



*Sistema operativo*

## Security Configuration Tool Set

Bajado desde [www.softdownload.com.ar](http://www.softdownload.com.ar)

---

### Resumen

Este documento describe Microsoft® Security Configuration Tool Set, un grupo de *snap-ins* de Microsoft Management Console (MMC) diseñados para reducir los costos relacionados con la configuración de seguridad y el análisis de las redes del sistema operativo basados en Windows NT® y Windows® 2000. Security Configuration Tool Set le permite configurar seguridad para los sistemas basados en Windows NT o Windows 2000, y después realizar análisis periódicos del sistema para asegurar que la configuración permanezca intacta o para realizar los cambios necesarios con el paso del tiempo. De igual forma, viene integrado con Administración de cambios y manejo de configuración para configurar de manera automática la política en un gran número de sistemas empresariales.

© 1999 Microsoft Corporation. Todos los derechos reservados.

*ESTE ES UN DOCUMENTO PRELIMINAR. La información contenida en este documento representa la visión actual de Microsoft Corporation en los asuntos analizados a la fecha de publicación. Debido a que Microsoft debe responder a las cambiantes condiciones de mercado no deberá interpretarse como un compromiso por parte de Microsoft, y la compañía no puede garantizar la exactitud de la información presentada después de la publicación.*

*Este documento estratégico es sólo para fines informativos. MICROSOFT NO OFRECE NINGUN TIPO DE GARANTIA, EXPRESA O IMPLICITA EN ESTE DOCUMENTO.*

*Microsoft, Active Desktop, BackOffice, el logotipo de BackOffice, MSN, Windows, y Windows NT son registros o marcas registradas de Microsoft Corporation en Estados Unidos y/u otros países.*

*Otros nombres de compañías o productos mencionados en el presente pueden ser marcas registradas de sus respectivos propietarios.*

*Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA*

*0499*

---

## TABLA DE CONTENIDOS

<b>INTRODUCCION .....</b>	<b>1</b>
¿Por qué son necesarias las Herramientas de configuración de seguridad?	1
Objetivos del diseño de las Herramientas de configuración de seguridad	2
Funciones de las Herramientas de configuración de seguridad	3
Alcance	3
Flexibilidad	4
Ampliación	4
Simplicidad	5
 <b>DESCRIPCION GENERAL DE LAS HERRAMIENTAS DE CONFIGURACION DE SEGURIDAD .....</b>	 <b>6</b>
Componentes de las Herramientas de configuración de seguridad	6
Configuraciones de seguridad	7
Configuración de seguridad y base de datos de análisis	8
Configuración de seguridad y áreas de análisis	10
Interfaces del usuario de las Herramientas de configuración de seguridad	11
Interfaces gráficas de usuario	14
Comando Secedit	15
 <b>CONFIGURAR LA SEGURIDAD.....</b>	 <b>20</b>
Políticas de cuenta	20
Políticas locales y registro de eventos	20
Grupos restringidos	21
Seguridad de registro	22
Seguridad del sistema de archivos	23
Seguridad de los servicios del sistema	23
 <b>ANALISIS DE SEGURIDAD .....</b>	 <b>26</b>
Políticas de cuenta y locales	27
Administración de grupo restringido	28
Seguridad de registro	28
Seguridad del sistema de archivo	29
Seguridad de servicios del sistema	30
 <b>INTEGRACION DE LAS POLITICAS DE GRUPO.....</b>	 <b>32</b>
Configuración de seguridad en los objetos de políticas de grupo	32
Políticas de seguridad adicionales	33
 <b>USO DE LAS HERRAMIENTAS .....</b>	 <b>35</b>
Para utilizar el Editor de configuración de seguridad	35
Para utilizar el administrador de configuración de seguridad	36
Para utilizar la extensión de configuraciones de seguridad en el editor de políticas de grupo	38
 <b>PARA MAYORES INFORMES.....</b>	 <b>42</b>

---

---

## **APENDICE A. IMPLEMENTACION DE ANEXOS DE SEGURIDAD43**

Introducción	43
Arquitectura	44
Creación de un DLL de mecanismo de anexo	45
Estructura de datos	45
Llamadas de respuesta Security Configuration Tool Set y APIs del <i>Helper</i>	47
Parámetros	48
Valores de devolución	48
Valores de devolución	49
Parámetros	49
Valores de retorno	49
Parámetros	50
Parámetros	51
Valores de retorno	52
Parámetros	52
Valores de retorno	52
Interfaces de anexo necesarias	53
Sintaxis	53
Parámetros	53
Valores de retorno	53
Sintaxis	56
Parámetros	56
Valores de retorno	56
Sintaxis	58
Parámetros	58
Valores de retorno	59
Instalación y registro	63
Creación de un <i>Snap-in</i> de extensión	63
Formato de portapapeles	65
Interfaces de <i>snap-in</i> de extensión	66
Instalación y registro	67
Inicialización—adición de un nodo de anexo	68
Implementación de ISceSvcAttachmentPersistInfo	70

---

---

## INTRODUCCION

Este documento describe las herramientas de configuración de seguridad, un grupo de herramientas de Microsoft Management Console (MMC) diseñadas para simplificar, integrar y centralizar las tareas de configuración de seguridad y análisis para sistemas basados en Windows NT® y Windows® 2000. Microsoft Management Console es una aplicación de interfaz de documentos múltiples basada en el sistema operativo Windows (MDI) que hace uso extenso de las tecnologías de Internet. MMC es la parte medular de la estrategia de administración Microsoft y está diseñada para proporcionar un *host* único para todas las herramientas de administración, facilita la delegación de tareas y disminuye los costos totales de propiedad para los usuarios empresariales de Windows y Windows NT. MMC por sí misma no proporciona ningún comportamiento de administración, sino que proporciona un ambiente común para *snap-ins*, el cual define el comportamiento de administración real. Los *snap-ins* son componentes administrativos integrados a una *host* común: la interfaz MMC.

Las herramientas de configuración de seguridad es un conjunto de *snap-ins* para MMC que está diseñado para proporcionar un *repository* central para las tareas administrativas relacionadas con la seguridad. Con las herramientas de configuración de seguridad, podrá utilizar un grupo integral de herramientas para configurar y analizar la seguridad en una o más máquinas basadas en Windows 2000 o Windows NT de su red.

### **¿Por qué son necesarias las Herramientas de configuración de seguridad?**

La versión actual del sistema operativo Microsoft Windows NT cuenta con excelentes funciones de seguridad integradas. Una conexión única al dominio basada en Windows NT permite que el usuario acceda a todos los recursos desde cualquier lugar de la red corporativa. El sistema proporciona herramientas para la política de seguridad y administración de cuenta, y el modelo de dominio Windows NT es flexible y puede soportar una amplia gama de configuraciones de red. Windows 2000 amplía estas funciones para proporcionar soporte para redes empresariales que utilizan Internet y los nuevos servicios distribuidos incluidos en el sistema operativo.

Desde el punto de vista del administrador, Windows NT proporciona varias herramientas gráficas que se pueden utilizar individualmente para configurar diversos aspectos de seguridad del sistema. Sin embargo, estas herramientas no están centralizadas, un administrador puede necesitar abrir tres o cuatro aplicaciones para configurar la seguridad de una computadora. Utilizar estas aplicaciones puede ser costoso y engorroso para varios clientes conscientes de la seguridad. Además, la configuración de seguridad puede ser compleja y con las funciones de seguridad distribuida agregadas a Windows 2000, esta complejidad ha aumentado.

Mientras que Windows NT 4.0 proporciona herramientas de configuración adecuadas (algunas inconvenientes), no cuenta con las herramientas para el

---

análisis de seguridad. La única herramienta en esta categoría es Visualizador de eventos, el cual no fue diseñado para realizar análisis de auditoría a nivel corporativo. Existen algunas herramientas de terceras partes para los mismos fines; sin embargo, incluso la mayoría de estas herramientas tampoco cuentan con funciones a nivel empresarial y no son completas.

Las Herramientas de configuración de seguridad están diseñadas para dar respuesta a la necesidad de una herramienta de configuración de seguridad central y proporcionará el marco de referencia para la funcionalidad de análisis a nivel empresarial en versiones futuras. Lo que es más importante, reducirá los costos de administración relacionados con la seguridad, al tiempo que define un punto único donde se puede ver, analizar y ajustar la seguridad de todo el sistema, según sea necesario. Esta meta es para proporcionar un grupo de herramientas completo, flexible, extensible y simple para la configuración y análisis de seguridad del sistema.

### **Objetivos del diseño de las Herramientas de configuración de seguridad**

El objetivo principal de las Herramientas de configuración de seguridad es proporcionar un punto único de administración para la seguridad del sistema basado en Windows NT y Windows 2000. Para llegar a la meta, la herramienta debe permitir al administrador:

- Configurar la seguridad en una o más computadoras basadas en Windows NT o Windows 2000.
- Realizar el análisis de seguridad en una o más computadoras basadas en Windows NT o Windows 2000.
- Completar estas tareas desde un marco de referencia integrado y uniforme.

El proceso de configuración de seguridad en una red basada en Windows NT o Windows 2000 puede ser complejo y detallado en términos de los componentes del sistema involucrado y al nivel de cambio que pueda ser necesario. Por esto, las herramientas de configuración de seguridad están diseñadas para permitirle realizar configuraciones a macronivel. En otras palabras, el grupo de herramientas le permite definir el número de configuraciones e implementarlas en segundo plano. Con esta herramienta, las tareas de configuración se pueden agrupar y automatizar; ya no requieren que se presionen varias teclas ni que se visiten repetidas veces aplicaciones diferentes para configurar un grupo de computadoras.

Las Herramientas de configuración de seguridad no están diseñadas para reemplazar las herramientas del sistema que resuelven diferentes aspectos de la seguridad del mismo, como son el Administrador del usuario, Administrador de servidor, Editor de lista de control de acceso (ACL) y demás. Ahora, su meta es completarlas definiendo un mecanismo que se puede interpretar como un archivo de configuración estándar y que realiza las operaciones que se requieren de manera automática en el segundo plano. Los administradores pueden seguir utilizando las herramientas existentes (o sus versiones más recientes) para cambiar

---

las configuraciones de seguridad individuales cuando sea necesario.

Para resolver la brecha en el análisis de seguridad en la administración de seguridad Windows NT, las herramientas de configuración de seguridad proporcionan un análisis a micronivel. El conjunto de herramientas está diseñado para proporcionar información sobre todos los aspectos del sistema relacionados con la seguridad. Los administradores de seguridad pueden ver la información y llevar a cabo la administración de riesgo de seguridad para toda su infraestructura de tecnología de información. En versiones futuras, podrán crear reportes y realizar consultas especializadas.

## **Funciones de las Herramientas de configuración de seguridad**

Las Herramientas de configuración de seguridad están diseñadas para ser completas, flexibles, ampliables y simple.

### **Alcance**

A diferencia de las demás funciones del sistema operativo, la seguridad es una característica del sistema como un todo. Casi todo componente de sistema es responsable de algunos aspectos de seguridad del mismo. Por lo tanto, preguntas como “¿mi computadora es segura?” o “¿mi red es segura?” son muy difíciles de responder. Por lo regular, un administrador de sistema debe examinar varios componentes diferentes del sistema y utilizar varias herramientas en un intento por contestar estas preguntas. El objetivo es que las herramientas de configuración de seguridad sea el recurso para responder preguntas relacionadas con la seguridad, ya sea generales (como las que se mencionan a continuación) o muy específicas. Para proporcionar administración e información de seguridad completa, las herramientas de configuración de seguridad permiten configurar y analizar todo lo siguiente:

- **Políticas de cuenta**—Puede utilizar la herramienta para establecer las políticas de acceso, incluyendo las políticas de bloqueo de cuenta local o de dominio y política de dominio Kerberos.
- **Políticas locales**—Puede configurar una política de auditoría local, asignación de derechos de usuario y varias opciones de seguridad como son el control de disco flexible, CD-ROM y demás.
- **Grupos restringidos**—Puede asignar un grupo de membresías para grupos integrados como son administradores, operadores de servidor, operadores de respaldo, usuarios de energía y demás, así como cualquier otro grupo específico que quisiera configurar. Esto no debería utilizarse como una herramienta de administración de membresía general, únicamente para controlar la membresía de grupos específicos que tienen capacidades de lectura asignadas.
- **Servicios del sistema**—Puede configurar la seguridad para los diferentes servicios instalados en un sistema, incluyendo los servicios de transporte de red, tales como TCP/IP, NetBIOS, compartir archivo CIFS, impresión, etc.

---

Estos se pueden configurar como opciones de inicio (automáticas, manuales o inhabilitadas) o también puede establecer control de acceso en estos servicios, otorgar o denegar acceso a inicio, paro, pausa y emitir comandos de control.

- **Distribución de archivo o carpeta**—Puede establecer configuraciones para el servicio de sistema de archivo Windows NT (NTFS) y redireccionador. Estos incluyen opciones para apagar el acceso anónimo y habilitar firmas de paquete y seguridad cuando se acceden varias distribuciones de archivo de red. Las versiones futuras incluirán otras subáreas específicas de servicio, incluyendo servicios tales Internet Information Server.
- **Registro de sistema**—Puede utilizar el grupo de herramientas para establecer la seguridad en las claves de registro.
- **Almacén del sistema**—Puede utilizar el grupo de herramientas para establecer la seguridad para volúmenes de archivo de sistema local y árboles de directorio.
- **Seguridad del directorio** – Puede utilizar el grupo de herramientas para administrar la seguridad en los objetos que residen en Windows 2000 Active Directory™.

### **Flexibilidad**

Las Herramientas de configuración de seguridad permiten definir las configuraciones de seguridad que incluyen configuraciones para los atributos de seguridad en cada una de las áreas que se describieron anteriormente. Al utilizar estas configuraciones, puede configurar el sistema. Asimismo, puede realizar el análisis de seguridad en el sistema utilizando estas configuraciones como recomendaciones.

Las configuraciones se guardan en archivos .inf basados en texto. La información de configuración se especifica en secciones diferentes, y la información se analiza a través del mecanismo de configuración del grupo de herramientas. Esta arquitectura es lo suficientemente flexible para soportar nuevas secciones en caso de que necesite especificar nuevas áreas de configuración de seguridad y análisis a medida que evoluciona el sistema.

Las herramientas de configuración de seguridad incluyen un grupo de configuraciones predefinidas que vendrán incluidas con esta primera versión. Puede optar por utilizar estas configuraciones como vienen, o puede utilizarlas como punto de inicio para la creación de sus propias configuraciones personalizadas. La herramienta de edición de configuración del grupo de herramientas, denominada *Editor de configuración de seguridad*, proporciona esta capacidad.

### **Ampliación**

Las Herramientas de configuración de seguridad están diseñadas para ser ampliable. Puede agregar ampliaciones como nuevas áreas de configuración y análisis de seguridad o como nuevos atributos dentro de un área existente. Debido a que la información de configuración se almacena en un formato de archivo .inf estándar, pueden ampliarse fácilmente sin afectar la compatibilidad establecida.



---

Además, *servicios del sistema* es un área definida actualmente que ha sido diseñada para ser ampliable. Permite que cualquier creador de servicio implemente un *anexo de configuración de seguridad*, que pueda configurar las configuraciones de seguridad para su servicio particular; así como también realizar cualquier análisis que pueda requerirse. Se pueden configurar diferentes sistemas basados en Windows NT para ejecutar diferentes grupos de servicios. Asimismo, Microsoft espera que los proveedores independientes de software (ISV) quienes desarrollan servicios deseen agregar su configuración y análisis de seguridad de servicio a todo su entorno de seguridad. Este conjunto de herramientas, soporta en un principio el anexo de configuración de seguridad para el servicio original Windows NT para compartir archivos de red (CIFS). Versiones futuras incluirán archivos adjuntos para IIS y demás.

### **Simplicidad**

Debido a que las Herramientas de configuración de seguridad están diseñadas para reducir los costos relacionados con la administración de seguridad en una red, es importante que la herramienta sea fácil de manejar y utilizar. El grupo de herramientas no contiene opciones complicadas, únicamente una interfaz de usuario gráfica uniforme y simple (GUI) para definir configuraciones, guardándolas en archivos y visualizando datos de análisis de seguridad almacenados en la base de datos de análisis de seguridad. La interfaz utiliza los menús de contexto estandarizados y vistas soportadas por Microsoft Management Console. No hay gráficas o estadísticas superfluas, únicamente una vista tabular simple de la información con dudas visuales que indican problemas de seguridad. Además, el grupo de herramientas contiene una utilidad de línea de comandos, Secedit.exe que permite que los administradores ejecuten la configuración y análisis como parte de un *script*. Los administradores pueden utilizar la interfaz gráfica o la línea de comandos para aplicar una configuración guardada y realizar análisis, permitiéndoles, de esta manera, arreglar fácilmente la herramienta dentro del modelo de administración existente. También pueden utilizar la interfaz gráfica para definir las configuraciones y explorar a través de los datos de análisis.

La siguiente sección de este documento proporciona una descripción general más a fondo de las herramientas de configuración de seguridad, su arquitectura y cómo se ajusta a Windows NT y Windows 2000.

---

## DESCRIPCION GENERAL DE LAS HERRAMIENTAS DE CONFIGURACION DE SEGURIDAD

Los Servicios de seguridad distribuida de Windows NT y Windows 2000 incluyen varias funciones nuevas para simplificar la administración de dominio, mejorar el rendimiento e integrar la tecnología de seguridad de Internet basada en la criptografía de clave pública. Entre algunos aspectos de los Servicios de seguridad distribuida se incluyen:

- La integración con el Servicio de directorio Windows 2000 Server (Active Directory) para proporcionar administración de cuenta flexible y escalable para grandes dominios, con control de acceso granular y delegación de administración.
- El protocolo de autenticación Kerberos versión 5, un estándar de seguridad Internet maduro, se implementa como el protocolo predeterminado para la autenticación de red y sienta las bases para la interoperabilidad de autenticación.
- La autenticación sólida que utiliza certificados de clave pública, asegura los canales basados en los protocolos estándar en la industria Secure Sockets Layer versión 3.0 y CryptoAPI versión 2.0 para la integridad y privacidad de datos a través de redes públicas.

Las mejoras de seguridad fueron específicamente diseñadas para cumplir las necesidades de las redes empresariales distribuidas. Mientras que los servicios de seguridad en Windows 2000 son impresionantes, es evidente la necesidad de una herramienta para configurar y administrar fácilmente dichas capacidades. Las herramientas de configuración de seguridad, un *snap-in* de Microsoft Management Console cumple con esta necesidad. (Para obtener una descripción detallada de Microsoft Management Console, consulte el documento estratégico titulado "Microsoft Management Console: Descripción general" en [microsoft.com](http://microsoft.com).)

### Componentes de las Herramientas de configuración de seguridad

El grupo de herramientas consiste en los siguientes componentes:

- **Servicio de configuración de seguridad**—Este servicio es el mecanismo principal de las herramientas de configuración de seguridad. Se ejecuta en cada sistema basado en Windows 2000 y es responsable de toda la funcionalidad de configuración y análisis de seguridad proporcionada por el grupo de herramientas. Este servicio es central para toda la infraestructura.
- **Seguridad de instalación**—La configuración de seguridad inicial realizada durante la instalación se hace mediante este grupo de herramientas, utilizando configuraciones predefinidas que vienen incluidas en el sistema. Esto crea una base de datos de seguridad inicial, denominada Política de computadora local, en cada computadora con una instalación completa de Windows 2000.

**Nota** Este no es el caso cuando se actualiza una máquina basada en Windows NT 4.0 o versión anterior ya que el cliente puede haber personalizado la configuración de seguridad, la cual no se puede sobrescribir. En este caso, el cliente puede utilizar la opción Configurar del

---

grupo de herramientas para aplicar una configuración.

- **Editor de configuración de seguridad**—Esta herramienta *snap-in* autónoma le permite definir configuraciones de seguridad independientes de la computadora, las cuales se guardan como archivos .inf basados en texto.
- **Administrador de configuración de seguridad**—Esta herramienta *snap-in* autónoma le permite importar una o más configuraciones guardadas en una base de datos de seguridad (la cual puede ser una base de datos de políticas de computadora local o una base de datos privada). Importar las configuraciones construye una base de datos de seguridad específica de la máquina, la cual almacena una configuración compuesta. Puede aplicar la configuración compuesta en la computadora y analizar la configuración del sistema actual comparada con la configuración compuesta almacenada en la base de datos.
- **Extensión de configuraciones de seguridad para el Editor de políticas de grupo**—Esta herramienta *snap-in* extiende el Editor de políticas de grupo. Le permite definir la configuración de seguridad como parte de *objeto de políticas de grupo*. Las políticas de grupo forman parte de la iniciativa Microsoft Windows Administration. Para obtener mayor información sobre las Políticas de grupo y Windows Administration, consulte <http://www.microsoft.com>. Posteriormente, los objetos de la política de grupo se pueden asignar a una computadora específica, o al dominio o enfoque de unidad organizacional en Active Directory, de manera que se apliquen a todas las computadoras que se encuentran en este enfoque. Las configuraciones de seguridad de los diversos objetos de la política de grupo; (unidades locales, de dominio y organizacionales) se propagan a la computadora y se importan a la base de datos de la política de computadora local en dicha computadora. La configuración compuesta a partir de esta base de datos se aplica a la computadora de manera periódica con el fin de asegurar que el sistema se adhiera a la política corporativa. A esto se le conoce como *política de seguridad* de la computadora.
- **Herramienta de línea de comando: Secedit.exe**—Esta es la interfaz de línea de comandos para algunas de las funciones del grupo de herramientas.

## Configuraciones de seguridad

El Editor de configuración de seguridad permite definir los archivos de configuración de seguridad con configuraciones de seguridad prescritas para atributos en cada *área* de seguridad (las áreas incluyen políticas de cuenta, políticas locales, grupos restringidos, el registro y demás). Los archivos de configuración de seguridad son archivos .inf basados en el texto estándar. Al utilizar administrador de configuración de seguridad se pueden importar estas configuraciones guardadas en la base de datos de seguridad en diferentes computadoras. De igual forma, se pueden importar estas configuraciones a los objetos de Política de grupo y hacer que se propaguen de manera automática a la base de datos de políticas de la computadora local.

El *snap-in* del Editor de configuración de seguridad proporciona una interfaz de usuario gráfica que le permite editar los archivos de configuración de seguridad para definir las configuraciones personalizadas. Proporciona capacidades para cortar y pegar, permitiéndole copiar parte de las configuraciones de diferentes archivos y crear una nueva configuración personalizada. (Ver Figura 1).

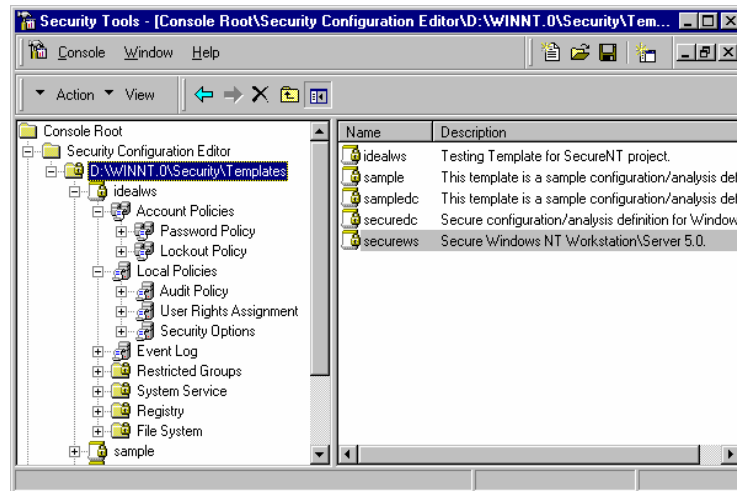


Figura 1. Editor de configuración de seguridad

Como se entrega, las Herramientas de configuración de seguridad incluye configuraciones estándar y recomendadas que son eficaces en configuraciones típicas Windows NT y Windows 2000, incluyendo aquellas instalaciones que tienen componentes Internet e Intranet. Las configuraciones predefinidas incluyen varias recomendaciones realizadas en el documento estratégico “Aseguramiento de las instalaciones Windows NT” en microsoft.com). Además, las capacidades de edición del *snap-in* le permiten utilizar los archivos de configuración de seguridad predefinidos o crear nuevos mediante su personalización para su ambiente particular.

### Configuración de seguridad y base de datos de análisis

La configuración de seguridad y base de datos de análisis es un almacén de datos específico de la computadora que se genera cuando se importan una o más configuraciones a una computadora particular. Puede ser una base de datos inicial creada cuando una computadora tiene una instalación completa de Windows 2000. Esta base de datos se conoce como la base de datos de política de la computadora local. En un principio, contiene la configuración de seguridad de su sistema directo de la caja, predeterminada. Puede exportar esta configuración a un archivo de configuración de seguridad, inmediatamente después de la instalación y guardarla. Esto es muy útil si se desea restablecer la configuración de seguridad inicial en cualquier punto posterior, por cualquier razón.

Una configuración de seguridad y base de datos de análisis, es el punto de inicio

para todas las configuraciones de análisis realizadas en el sistema. La base de datos se crea inicialmente desde un archivo de configuración independiente a la computadora descrito anteriormente. Las nuevas configuraciones se pueden agregar a la base de datos en intervalos sin tener que sobrescribir toda la configuración. (Ver Figura 2.)

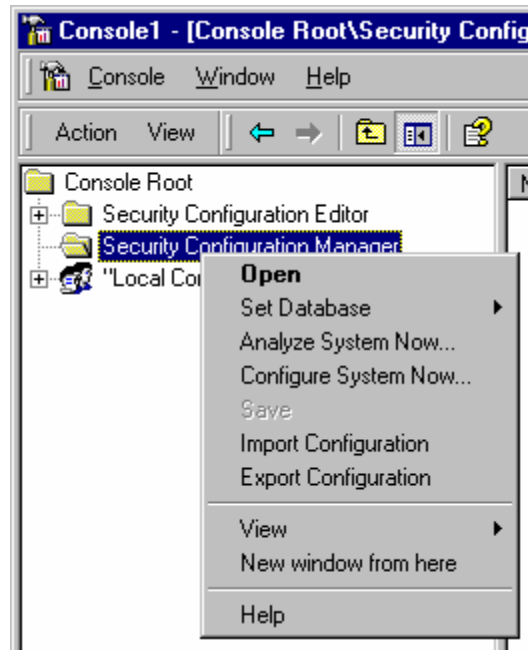


Figura 2. Menú en el Administrador de configuración de seguridad que muestra la forma en que se pueden seleccionar y/o crear bases de datos

La base de datos de política de computadora local es la base de datos de seguridad especial en el sistema. Define la política de seguridad vigente para ese sistema. En cualquier momento, el sistema se ejecuta con la configuración definida en la política. La política puede no definir toda la configuración. Esto significa que varios atributos de configuración pueden ser ignorados. Por ejemplo, la seguridad para cada ruta de archivo o carpeta puede no estar definida. Esto implica que los atributos de configuración de seguridad que no son reforzados por esta política pueden tomar cualquier valor: predefinido o definido por algún otro mecanismo, como ACL Editor en Windows Explorer para seguridad de archivos y carpeta. Los aspectos que no están respaldados por la política también se pueden configurar de manera manual utilizando bases de datos personales. Sin embargo, cualquiera de las configuraciones personalizadas que tengan conflicto con la política se sobrescriben según las definiciones que hay en la política. Las configuraciones de la base de datos personal son útiles en áreas como registro y el sistemas de archivo, donde varios usuarios en el sistema pueden asegurar su propio *hive* de registro y subramas de directorio de inicio.

Otro aspecto importante de la base de datos de seguridad es su uso al realizar el análisis. Puede utilizar un Administrador de configuración de seguridad para

realizar una comparación de la configuración del sistema actual contra la configuración almacenada en la base de datos. La realización del análisis le proporciona la información sobre dónde se puede estar desviando un sistema particular desde una configuración particular. Esto ayuda a la resolución de problemas, a la sintonización de políticas de seguridad y lo que es más importante, a la detección de cualquier defecto de seguridad que se pudiera presentar en el sistema con el tiempo. (Ver Figura 3.)

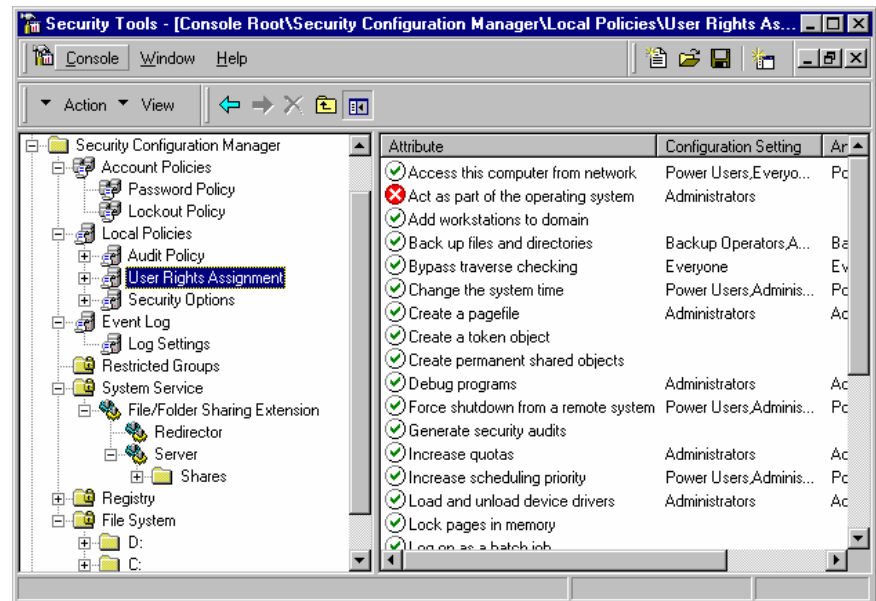


Figura 3. Administrador de configuración de seguridad mostrando análisis

## Configuración de seguridad y áreas de análisis

La configuración de seguridad para un sistema se subdivide en áreas de seguridad, según se estableció anteriormente. Microsoft ha identificado varias áreas de seguridad; sin embargo, se pueden agregar nuevas áreas en un futuro para soportar la funcionalidad de sistema mejorado sin interrumpir la compatibilidad de respaldo con los archivos y bases de datos de configuración existentes. Las áreas de seguridad actualmente soportadas son:

- **Políticas de cuenta**—Esta es un área que le permite establecer contraseñas, bloqueos de cuenta y políticas Kerberos. Las políticas Kerberos son relevantes únicamente en controladores de dominio Windows 2000.
- **Políticas locales**—Esta área le permite configurar la política de auditoría, asignación de derechos al usuario y opciones de seguridad de computadora.
- **Grupos restringidos**—Estas configuraciones administran las membresías de grupo para grupos seleccionados que pueda considerar delicados.
- **Arboles de objeto**—Existen tres áreas de seguridad en esta categoría:
  - Objetos de directorio—únicamente controladores de dominio Windows 2000.
  - Claves de registro.

- Sistema de archivo local.

Para cada árbol de objeto, los archivos de configuración definidos le permiten configurar (y analizar) configuraciones para descriptores de seguridad, incluyendo propiedad de objeto, la Lista de control de acceso (ACL) e información para la realización de auditorías.

- **Servicios del sistema**—Esta área incluye todos los servicios del sistema de red o locales. Esta área de seguridad está diseñada de tal forma que los proveedores independientes de software (ISVs) puedan crear archivos adjuntos de las Herramientas de configuración de seguridad para la configuración y análisis de servicios de sistema específicos. Asimismo, Microsoft creará archivos adjuntos para algunos servicios que vienen incluidos con el sistema. La primera versión incluirá un anexo para la configuración y análisis de seguridad en el servicio de Compartir archivos de red. Consulte el Apéndice A, Archivos adjuntos para la implementación de seguridad de servicio, para las instrucciones sobre implementación e instalación sobre ese tema.

## **Interfaces del usuario de las Herramientas de configuración de seguridad**

La GUI de las Herramientas de configuración de seguridad se proporciona como un grupo de *snap-ins* de Microsoft Management Console (MMC). La interfaz gráfica soporta las siguientes funciones administrativas:

- **Definición de configuraciones de seguridad**—El grupo de herramientas incluye el Editor de configuración de seguridad, el cual le permite definir y guardar una configuración. Debido a que las configuraciones se guardan como archivos .inf basados en texto, puede utilizar cualquier editor de texto para leer la configuración de muestra que se proporciona con la herramienta y comprender su formato; sin embargo, Microsoft no recomienda el uso del editor de texto para alterar un archivo de configuración. Si se hace, se podría alterar el formato del archivo inadvertidamente; con lo que no podría ser analizado por el mecanismo del Servicio de configuración de seguridad. Por lo contrario, se debe utilizar el *snap-in* del Editor de configuración de seguridad para crear o cambiar un archivo de configuración.

Para utilizar el Editor de configuración de seguridad, inicie MMC y agregue el *snap-in* autónomo del Editor de configuración de seguridad y todas sus extensiones dentro de la nueva consola MMC, las cuales se pueden guardar para un uso futuro. Para más información, lea la documentación de ayuda que viene en Microsoft Management Console.

- **Configuración de seguridad del sistema**—Para configurar la seguridad de un sistema basado en Windows NT o Windows 2000, puede utilizar una de las opciones que se encuentran en el grupo de herramientas:
  - **Extensión de las configuraciones de seguridad para Editor de políticas de grupo**—Esta opción se recomienda para configuración si tiene una infraestructura Windows basada en Active Directory. De igual forma,

---

puede ser utilizada de manera local en computadoras individuales con o sin Active Directory. En el caso local, se configura localmente un objeto de política de grupo en una computadora. Para utilizar esta opción, inicie Editor de políticas de grupo e indique un objeto de política de grupo adecuado, el cual puede ser el almacenado en Active Directory o el que se encuentra localmente en una computadora. Haga clic en **Configuraciones de computadora**, y después Haga clic en **Configuraciones de seguridad**<sup>1</sup>. El espacio del nombre que verá en este lugar es idéntico al que se presenta en el Editor de configuración de seguridad, donde se edita una configuración particular. Puede copiar y pegar nodos específicos (cada uno representando un área de seguridad particular) desde SCE en un nodo correspondiente en las Políticas de grupo o puede importar toda la configuración a las Políticas de grupo. Esto hace que la configuración de seguridad se guarde en un objeto de política de grupo y se aplique como parte del reforzamiento de las Políticas de grupo. Los objetos de política de grupo se aplican a una computadora, basándose en el enfoque Active Directory (unidades de dominio y organizacionales) bajo las cuales está la computadora. Esto puede provocar que se apliquen a la computadora diversas configuraciones de seguridad. Si contienen los mismos atributos, el último escritor gana, basado en el orden de aplicar objetos de política de grupo. Para más información sobre la infraestructura de política de grupo, consulte "Políticas de grupo Windows 2000" en microsoft.com.

- **Administrador de configuración de seguridad**—Esta opción de configuración se recomienda únicamente cuando no cuenta con una infraestructura Windows basada en Active Directory y no necesita aplicar la configuración periódicamente; en otras palabras, tendría que controlar en su lugar la configuración y análisis de manera manual. Para utilizar esto, inicie MMC y agregue el *snap-in* del Administrador de configuración de seguridad así como sus *snap-ins* de extensión. Por predeterminación, el *snap-in* indica a la base de datos de política de la computadora local. Usted puede seleccionar cambiar a una base de datos diferente dando un clic con el botón derecho en el nodo **Administrador de configuración de seguridad**, y después dando un clic en **Establecer base de datos** del menú **Contexto**. En el SCM, seleccione **Importar configuración** del menú **Contexto**. Esto abre la caja de diálogo **Abrir archivo**, la cual se utiliza para explorar la configuración guardada y seleccionarla. Repita este proceso importando las configuraciones guardadas adicionales como *configuraciones en incrementos*. Esta base de datos hace que surjan varias configuraciones para crear una configuración compuesta, con la que se resuelven conflictos con la regla el último escritor gana. Una vez que se importen las configuraciones a la base de datos seleccionada, Haga clic en

---

<sup>1</sup> Si utiliza la consola MMC denominada gpedit.msc, Configuraciones de seguridad ya estará cargada en ella, si carga el Editor de políticas de grupo en una nueva Consola, necesitará añadir Configuraciones de seguridad y todas sus sub-extensiones desde el indicador **Extensions**.



---

**Configurar ahora** del menú **Contexto** para aplicarla al sistema. Una caja de diálogo en proceso muestra la forma en que se está aplicando la configuración y por último mostrará un registro de error, en caso de que se encuentren errores en el proceso.

- **Herramienta de línea de comandos Secedit**—Esta opción se recomienda, si no tiene una infraestructura basada en Active Directory y tiene varias computadoras que necesiten configurarse con frecuencia. Inicie una ventana de consola, y especifique *Secedit.exe*; después seleccione las opciones aplicables como, dónde se deberá mantener la base de datos de seguridad, cuáles configuración(es) utilizar y demás. De igual forma, puede crear archivos de comando en serie y después programarlos para que se ejecuten en horas extra, utilizando el programador de tareas. Puede utilizar Microsoft System Management Server para distribuir esta tarea en varias computadoras.

**Nota** El grupo de herramientas, soporta la capacidad de aplicar múltiples configuraciones. Puede seleccionar aplicar en un principio una pequeña configuración y después agregar las configuraciones. La base de datos de seguridad almacena la forma emergente de múltiples configuraciones y las programaciones de configuración más recientes sobrescriben cualquier valor anterior para la misma.

- **Seguridad del sistema de análisis**—Para analizar la seguridad del sistema, Haga clic en **Analizar** en el menú **Contexto** dentro del *snap-in* del Administrador de configuración de seguridad, o utilice la utilidad de la línea de comandos para recopilar el análisis en la base de datos de seguridad. Esto puede realizarse en la forma de un *script* administrativo que se puede ejecutar inmediatamente o cuando su uso sea más conveniente. Asimismo, puede utilizar System Management Server para distribuir esta tarea en diferentes computadoras.
- **Ver datos de análisis de seguridad**—El Administrador de configuración de seguridad, permite ver la información de seguridad en cada área de seguridad. Las recomendaciones de configuración guardadas se presentan a lo largo de las configuraciones del sistema recopiladas a la fecha, y los iconos se utilizan para señalar cualquier área de problema donde las configuraciones actuales no coincidan con las guardadas en la configuración. Puede corregir los problemas reconfigurando el sistema dando un clic en **Configurar ahora...** del menú **Contexto**. El SCM también le permite modificar las programaciones de configuración guardadas de manera que coincidan con la configuración del sistema actual. Posteriormente, puede conservar la configuración actual, la cual está reflejada en la base de datos. Los análisis futuros ya no presentarán este problema. Esto también se puede utilizar para hacer cualquier cambio en la marcha que necesite aplicarse

**Nota** Mientras que varias interfaces de usuario gráficas proporcionan toda la funcionalidad de la lista anterior, la utilidad de la línea de comandos soporta únicamente la configuración del sistema y la recolección de datos de análisis. No soporta la creación o edición de

configuraciones ni la visualización de datos de análisis.

### Interfaces gráficas de usuario

Las siguientes interfaces gráficas de usuario se proporcionan con el grupo de herramientas:

- **Editor de configuración de seguridad**—Este es un *snap-in* autónomo que permite capacidades de edición para las configuraciones de seguridad. (Ver Figura 4.)

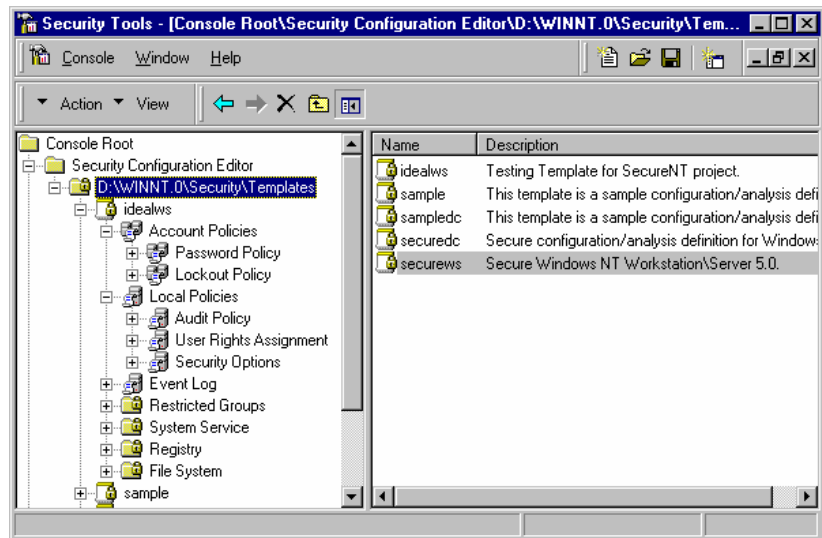


Figura 4. Editor de configuración de seguridad

- **Administrador de configuración de seguridad**—Este es un *snap-in* autónomo que permite la importación de configuraciones a una base de datos de seguridad, configuración del sistema con cualquiera de las configuraciones guardadas (compuestas) en la base de datos y el análisis del estado de seguridad actual comparado con la configuración guardada y el reporte de cualquier discrepancia (Ver Figura 5.)

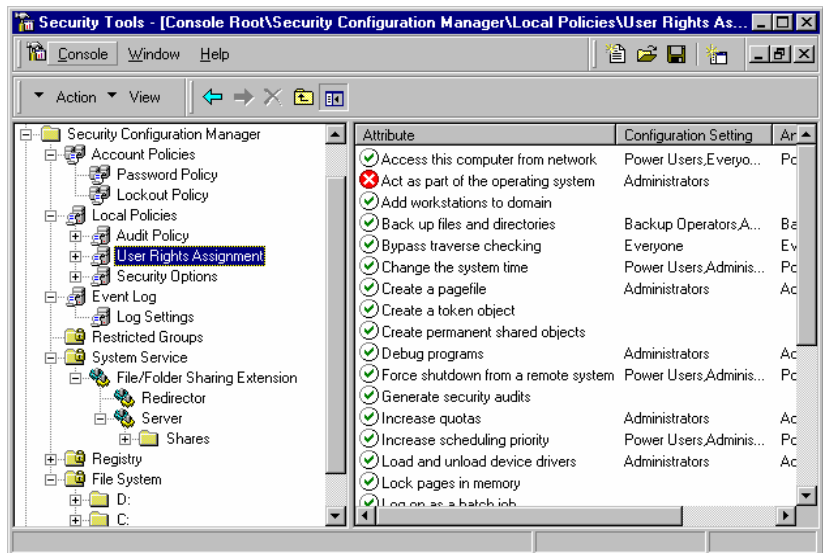


Figura 5. Administrador de configuración de seguridad

- **Extensión de las configuraciones de seguridad**—Este es un *snap-in* de extensión para el Editor de políticas de grupo. Permite guardar una configuración de seguridad como parte de los objetos de políticas de grupo, los cuales pueden ser asignados a computadoras individuales o grupos de computadoras y aplicarse de manera automática (Ver Figura 6.)

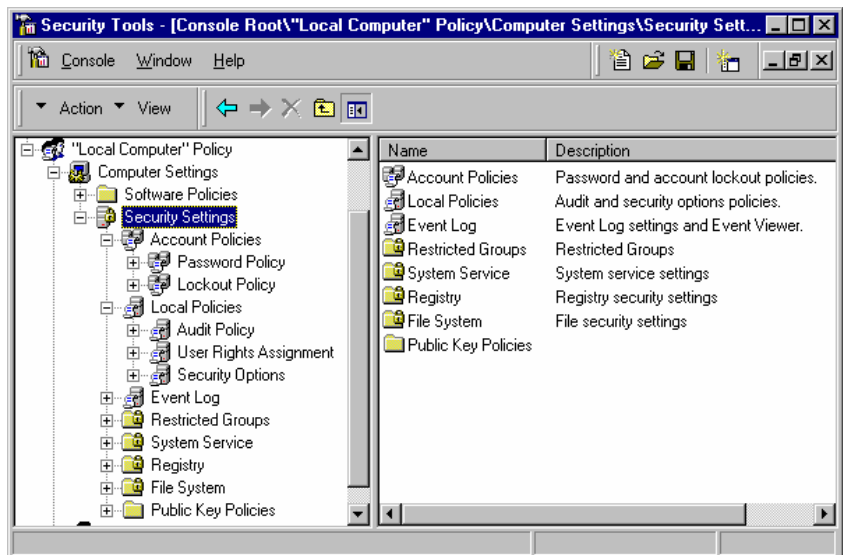
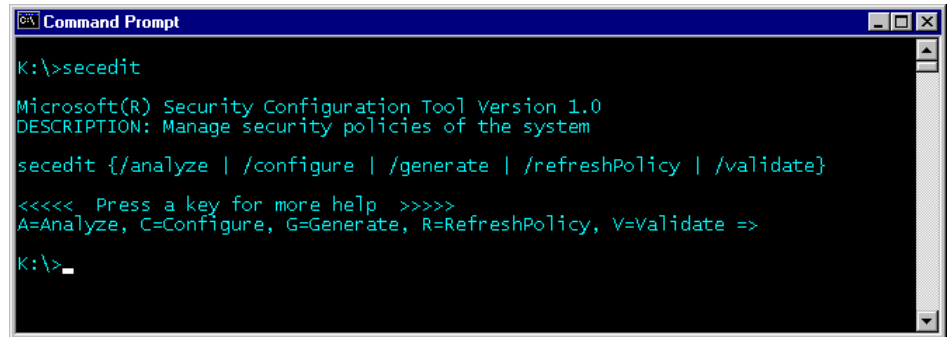


Figura 6. Extensión de configuraciones de seguridad para el Editor de políticas de grupo que muestra el GPE enfocado en una política de computadora local.

### Comando Secedit

La Figura 7 muestra los parámetros de uso disponibles con la utilidad de línea de comando Configuración de seguridad, Secedit.



```
K:\>secedit

Microsoft(R) Security Configuration Tool Version 1.0
DESCRIPTION: Manage security policies of the system

secedit [/analyze | /configure | /generate | /refreshPolicy | /validate]

<<<<< Press a key for more help >>>>>
A=Analyze, C=Configure, G=Generate, R=RefreshPolicy, V=Validate =>

K:\>_
```

Figura 7. Utilidad de línea de comando Secedit

La sintaxis del comando es:

```
secedit {/analyze | /configure | /generate | /refreshPolicy | /validate}
```

Las especificaciones de sintaxis para cada opción Secedit se describen a continuación.

#### **Análisis Secedit**

Lo siguiente analiza la seguridad del sistema:

```
secedit /analyze [/scppath scppath] [/sadpath sadpath] [/log logpath] [/verbose] [/quiet]
```

donde

- **/sadpath** *sadpath* es la ruta a la base de datos con la que Secedit realiza el análisis. Los resultados del análisis se almacenan en esta base de datos, junto con la información de configuración que ya existe. En caso de que no se especifique *sadpath*, entonces se utiliza la base de datos predeterminada. La base de datos predeterminada es %windir%\security\database\secedit.sdb para los administradores o userprofile%\secedit.sdb para los usuarios. Si *sadpath* es una nueva base de datos, debe especificarse el *scppath*.
- **/scppath** *scppath* es la ruta al archivo de configuración que deberá cargarse en la nueva base de datos antes de realizar el análisis. Si no se especifica *scppath*, el análisis se realiza comparando la información de configuración que ya está contenida en la base de datos *sadpath*. *Scppath* sólo es válido cuando *sadpath* es una nueva base de datos.
- **/log** *logpath* es la ruta para registrar el archivo para el proceso. Si no se proporciona, se utiliza el valor predeterminado %windir%\security\logs\scesrv.log.
- **/verbose** da instrucciones a Secedit para que proporcione información detallada del progreso.
- **/quiet** da instrucciones a Secedit para suprimir la pantalla y desconectarse.

---

### Configuración Secedit

Lo siguiente configura la seguridad para el sistema:

```
secedit /configure [/scppath scppath] [/areas areas]  
[/overwrite] [/sadpath sadpath] [/log logpath] [/verbose]  
[/quiet]
```

donde:

- **/sadpath sadpath** es la ruta a la base de datos que Secedit utilizará para configurar el sistema (con la adición de información en *scppath* si se especifica *scppath*). Si no se especifica *sadpath*, entonces se utiliza la base de datos predeterminada. La base de datos predeterminada es %windir%\security\database\secedit.sdb para los administradores o %userprofile%\secedit.sdb para los usuarios. Si *sadpath* es la nueva base de datos, debe especificarse *scppath*.
- **/scppath scppath** es la ruta al archivo de configuración que deberá cargarse en la base de datos antes de realizar la configuración. Si no se especifica *scppath*, el sistema se configura utilizando la información de configuración ya contenida en la base de datos *sadpath*.
- **/areas areas** especifica las áreas de seguridad que van a ser procesadas de la siguiente manera:
  - SECURITYPOLICY—Política local o política de dominio para el sistema.
  - USER\_MGMT—Configuraciones de cuenta del usuario para cada usuario.
  - GROUP\_MGMT—Configuraciones restringidas de grupo (únicamente para grupos especificados en el perfil).
  - USER\_RIGHTS—Uso de derechos de conexión y otorgamiento de privilegios,
  - DSOBJECTS—Seguridad en los objetos del directorio.
  - REGKEYS—Seguridad en las claves de registro local.
  - FILESTORE—Seguridad en el almacenamiento de archivos locales.
  - SERVICES—Configuración de seguridad para todos los servicios definidos.

El valor predeterminado es Todas las áreas. Cada área deberá estar separada por un espacio.

- **/log logpath** es la ruta para registrar el archivo para el proceso. Si no se proporciona se utiliza el valor predeterminado %windir%\security\logs\scesrv.log.
- **/verbose** da instrucciones a Secedit para proporciona información detallada de progreso.
- **/quiet** da instrucciones a Secedit para suprimir la pantalla y desconectarse.
- **/overwrite** especifica que la información de la configuración cargada de *scppath* deberá sobrescribir cualquier información de configuración existente que se mantenga actualmente en la base de datos. Cualquiera de las configuraciones futuras que utilicen esta base de datos están únicamente basadas en la información que se especifica en el archivo *scppath*. Si no se especifica **Sobrescribir**, la información del archivo *scppath* se agrega a

---

cualquier información existente en la base de datos *sadpath*. **Sobrescribir** es válido únicamente si se especifica **scppath**.

#### Generar Secedit

Lo siguiente genera un archivo de configuración de la base de datos:

```
secdit /generate /scppath scppath [/areas areas] [/sadpath sadpath] [/log logpath] [/verbose] [/quiet]
```

donde:

- **/sadpath sadpath** es la ruta a la base de datos que Secedit utilizará para obtener información y configuración del sistema. Si no se especifica *sadpath*, entonces se utiliza la base de datos predeterminada. La base de datos predeterminada es %windir%\security\database\secdit.sdb para los administradores o %userprofile%\secdit.sdb para los usuarios. Si *sadpath* es una nueva base de datos, debe especificarse *scppath*.
  - **/scppath scppath** es la ruta al archivo donde se guardará la información de configuración. *Scppath* debe especificarse para esta operación.
  - **/areas areas** especifica las áreas de seguridad que van a ser procesadas, de la siguiente manera:
    - SECURITYPOLICY—Política local y política de dominio para el sistema.
    - USER\_MGMT—Configuraciones de cuenta del usuario para cada usuario.
    - GROUP\_MGMT—Configuraciones de grupo restringidas (únicamente para grupos especificados en el perfil).
    - USER\_RIGHTS—Derechos de conexión del usuario y otorgar privilegios.
    - DSOBJECTS—Seguridad en los objetos de directorio.
    - REGKEYS—Seguridad en las claves de registro local.
    - FILESTORE—Seguridad en el almacenamiento de archivo local.
    - SERVICES—Configuración de seguridad para todos los servicios definidos.
- El valor predeterminado es Todas las áreas. Cada área deberá estar separada por un espacio.
- **/log logpath** es la ruta para registrar el archivo para el proceso. Si no se proporciona, se utiliza el valor predeterminado %windir%\security\logs\scesrv.log.
  - **/verbose** da instrucciones a Secedit para proporcionar información detallada del progreso.
  - **/quiet** da instrucciones a Secedit para eliminar la pantalla y desconectarse.

#### Generar Secedit

A continuación se inicia la propagación de política de seguridad en segundo plano.

```
secdit /RefreshPolicy {MACHINE_POLICY | USER_POLICY}
```

donde

- **RefreshPolicy** da instrucciones a Secedit para restablecer la política de seguridad de la siguiente manera:

- 
- MACHINE\_POLICY restablece la política para la máquina local
  - USER\_POLICY restablece la política para el usuario de esta ID de acceso.

#### **Generar Secedit**

Lo siguiente valida la sintaxis de un archivo de configuración del Editor de configuración de seguridad:

**secedit /validate filename**

donde

- **validate filename** especifica el archivo de configuración que se va a validar

## CONFIGURAR LA SEGURIDAD

Esta sección describe cómo utilizar las Herramientas de configuración de seguridad, para configurar los diversos aspectos de seguridad de un sistema basado en Windows 2000. Estas herramientas recaen por completo en las funciones de seguridad de Windows 2000, no alteran las capacidades de seguridad del sistema. El único fin del grupo de herramientas es permitirle una configuración y administración más sencillas de las funciones de seguridad avanzadas incluidas en la última versión del sistema operativo.

### Políticas de cuenta

En Windows 2000 existen dos tipos de cuenta, cuentas de dominio y cuentas locales. Las políticas de cuenta para las cuentas de dominio están configuradas en el dominio y las políticas de cuenta para cuentas locales están configuradas localmente en la computadora. Esto permite un control de seguridad granular, pero puede ser difícil de configurar. La Figura 8 muestra la vista de configuración para las políticas de cuenta.

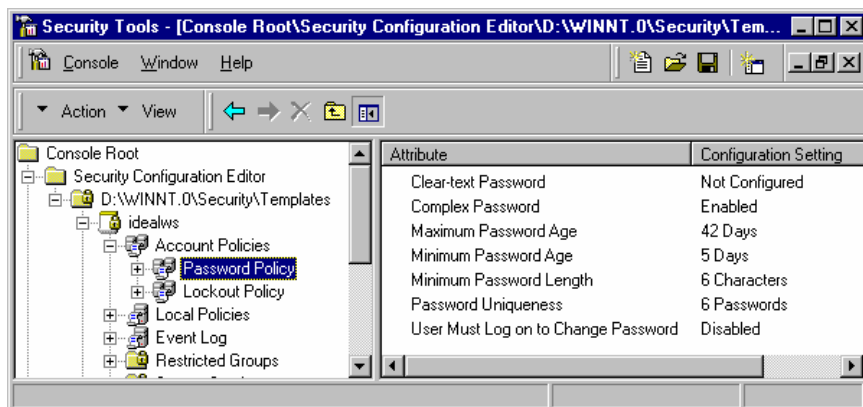


Figura 8. Configuración de políticas de cuenta

Una política de cuenta de dominio, define qué tan sólidas tienen que ser las contraseñas, el historial de contraseñas, la duración de las boletas Kerberos, bloqueos de cuentas y demás. Puede definir todos estos atributos desde la configuración de seguridad. De manera similar puede especificar localmente en una computadora las mismas políticas para las cuentas locales. La única excepción para esto es la política Kerberos, la cual no existe para cuentas locales, las cuales no son autenticadas utilizando Kerberos.

### Políticas locales y registro de eventos

En Windows 2000 las políticas locales son, por definición, locales para una computadora sin distinción entre las diferentes computadoras (controladores de dominio, servidores o estaciones de trabajo). Las políticas locales incluyen la política de auditoría, derechos de usuario y asignación de privilegios, así como varias opciones de seguridad que se pueden configurar de manera local en una



computadora particular basada en Windows 2000.

- La política de auditoría permite configurar cuáles eventos de seguridad se configuran en el registro de seguridad en esta computadora.
- Los derechos de usuario y asignación de privilegios le permiten controlar quién tiene derechos y privilegios en un sistema determinado.
- Las opciones de seguridad le permiten controlar quién tiene acceso a esos elementos, como el disco flexible y CD-ROM.

Al igual que con las políticas de cuenta, la política local se puede configurar o analizar utilizando opciones múltiples disponibles en el grupo de herramientas. La Figura 9 muestra algunas de las opciones disponibles para la configuración de políticas locales.

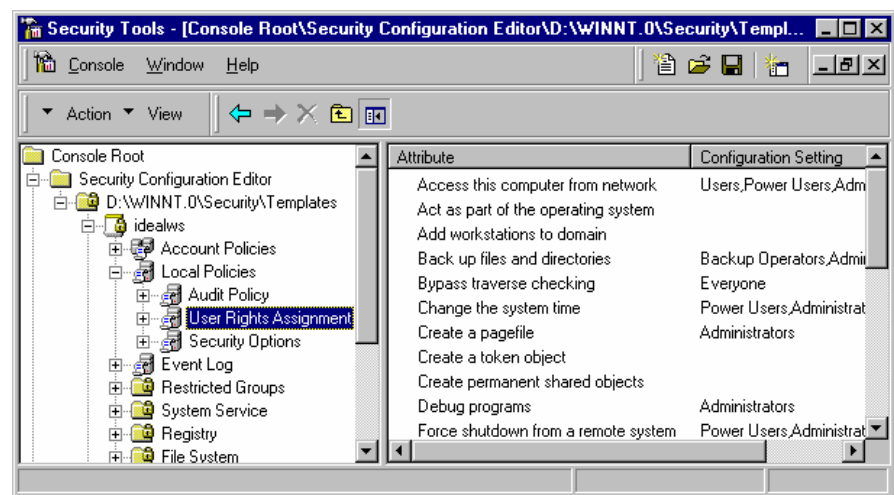


Figura 9. Configuración de políticas locales

## Grupos restringidos

El área de grupo restringido le permite administrar los miembros de grupos incorporados que tienen ciertas capacidades predefinidas. Estos grupos incluyen grupos incorporados como administradores, usuarios avanzados, operadores de impresión, operadores de servidor, etc., así como grupos de dominio, como son administradores de dominio.

Asimismo, puede agregar grupos que considere adecuados o privilegiados para la lista de Grupos restringidos, junto con su información de membresía. Esto le permite un seguimiento y administrar estos grupos como parte de la configuración o política de seguridad del sistema.

Además de los miembros de grupo, el área rastrea y controla la membresía inversa de cada grupo restringido en la columna **Miembros de**. Esta columna muestra otros grupos a los que puede pertenecer el grupo restringido. Puede utilizar este campo para controlar exactamente qué miembros de su grupo restringido pueden

unirse, además, puede utilizar esta función para limitar un grupo de usuarios a un grupo y evitar que se unan con otros. (Ver Figura 10.)

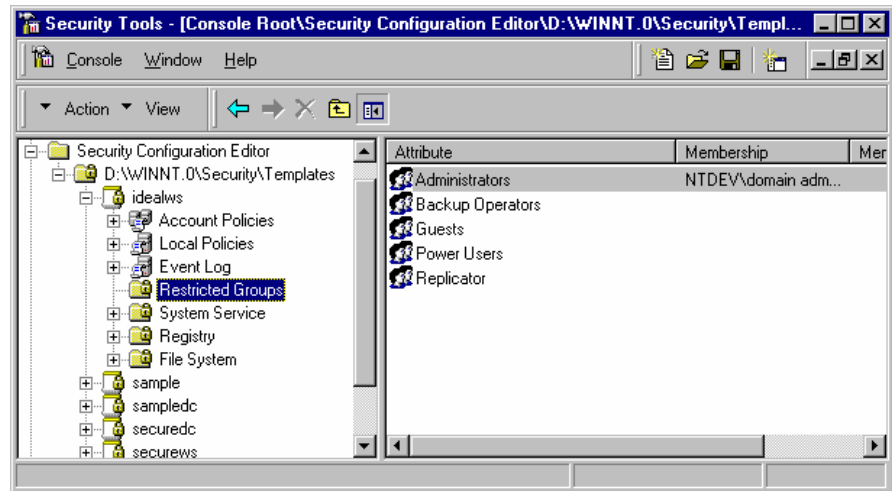


Figura 10. Configuración de grupos restringidos

La aplicación de la configuración asegura que las membresías de grupo se establecen como se especifica en el archivo de configuración. Los grupos y usuarios que no estén especificados se eliminan del grupo restringido. Además, la opción **Configuración de membresía inversa** asegura que cada grupo restringido es miembro únicamente de aquellos grupos que se especifican en la columna **Miembro de**.

## Seguridad de registro

El registro es otro árbol de objeto en el que las Herramientas de configuración de seguridad le permite administrar los objetos colocando un descriptor de seguridad en el objeto. Sin embargo, en el caso del registro, los objetos son claves de registro. Nuevamente, la configuración contiene la ruta clave de registro completa y el descriptor de seguridad en formato SDDL.

Ya que Windows 2000 soporta un modelo heredado dinámico para todos los proveedores de objetos, al aplicar la seguridad en las claves de registro, las Herramientas de configuración de seguridad siguen el mismo algoritmo que aparece en el árbol de directorio. La configuración de los *snap-in* para configuración de seguridad de registro se muestra en la Figura 11.

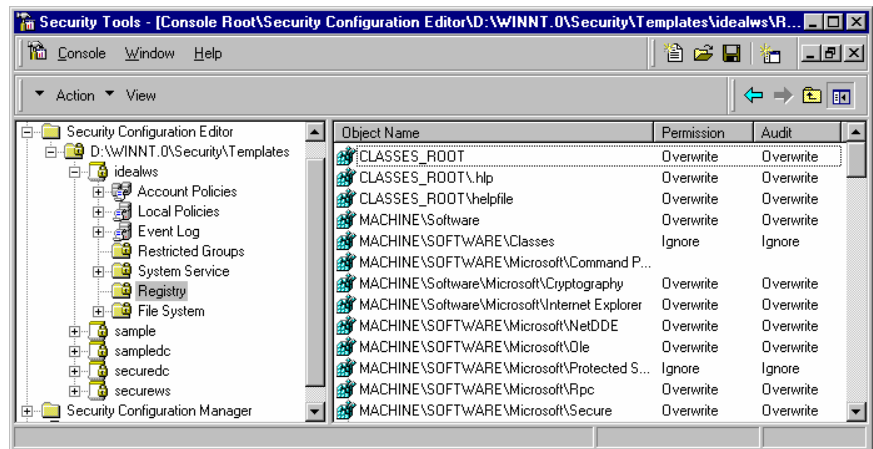


Figura 11. Programación de las configuraciones de seguridad de registro

## Seguridad del sistema de archivos

La seguridad del sistema de archivos local es el tercer árbol de objeto soportado dentro de las Herramientas de configuración de seguridad. Trata todos los volúmenes en un sistema como parte de un solo árbol, con nodos del primer nivel como el directorio raíz de cada volumen. Esto es similar a la configuración de seguridad de registro y directorio en el que el archivo de configuración contiene una lista de las rutas de directorio o archivo completamente calificada y descriptores de seguridad para cada una. Asimismo, el modelo heredado dinámico se soporta en los archivos NTFS. El esquema de configuración de los *snap-in* para la seguridad del sistema de archivos se muestra en la Figura 12.

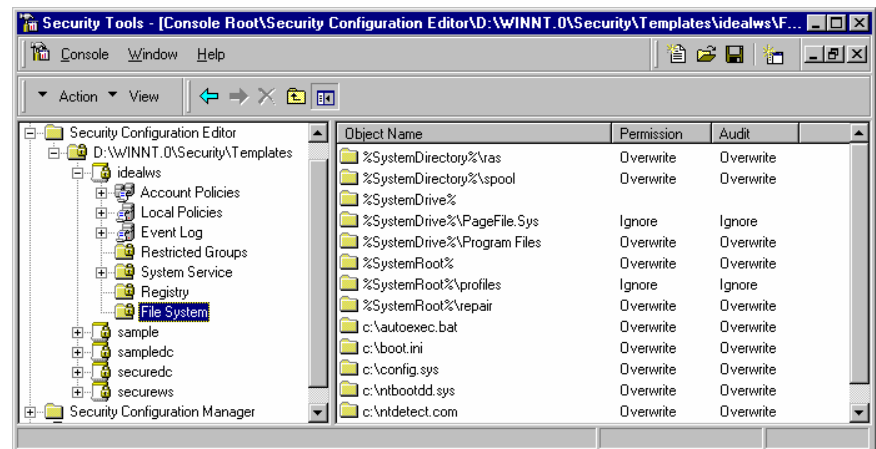


Figura 12. Programación de las configuraciones de seguridad del sistema de archivo

## Seguridad de los servicios del sistema

Los servicios del sistema incluyen una funcionalidad crítica, como son los servicios de red, servicios de archivo e impresión, servicios de telefonía y fax y servicios

Internet/Intranet. Debido a la gran variedad y diversidad de esta área, el área de servicios de sistema de las Herramientas de configuración de seguridad están diseñadas para expandirse. Las Herramientas de configuración de seguridad soportan directamente las configuraciones generales para cada servicio de sistema. Estas configuraciones generales incluyen el modo de inicio de servicios (automático, manual o inhabilitado) y seguridad en el servicio. El nombre del servicio debe ser el mismo que fue utilizado por el administrador de control de servicio. (Ver Figura 13.)

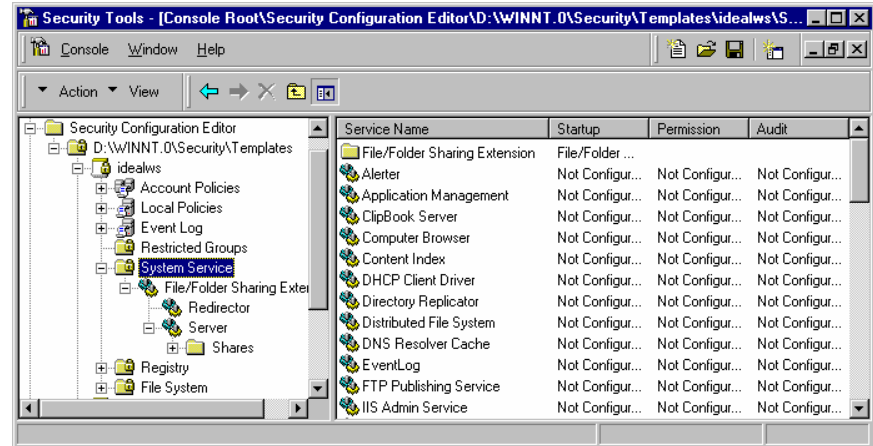


Figura 13. Configuración de seguridad de servicios del sistema

Para ampliar esta área de las Herramientas de configuración de seguridad de manera que pueda ser utilizada para establecer configuraciones específicas para un nuevo servicio, cree y adjunte un anexo de configuración de seguridad, que conste de lo siguiente:

- **Un mecanismo DLL** que exporte tres interfaces bien definidas. La implementación de todas estas interfaces es opcional. Se utiliza una interfaz para establecer las configuraciones, otra consulta las configuraciones para análisis (que se trata a continuación) y la tercera actualiza las configuraciones. Puede optar por implementar únicamente una configuración, sólo en análisis o ambas. Puede optar por soportar la edición del usuario de configuración almacenada en la base de datos. Deberá registrar el nombre de este DLL en un lugar conocido en el registro, junto con el nombre del servicio al que aplica. El servicio del Mecanismo de configuración de seguridad busca la clave de registro para obtener la lista de servicios y carga cada DLL adjunto. Posteriormente, el Mecanismo de configuración de seguridad solicita la interfaz correspondiente, dependiendo si se trata de una configuración del sistema o de una recopilación de la información de análisis. La interfaz se comunica con el anexo, el cual es por ende responsable de guardar la configuración o información de análisis en la sección específica dentro de la configuración y de utilizar la misma información para configurar el sistema o alertar al administrador.

- **Un *snap-in* de extensión**, el cual amplía los *snap-ins* de configuración de seguridad (el editor y al administrador) dentro de Microsoft Management Console. El *snap-in* de extensión consta de un nodo de panel de enfoques—con el espacio de su propio nombre—que extiende el nodo de servicios a las configuraciones de soporte específicas del servicio. Asimismo, el *snap-in* de extensión necesita exportar interfaces bien definidas para que se comuniquen con los *snap-in* de configuración de seguridad. El *snap-in* de extensión no se comunica directamente con su DLL del mecanismo. Un *snap-in* de extensión proporciona funcionalidad únicamente cuando es solicitado por un *snap-in* principal (en este caso el conjunto de herramientas de configuración).
- **Un *estuche de instalación*** que registra el mecanismo para las Herramientas de configuración de seguridad y el *snap-in* de extensión.

La Figura 14 muestra las piezas de un anexo y la manera en que se incorporan al *snap-in* del Grupo de herramientas de configuración y MMC.

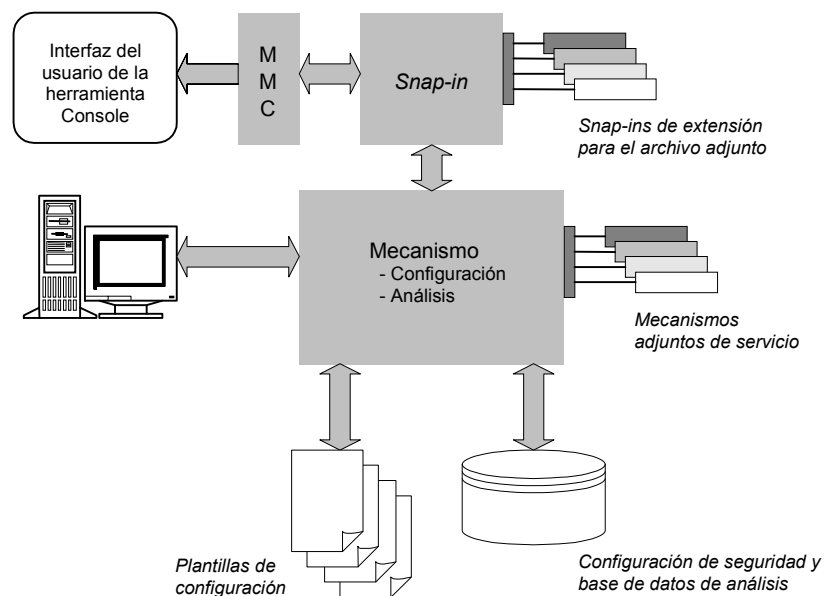


Figura 14. Security Configuration Tool Set y arquitectura de archivos adjuntos

Microsoft proporciona anexos para algunos servicios que vienen con el sistema. En su versión inicial, Microsoft planea enviar un anexo de configuración de seguridad para el servicio de distribución de archivos CIFS.

Además, la interfaz que se utiliza para extender el grupo de herramientas se describe en el Apéndice A, Implementación de anexos de seguridad de servicio.

---

## ANÁLISIS DE SEGURIDAD

Esta sección describe cómo utilizar las Herramientas de configuración de seguridad para analizar los diversos aspectos de seguridad de un sistema basado en Windows 2000. Las Herramientas de configuración de seguridad proporcionan una interfaz gráfica que le permite visualizar la información de análisis recopilada del sistema. Asimismo, puede utilizar el Administrador de configuración de seguridad o la utilidad de línea de comando, **secedit**, para recopilar los datos de análisis del sistema. Esto le permite reunir los datos de manera interactiva o programar la recopilación de datos como parte de un *script* de procesamiento en serie en horas extras, utilizando System Management Server o el programador de tareas.

A fin de promover la facilidad de uso (y eliminar la basta curva de aprendizaje normalmente relacionada con las nuevas herramientas de administración), el diseño GUI de la pantalla de análisis se ha mantenido sencillo y con fines informativos. En lugar de utilizar gráficos complicados o alertas de error, proporciona claves visuales simples (iconos) para identificar los problemas de seguridad, y proporciona la información requerida para componer estos problemas. La interfaz utiliza una tabla sencilla que enumera los atributos, sus valores correspondientes y los valores recomendados. Los problemas potenciales se identifican mediante los cambios en icono.

Las Herramientas de configuración de seguridad utilizan la configuración compuesta presente en la base de datos al realizar su análisis de seguridad. La configuración compuesta enumera las configuraciones preferentes o recomendadas y es necesaria para realizar las configuraciones y proporcionar la información de configuración recomendada de manera que los problemas potenciales en las configuraciones del sistema actual puedan encontrarse y componerse adecuadamente. El mecanismo de las Herramientas de configuración de seguridad consulta las configuraciones para diversos atributos de seguridad en cada una de las áreas de seguridad y compara los valores con las recomendaciones de la configuración compuesta. Si las configuraciones del sistema coinciden con la configuración, se presume que son correctas. De no ser así, se identifican como problemas potenciales que no requieren investigación. Estos problemas potenciales no se perciben y se muestran en la interfaz del administrador de configuración de seguridad.

De manera predeterminada, la configuración compuesta es la que se utiliza durante la configuración del sistema. Usted puede actualizar la configuración compuesta revisando ediciones, importando configuraciones adicionales o reemplazándolas completamente con una nueva configuración. La información del análisis es recopilada por el mecanismo y almacenada en una tecnología de base de datos ISAM de Microsoft. El uso de la tecnología de base de datos de Microsoft estándar es intencional. Se proporcionará para mecanismos de reporte integrados y capacidades de extremo superior tales como consultas, transacciones y demás. Asimismo, se proporcionará el soporte ODBC.

Además de analizar la configuración actual del sistema, la interfaz del administrador de configuración de seguridad le permite realizar cambios

---

interactivos de dos tipos: puede cambiar la configuración del sistema o puede cambiar la configuración almacenada.

- **El cambio de la configuración del sistema** incluye la actualización de las configuraciones del sistema de manera que coincidan con aquéllas recomendadas con la configuración compuesta almacenada en la base de datos. Al seleccionar la opción **Configurar** se vuelven a aplicar todas las configuraciones especificadas en la configuración compuesta almacenada en la base de datos.
- **El cambio de la configuración de seguridad compuesta** incluye la actualización de la configuración almacenada en la base de datos a fin de reflejar una nueva configuración del sistema. Puede utilizar esta opción, para indicarle al conjunto de herramientas que no le informe sobre configuraciones no estándar específicas que haya investigado y considere razonables. De igual forma, puede realizar cambios a las configuraciones almacenadas mediante la importación de archivos de configuración adicionales o reemplazando la configuración asignada actualmente por una nueva..

El Administrador de configuración de seguridad proporcionado con las Herramientas de configuración de seguridad muestran la información de configuración de seguridad del sistema organizada en áreas de seguridad, como se define anteriormente en este documento. En las siguientes secciones se describen las capacidades de análisis relacionadas con cada área.

### **Políticas de cuenta y locales**

Al analizar la seguridad del sistema, las Herramientas de configuración de seguridad consulta todos los atributos de seguridad definidos que recaen en esta área y los guarda en la sección de análisis actual de la base de datos. Posteriormente, puede utilizar el Administrador de configuración para ver esta información.

El Administrador de configuración de seguridad proporciona una vista tabular de información. Para cada atributo, muestra las configuraciones actuales y recomendadas (las configuraciones recomendadas se obtienen de la configuración compuesta en la base de datos). Los atributos que no sean iguales a las configuraciones recomendadas se identifican claramente por los iconos diferentes de manera que puedan ser reconocidos fácilmente y puedan corregir los problemas. Para corregir un problema, puede aceptar la configuración actual, en cuyo caso se modifica el valor de la configuración almacenada, o puede cambiar la configuración del sistema de manera que coincida con la recomendación, en cuyo caso el atributo correspondiente se reconfigura cuando se reconfigura el sistema.

La Figura 15 muestra el Administrador de configuración desplegando la información de políticas de seguridad.

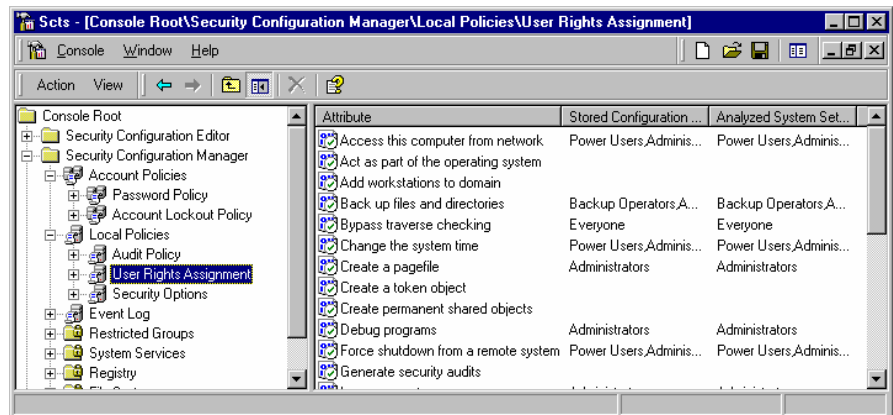


Figura 15. Análisis de las configuraciones de políticas locales y de cuenta

## Administración de grupo restringido

El análisis de grupos restringidos involucra el seguimiento de membresías de grupo, incluyendo membresías recursivas. Los problemas se identifican utilizando iconos diferentes. Para corregir un problema, puede aceptar las configuraciones actuales, en cuyo caso se modifica la configuración almacenada, o puede cambiar la configuración del sistema de manera que coincida con la recomendación, en cuyo caso se cambian las membresías de grupo problemáticas cuando se reconfigura el sistema.

La Figura 16 ilustra el Administrador de configuración mostrando la información de administración de grupo restringido.

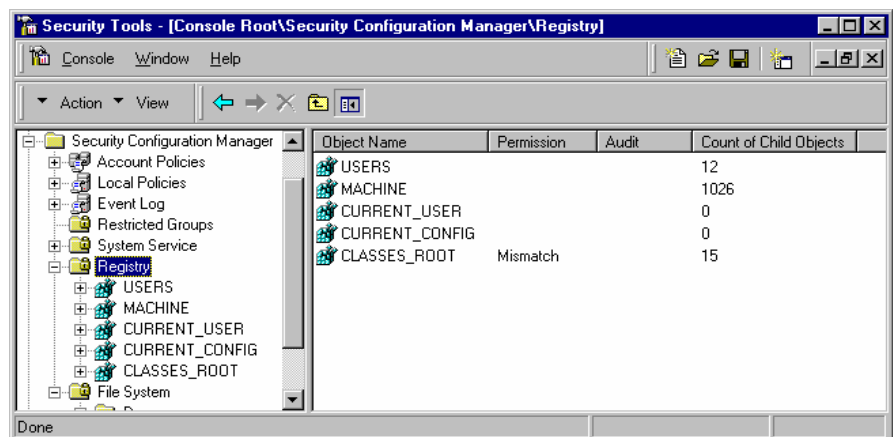


Figura 16. Análisis de la membresía del grupo restringido

## Seguridad de registro

El mecanismo en las Herramientas de configuración de seguridad utiliza las rutas para las claves de registro y sus descriptores de seguridad (las rutas y descriptores se almacenan en formato SDDL en la configuración compuesta) como base para su



análisis. El mecanismo analiza la información de registro y proporciona información sobre la similitud de los descriptores de seguridad una vez que han sido definidos. Nuevamente, el mecanismo utiliza ACEPTAR, Investigar y No configurado para categorizar la información del descriptor de seguridad en el árbol actual, como se compara con la configuración almacenada.

La Figura 17 ilustra el Administrador de configuración mostrando la información de seguridad de registro.

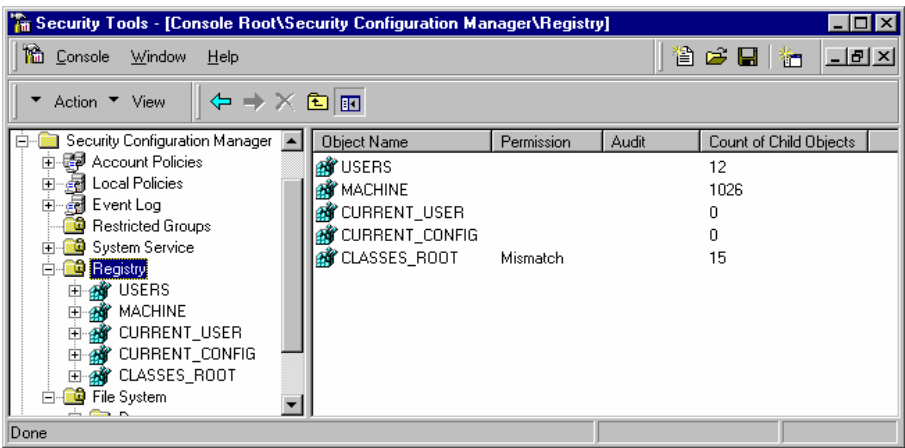


Figura 17. Análisis de las configuraciones de seguridad de registro

**Seguridad del sistema de archivo**

La seguridad del sistema de archivo local es el tercer objeto del árbol soportado dentro de las Herramientas de configuración de seguridad. El mecanismo de análisis de las Herramientas de configuración de seguridad utiliza la lista de las rutas de archivo o directorio totalmente calificadas así como sus descriptores de seguridad almacenados en la configuración asignada como base para su análisis. El mecanismo analiza la información y determina la similitud de los descriptores de seguridad real con los ya definidos. El mecanismo de análisis utiliza nuevamente ACEPTAR, Investigar, No configurado para categorizar la información del descriptor de seguridad en el árbol real, comparado con el de la configuración.

La Figura 18 ilustra el Visualizador de configuración mostrando la información de seguridad del sistema de archivo local.

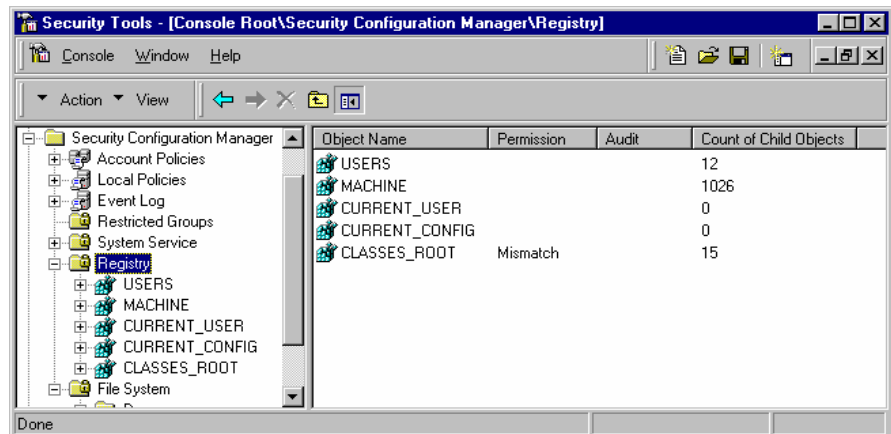


Figura 18. Análisis de las configuraciones de seguridad del sistema de archivo

## Seguridad de servicios del sistema

Las Herramientas de configuración de seguridad recopilan la información general de seguridad en todos los servicios configurados para ejecutarse en el sistema. La información general incluye las configuraciones de inicio y los descriptores de seguridad. El grupo de herramientas detecta los problemas, como las no coincidencias o archivos no especificados en la configuración, y los reporta.

El análisis de las configuraciones de seguridad específicas de servicio para cada servicio también se proporciona a través de la arquitectura anexa a la seguridad de servicio para las Herramientas de configuración de seguridad, según se analiza en la sección de configuración anterior. En este caso, las Herramientas de configuración de seguridad solicitan las interfaces definidas para permitir que el anexo recopile los datos necesarios y los almacene en el lugar específico en la base de datos. El Administrador de configuración llama posteriormente a la interfaz de análisis del *snap-in* de extensión para mostrar la información, así como para aceptar las acciones del usuario para corregir los problemas. (Ver Figura 19.)

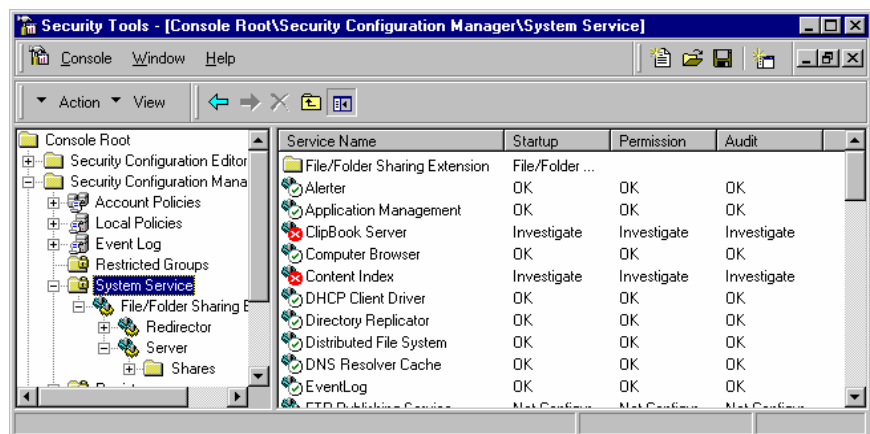


Figura 19. Análisis de las configuraciones de servicio del sistema

Como ya se indicó anteriormente, Microsoft enviará un anexo de configuración de seguridad para el Servicio de distribución de archivos CIFS en la versión inicial de las Herramientas de configuración de seguridad. El anexo de distribución de archivos le permite configurar y analizar la siguiente información de seguridad sobre el servicio:

- **Políticas**—Habilitación o inhabilitación de las firmas de paquete en los paquetes de red tanto para servidor como para el cliente, acceso anónimo compartir archivos, conductos y demás.
- **Compartir**—La seguridad en las diversas divisiones compartidas que se han hecho disponibles desde la computadora.

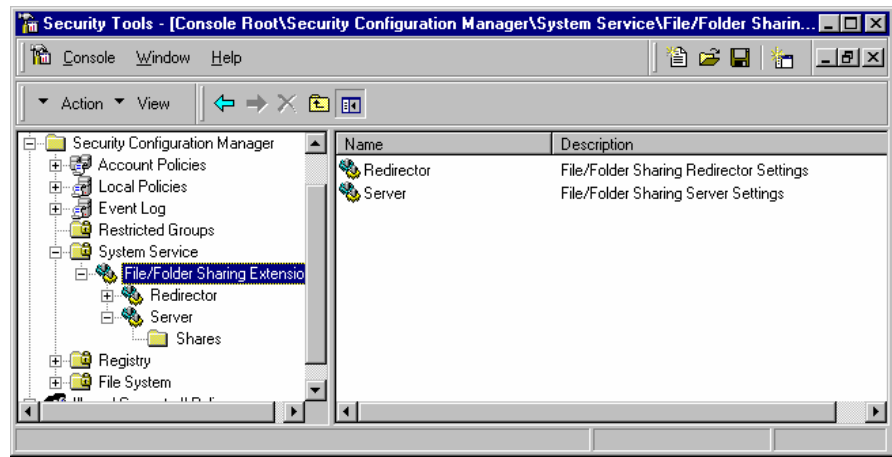


Figura 20. Análisis de las configuraciones de distribución de archivos

La interfaz que se utiliza para ampliar el Grupo de herramientas se documenta en el Apéndice A, Implementación de anexos de seguridad. Esta interfaz permite a los proveedores independientes de software crear anexos de seguridad para otros servicios.

---

## INTEGRACION DE LAS POLITICAS DE GRUPO

### Configuración de seguridad en los objetos de políticas de grupo

Como ya se analizó anteriormente, otra parte importante de las Herramientas de configuración de seguridad es su integración con la infraestructura de Política de grupo desarrollada para la iniciativa de Administración Microsoft Windows. El objetivo de esta iniciativa, es permitir a los administradores configurar un gran número de clientes mediante el establecimiento de políticas en el servidor y hacer que se propaguen de manera automática y se apliquen a los clientes. La Política de grupo utiliza Active Directory para permitir que las computadoras de usuarios se agrupen con base en el alcance. El alcance se define en uno de los niveles siguientes: sitios, dominio o unidades organizacionales. El soporte avanzado permite la agrupación de subgrupos dentro de una unidad organizacional. La política de grupo limitada también se puede definir de manera local en computadoras individuales donde se define como la política de computadora local. Para más información sobre esta infraestructura, consulte los documentos estratégicos de Administración Windows y Política de grupo en <http://www.microsoft.com>.

Una de las políticas que puede ser configurada y propagada es la política de seguridad. La política de seguridad, se define como un archivo de configuración de seguridad que está almacenado como parte del objeto de política de grupo. Este archivo de configuración de seguridad es idéntico al que se utiliza en cualquier otra parte del conjunto de herramientas. Por lo tanto, las áreas que abarca la parte de seguridad de la política de grupo incluyen:

- Políticas de cuenta
- Políticas locales
- Grupos restringidos
- Servicios del sistema
- Registro
- Sistema de archivo
- Objetos de directorio

La Figura 21 muestra el esquema de la parte de seguridad del objeto de políticas de grupo. Haga clic en **Configuraciones de computadora** y después en **Configuraciones de seguridad** para llegar a la parte de seguridad del objeto de políticas de grupo, que se ve idéntico al esquema de configuración en el Editor de configuración de seguridad y al Administrador de configuración de seguridad. Existe un soporte integrado entre las herramientas que permite cortar y pegar entre los mismos nodos, así como la capacidad de exportar la configuración de uno e importarla a otro.

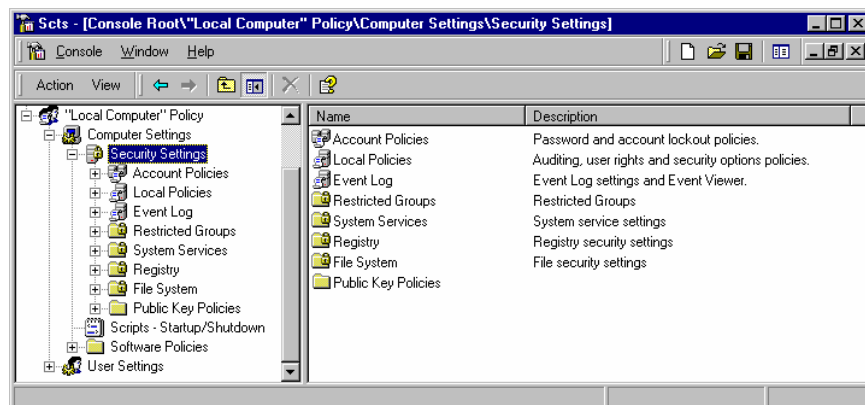


Figura 21. Esquema de seguridad del objeto de política de grupo.

## Políticas de seguridad adicionales

La parte de seguridad de la Política de grupo soporta políticas de seguridad adicionales que se utilizan en la empresa basadas en Active Directory. Estas políticas también se exponen bajo el nodo Configuraciones de Seguridad en cualquier objeto de la política de grupo (local o basadas en Active Directory). Estas incluyen:

- **Política de seguridad de protocolo Internet**—Esta política indica el objeto de política IPsec en Active Directory. Los objetos de la política IPsec definen los requerimientos de encriptación y firma para los paquetes IP entre una computadora de origen y diversas computadoras de destino. Para más información sobre IPsec, consulte los documentos estratégicos relevantes en <http://www.microsoft.com>.
- **Políticas de clave pública**—Estas políticas incluyen diversas subpolíticas que son utilizadas por las tecnologías basadas en la Infraestructura de clave pública incluida en Windows 2000. Estas subpolíticas incluyen:
  - **Agentes de recuperación de datos encriptados**—Esta política incluye un grupo de certificados X509 versión 3. La persona que cuente con la clave privada asociada con cada certificado tiene la capacidad de recuperar cualquier archivo encriptado utilizando el sistema de encriptación de archivos en cualquier computadora que se encuentre bajo la influencia de esta política. Para obtener más información sobre esta política y el sistema de encriptación de archivos, consulte el documento estratégico en el sistema de encriptación de archivos en <http://www.microsoft.com>.
  - **Certificados de raíz**—Esta política incluye un grupo de certificados autofirmados X509 versión 3 que pertenecen a varias autoridades de certificados. Cualquier certificado identificado como la raíz en un enfoque determinado de influencia (dominio, OU o local) representa una gran responsabilidad en la autoridad de dicho certificado. Todas las validaciones de certificados en certificados de entidad final en PKI deben

---

terminar en un certificado de raíz identificado aquí para el certificado de entidad final que será considerado como válido.

- **Listas de certificados**—Esta política incluye un grupo de certificados no autofirmados X509 versión 3 que pertenece a las autoridades de certificación. Estas autoridades de certificación se denominan en ocasiones *autoridades subordinadas*. Las listas de certificados incluyen información adicional sobre los propósitos que tiene CA y demás. Esto permite que los administradores limiten el enfoque de las diferentes autoridades de certificación en términos del tipo de certificados válidos que emiten. Para obtener más información sobre las listas de certificados y cómo pueden ser utilizadas, ver la documentación PKI en <http://www.microsoft.com>.

---

## USO DE LAS HERRAMIENTAS

### Para utilizar el Editor de configuración de seguridad

Para utilizar SCE, debe cargar primero el *snap-in* en la consola MMC.

#### Para cargar el SCE en la consola MMC

1. Inicie MMC. En el menú de Inicio Haga clic en **Ejecutar**. En la pantalla Abrir, escriba  
**Mmc.exe**
2. Haga clic en **Consola** y después Haga clic en **Agregar/eliminar Snap-ins**.
3. Haga clic en **Agregar**.
4. Seleccione **Editor de configuración de seguridad** de la lista y haga clic en **ACEPTAR**.
5. Haga clic en el señalador **Extensiones**. La lista desplegable deberá decir **Editor de configuración de seguridad**.
6. Seleccione todas las extensiones enumeradas.
7. Regrese a la lista desplegable para ver si aparece algún *snap-in* nuevo. De ser así, selecciónelo y agréguelo a sus extensiones.
8. Repita el paso anterior hasta que se hayan agregado todas las extensiones. Esto crea una consola MMC con SCE completamente cargado.
9. Haga clic en **Consola** y después Haga clic en **Guardar como** para guardar la consola para uso futuro.

#### Ejemplo 1: Para personalizar las configuraciones redefinidas

1. Inicie la consola SCE guardada.
2. Abra el nodo SCE. Deberá ver la ruta de búsqueda predeterminada para las configuraciones que se encuentran bajo su directorio del sistema.
3. Abra el nodo y verá la lista de configuraciones predeterminadas. La descripción asociada con cada configuración describe lo que puede hacer con una configuración particular.
4. Haga clic en **Seguridad básica**.
5. Haga clic en **Políticas locales** y después haga clic en **Opciones de seguridad**.
6. Haga clic en **Renombrar cuenta del administrador**.
7. No seleccione la caja para permitir la configuración.
8. Introduzca un nombre genérico como *"nobody"*
9. Repita el proceso con **Renombrar nombre de cuenta de visitante a**. Puede personalizar cualquier otro aspecto de la configuración de esta manera.
10. Haga clic con el botón derecho en el nodo **Seguridad base** y seleccione **Guardar como**.

- 
11. En la caja de diálogo **Abrir archivo**, dé el nombre de la ruta donde desea que se guarde esta configuración.

### **Ejemplo 2: Para crear una nueva configuración**

1. Inicie la consola SCE guardada.
2. Haga clic con el botón derecho en el nodo SCE, y haga clic en **Agregar ruta de búsqueda de configuración**.
3. Explore el directorio donde desea guardar su nueva configuración.
4. Haga clic en **ACEPTAR**.
5. Se agrega un nodo a la ruta seleccionada bajo el nodo SCE.
6. Haga clic con el botón derecho en el nodo, y seleccione **Nueva configuración**.
7. Un nuevo nodo que representa la configuración aparece bajo ese nodo. Esta configuración está completamente en blanco. Puede optar por hacer cualquiera de las tres cosas para llenar esta configuración:
  - **Importar configuraciones existentes**—Haga clic con el botón derecho en la nueva configuración y seleccione **Importar configuración**. Busque la configuración que desea importar y Haga clic en **ACEPTAR**.
  - **Personalizar valores de manera individual**—Navegue a través de los elementos individuales y establezca los valores, igual que en el ejemplo anterior.
  - **Copiar y pegar áreas desde las configuraciones existentes**—Vaya a la configuración que desee copiar. Seleccione el área relevante (políticas de cuenta, políticas locales, etc.). Haga clic con el botón derecho en el área y seleccione **Copiar**. Después vaya a la misma área en la nueva configuración, haga clic con el botón derecho y seleccione **Pegar**.

### **Para utilizar el administrador de configuración de seguridad**

Para utilizar el SCM, debe de cargar primero el *snap-in* en una consola MMC.

#### **Para cargar SCE en la consola MMC**

1. Inicie MMC. Desde menú Iniciar, Haga clic en **Ejecutar**. En la pantalla Abrir texto, escriba  
**Mmc.exe**
2. Haga clic en **Consola**, después haga clic en **Agregar/eliminar Snap-ins**.
3. Haga clic en **Agregar**.
4. Seleccione el **Administrador de configuración de seguridad** de la lista y Haga clic en **ACEPTAR**.
5. Haga clic en el señalador **Extensiones**. La lista desplegable deberá decir **Administrador de configuración de seguridad**.



- 
6. Seleccione todas las extensiones enumeradas.
  7. Regrese a la lista desplegable para ver si aparece algún *snap-in* nuevo. De ser así, selecciónelo una vez y agregue sus extensiones.
  8. Repita el paso anterior hasta que todas las extensiones se hayan agregado. Esto crea una consola MMC con SCM completamente cargado.
  9. Haga clic en **Consola** y después haga clic en **Guardar como** para guardar la consola para uso futuro.

#### **Ejemplo 1: Para aplicar una configuración predefinida en la computadora**

1. Inicie la consola SCM guardada. De manera predeterminada, el enfoque es un grupo en la base de datos de la política de computadora local.
2. Haga clic con el botón derecho en el nodo **SCM** y después haga clic en **Importar configuración**.
3. Utilice la pantalla **Abrir archivo** para encontrar la configuración que desea aplicar.
4. Asegúrese de que la caja de verificación para sobrescribir la configuración existente, no esté seleccionada ya que ésta no se sobrescribe a menos de que se especifique en la configuración importada.
5. Haga clic en **ACEPTAR**. Esto hace que la configuración seleccionada forme parte de la configuración almacenada en la política de computadora local.
6. Seleccione **Configurar ahora** del menú **Contexto** SCM.

#### **Ejemplo 2: Para asegurarse de que el sistema sea consistente con la base de datos de la política de computadora local**

1. Inicie la consola SCM guardada. De manera predeterminada, se enfoca en la política de base de datos de la computadora local.
2. Haga clic con el botón derecho en el nodo **SCM** y haga clic en **Analizar**.
3. Proporcione la ruta de archivo de registro de error y haga clic en **ACEPTAR**.
4. El diálogo en proceso que muestra el progreso continuo del análisis aparece en este momento.
5. Si existen errores Notepad se inicia con el archivo de registro para mostrar cualquier error.

Ahora puede navegar a través de las diversas áreas, por ejemplo, políticas de cuenta, políticas locales y demás y encontrar cualquier discrepancia que pueda existir. En un caso típico, no existe ninguna.

#### **Ejemplo 3: Para exportar la configuración de sistema actual en una computadora y replicarlo en otro sistema**

1. Inicie la consola SCM guardada en la computadora seleccionada. De manera predeterminada se enfoca en la base de datos de la política de computadora

---

local.

2. Haga clic con el botón derecho en el nodo **SCM** y haga clic en **Exportar configuración**.
3. Proporcione la ruta del archivo de configuración donde deberá escribirse la configuración. Esto puede ser una ruta de red para alguna ubicación distribuida. La configuración se escribe ahí cuando se lleva a cabo.
4. Para aplicar las diferentes computadoras, tiene diversas opciones posibles:
  - Si es únicamente un par de sistemas y desea hacerlo manualmente, utilice el Ejemplo 1 anterior para aplicar esa configuración en cada una de las computadoras.
  - Si es un gran número de computadoras y usted se encuentra en infraestructura basada en Active Directory, puede utilizar la extensión Editor de políticas de grupo, importar la configuración a un objeto de políticas de grupo (GPO) y hacer que se propague a un gran número de sistemas.
  - Si se trata de un gran número de computadoras y no tiene una infraestructura basada en Active Directory, puede utilizar servidor de la administración de sistemas para hacer que la configuración se aplique a diferentes computadoras, utilizando el *script* de comando que se denomina Secedit.exe.

#### **Ejemplo 4: Para analizar un sistema comparándolo con las configuraciones proporcionadas por una fuente externa**

1. Inicie la consola SCM guardada en la computadora
2. Haga clic con el botón derecho en **Nueva base de datos** y seleccione una nueva base de datos de seguridad.
3. Haga clic con el botón derecho en **Importar configuración** y proporcione uno de los archivos de configuración.
4. Repita el paso anterior para cada configuración que deberá incluirse.
5. Haga clic con el botón derecho en **Analizar**. Proporcione la **ruta del archivo de registro de error** y Haga clic en **ACEPTAR**.
6. El diálogo en proceso muestra lo que está ocurriendo. Una vez que se ha completado, puede navegar en diversas áreas y buscar discrepancias. Estas se encuentran claramente identificadas por los iconos X.

#### **Para utilizar la extensión de configuraciones de seguridad en el editor de políticas de grupo**

##### **Ejemplo 1: Para trabajar con la política de computadora local**

1. Haga clic con el botón derecho en el icono **Mi PC** en el escritorio.
2. Haga clic en **Administrar**. Esto inicia el *snap-in* de administración de

---

computadora.

3. En el menú **Herramientas del sistema**, seleccione **Política de computadora local**, señale **Configuraciones de computadora**, después seleccione **Configuraciones de seguridad**. Deberá ver el nodo de configuración de seguridad. Puede editar varias políticas, como contraseña, bloqueo, auditoría y derechos de usuario. Estos cambios se efectúan inmediatamente después de haber completado todos los cambios y cerrado el *snap-in*.

**Nota:** Si se encuentra en una infraestructura de política de grupo basada en un dominio, cualquiera de los cambios que usted realice se sobrescribirán mediante los cambios de Active Directory.

### **Ejemplo 2: Para definir las políticas de cuenta para el dominio y todas las computadoras en ese dominio**

1. Inicie **Administrador Active Directory**
2. En el menú Inicio, señale **Programas**, después señale **Herramientas administrativas** y después **Administrador Active Directory**.
3. Haga clic con el botón derecho en el nodo **Dominio**, haga clic en **Tareas** y después haga clic en **Administrar política de grupo**.
4. Aparece la caja de diálogo de asignación **Política de grupo**. Le muestra todos los GPO asignados existentes.
5. Haga clic en el GPO **Política de cuenta de dominio predeterminada**, y después Haga clic en **Editar**.
6. Esto hace que aparezca el Editor de política de grupo enfocado en la política seleccionada.
7. Haga clic en el nodo **Política**. En el menú **Configuraciones de computadora**, señale **Configuraciones de seguridad** y después haga clic en **Políticas de cuenta**.
8. Ahora puede abrir cada nodo bajo las políticas de cuenta.
  - Política de contraseña para configurar las opciones de política de contraseña para el dominio.
  - Política de bloqueo de cuenta para configurar las restricciones de bloqueo de cuenta.
  - Política Kerberos para configurar políticas relacionadas con Kerberos para el dominio.

### **Ejemplo 3: Para inhabilitar RAS, DHCP y DNS en todas las computadoras en las que tienen dominios excepto las específicas**

Existen dos partes para configurar esta política. Primero debería establecer una política de nivel superior para inhabilitar estos servicios en todas las computadoras del dominio. En segundo lugar, debería mover las computadoras específicas que ejecutan RAS, DHCP y DNS en unidades organizacionales separadas y configurar la política para habilitar el servicio correspondiente.

---

### Parte 1: Para establecer una política de nivel superior genérico

1. Inicie el Administrador Active Directory. En el menú **Inicio**, señale **Archivos de programa**, señale **Herramientas administrativas** y después haga clic en el **Administrador Active Directory**.
2. Haga clic con el botón derecho en el nodo de **Dominio**, haga clic en **Tareas** y después haga clic en **Administrar política de grupo**. Aparece la pantalla de asignación de Política de grupo. Muestra todos los GPO que están asignados.
3. Haga clic en **Agregar**. Esto inicia la pantalla de asignación GPO.
4. Haga clic en la opción **Nueva política de grupo** y reemplace el nombre proporcionado con el nombre *Inhabilitar servicios de red*.
5. Esto crea el GPO e inicia el GPE enfocado en ese GPO.
6. En el menú **Configuraciones de computadora**, señale **Configuraciones de seguridad** y después haga clic en **Servicios del sistema**.
7. Seleccione cada uno de estos tres servicios y haga doble clic para iniciar la caja de diálogo de configuración.
8. Establezca el Modo de inicio de servicio en **Inhabilitar** y haga clic en **ACEPTAR**.
9. Cierre el *snap-in*. Esto configura la política necesaria.

### Parte 2: Para trasladar las computadoras RAS, DHCP y DNS en unidades organizacionales y configurar la política de manera que habilite el servicio correspondiente

1. Inicie el administrador Active Directory. En el menú **Inicio**, señale **Archivos de programa**, señale **Herramientas administrativas**, después haga clic en **Administrador Active Directory**.
2. Navegue a la ubicación donde desea crear la unidad organizacional para colocar las computadoras que ejecutan en servidores RAS. Haga clic en **New**, y después haga clic en **Unidad organizacional** y escriba el siguiente nombre:  

Remote Access Server
3. Seleccione **OU RAS**. Haga clic con el botón derecho en **Tareas** y después haga clic en **Administrar política de grupo**. Aparece la caja de diálogo de asignación de política de grupo.
4. Haga clic en **Agregar**. Esto inicia la caja de diálogo de asignación GPO.
5. Seleccione la opción **Nueva política de grupo** e inserte **Habilitar RAS**. Esto crea el GPO y solicita el GPE en ese GPO.
6. En el menú **Configuraciones de computadora**, haga clic en **Configuraciones de seguridad** y después haga clic en **Servicios del sistema**.
7. Seleccione el **Servicio RAS** y después haga doble clic para iniciar la caja de

---

diálogo de configuración.

8. Establezca el modo de inicio de servicio a **Habilitado** y después haga clic en **ACEPTAR**.
9. Cierre el *snap-in*. Esto configura la política necesaria para los servidores RAS.
10. Repita los pasos anteriores para los servidores DHCP y DNS.

---

## **PARA MAYORES INFORMES**

Para obtener la información más reciente sobre Windows NT Server y Windows 2000, visite el sitio Web en <http://www.microsoft.com/ntserver> o el foro Windows NT Server en Microsoft Network (GO WORD: MSNTS).

---

## APENDICE A. IMPLEMENTACION DE ANEXOS DE SEGURIDAD

Este apéndice describe los procedimientos para la creación e implementación de los anexos para las Herramientas de configuración de seguridad.

### Introducción

La arquitectura de los anexos de seguridad requiere la implementación de las siguientes dos partes:

- Un DLL de mecanismo de anexo que implemente tres interfaces (se describen posteriormente en este apéndice).
- Un *snap-in* de extensión Microsoft Management Console (MMC) que proporcione el editor de configuración y la funcionalidad del administrador que se utiliza para configurar y analizar las configuraciones de seguridad específicas del anexo. Esta extensión puede exponerse como un nodo en uno de los dos lugares posibles en el espacio del nombre Security Configuration Tool Set:
  - Bajo el área de seguridad **Servicios** en Editor de configuración de seguridad y *snap-ins* del Administrador. Esto deberá utilizarse cuando el anexo implemente una configuración o análisis de seguridad específica del servicio.

Las Herramientas de configuración de seguridad manejan las configuraciones de seguridad generales para los servicios individuales de manera directa. Estas configuraciones generales incluyen la política de invocación de servicios (inhabilitado, automático o manual), así como los descriptores de seguridad para cada servicio. Por lo tanto, ningún anexo de configuración de seguridad deberá intentar instalar estas configuraciones. La arquitectura del anexo de seguridad de servicio dentro de Security Configuration Tool Set proporciona una infraestructura para configurar y analizar las configuraciones de seguridad específicas de servicio para los servicios individuales. Por ejemplo, *Spooler* es un servicio Windows NT que define *objetos privados* (en este caso, impresoras) que necesitan ser aseguradas. Además, cuenta con parámetros de configuración que son susceptibles a la seguridad. Para *Spooler*, un anexo de seguridad de servicio debe permitir la configuración y el análisis de las configuraciones de seguridad en objetos de impresora y parámetros susceptibles a la seguridad para este servicio.

- Al mismo nivel que **Servicios** y otras áreas de seguridad. Esto deberá utilizarse cuando el anexo implemente una configuración o análisis de seguridad más general. Por ejemplo, un anexo que rastrea los paquetes de servicios y *hot fixes* aplicados al sistema deberá ser colocado a este nivel, ya que se aplica a todo el sistema.

Las Herramientas de configuración de seguridad proporcionan un grupo de API de soporte de llamada de respuesta que el mecanismo del anexo o *snap-in* de extensión utiliza para consultar o establecer información específica de servicio contenida en la configuración de seguridad y base de datos de análisis.

## Arquitectura

La Figura 1A muestra las partes de la arquitectura *snap-in* donde se ajusta la infraestructura del anexo (*snap-ins* para la extensión de anexos, mecanismos de anexos y la base de datos de inspección).

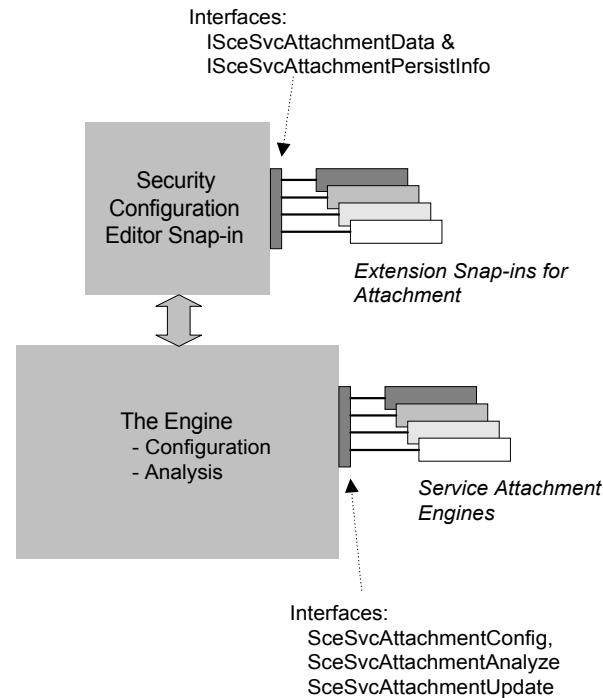


Figura 1A. Snap-in de Security Configuration tool set, mecanismo y arquitectura de extensión

Las Herramientas de configuración de seguridad, las cuales constan de un mecanismo principal y del *snap-in* MMC, proporcionan todo un grupo estructurado para la configuración y análisis de seguridad del sistema para las instalaciones de Windows NT y Windows 2000.

En el marco del anexo, los DLLs del mecanismo de anexo se registran con el mecanismo de configuración de seguridad. Posteriormente, el servicio de mecanismo de configuración de seguridad carga el anexo durante la ejecución. Llama a la interfaz de configuración de los anexos cuando el sistema está configurado, a la interfaz del análisis cuando el sistema es analizado y a la interfaz de actualización cuando los parámetros de la base de datos son modificados por el *snap-in* de extensión.

De manera similar, el *snap-in* de extensión para el anexo debe registrar una extensión *snap-in* las Herramientas de configuración de seguridad. Estos *snap-ins* de las Herramientas de configuración de seguridad cargan los *snap-ins* de extensión como un nodo bajo el área de seguridad de Servicios o al mismo nivel que el área de servicio basándose en la manera en que se registra la extensión tanto en las herramientas de edición como en las del administrador. Si se está escribiendo un



---

*snap-in* de extensión, debe permitir que la documentación del escritor de extensión MMC implemente un *snap-in* de extensión completo. Además, debe implementar la interfaz de modelo de objeto de componentes (COM) que se describe a continuación a fin de comunicarse con los *snap-ins* del Editor o Administrador de configuración de seguridad.

### Creación de un DLL de mecanismo de anexo

La creación de un anexo involucra la implementación de tres interfaces así como la instalación y registro del anexo con Security Configuration Tool Set. Este carga el anexo, después solicita estas interfaces, basado en operaciones invocadas por el usuario.

Antes de describir qué interfaces necesitan implementarse y cómo hacerlo, es importante definir varias estructuras de datos y APIs soportadas con Security Configuration Tool Set.

#### Estructura de datos

Observe que las estructuras de datos descritas en este documento se declaran en el archivo de encabezado Scesvc.h incluido en Microsoft Platform SDK.

- Códigos de estado SCE—Diversos códigos de estado de Security Configuration Tool Set devueltos por las funciones de ayuda y esperados a partir de las interfaces de los archivos adjuntos.

```
typedef DWORD          SCESTATUS;

#define SCESTATUS_SUCCESS          0L
#define SCESTATUS_INVALID_PARAMETER 1L
#define SCESTATUS_RECORD_NOT_FOUND 2L
#define SCESTATUS_INVALID_DATA    3L
#define SCESTATUS_OBJECT_EXIST    4L
#define SCESTATUS_BUFFER_TOO_SMALL 5L
#define SCESTATUS_PROFILE_NOT_FOUND 6L
#define SCESTATUS_BAD_FORMAT      7L
#define SCESTATUS_NOT_ENOUGH_RESOURCE 8L
#define SCESTATUS_ACCESS_DENIED   9L
#define SCESTATUS_CANT_DELETE    10L
#define SCESTATUS_PREFIX_OVERFLOW 11L
#define SCESTATUS_OTHER_ERROR    12L
#define SCESTATUS_ALREADY_RUNNING 13L
#define SCESTATUS_SERVICE_NOT_SUPPORT 14L
```

- Manejos SCE—Manejos *opaque* proporcionados por Security Configuration Tool Set para las interfaces de anexo para soportar las funciones de llamada de respuesta.

```
typedef PVOID SCE_HANDLE;
typedef ULONG SCE_ENUMERATION_CONTEXT, *PSCE_ENUMERATION_CONTEXT;
typedef struct _SCESVC_CALLBACK_INFO_ {

    SCE_HANDLE      sceHandle;
    PFSCE_QUERY_INFO pfQueryInfo;
    PFSCE_SET_INFO   pfSetInfo;
    PFSCE_FREE_INFO  pfFreeInfo;
    PFSCE_LOG_INFO   pfLogInfo;

} SCESVC_CALLBACK_INFO, *PSCESVC_CALLBACK_INFO;
```

- Información de configuración de servicio SCE—Estructura e información que va a ser utilizada por las interfaces del anexo cuando se consulte o configure la información de configuración a la base de datos o configuración a través de las interfaces de llamada de respuesta soportadas.

```
typedef enum _SCESVC_INFO_TYPE {
    SceSvcConfigurationInfo,
    SceSvcAnalysisInfo,
    SceSvcInternalUse // DO NOT USE.
} SCESVC_INFO_TYPE;

typedef struct _SCESVC_CONFIGURATION_LINE_ {
    LPTSTR Key;
    LPTSTR Value;
    DWORD ValueLen; // number of bytes
} SCESVC_CONFIGURATION_LINE, *PSCESVC_CONFIGURATION_LINE;

typedef struct _SCESVC_CONFIGURATION_INFO_ {
    DWORD Count;
    PSCESVC_CONFIGURATION_LINE Lines;
} SCESVC_CONFIGURATION_INFO, *PSCESVC_CONFIGURATION_INFO;
```

- Información de análisis de servicio SCE—Estructura de la información que va a ser utilizada por las interfaces del anexo al consultar o establecer la información de análisis para la base de datos a través de las interfaces de llamada de respuesta de soporte.

```
typedef enum _SCESVC_INFO_TYPE {
    SceSvcConfigurationInfo,
    SceSvcAnalysisInfo,
    SceSvcInternalUse // DO NOT USE
} SCESVC_INFO_TYPE;

typedef struct _SCESVC_ANALYSIS_LINE_ {
    LPTSTR Key;
    PBYTE Value;
    DWORD ValueLen; // number of bytes
} SCESVC_ANALYSIS_LINE, *PSCESVC_ANALYSIS_LINE;

typedef struct _SCESVC_ANALYSIS_INFO_ {
    DWORD Count;
    PSCESVC_ANALYSIS_LINE Lines;
} SCESVC_ANALYSIS_INFO, *PSCESVC_ANALYSIS_INFO;
```

---

## Llamadas de respuesta Security Configuration Tool Set y APIs del Helper

Las herramientas de configuración de seguridad proporcionan un grupo de funciones de llamada de respuesta y soporte que deberán utilizar los anexos para leer o escribir información en el archivo de configuración y la base de datos.

Estas funciones son:

- **PFSCE\_QUERY\_INFO**—Esta función de llamada de respuesta permite que el anexo obtenga información de configuración o análisis desde la base de datos para un servicio.
- **PFSCE\_SET\_INFO**—Esta función de llamada de respuesta permite que el anexo establezca la información de configuración o análisis en la base de datos para un servicio determinado.
- **PFSCE\_FREE\_INFO**—Esta función de llamada de respuesta deberá ser utilizada para liberar los buffers asignados por Configuration Tool Set para el anexo.
- **PFSCE\_FREE\_INFO**—Esta función de llamada de respuesta se utiliza para escribir información en el archivo de registro generado durante las diversas operaciones SCTS: configuración, análisis y propagación de política.
- **ConvertSecurityDescriptorToStringSecurityDescriptor**—Esta función toma un descriptor de seguridad Windows NT binario autorrelativo y lo regresa al texto para representarlo. Esto es útil para almacenar los descriptors de seguridad en los archivos de configuración.
- **ConvertStringSecurityDescriptorToSecurityDescriptor**—Esta función toma un texto del descriptor de seguridad que se generó originalmente a través de **ConvertSecurityDescriptorToStringSecurityDescriptor** y regresa un descriptor de seguridad Windows NT binario autorrelativo que lo represente. Esto es útil al leer un descriptor de seguridad textual desde un archivo de configuración y aplicarlo a un objeto en el sistema.

En el archivo de encabezado Scesvc.h se declaran las funciones de llamada de respuesta en Platform SDK y las funciones de soporte se declaran en el archivo de encabezado Sddl.h. Las bibliotecas estáticas para el enlace son Scesvc.lib y Advapi32.lib, disponibles para plataformas x86 y Alpha. Estas funciones se describen con más detalle a continuación.

### PFSCE\_QUERY\_INFO

Esta función de llamada de respuesta permite que el anexo consulte la información de configuración o análisis de la base de datos.

```
typedef
SCESTATUS
(*PFSCE_QUERY_INFO)(
    IN SCE_HANDLE      sceHandle,
    IN SCESVC_INFO_TYPE sceType,
    IN LPTSTR          lpPrefix OPTIONAL,
    IN BOOL             bExact,
    OUT PVOID           *ppvInfo,
    OUT PSCE_ENUMERATION_CONTEXT psceEnumHandle
);
```

### Parámetros

- *sceHandle*—SCE *Opaque* maneja el paso al anexo a través de Security Configuration Tool Set. Esto se utiliza para determinar dónde se almacena la información.
- *sceType*—Debe ser `SCE_SERVICE_CONFIGURATION_INFO` si la información de seguridad se está consultando o `SCE_SERVICE_ANALYSIS_INFO` si la información de análisis está siendo consultada.
- *lpPrefix*—Puede ser NULL. Si es NULL, se regresan todas las claves. Si se proporciona una cadena, la información devuelta contiene todas las claves (y valores correspondientes) con el mismo prefijo que se especificó en la cadena.
- *bExact*—No se utiliza si *lpPrefix* es NULL. Si el parámetro es TRUE, la clave que coincide exactamente con la cadena específica en *lpPrefix* se devuelve. Si este parámetro es FALSE, todas las claves (y sus valores) que tienen el mismo prefijo como se especifica en la cadena en *lpPrefix* se devuelven.
- *ppvInfo*—Indicador a indicador de tipo `SCESVC_CONFIGURATION_INFO` si *sceType* es `SceSvcConfigurationInfo`. De otra forma, deberá ser `SCESVC_ANALYSIS_INFO` si *sceType* es `SceSvcAnalysisInfo`. Security Configuration Tool Set—y no el anexo—asigna el *buffer*, por lo que el indicador debe señalar en NULL.
- *psceEnumHandle*—El manejo que debe ser utilizado en llamadas sucesivas para esta función. La función puede no regresar todas las claves en una sola llamada ya que podría tener un número grande de claves. (El número máximo de claves que se devuelven en una sola llamada es 256.)

### Valores de devolución

`SCESTATUS_SUCCESS` indica éxito. Uno de los siguientes indicadores significan falla:

- `SCESTATUS_INVALID_PARAMETER`
- `SCESTATUS_RECORD_NOT_FOUND`
- `SCESTATUS_BAD_FORMAT`
- `SCESTATUS_OTHER_ERROR`
- `SCESTATUS_NOT_ENOUGH_RESOURCE`

### PFSCE\_SET\_INFO

Esta API de llamada de respuesta permite que el anexo establezca y sobrescriba la información de configuración y análisis almacenada en la base de datos sobre un servicio particular.

```
typedef
SCESTATUS
(*PFSCE_SET_INFO)(
    IN SCE_HANDLE      sceHandle,
    IN SCESVC_INFO_TYPE sceType,
    IN LPTSTR          lpPrefix OPTIONAL,
    IN BOOL             bExact,
    IN PVOID           pvInfo
);
```

### Parámetros

- *SceHandle*—Manejador *Opaque* que Security Configuration Tool Set pasa al anexo. Esto se utiliza para determinar dónde se almacenó la información.
- *SceType*—Esto debe ser SCE\_SERVICE\_CONFIGURATION\_INFO si se ha establecido la información de configuración, o SCE\_SERVICE\_ANALYSIS\_INFO si se ha establecido la información de análisis.
- *lpPrefix*—Esto puede ser NULL. Si es NULL, toda la información de servicios se sobrescribe con la información proporcionada. Si se proporciona una cadena, la información sobrescrita contiene todas las claves (y valores correspondientes) con el mismo prefijo que se especificó en la cadena.
- *bExact*—No se utiliza si *lpPrefix* es NULL. Si este parámetro es VERDADERO, la clave que coincide exactamente con la cadena especificada en *lpPrefix* se sobrescribe. Si este parámetro es FALSE, todas las claves (y sus valores) tienen el mismo prefijo que se especifica en la cadena en *lpPrefix* se sobrescriben.
- *pvInfo*—Esto debe ser un indicador del tipo SCESVC\_CONFIGURATION\_INFO si *sceType* es *sceSvcConfigurationInfo*. De otra manera, debe ser SCESVC\_ANALYSIS\_INFO si *sceType* es *SceSvcAnalysisInfo*.

#### Valores de devolución

SCESTATUS\_SUCCESS indica éxito. Uno de los siguientes valores indican falla:

- SCESTATUS\_INVALID\_PARAMETER
- SCESTATUS\_RECORD\_NOT\_FOUND
- SCESTATUS\_BAD\_FORMAT
- SCESTATUS\_NOT\_ENOUGH\_RESOURCE
- SCESTATUS\_ACCESS\_DENIED
- SCESTATUS\_DATA\_OVERFLOW
- SCESTATUS\_OTHER\_ERROR

#### PFSCE\_FREE\_INFO

El anexo debe llamar esta función para liberar los *buffers* ubicados por Security Configuration Tool Set en las llamadas a **PFSCE\_QUERY\_INFO**.

```
typedef
SCESTATUS
(*PFSCE_FREE_INFO)(
    IN PVOID          pvServiceInfo
);
```

#### Parámetros

*pvServiceInfo* —Indicador para el *buffer* asignado.

#### Valores de retorno

SCESTATUS\_SUCCESS indica éxito.

SCESTATUS\_INVALID\_PARAMETER indica falla.

#### PFSCE\_LOG\_INFO

---

El anexo puede solicitar esta función para que escriba información en el archivo de registro generado cuando las herramientas de configuración de seguridad realizan la configuración, análisis y propagación de política en un sistema.

```
typedef
SCESTATUS
(*PFSCE_LOG_INFO)(
    IN INT ErrLevel,
    IN DWORD Win32rc,
    IN LPTSTR pErrFmt,
    ...
);
```

#### Parámetros

- *ErrLevel*—Especifica el nivel de registro de error al que se debe escribir la información de registro proporcionada para el archivo de registro. Si la operación invocada está en este nivel, se registra la información del anexo, de otra manera, se ignora. Los niveles definidos son:

```
#define SCE_LOG_LEVEL_ALWAYS    0
#define SCE_LOG_LEVEL_ERROR     1
#define SCE_LOG_LEVEL_DETAIL    2
#define SCE_LOG_LEVEL_DEBUG     3
```

- *Win32rc*—El valor de retorno que va a ser escrito en el registro. Este puede ser un valor de error devuelto por alguna API del sistema solicitada por el anexo para realizar la configuración o el análisis.
- *PErrFmt*—La cadena null-terminada que va a ser escrita en el archivo de registro.

---

## ConvertSecurityDescriptorToStringSecurityDescriptor

Esta es la función del *helper* que permite que un anexo se convierta en un descriptor de seguridad autorrelativo en una forma textual que pueda ser almacenada en el archivo de configuración y en la base de datos. Esta función es útil cuando el anexo está configurando la seguridad en un servicio que soporta objetos privados que no tienen descriptores de seguridad.

```
WINADVAPI
BOOL
WINAPI
ConvertSecurityDescriptorToStringSecurityDescriptorA(
    IN PSECURITY_DESCRIPTOR SecurityDescriptor,
    IN DWORD RequestedStringSDRevision,
    IN SECURITY_INFORMATION SecurityInformation,
    OUT LPSTR *StringSecurityDescriptor OPTIONAL,
    OUT PULONG StringSecurityDescriptorLen OPTIONAL
);
WINADVAPI
BOOL
WINAPI
ConvertSecurityDescriptorToStringSecurityDescriptorW(
    IN PSECURITY_DESCRIPTOR SecurityDescriptor,
    IN DWORD RequestedStringSDRevision,
    IN SECURITY_INFORMATION SecurityInformation,
    OUT LPWSTR *StringSecurityDescriptor OPTIONAL,
    OUT PULONG StringSecurityDescriptorLen OPTIONAL
);
```

### Parámetros

- *SecurityDescriptor*—Indicador para el descriptor de seguridad. (Consulte plataforma SDK para las funciones que manipulan los descriptores de seguridad).
- *RequestedStringSDRevision*—Especifica el nivel de revisión para la representación de texto del descriptor de seguridad. Debe ser SDDL\_REVISION.
- *SecurityInformation*—Especifica la parte de información de seguridad del descriptor de seguridad que debe convertirse en forma textual. (Consulte Plataforma SDK para los valores de SECURITY\_INFORMATION.)
- *StringSecurityDescriptor*—Especifica la forma de cadena del descriptor de seguridad devuelta por esta función. El *buffer* es asignado mediante la función y deberá ser liberado utilizando la función **SceSvcFree** cuando ya no es necesario.
- *StringSecurityDescriptorLen*—Indicador al **ULONG** que se llena con la longitud de la cadena.

La cadena para regresar la forma textual es asignada por esta función del *helper*. Debe ser liberada utilizando la función **LocalFree**.

---

### Valores de retorno

SCESTATUS\_SUCCESS indica éxito. Uno de los siguientes indican falla:

- SCESTATUS\_INVALID\_PARAMETER
- SCESTATUS\_NOT\_ENOUGH\_RESOURCE

### ConvertStringSecurityDescriptorToSecurityDescriptor

Esta es una función del *helper* que permite que un anexo vuelva a convertir una forma textual de un descriptor de seguridad (creado anteriormente utilizando **ConvertSecurityDescriptorToStringSecurityDescriptor**) a su forma binaria autorrelativa.

```
WINADVAPI
BOOL
WINAPI
ConvertStringSecurityDescriptorToSecurityDescriptorA(
    IN LPCSTR StringSecurityDescriptor,
    IN DWORD StringSDRevision,
    OUT PSECURITY_DESCRIPTOR *SecurityDescriptor,
    OUT PULONG SecurityDescriptorSize OPTIONAL
);
WINADVAPI
BOOL
WINAPI
ConvertStringSecurityDescriptorToSecurityDescriptorW(
    IN LPCWSTR StringSecurityDescriptor,
    IN DWORD StringSDRevision,
    OUT PSECURITY_DESCRIPTOR *SecurityDescriptor,
    OUT PULONG SecurityDescriptorSize OPTIONAL
);
```

### Parámetros

- *StringSecurityDescriptor*—Especifica la forma de texto del descriptor de seguridad.
- *RequestedStringSDRevision*—Especifica el nivel de revisión para la representación de texto del descriptor de seguridad. Debe ser SDDL\_REVISION.
  - *SecurityDescriptor*—Indicador para un indicador de descriptor de seguridad. Esta función asigna la memoria necesaria para crear el descriptor de seguridad autorrelativo. Debe ser liberado utilizando la función **SceSvcFree** cuando ya no es necesario.
  - *SecurityDescriptorSize*—Especifica el tamaño del escritor de seguridad asignado.

El *buffer* para regresar un descriptor de seguridad es asignado por esta función del *helper*. Debe ser liberado utilizando la función **LocalFree**.

### Valores de retorno

SCESTATUS\_SUCCESS indica éxito. Uno de los siguientes indican falla:

- SCESTATUS\_INVALID\_PARAMETER
- SCESTATUS\_RECORD\_NOT\_FOUND
- SCESTATUS\_NOT\_ENOUGH\_RESOURCE



---

## Interfaces de anexo necesarias

Las tres interfaces que el anexo debe implementar son:

- **SceSvcAttachmentConfig**—El Administrador de seguridad solicita esta interfaz cuando se configura el sistema.
- **SceSvcAttachmentAnalyze**—El Administrador de seguridad solicita esta interfaz cuando se analiza el sistema.
- **SceSvcAttachmentUpdate**—El Administrador de seguridad solicita esta interfaz cuando recibe una petición de actualización de configuración del *snapshot* MMC.

### SceSvcAttachmentConfig

#### Sintaxis

```
typedef
SCESTATUS
(*PF_ConfigAnalyzeService)(
    IN PSCE SVC_CALLBACK_INFO pSceCbInfo
);
```

#### Parámetros

- **PSceCbInfo**—La estructura que pasa al mecanismo del anexo a través de las Herramientas de configuración de seguridad cuando se invoca esta interfaz. Proporciona un manejo de contexto que es utilizado por varias de las funciones de llamada de respuesta. Asimismo, proporciona los indicadores de función para las funciones de llamada de respuesta.

Esta interfaz debe hacer lo siguiente:

- Utilizar la función de soporte Security Configuration Tool Set **PFSCE\_QUERY\_INFO** para consultar la información de configuración.
- Configurar el servicio.

#### Valores de retorno

- **SCESTATUS\_SUCCESS** indica éxito.
- Cualquier otro valor devuelto definido anteriormente.

#### Código de muestra

```
SCESTATUS
WINAPI
SceSvcAttachmentConfig(
    IN PSCE SVC_CALLBACK_INFO pSceCbInfo
)
{
    //
    //variable definitions
    //
    PSCE SVC_CONFIGURATION_INFO pConfigInfo = NULL;
    SCESTATUS retCode;
    SCE_ENUMERATION_CONTEXT EnumContext = 0;

    if ( pSceCbInfo == NULL ||
        pSceCbInfo->sceHandle == NULL ||
        pSceCbInfo->pfQueryInfo == NULL ||
        pSceCbInfo->pfSetInfo == NULL ||
        pSceCbInfo->pfFreeInfo == NULL ) {
```

```

        return(SCESTATUS_INVALID_PARAMETER);
    }

    //
    // now read the information and configure system using it.
    //
    // NOTE: you may decide to read all the information first
    // and then do the configure, it is implementor's choice.
    //

do {

    __try {
        retCode = (*(pSceCbInfo->pfQueryInfo)) (
            pSceCbInfo->sceHandle,
            SceSvcConfigurationInfo,
            NULL,
            FALSE,
            (PVOID *)&pConfigInfo,
            &EnumContext
        );

    } __except (EXCEPTION_EXECUTE_HANDLER) {
        retCode = SCESTATUS_SERVICE_NOT_SUPPORT;
    }

    if(retCode == SCESTATUS_SUCCESS &&
        pConfigInfo != NULL)
    {
        ULONG i;
        //
        // We have some information, let's configure.
        //
        for(i = 0; i < pConfigInfo->Count; i++)
        {
            if(pConfigInfo->Line[i].Key == NULL)
                continue;

            //
            // We have a key that we should process.
            // This will be the core of doing configuration.
            //
            ProcessConfigurationLine(pConfigInfo->Line[i]);
        }

        //
        // free the data we got back.
        //

        __try {
            (*(pSceCbInfo->pfFreeInfo)) ((PVOID)pConfigInfo);
        } __except (EXCEPTION_EXECUTE_HANDLER) {
            //nothing
        }

        PConfigInfo = NULL;
    }
    //
    // handle other return codes, as needed.
    //
} while ( retCode == SCESTATUS_SUCCESS && CountReturned > 0);

//
// if return code is not success, we should set up
// error message appropriately.
//

//

```

---

```
// return the retCode.  
//  
return retCode;  
}
```

---

## SceSvcAttachmentAnalyze

### Sintaxis

```
typedef
SCESTATUS
(*PF_ConfigAnalyzeService)(
    IN PSCE SVC_CALLBACK_INFO pSceCbInfo
);
```

### Parámetros

**PSceCbInfo**—Estructura que pasa al mecanismo de anexo a través de las Herramientas de configuración de seguridad cuando se invoca esta interfaz. Proporciona un manejo de contexto que es utilizado por diversas funciones de llamada de respuesta. Asimismo proporciona los indicadores a las funciones de llamada de respuesta.

Esta interfaz debe hacer lo siguiente:

- Consultar la información de configuración directamente desde el servicio.
- Utilizar **FSCE\_QUERY\_INFO** para consultar la información de configuración.
- Calcular las diferencias de los parámetros con base en el tipo y sintaxis.
- Utilizar **PFSCE\_SET\_INFO** para escribir la información diferencial para la base de datos.

### Valores de retorno

- SCESTATUS\_SUCCESS indica éxito.
- Cualquiera de los valores de error SCESTATUS son aceptados.

### Código de muestra

```
SCESTATUS
WINAPI
SceSvcAttachmentAnalyze(
    IN SCE_HANDLE sceHandle,
        OUT PWSTR *ppszErrorMessage,
        OUT PDWORD pdErrLength
);
{
    //
    // define various local variables.
    //

    if ( pSceCbInfo == NULL ||
        pSceCbInfo->sceHandle == NULL ||
        pSceCbInfo->pfQueryInfo == NULL ||
        pSceCbInfo->pfSetInfo == NULL ||
        pSceCbInfo->pfFreeInfo == NULL ) {

        return(SCESTATUS_INVALID_PARAMETER);
    }

    //
    // now read the base config information, query system
    // setting corresponding to it, compare them
    // and write to the database.
    //
    do {
```

```

__try {
    retCode = (*(pSceCbInfo->pfQueryInfo))(
        pSceCbInfo->sceHandle,
        SceSvcConfigurationInfo,
        NULL,
        FALSE,
        (PVOID *)&pConfigInfo,
        &EnumContext
    );

} __except (EXCEPTION_EXECUTE_HANDLER) {
    retCode = SCESTATUS_SERVICE_NOT_SUPPORT;
}

if(retCode == SCESTATUS_SUCCESS &&
    pConfigInfo != NULL)
{
    ULONG i;
    //
    // we have some information, let's configure.
    //
    for(i = 0; i < pConfigInfo->Count; i++)
    {
        if(pConfigInfo->Line[i].Key == NULL)
            continue;

        //
        // we have a key that we should query.
        // This function is expected to query
        // the system configuration corresponding
        // to the key value.
        //
        QueryConfigurationLine(pConfigInfo->Line[i].Key,
            &SystemValue);

        //
        // now compare the values.
        //
        CompareValue(pConfigInfo->Line[i].Key,
            SystemValue,
            pConfigInfo->Line[i].Value,
            &Result
        );

        //
        // Check if there is something that should
        // be written to analysis part of the
        // database.
        if(Result != NULL)
        {
            //
            // we will overwrite exactly one
            // value.
            // more efficient way to do this
            // would be to accumulate a
            // set of values and commit.
            //

            __try {
                retCode = (*(pSceCbInfo->pfSetInfo))(
                    pSceCbInfo->sceHandle,
                    SceSvcAnalysisInfo,
                    pConfigInfo->Line[i].Key,
                    TRUE,
                    (PVOID)&Result
                );
            }
        }
    }
}

```

```

        } __except
        (EXCEPTION_EXECUTE_HANDLER) {
            retCode =
            SCESTATUS_SERVICE_NOT_SUPPORT;
        }
        if(retCode != SCESTATUS_SUCCESS)
        {
            // if it doesn't get set, we
            // need to do some cleanup
            // here.
        }
    }

    //
    // free the data we got back.
    //
    SceSvcFree((PVOID)pConfigInfo);
    __try {
        (*(pSceCbInfo->pFreeInfo))((PVOID)pConfigInfo);
    } __except (EXCEPTION_EXECUTE_HANDLER) {
    }
    PConfigInfo = NULL;

    //
    // should also free possible buffers SystemValue and
    // Result, up to each attachment
    //

    }
    //
    // handle other return codes, as needed.
    //
} while ( retCode == SCESTATUS_SUCCESS && pConfigInfo != NULL);

//
// if return code is not success, we should set up
// error message appropriately, if error buffer is not NULL
//

//
// return the retCode.
//
return retCode;
}

```

### SceSvcAttachmentUpdate

Las herramientas de configuración de seguridad (o administrador), llama a esta interfaz cuando el *snap-in* de Editor de configuración de seguridad (o Manager) pasa cambios específicos del servicio a las programaciones de configuración almacenadas en la base de datos.

### Sintaxis

```

typedef
SCESTATUS
(*PF_UpdateService)(
    IN PSCE SVC_CALLBACK_INFO psceCbInfo,
    IN PSCE SVC_CONFIGURATION_INFO ServiceInfo
);

```

### Parámetros

- **PSceCbInfo**—Estructura que pasa al mecanismo de anexo a través de las Herramientas de configuración de seguridad cuando se invoca esta interfaz.

---

Proporciona el manejo de contexto que se va a utilizar en las diversas funciones de llamada de respuesta. Asimismo, proporciona los indicadores para las funciones de llamada de respuesta.

- **ServiceInfo**—Especifica la información de configuración actualizada, la cual se basa en las ediciones del usuario y es proporcionada por el *snap-in* de extensión del anexo. (Consulte la explicación de la estructura de datos **SCESVC\_CONFIGURATION\_INFO** en la sección de estructuras de datos),

Esta interfaz del anexo debe hacer lo siguiente:

- Utilizar **PFSCE\_QUERY\_INFO** para consultar la información base (información de configuración) almacenada en la base de datos.
- Utilizar **PFSCE\_SET\_INFO** para consultar el último grupo de diferencias (información de análisis) almacenadas en la base de datos.
- Utilizar *ServiceInfo* proporcionada para calcular la nueva información de configuración base.
- Utilizar *ServiceInfo* proporcionada y las últimas diferencias almacenadas para calcular la nueva información diferencial.
- Utilizar **PFSCE\_SET\_INFO** para escribir la nueva información de configuración base en la base de datos.
- Utilizar **PFSCE\_SET\_INFO** para escribir la nueva información diferencial en la base de datos.

#### Valores de retorno

- **SCESTATUS\_SUCCESS** indica éxito.
- Cualquiera de los valores de error **SCESTATUS** son aceptados.

#### Código de muestra

```
SCESTATUS
WINAPI
SceSvcAttachmentUpdate(
    IN SCE_HANDLE sceHandle,
    IN SCESVC_CONFIGURATION_INFO *ServiceInfo
);

{

if ( pSceCbInfo == NULL ||
    pSceCbInfo->sceHandle == NULL ||
    pSceCbInfo->pfQueryInfo == NULL ||
    pSceCbInfo->pfSetInfo == NULL ||
    pSceCbInfo->pfFreeInfo == NULL ||
    ServiceInfo == NULL ) {

    return(SCESTATUS_INVALID_PARAMETER);
}
//
// process each line of the passed information.
//
for(i=0; i < ServiceInfo->Count; i++)
{
    EnumContext = 0;

    __try {
        retCode = (*(pSceCbInfo->pfQueryInfo))(
            pSceCbInfo->sceHandle,
            SceSvcConfigurationInfo,
            ServiceInfo->Lines[i].key,
```

---

```

        TRUE,
        (PVOID *)&pConfigInfo,
        &EnumContext
    );
    } __except (EXCEPTION_EXECUTE_HANDLER) {
        retCode = SCESTATUS_SERVICE_NOT_SUPPORT;
    }

    if(retCode != SCESTATUS_SUCCESS &&
retCode != SCESTATUS_RECORD_NOT_FOUND)
{
        //
        // handle the error here.
        //
        break;
    }

    //
    // if the value specified is NULL, deletion
    // of the key is requested.
    //
    if(ServiceInfo->Line[i].value == NULL)
    {
        if(retCode == SCESTATUS_SUCCESS)
        {
            //
            // Lets ensure that analysis is ok.
            //
            EnumContext = 0;

            __try {

```



```

        retCode = (*(pSceCbInfo->pfQueryInfo))(
            pSceCbInfo->sceHandle,
            SceSvcAnalysisInfo,
            ServiceInfo->Lines[i].Key,
            TRUE,
            (PVOID *)&pAnalInfo,
            &EnumContext
        );
    } __except (EXCEPTION_EXECUTE_HANDLER) {
        retCode = SCESTATUS_SERVICE_NOT_SUPPORT;
    }
    if(retCode == SCESTATUS_RECORD_NOT_FOUND)
    {
        //
        // Analysis Info was not found,
        // this means it was matched during
        // actual analysis. Now, we are
        // deleting the configuration info,
        // hence current configuration is
        // what analysis should save.
        //
        UpdateInfo->Count = 1
        UpdateInfo->Line = &UpdateLine;
        UpdateLine.Key = pConfigInfo->
>Line[0].Key;
        UpdateLine.Value =
        (PBYTE)pConfigInfo->Line[0].Value;

        __try {
            retCode = (*(pSceCbInfo->
>pfSetInfo))(
                pSceCbInfo->sceHandle,
                SceSvcAnalysisInfo,
                NULL,
                TRUE,
                (PVOID)&UpdateInfo
            );

            } __except
            (EXCEPTION_EXECUTE_HANDLER) {
                retCode =
                SCESTATUS_SERVICE_NOT_SUPPORT;
            }
            if(retCode != SCESTATUS_SUCCESS)
            {
                //
                // cleanup, something
                // failed.
                //
            }
        }
        elseif (retCode == SCESTATUS_SUCCESS)
        {
            //
            // simply delete the configuration.
            // we already have analysis info in
            // place.
        }
        else
        {
            //
            // handle other error codes.
            //
        }

        //
        // delete the key
        //

```

```

        __try {
            retCode = (*(pSceCbInfo->pfSetInfo))(
                pSceCbInfo->sceHandle,
                SceSvcConfigurationInfo,
                ServiceInfo->Lines[i].key,
                TRUE,
                NULL
            );
        } __except (EXCEPTION_EXECUTE_HANDLER) {
            retCode = SCESTATUS_SERVICE_NOT_SUPPORT;
        }
        if(retCode != SCESTATUS_SUCCESS)
        {
            //
            // error cleanup.
            //
        }

    }
    //
    // SCESTATUS_RECORD_NOT_FOUND means nothing more.
    // as the key does not even exist.
    //
}
else
{
    //
    // value to set is non-NULL,
    // hence we must compare with current analysis
    // if it is same, then delete the current analysis
    // if it is different, do nothing to the analysis.
    // Simply update the configuration info.
    //
    // left as exercise to the implementor.
    //
}

if ( pConfigInfo != NULL ) {
    __try {
        (*(pSceCbInfo->pfFreeInfo))((PVOID)pConfigInfo);
    } __except (EXCEPTION_EXECUTE_HANDLER) {
    }
}
pConfigInfo = NULL;

if ( pAnaInfo != NULL ) {
    __try {
        (*(pSceCbInfo->pfFreeInfo))((PVOID)pAnaInfo);
    } __except (EXCEPTION_EXECUTE_HANDLER) {
    }
}
pAnaInfo = NULL;

}
//
// error cleanup
// set detail error message appropriately if the buffer
// is not NULL
//
return retCode;
}

```

---

## Instalación y registro

El DLL del anexo debe instalarse en el sistema basado en Windows NT o Windows 2000 donde se espera que sea utilizado. Además, las Herramientas de configuración de seguridad debe estar al tanto de la presencia del anexo.

### Para instalar y registrar el DLL

1. Copie el DLL del anexo a un directorio particular. El directorio recomendado es %windir%\Security\Attachments. Puede crear este directorio en caso de que no exista. Se espera que únicamente los administradores del sistema instalen los anexos en el sistema.
2. Cree una clave de registro:

**HKEY\_LOCAL\_MACHINE\  
Software\  
Microsoft\  
Windows NT\  
CurrentVersion\  
SecEdit\Services\  
[Service Name]**

El Nombre de servicio que se utiliza aquí es el nombre registrado para el anexo. Deberá ser único de manera que no se confunda con los demás. El nombre del servicio deberá ser el mismo nombre que se utiliza en Administrador de control de servicio si el anexo programa las configuraciones específicas de servicio. El nombre utilizado en Administrador de control de servicio es el nombre que sirve para enlazar cada servicio con las herramientas de configuración de seguridad.

3. Cree los siguientes valores en esta clave:
  - Value Name = ServiceAttachmentPath
  - VValue Type = REG\_SZ
  - VValue = The full path to the attachment DLL (for example, %windir%\Security\Attachments\Something.dll).

### Creación de un *Snap-in* de extensión

Los *snap-ins* de las Herramientas de configuración de seguridad están diseñadas para ser expandibles a fin de soportar los *snap-ins* de extensión del anexo. La comunicación entre los *snap-ins* de las Herramientas de configuración de seguridad y los de extensión es manejada por los mecanismos MMC estándar y dos interfaces bien definidas del Modelo de objeto componente (COM). El mecanismo del anexo es responsable de la configuración y análisis de la seguridad del servicio y de la actualización de la configuración del servicio en la base de datos; la extensión del anexo permite que el usuario visualice, cree y modifique información de configuraciones y análisis. Para que funcione de una manera correcta, el *snap-in* del anexo debe seguir los lineamientos del *snap-in* de extensión MMC y los lineamientos del anexo proporcionados en este documento.

Cada *snap-in* de anexo debe ser un *snap-in* de extensión y estos *snap-ins* de extensión proporcionan funcionalidad únicamente cuando son invocados por el *snap-in* de las Herramientas de configuración de seguridad (o Administrador). Cada *snap-in* de anexo puede ampliar únicamente los nodos de Servicios. Se declara a sí mismo como subordinado de los nodos de Servicios, y posteriormente, para cada concurrencia de tipo de nodo de Servicios, la consola MMC agrega automáticamente las extensiones del *snap-in* relacionado. Cada anexo cuenta con su propio nodo de panel de enfoque y el panel de resultados relacionados en MMC. Las extensiones del anexo deben permitir que el usuario cree o modifique las configuraciones de seguridad de servicio en una configuración administrada por el *snap-in* de Editor de configuración de seguridad (y Administrador). Asimismo, debe ser capaz de mostrar la configuración y/o configuraciones de seguridad de análisis con el estado de análisis. Debe soportar la edición de las configuraciones de servicio para un sistema, y los resultados del análisis deben ser actualizados con base en las configuraciones actualizadas.

A la extensión del anexo, le corresponde determinar el formato y lógica de implementación de su propio panel de resultados. Las interfaces COM proporcionan una manera de ampliar la funcionalidad de Editor de configuración de seguridad (y Manager) para servicios, sin dictar la manera en que cada extensión de servicio realiza sus tareas particulares. Consulte el esquema de la interfaz COM que se muestra en la Figura A2.

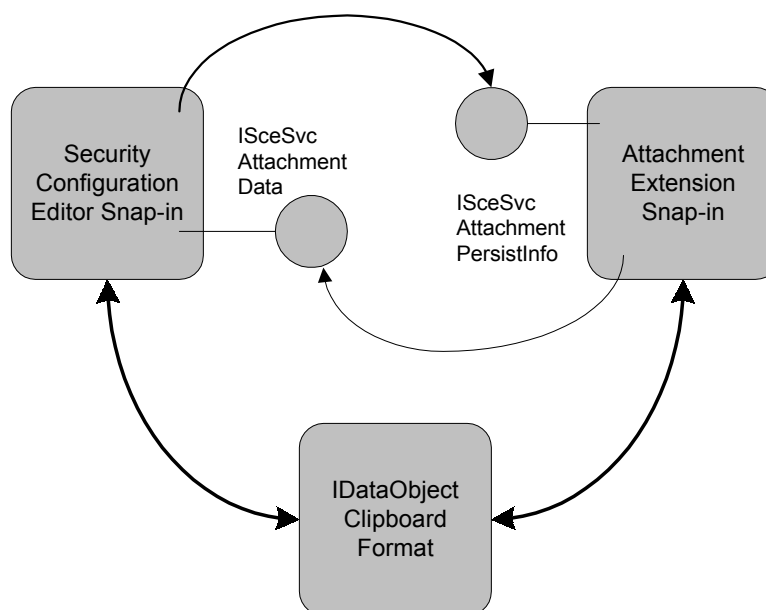


Figura A2. Esquema de la interfaz COM para el anexo

En esta ilustración, el *snap-in* de Editor de configuración de seguridad (o Manager) implementa la interfaz **ISceSvcAttachmentData**. La interfaz proporciona el *snap-in* del anexo para consultar la información de configuración y análisis de las

---

configuraciones o la base de datos. El *snap-in* del anexo implementa la interfaz **ISceSvcAttachmentPersistInfo**, la cual es utilizada por Editor de configuración de seguridad (o Administrador), a fin de obtener cualquier información modificada que pudiera necesitar escribirse para la configuración o la base de datos. Posteriormente el *snap-ins*, guarda esta información según corresponda.

Existen tres operaciones que debe soportar un *snap-in* de anexo:

- **Mostrar configuración y/o información de inspección**—Para mostrar la información, el nodo del *snap-in* del anexo extiende el *snap-in* de Editor de configuración de seguridad (o Administrador) a través del nodo Servicios. Los tipos de nodo de Editor de configuración de seguridad (o Administrador) que pueden extenderse son:
  - **Configuration Services NodeType** = {24a7f717-1f0c-11d1-affb-00c04fb984f9}
  - **Analysis Services NodeType** = {678050c7-1ff8-11d1-affb-00c04fb984f9}Al crear o editar una configuración, si se extiende el nodo de servicios, todos los *snap-in* de extensión registrados reciben una notificación directamente por parte de la MMC. Cada anexo deberá insertarse bajo el nodo Servicios y después completar los siguientes pasos:
  1. Utilizar el método **QueryInterface** para consultar la interfaz **ISceSvcAttachmentData**.
  2. Llamar al método **Inicializar** para informar a Security Configuration Tool Set que está cargado y establecer un contexto para comunicar la información adecuada.
  3. Utilizar el método **GetData**; para extraer la información inmediatamente o esperar hasta que su nodo sea seleccionado por el usuario.
- **Modificar la información de configuración de las configuraciones**—El *snap-in* del anexo debe permitir que el usuario modifique la información de configuración sobre el servicio. La información modificada debe retenerse mediante el *snap-in* del anexo hasta que Editor de configuración de seguridad (o Administrador) utilice la interfaz **ISceSvcAttachmentPersistInfo** para extraer la información. Para evitar fallas en la memoria, la memoria asignada deberá ser liberada por el propietario. Por esta razón, ambas interfaces tienen el método **FreeBuffer**.
- **Modificar la información de configuración en la base de datos**—Asimismo, el *snap-in* del anexo debe soportar las modificaciones para la información de configuración a través del nodo de inspección. Esto permite que el usuario realice cambios y vuelva a aplicar la configuración. La lógica para llevar a cabo este paso debe ser idéntica a la modificación de información en los archivos de configuración. Los cambios deberán ser realizados en la configuración guardada en la base de datos de inspección.

### Formato de portapapeles

```
#define CCF_SCESVC_ATTACHMENT ( L"CCF_SCESVC_ATTACHMENT" )
```

---

El portapapeles se utiliza para que cada *snap-in* de anexo extraiga el nombre del archivo de configuración del Editor de configuración de seguridad (o Administrador). El nombre del archivo de configuración es PWSTR. Este nombre de configuración se utiliza para comunicaciones avanzadas entre el anexo y Editor de configuración de seguridad (o Administrador) en el método **Inicializar**.

### Interfaces de *snap-in* de extensión

El *snap-in* de extensión consulta las siguientes interfaces de *snap-in* de Editor de configuración de seguridad (o Administrador).

#### ISceSvcAttachmentData

La interfaz se implementa mediante el *snap-in* de Editor de configuración de seguridad (o Administrador) a fin de soportar los *snap-ins* de extensión. El *snap-in* de extensión del anexo deberá utilizarse para recuperar la información específica del servicio para mostrar en pantalla la modificación del usuario.

```
class ISceSvcAttachmentData : public IUnknown
{
public:
    virtual /* [helpstring] */ HRESULT STDMETHODCALLTYPE GetData(
        /* [in] */ SCE_HANDLE sceHandle,
        /* [in] */ SCESVC_INFO_TYPE sceType,
        /* [out] */ PVOID *ppvData,
        /* [in out] */ PSCE_ENUMERATION_CONTEXT psceEnumHandle ) = 0;

    virtual /* [helpstring] */ HRESULT STDMETHODCALLTYPE Initialize(
        /* [in] */ LPCTSTR ServiceName,
        /* [in] */ LPCTSTR TemplateName,
        /* [in] */ LPUNKNOWN lpUnknown,
        /* [out] */ SCE_HANDLE *sceHandle) = 0;

    virtual /* [helpstring] */ HRESULT STDMETHODCALLTYPE FreeBuffer(
        /* [in] */ PVOID pvData) = 0;

    virtual /* [helpstring] */ HRESULT STDMETHODCALLTYPE CloseHandle(
        /* [in] */ SCE_HANDLE sceHandle) = 0;
};
```

#### ISceSvcAttachmentPersistInfo

Esta interfaz es una especie de compilación que debe ser implementada por cada *snap-in* de extensión de anexo. El *snap-in* de Editor de configuración de seguridad (o Administrador) solicita esta interfaz para verificar si existe información modificada que debe ser escrita nuevamente en el archivo de configuración o base de datos (utilizando *IsDirty*). Si este es el caso, llama al método **Guardar** para hacer que el *snap-in* de extensión comunique la información que debe ser guardada.

```
class ISceSvcAttachmentPersistInfo : public IUnknown
{
public:
    virtual /* [helpstring] */ HRESULT STDMETHODCALLTYPE Save(
        /* [out] */ SCE_HANDLE *sceHandle,
        /* [out] */ PVOID *ppvData,
        /* [out] */ PBOOL pbOverwriteAll ) = 0;

    virtual /* [helpstring] */ HRESULT STDMETHODCALLTYPE IsDirty() = 0;
```

```
virtual /* [helpstring] */ HRESULT STDMETHODCALLTYPE FreeBuffer(
    /* [in] */ PVOID pvData) = 0;
};
```

### Instalación y registro

El *snap-in* de Editor de configuración de seguridad (o Administrador) proporciona las extensiones únicamente a través del espacio de nombre Editor de configuración de seguridad (o Administrador). Los menús de contexto, barras de herramientas, botones de la barra de herramientas y páginas de propiedades no son ampliables en este punto. El *snap-in* del anexo deberá ampliar el espacio de nombre Editor de configuración de seguridad (o Administrador) poblando su propio nodo en lugares bien definidos en el espacio de nombre.

Los *snap-ins* del anexo deberán ser registrados bajo la clave de registro:

```
HKEY_LOCAL_MACHINE\
Software\
Microsoft\
MMC\
Snapins
```

La clave **StandAlone** no deberá crearse bajo el *snap-in* debido a que cada *snap-in* del anexo debe ser únicamente una extensión.

Asimismo, los *snap-ins* del anexo también deben registrarse bajo las subclaves Security Configuration Editor Services Node Type de la siguiente manera:

- Para ampliar el espacio del nombre de Editor de configuración de seguridad, utilice la clave de registro:

```
HKLM\
Software\
Microsoft\
MMC\
NodeTypes\
24a7f717-1f0c-11d1-affb-00c04fb984f9\
Extensions\
NameSpace
```

- Para ampliar el espacio de nombre de inspección de Administrador de configuración de seguridad (análisis), utilice la clave de registro:

```
HKLM\
Software\
Microsoft\
MMC\
NodeTypes\
```

---

678050c7-1ff8-11d1-affb-00c04fb984f9\

Extensions\

Namespace

Para mayores informes, consulte el archivo con el encabezado Scesvc.h en las plataformas SDK.

Para registrar los *snap-ins* del anexo como extensiones del *snap-in* de Editor de configuración de seguridad o Administrador, cree estas claves en su **DllRegisterServer** e implementaciones de función **IUnregisterServer**.

#### Inicialización—adición de un nodo de anexo

Cuando un nodo de Servicios se encuentra bajo Editor de configuración de seguridad o se amplía administrador de configuración de seguridad, MMC utiliza **IComponentData::Notify** y el evento **MMCN\_EXPAND** para notificar Editor de configuración de seguridad o Administrador y todas sus extensiones.

Posteriormente, las Herramientas de configuración de seguridad extraen su formato interno desde el **lpDataObject** y detiene el procesamiento posterior cuando ve el tipo de nodo Servicios. Asimismo, los *snap-ins* del anexo (registrados como extensiones) también extraen el tipo de nodo de **lpDataObject**. Si el tipo de nodo es uno de los tipos de nodo de Servicios definidos anteriormente, los *snap-ins* del anexo insertan sus nodos de raíz bajo el nodo *parent* especificado.

```
//
// detect which extension node to extend
//

GUID* nodeType = ExtractNodeType(lpDataObject);

if ( nodeType == NULL ) {
    return S_OK;
}

if ( ::IsEqualGUID(*nodeType, cNodetypeSceTemplateServices) == TRUE )
    folderType = ATTACHEMNT_STATIC; // defined by attachment writer.
else if ( ::IsEqualGUID(*nodeType, cNodetypeSceAnalysisServices)
== TRUE)
    folderType = ATTACHMENT_STATIC_ANALYSIS;
// defined by attachment writer

// Free resources
::GlobalFree(reinterpret_cast<HANDLE>(nodeType));

//
// As an extension snapin, the service attachment
// root node should be added
// Insert that node, and remember it
// as the root of the SMB Extension namespace.
//
CheckAndInsertRootNodeToMMCScopePane
```

El siguiente paso principal en la inicialización es establecer la comunicación con el *snap-in* de Editor de configuración de seguridad o Administrador. Esto es necesario ya que el anexo obtiene sus datos, así como cualquiera de los cambios realizados por el usuario, de Editor de configuración de seguridad o Administrador. Para hacerlo, siga estos pasos:



1. Obtenga el nombre de configuración. Si el tipo de nodo de Servicios que el anexo insertó fue el de la configuración, el anexo necesita conocer qué configuración es. Comunica esta configuración al Editor de configuración de seguridad o Administrador durante la inicialización de la interfaz. El nombre de la configuración puede obtenerse a través del formato del portapapeles, de la manera siguiente:

```
PWSTR * TemplateName =  
ExtractTemplateNameFromDataObject(lpDataObject);
```

2. Establezca el contexto con Editor de configuración de seguridad o Administrador. Una vez que se conoce el nombre de la configuración (o si el nodo Servicio es de tipo Inspección), el *snap-in* del anexo deberá consultar la interfaz **ISceSvcAttachmentData** y llamar el método **Inicializar** para establecer el contexto.

```
//  
// QueryInterface for the main snap-in's IUnknown.  
//  
LPUNKNOWN punk;  
  
hr = lpDataObject->QueryInterface(IID_IUnknown,  
    reinterpret_cast<void*>(&punk));  
  
//  
// QueryInterface ISceSvcAttachmentData  
//  
if ( SUCCEEDED(hr) ) {  
    hr = punk->QueryInterface(IID_ISceSvcAttachmentData,  
        reinterpret_cast<void*>(&pSceData));  
}  
  
...  
  
//  
// QueryInterface the attachment's IUnknown as  
// that is needed by the main snap-in.  
//  
((LPUNKNOWN)m_pSnapin)->QueryInterface(IID_IUnknown,  
    reinterpret_cast<void*>(&punk));  
  
//  
// Call Initialize to setup context with main snap-in.  
//  
m_pSceData->Initialize(ServiceName, TemplateName, punk, &sceHandle);  
  
...
```

**Nota** Debe llamar **CloseHandle** para cerrar una vez que *sceHandle* haya terminado.

3. Obtenga los datos correspondientes. El *snap-in* de anexo puede utilizar el contexto establecido para consultar los datos correspondientes de Editor de configuración de seguridad, según sea necesario, mediante el uso de la interfaz **GetData**. El anexo puede decidir hacer esto de manera proactiva tan pronto como se inicializa con Editor de configuración de seguridad, o puede esperar hasta que el usuario trate realmente de expandir el nodo del anexo dando un clic en él. El anexo puede mostrar la información recibida utilizando cualquiera de los controles UI disponibles.

```
//
```

---

```

// GetData - we get the configuration information here.
//
m_pSceData->GetData (sceHandle, SceSvcConfigurationInfo, &pData,
&enumHandle );

```

**Nota** Deberá utilizar el método **FreeBuffer** para liberar el *buffer* asignado por Editor de configuración de seguridad o Manager.

### Implementación de ISceSvcAttachmentPersistInfo

Después de la inicialización, es importante que el anexo implemente la interfaz **ISceSvcAttachmentPersistInfo**. Editor de configuración de seguridad o Administrador consulta esta interfaz varias veces, como lo hace al guardar la configuración o al cerrar el *snap-in*, con el fin de permitir que el anexo guarde cualquiera de las modificaciones que el usuario pueda haber realizado a la base de datos de inspección o a la configuración asociada.

```

class CSceSvcAttachmentPersistInfo:
public ISceSvcAttachmentPersistInfo,
public CComObjectRoot
{
BEGIN_COM_MAP(CSceSvcAttachmentPersistInfo)
COM_INTERFACE_ENTRY(ISceSvcAttachmentPersistInfo)
END_COM_MAP()

friend class CDataObject;
friend class CComponentDataImpl;

CSceSvcAttachmentPersistInfo();
~CSceSvcAttachmentPersistInfo();

public:

// ISceSvcAttachmentPersistInfo interface members
STDMETHOD(IsDirty)();
STDMETHOD(Save)(SCE_HANDLE *sceHandle, PVOID *ppvData,
PBOOL pboverwriteAll );
STDMETHOD(FreeBuffer)(PVOID pvData);

...

private:
CString m_TemplateName;
LPSCESVCATTACHMENTDATA m_pSceData;
SCE_HANDLE m_sceHandle;

...

};

//
// Implementing IsDirty()
//
STDMETHODIMP CSceSvcAttachmentPersistInfo::IsDirty()
{
if ( m_pSnapin == NULL ) {
return S_FALSE;
}
//
// just calling the snapin's main IsDirty.
//
return m_pSnapin->IsDirty();
}

//
// Implementing Save()

```

```

//
STDMETHODIMP CSceSvcAttachmentPersistInfo::Save(
    SCE_HANDLE *psceHandle,
    PVOID *ppvData,
    PBOOL pbOverwriteAll )
{
    if ( psceHandle == NULL || ppvData == NULL ||
    pbOverwriteAll == NULL ) {
        return E_INVALIDARG;
    }

    if ( m_pSnapin != NULL ) {

        m_pSnapin->SaveDataInBuffer(ppvData, pbOverwriteAll);

        *psceHandle = m_sceHandle;

    }

    return S_OK;
}

//
// Implementing FreeBuffer
//
STDMETHODIMP CSceSvcAttachmentPersistInfo::FreeBuffer(PVOID pvData)
{
    if ( pvData == NULL ) {
        return S_OK;
    }

    PSCESVC_ANALYSIS_INFO pTempInfo=(PSCESVC_ANALYSIS_INFO)pvData;

    if ( pTempInfo->Lines != NULL ) {

        for ( DWORD i=0; i < pTempInfo->Count; i++ ) {

            if ( pTempInfo->Lines[i].Key != NULL )
                LocalFree(pTempInfo->Lines[i].Key);

            if ( pTempInfo->Lines[i].Value != NULL )
                LocalFree(pTempInfo->Lines[i].Value);

        }

        LocalFree( pTempInfo->Lines);

    }

    LocalFree(pTempInfo);

    return S_OK;
}

```