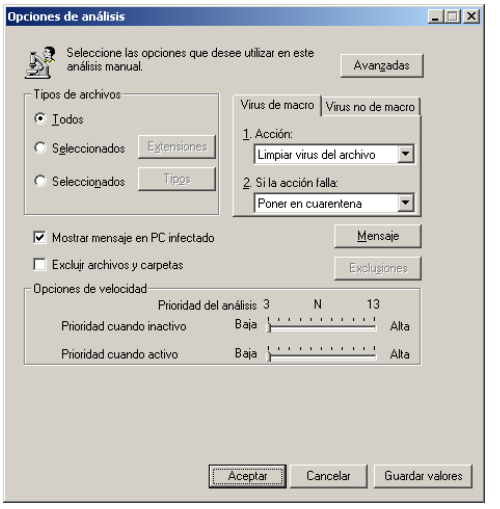
Si un equipo está apagado en el momento en que deba ejecutarse un análisis planificado, éste no se ejecutará a menos que el equipo esté configurado para ejecutar sucesos de análisis no realizados.

Vea "Establecimiento de opciones para análisis planificados no realizados" en la página 105.

Descripción de los análisis manuales

Los análisis manuales son aquellos que se realizan a petición del usuario, en los que se analizan los archivos y carpetas seleccionados de máquinas específicas. Los análisis manuales proporcionan resultados inmediatos de análisis que se efectúan en una pequeña área de la red o en una unidad de disco duro local. Las opciones de análisis se pueden definir en el cuadro de diálogo Opciones de análisis que se muestra en la Figura 3-1.

Figura 3-1 Cuadro de diálogo Opciones de análisis



Selección de equipos para analizar

En Symantec System Center se deben seleccionar los equipos que se desea analizar, lo que determina los tipos de análisis disponibles, el destino de los análisis y las opciones de análisis posibles.

En la Tabla 3-1 se muestra una lista de los distintos tipos de objetos que se pueden analizar.

Tabla 3-1 Elementos que se pueden analizar

Objeto seleccionado	Análisis disponibles
Jerarquía del sistema	Barrido de virus en todos los servidores y clientes de Symantec AntiVirus Corporate Edition de la red
Grupos de servidores múltiples	■ Barrido de virus de todos los servidores y clientes de Symantec AntiVirus Corporate Edition de los grupos de servidores seleccionados ■ Análisis planificado de los servidores de Symantec AntiVirus Corporate Edition seleccionados
Grupo de servidores	■ Barrido de virus de todos los servidores de Symantec AntiVirus Corporate Edition y de sus clientes dentro del grupo de servidores seleccionado ■ Análisis planificado de los servidores de Symantec AntiVirus Corporate Edition pertenecientes al grupo de servidores seleccionado

Tabla 3-1 Elementos que se pueden analizar

Objeto seleccionado	Análisis disponibles
Servidores seleccionados de un grupo de servidores	■ Barrido de virus de los servidores de Symantec AntiVirus Corporate Edition seleccionados ■ Análisis manual de los servidores de Symantec AntiVirus Corporate Edition seleccionados
Servidor individual	■ Barrido de virus del servidor de Symantec AntiVirus Corporate Edition y de todos sus clientes de Symantec AntiVirus Corporate Edition ■ Análisis manual del servidor de Symantec AntiVirus Corporate Edition ■ Análisis planificado del servidor de Symantec AntiVirus Corporate Edition o de sus clientes de Symantec AntiVirus Corporate Edition
Clientes de Symantec AntiVirus Corporate Edition seleccionados de un único servidor de Symantec AntiVirus Corporate Edition	Análisis manual de los clientes de Symantec AntiVirus Corporate Edition seleccionados que son administrados por el servidor de Symantec AntiVirus Corporate Edition
Un cliente de Symantec AntiVirus Corporate Edition concreto	■ Análisis manual del cliente de Symantec AntiVirus Corporate Edition seleccionado ■ Análisis planificado del cliente de Symantec AntiVirus Corporate Edition seleccionado

Nota: La configuración de los clientes se debe bloquear para que se puedan propagar en ellos las opciones de tiempo real configuradas en la consola de Symantec System Center.

Vea "Configuración de análisis en tiempo real" en la página 89.

Definición de opciones de análisis en varios equipos

Cuando se observan las opciones de protección en tiempo real, barrido de virus o análisis manual correspondientes a varios equipos seleccionados, las casillas de verificación y opciones de configuración presentan tres estados que sólo aparecen cuando los equipos tienen diferentes opciones configuradas. Haga clic en la misma opción varias veces para ver los distintos estados.

- Una marca de verificación negra en una casilla de verificación o un punto negro en una opción significan que la opción está seleccionada para todos los equipos del grupo. Al definir una opción en un estado distinto del atenuado, se restablecerá en los equipos seleccionados.
- Una casilla de verificación en blanco indica que la opción no está seleccionada en ninguno de los equipos del grupo. Al definir una opción en un estado distinto del atenuado, se restablecerá en los equipos seleccionados.
- Una marca de verificación atenuada en una casilla atenuada, una serie de opciones vacías o un campo vacío significan que algunos de los equipos del grupo tienen la opción seleccionada y otros no. Al definir una opción en un estado distinto del atenuado, se restablecerá en los equipos seleccionados.

Algunas opciones, como la exclusión de archivos y carpetas, no están disponibles cuando se seleccionan varios equipos, ya que dichas opciones se aplican sólo a un equipo concreto.

Preferencia de opciones de análisis

Los cambios de configuración que se realicen en el nivel del grupo de servidores anulan cualquier modificación efectuada en el nivel del servidor o del grupo de clientes.

Nota: Las opciones de protección en tiempo real funcionan de forma distinta que el resto de opciones de análisis. Las opciones de protección en tiempo real se deben bloquear en el nivel del grupo de servidores o servidor para poder distribuirlas a los clientes.

Vea "Descripción de los análisis en tiempo real" en la página 84.

Configuración de análisis en tiempo real

La configuración del análisis en tiempo real implica las siguientes tareas:

- Configurar la protección en tiempo real de los archivos.
- Configurar el análisis en tiempo real del correo electrónico.
- Determinar las exclusiones.
- Propagar las opciones de análisis en tiempo real a los grupos de servidores, a los servidores de Symantec AntiVirus Corporate Edition individuales y a los clientes de Symantec AntiVirus Corporate Edition de la red.

Configuración de la protección en tiempo real para archivos.

Cuando se configura la protección en tiempo real para los archivos, se selecciona un servidor o un grupo de servidores, se establecen los valores de análisis y se definen las opciones de análisis avanzadas.

Para configurar la protección en tiempo real para los archivos

1. Realice una de las acciones siguientes:
   - Haga clic con el botón derecho en el grupo de servidores o en los servidores de Symantec AntiVirus Corporate Edition que desee configurar y después haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Opciones de protección en tiempo real para servidores**.

     Si selecciona un grupo de servidores, Symantec System Center configurará todos los servidores incluidos en ese grupo.
   - Haga clic con el botón derecho en un solo servidor o en varios servidores y, a continuación, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Opciones de protección en tiempo real para clientes**.
   - Haga clic con el botón derecho en el grupo de servidores o en los servidores con clientes de Symantec AntiVirus Corporate Edition que desee configurar y después haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Opciones de protección en tiempo real para clientes**.

     Symantec System Center configurará todos los clientes asociados al servidor o al grupo de servidores en cuestión.
   - Haga clic con el botón derecho en un solo cliente o en varios clientes seleccionados de un servidor y, a continuación, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Opciones de protección en tiempo real para clientes**.
2. En el cuadro de diálogo Opciones de protección en tiempo real para clientes, asegúrese de que la casilla **Protección en tiempo real del sistema de archivos** esté seleccionada.

3. Establezca las opciones de protección en tiempo real.
   Podrá:
   - Seleccionar tipos y extensiones de archivos para el análisis.
   - Asignar las acciones primarias y secundarias para los virus detectados.
   - Mostrar un mensaje de aviso en los equipos infectados.
   - Excluir del análisis archivos y carpetas.
   - Seleccionar los tipos de unidades para el análisis.
4. Haga clic en **Avanzado**.
   Podrá:
   - Analizar los archivos cuando se modifiquen o se acceda a ellos.
   - Realizar una copia de respaldo de los archivos antes de intentar repararlos como medida de protección de los datos. Los archivos se codificarán y se creará una copia de respaldo de ellos en el directorio de cuarentena. Una vez que se realice la copia de respaldo, deberá restaurarse el archivo para poder acceder de nuevo a él.
   - En el caso de los servidores, determinar si se analizarán o no los archivos comprimidos. De forma predeterminada, los archivos comprimidos no se analizan en los servidores. Si se activa esta opción, podrá determinar los niveles que deben analizarse dentro de los archivos comprimidos. El valor predeterminado es de 3 niveles para los archivos comprimidos.
     En servidores de NetWare, Symantec AntiVirus Corporate Edition podrá analizar hasta tres niveles de compresión como máximo.
5. Haga clic en **Heurísticas** para cambiar el nivel de protección que ofrece la tecnología de análisis heurístico de Bloodhound.
   Esta tecnología puede detectar un alto porcentaje de virus desconocidos aislando y localizando las regiones lógicas de un archivo. Bloodhound analiza entonces la lógica de programa en busca de comportamientos correspondientes a virus.
6. Haga clic en **Aceptar** una vez que haya configurado las opciones que prefiera.

7 Haga clic en **Disquetes** si desea cambiar la configuración definida para el análisis de disquetes.

Seleccione una de las opciones siguientes:

- Buscar virus de arranque en los disquetes al acceder a ellos: Symantec AntiVirus Corporate Edition analiza los discos de la unidad de disquetes para comprobar la existencia de virus de arranque la primera vez que se accede a ella. Cuando se detecte un virus, deberá determinar si desea limpiar el virus del registro de arranque o no hacer nada.

  Si hace clic en la opción No hacer nada (registrar), se enviará una alerta cuando se detecte un virus pero no se llevará a cabo ninguna acción. Utilice esta opción si desea ejercer un control directo sobre el proceso de limpieza y gestión de los virus. Por ejemplo, después de recibir la alerta, podrá decidir el tipo de acciones que desee llevar a cabo.
- No comprobar disquetes al cerrar el sistema: Symantec AntiVirus Corporate Edition omite el análisis de los disquetes que pueda haber en las unidades correspondientes cuando el sistema se cierra normalmente.

8 Sólo en Windows 98, haga clic en **Supervisión** para desactivar la supervisión de actividades víricas.

Las actividades víricas son aquellas que realizan los virus cuando intentan infectar un archivo. Cualquiera de estas actividades puede ser legítima en función del contexto de trabajo. Se puede excluir la supervisión de las siguientes actividades:

- Formateo a bajo nivel del disco duro: toda la información de la unidad se elimina y no se puede recuperar. Este tipo de formateo lo suele realizar el fabricante. Si se detecta esta actividad, normalmente es una indicación de la presencia de un virus. (Esta opción no está disponible en los equipos de NEC PC98xx.)
- Escritura en sector de arranque del disco duro: existen muy pocos programas que escriban en el sector de arranque del disco duro. Esta actividad puede indicar la presencia de un virus desconocido.
- Escritura en sector de arranque del disquete: sólo unos pocos programas (como el comando Format del sistema operativo) escriben en el sector de arranque del disquete. Esta actividad puede indicar la presencia de un virus desconocido.

9 Bloquee las opciones de protección en tiempo real que quiera distribuir a los clientes.

10 Si está configurando opciones de protección en tiempo real para un grupo de servidores, haga clic en **Restablecer todo** para asegurarse de que todos los equipos estén utilizando la configuración de análisis en tiempo real establecida para este nivel.

Vea "Definición y restablecimiento de las opciones de protección en tiempo real" en la página 96.

11 Haga clic en **Aceptar**.

Selección de tipos de unidades para el análisis en tiempo real

Cuando configure opciones de protección en tiempo real para archivos, deberá especificar cuáles de los siguientes tipos de unidades desea que analice Symantec AntiVirus Corporate Edition:

- Unidad de disquetes (sólo Windows 3.1): Symantec AntiVirus Corporate Edition puede analizar archivos que se leen o se escriben en disquetes. Los disquetes son una fuente habitual de infecciones víricas, ya que los usuarios pueden usar disquetes que se hayan infectado en otros equipos, como sus equipos domésticos, por ejemplo.
- Unidad de CD-ROM (sólo Windows 3.1): en ocasiones, algunas empresas de software distribuyen discos CD-ROM que incluyen archivos infectados.
- Unidad de red: si se activa la protección en tiempo real en unidades de red, Symantec AntiVirus Corporate Edition puede analizar los archivos a medida que se escriben desde un cliente en un servidor (o desde un servidor en otro). Esta opción no es necesaria si se activa la protección en tiempo real en los servidores. Por ejemplo, supongamos un cliente A que tiene activado el análisis de unidades de red y un servidor B que tiene activada la protección en tiempo real. Cuando el cliente A escribe un archivo en una unidad de red del servidor B, Symantec AntiVirus Corporate Edition analiza el archivo en el cliente A y lo vuelve a analizar en el servidor B, lo que reduce el rendimiento de la red del equipo cliente.

Establecimiento de opciones avanzadas de protección en tiempo real del sistema de archivos

Hay tres opciones de protección del sistema de archivos que determinan las operaciones de archivo que se supervisan mediante la protección en tiempo real. La Tabla 3-2 recoge y describe estas opciones.

Tabla 3-2 Opciones avanzadas de la protección en tiempo real del sistema de archivos

Opción	Descripción	Cuándo utilizarla
Modificados (analizar al crear)	Se analizan los archivos cuando se escriben, modifican o copian.	Use esta opción para obtener un rendimiento un poco mayor, ya que la protección en tiempo real sólo analiza los archivos cuando se escriben, se modifican o se copian.
Accedidos o modificados (analizar al crear, abrir, mover, copiar o ejecutar).	Se analizan los archivos cuando se escriben, se abren, se mueven, se copian o se ejecutan.	Use esta opción si desea obtener una protección más completa para el sistema de archivos. Tenga en cuenta que esta opción puede repercutir negativamente en el rendimiento, ya que la protección en tiempo real analiza los archivos en todas las operaciones.
Abierto para copia de respaldo	En los equipos en los que se ejecuta Windows NT, 2000 o XP, esta opción hace que se analicen los archivos a los que se accede durante operaciones de copia de respaldo.	Esta opción se debe utilizar si no se ha realizado una búsqueda de virus en los archivos de los que se quieran crear copias de respaldo. El uso de esta opción puede ralentizar significativamente las operaciones de copia de respaldo, ya que se analiza cada uno de los archivos de los que se cree la copia.

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

Symantec AntiVirus Corporate Edition analiza los archivos adjuntos del correo electrónico de forma continua a medida que los datos se leen o se escriben en un equipo. Con el análisis del correo electrónico propio, Symantec AntiVirus Corporate Edition analiza los mensajes en busca de archivos adjuntos infectados cuando se abren.

Symantec AntiVirus Corporate Edition admite el análisis de correo electrónico sólo en clientes de Symantec AntiVirus Corporate Edition.

Para configurar el análisis del correo electrónico

1. En la consola de Symantec System Center, haga clic con el botón derecho en el grupo de servidores o en los servidores que desee configurar y después haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Opciones de protección en tiempo real para clientes**.
2. En la ficha Lotus Notes o Microsoft Exchange del cuadro de diálogo Opciones de protección en tiempo real para clientes, seleccione la casilla **Activar protección en tiempo real**.

   Se puede usar la ficha Microsoft Exchange para configurar Microsoft Exchange y Microsoft Outlook.
3. Establezca las opciones de protección en tiempo real.

   Podrá:

   - Seleccionar los tipos de archivos o las extensiones que desee analizar.
   - Asignar las acciones primarias y secundarias para los virus detectados.
   - Mostrar un mensaje de aviso en los equipos infectados.
   - Insertar un aviso dentro de un mensaje de correo electrónico.
   - Enviar un mensaje de correo electrónico al remitente de un archivo adjunto infectado.
   - Enviar un mensaje de correo electrónico a los destinatarios seleccionados cuando se detecte un virus.
4. Haga clic en **Avanzado** para configurar el análisis de los archivos comprimidos.

5 Establezca las opciones correspondientes y haga clic en **Aceptar**.

6 Bloquee o desbloquee las opciones según sea necesario.

7 Haga clic en **Restablecer todo** para asegurarse de que todos los equipos estén utilizando la configuración para los análisis en tiempo real establecida en un nivel superior.

Vea "Configuración de análisis en tiempo real" en la página 89.

Si su programa de correo electrónico no se admite

Si su sistema de correo electrónico no se encuentra entre los formatos de datos admitidos, podrá seguir protegiendo la red mediante la activación de la protección en tiempo real del sistema de archivos. Por ejemplo, si dispone de un sistema de correo electrónico de Novell GroupWise y uno de sus usuarios recibe un mensaje con un archivo adjunto infectado, Symantec AntiVirus Corporate Edition detectará el virus tan pronto como el usuario intente abrir el archivo adjunto. Esto se debe a que la mayoría de los programas de correo electrónico (como GroupWise) guardan los archivos adjuntos en un directorio temporal cuando se ejecutan desde el programa de correo electrónico. Si activa la protección en tiempo real del sistema de archivos, Symantec AntiVirus Corporate Edition detectará el virus cuando se escriba en el directorio temporal. Asimismo Symantec AntiVirus Corporate Edition detectará el virus si el usuario intenta guardar el archivo adjunto infectado en una unidad local o de red.

Determinación de exclusiones

Las exclusiones permiten equilibrar el nivel de protección que requiere la red y la cantidad de tiempo y recursos necesarios para proporcionar esa protección. Por ejemplo, si se analizan todos los tipos de archivos, se podrán excluir determinadas carpetas que contengan únicamente archivos de datos que no están expuestos a infecciones víricas. Esto hace que disminuya la sobrecarga asociada al análisis de archivos.

Definición y restablecimiento de las opciones de protección en tiempo real

Puede definir y restablecer la configuración de la protección en tiempo real en un grupo de servidores, en un servidor individual o en un grupo de clientes. Cuando defina o restablezca la configuración de la protección en tiempo real, tenga en cuenta las siguientes reglas:

- Cuando se modifican las opciones de protección en tiempo real para servidores de un servidor concreto, es posible transferir una configuración específica a ese servidor, lo que anula las opciones establecidas en el grupo de servidores. Si se restablece la configuración de la protección en tiempo real para servidores en el grupo de servidores, se anulan los cambios realizados en el servidor individual.
- Si se cambia la configuración de la protección en tiempo real para clientes en el nivel del servidor principal o del grupo de clientes, es posible transferir una configuración específica a los clientes de ese servidor principal o grupo de clientes.
  - Si se restablece la configuración de la protección en tiempo real para clientes en el nivel del grupo de servidores, se anulan los cambios realizados en el servidor principal o en el nivel del grupo de clientes para todos los clientes.
  - Al cambiar las opciones de protección en tiempo real para clientes en el nivel del servidor principal, se modifica la configuración de los clientes no asignados a ningún grupo de clientes. Los clientes que estén asignados a un grupo de clientes conservarán su configuración.
- Si se hace clic en Aceptar en el cuadro de diálogo Opciones de protección en tiempo real, sólo se propagan las opciones de configuración que se hayan cambiado o a las que se haya accedido en el cuadro de diálogo. Las opciones de configuración que no se hayan modificado o a las que no se haya accedido no se propagan. Por ejemplo, cuando se configuran las opciones de protección en tiempo real para clientes:
  - Se modifican las opciones de protección en tiempo real del sistema de archivos pero no se cambian las opciones de ninguna otra ficha de configuración o cuadro de diálogo ni se accede a ellas.
  - Se hace clic en Aceptar.
  - Sólo se propagan las opciones de protección en tiempo real del sistema de archivos.
- Si se hace clic en Restablecer todo, se propagan todas las opciones del cuadro de diálogo, independientemente de que se hayan modificado o se haya accedido a ellas o no.

Para definir y restablecer la configuración de la protección en tiempo real

1. Realice una de las siguientes acciones en Symantec System Center:
   - Si desea cambiar la configuración de la protección en tiempo real para servidores, haga clic con el botón derecho en un servidor o en un grupo de servidores y, a continuación, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Opciones de protección en tiempo real para servidores**.
   - Si desea cambiar la configuración de la protección en tiempo real para clientes, haga clic con el botón derecho en un servidor, en un grupo de servidores o en un grupo de clientes y, seguidamente, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Opciones de protección en tiempo real para clientes**.
2. En el cuadro de diálogo Opciones de protección en tiempo real, cambie una o varias opciones.
3. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Bloqueo y desbloqueo de opciones de protección en tiempo real

Los iconos de bloqueo del cuadro de diálogo Opciones de protección en tiempo real permiten controlar los valores de configuración que pueden modificar los usuarios en el cliente de Symantec AntiVirus Corporate Edition. La Tabla 3-3 recoge y describe los iconos de bloqueo.

Tabla 3-3 Bloqueo y desbloqueo de las opciones de protección en tiempo real

Icono	Descripción	Función
	Esta opción está desbloqueada.	Los usuarios pueden modificar las opciones desbloqueadas del cliente de Symantec AntiVirus Corporate Edition.
	Esta opción está bloqueada.	Esta opción no está disponible para los usuarios del cliente de Symantec AntiVirus Corporate Edition.

Configuración de análisis manuales

La configuración de un análisis manual implica las siguientes tareas:

- Seleccionar un cliente o un servidor de Symantec AntiVirus Corporate Edition.
- Seleccionar las carpetas para analizar.
- Especificar las opciones de análisis.
- Especificar las opciones avanzadas.

Nota: Si desea analizar todos los servidores y los clientes de un grupo de servidores, ejecute un barrido de virus o cree un análisis planificado.

Para configurar un análisis manual

1. En la consola de Symantec System Center, realice una de las siguientes acciones:
   - Haga clic con el botón derecho en un servidor o un cliente.
   - Seleccione un solo servidor o varios servidores del mismo grupo de servidores y después haga clic con el botón derecho en ellos.
   - Seleccione un solo cliente o varios clientes administrados por el mismo servidor y, a continuación, haga clic con el botón derecho en ellos.
2. Haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Iniciar análisis manual**.
3. En el cuadro de diálogo Seleccionar elementos, seleccione las carpetas que desee analizar.

   Si va a analizar varios equipos, esta opción no estará disponible. Vaya al paso 5.
4. Haga clic en **Guardar valores** si desea que Symantec AntiVirus Corporate Edition almacene las opciones seleccionadas para utilizarlas en análisis manuales que se realicen en el equipo más adelante.

   Symantec AntiVirus Corporate Edition también puede almacenar estas opciones para utilizarlas en análisis futuros cuando se seleccionen varios equipos.
5. Haga clic en **Opciones**.

6 En el cuadro de diálogo Opciones de análisis, podrá:

- Seleccionar los tipos de archivos o las extensiones que quiera analizar.
- Mostrar un mensaje de aviso en los equipos infectados.
- Excluir archivos y carpetas del análisis. (Esta opción no está disponible para múltiples clientes o servidores.)
- Establecer el uso de la CPU.
- Asignar las acciones primarias y secundarias para los virus detectados.

7 Haga clic en **Avanzadas**.

8 En el cuadro de diálogo Opciones avanzadas de análisis, podrá:

- Determinar si se analizarán o no los archivos comprimidos. Si se activa esta opción, podrá determinar los niveles que deben analizarse dentro de los archivos comprimidos. El valor predeterminado es de 3 niveles para los archivos comprimidos.
- Realizar una copia de respaldo de los archivos antes de intentar repararlos como medida de protección de los datos. Los archivos se codificarán y se realizará una copia de respaldo de ellos en el directorio de cuarentena. Una vez que se realice la copia de respaldo, deberá restaurarse el archivo para poder acceder de nuevo a él.
- Determinar si se mostrará un cuadro de diálogo de progreso en el equipo mientras se realice el análisis. Se puede configurar el cuadro de diálogo de progreso de forma que se cierre automáticamente cuando haya finalizado el análisis. También es posible mostrar u ocultar un botón de detención en el equipo remoto. Cuando esta opción está desactivada, el análisis no se puede detener desde el equipo remoto.
- Activar el análisis de archivos comprimidos en servidores de NetWare.

9 Haga clic en **Aceptar** para guardar las opciones avanzadas.

10 En el cuadro de diálogo Opciones de análisis, haga clic en **Guardar valores** si desea que Symantec AntiVirus Corporate Edition almacene estas opciones para utilizarlas en análisis manuales que se realicen en el equipo más adelante.

Symantec AntiVirus Corporate Edition también puede almacenar estas opciones para utilizarlas en análisis futuros cuando se seleccionen varios equipos.

11 Haga clic en **Aceptar** para continuar con estas opciones.

12 Haga clic en **Iniciar**.

Vea "Establecimiento del uso de la CPU" en la página 132.

Configuración de análisis planificados

La configuración de análisis planificados implica lo siguiente:

- Planificar análisis para los servidores y clientes de Symantec AntiVirus Corporate Edition
- Establecer opciones para análisis no realizados
- Modificar, suprimir o desactivar un análisis o ejecutar un análisis planificado manualmente, si es necesario

Los análisis planificados cuentan con opciones similares a las de los análisis en tiempo real, pero cada tipo de análisis se debe configurar de forma independiente. Por ejemplo, las opciones de exclusión que se definan para análisis en tiempo real sólo afectan a ese tipo de análisis, pero no a los análisis planificados.

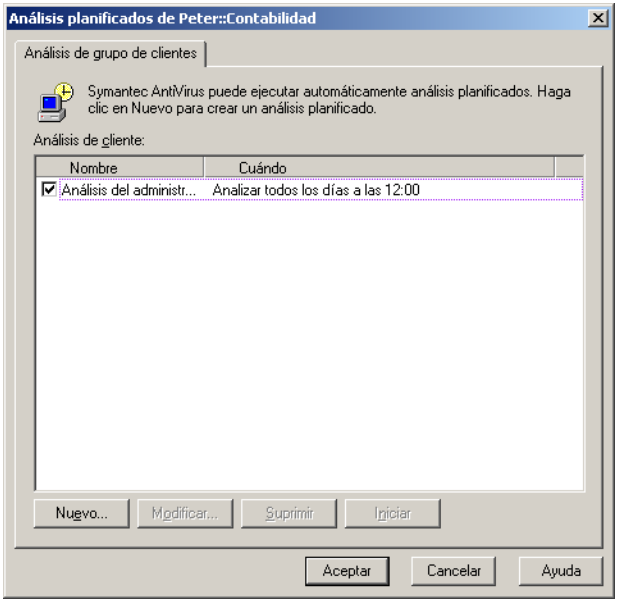
Planificación de análisis para grupos de servidores o servidores individuales de Symantec AntiVirus Corporate Edition

Se pueden planificar análisis para uno o varios grupos de servidores y para servidores individuales de Symantec AntiVirus Corporate Edition.

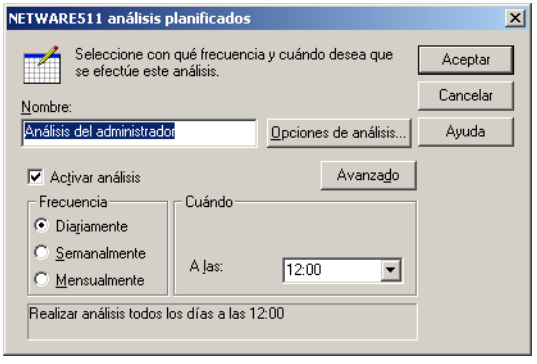
Para planificar un análisis para un grupo de servidores

1. En la consola de Symantec System Center, realice una de las siguientes acciones:
   - En el árbol de la consola, haga clic en **Jerarquía del sistema**. En el panel de la derecha, pulse Mayús o Ctrl y haga clic para seleccionar varios grupos de servidores y, a continuación, haga clic con el botón derecho en la selección.
   - Haga clic con el botón derecho en un grupo de servidores.
   - Haga clic con el botón derecho en un servidor.

2 Haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Análisis planificados**.



3 En la ficha Análisis de grupo de servidores del cuadro de diálogo Análisis planificados, haga clic en **Nuevo**.



4 En el campo Nombre del cuadro de diálogo Análisis planificados, escriba un nombre para el análisis.

5 Establezca una frecuencia para el análisis.

6 Establezca una hora para el análisis.

Es posible introducir cualquier hora en intervalos de 1 minuto o utilizar la lista desplegable para seleccionar una hora en intervalos de 15 minutos.

7. Haga clic en **Avanzado**.
8. En el cuadro de diálogo Opciones de planificación avanzadas, seleccione **Gestionar sucesos no realizados a** y establezca el límite de tiempo dentro del cual desea que se ejecute el análisis.

   Por ejemplo, puede que le interese que un análisis semanal se ejecute sólo si se produce en los tres días siguientes a la hora planificada para el suceso no realizado.
9. Haga clic en **Aceptar**.
10. En el cuadro de diálogo Análisis planificados, haga clic en **Opciones de análisis**.
11. En el cuadro de diálogo Seleccionar elementos, haga clic en **Opciones**.
12. En el cuadro de diálogo Opciones de análisis planificados, podrá:
    - Seleccionar tipos y extensiones de archivos para el análisis.
    - Mostrar un mensaje de aviso en el equipo infectado.
    - Excluir archivos del análisis por extensión de archivo.
    - Establecer el uso de la CPU.
    - Asignar las acciones primarias y secundarias para los virus detectados.
13. Haga clic en **Avanzadas**.
14. En el cuadro de diálogo Opciones avanzadas de análisis, podrá:
    - Mostrar una ventana de progreso del análisis en el equipo que se esté analizando.
    - Cerrar la ventana de progreso del análisis en el equipo cuando termine su ejecución.
    - Realizar una copia de respaldo de los archivos antes de intentar repararlos como medida de protección de los datos. Los archivos se codificarán y se creará una copia de respaldo de ellos en el directorio de cuarentena. Una vez que se realice la copia de respaldo, deberá restaurarse el archivo para poder acceder de nuevo a él.
    - Establecer opciones para el análisis de archivos comprimidos.
15. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

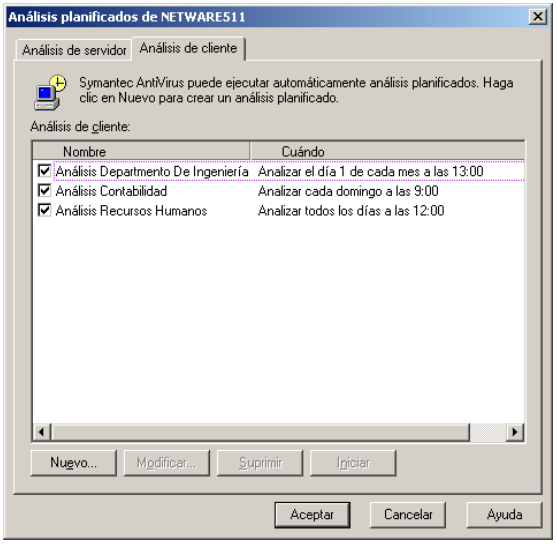
Vea "Configuración de opciones de análisis" en la página 110.

Planificación de análisis para clientes de Symantec AntiVirus Corporate Edition

Es posible planificar análisis para clientes de Symantec AntiVirus Corporate Edition en el nivel del servidor o del cliente de Symantec AntiVirus Corporate Edition.

Para planificar análisis para clientes de Symantec AntiVirus Corporate Edition

1. En la consola de Symantec System Center, haga clic con el botón derecho en un servidor o en un cliente concreto y, a continuación, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Análisis planificados**.
2. En la ficha Análisis de cliente del cuadro de diálogo Análisis planificados, haga clic en **Nuevo**.



3. En el campo Nombre del cuadro de diálogo Análisis planificados, escriba un nombre para el análisis.
4. Establezca una frecuencia para el análisis.
5. Establezca una hora para el análisis.

   Es posible introducir cualquier hora en intervalos de 1 minuto o utilizar la lista desplegable para seleccionar una hora en intervalos de 15 minutos.
6. Haga clic en **Avanzado**.

7. En el cuadro de diálogo Opciones de planificación avanzadas, seleccione la casilla **Gestionar sucesos no realizados a** y establezca el límite de tiempo dentro del que desee que se realice el análisis.

   Por ejemplo, puede que le interese que un análisis semanal se ejecute sólo si se produce en los tres días siguientes a la hora planificada para el suceso no realizado.

8. Haga clic en **Aceptar**.
9. En el cuadro de diálogo Análisis planificados, haga clic en **Opciones de análisis**.
10. Seleccione las carpetas que desee analizar. Esta opción no está disponible cuando se analizan varios equipos, ya que las carpetas son específicas de cada uno de ellos.
11. Haga clic en **Opciones**.
12. En el cuadro de diálogo Opciones de análisis planificados, podrá:
    - Seleccionar tipos y extensiones de archivos para el análisis.
    - Mostrar un mensaje de aviso en los equipos infectados.
    - Excluir archivos del análisis por tipo de archivo o por unidad y carpeta.
    - Establecer el uso de la CPU.
    - Asignar las acciones primarias y secundarias para los virus detectados.
13. Haga clic en **Avanzadas**.
14. En el cuadro de diálogo Opciones avanzadas de análisis, podrá:
    - Mostrar una ventana de progreso del análisis en el equipo que se esté analizando.
    - Cerrar la ventana de progreso del análisis en el equipo cuando termine su ejecución.
    - Realizar una copia de respaldo de los archivos antes de intentar repararlos como medida de protección de los datos. Los archivos se codificarán y se creará una copia de respaldo de ellos en el directorio de cuarentena. Una vez que se realice la copia de respaldo, deberá restaurarse el archivo para poder acceder de nuevo a él.
    - Establecer opciones para el análisis de archivos comprimidos.
15. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Vea "Configuración de opciones de análisis" en la página 110.

Establecimiento de opciones para análisis planificados no realizados

Si no se realiza un análisis planificado en un equipo (porque esté apagado, por ejemplo), Symantec AntiVirus Corporate Edition intentará llevar a cabo el análisis durante un intervalo de tiempo determinado. Si Symantec AntiVirus Corporate Edition no puede iniciar el análisis en ese intervalo, no lo llevará a cabo. Los intervalos de tiempo predeterminados son:

- Análisis diarios: 8 horas
- Análisis semanales: 3 días
- Análisis mensuales: 11 días

Se puede especificar un intervalo de tiempo para intentar realizar un análisis planificado.

Para establecer opciones para análisis planificados no realizados

1. En Symantec System Center, haga clic con el botón derecho en un servidor, un grupo de servidores, un grupo de clientes o un único cliente de Symantec AntiVirus Corporate Edition y después haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Análisis planificados**.
2. En el cuadro de diálogo Análisis planificados, seleccione un análisis de la lista.
3. Haga clic en **Modificar**.
4. En el cuadro de diálogo Análisis planificado, haga clic en **Avanzado**.
5. En el cuadro de diálogo Opciones de planificación avanzadas, haga clic en **Gestionar sucesos no realizados a**.
6. Determine el intervalo de tiempo que debe transcurrir antes de volver a intentar realizar el análisis planificado.
7. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Modificación, supresión o desactivación de análisis planificados

Si desea modificar las propiedades de un análisis planificado existente, podrá editarlo. Si no desea que se lleve a cabo un análisis planificado, podrá suprimirlo o desactivarlo.

Modificación, supresión o desactivación de análisis planificados

Es posible modificar, suprimir o desactivar análisis planificados.

Para modificar o suprimir un análisis planificado

1. En la consola de Symantec System Center, haga clic con el botón derecho en uno o en varios grupos de servidores, en un servidor o en un cliente del que desee modificar o suprimir un análisis planificado y, a continuación, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Análisis planificados**.
2. En el cuadro de diálogo Análisis planificados, seleccione una de las siguientes opciones:
   - Análisis de servidor: permite modificar o suprimir análisis de servidores. Esta opción no está disponible si se selecciona un equipo cliente en el paso 1.
   - Análisis de cliente: permite modificar o suprimir análisis de clientes. Esta opción no está disponible si se ha seleccionado un grupo de servidores en el paso 1.
3. Realice una de las acciones siguientes:
   - Seleccione un análisis existente y haga clic en **Modificar**. Cambie las propiedades que desee y haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.
   - Seleccione un análisis existente y haga clic en **Suprimir**. Haga clic en **Aceptar** hasta que aparezca la pantalla principal de Symantec System Center.

Para desactivar un análisis planificado

1. En la consola de Symantec System Center, haga clic con el botón derecho en uno o en varios grupos de servidores, en un servidor o en un cliente del que desee desactivar un análisis planificado y, a continuación, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Análisis planificados**.

   Los análisis que se pueden desactivar dependen del objeto que se seleccione.
2. En el cuadro de diálogo Análisis planificados, seleccione una de las siguientes opciones:
   - Análisis de servidor: permite desactivar los análisis de servidores. Esta opción no está disponible si se selecciona un equipo cliente en el paso 1.
   - Análisis de cliente: permite desactivar los análisis de clientes. Esta opción no está disponible si se ha seleccionado un grupo de servidores en el paso 1.
3. Elimine la marca del análisis previamente planificado.
4. Haga clic en **Aceptar**.

Ejecución manual de un análisis planificado

Cuando se crea y se guarda un análisis planificado, Symantec AntiVirus Corporate Edition almacena el grupo de servidores, el servidor o el equipo en el que se debe ejecutar y todas las opciones seleccionadas para el análisis.

Después de configurar un análisis planificado (con todas sus propiedades), puede que le interese ejecutarlo de forma manual en un momento distinto del elegido en un principio. Esto permite ahorrar esfuerzo en la configuración y ejecución de un análisis manual con propiedades similares.

Para ejecutar manualmente un análisis planificado

1. En la consola de Symantec System Center, haga clic con el botón derecho en un grupo de servidores o en un servidor y, a continuación, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Análisis planificados**.
2. En el cuadro de diálogo Análisis planificados, seleccione una de las siguientes opciones:
   - Análisis de servidor: permite ejecutar un análisis de servidor manualmente. Esta opción no está disponible si se ha seleccionado un grupo de servidores en el paso 1.
   - Análisis de cliente: permite ejecutar un análisis de cliente manualmente. Esta opción no está disponible si se ha seleccionado un grupo de servidores en el paso 1.

3 Seleccione un análisis planificado existente.

4 Haga clic en **Iniciar.**

Gestión de clientes de Symantec AntiVirus Corporate Edition que se conectan de forma intermitente

Cada servidor de Symantec AntiVirus Corporate Edition almacena una lista de los clientes de Symantec AntiVirus Corporate Edition que administra y proporciona esta información a Symantec System Center. De forma predeterminada, los clientes se verifican en el servidor principal correspondiente cada hora, y los servidores principales revisan su lista de clientes cada hora. Los servidores principales realizan un seguimiento de los tiempos de verificación de los clientes. Si un cliente no se verifica en el servidor principal durante más de tres días, el servidor principal lo elimina de su lista de clientes y lo registra como eliminado. Cuando la consola de Symantec System Center vuelva a solicitar al servidor principal la lista de sus clientes, ese cliente no estará incluido en ella.

Este comportamiento se puede controlar configurando las siguientes opciones:

- El intervalo que debe transcurrir para anular el cliente
- El intervalo de verificación de los clientes

Gestión de clientes de Symantec AntiVirus Corporate Edition que se conectan de forma intermitente

De forma predeterminada, el intervalo de verificación del cliente está establecido en 60 minutos, aunque es posible modificarlo mediante el valor de registro CheckConfigMinutes.

El intervalo para anular el cliente debe ser superior al intervalo de verificación porque, de lo contrario, el servidor principal eliminará y agregará clientes continuamente.

Si el servidor principal o el cliente no reciben la nueva configuración inmediatamente, ésta se actualizará durante el siguiente proceso de verificación del cliente.

Para modificar el intervalo de anulación de los clientes

1. En el servidor principal, localice la siguiente clave del registro:
   HKEY_LOCAL_MACHINE\Software\Intel\LANDesk\VirusProtect6\CurrentVersion
2. En el menú Edición, haga clic en **Nuevo** > **Valor DWORD**.
3. Establezca el siguiente nombre para ese valor:
   ClientExpirationTimeout
4. Haga clic con el botón derecho en la nueva clave y, a continuación, en **Modificar**.
5. En el cuadro de texto Información del valor, sustituya el cero por un número mayor.
   Si no se utiliza el valor ClientExpirationTimeout, el plazo predeterminado es de 720 horas. Utilice un valor más pequeño para reducir el número de minutos que deben transcurrir antes de que el cliente se elimine de la consola, o un valor mayor para aumentar el tiempo. Por ejemplo, si se da el caso de que se elimina un gran número de equipos cliente de Symantec System Center debido a que los usuarios se encuentran fuera de la oficina y los equipos están apagados, puede especificar un número mayor.
6. Haga clic en **Aceptar**.
7. Salga del Editor del registro.

Para modificar el intervalo de verificación de los clientes

1. En la consola de Symantec System Center, haga clic con el botón derecho en un servidor, un grupo de servidores o un grupo de clientes y, a continuación, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Administrador de definiciones de virus**.
2. En el cuadro de diálogo Administrador de definiciones de virus, seleccione la opción **Actualizar definiciones de virus del servidor principal**.
3. Haga clic en **Opciones**.
4. En el cuadro Buscar actualizaciones cada del cuadro de diálogo Configuración de actualización, escriba el intervalo en minutos.
5. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Configuración de opciones de análisis

Muchas de las opciones están disponibles en distintos tipos de análisis. Por ejemplo, se pueden asignar acciones primarias y secundarias al configurar análisis manuales, planificados o en tiempo real.

Asignación de acciones primarias y secundarias para los virus detectados

Se puede asignar tanto la acción primaria como la acción secundaria, en caso de que la primaria no pueda realizarse, que Symantec AntiVirus Corporate Edition deberá llevar a cabo cuando descubra un virus. Es posible asignar acciones distintas para los virus de macro y los que no sean de macro.

Se pueden asignar las siguientes acciones para los virus detectados:

- Limpiar virus del archivo: se intentará limpiar el archivo infectado tras la detección.
- Poner en cuarentena: se intentará mover el archivo infectado al área de cuarentena del equipo infectado tan pronto como se detecte. Cuando un archivo se mueve al área de cuarentena, ningún usuario podrá ejecutarlo hasta que se lleve a cabo una acción (por ejemplo, limpiarlo o suprimirlo) y se vuelva a colocar en su ubicación inicial.
- Suprimir archivo infectado: se intentará suprimir el archivo. Utilice esta opción solamente si puede reemplazar el archivo infectado por una copia de respaldo libre de virus de éste, ya que el archivo se suprimirá de forma permanente y no se podrá recuperar de la Papelera.
- No hacer nada (registrar): impide que se acceda al archivo, muestra un aviso de virus y registra el suceso. Use esta opción para controlar el modo en que se trata un virus. Cuando se le notifique la presencia de un virus, abra la Historia de virus del equipo, haga clic con el botón derecho en el nombre del archivo infectado, y elija una de las siguientes acciones: Limpiar, Suprimir permanentemente o Poner en cuarentena.

De forma predeterminada Symantec AntiVirus Corporate Edition intenta en primer lugar limpiar el archivo. Si Symantec AntiVirus Corporate Edition no puede limpiar el archivo, lo coloca en el área de cuarentena del equipo infectado, impide el acceso al archivo y registra el suceso.

Control de las posibilidades del usuario

Symantec AntiVirus Corporate Edition permite controlar diversos aspectos de las acciones que puede realizar el usuario del cliente de Symantec AntiVirus Corporate Edition. Es posible establecer cualquiera de las opciones siguientes:

- Impedir o permitir que los usuarios descarguen Symantec AntiVirus Corporate Edition.
- Solicitar una contraseña antes de permitir la desinstalación de un componente.
- Permitir a los usuarios interrumpir o detener análisis planificados.
- Mostrar una ventana de progreso de los análisis.
- Mostrar y personalizar un mensaje de aviso en un equipo infectado.
- Agregar un aviso de infección a un mensaje de correo electrónico.
- Notificar al remitente de un mensaje de correo electrónico infectado.
- Notificar a otros usuarios la recepción de un mensaje de correo electrónico infectado.

Prohibición o permiso para descargar Symantec AntiVirus Corporate Edition

Es posible impedir o permitir que los usuarios descarguen Symantec AntiVirus Corporate Edition.

Para impedir o permitir que los usuarios descarguen Symantec AntiVirus Corporate Edition

1. En Symantec System Center, haga clic con el botón derecho en un servidor, un grupo de servidores o un grupo de clientes y haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Opciones exclusivas para administradores de clientes**.
2. Haga clic en la pestaña Seguridad.
3. Cambie la opción seleccionada para **Bloquear la posibilidad de los usuarios de descargar servicios de Symantec AntiVirus**.
4. Haga clic en **Aceptar**.

Solicitud de una contraseña de desinstalación

Es posible hacer que Symantec AntiVirus Corporate Edition solicite una contraseña para que se pueda desinstalar un componente.

Para solicitar una contraseña de desinstalación

1. En Symantec System Center, haga clic con el botón derecho en un servidor, un grupo de servidores o un grupo de clientes y haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Opciones exclusivas para administradores de clientes**.
2. Haga clic en la pestaña Seguridad.
3. Marque la casilla **Solicitar contraseña para desinstalar el cliente de Symantec AntiVirus**.
4. Haga clic en **Cambiar**.
5. En el cuadro de diálogo Configuración de contraseña, introduzca la nueva contraseña y vuelva a escribirla para confirmarla.
6. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Permiso para que los usuarios interrumpan, pospongan o detengan análisis planificados

Puede permitir a los usuarios que interrumpan de forma temporal un análisis planificado, que lo pospongan o que lo detengan por completo. Se producen los siguientes resultados:

- Análisis interrumpido: cuando se interrumpe el análisis, el cuadro de diálogo de resultados del análisis permanece abierto, en espera de que el usuario reanude o cancele el análisis. Si se apaga el equipo, el análisis interrumpido no continuará.
- Análisis pospuesto: cuando se pospone un análisis planificado, existe la opción de aplazarlo durante una hora o durante tres horas (en función de la configuración). Además, es posible configurar el número de veces que se puede posponer un análisis. Cuando se pospone un análisis, el cuadro de diálogo de resultados se cierra y reaparece cuando finaliza el período de aplazamiento y se reanuda el análisis.

Permiso para que los usuarios interrumpan, pospongan o detengan análisis

Los análisis interrumpidos se reanudan automáticamente una vez que transcurre el intervalo de tiempo especificado. Sin embargo, los análisis que se hayan detenido no se reanudan.

Para permitir a los usuarios interrumpir o posponer análisis

1. En Symantec System Center, haga clic con el botón derecho en un grupo de servidores, un servidor o un grupo de clientes y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Análisis planificados**.
2. En el cuadro de diálogo Análisis planificados, realice una de las acciones siguientes:
   - Seleccione un análisis planificado y haga clic en **Modificar**.
   - Haga clic en **Nuevo** para crear un nuevo análisis.
3. En el cuadro de diálogo Análisis planificados, haga clic en **Opciones de análisis**.
4. En el cuadro de diálogo Seleccionar elementos, haga clic en **Opciones**.
5. En el cuadro de diálogo Opciones de análisis planificados, haga clic en **Avanzadas**.
6. En el cuadro de diálogo Opciones avanzadas de análisis, haga clic en **Mostrar estado en los sistemas que se estén analizando**.
7. Quite la marca de la casilla **Permitir al usuario detener el análisis**.
8. Seleccione la casilla **Permitir al usuario interrumpir/posponer el análisis**.
9. Haga clic en **Opciones de pausa del análisis**.
10. 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**.
11. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Para permitir a los usuarios detener análisis

1. En Symantec System Center, haga clic con el botón derecho en un servidor, un grupo de servidores o un grupo de clientes y, después, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Análisis planificados**.
2. En el cuadro de diálogo Análisis planificados, realice una de las acciones siguientes:
   - Seleccione un análisis planificado y haga clic en **Modificar**.
   - Haga clic en **Nuevo** para crear un nuevo análisis.
3. En el cuadro de diálogo Análisis planificados, haga clic en **Opciones de análisis**.
4. En el cuadro de diálogo Seleccionar elementos, haga clic en **Opciones**.
5. En el cuadro de diálogo Opciones de análisis planificados, haga clic en **Avanzadas**.
6. En el cuadro de diálogo Opciones avanzadas de análisis, haga clic en **Mostrar estado en los sistemas que se estén analizando**.
7. Marque la opción **Permitir al usuario detener el análisis**.
8. Quite la marca de la casilla **Permitir al usuario interrumpir/posponer el análisis**.
9. Si desea que el indicador de progreso se cierre automáticamente tras el análisis, seleccione **Cerrar la ventana de progreso del análisis al terminar**.
10. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Visualización y personalización de mensajes de aviso en los equipos infectados

Cuando se ejecuta un análisis remoto en el equipo de un usuario, se le puede notificar inmediatamente cualquier problema mostrando un mensaje de aviso en la pantalla del equipo infectado. Se puede personalizar el mensaje incluyendo información como el nombre del virus, el nombre del archivo infectado, el estado de la infección, etc.

El mensaje de aviso predeterminado contiene variables de mensaje y texto. Las variables de mensaje aparecen entre corchetes. Todo lo que se encuentre fuera de los corchetes constituye texto. Es posible cambiar el texto y las variables de mensaje incluidos en el mensaje de aviso para que éste se adapte a sus necesidades. La Tabla 3-4 describe las variables de mensaje.

Tabla 3-4 Variables de mensaje de aviso

Variable	Texto
[RegistradoPor]	Tipo de análisis que ha registrado el suceso: en tiempo real, planificado o manual.
[Suceso]	Tipo de suceso, como Virus detectado, por ejemplo.
[NombreDeVirus]	Nombre del virus detectado.
[RutaYNombreDeArchivo]	Ruta completa y nombre del archivo.
[Ubicación]	Ubicación de la unidad en el equipo infectado.
[PC]	Nombre del equipo.
[Usuario]	Nombre de inicio de sesión en la red del usuario.
[AcciónEfectuada]	Acción que se ha llevado a cabo en el archivo infectado (por ejemplo, limpiar el archivo, ponerlo en cuarentena, suprimirlo o no hacer nada).
[FechaDeDetección]	Fecha y hora en que se encontró el virus.
[Estado]	Estado del archivo: Infectado, No infectado o Suprimido. (Esta variable de mensaje no se usa de forma predeterminada. Si desea que se muestre esta información, deberá añadir esta variable de mensaje de forma manual al mensaje de aviso.)

Por ejemplo, un mensaje de aviso podría tener el siguiente aspecto:

```
Tipo de análisis: Análisis planificado
Suceso: Virus detectado
Nombre del virus: Stoned-C
Archivo: C:\Autoexec.bat
Ubicación: C:
PC: ACCTG-2
Usuario: JSerrano
Acción efectuada: Limpiado
```

Para mostrar y personalizar un mensaje de aviso en un equipo infectado

1. En la consola de Symantec System Center, haga clic con el botón derecho en un grupo de servidores, en un servidor de Symantec AntiVirus Corporate Edition o en un grupo de clientes y, a continuación, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Opciones de protección en tiempo real para clientes**.
2. En el cuadro de diálogo Opciones de protección en tiempo real para clientes, haga clic en **Mostrar mensaje en PC infectado**.
3. Realice una de las acciones siguientes:
   - Haga clic en **Aceptar** para aceptar el mensaje predeterminado.
   - Haga clic en **Mensaje** y personalice el texto. Después, haga clic en **Aceptar**.
4. Haga clic en **Aceptar** hasta que desaparezca el cuadro de diálogo Opciones de protección en tiempo real para clientes.

Inserción de un aviso de infección en un mensaje de correo electrónico infectado

Para los programas de correo electrónico admitidos, se puede configurar la protección en tiempo real con el fin de insertar un aviso en el cuerpo de los mensajes de correo electrónico infectados. Este tipo de advertencia resulta fundamental si Symantec AntiVirus Corporate Edition no puede limpiar el virus del mensaje y si el archivo adjunto infectado se mueve, se suprime, se cambia de nombre o se ignora. El aviso informa sobre el virus encontrado y detalla la acción que se ha llevado a cabo.

Symantec AntiVirus Corporate Edition añade el siguiente texto al principio del mensaje de correo electrónico que contiene el archivo infectado:

Symantec AntiVirus Corporate Edition ha detectado un virus en un archivo adjunto procedente de [RemitenteDeCorreo].

Asimismo, se añade al mensaje la siguiente información relativa a cada archivo infectado:

- Nombre del archivo adjunto
- Nombre del virus
- Acción que se ha llevado a cabo (por ejemplo, limpiar el archivo, ponerlo en cuarentena, suprimirlo o no hacer nada)
- Estado del archivo (infectado o no infectado)

Se pueden personalizar el asunto y el cuerpo del mensaje.

El mensaje incluye el campo [RemitenteDeCorreo]. Todos los campos que aparecen entre corchetes contienen información variable. Si lo desea, puede personalizar el aviso predeterminado haciendo clic en el mensaje con el botón derecho y seleccionando los campos que desee insertar.

El aviso aparecerá ante el destinatario de la siguiente forma:

Symantec AntiVirus Corporate Edition ha detectado un virus en un archivo adjunto procedente de Juan.Serrano@miempresa.com.

Para insertar un aviso de infección en un mensaje de correo electrónico infectado

1. En la consola de Symantec System Center, haga clic con el botón derecho en un grupo de servidores, en un servidor de Symantec AntiVirus Corporate Edition o en un grupo de clientes y, a continuación, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Opciones de protección en tiempo real para clientes**.
2. En las fichas Lotus Notes o Microsoft Exchange del cuadro de diálogo Opciones de protección en tiempo real para clientes, haga clic en **Insertar aviso en mensaje de correo**.
3. Realice una de las acciones siguientes:
   - Haga clic en **Aceptar** para aceptar el aviso predeterminado.
   - Haga clic en **Aviso** y personalice el texto; después, haga clic en **Aceptar**.
4. Haga clic en **Aceptar** hasta que desaparezca el cuadro de diálogo Opciones de protección en tiempo real para clientes.

Notificación al remitente de un mensaje de correo electrónico infectado

Para los programas de correo electrónico admitidos, se pueden configurar opciones de protección en tiempo real con el fin de responder automáticamente al remitente de un mensaje de correo que contiene un archivo adjunto infectado.

Symantec AntiVirus Corporate Edition envía un mensaje de correo electrónico de respuesta con el asunto:

Virus detectado en el mensaje "[AsuntoDelMensaje]"

El cuerpo del mensaje comunica quién envió el archivo adjunto infectado:

Symantec AntiVirus Corporate Edition ha detectado un virus en un archivo adjunto que [RemitenteDeCorreo] envió a [ListaDeDestinatarios].

Asimismo, se añade al mensaje la siguiente información relativa a cada archivo infectado:

- Nombre del archivo adjunto
- Nombre del virus
- Acción que se ha llevado a cabo (por ejemplo, limpiar el archivo, ponerlo en cuarentena, suprimirlo o no hacer nada)
- Estado del archivo (infectado o no infectado)

Para notificar al remitente de un mensaje de correo electrónico infectado

1. En la consola de Symantec System Center, haga clic con el botón derecho en un grupo de servidores, en un servidor de Symantec AntiVirus Corporate Edition o en un grupo de clientes y, a continuación, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Opciones de protección en tiempo real para clientes**.
2. En las fichas Lotus Notes o Microsoft Exchange del cuadro de diálogo Opciones de protección en tiempo real para clientes, haga clic en **Protección en tiempo real para Lotus Notes** (**Microsoft Exchange**).
3. Haga clic en **Enviar mensaje al remitente**.
4. Haga clic en **Mensaje**.
5. Realice una de las acciones siguientes:
   - Haga clic en **Aceptar** para aceptar el mensaje predeterminado.
   - Haga clic en **Mensaje** y personalice el texto; después, haga clic en **Aceptar**.
6. Haga clic en **Aceptar** hasta que desaparezca el cuadro de diálogo Opciones de protección en tiempo real para clientes.

Notificación a otros usuarios sobre la recepción de un mensaje de correo electrónico infectado

Para los programas de correo electrónico admitidos, se puede configurar la protección en tiempo real con el fin de notificar a otros usuarios cuando se abra un mensaje de correo que contenga un archivo adjunto infectado.

Symantec AntiVirus Corporate Edition envía a los destinatarios seleccionados un mensaje de correo electrónico con el asunto:

Virus detectado en el mensaje "[AsuntoDelMensaje]"

El cuerpo del mensaje informa sobre la identidad del remitente del archivo adjunto infectado:

Symantec AntiVirus Corporate Edition ha detectado un virus en un archivo adjunto procedente de [RemitenteDeCorreo].

Asimismo, se añade al mensaje la siguiente información relativa a cada archivo infectado:

- Nombre del archivo adjunto
- Nombre del virus
- Acción que se ha llevado a cabo (por ejemplo, limpiar el archivo, ponerlo en cuarentena, suprimirlo o no hacer nada)
- Estado del archivo (infectado o no infectado)

Para notificar a otros usuarios la existencia de un mensaje de correo electrónico infectado

1. En la consola de Symantec System Center, haga clic con el botón derecho en un grupo de servidores, en un servidor de Symantec AntiVirus Corporate Edition o en un grupo de clientes y, a continuación, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Opciones de protección en tiempo real para clientes**.
2. En las fichas Lotus Notes o Microsoft Exchange del cuadro de diálogo Opciones de protección en tiempo real para clientes, haga clic en **Protección en tiempo real para Lotus Notes** (**Microsoft Exchange**).
3. Haga clic en **Enviar mensaje a los seleccionados**.
4. Haga clic en **Direcciones**.
5. En el cuadro de diálogo Dirección de correo electrónico, introduzca una o varias direcciones de correo electrónico a las que se enviará la notificación.
6. Haga clic en **Aceptar**.
7. Haga clic en **Mensaje**.
8. Realice una de las acciones siguientes:
   - Haga clic en **Aceptar** para aceptar el mensaje predeterminado.
   - Haga clic en **Crear** y personalice el mensaje; después, haga clic en **Aceptar**.
9. Haga clic en **Aceptar** hasta que desaparezca el cuadro de diálogo Opciones de protección en tiempo real para clientes.

Exclusión de archivos en los análisis

Las exclusiones permiten equilibrar el nivel de protección que requiere la red y la cantidad de tiempo y recursos necesarios para proporcionar esa protección. Por ejemplo, si se analizan todos los tipos de archivos, se podrán excluir determinadas carpetas que contengan únicamente archivos de datos que no están expuestos a infecciones víricas. Esto hace que disminuya la sobrecarga asociada al análisis de archivos.

Mediante Symantec System Center se pueden definir exclusiones para extensiones de archivos y carpetas específicas. Además, determinados análisis de Symantec AntiVirus Corporate Edition permiten excluir carpetas por nombre (por ejemplo, se puede excluir del análisis la ruta C:\Temp\Install). Para mantener la seguridad, no es posible ver o excluir archivos específicos desde Symantec System Center. Aunque sí se puede, por el contrario, excluir archivos específicos desde la interfaz de usuario del cliente o servidor de Symantec AntiVirus Corporate Edition. Puede que desee excluir archivos que originen alertas de falsos positivos. Por ejemplo, si ha utilizado un programa de análisis de virus distinto para limpiar archivos infectados y el programa no ha eliminado completamente el código del virus, puede que el archivo sea inofensivo, pero que el código de virus desactivado haga que Symantec AntiVirus Corporate Edition registre un falso positivo. Consulte con el soporte técnico de Symantec si no está seguro de que un archivo esté infectado. La Tabla 3-5 describe las exclusiones.

Tabla 3-5 Exclusiones por tipo de objeto

Tipo de objeto	Exclusiones disponibles
Grupo de servidores	Análisis de servidor: extensiones de archivos y carpetas por nombre
Servidor	■ Análisis de servidor: extensiones de archivos, unidades, archivos y carpetas ■ Análisis de cliente: extensiones de archivos, unidades y carpetas por nombre
Grupo de clientes	Análisis de cliente: extensiones de archivos, unidades y carpetas por nombre
Servidores de NetWare	Archivos por unidades y carpetas por nombre; no se pueden excluir archivos por extensiones

Definición de exclusiones

Symantec AntiVirus Corporate Edition comprueba las exclusiones especificadas antes o después de que se ejecute el análisis:

- Si las exclusiones se aplican antes del análisis, los elementos excluidos no se analizarán. Si el archivo no está excluido, se analiza.
- Cuando se aplican las exclusiones después de que se haya ejecutado el análisis, solamente se presentará información sobre los virus encontrados si los archivos afectados no se han excluido. En los análisis en tiempo real, Symantec AntiVirus Corporate Edition no realiza ninguna acción en los archivos excluidos.
- En los barridos de virus y en los análisis manuales, en tiempo real y planificados, Symantec AntiVirus Corporate Edition no realiza ninguna acción en los archivos excluidos.

Tanto la activación como la desactivación de las exclusiones previas al análisis pueden mejorar el rendimiento en función de la situación. Por ejemplo:

- Si se copia una carpeta de gran tamaño incluida en la lista de exclusiones y las exclusiones previas al análisis están activadas, el proceso de copia no llevará mucho tiempo, ya que el contenido de la carpeta se excluirá antes del análisis.
- Si se copia una carpeta de gran tamaño que no se encuentre en la lista de exclusiones, la desactivación de las exclusiones previas al análisis mejorará el rendimiento.

Para definir exclusiones

1. En el cuadro de diálogo de opciones correspondiente al tipo de análisis que desee configurar, haga clic en **Excluir archivos y carpetas**.
2. Haga clic en **Exclusiones**.
3. En el cuadro de diálogo Exclusiones, marque la casilla **Comprobar exclusiones antes del análisis** para activar las exclusiones previas al análisis.
4. En función del tipo y del número de equipos que se estén configurando, es posible realizar las siguientes tareas:
   - Seleccionar extensiones de archivos para excluirlas, por extensión o utilizando caracteres comodines.
   - Seleccionar archivos para excluirlos en carpetas determinadas, por extensión, con caracteres comodines o por tipo de archivo.
   - Seleccionar carpetas para excluirlas del análisis.
5. Haga clic en **Aceptar** hasta que aparezca la consola de Symantec System Center.

Selección de tipos y extensiones de archivos para el análisis

De forma predeterminada, Symantec AntiVirus Corporate Edition analiza todos los archivos durante los análisis de virus. Si no se trata de análisis en tiempo real, puede determinar que se analicen sólo los archivos que pertenezcan a un tipo específico o que tengan una extensión concreta. Los análisis por tipo de archivo están disponibles cuando se seleccionan los siguientes objetos y tipos de análisis:

- Objeto cliente: análisis manual, análisis planificado y protección en tiempo real para clientes.
- Objeto servidor: barrido de virus, análisis manual, análisis de servidor planificado y protección en tiempo real para servidores (sólo en Windows).

Cuando se realizan análisis por tipo de archivo, Symantec AntiVirus Corporate Edition lee el encabezado de cada archivo para determinar su tipo. Por ejemplo, si se activa el análisis de documentos, Symantec AntiVirus Corporate Edition analiza todos los documentos, incluso si tienen un nombre que no incluya una extensión estándar, como Documento3.mlt en lugar de Documento3.doc.

Nota: Esta opción no se aplica a los servidores de NetWare, sólo a los equipos de Windows.

Cuando se realizan análisis por extensiones de archivo, Symantec AntiVirus Corporate Edition no lee el encabezado del archivo para determinar su tipo, sino que analiza únicamente los archivos que tengan la extensión que se haya especificado. La Tabla 3-6 describe las extensiones recomendadas.

Tabla 3-6 Extensiones de archivo recomendadas para el análisis

Extensión de archivo	Descripción
386	Controlador
ACM	Controlador; gestor de compresión de audio
ACV	Controlador; gestor de compresión y descompresión de audio
ADT	Archivo ADT; fax
AX	Archivo AX
BAT	Archivo por lotes
BTM	Archivo por lotes
BIN	Archivo binario

Tabla 3-6 Extensiones de archivo recomendadas para el análisis

Extensión de archivo	Descripción
CLA	Clase de Java
COM	Archivo ejecutable
CPL	Panel de control de subprogramas para Microsoft Windows
CSC	Script de Corel
DLL	Biblioteca de vínculos dinámicos
DOC	Microsoft Word
DOT	Microsoft Word
DRV	Controlador
EXE	Archivo ejecutable
HLP	Archivo de Ayuda
HTA	Aplicación HTML
HTM	HTML
HTML	HTML
HTT	HTML
INF	Script de instalación
INI	Archivo de inicio
JS	JavaScript
JSE	JavaScript codificado
JTD	Ichitaro
MDB	Microsoft Access
MP?	Microsoft Project
MSO	Microsoft Office 2000
OBD	Cuaderno de Microsoft Office
OBT	Cuaderno de Microsoft Office

Tabla 3-6 Extensiones de archivo recomendadas para el análisis

Extensión de archivo	Descripción
OCX	Control personalizado de la tecnología de vinculación e incrustación de objetos de Microsoft (MS OLE)
OV?	Archivo de superposición
PIF	Archivo de información de programa
PL	Código fuente de programa PERL (UNIX)
PM	Gráficos de mapas de bits de Presentation Manager
POT	Microsoft PowerPoint
PPT	Microsoft PowerPoint
PPS	Microsoft PowerPoint
RTF	Documento de texto enriquecido
SCR	Fax, protector de pantalla, captura de pantalla; script de Faxview, Microsoft Windows
SH	Archivo de intérprete de comandos (UNIX)
SHB	Archivo de Corel Show Background
SHS	Archivo temporal de intérprete de comandos
SMM	Archivo de AmiPro
SYS	Controlador de dispositivo
VBE	BIOS VESA (funciones principales)
VBS	VBScript
VSD	Visio
VSS	Visio
VST	Visio
VXD	Controlador virtual de dispositivo
WSF	Script de Windows
WSH	Archivo de configuración de Windows Script Host
XL?	Microsoft Excel

Selección de tipos y extensiones de archivos para el análisis

En todos los tipos de análisis se pueden seleccionar archivos para analizar según la extensión y el tipo de programa. En el caso de los análisis planificados y manuales, se pueden seleccionar además archivos por extensión y por tipo de programa en el nivel de carpeta.

Para seleccionar archivos para analizar por extensión

1. En el cuadro de diálogo de opciones de análisis correspondiente al análisis que vaya a configurar, haga clic en el botón **Seleccionados** apropiado.
2. Haga clic en **Extensiones**.
3. En el cuadro de diálogo Extensiones seleccionadas, puede elegir una de las siguientes opciones:
   - Agregar: permite agregar extensiones propias escribiéndolas y haciendo clic en **Agregar**.
   - Documentos: permite agregar todas las extensiones de documentos.
   - Programas: permite agregar todas las extensiones de programa.
   - Predeterminadas: permite agregar todas las extensiones y tipos de programas.
4. Haga clic en **Aceptar** hasta que aparezca la consola de Symantec System Center.

Para seleccionar archivos para analizar por tipo de programa

1. En el cuadro de diálogo de opciones de análisis correspondiente al análisis que vaya a configurar, haga clic en el botón **Seleccionados** apropiado.
2. Haga clic en **Tipos**.
3. En el cuadro de diálogo Tipos seleccionados, elija una de las siguientes opciones:
   - Archivos de documento: se analizan archivos de documento sin tener en cuenta su extensión.
   - Archivos de programa: se analizan archivos de programa de MS DOS y Windows.
4. Haga clic en **Aceptar** hasta que aparezca la consola de Symantec System Center.

Para seleccionar archivos por carpeta en análisis manuales

1. En la consola de Symantec System Center, haga clic con el botón derecho en el objeto que vaya a analizar y después haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Iniciar análisis manual**.
2. En el cuadro de diálogo Seleccionar elementos, elija las carpetas que desee analizar.
3. Haga clic en **Opciones** y seleccione las extensiones y los tipos de archivo que se deban analizar en las carpetas seleccionadas.
4. Haga clic en **Aceptar** hasta que aparezca la consola de Symantec System Center.

Para seleccionar archivos por carpeta en análisis planificados

1. En la consola de Symantec System Center, haga clic con el botón derecho en el objeto que vaya a analizar y después haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Análisis planificados**.
2. Seleccione un análisis de la lista Análisis de servidor en la ficha con este mismo nombre.
3. Haga clic en **Modificar**.
4. En el cuadro de diálogo Análisis planificados, haga clic en **Opciones de análisis**.
5. En el cuadro de diálogo Seleccionar elementos, elija las carpetas que desee analizar.
6. Haga clic en **Opciones** y seleccione las extensiones y los tipos de archivo que se deban analizar en las carpetas seleccionadas.
7. Haga clic en **Aceptar** hasta que aparezca la consola de Symantec System Center.

Mientras realice las selecciones oportunas en la vista de árbol, los iconos cambiarán según lo que recoge la Tabla 3-7.

Tabla 3-7 Iconos de la vista de árbol

Icono	Descripción
	Symantec AntiVirus Corporate Edition analizará todos los archivos de la carpeta y todos los archivos incluidos en las subcarpetas.
	Symantec AntiVirus Corporate Edition analizará uno o varios elementos seleccionados en la carpeta o en una de las subcarpetas.
	Symantec AntiVirus Corporate Edition analizará el archivo seleccionado. Esta opción sólo está disponible desde la interfaz de cliente o de servidor.
	Symantec AntiVirus Corporate Edition no analizará la carpeta ni los elementos incluidos en ella.

Definición de opciones para el análisis de archivos comprimidos

La Tabla 3-8 recoge y describe las opciones disponibles para analizar archivos comprimidos.

Tabla 3-8 Opciones para analizar archivos comprimidos

Sistema operativo	Opción de análisis
Windows	Symantec AntiVirus Corporate Edition analizará los archivos comprimidos durante los análisis manuales y planificados. Debido a la gran carga de procesamiento que supone, la protección en tiempo real del sistema de archivos no analiza los archivos incluidos dentro de archivos comprimidos en los equipos de Windows; sin embargo, los archivos se analizan cuando se extraen de los archivos comprimidos.
NetWare	Symantec AntiVirus Corporate Edition analizará los archivos comprimidos durante los análisis en tiempo real y planificados. Para analizar el contenido de un archivo comprimido, Symantec AntiVirus Corporate Edition extrae cada archivo, uno a uno, del contenedor y lo copia en el volumen SYS, donde lo analiza. El volumen SYS debe tener suficiente espacio disponible para albergar el archivo de mayor tamaño del contenedor.

El cuadro de diálogo Opciones avanzadas de análisis proporciona opciones que permiten analizar archivos comprimidos incluidos en otros archivos comprimidos. Si se selecciona la casilla de verificación Analizar archivos incluidos en archivos comprimidos, Symantec AntiVirus Corporate Edition analizará el contenedor (Archivos.zip, por ejemplo) y el contenido, es decir, cada uno de los archivos comprimidos. Symantec AntiVirus Corporate Edition permite analizar hasta un máximo de diez niveles de archivos comprimidos anidados, aunque en los servidores de NetWare el límite está en tres niveles.

Nota: No es posible detener un análisis que se esté llevando a cabo en un archivo comprimido. Si hace clic en Detener análisis, Symantec AntiVirus Corporate Edition detiene el proceso cuando finaliza el análisis del archivo comprimido.

Configuración de las opciones de HSM

Symantec AntiVirus Corporate Edition incluye opciones que permiten ajustar los análisis de los archivos gestionados por el sistema de administración jerárquica de almacenamiento (HSM) y por el sistema de copias de respaldo sin conexión. Los sistemas HSM migran los archivos a sistemas de almacenamiento secundarios, como CD, cintas, redes de almacenamiento, etc., pero pueden dejar partes del archivo original en el disco. Pueden surgir problemas relacionados con el rendimiento y el espacio en el disco durante los análisis si Symantec AntiVirus Corporate Edition accede a todos los punteros y el sistema HSM vuelve a colocar los archivos en el disco original. Consulte a su distribuidor del sistema HSM o de copia de respaldo para establecer la configuración adecuada. La configuración dependerá del funcionamiento concreto de cada aplicación HSM.

La Tabla 3-9 recoge las opciones de análisis relacionadas con HSM para Windows 2000 y posterior.

Tabla 3-9 Opciones de migración de almacenamiento (Windows 2000 y superior)

Opción	Descripción
Omitir archivos sin conexión	El archivo se omitirá si se define el bit de desconexión. Un pequeño reloj en el icono del archivo en el Explorador de Windows indica que este bit está definido. Cualquier aplicación puede definir este bit sin que el archivo esté realmente sin conexión.
Omitir archivos dispersos y sin conexión	Algunas aplicaciones definen el bit de archivo disperso para indicar que parte del archivo no se encuentra en el disco. Debido a que algunos productos HSM definen este bit y otros no, conviene consultar con el distribuidor de HSM para comprobar si está o no definido en cada caso. En el caso de los archivos dispersos, en el disco permanece un puntero del archivo mientras que la mayor parte de su contenido se mueve al dispositivo de almacenamiento sin conexión.
Omitir archivos dispersos y sin conexión con un punto de reanálisis	Algunos distribuidores utilizan puntos de reanálisis. Las aplicaciones que emplean puntos de reanálisis utilizan también los controladores de dispositivos adecuados para administrar estos puntos en los archivos. Éste es el valor predeterminado de Symantec AntiVirus Corporate Edition porque resulta la opción más fiable para los distribuidores que utilizan puntos de reanálisis. Consulte con su distribuidor de HSM para saber si esta opción es adecuada. Los puntos de reanálisis hacen que una parte del archivo permanezca en el disco mientras que se accede al resto de forma transparente mediante un filtro de aplicación (el controlador de dispositivo).

Tabla 3-9 Opciones de migración de almacenamiento (Windows 2000 y superior)

Opción	Descripción
Analizar partes residentes de archivos dispersos y sin conexión	Symantec AntiVirus Corporate Edition identifica las partes residentes de un archivo. Si el archivo está disperso, sólo se analiza la parte residente, mientras que la parte no residente permanece en el dispositivo de almacenamiento secundario. Debido a que algunos distribuidores admiten esta función y otros no, deberá consultar con el distribuidor de HSM para determinar si esta opción es adecuada.
Analizar todos los archivos, forzando demigración (unidad de relleno)	Se analiza todo el archivo, lo que fuerza la demigración desde un almacenamiento secundario si es necesario. Debido a que el tamaño del dispositivo de almacenamiento secundario normalmente es mayor que el del volumen local, es posible que con esta opción se agote la capacidad del volumen local, por lo que puede fallar la apertura de archivos siguientes para su análisis.
Analizar todos los archivos sin forzar demigración (lenta)	Symantec AntiVirus Corporate Edition copia un archivo desde el dispositivo de almacenamiento secundario al disco duro local como archivo temporal para analizarlo, pero la aplicación HSM mantiene el archivo original en el dispositivo secundario. Este método resulta muy lento y no lo admiten todos los distribuidores de HSM. Debido a que se copian los archivos desde el dispositivo de almacenamiento secundario al disco para su análisis, la demanda de recursos se eleva considerablemente. El rendimiento del procesador y de la red puede verse reducido más aún si se detecta contenido infectado y se debe transferir una eliminación o una reparación al dispositivo de almacenamiento secundario.

Tabla 3-9 Opciones de migración de almacenamiento (Windows 2000 y superior)

Opción	Descripción
Analizar los archivos usados recientemente sin forzar demigración	Para reducir algunos de los problemas de demanda de recursos, se debe usar esta opción, la cual permite especificar que se analicen sólo los archivos que se hayan migrado recientemente y que, por tanto, puedan todavía encontrarse en los dispositivos de almacenamiento secundarios más rápidos. Puede ser adecuado analizar los archivos si todavía se encuentran en un disco secundario rápido, pero omitir la demigración y el análisis si los archivos llevan mucho tiempo guardados en un dispositivo de almacenamiento a largo plazo, más lento. Por ejemplo, puede que los archivos se migren en primer lugar a un disco remoto cuando transcurran 30 días sin que se haya accedido a ellos y que, después de 60 días, se migren a un CD o a una red de almacenamiento. En muchos casos, puede que este método siga resultando lento debido a que el acceso a los archivos, aunque no se fuerce la demigración, puede constituir una operación relativamente lenta.
Abrir archivos con semántica de respaldo	Permite analizar archivos que, por razones de seguridad, sólo pueden ser leídos normalmente por usuarios concretos.

La Tabla 3-10 recoge la opción de análisis relacionada con HSM para NetWare.

Tabla 3-10 Opción de migración de almacenamiento (NetWare)

Opción	Descripción
Analizar archivos migrados o comprimidos de NetWare	Se analizan los archivos migrados o comprimidos de NetWare.

Para configurar las opciones de HSM

- En el cuadro de diálogo Opciones avanzadas de análisis correspondiente al tipo de análisis que desee configurar, seleccione las opciones oportunas.

Omisión de la protección en tiempo real de archivos de los que se esté realizando copia de respaldo

Se puede hacer que Symantec AntiVirus Corporate Edition omita la protección en tiempo real durante operaciones de copia de respaldo. Esta opción permite que el software de copia de respaldo funcione sin experimentar la sobrecarga adicional de operaciones de análisis de protección en tiempo real. Se aplica sólo a los archivos de los que se está realizando una copia de respaldo. Los archivos que se recuperen a partir de una copia de respaldo se analizarán sin tener en cuenta esta opción.

Nota: Esta opción sólo está disponible para Windows NT, 2000 y XP.

Para omitir la protección en tiempo real de archivos de los que se esté realizando una copia de respaldo

1. En el cuadro de diálogo Opciones de protección en tiempo real, haga clic en **Avanzadas**.
2. En el cuadro de diálogo Opciones avanzadas del sistema de archivos, quite la marca de la casilla **Abierto para copia de respaldo**.

Establecimiento del uso de la CPU

En el caso de los análisis planificados y manuales, Symantec AntiVirus Corporate Edition permite controlar la prioridad de los análisis en la CPU. Conceder menor prioridad a un análisis significa que éste tardará más en finalizar, pero por otra parte supone liberar la CPU para otras tareas. Puede que le interese establecer una prioridad más baja en ciertas situaciones. Por ejemplo, si va a realizar análisis a la hora del almuerzo en los días laborables, puede que sea conveniente reducir la prioridad del análisis para minimizar el impacto en la productividad de los usuarios.

La prioridad del análisis se establece mediante los controles deslizantes del cuadro de diálogo Opciones de análisis. Se puede especificar la prioridad del análisis para:

- Equipos con Windows: la prioridad varía en función de que el equipo esté inactivo o no. La opción que se aplica cuando el equipo está inactivo indica la prioridad que se le debe asignar a los análisis cuando no haya actividad en el equipo, mientras que la opción que se aplica cuando el equipo no está inactivo establece la prioridad de los análisis cuando el equipo está en funcionamiento.
- Equipos con NetWare: Symantec AntiVirus Corporate Edition permite establecer la velocidad de carga en servidores de NetWare. Cuanto más baja sea la velocidad de carga, más tiempo tardará en finalizar el análisis del servidor.

Capítulo 4

Actualización de las definiciones de virus

En este capítulo se tratan los temas siguientes:

- Acerca de los archivos de definiciones de virus
- Métodos de actualización de los archivos de definiciones de virus
- Actualización de los archivos de definiciones de virus en servidores de Symantec AntiVirus Corporate Edition
- Actualización de los archivos de definiciones de virus en clientes de Symantec AntiVirus Corporate Edition
- Control de los archivos de definiciones de virus
- Prueba de los archivos de definiciones de virus
- Situaciones posibles de actualización

Acerca de los archivos de definiciones de virus

Los archivos de definiciones de virus contienen código de muestra de miles de virus. Cuando Symantec AntiVirus Corporate Edition analiza el equipo en busca de virus, trata de encontrar coincidencias entre los archivos y las muestras de código de los archivos de definiciones. Si Symantec AntiVirus Corporate Edition detecta una coincidencia, el archivo puede estar infectado.

Todos los servidores y clientes que ejecutan Symantec AntiVirus Corporate Edition disponen de una copia de los archivos de definiciones de virus. Estos archivos pueden quedar obsoletos a medida que se descubren virus nuevos. Symantec actualiza los archivos de definiciones de virus una vez a la semana por lo general, o con mayor frecuencia si es necesario. Es importante mantener al día los archivos de definiciones de virus para contar con el máximo nivel de protección en la red.

Métodos de actualización de los archivos de definiciones de virus

Se puede elegir entre cuatro métodos distintos para descargar definiciones de virus y configurar los clientes y los servidores para que las obtengan. La Tabla 4-1 describe los métodos de actualización de los archivos de definiciones de virus.

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

Método	Descripción	Cuándo utilizarlo
Método de transporte de definiciones de virus	Cuando un servidor primario de la red recibe nuevas definiciones de virus a través del sitio FTP de Symantec o mediante el servidor de LiveUpdate, comienza una operación de transferencia. El servidor primario transfiere un paquete de definiciones de virus a todos los servidores secundarios del grupo de servidores. Los servidores secundarios extraen las definiciones y las colocan en el directorio apropiado. Los clientes reciben el paquete del servidor principal correspondiente, extraen las definiciones y las colocan en el directorio apropiado.	El método de transporte de definiciones de virus se debe emplear cuando se desean controlar las actualizaciones de los archivos de definiciones de virus desde Symantec System Center. Además, este método se debe emplear durante una infección vírica para transferir de forma inmediata los archivos de definiciones de virus más recientes a los equipos de la red interna.
LiveUpdate	Cuando un cliente o un servidor donde esté instalado LiveUpdate solicita nuevas definiciones, comienza una operación de transferencia planificada. LiveUpdate puede estar configurado en cada equipo para solicitar la actualización de un servidor de LiveUpdate interno o del servidor de LiveUpdate de Symantec directamente.	Se debe utilizar LiveUpdate cuando se desee que los equipos protegidos obtengan las actualizaciones de los archivos de definiciones de virus de un servidor de LiveUpdate interno o de Symantec directamente.

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

Método	Descripción	Cuándo utilizarlo
Sondeo de Cuarentena central	El servidor de Cuarentena central sondea periódicamente la pasarela de Symantec Digital Immune System con el fin de obtener nuevos archivos de definiciones de virus. Cuando están disponibles nuevas definiciones, el servidor de Cuarentena central puede transferirlas automáticamente al equipo que las necesite.	Use Cuarentena central cuando desee automatizar la distribución de las actualizaciones de los archivos de definiciones de virus en la red.
Intelligent Updater	Intelligent Updater es un archivo ejecutable y autoextraíble que contiene archivos de definiciones de virus.	Use Intelligent Updater cuando necesite distribuir las actualizaciones de los archivos de definiciones de virus a usuarios que no cuenten con conexiones de red activas.

La mejor opción: utilización del método de transporte de definiciones de virus combinado con LiveUpdate

Es posible utilizar el método de transporte de definiciones de virus en combinación con LiveUpdate. LiveUpdate permite actualizar los componentes de software de Symantec AntiVirus Corporate Edition. El método de transporte de definiciones de virus permite planificar y transferir actualizaciones de los archivos de definiciones de virus desde Symantec System Center. Además, el método de transporte de definiciones de virus se puede utilizar como sistema de emergencia para distribuir nuevos archivos de definiciones de virus rápidamente cuando la red se vea amenazada por un nuevo virus.

Si bien el método de transporte de definiciones de virus es el más extendido, algunas redes de gran tamaño dependen de LiveUpdate. Estas instalaciones no permiten que un elevado número de servidores y clientes accedan al sitio Web de Symantec directamente. Uno o varios servidores actúan como servidores de LiveUpdate internos para todos los demás servidores de la red y, en algunas instalaciones, para todos los clientes.

Actualización de los archivos de definiciones de virus en servidores de Symantec AntiVirus Corporate Edition

Hay tres métodos posibles para actualizar los archivos de definiciones de virus en los servidores:

- Método de transporte de definiciones de virus
- LiveUpdate
- Intelligent Updater
- Sondeo de Cuarentena central

Vea "Métodos de actualización de los archivos de definiciones de virus" en la página 135.

Actualización y configuración de servidores de Symantec AntiVirus Corporate Edition mediante el método de transporte de definiciones de virus

Actualice los servidores de Symantec AntiVirus Corporate Edition manualmente cuando tenga que forzar una actualización inmediata. Planifique actualizaciones automáticas para gestionar las actualizaciones de los archivos de definiciones de virus rutinarias que no requieran que el usuario realice ninguna acción adicional.

Actualización manual o automática de servidores mediante el método de transporte de definiciones de virus

Es posible actualizar los servidores manual o automáticamente.
Las actualizaciones sólo tienen lugar cuando los archivos de definiciones de virus de los servidores son anteriores a los archivos disponibles en el servidor de LiveUpdate.

Para actualizar todos los servidores desbloqueados del sistema

1. En Symantec System Center, haga clic con el botón derecho en la jerarquía del sistema y haga clic en **Symantec AntiVirus** > **Actualizar definiciones de virus**.
2. Haga clic en **Sí** en el cuadro de diálogo de confirmación.
3. Haga clic en **Aceptar** en el cuadro de diálogo de estado.

Para actualizar servidores manualmente

1. En Symantec System Center, haga clic con el botón derecho en un servidor o en un grupo de servidores y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Administrador de definiciones de virus**.
2. Seleccione una de las opciones siguientes:
   - Actualizar sólo el servidor primario del grupo de servidores: si desea actualizar todos los servidores del grupo desde el servidor primario.
   - Actualizar cada servidor del grupo individualmente: para actualizar los servidores por separado.

   La opción que seleccione afectará a todos los servidores del grupo de servidores, tanto si hace clic con el botón derecho en un grupo de servidores como en un solo servidor.
3. Haga clic en **Configurar**.
4. Haga clic en **Actualizar ahora**.

   A continuación, aparecerá un mensaje con información sobre cómo se puede visualizar la fecha del nuevo archivo de definiciones de virus.
5. Lea la información incluida en el mensaje y haga clic en **Aceptar** hasta que vuelva a aparecer la consola principal de Symantec System Center.

Para actualizar servidores automáticamente

1. En Symantec System Center, haga clic con el botón derecho en un grupo de servidores o en un servidor y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Administrador de definiciones de virus**.
2. Seleccione una de las opciones siguientes:
   - Actualizar sólo el servidor primario del grupo de servidores: si desea actualizar automáticamente todos los servidores del grupo desde el servidor primario.
   - Actualizar cada servidor del grupo individualmente: para actualizar los servidores por separado.

   La opción seleccionada afectará a todos los servidores del grupo, tanto si hace clic con el botón derecho en un servidor individual como en un grupo de servidores.
3. Haga clic en **Configurar**.
4. Asegúrese de que la casilla de verificación Planificar actualizaciones automáticas esté seleccionada y, después, haga clic en **Planificar**.

5 Seleccione las restantes opciones a fin de determinar cuándo se producirá la actualización del archivo de definiciones de virus (por ejemplo, todos los jueves a las 10:00 p.m.).

6 Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Actualización de un servidor primario maestro

Configure un servidor primario maestro para limitar la exposición de la red a Internet.

Para configurar un servidor primario maestro

1 En Symantec System Center, haga clic con el botón derecho en un servidor y, a continuación, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Administrador de definiciones de virus**.

2 En el cuadro de diálogo Administrador de definiciones de virus, haga clic en **Actualizar sólo el servidor primario del grupo de servidores**.

3 Haga clic en **Configurar**.

4 En el cuadro de diálogo Configuración de actualizaciones de servidores primarios, haga clic en **Origen**.

5 En la lista Actualizar el archivo de definiciones mediante del cuadro de diálogo Configurar conexión, haga clic en **Otro servidor protegido** y, a continuación, haga clic en **Configurar** si es necesario.

6 En el cuadro de diálogo Configurar actualización desde el servidor, seleccione el servidor primario maestro de la lista de servidores que aparece.

7 Haga clic en **Aceptar**.

8 En el cuadro de diálogo Configuración de actualizaciones de servidores primarios, lleve a cabo una de las acciones siguientes:

- Haga clic en **Actualizar ahora** para obtener los archivos de definiciones de virus desde el servidor primario maestro de forma inmediata.
- Para planificar actualizaciones automáticas, haga clic en **Planificar actualizaciones automáticas** y después en **Planificar** y establezca la frecuencia y la hora para que el servidor compruebe la existencia de actualizaciones en el servidor primario maestro.

9 Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Actualización de servidores de NetWare utilizando el método de transporte de definiciones de virus

La actualización de un servidor de NetWare es similar a la de cualquier otro tipo de servidor, con las siguientes diferencias:

- Se puede designar un servidor de NetWare como servidor primario de la red o designar un equipo de Windows NT o 2000 como servidor primario. Si los servidores de NetWare se ejecutan en equipos más rápidos o con conexiones con mayor ancho de banda que los servidores de Windows NT o 2000, se puede designar un servidor de NetWare como servidor primario para mejorar el rendimiento.
- En los servidores primarios de NetWare se deben estar ejecutando TCP/IP y FTP (FTP no está activado de forma predeterminada en estos servidores), y deben permitir la conexión a Internet. Además, en los entornos de Netware es preciso que se ejecute la consola de Symantec System Center en un equipo con Windows NT o 2000.
- Los servidores de NetWare no almacenan la dirección de los servidores de Windows NT o 2000 en la antememoria de direcciones, por lo que, si no se ejecuta TCP/IP en el servidor de NetWare y no se utiliza un servidor de sistema de nombres de dominio (DNS), pueden generarse problemas al actualizar un servidor de NetWare desde un servidor de Windows NT o 2000 que resida en un grupo de servidores distinto.

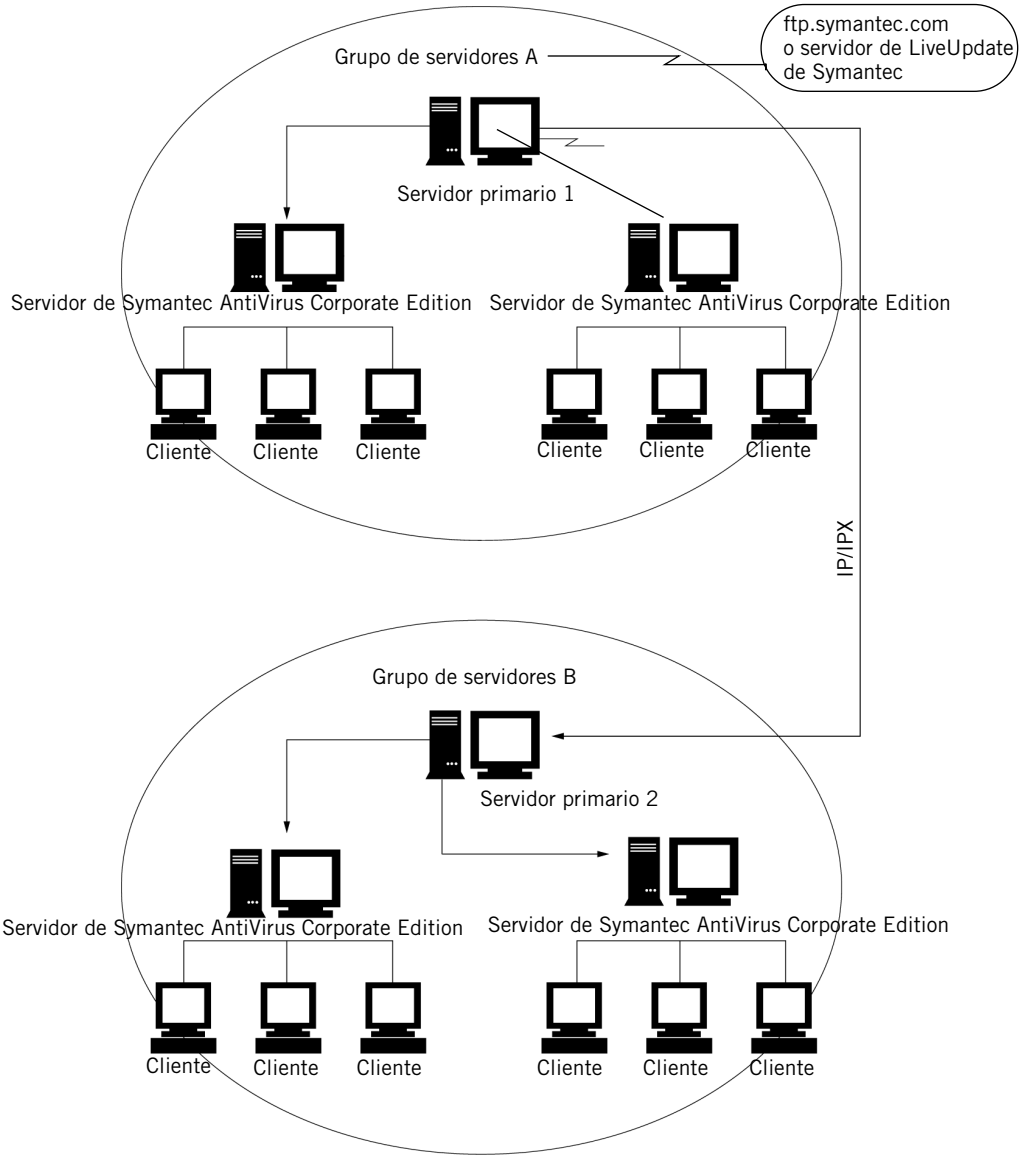
Para actualizar servidores de NetWare sin TCP/IP

- Asigne temporalmente el servidor de NetWare a un grupo de servidores que cuente con un servidor de Windows NT que utilice el protocolo IPX.

  Transcurrido un día, podrá volver a asignar el servidor de NetWare a su grupo de servidores original. La dirección del servidor de Windows NT o 2000 se habrá añadido a la antememoria de direcciones del servidor de NetWare, permitiéndole así localizar el servidor de Windows NT o 2000 con objeto de obtener el archivo de definiciones de virus actualizado.

Figura 4-1 ilustra una de las formas en que se puede configurar la actualización de los archivos de definiciones de virus del equipo si se dispone de una pequeña red de seis servidores de archivos divididos en dos grupos de servidores.

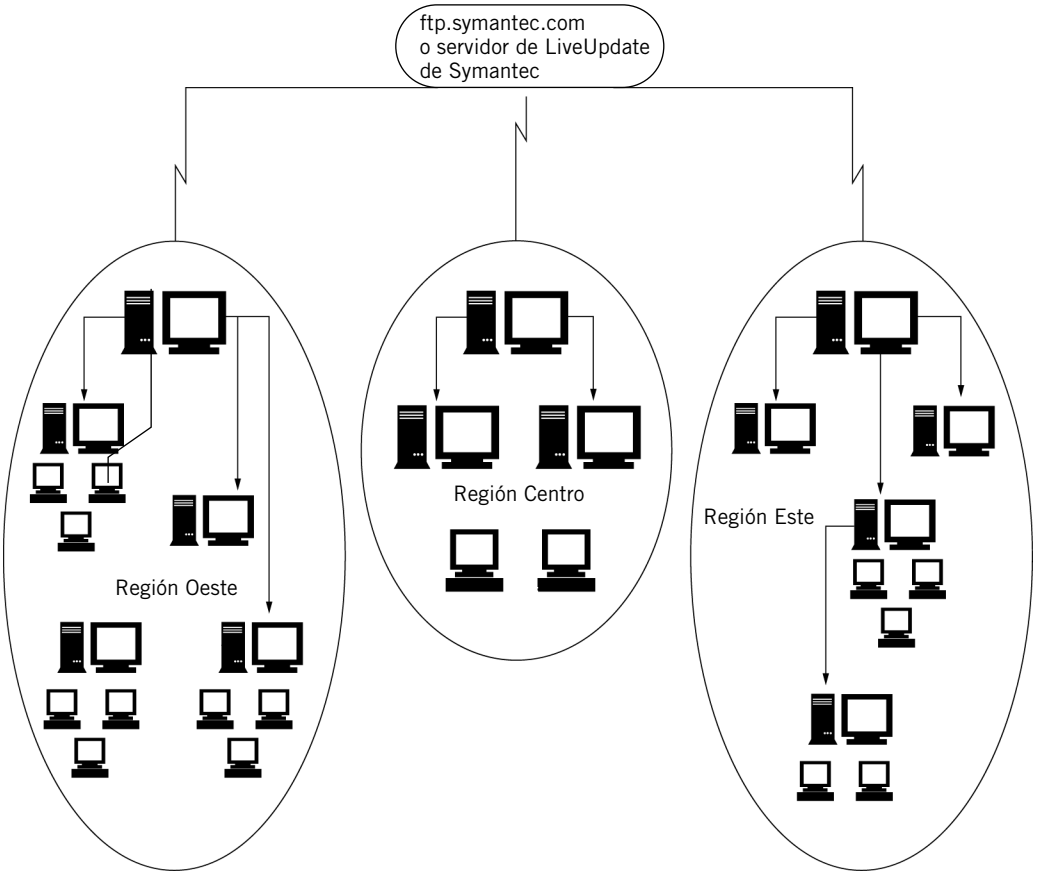
Figura 4-1 Actualización de los archivos de definiciones de virus mediante el método de transporte de definiciones de virus



Se debe configurar un servidor primario para obtener los últimos archivos de actualización de las definiciones de virus; se pueden descargar a través de FTP o de otro equipo. Se debe activar el uso compartido de los archivos de definiciones de virus de forma que los servidores de Symantec AntiVirus Corporate Edition del grupo de servidores A obtengan automáticamente las últimas actualizaciones del servidor primario 1. Los clientes recibirán las actualizaciones automáticamente de los correspondientes servidores principales de Symantec AntiVirus. Se debe configurar el servidor primario 2 para que obtenga las últimas actualizaciones del servidor primario 1. De esta forma, el servidor primario 1 se convierte en un servidor primario maestro. Los servidores de Symantec AntiVirus Corporate Edition del grupo de servidores B recibirán las actualizaciones del servidor primario correspondiente. A su vez, los clientes recibirán automáticamente las actualizaciones de los servidores de Symantec AntiVirus Corporate Edition correspondientes.

La Figura 4-2 ilustra el modo en que se podría configurar la actualización de los archivos de definiciones de virus en caso de que la organización contara con varios sitios vinculados mediante una red de área extensa (WAN).

Figura 4-2 Actualización de archivos de definiciones de virus para varios sitios de una red de área extensa (WAN)



Los servidores primarios de los grupos de servidores ubicados en diferentes redes de área extensa (WAN) obtienen las actualizaciones desde el sitio FTP o desde el servidor de LiveUpdate de Symantec. Acto seguido, los servidores primarios distribuyen la actualización a los servidores primarios de otros grupos de servidores pertenecientes a sus redes de área local (LAN). Por último, los servidores primarios distribuyen la actualización a los otros servidores y clientes protegidos pertenecientes a su grupo de servidores.

Actualización de servidores mediante LiveUpdate

Dependiendo del tamaño de la red, se puede emplear LiveUpdate para actualizar los archivos de definiciones de virus de dos formas distintas:

- En redes pequeñas (menos de 1000 nodos), se deben configurar los servidores administrados para que obtengan las actualizaciones directamente del sitio FTP de Symantec, del servidor de LiveUpdate de Symantec o de un servidor de LiveUpdate interno.
- En redes grandes (más de 1000 nodos), se debe configurar un servidor de LiveUpdate interno, descargar las actualizaciones a ese servidor y hacer que los servidores administrados obtengan las actualizaciones de ese servidor de LiveUpdate interno.

Actualización de servidores de Symantec AntiVirus Corporate Edition desde el sitio FTP o el servidor de LiveUpdate de Symantec

Es preciso configurar la actualización en el servidor primario de cada grupo de servidores para garantizar que los archivos de definiciones de virus estén al día. Es posible además configurar servidores individuales para que obtengan las actualizaciones directamente de Symantec.

Actualización de servidores de Symantec AntiVirus Corporate Edition directamente desde el sitio FTP o desde el servidor de LiveUpdate de Symantec

Es posible actualizar todos los servidores de Symantec AntiVirus Corporate Edition de un grupo de servidores desde un servidor primario o actualizar cada uno de los servidores del grupo por separado.

Para actualizar servidores primarios

1. Desde Symantec System Center, haga clic con el botón derecho en un grupo de servidores y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Administrador de definiciones de virus**.
2. En el cuadro de diálogo Administrador de definiciones de virus, haga clic en **Actualizar sólo el servidor primario del grupo de servidores**.
3. Haga clic en **Configurar**.

4. En el cuadro de diálogo Configuración de actualizaciones de servidores primarios, lleve a cabo una de las siguientes acciones:
   - Haga clic en **Actualiza ahora** si desea ejecutar una sesión de LiveUpdate de forma inmediata.
   - Haga clic en **Planificar actualizaciones automáticas**, a continuación en **Planificar** y defina una frecuencia y una hora para que el servidor ejecute una sesión de LiveUpdate.
5. Haga clic en **Aceptar**.
6. En el cuadro de diálogo Configuración de actualizaciones de servidores primarios, haga clic en **Origen**.
7. En la lista Actualizar el archivo de definiciones mediante, haga clic en **LiveUpdate**.
8. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Para actualizar servidores por separado desde el sitio FTP de Symantec o desde el servidor de LiveUpdate

1. Desde Symantec System Center, haga clic con el botón derecho en un grupo de servidores y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Administrador de definiciones de virus**.
2. En el cuadro de diálogo Administrador de definiciones de virus, haga clic en **Actualizar cada servidor del grupo individualmente**.
3. Haga clic en **Configurar**.
4. En el cuadro de diálogo Configuración de actualizaciones de servidores primarios, haga clic en **Origen**.
5. Haga clic en **LiveUpdate (Win32)/FTP (NetWare)**.
6. Haga clic en **Aceptar**.
   Si está configurando un servidor de NetWare, asegúrese de que esté ejecutando FTP.
7. Realice una de las acciones siguientes:
   - Haga clic en **Actualiza ahora** si desea ejecutar una sesión de LiveUpdate de forma inmediata.
   - Haga clic en **Planificar actualizaciones automáticas,** a continuación en **Planificar** y defina una frecuencia y una hora para que el servidor ejecute una sesión de LiveUpdate.
8. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Actualización de servidores desde un servidor de LiveUpdate interno

Es posible configurar un servidor de LiveUpdate interno en cualquier equipo. Si se emplea un servidor de Symantec AntiVirus Corporate Edition como servidor de LiveUpdate interno, se pueden utilizar los métodos de actualización estándar disponibles en el cuadro de diálogo Administrador de definiciones de virus para actualizar manual o automáticamente los archivos de definiciones de virus en el servidor. Si se emplea un equipo en el que no se ejecute Symantec AntiVirus Corporate Edition como servidor de LiveUpdate interno, se debe emplear la utilidad de administración de LiveUpdate para actualizar las definiciones de virus en ese servidor.

Vea "Actualización de servidores mediante LiveUpdate" en la página 143.

Consulte la guía del administrador de LiveUpdate, *LiveUpdate Administrator's Guide,* si desea obtener información adicional (en inglés).

Para actualizar servidores desde un servidor de LiveUpdate interno

1. Desde Symantec System Center, haga clic con el botón derecho en un grupo de servidores y a continuación haga clic en **Todas las tareas** > **LiveUpdate** > **Configurar**.
2. En el cuadro de diálogo **Configurar LiveUpdate,** haga clic en **Servidor de LiveUpdate interno**.
3. Especifique las siguientes opciones del servidor de LiveUpdate interno:

Nombre	El nombre del servidor. Éste aparecerá cuando se ejecute LiveUpdate.
Ubicación	Este campo es opcional. Puede escribir información descriptiva relacionada con el servidor (por ejemplo, el nombre del sitio).
Nombre de inicio de sesión	El nombre de inicio de sesión correspondiente al servidor. Deje este cuadro en blanco si desea que los usuarios puedan iniciar la sesión y obtener archivos sin necesidad de introducir información.
Contraseña	La contraseña de inicio de sesión correspondiente al servidor. Deje este cuadro en blanco si desea que los usuarios puedan iniciar la sesión y obtener archivos sin necesidad de introducir información.

URL o dirección IP

- Si utiliza el método de actualización mediante FTP (recomendado), haga clic en FTP bajo el campo Tipo y, a continuación, escriba la dirección FTP del servidor. Por ejemplo: ftp.miservidorliveupdate.com
- Si emplea el método de actualización mediante HTTP, haga clic en HTTP bajo el campo Tipo y, después, introduzca la dirección URL correspondiente al servidor. Por ejemplo:

  http:\\miservidorliveupdate.com o 155.66.133.11\Export\Home\Ludepot
- Si utiliza el método de actualización mediante LAN, haga clic en LAN bajo el campo Tipo y escriba la ruta de acceso UNC del servidor. Por ejemplo: \\Miservidor\LUDepot

  En el cuadro Inicio de sesión, introduzca el nombre y la contraseña para acceder al servidor.

Si deja en blanco los cuadros Nombre de inicio de sesión y Contraseña, el inicio de sesión será anónimo. Para ello, este tipo de inicio de sesión debe activarse en el servidor FTP. Si su política prohíbe el inicio de sesión anónimo en los servidores FTP, escriba el nombre y la contraseña de inicio de sesión correspondientes al directorio y al servidor FTP a los que se vaya a acceder.

4 Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Selección de varios servidores de LiveUpdate internos para casos de redireccionamiento por fallo

Con el fin de compensar la posible falta de disponibilidad de algunos servidores de LiveUpdate internos, Symantec AntiVirus Corporate Edition admite que se configuren varios de ellos.

Actualización de servidores mediante Intelligent Updater

Para distribuir definiciones de virus actualizadas, descargue Intelligent Updater y, a continuación, utilice el mecanismo de distribución que prefiera para enviar las actualizaciones a los servidores y clientes administrados. Intelligent Updater está disponible como un único archivo o como un paquete dividido, distribuido en varios archivos más pequeños. El archivo único es adecuado para equipos que cuenten con conexiones de red. El paquete dividido se puede copiar en disquetes y utilizarlos para actualizar equipos que no cuenten con conexiones de red o con acceso a Internet.

Actualización de servidores con archivos de Intelligent Updater

Descargue Intelligent Updater del sitio Web de Symantec e instálelo en los servidores en los que se encuentren los archivos de definiciones de virus más recientes.

Nota: Asegúrese de utilizar los archivos de Intelligent Updater para Symantec AntiVirus Corporate Edition en lugar de la versión del producto para consumidores.

Para descargar Intelligent Updater

1. Con la ayuda del explorador de Web, vaya a:
   http://securityresponse.symantec.com
2. Haga clic en **Download Virus Definitions**.
3. Haga clic en **Download Updates** (**Intelligent Updater Only**).
4. Seleccione el idioma y el producto adecuados.
5. Haga clic en **Download Updates**.
6. Haga clic en el archivo con extensión.exe.
7. Cuando se le solicite que especifique una ubicación para guardar los archivos, seleccione una carpeta del disco duro.

Para instalar los archivos de definiciones de virus

1. Localice el archivo de Intelligent Updater que haya descargado de Symantec.
2. Haga doble clic en el archivo y siga las instrucciones que aparecerán en pantalla.
   Si utiliza Windows 3.1 o DOS, debe reiniciar el equipo después de cada actualización. No es necesario reiniciar equipos de Windows 95, 98, ME, NT, 2000 o XP.

Actualización de servidores mediante el sondeo de Cuarentena central

Si se utiliza Cuarentena central de Symantec, se puede configurar el servidor de Cuarentena central para que sondee periódicamente la pasarela de Symantec Digital Immune System con el fin de obtener nuevos archivos de definiciones de virus. Cuando estén disponibles nuevas definiciones, el servidor de Cuarentena central puede transferirlas automáticamente a los equipos que las necesiten mediante el método de transporte de definiciones de virus.

Consulte la guía del administrador de Cuarentena central, *Symantec Central Quarantine Administrator's Guide,* si desea obtener más información (en inglés).

Reducción del tráfico en la red y gestión de actualizaciones no realizadas

LiveUpdate proporciona opciones de planificación avanzadas que permiten reducir el tráfico en la red y gestionar las actualizaciones no realizadas. La Tabla 4-2 describe las opciones de planificación de LiveUpdate.

Tabla 4-2 Opciones de planificación de LiveUpdate

Opción	Descripción	Cuándo utilizarla
Opciones de cálculo aleatorio	Permiten planificar actualizaciones aleatorias: ■ Un número específico de minutos antes o después de la hora planificada ■ Cualquier día de la semana dentro de un intervalo de tiempo definido ■ Un número específico de días antes o después de la fecha planificada	Cuando se quieren escalonar las actualizaciones para varios equipos con el fin de reducir el impacto en el tráfico de la red. De forma predeterminada, Symantec AntiVirus Corporate Edition calcula aleatoriamente las sesiones de LiveUpdate para reducir los picos en el ancho de banda.
Opciones de sucesos no realizados	Determinan cómo se deben gestionar los sucesos de LiveUpdate no realizados. Un suceso puede no realizarse si el equipo está apagado en el momento en que se deba ejecutar una sesión planificada de LiveUpdate. Las opciones de configuración pueden establecerse de tal forma que los sucesos de LiveUpdate que no se hayan podido realizar se ejecuten más tarde.	Cuando se quiera garantizar que los equipos que no estén disponibles cuando se produzca un suceso de LiveUpdate planificado intentarán obtener las definiciones más tarde.

Reducción del tráfico en la red y gestión de actualizaciones no realizadas

Se pueden definir planificaciones aleatorias independientes para los servidores y los clientes de Symantec AntiVirus Corporate Edition de la red con el fin de reducir el impacto en el tráfico de ésta.

Se pueden definir políticas independientes para gestionar sucesos de LiveUpdate no realizados en servidores y clientes de Symantec AntiVirus Corporate Edition.

Para calcular aleatoriamente las actualizaciones planificadas mediante LiveUpdate en los servidores

1. En Symantec System Center, haga clic con el botón derecho en un grupo de servidores o en un servidor y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Administrador de definiciones de virus**.
2. En el cuadro de diálogo Administrador de definiciones de virus, haga clic en **Configurar**.
3. En el cuadro de diálogo Configuración de actualizaciones de servidores primarios, marque la casilla de verificación **Planificar actualizaciones automáticas**.
4. Haga clic en **Planificar**.
5. Establezca la frecuencia y la hora para que el servidor compruebe la existencia de nuevas actualizaciones.
6. En el cuadro de diálogo Planificación de la actualización de definiciones de virus, haga clic en **Avanzadas**.
7. En el cuadro de diálogo Opciones de planificación avanzadas, bajo Opciones de cálculo aleatorio, active la casilla **Opciones** y especifique las opciones correspondientes a los minutos, al día de la semana o al día del mes.
8. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Para calcular aleatoriamente las actualizaciones planificadas mediante LiveUpdate en los clientes

1. En Symantec System Center, haga clic con el botón derecho en un grupo de servidores o en un servidor y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Administrador de definiciones de virus**.
2. En el cuadro de diálogo Administrador de definiciones de virus, active la casilla **Planificar actualizaciones automáticas de las definiciones de virus mediante LiveUpdate en el cliente**.
3. En el cuadro de diálogo Planificación de la actualización de definiciones de virus, haga clic en **Planificar**.
4. Establezca la frecuencia y la hora para que los clientes comprueben la existencia de nuevas actualizaciones.
5. Haga clic en **Avanzadas**.
6. En el cuadro de diálogo Opciones de planificación avanzadas, bajo Opciones de cálculo aleatorio, marque la casilla **Opciones** y especifique las opciones correspondientes a los minutos, al día de la semana o al día del mes.
7. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Para gestionar sucesos de LiveUpdate no realizados en servidores

1. En Symantec System Center, haga clic con el botón derecho en un grupo de servidores o en un servidor y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Administrador de definiciones de virus**.
2. En el cuadro de diálogo Administrador de definiciones de virus, haga clic en **Configurar**.
3. Haga clic en **Planificar actualizaciones automáticas**.
4. En el cuadro de diálogo Configuración de actualizaciones de servidores primarios, haga clic en **Planificar**.
5. En el cuadro de diálogo Planificación de la actualización de definiciones de virus, haga clic en **Avanzadas**.
6. En el cuadro de diálogo Opciones de planificación avanzadas, active la casilla **Gestionar sucesos no realizados a**.
7. Establezca el límite de tiempo para que se ejecute el análisis.

   Por ejemplo, puede que le interese que se ejecute una actualización mediante LiveUpdate una vez por semana sólo si se produce en los tres días siguientes a la hora planificada para el suceso no realizado.
8. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Para gestionar sucesos de LiveUpdate no realizados en clientes

1. En Symantec System Center, haga clic con el botón derecho en un grupo de servidores o en un servidor y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Administrador de definiciones de virus**.
2. En el cuadro de diálogo Administrador de definiciones de virus, haga clic en **Planificar actualizaciones automáticas de las definiciones de virus mediante LiveUpdate en el cliente**.
3. Haga clic en **Planificar**.
4. En el cuadro de diálogo Planificación de la actualización de definiciones de virus, haga clic en **Avanzadas**.
5. Marque **Gestionar sucesos no realizados a**.
6. Establezca el límite de tiempo para que se produzca el análisis.
7. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

   Por ejemplo, puede que le interese que se ejecute una actualización mediante LiveUpdate una vez por semana sólo si se produce en los tres días siguientes a la hora planificada para el suceso no realizado.

Actualización de los archivos de definiciones de virus en clientes de Symantec AntiVirus Corporate Edition

Para actualizar los archivos de definiciones de virus de los clientes de Symantec AntiVirus Corporate Edition, se puede emplear cualquiera de los siguientes medios:

- Método de transporte de definiciones de virus
- LiveUpdate
- Intelligent Updater
  Vea "Selección de varios servidores de LiveUpdate internos para casos de redireccionamiento por fallo" en la página 146.
- Sondeo de Cuarentena central
  Vea "Actualización de servidores mediante el sondeo de Cuarentena central" en la página 147.

Vea "Métodos de actualización de los archivos de definiciones de virus" en la página 135.

Actualización de los archivos de definiciones de virus en los clientes de Symantec AntiVirus Corporate Edition

Los clientes de Symantec AntiVirus Corporate Edition se pueden actualizar empleando el método de transporte de definiciones de virus, LiveUpdate o ambos.

Para actualizar clientes utilizando el método de transporte de definiciones de virus

1. En la consola de Symantec System Center, haga clic con el botón derecho en un grupo de servidores y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Administrador de definiciones de virus**.
2. En el cuadro de diálogo Administrador de definiciones de virus, marque la casilla **Actualizar definiciones de virus desde el servidor principal**.
3. Haga clic en **Opciones**.
4. En el cuadro de diálogo Opciones de actualización, defina la frecuencia con la que el servidor principal debe transferir las actualizaciones.
5. Haga clic en **Aceptar**.
6. En el cuadro de diálogo Administrador de definiciones de virus, quite la marca de la casilla **Planificar actualizaciones automáticas mediante LiveUpdate en el cliente**.
7. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Para actualizar los clientes mediante LiveUpdate

1. En la consola de Symantec System Center, haga clic con el botón derecho en un grupo de servidores y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Administrador de definiciones de virus**.
2. En el cuadro de diálogo Administrador de definiciones de virus, haga clic en **Planificar actualizaciones automáticas mediante LiveUpdate en el cliente**.
3. Haga clic en **Planificar**.
4. En el cuadro de diálogo Planificación de la actualización de definiciones de virus, seleccione la frecuencia, el día y la hora en que se llevará a cabo la actualización.
5. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Para actualizar los clientes usando el método de transporte de definiciones de virus y LiveUpdate

1. En la consola de Symantec System Center, haga clic con el botón derecho en un grupo de servidores y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Administrador de definiciones de virus**.
2. En el cuadro de diálogo Administrador de definiciones de virus, marque la casilla **Actualizar definiciones de virus desde el servidor principal**.
3. Haga clic en **Planificar actualizaciones automáticas mediante LiveUpdate en el cliente**.
4. Haga clic en **Planificar**.
5. En el cuadro de diálogo Planificación de la actualización de definiciones de virus, seleccione la frecuencia, el día y la hora en que se llevará a cabo la actualización.
6. Haga clic en **Aceptar**.
7. Haga clic en **Opciones**.
8. En el cuadro de diálogo Opciones de actualización, defina la frecuencia con la que el servidor principal debe transferir las actualizaciones.
9. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Configuración de clientes administrados para que utilicen un servidor de LiveUpdate interno

Es posible configurar desde Symantec System Center las opciones de LiveUpdate correspondientes a los equipos administrados que tengan instalado el cliente de Symantec AntiVirus Corporate Edition. En el caso de los clientes de Symantec AntiVirus Corporate Edition no administrados, se debe usar el Administrador de LiveUpdate para crear un archivo.hst personalizado.

Si desea obtener información sobre cómo configurar LiveUpdate para clientes de Symantec AntiVirus Corporate Edition no administrados, consulte la Ayuda del Administrador de LiveUpdate.

Para configurar un cliente de Symantec AntiVirus Corporate Edition administrado para que utilice un servidor de LiveUpdate interno

1. Haga clic con el botón derecho en un servidor principal y después haga clic en **Todas las tareas** > **LiveUpdate** > **Configurar**.
2. En el cuadro de diálogo Configurar LiveUpdate, haga clic en **Servidor de LiveUpdate interno**.
3. Si utiliza un servidor FTP o HTTP, escriba la información adecuada en los cuadros Nombre de inicio de sesión y Contraseña.
4. En el cuadro Conexión, introduzca cualquiera de los datos siguientes:
   - La ruta UNC a la carpeta compartida
   - La dirección URL o IP correspondiente al servidor FTP o HTTP
5. Seleccione una de las siguientes opciones de la lista Tipo:
   - LAN
   - FTP
   - HTTP
6. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

   Si utiliza varios servidores principales, repita los pasos del 1 al 6 con cada uno de ellos, de modo que todos los servidores y clientes de Symantec AntiVirus Corporate Edition reciban los cambios. Es posible, asimismo, definir la configuración de LiveUpdate en un grupo completo haciendo clic con el botón derecho en el grupo de servidores.

Activación y configuración de LiveUpdate continuo para clientes administrados

Si un cliente de Symantec AntiVirus Corporate Edition administrado se conecta al servidor principal con poca frecuencia (por ejemplo, un equipo portátil que se utiliza fuera de la oficina), puede no recibir las últimas actualizaciones de los archivos de definiciones de virus. En estos casos, LiveUpdate continuo ofrece una opción alternativa para recibir las actualizaciones directamente de Symantec cuando el equipo se conecte a Internet.

Con LiveUpdate continuo, es posible especificar el número máximo de días que pueden permanecer obsoletos los archivos de definiciones de virus en los equipos de Symantec AntiVirus Corporate Edition antes de que se fuerce una actualización. Cuando el cliente de Symantec AntiVirus Corporate Edition determina que los archivos de definiciones de virus han sobrepasado este límite, inicia una sesión de LiveUpdate silenciosa (sin necesidad de que intervenga el usuario) cuando se establece una conexión a Internet.

Activación y configuración de LiveUpdate continuo

Se puede activar LiveUpdate continuo desde Symantec System Center o modificando valores del registro en los clientes de Symantec AntiVirus Corporate Edition. Es posible configurar las opciones de LiveUpdate continuo mediante la adición de valores en el registro de los clientes.

Para activar LiveUpdate continuo utilizando Symantec System Center

1. En Symantec System Center, haga clic con el botón derecho en un grupo de servidores, en un servidor de Symantec AntiVirus Corporate Edition, en un grupo de clientes o en un único cliente de Symantec AntiVirus Corporate Edition y, a continuación, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Administrador de definiciones de virus**.
2. En el cuadro de diálogo Administrador de definiciones de virus, haga clic en **Activar LiveUpdate continuo**.
3. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Para activar LiveUpdate continuo cambiando valores del registro

1. Utilizando el Editor del Registro, acceda a: HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\PatternManager
2. Agregue EnableAdminForcedLU como nuevo valor DWORD.
3. Establezca para el nuevo DWORD uno de los siguientes valores:
   - 1: Activar
   - 0: Desactivar

Para configurar LiveUpdate continuo

- Haga uso de los siguientes valores del registro para configurar LiveUpdate continuo:

EnableAdminForcedLU	Establezca este valor en 0 para desactivar LiveUpdate continuo o en 1 para activarlo.
MaxDefsDaysOldAllowed	Especifique el número de días que pueden tener los archivos de definiciones de virus antes de que Symantec AntiVirus Corporate Edition ejecute una sesión silenciosa de LiveUpdate.
AdminForcedLUCheckInterval	Especifique el intervalo en segundos para la comprobación de definiciones antiguas.
AFLUDelay	Establezca el tiempo de retraso (entre 10 y 180 minutos) con que se iniciará la función LiveUpdate continuo. Este tiempo de retraso sólo es válido cuando la función está activada. El tiempo de retraso real es un número aleatorio comprendido entre 8 y N+8, donde N es el valor de la clave de registro. El valor predeterminado es de 30 minutos.

Nota: Es recomendable definir el valor de MaxDefsDaysOldAllowed en 8 días como mínimo. Si se definen valores inferiores, pueden producirse problemas al intentar recuperar archivos de definiciones de virus anteriores, ya que los archivos que se deseen recuperar pueden exceder el número máximo de días permitidos por LiveUpdate continuo antes de forzar la actualización.

Configuración de las políticas de uso de LiveUpdate

Existe la posibilidad de configurar políticas de uso de LiveUpdate para clientes administrados. Cuando se seleccionan estas opciones, aparecen como no disponibles en el cliente. Las políticas determinan si las siguientes actividades pueden llevarse a cabo en el cliente:

- Cambiar la planificación de actualizaciones de LiveUpdate.
- Ejecutar LiveUpdate manualmente.

Para definir las políticas de uso de LiveUpdate

1. En la consola de Symantec System Center, haga clic con el botón derecho en un servidor o un grupo de servidores y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Administrador de definiciones de virus**.
2. Realice una de las acciones siguientes:
   - Haga clic en **No permitir que el cliente modifique la planificación de LiveUpdate** para impedir que se pueda modificar la planificación de actualizaciones de LiveUpdate en el cliente. (La opción Planificar actualizaciones automáticas mediante LiveUpdate en el cliente debe estar seleccionada o, de lo contrario, esta opción no estará disponible.)
   - Desactive la casilla **Descargar actualizaciones del producto con LiveUpdate** para impedir la actualización de aplicaciones.
   - Marque la casilla **No permitir que el cliente ejecute LiveUpdate manualmente** para impedir que LiveUpdate se pueda ejecutar en el cliente de forma manual.

Nota: Si alguna de las casillas No permitir que el cliente modifique la planificación de LiveUpdate o No permitir que el cliente ejecute LiveUpdate manualmente está desactivada, LiveUpdate podrá ejecutarse desde el cliente en cualquier momento.

Control de los archivos de definiciones de virus

La consola de Symantec System Center proporciona un conjunto de herramientas que permiten controlar la distribución de archivos de definiciones de virus en la red. Use estas herramientas para realizar las siguientes tareas:

- Comprobar la fecha de los archivos de definiciones de virus en los servidores.
- Ver la lista de virus de los servidores y los clientes.
- Recuperar un archivo de definiciones de virus previo en toda la red.

Si los archivos de definiciones de virus nuevos causan falsos positivos u otro tipo de problemas en un servidor específico, se puede comprobar el número de versión de los archivos de definiciones de virus de ese equipo e implantar un conjunto de definiciones anterior desde la consola de Symantec System Center. Todos los servidores y clientes que pertenezcan al grupo recuperarán los archivos de definiciones de virus especificados. Además, es posible controlar la versión de los archivos de definiciones de virus que se emplean en todos los servidores y clientes de un grupo de servidores. Así, es posible obligar a los usuarios que hayan descargado un archivo de definiciones de virus que aún no haya sido aprobado para su uso en una empresa a utilizar otro archivo. Gracias a la sencillez con que puede deshacerse la distribución de un archivo de definiciones de virus, es posible distribuir los nuevos archivos de definiciones en menos tiempo.

Symantec System Center muestra un icono de advertencia en el caso de que un archivo de definiciones de virus esté obsoleto en uno o varios equipos administrados por un servidor principal, en un grupo de servidores o en un grupo de clientes.

Para buscar los equipos que cuentan con definiciones obsoletas

- Expanda el servidor, el grupo de servidores o el grupo de clientes para encontrar iconos de advertencia adicionales.

Comprobación del número de versión de los archivos de definiciones de virus

Symantec System Center permite ver el número de versión de los archivos de definiciones de virus que se emplean en servidores de Symantec AntiVirus Corporate Edition, en grupos de servidores, en grupos de clientes y en clientes de Symantec AntiVirus Corporate Edition por separado.

Para comprobar el número de versión de los archivos de definiciones de virus

- En Symantec System Center, haga clic con el botón derecho en un grupo de servidores, un grupo de clientes, un servidor de Symantec AntiVirus Corporate Edition o un cliente y, a continuación, haga clic en **Propiedades**.

  En el cuadro Definiciones de virus de la ficha Symantec AntiVirus, la versión del archivo se muestra como una fecha numérica seguida de un número de versión.

  Pueden transcurrir varios minutos antes de que la información esté disponible desde la consola una vez actualizados los archivos de definiciones de virus de un equipo.

Visualización de la lista de virus

Existe la posibilidad de ver una lista de los virus que pueden detectarse en un servidor o un cliente seleccionado. La lista de virus garantiza que el equipo seleccionado se encuentra protegido ante un virus concreto.

Para ver la lista de virus

- Haga clic con el botón derecho en el servidor o el cliente y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Ver lista de virus**.

Uso de versiones anteriores de los archivos de definiciones de virus

Es posible utilizar versiones anteriores de los archivos de definiciones de virus de un grupo de servidores. Puede ser necesario si, por ejemplo, el archivo más reciente ha generado falsos positivos durante el proceso de detección de virus.

Nota: El uso de versiones anteriores de los archivos de definiciones de virus provoca la eliminación de las definiciones de virus más recientes.

Para utilizar versiones anteriores de los archivos de definiciones de virus

1. En Symantec System Center, haga clic con el botón derecho en un grupo de servidores o en un servidor y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Administrador de definiciones de virus**.
2. Asegúrese de que la casilla de verificación Actualizar sólo el servidor primario del grupo de servidores del cuadro de diálogo Administrador de definiciones de virus esté marcada y después haga clic en **Configurar**.
3. En el cuadro de diálogo Configuración de actualizaciones de servidores primarios, haga clic en **Archivo de definiciones**.
4. En el cuadro de diálogo Selección de archivo de definiciones de virus, elija el archivo de definiciones de virus que desee volver a utilizar y seguidamente haga clic en **Aplicar**.
5. Haga clic en **Sí** para sustituir el archivo en uso.
6. Haga clic en **Aceptar** hasta que aparezca la ventana principal de Symantec System Center.

Prueba de los archivos de definiciones de virus

Muchos administradores prefieren comprobar los archivos de definiciones de virus en una red de prueba antes de ponerlos a disposición de los usuarios en un servidor operativo. Para probar los archivos de definiciones de virus, realice las siguientes acciones:

- Instale el servidor de Symantec AntiVirus Corporate Edition en un servidor primario de la red de prueba.
- Desde el servidor primario de la red de prueba, ejecute LiveUpdate con objeto de descargar el archivo de definiciones de virus.
- Acceda a www.eicar.org y descargue el archivo de prueba de antivirus para probar el funcionamiento de los archivos de definiciones de virus.
- Cuando finalice la prueba, copie los archivos de definiciones de virus de la carpeta \Archivos de programa\Nav del servidor de prueba a la misma carpeta de los servidores primarios de la red de producción.
- Una vez que los archivos de definiciones de virus se encuentran en los servidores primarios, pueden distribuirse a otros servidores del grupo.

Nota: Los clientes estarán configurados para obtener automáticamente los archivos de definiciones de virus de los servidores principales si está activada la opción Actualizar definiciones de virus desde el servidor principal del cuadro de diálogo Administrador de definiciones de virus.

Situaciones posibles de actualización

Los siguientes ejemplos muestran cómo realizan las actualizaciones los administradores de dos empresas distintas:

- El administrador de la Empresa A descarga los nuevos archivos de definiciones de virus desde el sitio FTP o el servidor de LiveUpdate de Symantec a un servidor primario de la red de prueba. Acto seguido, comprueba estos archivos y, una vez finalizada la comprobación, los copia al servidor primario maestro de la red operativa. Los demás servidores primarios se encuentran configurados para obtener la actualización desde el servidor primario maestro, mientras que el resto de los equipos conectados utiliza el método de transporte de definiciones de virus. Los servidores secundarios obtienen la actualización desde su servidor primario. A su vez, los clientes obtienen la actualización desde su servidor principal. (En el caso de clientes con Windows 3.1 y MS-DOS, ésta se recibe al producirse la siguiente conexión con el sistema.)
- El administrador de la Empresa B descarga los nuevos archivos de definiciones de virus desde el sitio FTP o el servidor de LiveUpdate de Symantec a la red de prueba. Acto seguido, comprueba estos archivos y, una vez finalizada la comprobación, los descarga desde el sitio FTP o el servidor de LiveUpdate de Symantec al servidor de LiveUpdate interno perteneciente a la red operativa. Algunos de los usuarios de bajo riesgo pueden atravesar el firewall. Así, al ejecutar LiveUpdate en esos equipos, los archivos de definiciones de virus se descargan directamente desde el sitio FTP o el servidor de LiveUpdate de Symantec.

Capítulo 5

Respuesta a infecciones víricas

En este capítulo se tratan los temas siguientes:

- Acerca de la respuesta a infecciones víricas
- Preparación para responder a una infección vírica
- Tratamiento de una infección vírica en la red

Acerca de la respuesta a infecciones víricas

Para poder responder a infecciones víricas es preciso estar preparado antes de que se produzcan y contar con una estrategia definida para gestionar las infecciones en caso de que ocurran.

Además de instalar Symantec AntiVirus Corporate Edition en los servidores y las estaciones de trabajo de la red, es necesario realizar las siguientes tareas con el fin de prepararse para responder a infecciones víricas:

- Crear y revisar un plan de respuesta ante infecciones de virus.
- Definir las acciones de Symantec AntiVirus Corporate Edition para gestionar los virus.
- La estrategia para gestionar infecciones víricas incluye lo siguiente:
  - Activar mensajes y alertas de virus.
  - Ejecutar un barrido de virus en la red.
  - Realizar seguimientos de los virus mediante registros.
  - Utilizar la consola de Cuarentena central para supervisar las máquinas infectadas de la red y enviar muestras de los archivos que puedan estar infectados a Symantec Security Response para que los analicen y eliminen la infección.

Preparación para responder a una infección vírica

Con el fin de estar preparado para responder a una infección vírica, conviene crear un plan de respuesta ante infecciones y definir acciones para gestionar los archivos que puedan estar infectados.

Creación de un plan de respuesta a infecciones víricas

Para poder ofrecer una respuesta efectiva a una infección vírica en la red, es preciso contar con un plan que permita reaccionar rápida y eficazmente. La Tabla 5-1 resume las acciones necesarias para crear un plan de respuesta ante infecciones.

Tabla 5-1 Plan de respuesta ante infecciones víricas

Tarea	Descripción
Comprobar que los archivos de definiciones de virus estén al día	Comprobar que los equipos infectados cuenten con los archivos de definiciones de virus más recientes y utilizar el método de transporte de definiciones de virus para dotarlos de nuevas definiciones si es preciso. Vea "Acerca de los archivos de definiciones de virus" en la página 134.
Realizar un mapa de la topología de la red	Preparar un mapa de la topología de la red que permita aislar y limpiar sistemáticamente los equipos por segmentos antes de volver a conectarlos a la red local. El mapa debe incluir la siguiente información: ■ Nombres y direcciones de los servidores ■ Nombres y direcciones de los clientes ■ Protocolos de red ■ Recursos compartidos
Identificar el virus	Los registros de Symantec AntiVirus Corporate Edition constituyen una fuente de información fiable sobre los virus de la red. Si es posible identificar un virus a partir de los registros, se puede obtener información sobre cómo eliminarlo en la enciclopedia de virus de Symantec Security Response.
Responder a virus desconocidos	Si no se puede identificar el virus de un archivo sospechoso examinando los registros y el archivo no se limpia con las últimas definiciones de virus, acceda a la dirección http://securityresponse.symantec.com y consulte la información (en inglés) de las áreas Latest Virus Threats (amenazas de virus más recientes) y Security Advisories (consejos de seguridad).

Tabla 5-1 Plan de respuesta ante infecciones víricas

Tarea	Descripción
Conocer las soluciones de seguridad	Además de estar familiarizado con la topología de la red, debe conocer la instalación de Symantec AntiVirus Corporate Edition, así como la de cualquier otro producto de seguridad que se emplee en la red. Considere las preguntas siguientes: ■ ¿Cuáles son los programas de seguridad que protegen los servidores y estaciones de trabajo de la red? ■ ¿Cuál es la planificación para actualizar las definiciones de virus? ■ ¿De qué métodos alternativos se dispone para obtener las actualizaciones si los canales normales son atacados? ■ ¿Qué archivos de registro están disponibles para realizar un seguimiento de los virus en la red?
Contar con un plan de copias de respaldo	En el caso de que se produzca una infección vírica catastrófica, puede que sea necesario restaurar servidores y clientes para garantizar que la red no se ha visto comprometida. Resulta fundamental en estos casos contar con un plan de copias de respaldo para restaurar los equipos afectados.

Definición de acciones de Symantec AntiVirus Corporate Edition para gestionar los archivos sospechosos

De forma predeterminada, Symantec AntiVirus Corporate Edition realiza las siguientes acciones cuando identifica un archivo sospechoso:

- Symantec AntiVirus Corporate Edition intenta reparar el archivo.
- Si el archivo no se puede reparar con el juego de archivos de definiciones de virus en uso, el archivo infectado se pone en cuarentena en el equipo local. Además, se registra una entrada relativa al suceso de virus en el archivo de registro del cliente de Symantec AntiVirus Corporate Edition. Los datos del cliente de Symantec AntiVirus Corporate Edition se envían a un servidor primario. Los datos de registro se pueden ver desde la consola de Symantec System Center.

Se pueden llevar a cabo las acciones adicionales que se indican a continuación con el fin de completar la estrategia para el tratamiento de virus:

- Definir distintas acciones de reparación, según el tipo de virus. Por ejemplo, puede hacer que Symantec AntiVirus Corporate Edition repare automáticamente virus de macro, pero que pregunte la acción que se deba realizar cuando se detecte un virus de archivos de programa.
- Asignar una acción de reserva para los archivos que Symantec AntiVirus Corporate Edition no pueda reparar, como suprimir el archivo infectado, por ejemplo.
- Recibir alertas de virus, como un aviso en un buscapersonas o un mensaje de correo electrónico, si se utiliza AMS^2.
- Configurar el área de cuarentena local para que envíe los archivos infectados a Cuarentena central. Se puede configurar Cuarentena central para que intente reparar los archivos mediante sus propios archivos de definiciones de virus (que pueden ser más recientes que los de los equipos locales), o para que envíe muestras de los archivos infectados a Symantec Security Response para su análisis.

Vea "Acerca de Alert Management System" en la página 54.

Consulte la guía del administrador de Cuarentena central, *Symantec Central Quarantine Administrator's Guide,* si desea obtener más información (en inglés).

Depuración automática de archivos sospechosos del área de cuarentena local

Cuando Symantec AntiVirus Corporate Edition detecta un archivo sospechoso, lo coloca en la carpeta del área de cuarentena local del equipo afectado. La función de depuración de cuarentena permite eliminar automáticamente archivos del área de cuarentena que sean anteriores a una determinada fecha.

La configuración de registro de la función de depuración de cuarentena se encuentra en la siguiente clave del registro:

\\HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\Quarantine

La Tabla 5-2 recoge las opciones de depuración de cuarentena posibles.

Tabla 5-2 Opciones de depuración de cuarentena

Valor	Opciones	Descripción
QuarantinePurgeEnabled	0/1	Desactiva o activa la depuración
QuarantinePurgeAgeLimit	X	Permite especificar el número máximo de días que puede permanecer un archivo en el directorio de cuarentena
QuarantinePurgeFrequency	X	Permite establecer la frecuencia de depuración: 0=Días, 1=Meses, 2=Años
BackupItemPurgeEnabled	0/1	Desactiva o activa la depuración de archivos de copia de respaldo
BackupItemPurgeAgeLimit	X	Permite especificar el número máximo de días que puede permanecer un archivo de copia de respaldo en el área de cuarentena
BackupItemPurgeFrequency	X	Permite establecer la frecuencia de depuración de los archivos de copia de respaldo: 0=Días, 1=Meses, 2=Años
RepairedItemPurgeEnabled	0/1	Desactiva o activa la depuración de archivos reparados
RepairedItemPurgeFrequency	X	Permite establecer la frecuencia de depuración de los archivos reparados: 0=Días, 1=Meses, 2=Años

Tratamiento de una infección vírica en la red

Symantec AntiVirus Corporate Edition proporciona las siguientes herramientas para tratar las infecciones víricas de la red:

- Alertas: se envían alertas de AMS^2 e integradas.
- Barridos de virus: se fuerza un análisis de virus en toda la jerarquía del sistema, en el grupo de servidores o en un solo servidor.
- Registros de sucesos e historias: permiten realizar un seguimiento de los virus y de los envíos a Cuarentena central desde un grupo de servidores, un solo servidor o un solo cliente.
- Consola de Cuarentena central: permite realizar un seguimiento de los envíos a Symantec Security Response.
- Disco de emergencia: permite limpiar los virus del sector de arranque.

Uso de mensajes y alertas de virus

Se pueden utilizar las alertas y los mensajes para obtener información sobre los archivos sospechosos que Symantec AntiVirus Corporate Edition detecte en la red. Symantec AntiVirus Corporate Edition ofrece los siguientes mecanismos de notificación:

- AMS^2: si se configuran para ello, los clientes de Symantec AntiVirus Corporate Edition pueden enviar sucesos de virus a un servidor de AMS^2. Se pueden configurar los servidores de AMS^2 para que envíen alertas a un buscapersonas, a una dirección de correo electrónico o a cualquier otro dispositivo de notificación.

  Consulte "Acerca de Alert Management System" en la página 54.
- Mensajes personalizados: desde la consola de Symantec System Center se puede definir un mensaje personalizado para que se muestre en los clientes de Symantec AntiVirus Corporate Edition cuando se detecte un archivo sospechoso.

  Consulte "Visualización y personalización de mensajes de aviso en los equipos infectados" en la página 114.

Ejecución de barridos de virus

Si se detectan varios archivos sospechosos, no se podrá tener certeza de si el problema se encuentra localizado en el equipo o el servidor donde se haya detectado, o si se ha extendido a otras áreas de la red. Puede ser recomendable iniciar un barrido de virus mediante Symantec System Center. El número de equipos que se verificarán depende de la forma en que se inicie el barrido.

Si no se puede acceder a un cliente de Symantec AntiVirus Corporate Edition durante un barrido de virus, Symantec AntiVirus Corporate Edition realizará una de las siguientes acciones:

- En sistemas operativos de 32 bits: se analizará el equipo tan pronto como se encienda. No es necesario que la computadora inicie una sesión en la red.
- En sistemas operativos de 16 bits: se analizará el equipo tan pronto como se encienda e inicie la sesión en la red.

Según el objeto que se seleccione en la consola de Symantec System Center, se podrá ejecutar un barrido de virus en toda la red, en un grupo de servidores o en un solo servidor.

Advertencia: Un barrido de virus puede crear un tráfico de red considerable, cuya densidad y duración dependerán del tamaño de la red. Una vez iniciado un barrido de virus no es posible detenerlo hasta que finaliza.

Para ejecutar un barrido de virus

1. En Symantec System Center, haga clic con el botón derecho en la red, en un grupo de servidores o en un servidor y, a continuación, haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Iniciar barrido de virus**.
2. Escriba un nombre para el barrido en el cuadro Nombre.
3. Haga clic en **Iniciar**.
   Vea "Configuración de opciones de análisis" en la página 110.

Seguimiento de alertas de virus mediante registros de sucesos e historias

Es posible realizar un seguimiento de las alertas de detección de virus desde la consola de Symantec System Center. De forma predeterminada, las alertas de detección de virus aparecerán durante tres días, si bien se puede modificar el número de días.

Consulte "Acerca de las historias y los registros de sucesos" en la página 190.

Seguimiento de envíos a Symantec Security Response con la consola de Cuarentena central

Symantec System Center registra un suceso cada vez que un cliente de Symantec AntiVirus Corporate Edition envía un archivo sospechoso a Symantec Security Response. Además de registrar el suceso, se puede realizar un seguimiento del estado en tiempo real de los envíos a Symantec Security Response desde la consola de Cuarentena central.

Si desea obtener información (en inglés) sobre cómo utilizar la consola de Cuarentena central, consulte la guía del administrador de Cuarentena central, *Symantec Central Quarantine Administrator's Guide*.

Capítulo 6

Administración de clientes de uso móvil

En este capítulo se tratan los temas siguientes:

- Acerca de los clientes de uso móvil
- Componentes de los clientes de uso móvil
- Funcionamiento del soporte para clientes de uso móvil
- Implantación del soporte para clientes de uso móvil
- Configuración de las opciones de clientes de uso móvil
- Opciones de la línea de comandos
- Valores del registro

Acerca de los clientes de uso móvil

Los clientes de uso móvil pueden realizar las siguientes tareas:

- Identificar automáticamente el servidor principal más adecuado, basándose en la velocidad y la proximidad, y convertirse en un cliente administrado por ese servidor. Por ejemplo, cuando un usuario móvil que normalmente se encuentra en Nueva York se desplaza a California, el cliente de uso móvil detecta la nueva dirección de red y asigna al portátil del usuario el servidor principal más adecuado.
- Conectar con el servidor principal apropiado más próximo siempre que cambia su dirección de red.
- Conectar con un servidor principal distinto si el servidor que utiliza deja de estar disponible.
- Comprobar periódicamente el servidor principal más próximo para ajustarse a los posibles cambios en los servidores o en la carga de éstos.
- Intentar equilibrar la carga de un grupo de servidores equivalentes al seleccionar un servidor principal.
- En el caso de clientes no administrados que se convierten en clientes administrados, identificar automáticamente el servidor principal más adecuado cuando el cliente se conecta a la red. Por ejemplo, es posible que una empresa tenga un centro de distribución para equipos nuevos. Los administradores pueden activar el uso móvil en esos equipos antes de enviarlos a las sucursales, lo que supone que deben especificar todos los servidores de uso móvil posibles en ellos. Cuando los usuarios finales conectan sus nuevos equipos a la red, Symantec AntiVirus Corporate Edition les asigna automáticamente el servidor principal más adecuado.

Componentes de los clientes de uso móvil

En la Tabla 6-1 se incluyen los componentes de los clientes de uso móvil.

Tabla 6-1 Componentes de los clientes de uso móvil

Componente	Descripción
Lista de servidores de nivel 0	Recoge una lista de los servidores de nivel 0 disponibles como posibles servidores de uso móvil para un cliente de uso móvil determinado. Los clientes de uso móvil almacenan esta información en sus registros. Vea "Análisis de la red de Symantec AntiVirus Corporate Edition y elaboración de un mapa" en la página 175. Vea "Creación de una lista de servidores de Symantec AntiVirus Corporate Edition del nivel 0" en la página 177.
Lista jerárquica de servidores	Recoge una lista de todos los servidores de uso móvil, agrupados por nivel jerárquico. Los servidores de uso móvil almacenan esta información en sus registros. Vea "Análisis de la red de Symantec AntiVirus Corporate Edition y elaboración de un mapa" en la página 175. Vea "Creación de una lista jerárquica de servidores de Symantec AntiVirus Corporate Edition" en la página 177.
Roamadmn.exe	Configura el acceso móvil en los servidores de Symantec AntiVirus Corporate Edition. Vea "Configuración del soporte para clientes de uso móvil en servidores de uso móvil" en la página 181.
Navroam.exe	Proporciona información sobre los servidores de uso móvil a los clientes móviles. Vea "Configuración del soporte para clientes de uso móvil en los clientes" en la página 178.

Funcionamiento del soporte para clientes de uso móvil

En el soporte para clientes de uso móvil se emplean dos tipos de listas: una o varias listas de servidores de nivel 0 y una lista jerárquica de los servidores que darán soporte a los clientes de uso móvil. Los clientes de uso móvil almacenan la lista del nivel 0 en sus registros y la utilizan para identificar los servidores a los que se intentarán conectar. Cuando se desee implementar el soporte para clientes móviles en la red, se debe comenzar por crear la lista (o las listas) de servidores de nivel 0 y la lista jerárquica. Tras distribuir los datos, en los clientes de uso móvil tiene lugar lo siguiente:

- El archivo Navroam.exe se ejecuta en el cliente de Symantec AntiVirus Corporate Edition al iniciarlo y selecciona el servidor de Symantec AntiVirus Corporate Edition más apropiado, según los valores del registro y la información que se obtenga del servidor.
- El servidor seleccionado proporciona al cliente una lista de los servidores que se encuentran en el siguiente nivel de la jerarquía de la red. Navroam explora toda la jerarquía de la red hasta el nivel más bajo. El último servidor se convierte en el nuevo servidor principal del cliente y transmite inmediatamente la configuración completa al cliente de uso móvil.
- Navroam realiza las siguientes comprobaciones a intervalos regulares:
  - Comprueba la disponibilidad y el tiempo de respuesta del servidor principal. Si el servidor principal no está disponible, o si hay otro servidor principal que pueda proporcionar un mayor rendimiento, Navroam conecta el cliente con un nuevo servidor principal de la red.
  - Comprueba la dirección de red del equipo. Si la dirección ha cambiado, se conecta al nuevo servidor principal más adecuado.
  - Si el cliente tenía asignado previamente otro servidor principal, Navroam intenta borrarse de ese servidor después de registrarse en el nuevo.

Implantación del soporte para clientes de uso móvil

Para implantar el soporte para clientes de uso móvil, se deben realizar las siguientes acciones:

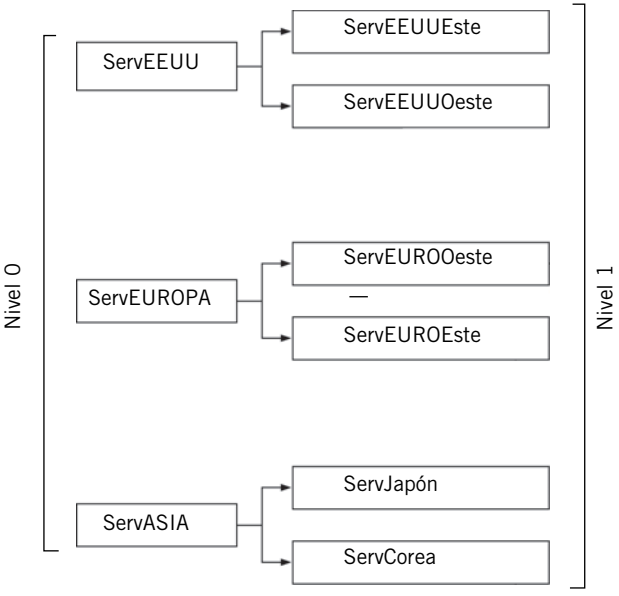
- Analizar la red de Symantec AntiVirus Corporate Edition y elaborar un mapa.
- Identificar los servidores de cada región que dirigen a los clientes de uso móvil al siguiente nivel de servidores.
- Crear una lista de servidores del nivel 0 para los clientes de uso móvil.
- Crear una lista jerárquica de todos los servidores de uso móvil, distribuidos en niveles jerárquicos e identificados por tipo (como servidor de cuarentena o de alertas, por ejemplo), si es necesario.
- Configurar el soporte para clientes de uso móvil en estos clientes.
- Configurar el soporte para clientes de uso móvil en los servidores móviles.

Análisis de la red de Symantec AntiVirus Corporate Edition y elaboración de un mapa

Si la red de que dispone está compuesta por muchos servidores, es probable que quiera asignar sólo algunos de ellos como servidores de uso móvil. La creación de un mapa jerárquico de la red le permitirá identificar rápidamente los servidores de uso móvil de ésta.

La Figura 6-1 representa un mapa de la red de una empresa establecida en tres continentes. Aunque esta organización puede contar con más servidores de Symantec AntiVirus Corporate Edition de los que aparecen en el mapa, sólo los servidores representados en él están identificados como servidores de referencia regionales.

Figura 6-1 Ejemplo de mapa de empresa



Identificación de los servidores de cada nivel jerárquico

Para identificar los servidores de cada nivel jerárquico, se deben analizar las necesidades de los usuarios móviles. Por ejemplo, puede ser necesario determinar si los usuarios móviles viajan por distintos países, por un mismo país o por un área geográfica más pequeña. Si los usuarios viajan por distintos países, la lista de servidores correspondiente incluirá los nombres de los servidores de los países en el nivel 0. Si se desplazan dentro de un mismo país, la lista de servidores correspondiente incluirá servidores desde el nivel 1.

Según la velocidad de la red, la lista de servidores podría incluir únicamente los servidores del nivel superior (nivel 0 en la Figura 6-1), lo que simplifica la creación de la lista de servidores del cliente. La única limitación al número de niveles que se pueden definir está impuesta por el límite de 512 caracteres de tamaño del archivo de texto.

Creación de una lista de servidores de Symantec AntiVirus Corporate Edition del nivel 0

La lista de servidores de un cliente se debe crear en un archivo de texto utilizando un editor como el Bloc de notas, por ejemplo. El archivo de texto de la lista de servidores debe incluir líneas con el formato siguiente:

<local><tipo de servidor><nivel><lista de servidores>

donde:

- <local> indica al cliente que debe intentar contactar con el nivel 0 de servidores cuando busque un servidor de uso móvil;
- <tipo de servidor> corresponde al tipo de servidor (servidor principal, de cuarentena, de Grc.dat o de alertas);
- <nivel> es 0;
- <lista de servidores> representa la lista de servidores, separados por comas (se pueden incluir espacios entre las comas si se desea).

Por ejemplo, el archivo de texto de la lista de servidores de un cliente correspondiente a la Figura 6-1 sería el siguiente:

<local> Principal 0 ServEEUU,ServEUROPA,ServASIA

Ésta es la única línea en la lista de servidores correspondiente a los clientes de uso móvil en el ejemplo. La lista indica a los clientes que deben contactar únicamente con estos tres servidores y comparar los tiempos de respuesta. Según el servidor que ofrezca la mejor respuesta, el cliente continuará la búsqueda en los siguientes niveles de la lista en uno de los tres continentes.

Creación de una lista jerárquica de servidores de Symantec AntiVirus Corporate Edition

Para crear la lista jerárquica se utilizará un editor de texto como Bloc de notas. Se deben incluir líneas con el siguiente formato:

<equipo> <tipo de servidor> <nivel> <lista de servidores>

donde:

- <equipo> corresponde al nombre de host del servidor;
- <tipo de servidor> corresponde al tipo de servidor, como servidor principal, de cuarentena, de Grc.dat o de alertas, por ejemplo;
- <nivel> es el nivel especificado en el archivo de texto de la lista de servidores;
- <lista de servidores> representa la lista de servidores, separados por comas (se pueden incluir espacios entre las comas si se desea).

Por ejemplo, en el mapa de empresa de la Figura 6-1, la rama de EE.UU. tendría la siguiente lista de servidores:

ServEEUU Principal 1 ServEEUUOeste,ServEEUUEste

Configuración del soporte para clientes de uso móvil en los clientes

La configuración del soporte para clientes de uso móvil en este tipo de clientes implica las siguientes tareas:

- Activación y configuración del soporte para uso móvil en cada cliente de uso móvil
- Adición de información de servidores de nivel 0 al registro de cada cliente de uso móvil

Activación y configuración del soporte para uso móvil en cada cliente de uso móvil

Se puede activar y configurar el soporte para uso móvil en los clientes de Symantec AntiVirus Corporate Edition definiendo los valores necesarios en un archivo de configuración (Grc.dat) o editando directamente el registro de cada cliente de uso móvil mediante el Editor del Registro. Escriba los valores del registro en la siguiente clave:

HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\ProductControl

La Tabla 6-2 recoge y describe los distintos valores del registro.

Tabla 6-2 Valores del registro de los clientes de uso móvil

Valor	Descripción
ProductControl\RoamClient	1: Activa el soporte para clientes de uso móvil (predeterminado). 0: Desactiva el soporte para clientes de uso móvil.
ProductControl\RoamQuarantine	1: Activa el uso móvil de Cuarentena central. 0: Desactiva el uso móvil de Cuarentena central (predeterminado).
ProductControl\RoamAlerts	1: Activa el uso móvil del servidor de alertas. 0: Desactiva el uso móvil del servidor de alertas (predeterminado).

Tabla 6-2 Valores del registro de los clientes de uso móvil

Valor	Descripción
ProductControl\CheckForNewParent IntervalInSeconds	Frecuencia en segundos con que se buscará un nuevo servidor principal (el valor predeterminado es cada 30 segundos).
ProductControl\CheckParentIntervalIn Minutes	Frecuencia en minutos con que se comprobará la disponibilidad del servidor principal (el valor predeterminado es cada 120 minutos).
ProductControl\SampleCountForParent Check	Número de veces que se debe comprobar la disponibilidad y el tiempo de respuesta de cada servidor principal. Se obtiene una media de todas las respuestas para calcular el tiempo de respuesta final (el valor predeterminado es 7).
ProductControl\FindNearestParent IntervalInMinutes	Intervalo en minutos tras el cual se debe buscar un servidor principal más próximo (el valor predeterminado es de 60 minutos).
ProductControl\RoamManagingParent Level0	Lista de los servidores principales cuya proximidad se debe comprobar.
ProductControl\RoamManagingGRC Level0	Lista de servidores de GRC cuya proximidad se debe comprobar.
ProductControl\RoamManaging QuarantineLevel0	Lista de servidores de cuarentena cuya proximidad se debe comprobar.
ProductControl\RoamManagingAlert Level0	Lista de servidores de alertas cuya proximidad se debe comprobar.

Si desea obtener información sobre el uso del archivo de configuración, consulte la *Guía de referencia de Symantec AntiVirus Corporate Edition*.

Adición de información de servidores de nivel 0 al registro de cada cliente de uso móvil

Symantec AntiVirus Corporate Edition proporciona los dos métodos siguientes para agregar información de servidores de nivel 0 al registro de los clientes de uso móvil:

- Crear un archivo de configuración (Grc.dat) que contenga los valores de registro necesarios e implantarlo cuando se distribuyan los clientes de uso móvil.
- Utilizar NAVRoam.exe para combinar los valores de registro necesarios en el registro de cada cliente de uso móvil. De forma predeterminada Symantec AntiVirus Corporate Edition copia el archivo NAVRoam.exe en el directorio de instalación de los clientes durante la instalación.

Si desea obtener información sobre el uso del archivo de configuración, consulte la *Guía de referencia de Symantec AntiVirus Corporate Edition*.

Para importar la información de la lista de servidores utilizando NAVRoam

1. Cree una carpeta denominada ToNAV en el directorio donde se encuentren los archivos originales de instalación del cliente de Symantec AntiVirus Corporate Edition y coloque en ella el archivo con la lista de servidores.
2. Instale el cliente de Symantec AntiVirus Corporate Edition.
   Durante el proceso de instalación se copiará automáticamente el contenido de la carpeta ToNAV en la carpeta de instalación adecuada.
3. Desde una solicitud de comando, acceda a la carpeta que contenga el archivo NAVRoam.exe y de la lista de servidores y escriba:
   NAVRoam /import listadeservidores.txt
   donde listadeservidores.txt es el archivo de texto que contiene la información de la lista de servidores.

Vea "Opciones de la línea de comandos" en la página 184.

Configuración del soporte para clientes de uso móvil en servidores de uso móvil

Para configurar el uso móvil de un servidor de Symantec AntiVirus Corporate Edition, es preciso realizar las siguientes tareas:

- Activar el uso móvil definiendo una clave de registro en cada servidor de uso móvil.
- Distribuir la lista jerárquica de servidores a cada servidor de uso móvil con RoamAdmn.exe, que está ubicado en Disk 1, en la carpeta AdmTools.
- Configurar, si se desea, servidores de Symantec AntiVirus Corporate Edition alternativos, de respaldo y de balanceo de carga.

Activación del uso móvil y distribución de la lista jerárquica de servidores

Para activar el uso móvil es preciso agregar un valor al registro de cada servidor de uso móvil y distribuir la información de la lista de servidores. A continuación, se debe copiar el archivo RoamAdmn.exe al equipo desde el que se vaya a trabajar para distribuir la lista jerárquica de servidores a los servidores de uso móvil. Cuando se ejecuta RoamAdmn, se comunica con cada uno de los servidores que aparecen al principio de cada línea en la lista jerárquica de servidores. En cada servidor, RoamAdmn agrega un valor del registro que contiene los servidores situados en el siguiente nivel de la jerarquía. Si no se puede conectar con un servidor, se ignora.

Para activar el uso móvil

- Agregue los valores de DWORD a la siguiente clave de registro:
  HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\ProductControl\RoamServer

Para distribuir la lista jerárquica de servidores

- En la línea de comandos, escriba lo siguiente:
  RoamAdmn /import listadeservidores.txt
  donde listadeservidores.txt representa el nombre de la lista jerárquica de servidores que se haya creado.

Ejemplo de servidor de uso móvil

Una empresa dispone de un equipo desde el que son visibles todos los servidores de uso móvil. El archivo listaservidores.txt incluye las siguientes líneas:

ServEEUU Principal 1 ServEEUUOeste,ServEEUUEste

ServEUROPA Principal 1 ServEUROEste,ServEUROOeste

ServASIA Principal 1 ServJapón,ServCorea

La Tabla 6-3 describe los datos del archivo listadeservidores.txt tal y como aparecen en el registro de cada servidor de uso móvil.

Tabla 6-3 Valores de registro de ejemplo

Nombre del servidor	Valor del registro	Datos
ServEEUU	RoamManagingParentLevel1	ServEEUUOeste,ServEEUUEste
ServEUROPA	RoamManagingParentLevel1	ServEUROEste,ServEUROOeste
ServASIA	RoamManagingParentLevel1	ServJapón,ServCorea

Configuración de las opciones de clientes de uso móvil

La Tabla 6-4 recoge y describe las opciones para clientes de uso móvil.

Tabla 6-4 Opciones de clientes de uso móvil

Opción	Descripción
Balanceo de carga	Si cuenta con varios servidores y desea distribuir los clientes de uso móvil entre ellos, se puede equilibrar la carga haciendo que los servidores de uso móvil sean tratados como iguales con independencia del tiempo que lleve a los clientes contactar con ellos. Los clientes de uso móvil contactarán con cada servidor de la lista. Los servidores de uso móvil mantienen un recuento de los clientes de Symantec AntiVirus Corporate Edition que administran y devuelven este valor al cliente móvil. Éste selecciona entonces el servidor que cuente con un número menor de clientes y lo convierte en su nuevo servidor principal. El equilibrio de la carga es más importante que encontrar el servidor más próximo.

Tabla 6-4 Opciones de clientes de uso móvil

Opción	Descripción
Servidores de respaldo	Se pueden especificar servidores de respaldo para que respondan a los clientes cuando otros servidores de uso móvil no estén disponibles. El cliente móvil comprueba el tiempo de respuesta del primer servidor de la lista que responde. Si el primer servidor de respaldo falla, los clientes de uso móvil administrados por él pasan al siguiente servidor de respaldo disponible en la lista cuando comprueban si su servidor principal está disponible. El equilibrio de la carga no se aplica a los servidores de respaldo.
Servidores alternativos	Además de los servidores principales, es posible configurar también los clientes de uso móvil para que se conecten con un servidor de Cuarentena central (que debe tener instalado también el servidor de Symantec AntiVirus Corporate Edition), con un servidor de alertas (AMS^2) y con un servidor de Grc.dat. Este último es un servidor que proporciona la configuración de Grc.dat a los clientes de uso móvil. Si se emplea nearest_GRC, se consigue que el cliente de uso móvil obtenga la configuración de políticas desde el servidor especificado y la procese inmediatamente. **Nota:** Un cliente no se puede conectar con varios servidores principales del mismo tipo.

Configuración de las opciones de los clientes de uso móvil

Para configurar las opciones de los clientes de uso móvil, se deben especificar el balanceo de carga y los servidores de respaldo y activar el uso móvil en otro tipo de servidores.

Para especificar el balanceo de carga entre servidores

- Utilice un signo igual (=) entre los servidores de la lista jerárquica de servidores.

  Por ejemplo:

  ServEEUUSudeste Principal 4 ServMiami=ServAtlanta=ServRichmond

Para especificar un servidor de respaldo

- Use el símbolo mayor que (>) en la lista jerárquica de servidores.

  Por ejemplo:

  ServEEUUSudeste Principal 4 ServMiami>ServAtlanta>ServRichmond

Para activar el uso móvil en otro tipo de servidores

1 Defina en 1 los valores del registro que correspondan al tipo de servidor.
Vea "Valores del registro" en la página 186.

2 En la línea de comandos, escriba cualquiera de las opciones siguientes:
NAVRoam /nearest_parent
NAVRoam /nearest_quarantine
NAVRoam /nearest_GRC
NAVRoam /nearest_alerts
La diferencia principal entre /nearest_parent y /nearest_GRC se produce al procesar el archivo de configuración (Grc.dat). Si se utiliza /nearest_parent, el cliente de uso móvil buscará el servidor principal más próximo. La configuración de políticas no se procesa hasta que el cliente realice la verificación con su servidor principal. Si se utiliza /nearest_GRC, el cliente de uso móvil obtiene la configuración de políticas desde el servidor principal y la procesa inmediatamente.

Opciones de la línea de comandos

La Tabla 6-5 describe las opciones de la línea de comandos que se pueden utilizar con NAVRoam.exe y RoamAdmn.exe.

Es preciso contar con derechos de administrador locales para utilizar las opciones de la línea de comandos.

Tabla 6-5 Opciones de la línea de comandos

Opción	Descripción
/h	Muestra una lista de las opciones con descripciones de su uso.
/import <lista de servidores>	Configura las claves del registro del cliente o del servidor. Cuando se utiliza RoamAdmn.exe, se puede importar la lista de servidores a los servidores remotos. Cuando se emplea NAVRoam.exe, es posible importar la lista de servidores al registro del equipo local. <lista de servidores> es el archivo de texto en el que se incluye una lista de los posibles servidores principales.

Tabla 6-5 Opciones de la línea de comandos

Opción	Descripción
/export <archivo>	Informa de todos los servidores de uso móvil que el cliente puede detectar en todos los niveles y para todos los tipos de servidores principales (incluidos servidores principales, de cuarentena, de alertas y de Grc.dat). <archivo> es el nombre del archivo en el que se escribe la información. Es posible utilizar el archivo creado con el comando de exportación como lista de servidores a la hora de importar.
/install <ruta> <nombre del nuevo servicio> <nombre del nuevo ejecutable>	Registra e inicia el servicio de cliente de uso móvil. El servicio se ejecuta hasta que se apaga el equipo. <ruta> indica la ruta a la carpeta en la que se desea copiar NAVRoam.exe. <nombre del nuevo servicio> es NAVRoam.exe. <nombre del nuevo ejecutable> es NAVRoam.exe.
/remove <nombre del nuevo servicio>	Detiene NAVRoam.exe y lo elimina.
/nearest	Busca y configura el servidor principal adecuado más próximo para los servidores principales, de cuarentena, de alertas o de Grc.dat. Es preciso configurar manualmente en el registro la ruta GRC del servidor principal.
/nearest_parent	Busca y configura el servidor principal más próximo.
/nearest_quarantine	Busca y configura el servidor de cuarentena principal más próximo.
/nearest_GRC	Busca el servidor de Grc.dat más próximo y aplica su archivo de configuración (Grc.dat). Es preciso configurar manualmente en el registro la ruta GRC del servidor principal.
/nearest_alerts	Busca y configura el servidor de alertas (AMS^2) más próximo.
/check_parent	Comprueba que el servidor principal se esté ejecutando.
/shutdown	Desconecta el cliente del servidor principal.

Tabla 6-5 Opciones de la línea de comandos

Opción	Descripción
/time-network <tiempo transcurrido en segundos> <tiempo delta en milisegundos> <servidores>	Indica el tiempo medio que se tarda en conectar con los servidores especificados. <tiempo transcurrido en segundos> indica el número de segundos que deben transcurrir para permitir que se ejecute el proceso. <tiempo delta en milisegundos> indica la frecuencia en milisegundos con la que se debe contactar con el servidor. Por ejemplo, el valor 10.000 indicaría que el cliente tendría que ponerse en contacto con el servidor cada diez segundos. <servidores> indica los servidores con los que se debe contactar. Los nombres de los servidores deben ir separados por comas. No deben incluirse espacios, ni entre los nombres de los servidores ni entre las comas.

Valores del registro

Es posible modificar los valores del registro de uso móvil utilizando un editor del registro como Regedit o Regedt32.

El comportamiento del agente se controla mediante las claves del registro situadas en la ruta siguiente:

HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\ProductControl

La Tabla 6-6 describe los valores del registro para clientes de uso móvil.

Tabla 6-6 Valores del registro para clientes de uso móvil

Valor del registro	Descripción
CheckForNewParentIntervalInSeconds	Si un equipo no puede encontrar el servidor principal más próximo cuando se inicia por primera vez, se realizan comprobaciones periódicas para comprobar si la red está funcionando. El intervalo se configura mediante esta clave del registro. El valor predeterminado es de 30 segundos.

Tabla 6-6 Valores del registro para clientes de uso móvil

Valor del registro	Descripción
CheckParentIntervalInMinutes	Determina la frecuencia con la que el equipo comprueba si el servidor principal se encuentra disponible. Si el servidor principal no está disponible, intenta detectar uno nuevo. El valor predeterminado es de 120 minutos.
RoamClient	Indica al agente que debe establecer el cliente como equipo secundario del servidor principal más próximo. El valor predeterminado es 1. Si no se desea que el equipo se convierta en secundario del servidor principal más cercano, se deberá asignar el valor 0.
RoamQuarantine	Si el valor es 1, el envío a cuarentena se realiza al servidor más próximo que se encuentre con las claves de búsqueda de cuarentena. El valor predeterminado es 0.
RoamAlerts	Si el valor es 1, el envío de alertas de AMS^2 se realiza al servidor más próximo que se encuentre desde las claves de búsqueda de alertas. El valor predeterminado es 0.
RoamGRC	Si el valor es 1, el cliente se desplaza al servidor desde el que debería recibir las actualizaciones del archivo de políticas (Grc.dat). El valor predeterminado es 0.
RoamServer	Si el valor está definido en 1, el cliente se comunica con el servidor principal más adecuado. El valor predeterminado es 0.

Tabla 6-6 Valores del registro para clientes de uso móvil

Valor del registro	Descripción
ParentGRCPath	Asigna a ParentGRCPath el valor del archivo de configuración (Grc.dat). El agente copia este archivo en el equipo local y lo aplica. Consulte la información de RoamGRC proporcionada anteriormente. Si se asigna el valor 1 tanto a RoamClient como a RoamGRC, NAVRoam.exe copia el archivo de configuración del servidor principal y después el archivo de configuración del servidor principal de GRC y reemplaza con éste la copia obtenida del servidor principal.
ParentLiveUpdateHstPath	Define el directorio incluido en el directorio principal de NAV; por ejemplo, \MihostLiveUpdate\Liveupdt.hst. El archivo.hst debe copiarse en Unidad/Archivos de programa/Symantec/LiveUpdate. El agente copia el archivo de host de LiveUpdate a esta ubicación.

Capítulo 7

Trabajo con historias y registros de sucesos

En este capítulo se tratan los temas siguientes:

- Acerca de las historias y los registros de sucesos
- Ordenación y filtrado de los datos de las historias y los registros de sucesos
- Visualización de historias
- Supresión de historias y registros de sucesos

Acerca de las historias y los registros de sucesos

Las historias y los registros de sucesos proporcionan un método centralizado para controlar las actividades y los análisis de virus en la red. Symantec System Center permite realizar las siguientes tareas:

- Ver información correspondiente a un grupo de servidores, a un servidor determinado o a una estación de trabajo administrada de forma independiente. Además, cada cliente de Symantec AntiVirus Corporate Edition almacena su propia información en el registro de sucesos local. Esta información se puede ver desde la interfaz de usuario del cliente de Symantec AntiVirus Corporate Edition.
- Ordenar y filtrar los datos de registros de sucesos e historias.
- Realizar distintas acciones basándose en los datos de las historias y los registros de sucesos. Por ejemplo, si una historia de virus muestra que se ha detectado un virus, se pueden emprender acciones como eliminar el virus o llevar el archivo infectado a Cuarentena central.
- Exportar los datos con el formato de Microsoft Access (como archivo.mdb) o como un archivo de valores separados por comas (CSV).
- Eliminar datos de las historias y los registros de sucesos.

Symantec AntiVirus Corporate Edition proporciona distintos tipos de historias y de registros de sucesos, tal y como se muestra en la Tabla 7-1.

Tabla 7-1 Tipos de historias y registros de sucesos

Nombre	Descripción	Disponible para
Registro de sucesos	Proporciona información acerca de las operaciones de inicio y cierre de Symantec AntiVirus Corporate Edition, acerca de los análisis que se han iniciado, detenido o interrumpido, los cambios de configuración, las actualizaciones de los archivos de definiciones de virus, las infecciones víricas, los elementos que se han enviado a Cuarentena central y los elementos que se han enviado a Symantec Security Response.	■ Grupos de servidores ■ Servidores individuales ■ Clientes individuales

Tabla 7-1 Tipos de historias y registros de sucesos

Nombre	Descripción	Disponible para
Historia de análisis	Proporciona información acerca de los análisis que se han ejecutado o se están ejecutando en clientes de Symantec AntiVirus Corporate Edition, en un grupo de servidores, en un servidor o en una estación de trabajo individual. Puede especificar un intervalo de tiempo para filtrar la vista. Por ejemplo, puede que le interese ver solamente los análisis que se han ejecutado en los últimos 7 días.	■ Grupos de servidores ■ Servidores individuales ■ Clientes individuales
Historia de virus	Muestra todos los virus que se han detectado en los equipos o grupos de servidores seleccionados. Es posible seleccionar un elemento de la lista y realizar acciones adicionales, tales como suprimirlo o ponerlo en cuarentena. La historia de virus muestra gran cantidad de detalles sobre las infecciones, como el nombre y la ubicación del archivo infectado, el nombre del equipo infectado, la acción primaria y secundaria configuradas para el virus detectado y la acción llevada a cabo sobre el virus.	■ Grupos de servidores ■ Servidores individuales ■ Clientes individuales
Historia de barridos de virus	Proporciona información acerca de barridos de virus correspondientes a servidores o grupos de servidores.	■ Grupos de servidores ■ Servidores individuales

Ordenación y filtrado de los datos de las historias y los registros de sucesos

Cuando se visualiza una historia de virus, una historia de barridos de virus, una historia de análisis o el registro de sucesos, se pueden filtrar los elementos de las siguientes formas:

- Hoy
- Pasados 7 días
- El mes actual
- Todos los elementos
- Un intervalo seleccionado

También se pueden filtrar los sucesos por tipo seleccionando sólo aquellos que se deban ver.

Ordenación y filtrado de los datos de registros de sucesos e historias

Cuando se visualizan las historias y los registros de sucesos, es posible ordenar los datos de cualquier columna.

Es posible filtrar los datos de historias y registros de sucesos por fecha. También se puede filtrar la información por tipo de suceso en los registros de sucesos.

Para ordenar los datos

- Haga clic en el encabezado de columna.
  El icono de orden ascendente aparece dentro del encabezado de una columna la primera vez que se hace clic en él. El icono de orden descendente aparece la siguiente vez que se hace clic en el encabezado de la columna.

Para filtrar los datos de historias y registros de sucesos por fecha

1. En la consola de Symantec System Center, haga clic con el botón derecho en un servidor o un grupo de servidores y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Registros** y seleccione una de las opciones siguientes:
   - Registro de sucesos
   - Historia de análisis
   - Historia de virus
   - Historia de barridos de virus
2. En la lista correspondiente, seleccione una de las opciones siguientes:
   - Hoy
   - Pasados 7 días
   - Este mes
   - Todos los elementos
   - Interv. selec.
     Si selecciona **Interv. selec.,** deberá seleccionar una fecha de inicio y otra de fin y a continuación hacer clic en **Aceptar**.

Para filtrar los datos de historias y registros de sucesos por tipo de suceso

1. En la consola de Symantec System Center, haga clic con el botón derecho en un servidor o un grupo de servidores y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Registros** > **Registro de sucesos**.
2. En el cuadro de diálogo Registro de sucesos, haga clic en el icono de filtro.

3 En el cuadro de diálogo Filtrar registro de sucesos, seleccione los sucesos que desee mostrar:
   - Cambio de configuración
   - Inicio y cierre de Symantec AntiVirus
   - Archivo de definiciones de virus
   - Analizar omisiones
   - Enviado al servidor de cuarentena
   - Enviado a Symantec Security Response

4 Haga clic en **Aceptar**.

Visualización de historias

La Tabla 7-2 describe las historias que se pueden ver en la consola de Symantec System Center.

Tabla 7-2 Historias

Historia	Descripción
Historias de virus	■ En un grupo de servidores, se muestran todos los virus que se hayan encontrado en ese grupo de servidores. ■ En un servidor individual, se muestran todos los virus que se hayan encontrado en los clientes administrados por ese servidor. ■ En un cliente, se muestran todos los virus encontrados en él.
Historias de barridos de virus	■ En un grupo de servidores y un servidor individual, se muestran todos los barridos de virus correspondientes a todos los servidores del grupo o al servidor individual.
Historias de análisis de virus (en curso y planificados)	■ En un grupo de servidores, se muestran todos los análisis de virus correspondientes a ese grupo de servidores. ■ En un servidor individual, se muestran todos los barridos de virus correspondientes a los clientes administrados por ese servidor. ■ En un cliente, se muestran todos los barridos de virus correspondientes a ese cliente.

Ver historias

Es posible ver historias de virus, historias de barridos de virus e historias de análisis de virus.

Vea "Utilización de las historias de virus" en la página 194.

Para ver una historia de virus

- En la consola de Symantec System Center, haga clic con el botón derecho en un servidor, un grupo de servidores o un cliente y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Registros** > **Historia de virus**.

Vea "Descripción de los iconos de la ventana Registro de sucesos" en la página 199.

Para ver una historia de barridos de virus

1. En la consola de Symantec System Center, haga clic con el botón derecho en un servidor o un grupo de servidores y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Registros** > **Historia de barridos de virus**.
2. En el cuadro de diálogo Historia de barridos de virus, haga clic en **Ver resultados** para examinar los resultados de barridos anteriores.

Para ver una historia de análisis de virus

- En la consola de Symantec System Center, haga clic con el botón derecho en un servidor, un grupo de servidores o un cliente y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Registros** > **Historia de análisis**.

Utilización de las historias de virus

La ventana Historia de virus incluye iconos que muestran información sobre los virus detectados y permite realizar distintas acciones, como guardar los datos en un archivo CSV.

Nota: No es posible realizar acciones adicionales en los datos relacionados con el correo electrónico y sólo se pueden realizar acciones limitadas en la información relativa a los archivos comprimidos.

La Tabla 7-3 recoge y describe los iconos de la ventana Historia de virus.

Tabla 7-3 Iconos de la ventana Historia de virus

Icono	Descripción
	El archivo está infectado.
	El archivo no está infectado. El archivo no ha estado nunca infectado o ha sido limpiado. Si desea obtener más información, consulte la acción efectuada sobre ese archivo.
	Se ha producido un error relacionado con el archivo.
	Permite cerrar la ventana Historia de virus.

La Tabla 7-4 recoge y describe las acciones disponibles en la ventana Historia de virus.

Tabla 7-4 Acciones de la ventana Historia de virus

Acción	Descripción
Deshacer acción	Symantec AntiVirus Corporate Edition permite deshacer la última acción que se haya realizado con un archivo infectado, incluyendo su eliminación del área de cuarentena y la eliminación de la extensión.vbn de un archivo cuyo nombre se haya cambiado. Symantec AntiVirus Corporate Edition no puede restaurar un archivo que se haya suprimido de forma permanente. No es posible deshacer acciones realizadas en archivos comprimidos.
Limpiar	Los archivos de definiciones de virus de Symantec AntiVirus Corporate Edition se actualizan frecuentemente. Un archivo que no se haya podido limpiar el día anterior o unas pocas semanas antes tal vez pueda limpiarse cuando se hayan actualizado los archivos de definiciones de virus. No es posible deshacer esta acción en los archivos comprimidos.
Suprimir permanentemente	Se puede suprimir de manera permanente cualquier archivo infectado (incluidos los comprimidos) que se encuentre almacenado en el área de cuarentena o desde la historia de virus. Los archivos suprimidos de manera permanente no se pueden recuperar.
Poner en cuarentena	Si descubre que Symantec AntiVirus Corporate Edition no ha realizado acción alguna con un archivo infectado, debe moverlo al área de cuarentena para impedir que el virus se extienda. Los archivos comprimidos también se pueden colocar en cuarentena.
Exportar	Se puede exportar la información acerca de un elemento específico de una historia de virus o un registro de sucesos como archivo CSV o como archivo de base de datos de Microsoft Access.

Utilización de las historias de virus

Desde las historias de virus se puede deshacer la última acción realizada sobre un archivo, limpiar el archivo, suprimirlo permanentemente o moverlo a Cuarentena central. Asimismo es posible exportar los datos de las historias de virus.

Para deshacer la última acción realizada

1. Haga clic con el botón derecho en un archivo y a continuación haga clic en **Deshacer acción**.
2. En el cuadro de diálogo Efectuar acción, haga clic en **Iniciar Deshacer**.

Para limpiar un archivo infectado

1. Haga clic con el botón derecho en un archivo y a continuación haga clic en **Limpiar**.
2. En el cuadro de diálogo Efectuar acción, haga clic en **Iniciar Limpiar**.

Para suprimir permanentemente un archivo infectado

1. Haga clic con el botón derecho en un archivo y a continuación haga clic en **Suprimir permanentemente**.
2. En el cuadro de diálogo Efectuar acción, haga clic en **Iniciar Suprimir**.
   Los archivos suprimidos de manera permanente no se pueden recuperar.

Para mover un archivo a Cuarentena central

1. Haga clic con el botón derecho en un archivo y a continuación haga clic en **Poner en cuarentena**.
2. En el cuadro de diálogo Efectuar acción, haga clic en **Cuarentena**.

Para exportar los datos de las historias de virus

1. Haga clic con el botón derecho en el archivo y a continuación haga clic en **Exportar**.
2. En la lista Guardar como, seleccione una de las opciones siguientes:
   - CSV
   - Base de datos de Access
3. En el cuadro Nombre del archivo, escriba un nombre adecuado.
4. Haga clic en **Aceptar**.

Utilización de las historias de análisis

La ventana Historia de análisis incluye iconos que muestran información sobre los virus detectados y permite realizar distintas acciones, como guardar los datos en un archivo CSV.

Nota: No es posible llevar a cabo acciones adicionales sobre los datos de correo electrónico y sólo se pueden realizar ciertas acciones sobre los archivos comprimidos.

La Tabla 7-5 recoge y describe los iconos de la ventana Historia de análisis.

Tabla 7-5 Iconos de la ventana Historia de análisis

Icono	Descripción
	El archivo está infectado.
	El archivo no está infectado. El archivo no ha estado nunca infectado o ha sido limpiado. Si desea obtener más información, consulte la acción efectuada sobre ese archivo.
	Permite cerrar la ventana Historia de análisis.
	Muestra propiedades de los elementos.
	Guarda los datos que se muestran en la ventana Historia de análisis como un archivo de valores separados por comas (.csv).
	Muestra la Ayuda de la ventana Historia de análisis.

La Tabla 7-6 recoge y describe las acciones disponibles en la ventana Historia de análisis.

Tabla 7-6 Acciones de la ventana Historia de análisis

Acción	Descripción
Deshacer acción	Symantec AntiVirus Corporate Edition permite deshacer la última acción que se haya realizado con un archivo infectado, incluyendo su eliminación del área de cuarentena y la eliminación de la extensión.vbn de un archivo cuyo nombre se haya cambiado. Symantec AntiVirus Corporate Edition no puede restaurar un archivo que se haya suprimido de forma permanente. No es posible deshacer acciones realizadas en archivos comprimidos.

Tabla 7-6 Acciones de la ventana Historia de análisis

Acción	Descripción
Limpiar	Los archivos de definiciones de virus de Symantec AntiVirus Corporate Edition se actualizan frecuentemente. Un archivo que no se haya podido limpiar previamente tal vez pueda limpiarse cuando se hayan actualizado los archivos de definiciones de virus. No es posible realizar esta acción en los archivos comprimidos.
Suprimir permanentemente	Se puede suprimir de manera permanente cualquier archivo infectado (incluidos los comprimidos) que se encuentre almacenado en el área de cuarentena o desde la historia de análisis. Los archivos suprimidos de manera permanente no se pueden recuperar.
Poner en cuarentena	Si descubre que Symantec AntiVirus Corporate Edition no ha realizado acción alguna con un archivo infectado, debe moverlo al área de cuarentena para impedir que el virus se extienda. Los archivos comprimidos también se pueden colocar en cuarentena.
Exportar	Se puede exportar la información acerca de un elemento específico de una historia de análisis o un registro de sucesos como archivo CSV o como archivo de base de datos de Microsoft Access.

Utilización de las historias de análisis

Desde las historias de análisis se puede deshacer la última acción realizada sobre un archivo, limpiar el archivo, suprimirlo permanentemente o moverlo a Cuarentena central. Asimismo es posible exportar los datos de las historias de análisis.

Para deshacer la última acción realizada

1. Haga clic con el botón derecho en un archivo y a continuación haga clic en **Deshacer acción**.
2. En el cuadro de diálogo Efectuar acción, haga clic en **Iniciar Deshacer**.

Para limpiar un archivo infectado

1. Haga clic con el botón derecho en un archivo y a continuación haga clic en **Limpiar**.
2. En el cuadro de diálogo Efectuar acción, haga clic en **Iniciar Limpiar**.

Para suprimir permanentemente un archivo infectado

1. Haga clic con el botón derecho en un archivo y a continuación haga clic en **Suprimir permanentemente**.
2. En el cuadro de diálogo Efectuar acción, haga clic en **Iniciar Suprimir**.
   Los archivos suprimidos de manera permanente no se pueden recuperar.

Para mover un archivo a Cuarentena central

1. Haga clic con el botón derecho en el archivo y a continuación haga clic en **Poner en cuarentena**.
2. En el cuadro de diálogo Efectuar acción, haga clic en **Cuarentena**.

Para exportar los datos de las historias de análisis

1. Haga clic con el botón derecho en el archivo y a continuación haga clic en **Exportar**.
2. En la lista Guardar como, seleccione una de las opciones siguientes:
   - CSV
   - Base de datos de Access
3. En el cuadro Nombre del archivo, escriba un nombre adecuado.
4. Haga clic en **Aceptar**.

Descripción de los iconos de la ventana Registro de sucesos

La ventana Registro de sucesos incluye iconos que muestran información sobre los virus detectados y permite realizar distintas acciones, como guardar los datos en un archivo CSV.

La Tabla 7-7 recoge y describe los iconos de la ventana Registro de sucesos.

Tabla 7-7 Iconos de la ventana Registro de sucesos

Icono	Descripción
	Proporciona información acerca de un suceso.
	Indica que se ha producido un error relacionado con este suceso.
	Permite cerrar la ventana Registro de sucesos.
	Permite ver las propiedades del elemento.

Tabla 7-7 Iconos de la ventana Registro de sucesos

Icono	Descripción
	Permite guardar los datos que se muestran en la ventana Registro de sucesos como archivo CSV o como archivo de base de datos de Microsoft Access.
	Filtra el registro de sucesos según las siguientes categorías: ■ Cambio de configuración ■ Inicio/cierre de Symantec AntiVirus Corporate Edition ■ Archivo de definiciones de virus ■ Omisiones de análisis ■ Envíos a cuarentena ■ Envíos a Symantec Security Response
	Muestra la Ayuda sobre el Registro de sucesos.

Supresión de historias y registros de sucesos

Puede configurar Symantec AntiVirus Corporate Edition para que suprima automáticamente los datos de las historias y los registros de sucesos anteriores a una fecha específica.

Para definir la frecuencia de supresión de los datos

1. En la consola de Symantec System Center, haga clic con el botón derecho en un servidor, un grupo de servidores o un cliente y a continuación haga clic en **Todas las tareas** > **Symantec AntiVirus** > **Configurar historia**.
2. En el cuadro de diálogo Opciones de historias, seleccione el periodo de tiempo tras el cual se deben suprimir los datos de las historias y los registros de sucesos.
3. Haga clic en **Aceptar**.

   Con este procedimiento los datos no se eliminan de forma permanente, sino que se ocultan en las vistas de las historias y los registros de sucesos. Para suprimir de manera permanente elementos de los registros de sucesos o de las historias, deberá suprimir los archivos.log que contengan esos elementos. Los sucesos se registran en los archivos.log correspondientes a cada día de la semana y ubicados en el directorio Logs. A estos archivos se les asignan nombres que reflejan el día en que se han creado.

Índice

A

Acciones de alerta
  acerca de 56
  configuración
    carga de un NLM 63
    cuadro de mensaje 61
    ejecución de un programa 62
    envío de un mensaje a buscapersonas 65
    envío de un mensaje de correo por Internet 64
    mensaje de difusión general 62
    mensajes 57
    módem 67
    servicios de mensajes de buscapersonas 69
  exportación a otros equipos 73
  limitadas a determinadas zonas de la red 59
  pruebas 73
  visualización del registro de alertas 75
Alert Management System
  acerca de 54
  envío de alertas desde los clientes no administrados 80
Alerta de aparición de un cuadro de mensaje, configuración 61
Alerta de carga de un NLM, configuración 63
Alerta de ejecución de un programa, configuración 62
Alerta de envío de mensajes a buscapersonas
  configuración 65
  configuración del servicio de buscapersonas 68
Alerta de envío de un mensaje de correo por Internet, configuración 64
Almacenamiento y modificación de contraseñas 38
Análisis
  análisis planificados
    desactivación 106
    ejecución manual 107
    modificación 106
    supresión 106
  archivos comprimidos 127
  asignación de acciones 110
  configuración
    opciones en varios equipos seleccionados 88
    protección en tiempo real para archivos 89
    uso de la CPU 132
  configuración de análisis manuales 128
  opciones
    análisis de inicio de sesión 132
    análisis planificados 100
    manual 128
    protección en tiempo real para archivos 89
    selección de los tipos de unidades para el análisis 92
  opciones atenuadas o ausentes 88
  opciones para análisis manuales, planificados y en tiempo real 110
  selección de archivos y carpetas para analizar 125
  supresión de análisis planificados 106
  virus 83
  visualización de un mensaje de aviso en el cliente 114
Análisis en tiempo real
  acerca de 84
  configuración para aplicaciones de correo 89
  problemas de compatibilidad de correo electrónico 95
Análisis manuales
  configuración 98
  opciones 84
Antememoria
  contraseñas de grupos de servidores 38
  reconocimiento de equipos 24
Archivos
  colocación en cuarentena 196, 199
  deshacer la acción realizada 196, 198
  exclusión del análisis 120
  limpieza de archivos infectados 196, 198
  supresión de archivos infectados 196, 199

Archivos de definiciones de virus
comprobación de la fecha 158
distribución 157
Intelligent Updater 146
LiveUpdate 143
métodos de actualización 135
uso de versiones anteriores 158

C

Cargar sólo desde antememoria, reconocimiento 20
Clientes
generalidades sobre el control de análisis centralizado 89
visualización de la lista de virus 158
Configuración
acciones de alerta 56
Alert Management System, módems 67
análisis manuales 98
análisis planificados 100
opciones de análisis
acerca de 110
varios equipos seleccionados 88
opciones de análisis de inicio de sesión 132
opciones para análisis manuales, planificados y en tiempo real 110
opciones para excluir archivos de los análisis 120
protección en tiempo real para aplicaciones de correo electrónico 89
servicio de envío de mensajes a buscapersonas 67
Configuración de las alertas, aceleración con el reconocimiento avanzado 59
Consola
actualización 29
iconos 15
inicio 13
localización de los elementos encontrados 29
vistas 13
Correo electrónico y Lotus Notes, configuración de análisis 89
CPU, configuración de su uso 132
Cuarentena, mover archivos 196, 199

D

Disco de emergencia, recuperación de un virus de arranque 169

E

Equipos
localización de los elementos encontrados en la consola 29
Estado 34
Estado de la exportación, visualización 75
Exclusiones de archivos 121

F

Fecha de los archivos de definiciones de virus, comprobación 158

G

Grcsrv.dat 42
Grupos de clientes
crear 44, 49
Grupos de servidores
actualización de la consola 29
agrupación de servidores 35
almacenamiento de contraseñas 38
bloqueo y desbloqueo 36, 37
cambio de nombre 39
contraseñas almacenadas en antememoria 38
crear 36
desbloqueo y bloqueo 36, 37
filtrado de vistas 42
modificación de contraseñas 37
planificación 42
reconocimiento de servidores y clientes 13
selección del servidor primario 40
supresión 43
traslado de un servidor a un nuevo grupo de servidores 42
visualización 42

H

Historia de análisis
iconos 197
ordenación de columnas 191

Historia de virus
consultar 193
iconos 194
ordenación de columnas de datos 191
Historias
consultar 193
supresión 200

I

Iconos
historia de análisis 197
historia de virus 194
Infecciones, administración 161
Inicio de sesión, opciones de análisis 132
Intelligent Updater 157

L

Lista de virus 158
LiveUpdate 34
configuración de las políticas para clientes 156
configuración de servidores para obtener actualizaciones desde el sitio FTP de Symantec 143
uso con un servidor de LiveUpdate interno 145
Lotus Notes, configuración de análisis 89

M

Mensaje de aviso, visualización en un equipo infectado 114
Mensaje de buscapersonas, introducción 69
Mensaje de difusión general, configuración 62
Método de transporte de definiciones de virus
actualización de servidores de NetWare 140
ejemplos de implementación 158
Módems, configuración para su uso con Alert Management System 67

N

NetWare 31

R

Reconocimiento avanzado 59
Reconocimiento de IP 22
Reconocimiento intenso 21, 25
Reconocimiento local 20, 24
Reconocimiento mediante la antememoria de direcciones 20
Registro de alertas
alertas mostradas 75
copia de contenidos en el Portapapeles 77
filtrado de la lista 79
supresión de entradas 77
visualización de información más detallada 77
Registro de sucesos, ordenación de columnas 191

S

Servicio de reconocimiento
reconocimiento avanzado 59
reconocimiento de IP 22
reconocimiento intenso 21
reconocimiento local 20
reconocimiento mediante la antememoria de direcciones 20
Servicios de mensajes de buscapersonas, configuración para su uso con AMS 69
Servidor primario 30
Servidor principal 31
Servidor secundario 31
Servidores
agrupación en grupos de servidores 35
cambio de servidores primarios y principales 41
primarios 30
principales 31
secundarios 31
tipos
servidor primario 30
servidor principal 31
Servidor secundario 31
traslado a un nuevo grupo de servidores 42
visualización de la lista de virus 158
visualización en la consola 29
Soporte para clientes de uso móvil, funcionamiento 174
Subred, reconocimiento de IP 22
Supresión de análisis planificados 106
Symantec System Center
actualización de la consola 29
iconos 15
inicio 13
localización de los elementos encontrados 29
vistas de la consola 13

T

Tipos de registro 193

V

Vistas
    cambio 15
    mostradas en la consola 13

Soluciones de Servicio y Soporte

Symantec tiene como objetivo ofrecer el mejor servicio en todo el mundo. Nuestra meta es ofrecerle ayuda profesional para la utilización de nuestro software y servicios, cualquiera que sea el lugar del mundo en que se encuentre.

Las soluciones de Soporte técnico y Servicio al cliente varían según el país.

Si tiene alguna pregunta respecto a los servicios que se describen a continuación, consulte la sección "Para contactar el Servicio y Soporte mundial" al final de este capítulo.

Registro y licencias

Si el producto que está implementando requiere ser registrado y/o una clave de licencia, la manera más rápida y fácil de registrar su servicio es acceder a nuestro sitio de registro y programas de licenciamiento en www.symantec.com/certificate. También puede ir a http://www.symantec.com/techsupp/ent/enterprise.html, seleccionar el producto que desea registrar y desde la página principal del producto, seleccionar el vínculo Registro y licencias.

Si ha adquirido una suscripción de soporte, tiene derecho a recibir asistencia técnica de Symantec por teléfono y por Internet. Cuando se ponga en contacto con el servicio de soporte por primera vez, tenga a mano el número de licencia que aparece en su Certificado de licencia o el Id de contacto que se genera al registrar el soporte, para que el personal pueda comprobar su autorización de soporte. Si no ha adquirido una suscripción de soporte, póngase en contacto con su distribuidor o con el Servicio de Atención al Cliente de Symantec para obtener información sobre cómo adquirir soporte técnico de Symantec.

Actualizaciones de seguridad

Para obtener la información más reciente sobre las últimas amenazas de seguridad y de virus, vaya al sitio Web de Symantec Security Response (antes conocido como SARC) en:

http://securityresponse.symantec.com.

Este sitio contiene extensa información sobre amenazas de seguridad y de virus, así como las últimas definiciones de virus. Las definiciones también pueden descargarse utilizando la función LiveUpdate de su producto.

Renovación de la suscripción de actualizaciones antivirus

La adquisición del servicio de mantenimiento de su producto le da derecho a descargar definiciones de virus gratuitas durante el plazo de validez de su acuerdo de mantenimiento. Si su acuerdo de mantenimiento ha caducado, póngase en contacto con su distribuidor o con el Servicio de Atención al Cliente de Symantec para obtener información sobre la renovación del acuerdo.

Los sitios Web de Symantec:

Página principal de Symantec (por idioma):

Alemán:	http://www.symantec.de
Español:	http://www.symantec.com/region/es http://www.symantec.com/mx
Francés:	http://www.symantec.fr
Inglés:	http://www.symantec.com
Italiano:	http://www.symantec.it
Holandés:	http:// www.symantec.nl
Portugués:	http://www.symantec.com/br

Symantec Security Response:

http://securityresponse.symantec.com

Página de Servicio y Soporte Empresarial de Symantec:

http://www.symantec.com/techsupp/ent/enterprise.html

Boletines de noticias de productos:

EE.UU., Pacífico Asiático / inglés:

http://www.symantec.com/techsupp/bulletin/index.html

Europa, Oriente Medio y África / inglés:

http://www.symantec.com/region/reg_eu/techsupp/bulletin/index.html

Alemán:

http://www.symantec.com/region/de/techsupp/bulletin/index.html

Francés:

http://www.symantec.com/region/fr/techsupp/bulletin/index.html

Holandés:

http://www.symantec.com/region/nl/techsupp/bulletin/index.html

Italiano:

http://www.symantec.com/region/it/techsupp/bulletin/index.html

América Latina

Español:

http://www.symantec.com/region/mx/techsupp/bulletin/index.html

Portugués:

http://www.symantec.com/region/br/techsupp/bulletin/index.html

Soporte Técnico

Nuestro grupo de soporte técnico global, por ser parte integrante de Symantec Security Response, mantiene centros de soporte en todas partes del mundo. Nuestro papel principal es responder a preguntas específicas sobre características/funciones de los productos, instalaciones y configuración, además de elaborar el contenido de nuestra Base de conocimientos accesible por Internet. Trabajamos en colaboración con las otras áreas funcionales de Symantec para responder a sus preguntas oportunamente. Por ejemplo, trabajamos con Ingeniería de productos, así como con nuestros Centros de Investigación de Seguridad para suministrar Servicios de alerta y actualizaciones de definiciones de virus cuando hay ataques de virus y alertas de seguridad. Nuestros servicios más importantes incluyen:

- Una gama de opciones de soporte que le dan la flexibilidad de poder seleccionar la amplitud de servicio necesaria para una organización de cualquier tamaño.
- Componentes de soporte telefónico y de Web que le proporcionan respuestas rápidas y la información más reciente.
- Actualizaciones de producto que proporcionan protección automática y actualizada de software.
- Actualizaciones de contenido para definiciones de virus y firmas de seguridad que le garantizan el más alto nivel de protección.
- Soporte global de los expertos de Symantec Security Response, disponible las 24 horas del día, 7 días por semana, en todo el mundo, en varios idiomas.
- Funciones avanzadas tales como el Servicio de alertas de Symantec y el rol de Administrador de cuentas técnico que suministran respuestas mejoradas y soporte de seguridad proactivo.

Consulte nuestro sitio Web para obtener información actualizada sobre los programas de soporte.

Para contactarnos

Los clientes que tienen un acuerdo de soporte válido pueden ponerse en contacto con el equipo de Soporte Técnico por teléfono, a través de la Web en la dirección URL a continuación o utilizando los sitios de soporte regionales que se indican más adelante en este documento.

www.symantec.com/techsupp/ent/enterprise.html

Cuando se ponga en contacto con el personal de Soporte Técnico, asegúrese de tener a mano la siguiente información:

- Número de versión del producto
- Información del hardware
- Memoria disponible, espacio en disco, información sobre el NIC (tarjeta interfaz de red)
- Sistema operativo
- Versión y nivel de parche
- Topología de la red
- Router, gateway y dirección IP
- Descripción del problema
- Mensajes de error/archivos de registro
- Soluciones intentadas antes de ponerse en contacto con Symantec
- Cambios recientes en la configuración del software y/o cambios en la red.

Servicio de Atención al Cliente de Symantec

El Centro de Servicio de Atención al Cliente de Symantec puede prestarle ayuda en asuntos no técnicos, tales como:

- Información general sobre productos (características, idiomas disponibles, distribuidores en su área, etc.).
- Solución de problemas básicos, tales como comprobar el número de versión del producto.
- Información más reciente sobre actualizaciones y nuevas versiones de productos.
- Cómo actualizar su producto.
- Cómo registrar su producto y/o licencias.

- Información sobre los programas de licenciamiento de Symantec.
- Información sobre seguros de actualización y contratos de mantenimiento.
- Reemplazo de CD y manuales.
- Actualización de su registro de producto para reflejar un cambio de nombre o dirección.
- Consejos sobre las opciones de soporte técnico de Symantec.

El sitio Web de Servicio y Soporte de Symantec ofrece extensa información de servicio al cliente. Esta información también se puede obtener llamando al Centro de Servicio al cliente de Symantec. Consulte la sección "Para contactar el Servicio y Soporte mundial", que aparece al final de este capítulo, para obtener el número y las direcciones Web del Servicio al cliente de su área.

Para contactar el Servicio y Soporte mundial

En Europa, Oriente Medio, África y América Latina

Sitios Web de Servicio y Soporte de Symantec

Alemán:	www.symantec.de/desupport/
Español:	www.symantec.com/region/mx/techsupp/
Francés:	www.symantec.fr/frsupport/
Inglés:	www.symantec.com/eusupport/
Italiano:	www.symantec.it/itsupport/
Holandés:	www.symantec.nl/nlsupport/
Portugués:	www.symantec.com/region/br/techsupp/
Dirección FTP de Symantec: (para descargar notas técnicas y los últimos parches)	ftp.symantec.com

Visite el Servicio y Soporte de Symantec en la Web para obtener información técnica y no técnica sobre su producto.

Symantec Security Response:

http://securityresponse.symantec.com

Boletines de noticias de productos:

EE.UU. / inglés:

http://www.symantec.com/techsupp/bulletin/index.html

Europa, Oriente Medio, África y América Latina / inglés:

http://www.symantec.com/region/reg_eu/techsupp/bulletin/index.html

Alemán:

http://www.symantec.com/region/de/techsupp/bulletin/index.html

Español:

http://www.symantec.com/region/mx/techsupp/bulletin/index.html

Francés:

http://www.symantec.com/region/fr/techsupp/bulletin/index.html

Holandés:

http://www.symantec.com/region/nl/techsupp/bulletin/index.html

Italiano:

http://www.symantec.com/region/it/techsupp/bulletin/index.html

Portugués:

http://www.symantec.com/region/br/techsupp/bulletin/index.html

Servicio de Atención al Cliente de Symantec

Proporciona información y consejos no técnicos por teléfono en los siguientes idiomas: inglés, alemán, francés, italiano y españo.

Alemania	+ (49) 69 6641 0315
Austria	+ (43) 1 50 137 5030
Bélgica	+ (32) 2 2750173
Dinamarca	+ (45) 35 44 57 04
España	+ (34) 91 7456467
Finlandia	+ (358) 9 22 906003
Francia	+ (33) 1 70 20 00 00
Holanda	+ (31) 20 5040698
Irlanda	+ (353) 1 811 8093
Italia	+ (39) 02 48270040
Luxemburgo	+ (352) 29 84 79 50 30
Noruega	+ (47) 23 05 33 05
RU	+ (44) 20 7744 0367
Sudáfrica	+ (27) 11 797 6639
Suecia	+ (46) 8 579 29007
Suiza	+ (41) 2 23110001
Otros países (sólo en inglés)	+ (353) 1 811 8093

Servicio de Atención al Cliente de Symantec – Dirección postal

Symantec Ltd.
Customer Service Centre
Europa, Oriente Medio y África (EMEA)
PO Box 5689
Dublín 15
Irlanda

En América Latina

Symantec proporciona Soporte técnico y Servicio de Atención al Cliente en todo el mundo. Los servicios varían según los países e incluyen socios internacionales, representantes de Symantec en las zonas en que Symantec no tiene una oficina. Para más información, póngase en contacto con la oficina de Servicio y Soporte Symantec de su región.

Argentina y Uruguay

Symantec Region Sur
Cerrito 1054 - Piso 9
1010 Buenos Aires
Argentina

Central telefónica	+54 (11) 5382-3802
Sitio Web	http://www.service.symantec.com/mx

Brasil

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12° andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

Central telefónica	+55 (11) 5189-6300
Fax	+55 (11) 5189-6210
Sitio Web	http://www.service.symantec.com/br

México

Symantec México
Blvd Adolfo Ruiz Cortines,
No. 3642 Piso 14
Col. Jardines del Pedregal
Ciudad de México, D.F.
C.P. 01900
México

Central telefónica	+52 (5) 661-6120
Sitio Web	http://www.service.symantec.com/mx

Resto de América Latina

Symantec Corporation
9100 South Dadeland Blvd.
Suite 1810
Miami, FL 33156
U.S.A.

Sitio Web	http://www.service.symantec.com/mx

En el Pacífico Asiático

Symantec proporciona Soporte técnico y Servicio de Atención al Cliente en todo el mundo. Los servicios varían según los países e incluyen socios internacionales, representantes de Symantec en las zonas en que Symantec no tiene una oficina. Para más información, póngase en contacto con la oficina de Servicio y Soporte Symantec de su región.

Oficinas de Servicio y Soporte

AUSTRALIA

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Australia

Central telefónica	+61 2 8879 1000	
Fax	+61 2 8879 1001	
Sitio Web	http://service.symantec.com	
Soporte Gold	1800 805 834	gold.au@symantec.com
Admin. contratos de soporte	1800 808 089	contractsadmin@symantec.com

CHINA

Symantec China
Unit 1-4, Level 11,
Tower E3, The Towers, Oriental Plaza
No.1 East Chang An Ave.,
Dong Cheng District
Beijing 100738
China P.R.C.

Central telefónica	+86 10 8518 3338
Soporte Técnico	+86 10 8518 6923
Fax	+86 10 8518 6928
Sitio Web	http://www.symantec.com.cn

COREA

Symantec Korea
15,16th Floor
Dukmyung B/D
170-9 Samsung-Dong
KangNam-Gu
Seoul 135-741
Corea del Sur

Central telefónica	+822 3420 8600
Fax	+822 3452 1610
Soporte Técnico	+822 3420 8650
Sitio Web	http://www.symantec.co.kr

HONG KONG

Symantec Hong Kong
Central Plaza
Suite #3006
30th Floor, 18 Harbour Road
Wanchai
Hong Kong

Central telefónica	+852 2528 6206
Soporte Técnico	+852 2528 6206
Fax	+852 2526 2646
Sitio Web	http://www.symantec.com.hk

INDIA

Symantec India
Suite #801
Senteck Centrako
MMTC Building
Bandra Kurla Complex
Bandra (East)
Mumbai 400051, India

Central telefónica	+91 22 652 0658
Fax	+91 22 652 0671
Sitio Web	http://www.symantec.com/india
Soporte Técnico:	+91 22 657 0669

MALASIA

Symantec Corporation (Malaysia) Sdn Bhd
31-3A Jalan SS23/15
Taman S.E.A.
47400 Petaling Jaya
Selangor Darul Ehsan
Malasia

Central telefónica	+603 7805 4910
Fax	+603 7804 9280
Correo electrónico empresarial	gold.apac@symantec.com
Nº empresarial gratuito	+1800 805 104
Sitio Web	http://www.symantec.com.my

NUEVA ZELANDA

Symantec New Zealand
Level 5, University of Otago Building
385 Queen Street
Auckland Central 1001
Nueva Zelanda

Central telefónica	+64 9 375 4100	
Fax	+64 9 375 4101	
Sitio Web de soporte	http://service.symantec.co.nz	
Soporte Gold	0800 174 045	gold.nz@symantec.com
Admin. contratos de soporte	0800 445 450	contractsadmin@symantec.com

SINGAPUR

Symantec Singapore
3 Phillip Street
#17-00 & #19-00 Commerce Point
Singapore 048693

Central telefónica	+65 6239 2000
Fax	+65 6239 2001
Soporte Técnico	+65 6239 2099
Sitio Web	http://www.symantec.com.sg

TAIWÁN

Symantec Taiwan
2F-7, No.188 Sec.5
Nanjing E. Rd.,
105 Taipei
Taiwán

Central telefónica	+886 2 8761 5800
Soporte corporativo	+886 2 8761 5800
Fax	+886 2 2742 2838
Sitio Web	http://www.symantec.com.tw

Se ha hecho todo lo posible para que la información contenida en este documento esté libre de errores. Sin embargo, dicha información puede estar sujeta a modificaciones. Symantec Corporation se reserva el derecho de realizar dichas modificaciones sin previo aviso.