Guía de referencia de Symantec AntiVirus™ Corporate Edition

Guía de referencia de Symantec AntiVirus™ Corporate Edition

Documentación. Versión 8.0

Información de copyright

Marcas comerciales

Impreso en Irlanda.

10 9 8 7 6 5 4 3 2 1

Contenido

Capítulo 1

Introducción a esta guía de referencia

Temas de esta guía de referencia

Esta guía de referencia contiene información técnica sobre el producto Symantec AntiVirus Corporate Edition y sobre las herramientas incluidas en el CD de Symantec AntiVirus Corporate Edition. Esta guía está dirigida tanto a administradores de sistemas como a otras personas encargadas de instalar y mantener este producto en entornos de redes corporativas.

La Tabla 1-1 recoge y describe los temas incluidos en esta guía de referencia.

Tabla 1-1 Temas de esta guía de referencia

Tema	Descripción
Situaciones posibles	Este capítulo proporciona ejemplos de posibles implantaciones de Symantec AntiVirus Corporate Edition en tres organizaciones de distinto tamaño: de tamaño medio, de gran tamaño y multinacionales. Aunque su situación particular no coincida exactamente con ninguno de los ejemplos, podrá obtener una idea aproximada de cómo otras organizaciones han implantado soluciones de seguridad, así como del tipo de elementos que han influido en sus decisiones.
La herramienta Reset ACL	La mayoría de los valores de configuración de Symantec AntiVirus Corporate Edition se almacenan en el registro de Windows. La herramienta Reset ACL permite restringir el acceso a estos valores del registro en Windows XP, 2000 y NT para impedir que usuarios no autorizados realicen cambios.

Tabla 1-1 Temas de esta guía de referencia

Tema	Descripción
La herramienta Importer	La herramienta Importer es una utilidad de la línea de comandos diseñada específicamente para utilizarla con Symantec System Center. La herramienta Importer permite importar tantos conjuntos de nombres de equipos y direcciones IP como sean necesarios. Symantec AntiVirus Corporate Edition puede localizarlos de esta forma durante el proceso de reconocimiento en aquellas situaciones en las que los nombres de los equipos no se puedan resolver mediante WINS o DNS.
Servicios de Windows XP, 2000 y NT	Este capítulo muestra los nombres de los servicios que Symantec AntiVirus Corporate Edition y Symantec System Center ejecutan automáticamente. Los nombres aparecen en el componente Servicios del Panel de control de Windows XP, 2000 y NT.
Entradas del registro de sucesos en Windows XP, 2000 y NT	Este capítulo recoge y describe los sucesos asociados a Symantec AntiVirus Corporate Edition tal como aparecen en el registro de sucesos de Windows.

Capítulo 2

Situaciones posibles

En este capítulo se tratan los temas siguientes:

Situación 1: Organización de tamaño medio

Esta organización consta de una oficina y varios usuarios remotos. El entorno de la organización incluye los siguientes elementos:

- La organización tiene un total de 1.000 estaciones de trabajo, de las cuales el 96 % utiliza Windows 98 o ME. El departamento MIS utiliza Windows 2000 o XP en las estaciones de trabajo de los usuarios particulares.
- Varios usuarios trabajan a distancia desde sus equipos domésticos, que disponen de Windows 98 o ME.
- Actualmente, el 98 % de los servidores de la organización son de NetWare, aunque también hay varios servidores de Windows 2000.
- Microsoft Word y Microsoft Excel son las aplicaciones que se utilizan con más frecuencia.

Organizaciones de tamaño medio: distribución de Symantec AntiVirus Corporate Edition

En las organizaciones de tamaño medio se distribuye Symantec AntiVirus Corporate Edition de la siguiente forma:

- Se crean paquetes de distribución mediante Symantec Packager. Los administradores utilizan varias herramientas de distribución distintas. Por ejemplo, un administrador distribuye instalaciones silenciosas a través de secuencias de comandos de inicio de sesión, mientras que otro administrador emplea un método de instalación de clientes mediante Web.
- A los usuarios remotos se les proporciona un CD para instalar un cliente no administrado de Symantec AntiVirus Corporate Edition.

Organizaciones de tamaño medio: gestión de alertas

En las organizaciones de tamaño medio se gestionan las alertas de la siguiente forma:

- AMS^2 se instala en el servidor primario. Cuando se detecta un virus, se envía un mensaje de correo electrónico a la cuenta del administrador.
- Los registros de AMS^2 se supervisan desde Symantec System Center para detectar sucesos o virus que exijan una atención especial.

Organizaciones de tamaño medio: protección del entorno contra los virus

En las organizaciones de tamaño medio el entorno se protege contra los virus de la siguiente forma:

- El programa servidor de Symantec AntiVirus Corporate Edition se instala en servidores de NetWare.
- Todas las estaciones de trabajo están protegidas por el cliente de Symantec AntiVirus Corporate Edition. Estas estaciones utilizan las opciones de Symantec AntiVirus Corporate Edition definidas por el departamento MIS. El departamento MIS bloquea las opciones de Symantec AntiVirus Corporate Edition para impedir que los usuarios puedan modificar la forma en que Symantec AntiVirus Corporate Edition protege los equipos contra los virus.
- El departamento MIS instala Symantec System Center en un equipo de Windows 2000 Professional para administrar la protección antivirus.
- Un servidor no operativo de Windows 2000 se define como único servidor primario. Al utilizar un servidor no operativo se ahorran recursos en los servidores que sí son operativos. El servidor primario se actualiza de forma automática mediante LiveUpdate y a continuación emplea el método de transporte de definiciones de virus para transferir los archivos de definiciones a todos los servidores de NetWare y a todos los clientes administrados.
- Las estaciones de trabajo que el departamento MIS considera menos seguras se integran en el mismo grupo de clientes. El departamento MIS configura las opciones de Symantec AntiVirus Corporate Edition en este grupo de clientes con el fin de proporcionarles un mayor nivel de protección que al resto de estaciones de trabajo.
- Las alertas y las actualizaciones de las definiciones de virus se supervisan regularmente desde la consola de Symantec System Center. El administrador comprueba periódicamente los datos del registro de sucesos y de la historia de virus para detectar sucesos o virus que puedan necesitar una atención especial.

- La mayoría de los servidores de NetWare son servidores de archivos y de aplicaciones. Los usuarios acceden con frecuencia a los archivos de estos servidores. De forma predeterminada, la protección en tiempo real para servidores de Symantec AntiVirus Corporate Edition analiza los archivos cuando se crean, se mueven, se abren, se copian, se ejecutan, se guardan o se les cambia el nombre. El departamento MIS configura la protección en tiempo real para servidores de forma que se analicen los archivos sólo cuando se creen, se muevan o se les cambie el nombre, lo que mejora el rendimiento al reducirse el número de operaciones de archivo que se deben supervisar.
- El administrador planifica un análisis de grupo de servidores en todos los servidores de Symantec AntiVirus Corporate Edition que se lleva a cabo en las horas en que no están operativos. La ejecución del análisis antivirus se planifica para que se ejecute a una hora distinta de la hora a la que se realizan copias de respaldo durante la noche, de forma que no interfieran.
- El administrador planifica un análisis de clientes semanal.

Organizaciones de tamaño medio: actualización de definiciones de virus

En las organizaciones de tamaño medio las definiciones de virus se actualizan de la siguiente forma:

- Los servidores de NetWare no pueden utilizar el método automático de actualización de archivos de definiciones de virus porque no están configurados para admitir conexiones mediante FTP. El administrador planifica la ejecución de un archivo por lotes dos veces por semana. El archivo por lotes descarga el archivo de definiciones de virus desde el sitio FTP de Symantec y lo copia en el directorio SAV del servidor primario.
- Los servidores secundarios recuperan automáticamente las actualizaciones desde el servidor primario.
- La mayor parte de los clientes de Symantec AntiVirus Corporate Edition reciben automáticamente los archivos de definiciones de virus desde el servidor principal correspondiente, usando para ello el método de transporte de definiciones de virus. En el mismo momento en que el servidor principal recibe nuevos archivos de definiciones de virus, comienza a enviar las actualizaciones de las definiciones de virus a los clientes. El servidor principal puede actualizar varios clientes al mismo tiempo y actualizar simultáneamente un cliente de cada subred para reducir el tráfico en la red.
- Los clientes remotos obtienen las actualizaciones de archivos de definiciones desde Symantec ejecutando LiveUpdate.

Situación 2: Organización de gran tamaño

Esta organización se compone de una oficina central y de 50 sucursales repartidas por distintas ciudades de un mismo país. El entorno de la organización incluye los siguientes elementos:

- La oficina central cuenta con 5.000 estaciones de trabajo ubicadas en cinco edificios distintos y cada una de las sucursales tiene una media de 100 estaciones de trabajo.
- Hay 420 servidores en la organización; de ellos el 95 % utiliza Windows NT o 2000 y el 5 % NetWare. La mayoría de los servidores están en la oficina central, de forma que muchas de las sucursales no tienen servidor local. Hay dos servidores Terminal Server.
- La organización tiene un total de 10.000 estaciones de trabajo, de las cuales el 50 % utiliza Windows 2000 y el otro 50 % Windows 98, ME o XP.
- Hay 60 terminales conectadas a los servidores Terminal Server.
- Las sucursales están conectadas a la oficina corporativa a través de una conexión WAN de 56 KB y la oficina corporativa cuenta con una conexión a Internet de 128 KB. Debido a la limitada anchura de banda, es muy importante que se mantenga al mínimo el tráfico de red de estas conexiones.
- Microsoft Exchange, Microsoft Word y Microsoft Excel son las aplicaciones que más se utilizan. La mayoría de las estaciones de trabajo de la organización son altamente susceptibles a los virus de macro, a los virus que se propagan a través del correo electrónico y a las amenazas combinadas.

Organizaciones de gran tamaño: distribución de instalaciones de cliente

En las organizaciones de gran tamaño se distribuyen las instalaciones de cliente de la siguiente forma:

- Desde la oficina central, el departamento MIS distribuye los paquetes de instalación y migración para los equipos locales utilizando Novell ZENworks. Se crean paquetes de distribución personalizados mediante Symantec Packager. Los datos que requieren los productos de Symantec AntiVirus Corporate Edition en los discos duros de los usuarios se reducen instalando únicamente los componentes que el departamento MIS quiere que utilicen los usuarios. Al configurar los paquetes, el departamento MIS elige la instalación silenciosa y especifica los valores de configuración de Symantec AntiVirus Corporate Edition que pueden modificar los usuarios.
- Las sucursales no utilizan Symantec Packager para la distribución, ya que se cuenta con una anchura de banda limitada para conectar con la oficina central. Para instalar Symantec AntiVirus Corporate Edition en las estaciones de trabajo, los usuarios de las sucursales utilizan un método de instalación mediante Web. El departamento MIS envía a estos usuarios un mensaje de correo electrónico con instrucciones y un vínculo a una URL para acceder al instalador mediante Web.

Organizaciones de gran tamaño: gestión de alertas

En las organizaciones de gran tamaño se gestionan las alertas de la siguiente forma:

- Cada servidor primario es también un servidor del sistema AMS^2. Todas las alertas, tanto de los demás servidores (incluyendo la consola de Terminal Server) como de las estaciones de trabajo, se envían a estos servidores.
- Cuando se detecta un virus, el sistema AMS^2 envía un mensaje de correo electrónico al administrador que esté encargado de la protección antivirus.
- Los registros de AMS^2 se supervisan desde Symantec System Center para detectar sucesos, virus o amenazas combinadas que exijan una atención especial.

Organizaciones de gran tamaño: protección del entorno contra los virus

En las organizaciones de gran tamaño el entorno se protege contra los virus de la siguiente forma:

- Para proteger la organización contra las infecciones procedentes de Internet, el departamento MIS utiliza Symantec Enterprise Firewall.
- El servidor de Microsoft Exchange está protegido por Symantec AntiVirus/ Filtering para Microsoft Exchange.
- Todos los servidores de NetWare están protegidos por el servidor de Symantec AntiVirus Corporate Edition.
- Todos los servidores de Windows NT o 2000 que administran clientes de Symantec AntiVirus Corporate Edition están protegidos por el servidor de Symantec AntiVirus Corporate Edition. Todos los demás servidores de Windows NT o 2000 están protegidos por el cliente de Symantec AntiVirus Corporate Edition.
- El servidor de Symantec AntiVirus Corporate Edition se ejecuta en los servidores Terminal Server.
- Todas las estaciones de trabajo están protegidas por el client de Symantec AntiVirus Corporate Edition. Estas estaciones utilizan las opciones de Symantec AntiVirus Corporate Edition definidas por el departamento MIS. El correo electrónico se analiza mediante el complemento para correo electrónico de Symantec AntiVirus Corporate Edition. El departamento MIS bloquea las opciones de Symantec AntiVirus Corporate Edition para evitar que los usuarios modifiquen la forma en que se protegen sus equipos contra los virus.
- El departamento MIS configura varios grupos de servidores y de clientes de Symantec AntiVirus Corporate Edition. Antes de configurar estos grupos, el departamento crea un plan completo que está diseñado para cubrir numerosos aspectos, como los requisitos físicos del servidor, las velocidades de conexión y los niveles de seguridad necesarios para los distintos departamentos y grupos, acordes con sus propias necesidades y niveles de vulnerabilidad.
- Symantec System Center se instala en la oficina central para que los administradores puedan configurar las opciones antivirus desde una ubicación central.

- Los servidores en los que se ejecuta el servidor de Symantec AntiVirus Corporate Edition se encuentran divididos en varios grupos distintos. Por ejemplo, todos los servidores Terminal Server y de NetWare en los que se ejecuta el servidor de Symantec AntiVirus Corporate Edition pertenecen al mismo grupo de servidores porque comparten las mismas funciones y los mismos requisitos de carga y sobrecarga.
- El número de clientes asociados a cada servidor principal varía entre 3.500 y 15.000. Aproximadamente diez clientes realizan la verificación con el servidor principal cada minuto.
- Se configuran grupos de clientes para cada departamento. Por ejemplo, los equipos del grupo Desarrollo se asignan a un grupo de clientes que cuenta con una configuración de seguridad de un nivel inferior. Los equipos del departamento del servicio al cliente son muy susceptibles a los virus que se propagan a través del correo electrónico, por lo que estos equipos se integran en un grupo de clientes en el que todos los valores de configuración del client de Symantec AntiVirus Corporate Edition se encuentran bloqueados.
- Algunos clientes locales y remotos se dividen en diferentes grupos de clientes debido a que utilizan diferentes métodos para actualizar las definiciones de virus.
- En los servidores de Windows NT o 2000 que no actúan como servidores principales se ejecuta el client de Symantec AntiVirus Corporate Edition. Los usuarios acceden con frecuencia a los archivos de estos servidores. De forma predeterminada, la protección en tiempo real para clientes de Symantec AntiVirus Corporate Edition analiza los archivos cuando se crean, se mueven, se abren, se copian, se ejecutan, se guardan o se les cambia el nombre. El departamento MIS configura la protección en tiempo real para clientes de forma que se analicen los archivos sólo cuando se creen, se muevan o se les cambie el nombre, lo que mejora el rendimiento al reducirse el número de operaciones de archivo que se deben supervisar.
- Los clientes se configuran de forma que, cuando un usuario desactiva la protección en tiempo real del sistema de archivos, ésta se vuelve a activar automáticamente transcurridos treinta minutos.
- Symantec AntiVirus Corporate Edition está configurado para enviar al servidor de Cuarentena central los archivos infectados que no puedan repararse. El administrador envía los archivos sospechosos a Symantec Security Response para su análisis. En Symantec Security Response se analizan los archivos enviados, tras lo cual se remite un informe al administrador con nuevos archivos de definiciones o con cualquier otra solución.

- El administrador planifica un análisis de grupos de servidores para todos los equipos en los que se ejecute el server de Symantec AntiVirus Corporate Edition que se lleva a cabo en las horas en que no están operativos. La ejecución del análisis antivirus se planifica para que se ejecute a una hora distinta de la hora a la que se realizan copias de respaldo durante la noche, de forma que no interfieran.
- Los administradores planifican análisis de clientes para que se ejecuten cada cinco días. En el cuadro de diálogo Opciones exclusivas para administradores de clientes, se configura Symantec AntiVirus Corporate Edition para posponer los análisis planificados cuando los equipos clientes utilicen batería. De esta forma, el análisis planificado no se ejecuta hasta que el portátil se conecta a una toma de corriente.
- Para los análisis planificados y manuales, se configura el uso de la CPU en equipos de Windows a partir de criterios basados en los momentos de actividad o inactividad. Las opciones de inactividad permiten una mayor utilización de la CPU cuando el equipo no se está utilizando, mientras que las opciones de actividad se configuran para permitir una menor utilización de la CPU, lo que minimiza el impacto en la productividad del usuario.

Organizaciones de gran tamaño: actualización de definiciones de virus

En las organizaciones de gran tamaño las definiciones de virus se actualizan de la siguiente forma:

- El departamento MIS implanta un sistema que reduce el tráfico en Internet. El administrador selecciona un servidor FTP establecido que hace que una parte de la intranet de la organización actúe como servidor de LiveUpdate, pero no se trata de un servidor dedicado de LiveUpdate o de Symantec AntiVirus Corporate Edition. La utilidad de administración de LiveUpdate obtiene las actualizaciones de productos y de archivos de definiciones de virus de Symantec AntiVirus Corporate Edition desde el sitio FTP de Symantec y las transfiere al servidor FTP de la oficina central.
- Se planifica la utilidad de administración de LiveUpdate para que se descarguen los paquetes nuevos diariamente, en horas no productivas.

- Los servidores primarios recuperan las actualizaciones de las definiciones de virus desde el servidor interno de LiveUpdate y las transfieren a los servidores secundarios.
- Los servidores principales transfieren las actualizaciones de las definiciones de virus a los clientes empleando el método de transporte de definiciones de virus. El tamaño del archivo de definiciones de virus es bastante pequeño. El departamento MIS configura Symantec AntiVirus Corporate Edition para distribuir eficazmente los archivos de definiciones. En la transferencia se emplean múltiples subprocesos que actúan a velocidades distintas (desde muy rápida hasta muy lenta). Cada subproceso distribuye los datos a una sola subred al mismo tiempo, hasta completar el proceso en todos los clientes de la subred.

Situación 3: Organización multinacional

Esta organización tiene oficinas distribuidas por distintos países. La organización cuenta con 150 oficinas compuestas por un número de empleados comprendido entre 20 y 3.000. El entorno de la organización incluye los siguientes elementos:

- 2.500 servidores, de los cuales el 10 % utiliza NetWare, el 20 % Windows NT, el 65 % Windows 2000 y el 5 % Unix.
- La organización tiene un total de 35.000 estaciones de trabajo, de las cuales el 50 % utiliza Windows 98, ME o XP y el otro 50 % Windows NT o 2000.
- Muchos de los usuarios de Windows NT o 2000 no disfrutan de derechos de administración en sus estaciones de trabajo.
- Muchos de los equipos de Windows son portátiles.
- El departamento MIS emplea una utilidad de distribución de software para instalar el software en todas las estaciones de trabajo.
- Las aplicaciones Lotus Notes, Microsoft Exchange, Microsoft Word y Microsoft Excel son las que más se utilizan.

Esta organización utiliza Tivoli SecureWay Risk Manager 3.7, que se suministra con un adaptador para Symantec AntiVirus Corporate Edition. Este adaptador permite a Tivoli SecureWay Risk Manager leer el registro de sucesos de Symantec AntiVirus Corporate Edition. Entre la información que recoge y muestra Tivoli SecureWay Risk Manager se incluye lo siguiente:

- Estado de las actualizaciones de las definiciones de virus
- Información de historial acerca de los análisis
- Estadísticas relacionadas con el número de infecciones sufridas en la organización

Organizaciones multinacionales: distribución de Symantec AntiVirus Corporate Edition

En las organizaciones multinacionales se distribuye Symantec AntiVirus Corporate Edition de la siguiente forma:

- El departamento MIS distribuye los paquetes de instalación y migración a los equipos locales utilizando Microsoft SMS. Los paquetes de distribución se crean mediante Symantec Packager. Los diferentes paquetes se distribuyen desde los distintos servidores principales a cada grupo de clientes, dependiendo de la ubicación de estos clientes y de las necesidades especiales de cada uno. Los datos que requieren los productos de Symantec AntiVirus Corporate Edition en los discos duros de los usuarios se reducen instalando únicamente los componentes que el departamento MIS quiere que utilicen los usuarios. Durante la configuración de los paquetes, el departamento MIS elige la instalación interactiva y especifica los valores de configuración de Symantec AntiVirus Corporate Edition que pueden modificar los usuarios.
- El departamento MIS crea también un CD de instalación especial de Symantec AntiVirus Corporate Edition para los usuarios de equipos portátiles. Este CD contiene un paquete de instalación muy parecido al mencionado anteriormente.
- Las sucursales pequeñas que no utilizan SMS emplean un método de instalación mediante Web para distribuir los paquetes de instalación. El departamento MIS envía a estos usuarios un mensaje de correo electrónico con instrucciones y un vínculo a una URL para acceder al instalador mediante Web.

Organizaciones multinacionales: gestión de alertas, registros e informes

En las organizaciones multinacionales se gestionan las alertas de la siguiente forma:

- Los sucesos de Symantec AntiVirus Corporate Edition se envían a Symantec Enterprise Security a través del recopilador de Symantec AntiVirus Corporate Edition. El departamento MIS utiliza Symantec Enterprise Security para registrar sucesos, crear notificaciones de alerta como respuesta a los sucesos y generar informes predefinidos y personalizados que incluyen el estado de los sucesos.
- Se establecen umbrales para administrar las alertas y las notificaciones. El departamento MIS utiliza buscapersonas, correo electrónico y capturas SNMP para las notificaciones de alerta.

- El departamento MIS consulta, filtra y clasifica los sucesos para determinar qué sistemas están desprotegidos, obsoletos o afectados por sucesos de extrema gravedad.
- El departamento MIS genera informes con tablas y gráficos que recogen el estado de los sucesos, tomando como base las vistas filtradas creadas por el propio departamento. Algunos informes son para uso interno y otros se transfieren a los directores y administradores principales del departamento.

Organizaciones multinacionales: protección del entorno contra los virus

En las organizaciones multinacionales el entorno se protege contra los virus de la siguiente forma:

- Para proteger la organización de posibles infecciones que se transmitan por mensajes de correo electrónico en Internet, el departamento MIS ejecuta Symantec AntiVirus para SMTP Gateways.
- Los servidores de Lotus Notes están protegidos por Symantec AntiVirus/ Filtering para Domino.
- Los servidores de Microsoft Exchange están protegidos por Symantec AntiVirus/Filtering para Microsoft Exchange.
- Todos los servidores de NetWare están protegidos por el servidor de Symantec AntiVirus Corporate Edition.
- La mayoría de los servidores de Windows NT o 2000 están protegidos por el client de Symantec AntiVirus Corporate Edition. Los escasos servidores dedicados que forman parte de la implantación antivirus de la organización están protegidos por el server de Symantec AntiVirus Corporate Edition. Los servidores Terminal Server y los de NetWare también están protegidos por el server de Symantec AntiVirus Corporate Edition.

- Todas las estaciones de trabajo están protegidas por el client de Symantec AntiVirus Corporate Edition. Estas estaciones utilizan las opciones de Symantec AntiVirus Corporate Edition definidas por el departamento MIS, incluida la protección para el correo electrónico de lo clientes. El departamento MIS bloquea las opciones de Symantec AntiVirus Corporate Edition para impedir que los usuarios puedan modificar la forma en que Symantec AntiVirus Corporate Edition protege sus equipos contra los virus. Se asignan configuraciones antivirus especiales a los grupos de clientes que tienen necesidades especiales, como los que tienen un alto riesgo en su seguridad.
- Las sucursales con conexiones rápidas se incluyen en un grupo de servidores con múltiples grupos de clientes para los distintos departamentos.
- Algunas sucursales con conexiones lentas tienen sus propios grupos de servidores. El administrador de cada una de las sucursales es el responsable de su protección antivirus. Algunas sucursales con conexiones lentas tienen sus propios servidores principales en vez de grupos de servidores y utilizan el método de transporte de definiciones de virus. El servidor primario, ubicado en el centro de datos principal, envía los archivos de definiciones de virus a través de una conexión de 56 KB. Los servidores principales envían los archivos de definiciones a los clientes a través de la red de área local de la sucursal. En el caso de sucursales pequeñas que carezcan de servidor, los clientes se asignan a un servidor principal remoto y se configuran para ejecutar LiveUpdate de forma aleatoria. Los clientes se configuran para que comprueben si había una sesión de LiveUpdate planificada que se haya ejecutado mientras el cliente no estaba disponible; si es así, el cliente ejecuta LiveUpdate cuando se inicia el sistema.
- Casi todas las funciones de Symantec AntiVirus Corporate Edition se administran desde la oficina central del departamento MIS. Este departamento mantiene políticas de seguridad estándar y coherentes para los clientes.
- Hay administradores en las sucursales de gran tamaño que cuentan con conexiones lentas. La consola de Symantec System Center sólo se ejecuta en la oficina central del departamento MIS y en estas oficinas. Los administradores de las sucursales poseen las contraseñas de los grupos de servidores de los que son responsables.
- Los grupos de clientes se configuran para proporcionar el nivel adecuado de protección. El departamento de ventas está ubicado en cuatro oficinas distintas. Todos sus equipos clientes están incluidos en el grupo de clientes Ventas. El departamento de desarrollo está ubicado en una sola oficina y cuenta con su propio grupo de clientes. Las opciones antivirus de este grupo son menos restrictivas, por lo que pueden desactivar la protección antivirus cuando, por ejemplo, deban compilar un programa.

- En los servidores de Windows NT o 2000 que no actúan como servidores principales se ejecuta el client de Symantec AntiVirus Corporate Edition. Los usuarios acceden con frecuencia a los archivos de estos servidores. De forma predeterminada, la protección en tiempo real para clientes de Symantec AntiVirus Corporate Edition analiza los archivos cuando se crean, se mueven, se abren, se copian, se ejecutan, se guardan o se les cambia el nombre. El departamento MIS configura la protección en tiempo real para clientes de forma que se analicen los archivos sólo cuando se creen, se muevan o se les cambie el nombre, lo que mejora el rendimiento al reducirse el número de operaciones de archivo que se deben supervisar.
- Los usuarios de equipos portátiles se configuran como clientes móviles. Cuando establecen la conexión con la red interna a través del módem, se asignan al servidor principal más adecuado según criterios de velocidad y proximidad. Symantec AntiVirus Corporate Edition comprueba la existencia de actualizaciones y puede recibir pequeños archivos de configuración para actualizar las opciones.
- Las estaciones de trabajo que no tienen necesidades especiales comparten un servidor principal. Cada servidor principal puede tener asignado un máximo de 5.000 clientes. Estos clientes realizan la verificación con su servidor principal cada 200 minutos.
- Symantec AntiVirus Corporate Edition envía los archivos infectados que no se pueden reparar al servidor de Cuarentena central. Los archivos sospechosos se envían a Symantec Security Response a través de Digital Immune System para proceder a su análisis. Digital Immune System (DIS) analiza los archivos recibidos y, a continuación, crea nuevas definiciones de virus y las pone a disposición de los usuarios a través de su pasarela, o bien envía el archivo a Symantec Security Response para un examen más detallado.
- Los clientes se configuran de forma que, cuando un usuario desactive la protección en tiempo real del sistema de archivos, ésta se vuelva a activar automáticamente transcurridos treinta minutos.
- El administrador planifica un análisis de grupos de servidores para todos los equipos que ejecutan el servidor de Symantec AntiVirus Corporate Edition que se lleva a cabo en las horas en que no están operativos. La ejecución del análisis antivirus se planifica para que se ejecute a una hora distinta de la hora a la que se realizan copias de respaldo durante la noche, de forma que no interfieran.

- El administrador planifica un análisis de clientes semanal. En el cuadro de diálogo Opciones exclusivas para administradores de clientes, se configura Symantec AntiVirus Corporate Edition para posponer los análisis planificados cuando los clientes funciones con batería. De esta forma, el análisis planificado no se ejecuta hasta que el portátil se conecta a una toma de corriente.
- En el grupo de clientes Ventas, el administrador configura el análisis planificado de forma que los vendedores puedan retrasarlo. Si el análisis planificado se inicia cuando se está realizando una tarea determinada, como una presentación, el vendedor puede utilizar el botón Posponer para retrasar el análisis tres horas. El vendedor puede utilizar este botón dos veces antes de que se ejecute el análisis planificado.
- Para los análisis planificados y manuales, se configura el uso de la CPU en equipos de Windows a partir de criterios basados en los momentos de actividad o inactividad. Las opciones de inactividad permiten una mayor utilización de la CPU cuando el equipo no se está utilizando, mientras que las opciones de actividad se configuran para permitir una menor utilización de la CPU, lo que minimiza el impacto en la productividad del usuario.

Organizaciones multinacionales: actualización de definiciones de virus

En las organizaciones multinacionales las definiciones de virus se actualizan de la siguiente forma:

- Uno de los servidores de Windows 2000 de la oficina central se designa para que actúe como servidor primario maestro. Este servidor recibe las actualizaciones de los archivos de definiciones desde Symantec a través de LiveUpdate de forma planificada.
- Los servidores primarios obtienen las definiciones del servidor primario maestro en el momento y con la frecuencia planificados y las transfieren a los servidores principales. El servidor principal actualiza varios clientes al mismo tiempo y actualiza simultáneamente un cliente de cada subred, reduciendo así el tráfico de red.

- La mayoría de los usuarios móviles reciben las definiciones de virus desde el servidor principal de uso móvil que tengan asignado. Los archivos de definiciones de virus tienen un tamaño reducido, por lo que no lleva mucho tiempo transferirlos a través de una conexión de acceso telefónico a redes. Los usuarios móviles también utilizan LiveUpdate continuo como opción de reserva para recibir las actualizaciones directamente desde Symantec cada vez que el equipo se conecta a Internet. El departamento MIS especifica un límite máximo de días para que los archivos de definiciones de virus ubicados en un equipo en el que se utilice Symantec AntiVirus Corporate Edition puedan permanecer sin actualizar antes de forzar su actualización. Cuando el client de Symantec AntiVirus Corporate Edition determina que los archivos de definiciones de virus han sobrepasado este límite, inicia una sesión silenciosa de LiveUpdate en cuanto detecta una conexión a Internet.
- Los usuarios móviles con conexión de acceso telefónico a redes tienen una secuencia de comandos de inicio de sesión o un script de RAS o VPN que activa LiveUpdate para actualizar los archivos de definiciones de virus en cuanto el usuario se autentica en el servidor de RAS o VPN.

Capítulo 3

La herramienta Reset ACL

En este capítulo se tratan los temas siguientes:

Acerca de la herramienta Reset ACL

La herramienta Reset ACL (Resetacl.exe) permite limitar el acceso a la clave del registro de Symantec AntiVirus Corporate Edition en equipos de Windows XP, 2000 y NT 4.0.

De forma predeterminada, estos equipos permiten que todos los usuarios modifiquen los datos almacenados en el registro correspondientes a cualquier aplicación, incluido Symantec AntiVirus Corporate Edition. Reset ACL elimina los permisos que otorgan acceso total a todos los usuarios a la siguiente clave del registro de Symantec AntiVirus Corporate Edition y a las subclaves correspondientes:

HKLM\SOFTWARE\Intel\LANDesk\VirusProtect6\CurrentVersion

Restricción del acceso al registro mediante la herramienta Reset ACL

Se puede utilizar la herramienta Reset ACL para restringir el acceso al registro.

Para restringir el acceso al registro mediante la herramienta Reset ACL

1. Distribuya el archivo Resetacl.exe, que se encuentra en la carpeta Tools del CD de Symantec AntiVirus Corporate Edition, a los equipos que no sean seguros.
2. Ejecute Resetacl.exe en cada uno de estos equipos.

Una vez ejecutado Resetacl.exe, únicamente los usuarios con derechos de administrador podrán modificar los valores de la clave del registro.

A pesar de que la herramienta Reset ACL aumenta considerablemente la seguridad de Symantec AntiVirus Corporate Edition en estos equipos, los administradores deben tener en cuenta que existen algunas contraprestaciones.

Además de perder el acceso al registro, los usuarios que no tengan derechos de administrador no podrán realizar las siguientes acciones:

- Iniciar o detener el servicio de Symantec AntiVirus Corporate Edition.
- Ejecutar LiveUpdate.
- Planificar LiveUpdate.
- Configurar Symantec AntiVirus Corporate Edition.
  Por ejemplo, los usuarios no podrán definir opciones de protección en tiempo real o de análisis del correo electrónico.

Las opciones asociadas con estas acciones aparecerán sombreadas en la interfaz de Symantec AntiVirus Corporate Edition.

Por otra parte, los usuarios podrán modificar las opciones de análisis, pero los cambios no se guardarán en el registro ni se procesarán. Los usuarios también podrán guardar las opciones de análisis manuales como predeterminadas, pero los cambios no se escribirán en el registro.

La herramienta Importer

En este capítulo se tratan los temas siguientes:

Acerca de la herramienta Importer

La herramienta Importer (Importer.exe) permite que la consola de Symantec System Center identifique equipos en un entorno que no sea WINS. De esta forma, Symantec AntiVirus Corporate Edition puede localizar equipos durante el proceso de reconocimiento de red cuando los nombres no se puedan buscar mediante WINS/DNS. Se trata de una utilidad de la línea de comandos.

Además de importar los pares de nombres y direcciones IP de los equipos ubicados en entornos que no sean WINS, es posible agregar al archivo de texto el par de nombre y dirección IP de cualquier otro equipo para que pueda localizarse en procesos de reconocimiento futuros. Por ejemplo, se puede agregar el nombre y la dirección de un equipo que no haya sido reconocido correctamente por alguna razón desconocida.

Nota: En la mayoría de los casos, no es necesario utilizar la herramienta Importer. La función Buscar equipo de Symantec System Center puede buscar e identificar normalmente los servidores de Symantec AntiVirus Corporate Edition en la red mediante la antememoria de direcciones y el proceso de reconocimiento habitual.

Funcionamiento de la herramienta Importer

La herramienta Importer se puede ejecutar en cualquier equipo en el que esté instalado Symantec System Center. Se puede utilizar esta herramienta para importar pares de nombres de equipos y direcciones IP desde un archivo de texto en las entradas de registro de la antememoria de direcciones que se emplean en Symantec System Center.

Una vez importados los pares de nombres de equipo y direcciones IP, se crean las entradas en el registro en la siguiente clave:

HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\AddressCache

Se debe ejecutar un reconocimiento local o intenso tras importar el archivo de datos. El proceso de reconocimiento solicita las direcciones de los equipos. Los equipos en los que se ejecuta el servidor de Symantec AntiVirus Corporate Edition se agregan al servicio de reconocimiento en la memoria y se crean entradas completas en el registro para ellos. De esta forma, el servicio de reconocimiento puede detectar los equipos cada vez que se ejecuta.

Ubicación de la herramienta Importer

La herramienta Importer está integrada por un solo archivo, Importer.exe. Este archivo se encuentra en el CD de Symantec AntiVirus Corporate Edition, en la carpeta Tools.

Se puede copiar el archivo Importer.exe en cualquier carpeta de un equipo en el que esté instalado Symantec System Center y ejecutarlo.

Importación de direcciones mediante la herramienta Importer

Para importar direcciones en la antememoria de direcciones, se debe iniciar la sesión con derechos de administrador. Esto se debe a que es preciso contar con acceso de escritura para la clave HKEY_LOCAL_MACHINE.

Importar direcciones mediante la herramienta Importer

Para importar direcciones mediante la herramienta Importer se deben realizar las siguientes acciones:

- Crear un archivo de datos que contenga pares de nombres de equipos y direcciones IP.
- Ejecutar la herramienta Importer.

  Nota: Se debe ejecutar la herramienta Importer desde el símbolo del sistema.

- Ejecutar el servicio de reconocimiento.

Para crear un archivo de datos

1. Cree un archivo nuevo con un editor de texto como el Bloc de notas.
2. Escriba los datos siguiendo este formato:
   <nombre del servidor><coma><dirección IP><salto de línea>
   No cometa ningún error al escribir las direcciones IP de los servidores, ya que no se efectúa ninguna comprobación para determinar si hay dos servidores con la misma dirección IP en el archivo de texto de Importer.

3 Guarde el archivo.

Por ejemplo, un archivo de datos con el nombre Equipos.txt tendría el siguiente aspecto:

Equipo 1, 155.64.3.121
Equipo 2, 155.64.3.122
Equipo 3, 155.64.3.123
Equipo 4, 155.64.3.124
Equipo 5, 155.64.3.125
Equipo 6, 155.64.3.126

Nota: Si desea marcar una dirección como comentario, sólo tendrá que escribir un punto y coma (;) o dos puntos (:) a la izquierda de ella. Por ejemplo, si sabe que un segmento de la red está fuera de servicio, puede marcar como comentario las direcciones de subred correspondientes.

Para ejecutar la herramienta Importer

1 Desde el símbolo de sistema de la línea de comandos, escriba lo siguiente:

<ruta> importer <nombre de archivo>

donde <ruta> representa la ruta completa al archivo Importer.exe y <nombre de archivo> representa la ruta completa al archivo de importación, como, por ejemplo, C:\Equipos\Equipos.txt

2 Pulse **Intro.**

Eliminación de entradas de la antememoria de direcciones

Los datos que se importan desde el archivo de datos no sobrescriben la información que ya esté almacenada en la antememoria de direcciones. Si se deben sobrescribir determinados datos, como una dirección de un equipo incorrecta, será necesario borrar la antememoria antes de ejecutar la herramienta Importer.

Nota: Tras importar el contenido del archivo de datos, no haga clic en Borrar antememoria ahora, ya que, si lo hace, se eliminará el contenido de la antememoria de direcciones, incluidos los datos importados.

Para eliminar entradas de la antememoria de direcciones

1. Desde el menú Herramientas de la consola de Symantec System Center, haga clic en **Servicio de reconocimiento**.
2. En Información de antememoria, haga clic en **Borrar antememoria ahora**.

Tras ejecutar el servicio de reconocimiento después de importar los datos, estarán disponibles los datos correctos para futuras sesiones de reconocimiento.

Utilización avanzada

En este caso, la línea de comandos requiere cuatro parámetros:

- Ruta al archivo de importación
- Primer delimitador
- Segundo delimitador
- Orden (1 = nombre de equipo/dirección IP, 2 = dirección IP/nombre de equipo; el predeterminado es 1).

Nota: El segundo delimitador debe ser un solo carácter. Por ejemplo, no se puede utilizar el signo & ya que el usuario debería escribir lo siguiente: "&"

Por ejemplo, un archivo de importación llamado Equipos.txt, ubicado en C:\EQUIPOS, podría contener el texto siguiente:

155.64.3.121/Servidor 1

155.64.3.122/Servidor 2

155.64.3.123/Servidor 3

En el ejemplo anterior se utiliza el orden (2): dirección IP/nombre de equipo. El primer parámetro es una barra diagonal (/) y el segundo es un salto de línea. Por tanto, la sintaxis correspondiente para la línea de comandos sería:

importer C:\EQUIPOS\equipos.txt / LF 2

Una vez importados los pares de nombres de equipos y direcciones IP, se crean las entradas en el registro en la siguiente clave:

HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\AddressCache

Debe ejecutar un reconocimiento local o intenso cuando haya importado el archivo de datos. El proceso de reconocimiento solicita las direcciones IP de los equipos. Los equipos en los que se ejecuta Symantec AntiVirus Corporate Edition se agregan al servicio de reconocimiento en la memoria y se crean para ellos entradas completas en el registro. De esta forma, el servicio de reconocimiento puede detectar los equipos cada vez que se ejecuta.

Obtención de ayuda al utilizar la herramienta Importer

Se puede obtener ayuda acerca de los parámetros y la sintaxis de la herramienta Importer.

Para obtener ayuda al utilizar la herramienta Importer

1. En la línea de comandos, escriba lo siguiente:
   Importer
2. Pulse **Intro.**

La herramienta Importer muestra la información de ayuda siguiente:

```
Simple Usage : IMPORTER <filename>

<filename> : full path of import file

File format : <server name><comma><ip address><linefeed>

Example File : Server 1.155,64.30,121

Server 2.155,64.30,122

Server 3,155.64.3.123

press "a" for advanced usage

When "a" is pressed for advanced usage, the following help will be
displayed:

Advanced Usage: IMPORTER <filename> <delimiter 1> <delimiter 2>
<order>

<filename> : full path of import file

<delimiter 1> : separator between first and second item in pair

<delimiter 2> : separator between pairs

NOTE: for carriage return/linefeed delimiters, use LF

for space delimiters, use SP

for comma, use,

<order> : order of computer name/ip address pairs

1 = computer name/ip address order

2 = ip address/computer name order
```

```
EXAMPLE -
File contents : 155.64.3.121/Server 1
155.64.3.122/Server 2
155.64.3.123/Server 3
Command line : IMPORTER C:\MyFolder\MyFile.txt / LF 2
```

Problemas conocidos

La herramienta Importer depende de la clave del registro HKLM\SOFTWARE\Intel\LANDesk\VirusProtect6\CurrentVersion\AddressCache que utiliza Symantec System Center. Si esta clave no existe, aparece un mensaje de error.

La herramienta Importer modifica la clave AddressCache ubicada en HKLM, por lo que el usuario debe disponer de derechos de administrador en el equipo local.

La herramienta Importer ayuda a Symantec System Center en el proceso de reconocimiento, y determina también si Symantec System Center está presente en el equipo local. Si no lo está, aparece un mensaje de error.

Tras realizar una importación, los pares de nombres y direcciones IP incluidos en el registro aún no están completos, ya que sólo muestran el equipo con los valores de tipo dword Address_0 y Protocol. Es preciso ejecutar un reconocimiento para completar el proceso (usando el botón Ejecutar reconocimiento ahora del cuadro de diálogo de propiedades del servicio de reconocimiento).

No haga clic en el botón Borrar antememoria ahora incluido en el cuadro de diálogo de propiedades del servicio de reconocimiento, ya que se borraría el contenido de la antememoria de direcciones, incluidos los datos importados.

La herramienta Importer no puede ayudar en el proceso de reconocimiento de equipos durante la instalación.

Nota: Cuando se transfieren el cliente y el servidor de Symantec AntiVirus Corporate Edition a equipos remotos, se muestra una opción de importación en el cuadro de diálogo de selección de equipos. No se debe confundir esta opción de importación con la opción de importación que aparece en las pantallas de instalación del cliente en NT y de distribución del servidor de Symantec AntiVirus.

La herramienta Importer no sobrescribe las direcciones existentes en la antememoria de direcciones (esta característica es intencionada). Sin embargo, puede darse el caso de que haya alguna dirección IP incorrecta en la antememoria. En ese caso, la herramienta Importer no podrá corregirla.

Capítulo 5

Servicios de Windows XP, 2000 y NT

En este capítulo se tratan los temas siguientes:

Servicios de Symantec AntiVirus Corporate Edition

La Tabla 5-1 recoge los nombres y las descripciones de los servicios de servidor de Symantec AntiVirus Corporate Edition. Estos nombres aparecen en la opción Servicios del Panel de control de Windows XP, 2000 y NT.

Tabla 5-1 Servicios de servidor de Symantec AntiVirus Corporate Edition

Nombre del servicio	Nombre binario	Descripción
Servidor de Symantec AntiVirus	Rtvscan.exe	Servicio principal de Symantec AntiVirus Corporate Edition. La mayoría de las tareas relacionadas con el servidor de Symantec AntiVirus Corporate Edition se
Defwatch	Defwatch.exe	Servicio que permite detectar la aparición de nuevas definiciones de virus. Ejecuta un análisis de los archivos en cuarentena cuando se reciben nuevas definiciones de virus.
Intel PDS	Pds.exe	Servicio de reconocimiento mediante ping de Intel. Permite que se detecte Symantec AntiVirus Corporate Edition en el equipo. Las aplicaciones se registran con este servicio, junto con un número de identificación de la aplicación y un paquete pong que se devuelve como respuesta a solicitudes ping.

La Tabla 5-2 recoge los nombres y las descripciones de los servicios de cliente de Symantec AntiVirus Corporate Edition. Estos nombres aparecen en la opción Servicios del Panel de control de Windows XP, 2000 y NT.

Tabla 5-2 Servicios de cliente de Symantec AntiVirus Corporate Edition

Nombre del servicio	Nombre binario	Descripción
Cliente de Symantec AntiVirus	Rtvscan.exe	Servicio principal de Symantec AntiVirus Corporate Edition. La mayoría de las tareas relacionadas con el cliente de Symantec AntiVirus Corporate Edition se desarrollan mediante este servicio.
Defwatch	Defwatch.exe	Servicio que permite detectar la aparición de nuevas definiciones de virus. Ejecuta un análisis de los archivos en cuarentena cuando se reciben nuevas definiciones de virus.

Servicios de Symantec System Center

La Tabla 5-3 recoge los nombres y las descripciones de los servicios de Symantec System Center. Estos nombres aparecen en la opción Servicios del Panel de control de Windows XP, 2000 y NT.

Tabla 5-3 Servicios de Symantec System Center

Nombre del servicio	Nombre binario	Descripción
Servicio de reconocimiento de Symantec System Center	Nsctop.exe	Servicio de reconocimiento empleado para detectar servidores de Symantec AntiVirus Corporate Edition en la red. El servicio de reconocimiento se encarga además de incluir objetos en la consola.

La Tabla 5-4 recoge los nombres y las descripciones de los servicios de Alert Management System^2. Estos nombres aparecen en la opción Servicios del Panel de control de Windows XP, 2000 y NT.

Tabla 5-4 Servicios de Alert Management System^2

Nombre del servicio	Nombre binario	Descripción
Intel Alert Handler	Hndlrsvc.exe	Servicio de gestión de alertas de AMS^2. Proporciona acciones de alerta a través de medios como cuadros de mensaje, mensajes de buscapersonas, correo electrónico, etc.
Intel Alert Originator	Iao.exe	Servicio originador de alertas de AMS^2. Permite que se reciban las alertas en el equipo. Las alertas se pueden recibir desde el equipo local (en el caso de un servidor primario) o desde un equipo remoto (en el caso de clientes no administrados que utilicen un servidor de AMS^2 centralizado).
Intel File Transfer	Xfr.exe	Servicio de intercambio de archivos. Proporciona funciones de intercambio de archivos de AMS^2.
Intel PDS	Pds.exe	Servicio de reconocimiento mediante ping de Intel. Permite que se detecte Symantec AntiVirus Corporate Edition en el equipo. Las aplicaciones se registran con este servicio, junto con un número de identificación de la aplicación y un paquete pong que se devuelve como respuesta a solicitudes ping.

Capítulo 6

Entradas del registro de sucesos en Windows XP, 2000 y NT

Sucesos de Symantec AntiVirus Corporate Edition

La Tabla 6-1 recoge los sucesos que genera Symantec AntiVirus Corporate Edition en el registro de sucesos de Windows XP, 2000 y NT.

Tabla 6-1 Sucesos generados en el registro de sucesos de Windows

Suceso	Número de suceso	Descripción
Event_Scan_Stop	2	Se produce cuando finaliza el análisis.
Event_Scan_Start	3	Se produce cuando empieza el análisis.
Event_Pattern_Update	4	Se produce cuando el servidor principal envía un archivo .vdb a un servidor secundario.
Event_Infection	5	Se produce cuando se detecta un virus durante el análisis.
Event_File_Not_Open	6	Se produce cuando no se consigue acceder a un archivo o directorio durante el análisis.
Event_Load_Pattern	7	Se produce cuando Symantec AntiVirus Corporate Edition carga un nuevo archivo .vdb.

Tabla 6-1 Sucesos generados en el registro de sucesos de Windows

Suceso	Número de suceso	Descripción
Event_Trap	11	Se produce cuando el análisis del correo electrónico en tiempo real gestiona adjuntos de correo.
Event_Config_Change	12	Se produce cuando un servidor actualiza su configuración conforme a los cambios realizados desde la consola, excluyendo los cambios realizados en las claves del registro PRODUCTCONTROL o DOMAINDATA.
Event_Shutdown	13	Se produce cuando se descarga el servicio de Symantec AntiVirus Corporate Edition.
Event_Startup	14	Se produce cuando se carga el servicio de Symantec AntiVirus Corporate Edition.
Event_Pattern_Download	16	Se produce cuando se descargan nuevas definiciones mediante una actualización planificada.
Event_Too_Many_Viruses	17	Se produce cuando Symantec AntiVirus Corporate Edition suprime o pone en cuarentena más de 5 archivos infectados en menos de un minuto. Ambos valores, tanto el número de archivos como el intervalo de tiempo, se pueden configurar desde el registro. Los valores predeterminados son 5 archivos en 60 segundos.
Event_Fwd_To_Qserver	18	Se produce cuando los archivos ubicados en el área de cuarentena se envían a un servidor de cuarentena.

Tabla 6-1 Sucesos generados en el registro de sucesos de Windows

Suceso	Número de suceso	Descripción
Event_Backup_Restore_Error	20	Se produce cuando Symantec AntiVirus Corporate Edition no consigue crear una copia de respaldo de un archivo o restaurar un archivo desde el área de cuarentena.
Event_Scan_Abort	21	Se produce cuando se detiene un análisis antes de que finalice.
Event_Rts_Load_Error	22	Se produce cuando no se puede cargar la Auto-Protección.
Event_Rts_Load	23	Se produce cuando la Auto-Protección se carga correctamente.
Event_Rts_Unload	24	Se produce cuando se descarga la Auto-Protección.
Event_Remove_Client	25	Se produce cuando un servidor principal elimina un equipo de su lista de clientes. Ocurre de forma predeterminada cuando un equipo cliente no se verifica en el servidor principal durante más de 30 días.
Event_Scan_Delayed	26	Se produce cuando se pospone o retrasa un análisis planificado.
Event_Scan_Restart	27	Se produce cuando se reinicia un análisis pospuesto o interrumpido.

Índice

P

R

S

W

X

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
Sudáfrica	+ (27) 11 797 6639
Suecia	+ (46) 8 579 29007
Suiza	+ (41) 2 23110001
RU	+ (44) 20 7744 0367
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.