ESET Remote Administrator

Manual de instalación
y Guía del usuario

Protegemos su mundo digital

índice

ESET Remote Administrator

Copyright © 2009 de ESET, spol. s r. o.

ESET Smart Security ha sido desarrollado por ESET, spol. s r.o.
Para obtener más información, acceda a www.eset.com.
Todos los derechos reservados. Ninguna parte de esta documentación podrá reproducirse, almacenarse en un sistema de recuperación o transmitirse en forma o modo alguno, ya sea por medios electrónicos, mecánicos, fotocopia, grabación, escaneo o cualquier otro medio sin contar con la autorización escrita del autor.
ESET, spol. s r.o. se reserva el derecho a cambiar cualquier elemento del software de la aplicación sin previo aviso.

Atención al cliente internacional: www.eset.eu/support
Atención al cliente para América del Norte: www.eset.com/support

REV.20090620-001

1. Introducción

ESET Remote Administrator (ERA) es una aplicación que permite administrar los productos de ESET en un entorno de red, incluyendo estaciones de trabajo y servidores, desde una ubicación central. Con el sistema de administración de tareas integrado de ESET Remote Administrator, puede instalar soluciones de seguridad ESET en equipos remotos y responder rápidamente ante amenazas y problemas nuevos.

ESET Remote Administrator no proporciona por sí mismo ninguna otra forma de protección frente a los códigos maliciosos. ERA depende de la presencia de una solución de seguridad ESET en las estaciones de trabajo o servidores, como ESET NOD32 Antivirus o ESET Smart Security.

Para realizar la implantación completa de un conjunto de soluciones de seguridad ESET, adopte los siguientes pasos:
- Instalación del servidor ERA (ERAS),
- Instalación de la consola ERA (ERAC),
- Instalación de equipos cliente (ESET NOD32 Antivirus, ESET Smart Security, Linux ESET Security client, etc.).

NOTA: *algunas partes de este documento emplean variables de sistema que se refieren a la ubicación exacta de las carpetas y archivos:*
%ProgramFiles % = *normalmente* C:\Program Files
%ALLUSERSPROFILE % = > *normalmente* C:\Documents and Settings\All Users

1.1 Arquitectura del programa

Técnicamente, ESET Remote Administrator consta de dos componentes individuales: el servidor ERA (ERAS) y la consola ERA (ERAC). Puede ejecutar un número ilimitado de consolas y servidores ERA en la red, ya que no existen limitaciones en el acuerdo de licencia de uso. La única limitación está marcada por el número total de clientes de la instalación que ERA puede administrar (consulte la sección 1.1.6, "Claves de licencia").

1.1.1 Servidor ERA (ERAS)

El componente de servidor de ERA se ejecuta como un servicio dentro de los siguientes sistemas operativos basados en Microsoft Windows® NT: NT4, 2000, XP, 2003, Vista y 2008. La principal tarea de este servicio es recoger información de los clientes y enviarles distintas solicitudes. Estas solicitudes, incluidas las tareas de configuración, las solicitudes de instalación remota, etc., se crean a través de la consola ERA (ERAC). El ERAS es un punto de encuentro entre la ERAC y los equipos cliente (un lugar en el que toda la información se procesa, se mantiene o se modifica antes de transferirse a los clientes o a la ERAC).

1.1.2 Consola ERA (ERAC)

La ERAC es el componente cliente de ERA y se instala habitualmente en una estación de trabajo. El administrador usa esta estación de trabajo para controlar las soluciones ESET en clientes individuales de forma remota. Con una ERAC, el administrador puede conectarse al componente servidor de ERA, en el puerto TCP 2223. La comunicación se controla a través del proceso console.exe, que se encuentra generalmente en el directorio:

%ProgramFiles %\ESET\ESET Remote Administrator\Console

Al instalar una ERAC, es posible que tenga que indicar el nombre de un ERAS. En el arranque, la consola se conecta automáticamente a este servidor. También se puede configurar la ERAC después de la instalación.

La ERAC genera registros gráficos en HTML que se guardan localmente. El resto de la información se envía desde el ERAS a través del puerto TCP 2223.

2. Instalación de un servidor ERA y una consola ERA

2.1 Requisitos

El ERAS funciona como un servicio, por lo que requiere un sistema operativo basado en Microsoft Windows NT (NT4, 2000, XP, 2003, Vista o 2008). No es necesario disponer de Microsoft Windows Server Edition para que funcione el ERAS. Un equipo con un ERAS instalado siempre deberá estar en línea y accesible a través de la red de equipos mediante:

- Clientes (generalmente, estaciones de trabajo)
- PC con consola ERA
- Otras instancias del ERAS (si está replicado)

2.1.1 Requisitos de hardware

El efecto en el rendimiento del sistema es mínimo. Sin embargo, depende del número de clientes, del tipo de base de datos que el ERAS utilice, del nivel de registro, etc. La configuración de HW mínima para la implantación de un ERAS coincide con la configuración mínima recomendada para el sistema operativo de Microsoft Windows del equipo.

2.1.2 Puertos utilizados

La tabla siguiente enumera las posibles comunicaciones de red con un ERAS instalado. El proceso EHttpSrv.exe escucha en el puerto TCP 2221 y el proceso era.exe escucha en los puertos TCP 2222, 2223, 2224 y 2846. El resto de comunicaciones se produce utilizando procesos del sistema operativo original (por ejemplo, "NetBIOS sobre TCP/IP").

Protocolo	Puerto	Descripción
TCP	2221 (escucha del ERAS)	Puerto predeterminado que la función del servidor local de actualización integrada en ERAS utiliza (versión HTTP)
TCP	2222 (escucha del ERAS)	Comunicación entre clientes y el ERAS
TCP	2223 (escucha del ERAS)	Comunicación entre la ERAC y el ERAS

Si se utilizan todas las funciones del programa, deberán abrirse los siguientes puertos de red:

Protocolo	Puerto	Descripción
TCP	2224 (escucha del ERAS)	Comunicación entre el agente einstaller.exe y el ERAS durante la instalación remota
TCP	2846 (escucha del ERAS)	Replicación del ERAS
TCP	139 (puerto de destino desde el punto de vista del ERAS)	Copia del agente einstaller.exe del ERAS a un cliente, utilizando el recurso compartido admin$
UDP	137 (puerto de destino desde el punto de vista del ERAS)	"Resolución del nombre" durante la instalación remota
UDP	138 (puerto de destino desde el punto de vista del ERAS)	"Exploración" durante la instalación remota
TCP	445 (puerto de destino desde el punto de vista del ERAS)	Acceso directo a recursos compartidos utilizando TCP/IP durante la instalación remota (una alternativa a TCP 139)

Los puertos predeterminados 2221, 2222, 2223, 2224 y 2846 se pueden cambiar en caso de que ya haya otras aplicaciones que los estén utilizando.

Para cambiar los puertos predeterminados que ERA utiliza, haga clic en **Herramientas > Opciones del servidor...** Para cambiar el puerto 2221, seleccione la ficha **Actualizaciones** y cambie el valor de **Puerto de servidor HTTP**. Los puertos 2222, 2223, 2224 y 2846 se pueden modificar en la sección **Puertos** de la ficha **Otras opciones**.

Los puertos predefinidos 2222, 2223, 2224 y 2846 también se pueden modificar durante el modo de instalación avanzado (ERAS).

2.2 Guía de instalación básica

2.2.1 Información general del entorno (estructura de la red)

Una red empresarial consta generalmente de una red de área local (LAN), por ello se aconseja la instalación de un ERAS y de un servidor local de actualización. El servidor local de actualización se puede crear en el ERAS o en ESET NOD32 Antivirus Business Edition /ESET Smart Security Business Edition.

Supongamos que todos los clientes sean estaciones de trabajo y portátiles equipados con Microsoft Windows 2000/XP/Vista, conectados por red dentro de un dominio. El servidor llamado GHOST está en línea las 24 horas del día, todos los días de la semana, y puede ser una estación de trabajo Windows, Professional o Server Edition (no tiene porqué ser un servidor Active Directory). Además, supondremos que no hay portátiles disponibles en la red de la empresa durante la instalación de las soluciones cliente de ESET. La estructura de la red podrá parecerse a la que se muestra a continuación:

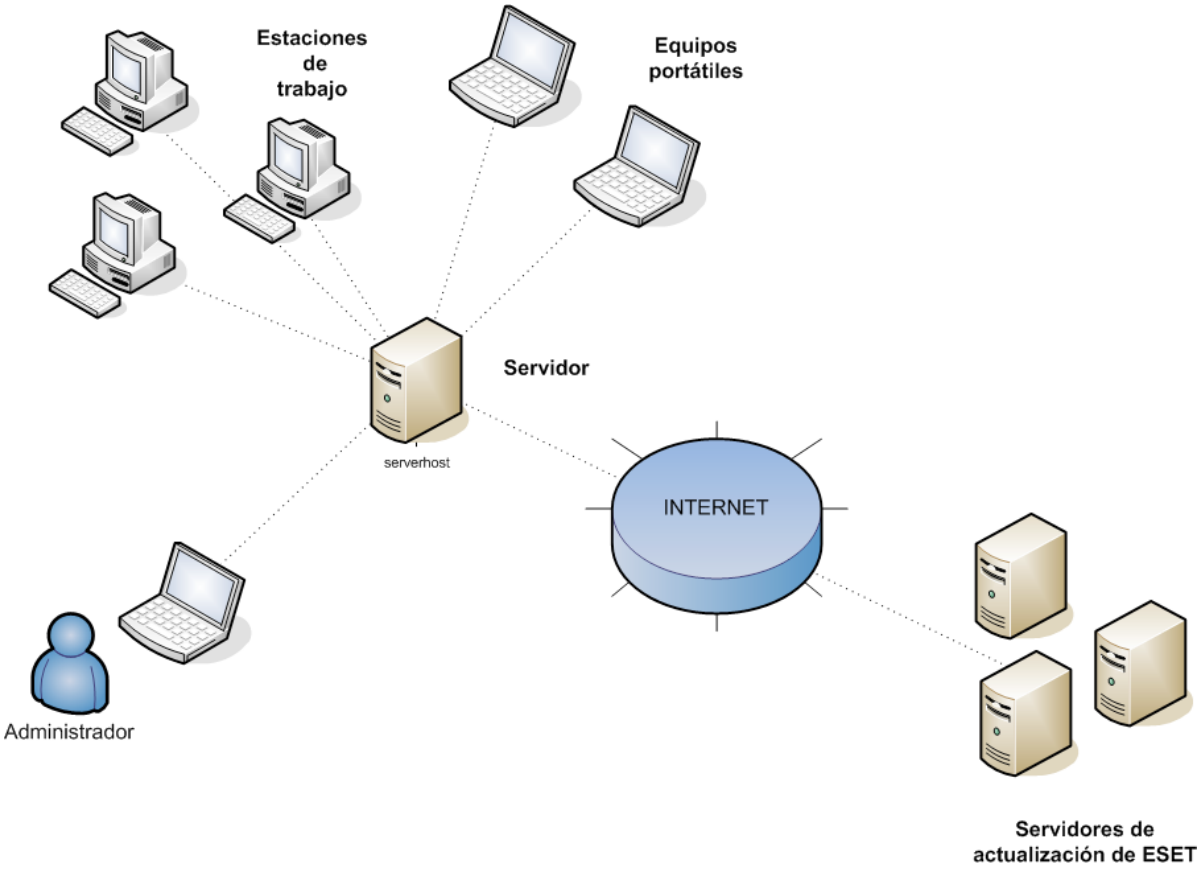


Figura 2-1

2.2.2 Antes de la instalación

Antes de la instalación, deben descargarse los paquetes de instalación siguientes del sitio web de ESET:

Componentes de ESET Remote Administrator:

ESET Remote Administrator – Servidor
ESET Remote Administrator – Consola

Soluciones cliente de ESET:

ESET Smart Security 4.0
ESET Smart Security 3.0
ESET NOD32 Antivirus 4.0
ESET NOD32 Antivirus 3.0
ESET NOD32 Antivirus 2.7

Descargue sólo las soluciones cliente que usará en las estaciones de trabajo cliente.

2.2.3 Instalación

2.2.3.1 Instalación del servidor ERA

Instale el ERAS en el servidor llamado GHOST. Puede elegir entre los modos de instalación Avanzada o Típica.

Si selecciona la instalación Típica, el programa le solicitará que inserte una clave de licencia, un archivo con la extensión .lic, que hace posible el funcionamiento del ERAS durante el período estipulado en la licencia. A continuación, el programa le pedirá que establezca unos parámetros para las actualizaciones (nombre de usuario, contraseña y servidor de actualización). Sin embargo, puede continuar con el paso siguiente y definir estos parámetros más tarde.

Si selecciona la instalación Avanzada, el instalador le presentará más parámetros para que los configure. Podrá modificar estos parámetros posteriormente a través de la ERAC, pero en la mayoría de los casos no será necesario. La única excepción es el nombre del servidor, que debe ser equivalente al nombre de DNS o el valor %COMPUTERNAME % del sistema operativo o la dirección IP asignada al equipo. Ésta es la información más importante para llevar a cabo la instalación remota. Si no se especifica el nombre durante la instalación, el instalador automáticamente empleará el valor de la variable de sistema %COMPUTERNAME %, lo que en la mayoría de los casos es suficiente.

También es importante seleccionar la base de datos correcta, en la que se almacenará la información de ERAS. Para obtener más información, vea la sección 2.2.3.4, "Bases de datos compatibles con el servidor de ERA".

De manera predeterminada, los componentes del programa del ERAS se instalan en la carpeta siguiente:

%ProgramFiles %\ESET\ESET Remote Administrator\Server

Otros componentes de datos, tales como registros, paquetes de instalación, configuración, etc. se almacenan en:

%ALLUSERSPROFILE %\Application Data \ESET\ESET Remote Administrator\Server

Una vez finalizada la instalación, el servicio del ERAS se inicia automáticamente. La actividad del ERAS queda registrada en esta ubicación:

%ALLUSERSPROFILE %\Application Data\ESET\ESET Remote Administrator\Server\logs\era.log

2.2.3.2 Instalación de la consola ERA

Instale la consola de ESET Remote Administrator en el PC/portátil del administrador (como se muestra en la parte inferior izquierda de la Figura 2-1). Al final del modo de instalación Avanzada, escriba el nombre del servidor de ERA (o la dirección IP) al que debe conectarse automáticamente la ERAC cuando se inicie. En nuestro ejemplo, el nombre del servidor es GHOST.

Tras la instalación inicie la ERAC y compruebe la conexión al ERAS. No se requiere ninguna contraseña de forma predeterminada para conectarse a un servidor ERA (el campo de texto de la contraseña está vacío), pero se recomienda encarecidamente establecer una. Para crear una contraseña para la conexión a un servidor ERA: haga clic en **Archivo > Cambiar contraseña...** y modifique la contraseña para la consola haciendo clic en el botón **Cambiar...**

El administrador puede especificar una contraseña para el acceso como administrador y el acceso de sólo lectura (que sólo permite ver la configuración del ERAS).

2.2.3.3 Cómo activar y configurar el servidor local de actualización

Puede usar la consola ERA para activar el servidor de actualización de LAN (el servidor local de actualización en el servidor ERA). Este servidor puede usarse como fuente de archivos de actualización para estaciones de trabajo ubicadas en la LAN. Al activar el servidor local de actualización, se reduce el volumen de datos que se transfiere a través de la conexión a Internet.

Siga estos pasos:

1. Conecte la consola ERA al servidor ERA haciendo clic en **Archivo > Conectar.**
2. Desde la consola ERA, haga clic en **Herramientas > Opciones del servidor...** y haga clic en la ficha **Actualizaciones**.
3. **En el menú desplegable** Servidor de actualización, elija **Seleccionar automáticamente** y deje el Intervalo de actualización en 60 minutos. Indique el **Nombre de usuario de actualización** (EAV-***), haga clic en **Establecer contraseña..** y escriba o pegue la contraseña que ha recibido con el nombre de usuario.
4. Seleccione la opción **Crear servidor local de actualización**. Conserve la ruta predeterminada para los archivos del servidor local de actualización y el puerto del servidor HTTP (2221). Deje **Autentificación** con el valor NINGUNA.
5. Haga clic en la ficha **Otras opciones** y haga clic en **Modificar configuración avanzada...** En el árbol de configuración avanzada, acceda a **Servidor ERA > Configuración > Servidor local de actualización > Crear servidor local de actualización para los componentes del programa seleccionados**. Haga clic en **Modificar** en la parte derecha y seleccione los componentes de programa que desea descargar. Seleccione los componentes para todas las versiones de idioma que se usarán en la red.
6. En la ficha **Actualizaciones**, haga clic en **Actualizar ahora** para crear el servidor local de actualización.

Para obtener opciones de configuración del servidor local de actualización más detalladas, consulte la sección 7.3 3, "Cómo activar y configurar el servidor local de actualización".

2.2.3.4 Tipos de bases de datos compatibles con el servidor de ERA

El programa usa de forma predeterminada el motor de Microsoft Access (base de datos Jet). ERAS 3.0 también es compatible con las siguientes bases de datos:
- Microsoft SQL Server
- MySQL
- Oracle

El tipo de base de datos se puede seleccionar durante el modo de instalación Avanzada del ERAS. Tras la instalación, no podrá modificarse la versión de la base de datos.

2.2.3.4.1 Requisitos básicos

En primer lugar, hace falta crear la base de datos en un servidor de bases de datos. El instalador del ERAS puede crear una base de datos MySQL vacía, que automáticamente recibe el nombre de *ESETRADB*.

El instalador crea, de forma predeterminada y automáticamente, una base de datos nueva. Para crear la base de datos manualmente, seleccione la opción **Exportar secuencia de comandos**. Asegúrese de que no está seleccionada la opción **Crear tablas en la nueva base de datos automáticamente**.

Configuración de intercalación
La clasificación se lleva a cabo empleando los parámetros predeterminados de cada base de datos. Es necesario anular la diferenciación entre mayúsculas y minúsculas CASE INSENSITIVITY (CI).

Para activarla:

- Para MS_SQL y MySQL, configure un COLLATE con la opción CI activada.
- Para ORACLE, configure un NLS_SORT con la opción CI activada.
- Para MS Access, no es necesaria esta acción ya que de forma predeterminada no diferencia entre mayúsculas y minúsculas.

Juego de caracteres
Es importante usar el juego de caracteres UNICODE (se recomienda la codificación UTF-8), especialmente si existen clientes con configuraciones locales específicas o si ERA se ejecuta en una versión localizada. Si no se prevé la replicación y si todos los clientes se conectan al mismo servidor, puede usar el juego de caracteres para el ERA que desea instalar.

2.2.3.4.2 Configuración de la conexión de la base de datos

Después de crear una base de datos nueva, especifique los parámetros de conexión para el servidor de base de datos mediante una de estas dos opciones:

1. Mediante un DSN (nombre de origen de datos)
   Para abrir el DSN manualmente, abra el Administrador de orígenes de datos ODBC (haga clic en **Inicio –> Ejecutar** y escriba **odbcad32.exe**).

   Ejemplo de conexión de un DSN:
   DSN =ERASqlServer

2. Directamente, mediante una cadena de conexión completa
   Deben especificarse todos los parámetros requeridos – *controlador*, *servidor* y *nombre de la base de datos*.

   Este es un ejemplo de una cadena de conexión completa para MS SQL Server:
   Controlador ={SQL Server}; Servidor =nombredehost; Base de datos =ESETRADB

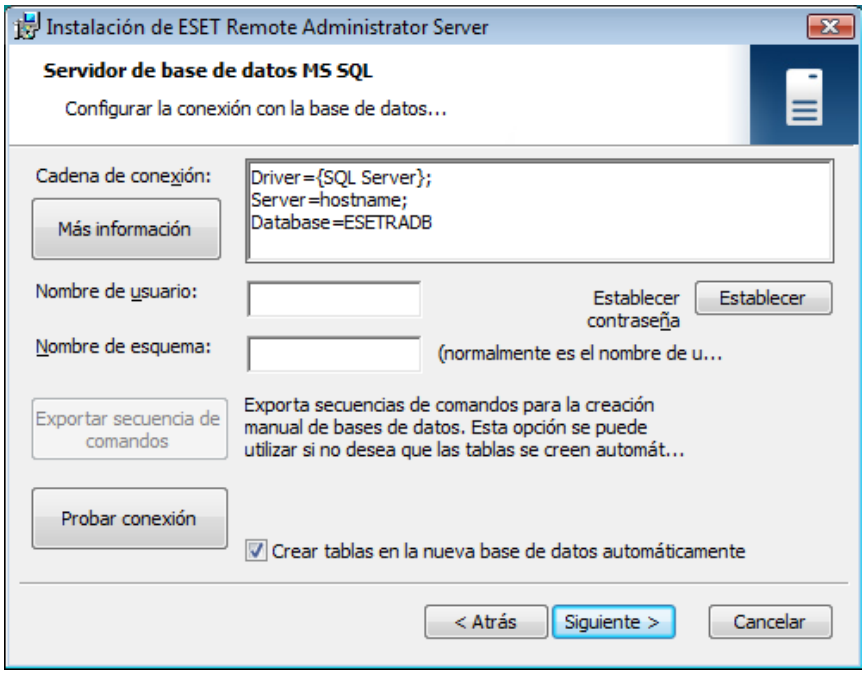


Figura 2-2

Este es un ejemplo de una cadena de conexión completa para Oracle Server:
Controlador ={Oracle en instantclient10_1}; dbq =nombre de host: 1521/ESETRADB

Este es un ejemplo de una cadena de conexión completa para MySQL Server:
Controlador ={MySQL ODBC 3.51}; Servidor =nombre de host; Base de datos =ESETRADB

A continuación, establezca el **Nombre de usuario** y la contraseña de la conexión (con el botón **Establecer contraseña**). Las bases de datos de Oracle y MS SQL Server necesitan también un **Nombre de esquema** (para MS SQL Server esto es generalmente igual al nombre de usuario).
Haga clic en **Probar conexión** para comprobar la conexión con el servidor de bases de datos.

2.2.3.4.3 Instalación sobre una base de datos ya existente

Si ya hay tablas en la base de datos, el instalador mostrará una notificación. Para sobrescribir el contenido de una tabla existente, seleccione **Sobrescribir** (Advertencia: este comando elimina el contenido de las tablas y también sobrescribe la estructura). Seleccione **Ignorar** para dejar las tablas intactas.

NOTA: *Si selecciona Ignorar, podrán aparecer, en ciertas circunstancias, errores de incoherencia en las bases de datos, especialmente cuando las tablas estén dañadas o no sean compatibles con la versión actual.*

Para cancelar la instalación del ERAS y analizar la base de datos manualmente, haga clic en **Cancelar**.

2.2.3.5 Instalación remota en estaciones de trabajo clientes en la red

En el supuesto de que todas las estaciones de trabajo estén activadas, el método de instalación impulsada resulta el método más efectivo. Antes de iniciar una instalación impulsada, descargue primero los archivos de instalación .msi para ESET Smart Security o ESET NOD32 Antivirus del sitio web de ESET y cree un paquete de instalación. Puede crear un archivo de configuración XML que se aplicará automáticamente cuando se ejecute el paquete. Encontrará más información sobre la instalación remota en el capítulo 4., "Instalación de soluciones cliente de ESET".

2.2.3.6 Instalación remota en portátiles que no están actualmente presentes en la red

Los portátiles que están fuera de la red local requieren un tipo diferente de instalación remota, puesto que la instalación debe realizarse después de iniciar sesión en el dominio. Para estos dispositivos, se sugiere el método de secuencia de comandos de inicio de sesión.

Encontrará más información sobre la instalación remota de la secuencia de comandos de inicio de sesión en el capítulo 4., "Instalación de soluciones cliente de ESET".

2.3 Situación: instalación en un entorno empresarial

2.3.1 Información general del entorno (estructura de la red)

A continuación, se muestra una copia de la estructura de red anterior, con una sucursal adicional, varios clientes y servidor llamado LITTLE. Supongamos que existe un canal VPN lento entre la sede y la sucursal. En este caso, el servidor local de actualización debería instalarse en el servidor LITTLE. También instalaremos un segundo servidor ERA en LITTLE para crear un entorno más intuitivo y minimizar el volumen de datos transferidos.

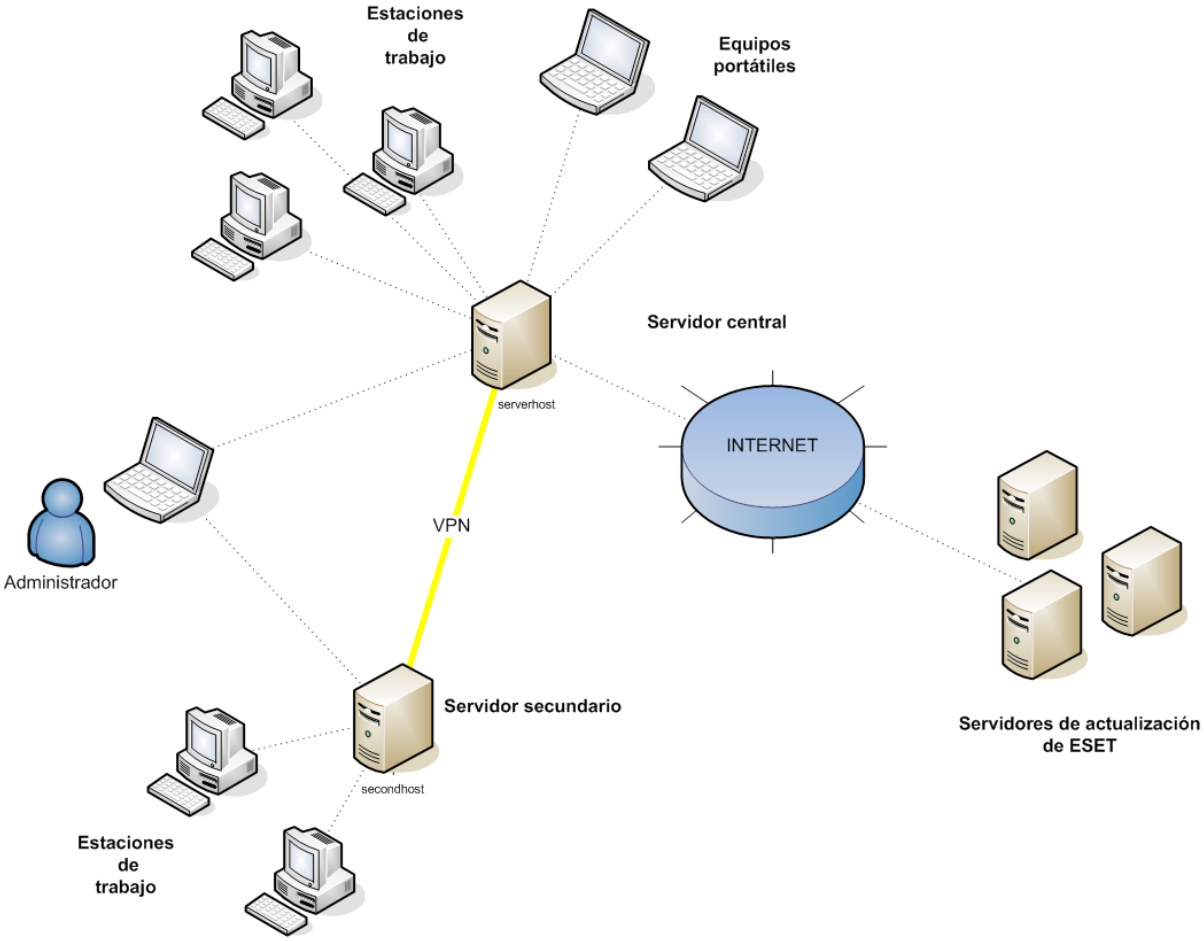


Figura 2-3

2.3.3 Instalación

2.3.3.1 Instalación en la sede

Las instalaciones de ERAS, ERAC y estaciones de trabajo cliente son muy similares a los casos anteriores. La única diferencia radica en la configuración del ERAS maestro (GHOST). En **Herramientas > Opciones del servidor... > Replicación**, active la casilla de verificación **Activar replicación "desde"** e indique el nombre del servidor secundario en **Servidores permitidos**. En nuestro ejemplo, el servidor inferior se llama LITTLE.

Si existe una contraseña de replicación definida en el servidor superior (**Herramientas > Opciones del servidor... > Seguridad > Contraseña para la replicación**), esa misma contraseña se utilizará para la autentificación del servidor inferior.

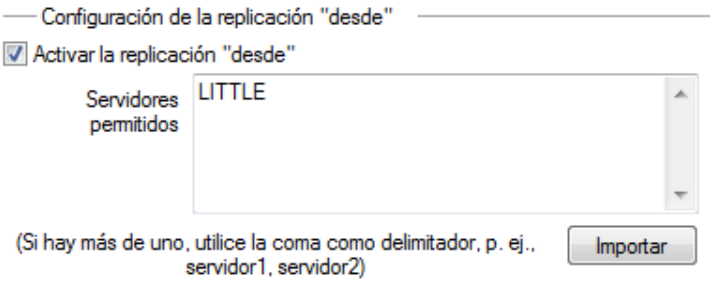


Figura 2-4

2.3.3.2 Sucursal: instalación del servidor ERA

Como en el anterior ejemplo, instale el ERAS y la ERAC secundarios. De nuevo, active y configure la configuración de replicación. En esta ocasión, active la casilla de verificación **Activar replicación "a"** (**Herramientas> Opciones del servidor... > Replicación**) y defina el nombre del ERAS maestro. Se recomienda utilizar la dirección IP del servidor maestro[1], la cual es la dirección IP del servidor GHOST.

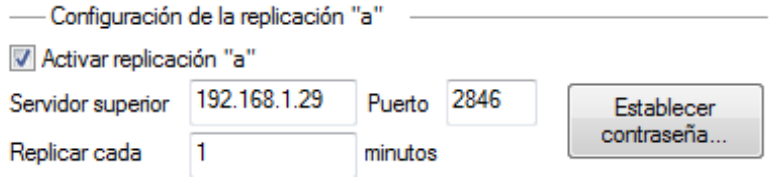


Figura 2-5

2.3.3.3 Sucursal: instalación del servidor HTTP local de actualización

También se puede utilizar aquí la configuración de instalación del servidor local de actualización del caso anterior. Los únicos cambios se producen en las secciones que definen el nombre de usuario y la contraseña.

Como se ve en la Figura 2-3, las actualizaciones para la sucursal no se descargan de los servidores de actualización de ESET, sino del servidor de la sede (GHOST). La fuente de actualización se define por la dirección URL siguiente:

http://ghost:2221 (o http://IP_dirección_de_ghost:2221)

De forma predeterminada, no es necesario especificar un nombre de usuario ni una contraseña, porque el servidor HTTP integrado no requiere autentificación.

Para obtener más información acerca de la configuración del servidor local de actualización en ERAS, consulte la sección 7.3, "Servidor local de actualización".

[1] Para evitar posibles problemas de traducción de DNS al convertir nombres en direcciones IP entre redes (en función de la configuración de DNS).

2.3.3.4 Sucursal: instalación remota en clientes

Una vez más, se puede utilizar el modelo anterior, excepto que se pueden realizar todas las operaciones con la ERAC conectada directamente a la ERAS de la sucursal (LITTLE)[2].

2.3.4 Otros requisitos para los entornos empresariales

En las redes más grandes, se pueden instalar varios servidores ERA para realizar instalaciones remotas de equipos cliente a partir de servidores que son más accesibles. Para ello, el ERAS ofrece la "replicación" (consulte las secciones 2.3.3.1 y 2.3.3.2), que permite que la información almacenada se reenvíe a un ERAS principal ("servidor superior"). La replicación se puede configurar mediante la ERAC.

La función de replicación es muy útil para empresas con varias sucursales u oficinas remotas. Este sería el escenario de implantación del modelo: Instale el ERAS en cada oficina y realice la replicación de cada uno de ellos hacia un ERAS central. La ventaja de esta configuración resulta especialmente interesante en redes privadas conectadas a través de VPN, que son generalmente más lentas. El administrador sólo tendrá que conectarse a un ERAS central (la comunicación que se indica con la letra A en la figura 2-6). No es necesario utilizar la VPN para acceder a departamentos individuales (comunicaciones B, C, D y E). Se evita utilizar el canal de comunicación más lento gracias al uso de la replicación del ERAS.

La configuración de replicación permite al administrador definir qué información se transferirá a los servidores superiores automáticamente en un intervalo predefinido y qué información se enviará a petición desde el administrador del servidor superior. La replicación hace de ERA una aplicación más intuitiva y también minimiza el tráfico de red.

Otra ventaja de la replicación es que varios usuarios pueden iniciar sesión con distintos niveles de permiso.
El administrador que accede al ERAS london2.company.com con la consola (comunicación E) sólo puede controlar los clientes que se conecten a london2.company.com. El administrador que accede a central company.com (A) puede controlar todos los clientes ubicados en la sede de la empresa y en los departamentos/sucursales.

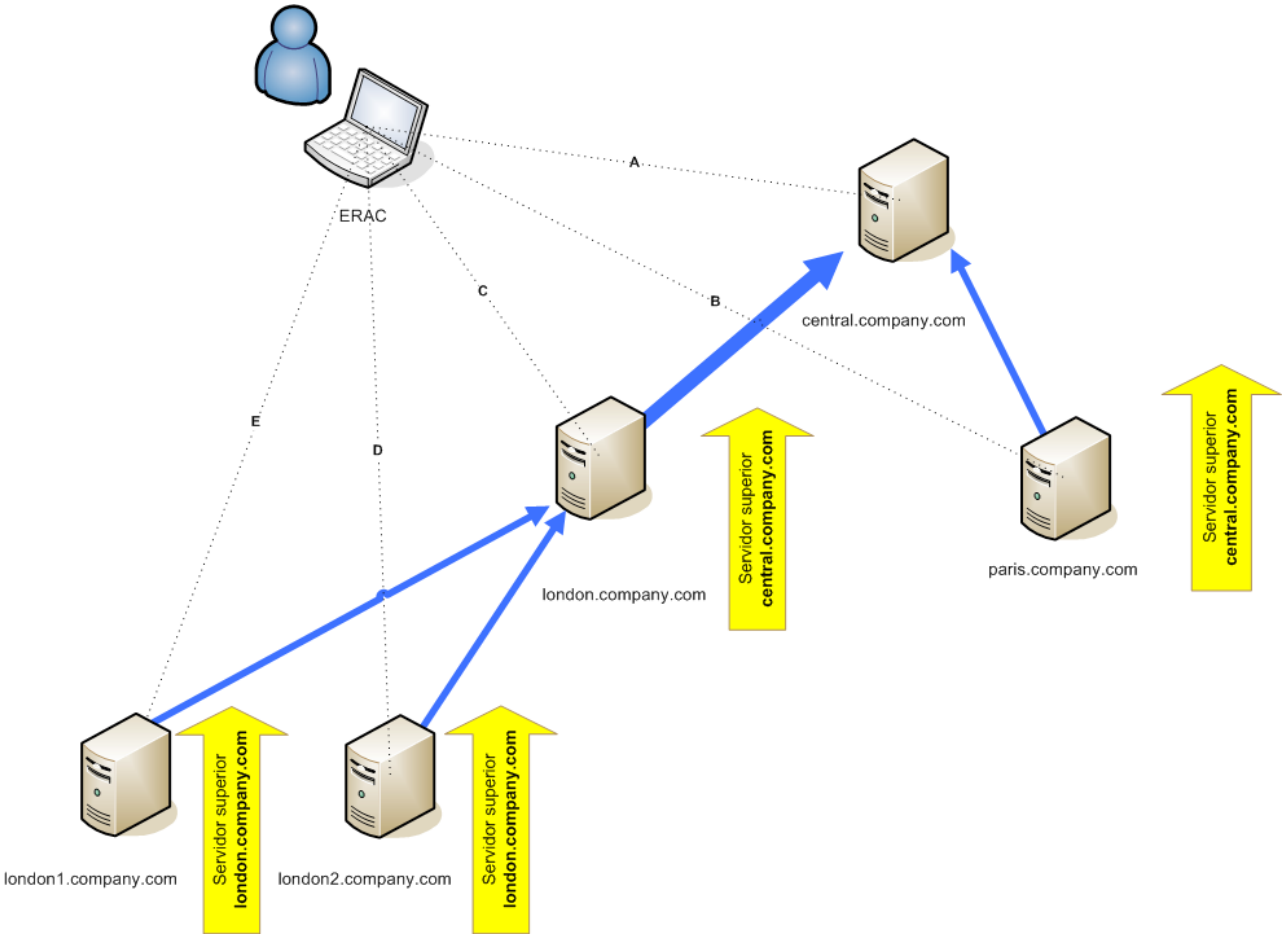


Figura 2-6

[2] Esto se hace para evitar que los paquetes de instalación se transfieran a través del canal VPN, lo que supone un proceso más lento.

3. Trabajo con ERAC

3.1 Conexión al ERAS

La mayoría de las características de la ERAC sólo están disponibles después de conectarse al ERAS. Especifique el servidor mediante el nombre o la dirección IP antes de conectarse:

Abra la ERAC, haga clic en **Archivo > Modificar conexiones...** (o **Herramientas > Opciones de la consola...**) y haga clic en la ficha **Conexión**.

Haga clic en el botón **Agregar o Quitar...** para agregar nuevos servidores de ERA, o bien para modificar los que ya están dentro de la lista. Elija el servidor que desee en el menú desplegable **Seleccionar conexión**. A continuación, haga clic en el botón **Conectar**.

Otras opciones de esta ventana:

- **Conectar con el servidor seleccionado al iniciar la consola**
  Si se selecciona esta opción, la consola se conectará automáticamente con el ERAS al iniciarse.
- **Mostrar mensaje cuando se produzca un error de conexión**
  Si se produce un error de comunicación entre la ERAC y el ERAS, se muestra una alerta.

Las conexiones se pueden proteger mediante contraseñas. Para conectarse a un ERAS no se requiere ninguna contraseña de forma predeterminada, pero le recomendamos encarecidamente que se establezca una. Para crear una contraseña para conectarse a un ERAS:

Haga clic en **Archivo > Cambiar contraseña...** y, a continuación, haga clic en el botón **Cambiar...** situado a la derecha de **Contraseña para la consola**.

Al escribir una contraseña, hay una opción para **Recordar contraseña**. Le rogamos que sopese los riesgos para la seguridad que supone utilizar esta opción. Para eliminar todas las contraseñas guardadas, haga clic en **Archivo > Borrar contraseñas en caché...**

Cuando esté establecida la comunicación, el encabezado del programa cambiará a *Conectado [nombre_del_servidor]*. También puede hacer clic en **Archivo > Conectar** para conectarse al ERAS.
Al iniciarse el programa, seleccione el **Tipo de acceso** en el menú desplegable **Acceso**, ya sea de **Administrador** o **Sólo lectura**).

3.2 ERAC – ventana principal

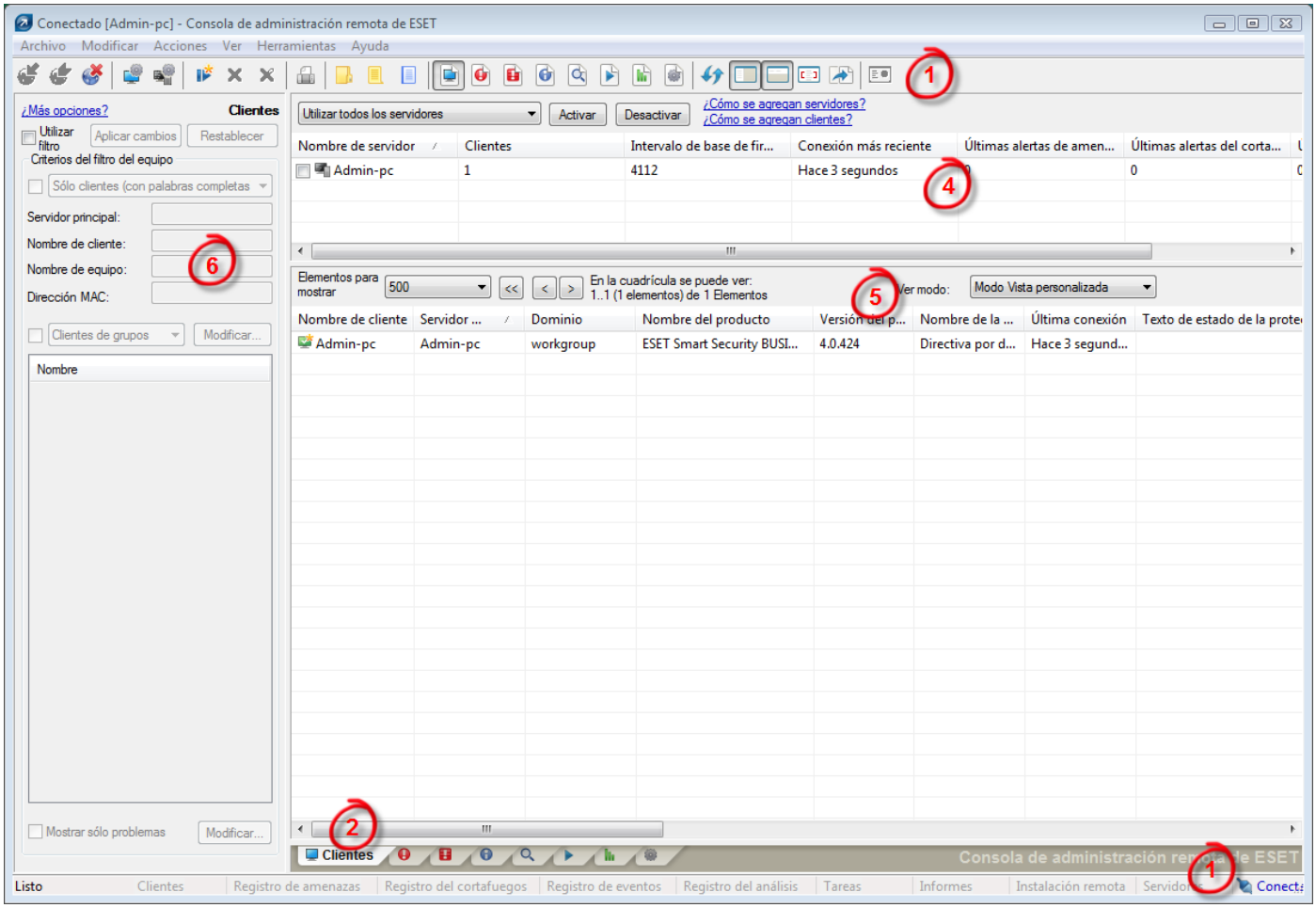


Figura 3-1 Ventana principal de la consola ESET Remote Administrator

El estado de comunicación actual entre la ERAC y el ERAS se muestra en la barra de estado (1). Todos los datos necesarios del ERAS se actualizan regularmente (cada minuto, de forma predeterminada. Consulte **Herramientas > Opciones de la consola...**). También se puede ver el progreso de la actualización en la barra de estado.

NOTA: *pulse F5 para actualizar los datos que se muestran.*

La información se divide en varias fichas, siguiendo un orden de importancia (2). En la mayoría de los casos, se pueden ordenar los datos de forma ascendente o descendente, haciendo clic en un atributo (5) y realizando de forma simultánea una operación de arrastrar y soltar para la reorganización. Si se van a procesar varias filas de datos, puede limitarlas utilizando el menú desplegable **Elementos para mostrar** y los botones de **exploración página a página**. Seleccione el modo Vista para mostrar los atributos en función de sus necesidades (para obtener más información, consulte la sección 3.3, "Filtrado de la información").

El apartado Servidor (4) es importante si replica servidores ERA. Esta sección muestra información de resumen acerca de la consola a la que el ERAS está conectado, así como datos acerca de los servidores ERA secundarios o "inferiores". El menú desplegable Servidores de la sección 4 influenciará el enfoque de la información que se muestra en la sección 5.

- **Usar todos los servidores**
  Muestra información procedente de todos los servidores ERA – apartado (5).

- **Usar sólo los servidores seleccionados**
  Muestra información procedente de servidores ERA seleccionados – apartado (5).

- **Excluir los servidores seleccionados**
  Excluye la información de servidores ERA seleccionados.

Columnas del apartado 4:

- **Nombre de servidor**
  Muestra el nombre del servidor.
- **Clientes**
  Número total de clientes conectados a o presentes en la base de datos del ERAS seleccionado.
- **Rango de bases de firmas de virus**
  Versión de las bases de firmas de virus entre los clientes del ERAS seleccionado.
- **Conexión menos reciente**
  Versión más antigua de las bases de firmas de virus entre los clientes del ERAS seleccionado.
- **Últimas alertas de amenaza**
  Número total de alertas de virus (consulte el atributo **Última alerta de amenaza** en la sección 5).
- **Últimas alertas de cortafuegos**
  Número total de alertas de cortafuegos.
- **Últimas advertencias de suceso**
  Número total de sucesos actuales (consulte el atributo **Último suceso** de la sección 5).

Si no está actualmente conectado, puede hacer clic con el botón secundario en el apartado Servidor (4) y seleccionar **Conectar con este servidor** para conectar con un ERAS determinado.

Se mostrará más información en el apartado Servidor (4) si la replicación está activada.

Se puede acceder a las funciones más importantes de la ERAC desde el menú principal o desde la barra de herramientas de la ERAC (3).

El último apartado es **Criterios del filtro del equipo** (6) – consulte el apartado 3.3, "Filtrado de la información".

3.3 Filtrado de la información

La ERAC proporciona varias herramientas y características que hacen posible que el usuario administre fácilmente los clientes y eventos.

3.3.1 Grupos

Los clientes individuales se pueden dividir en grupos haciendo clic en **Herramientas > Editor de grupos...** en la ERAC. Se pueden usar grupos más tarde al aplicar filtros o crear tareas. Los grupos son independientes de cada ERAS y no son replicados. La función **Sincronizar con Active Directory** en el Editor de grupos permite al administrador clasificar los clientes en grupos, siempre que el nombre del cliente sea igual al tipo de objeto "equipo" en el lado de Active Directory (AD) y pertenezca a grupos de AD.

NOTA: *para que el ERAS pueda sincronizarse con Active Directory, no es necesario que el ERAS esté instalado en el controlador de dominio. El único requisito es que sea posible acceder al controlador de dominio desde el equipo en el que esté ubicado el ERAS. Para configurar la autentificación en el controlador de dominio, acceda a* ***Herramientas > Opciones del servidor > Otras opciones > Modificar opciones avanzadas > ESET Remote Administrator > Servidor ERA > Configuración > Active Directory****. El formato del nombre del servidor es LDAP://nombredeservidor o GC://nombredeservidor. Si está vacío, se utiliza un catálogo global (GC).*

Para obtener más información sobre la administración de los grupos y la sincronización con AD en el nivel de unidad organizativa (como departamento de asistencia técnica, departamento de marketing, etc.), consulte la sección 5.2, "Grupos".

3.3.2 Filtro

El filtrado permite al administrador visualizar solamente la información relacionada con unas estaciones de trabajo o unos servidores concretos. Para mostrar las opciones de filtrado, haga clic en **Ver > Mostrar u ocultar panel de filtro** del menú ERAC.

Para activar el filtrado, seleccione la opción **Utilizar filtro** de la parte superior izquierda de la ERAC y haga clic en el botón **Aplicar cambios**. Todas las modificaciones futuras a los criterios de filtro actualizarán automáticamente los datos mostrados, salvo que se configure de otro modo en la ficha **Herramientas > Opciones de la consola... > Otras opciones**. En el apartado **Criterios del filtro del equipo**, defina los criterios de filtrado (**Servidor principal, Nombre del cliente, Nombre del equipo, Dirección MAC**).

En el apartado **Criterios del filtro del equipo**, puede filtrar los clientes/servidores ERA siguiendo los criterios siguientes:

- **Sólo clientes (con palabras completas)**
  El resultado incluye sólo los clientes con nombres idénticos a la cadena de caracteres.
- **Sólo clientes que comiencen por (?,*)**
  El resultado sólo incluirá a los clientes cuyos nombres empiecen por la cadena de caracteres especificada.
- **Sólo clientes que contengan (?,*)**
  El resultado sólo incluirá a los clientes cuyos nombres contengan la cadena de caracteres especificada.
- **Excluir clientes (con palabras completas), Excluir clientes que comiencen por (?,*), Excluir clientes que contengan (?,*)**
  Estas opciones producirán los resultados opuestos a los tres anteriores.

Los campos Servidor principal, Nombre de cliente, Nombre de equipo y dirección MAC admiten cadenas de caracteres completas. Si cualquiera de estos campos está rellenado, se ejecuta una consulta de base de datos en función del campo rellenado. Se usa el operador lógico *AND*.

El apartado siguiente permite el filtrado de clientes por grupos:

- **Clientes en grupos**
  Sólo muestra a clientes pertenecientes al grupo (o grupos) especificado.
- **Clientes de otros grupos o N/D**
  El resultado sólo incluirá a clientes pertenecientes a otros grupos o clientes que no sean miembros de ningún grupo. Se mostrará si un cliente pertenece a grupos especificados y no especificados.
- **Clientes sin grupos**
  Sólo se muestran los clientes que no forman parte de ningún grupo.

La última opción incluye un filtrado por problema (el resultado incluirá los clientes con el tipo de problema especificado). Para mostrar la lista de problemas, seleccione la opción **Mostrar sólo problemas** y haga clic en **Modificar...** Seleccione los problemas que desea mostrar y haga clic en **Aceptar** para mostrar los clientes con los problemas seleccionados.

Todos los cambios que se realicen en la configuración de filtrado se aplicarán después de hacer clic en el botón **Aplicar cambios.** Para restablecer los valores predeterminados, haga clic en **Restablecer.** Para crear automáticamente nuevos resultados con cada modificación de la configuración de filtrado, seleccione la opción **Herramientas > Opciones de la consola... > Otras opciones... > Aplicar cambios automáticamente**.

3.3.3 Menú contextual

Utilice el botón derecho del ratón para invocar el menú contextual y ajustar los elementos de las columnas. Las opciones del menú contextual incluyen:

- **Seleccionar todo**
  Selecciona todas las entradas.
- **Seleccionar por "..."**
  Esta opción le permite hacer clic con el botón secundario sobre cualquier atributo y seleccionar, de forma automática (resaltándolas), todas las demás estaciones de trabajo o servidores con ese mismo atributo. La cadena de caracteres ... se sustituye automáticamente por el valor de la ficha actual.
- **Selección inversa**
  Realiza una selección inversa de las entradas.
- **Ocultar seleccionados**
  Oculta las entradas seleccionadas.
- **Ocultar no seleccionados**
  Oculta todas las entradas no seleccionadas de la lista.

Las dos últimas opciones son efectivas si se necesita más organización después de usar los métodos de filtrado anteriores. Para desactivar todos los filtros definidos por el menú contextual, haga clic en **Ver > Vista recortada** o haga clic en el icono  de la barra de herramientas de la ERAC. También puede pulsar **F5** para actualizar la información que se muestra y desactivar los filtros.

Ejemplo:

- Para que sólo se muestren clientes con alertas de amenazas:
  En la ficha **Clientes**, haga clic con el botón derecho en cualquier panel vacío con Última alerta de virus y, en el menú contextual, elija **Seleccionar por "..."**. A continuación, también en el menú contextual, haga clic en **Ocultar seleccionados**.

- Para mostrar las alertas de amenazas de los clientes "Joseph" y "Charles":
  Haga clic en la ficha **Registro de amenazas** y haga clic con el botón derecho en cualquier atributo de la columna Nombre del cliente que tiene el valor Joseph. En el menú contextual, haga clic en **Seleccionar por "Joseph"**. A continuación, mantenga pulsada la tecla CTRL, haga clic con el botón secundario y luego haga clic en **Seleccionar por "Charles"**. Por último, haga clic con el botón secundario y, en el menú contextual, seleccione **Ocultar no seleccionados** y suelte la tecla CTRL.

La tecla CTRL se puede utilizar para seleccionar y anular la selección de entradas específicas, la tecla MAYÚS se puede usar para marcar y desmarcar un grupo de entradas.

NOTA: *el filtrado también se puede usar para simplificar la creación de nuevas tareas para clientes específicos (resaltados). Existen muchas formas de usar el filtrado de forma efectiva, pruebe con varias combinaciones.*

Vistas

En la ficha **Clientes** el número de columnas que se muestran se pueden ajustar usando el menú desplegable **Modo vista** en la parte más a la derecha de la consola. El **Modo vista completa** muestra todas las columnas, mientras el **Modo vista mínima** sólo muestra las columnas más importantes. Estos modos están predefinidos y no pueden modificarse. Para activar la vista personalizada, seleccione **Modo vista personalizada**. Se puede configurar en la ficha **Herramientas > Opciones de la consola... > Mostrar u ocultar columnas**.

3.4 Fichas de la ERAC

3.4.1 Descripción general de las fichas y los clientes

La mayoría de la información de las fichas está relacionada con los clientes conectados. Cada cliente conectado a ERAS se identifica con los atributos siguientes:
Nombre del equipo (nombre del cliente) + Dirección MAC + Servidor principal[3]

El comportamiento del ERAS en relación con algunas operaciones de red (como el cambio de nombre de un PC) se puede definir en la configuración avanzada de ERAS. Puede ayudar a evitar la duplicación de entradas en la ficha **Clientes**. Por ejemplo, si se ha cambiado el nombre de uno de los ordenadores de la red, pero se ha mantenido su dirección MAC, puede evitar que se cree una nueva entrada en la ficha **Clientes**.

Los clientes que se conecten al ERAS por primera vez presentan el valor **Sí** en la columna **Usuario nuevo**. También están señalados con un pequeño asterisco en la esquina superior derecha del icono del cliente (consulte la Figura 3-2). Esta función permite al administrador detectar fácilmente un equipo de nueva conexión. Este atributo puede tener significados diferentes en función de los procedimientos operativos del administrador.

Figura 3-2

Si se ha configurado un cliente y se ha movido a un grupo determinado, el estado nuevo se puede desactivar haciendo clic con el botón secundario en el cliente y seleccionando **Establecer/restablecer indicadores > Restablecer marca "Nuevo"**. El icono del cliente cambiará al que se muestra en la Figura 3-3 y el atributo **Usuario nuevo** cambiará a **No.**

Figura 3-3

NOTA: *el atributo Comentario es opcional en las tres fichas. El administrador puede insertar cualquier descripción aquí (por ejemplo, "Despacho n.º 129").*

Los valores temporales del ERAS se pueden mostrar en modo relativo ("Hace 2 días"), en modo absoluto (20. 5. 2008) o en el modo del sistema (configuración regional).

---

[3] En versiones anteriores de ERA, los clientes se identificaban con los atributos siguientes: Nombre de equipo + Servidor principal

En la mayoría de los casos, se pueden ordenar los datos de forma ascendente o descendente, haciendo clic en un atributo (5) y realizando de forma simultánea una operación de arrastrar y soltar para la reorganización.

Al hacer clic en determinados valores, se activan otras fichas para mostrar información más detallada. Por ejemplo, si hace clic en un valor en la columna **Última alerta de amenaza**, el programa se moverá a la ficha **Registro de amenazas** para mostrar las entradas del registro de amenazas relacionadas con el cliente determinado. Si hace clic en un valor que contiene demasiada información para mostrar en una vista de ficha, se abrirá una ventana de diálogo mostrando la información detallada acerca del cliente correspondiente.

3.4.2 Replicación e información en fichas individuales

Si la ERAC está conectada a un ERAS que está funcionando como servidor superior, toda la información de los servidores inferiores se mostrará automáticamente, salvo que el servidor inferior no esté configurado para ello.

En este caso, podrían faltar los datos siguientes:

- Registros de alertas detalladas (ficha **Registro de amenazas**)
- Registros del análisis a petición (ficha **Registro de análisis**)
- Configuración del cliente actual detallada en formato .xml (ficha **Clientes**, columna **Configuración**, **Estado de la protección, Características de protección, Información del sistema**)

También es posible que falte la información del programa ESET SysInspector. ESET SysInspector está integrado con los productos de generación 4.x y superior de ESET.

En la ventana de diálogo en la que esta información estaría presente en otros casos, se muestra el botón **Solicitar** (**Acciones > Propiedades > Configuración**). Al hacer clic en este botón, se descarga la información que falta a través de un ERAS inferior. Puesto que la replicación se inicia siempre en un ERAS inferior, la información que falta se entregará dentro del intervalo de replicación predefinido.

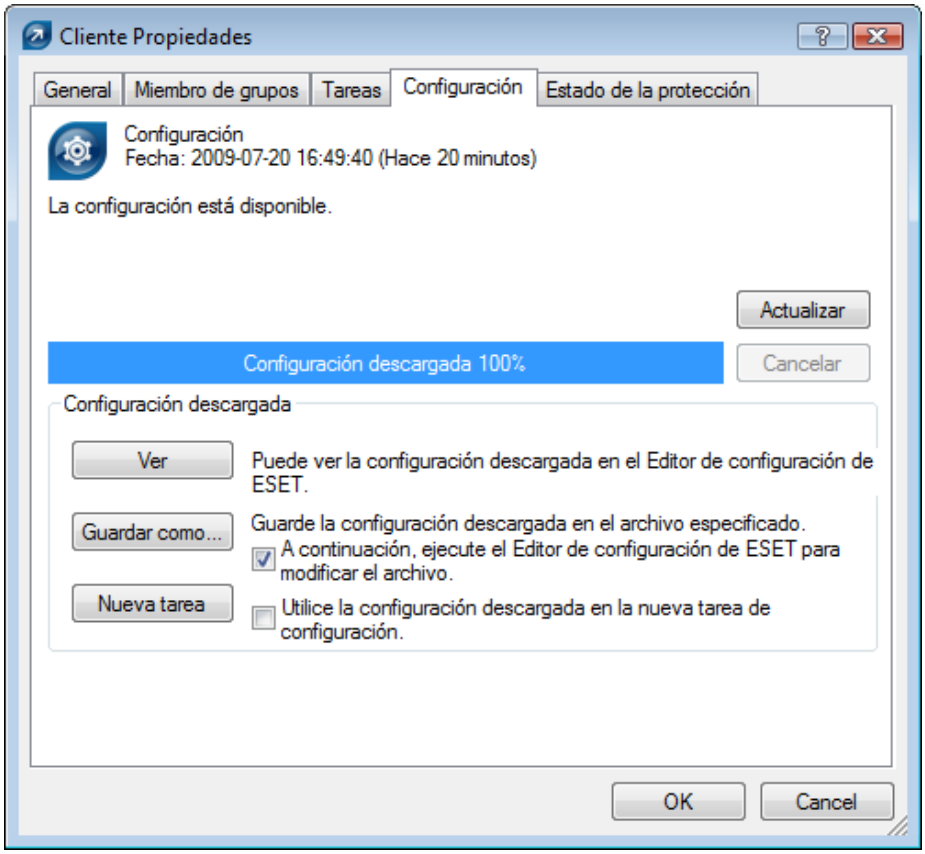


Figura 3-4 Haga clic en Solicitar para recuperar la información que falte de servidores ERA inferiores.

3.4.3 Ficha Clientes

Esta ficha muestra información general acerca de clientes individuales.

Atributo	Descripción
Nombre de equipo	Nombre de la estación de trabajo o del servidor (nombre de host)
Dirección MAC	Dirección MAC (adaptador de red)
Servidor principal	Nombre del ERAS con el que un cliente se está comunicando
Dominio	Dominio o nombre de grupo al que pertenece un cliente (no son grupos creados en ERAS)
IP	Dirección IP
Nombre del producto	Nombre del producto de seguridad ESET
Versión del producto	Versión del producto de seguridad ESET
Nombre de la directiva	Nombre de la directiva asignada a un cliente
Última conexión	Hora en la que el cliente se conectó por última vez al ERAS (todos los demás datos recogidos de los clientes incluyen esa marca de tiempo, excepto algunos datos obtenidos mediante replicación)
Texto de estado de la protección	El estado actual del producto de seguridad de ESET instalado en un cliente.
Base de firmas de virus	Versión de una base de datos de firmas de virus
Última alerta de amenaza	Última incidencia de virus
Última alerta del cortafuegos	Último suceso detectado por el cortafuegos personal de ESET Smart Security (se muestran los sucesos del nivel Advertencia y superiores)
Última advertencia de suceso	Último mensaje de error
Últimos archivos analizados	Número de archivos analizados durante el último análisis a petición
Últimos archivos infectados	Número de archivos infectados durante el último análisis a petición
Últimos archivos limpiados	Número de archivos limpiados (o eliminados) durante el último análisis a petición
Última fecha de análisis	Fecha del último análisis a petición
Solicitud de reinicio	¿Es necesario reiniciar (por ejemplo, después de la actualización de un programa)?
Fecha de solicitud de reinicio	Fecha de la primera solicitud de reinicio
Último producto iniciado	Hora en que se ejecutó el programa cliente por última vez
Fecha de instalación del producto	Fecha en la que se instaló el producto de seguridad de ESET en el cliente
Usuario móvil	Los clientes con este atributo realizarán la tarea "actualizar ahora" cada vez que establezcan una conexión con el ERAS (opción recomendada para los portátiles)
Nuevo cliente	¡Equipo de reciente conexión (consulte la sección 3.4.1, "Descripción general de las fichas y los clientes")
Nombre del sistema operativo	Nombre del sistema operativo cliente
Sistema operativo	Plataforma de sistema operativo (Windows, Linux, etc.).
Plataforma de hardware	32-bits / 64-bits
Configuración	Configuración actual del cliente en .xml (incluye la fecha y hora de creación de la configuración)
Estado de la protección	Indicación general de estado (de naturaleza parecida al atributo Configuración)
Características de protección	Indicación general de estado de los componentes del programa (parecida al atributo Configuración)
Información del sistema	El cliente envía información del sistema al ERAS (incluida la hora de envío de la información de sistema)
SysInspector	Los clientes con versiones que contengan la herramienta ESET SysInspector pueden enviar registros desde esta aplicación complementaria.
Información personalizada	Información personalizada para mostrar, especificada por el administrador (esta opción se puede configurar en ERAC a través de ***Herramientas > Opciones del servidor... > ficha Otras opciones > Modificar configuración avanzada... > ESET Remote Administrator > Servidor ERA > Configuración > Otras opciones > Información personalizada del cliente***).
Comentarios	Un comentario corto que describe el cliente (escrito por el administrador)

NOTA: *algunos valores sólo tienen fines informativos y pueden dejar de ser actuales cuando el administrador los visualiza en la consola. Por ejemplo, tal vez se haya producido un error en una actualización a las 7:00 horas, pero a las 8:00 horas se ha realizado correctamente. Estos valores pueden incluir datos de* **Última alerta de amenaza** *y de* **Última advertencia de suceso**. *Si el administrador procesa esta información y sabe que está obsoleta, se puede borrar haciendo clic con el botón secundario y seleccionando* **Borrar información > Borrar información de la "Última alerta de amenaza"** *o* **Borrar la información de "Última alerta de amenaza"**. *Se eliminará la información relativa al último incidente relacionado con virus o al último suceso del sistema.*

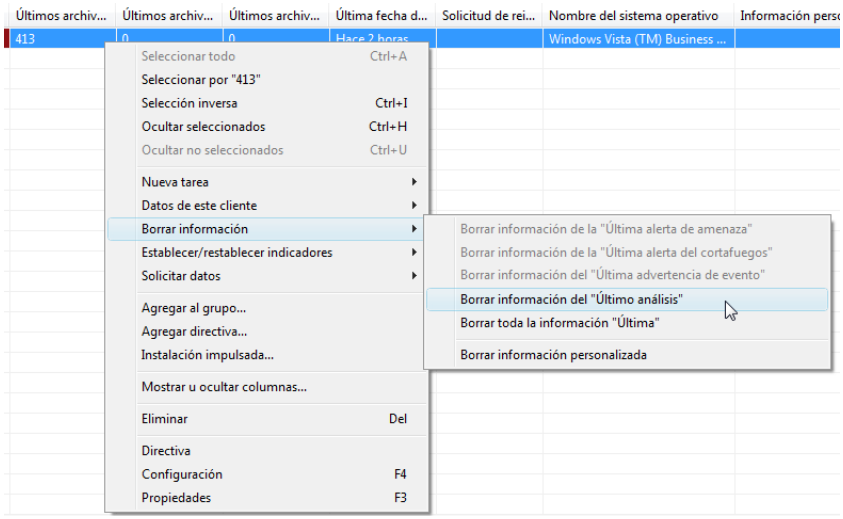


Figura 3-5 Los sucesos obsoletos de las columnas Última alerta de amenaza y Última advertencia de suceso se pueden quitar fácilmente.

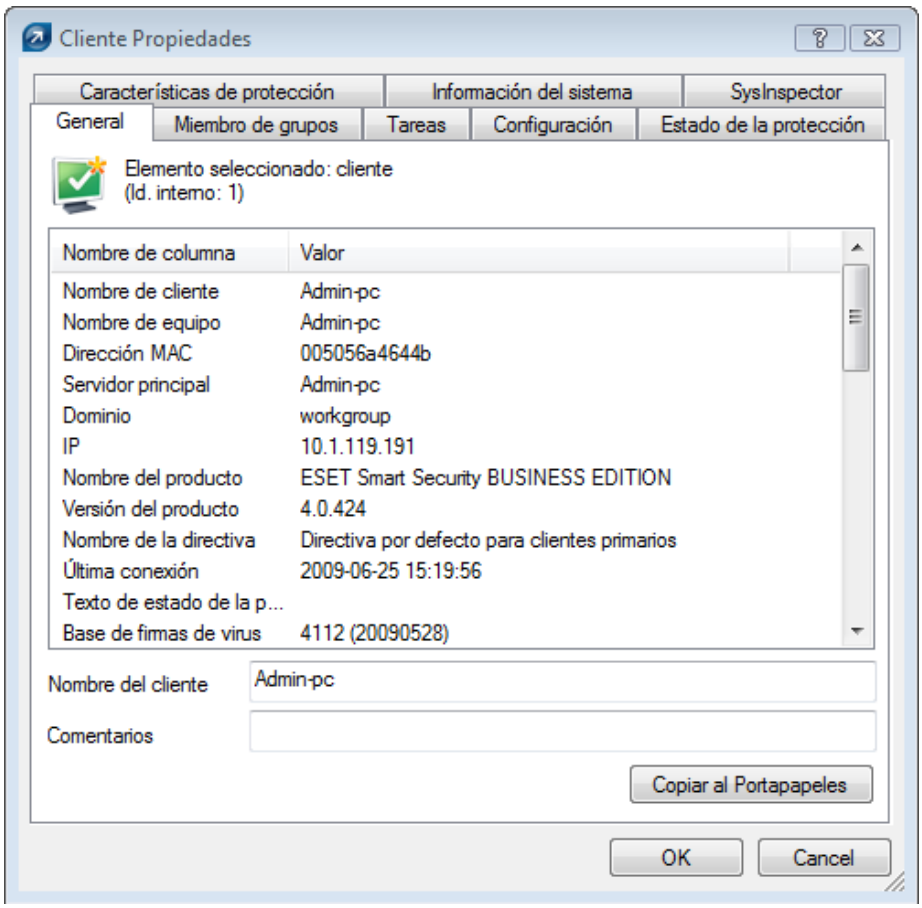


Figura 3-6 Información detallada sobre una estación de trabajo cliente.

La ficha **Clientes** proporciona varias opciones después de hacer doble-clic en un cliente:

- **General**
  Contiene información similar a la que se muestra en la ficha **Clientes**. Aquí puede especificar el **Nombre de cliente**, el nombre bajo el que el cliente es visible en ERA, además de un comentario opcional.

- **Miembro de grupos**
  Esta ficha muestra una lista de todos los grupos a los que pertenece el cliente. Para obtener más información, consulte la sección 3.3, "Filtrado de la información".

- **Tareas**
  Tareas relacionadas con el cliente en cuestión. Para obtener más información, consulte la sección 5.1, "Tareas".

- **Configuración**
  Esta ficha le permite ver o exportar a un archivo .xml la configuración actual del cliente. En secciones posteriores de este manual explicaremos cómo pueden utilizarse los archivos .xml para crear una plantilla de configuración para los archivos de configuración .xml nuevos o modificados. Para obtener más información, consulte la sección 5.1, "Tareas".

- **Estado de la protección**
  Indicación general de estado relativa a todos los programas de ESET. Algunas de estas indicaciones son interactivas, por lo que es posible intervenir de forma inmediata. Esta funcionalidad es útil, ya que evita que haya que definir manualmente una tarea nueva para solucionar un problema de protección concreto.

- **Características de protección**
  Estado de los componentes de todas las características de seguridad de ESET (módulo contra correo electrónico no deseado, cortafuegos personal, etc.)

- **Información del sistema**
  Información detallada acerca del programa instalado, la versión de los componentes del mismo, etc.

- **Ficha SysInspector**
  Información detallada acerca de los procesos de inicio y los procesos que se ejecutan en segundo plano.

3.4.4 Ficha Registro de amenazas

Esta ficha contiene información detallada acerca de incidencias de amenazas o virus individuales.

Atributo	Descripción
Nombre del cliente	Nombre del cliente que informa de la alerta de amenaza
Nombre de equipo	Nombre de la estación de trabajo/servidor (nombre de host)
Dirección MAC	Dirección MAC (adaptador de red)
Servidor principal	Nombre del ERAS con el que un cliente se está comunicando
Fecha de recepción	Fecha y hora a la que ERAS registra el suceso
Fecha de ocurrencia	Fecha y hora a la que se produce el suceso
Nivel	Nivel de alerta
Analizador	Nombre de la característica de seguridad que detectó la amenaza
Objeto	Tipo de objeto
Nombre	Generalmente, una carpeta en la que se ubica la infección
Amenaza	Nombre del código malicioso detectado
Acción	Acción emprendida por la característica de seguridad determinada
Usuario	Nombre del usuario que se identificó al producirse el incidente
Información	Información sobre las amenazas detectadas
Detalles	Estado del envío del registro de clientes

3.4.5 Ficha Registro del cortafuegos

Esta ficha muestra la información relacionada con la actividad del cortafuegos del cliente.

Atributo	Descripción
Nombre del cliente	Nombre del cliente que informa del suceso
Nombre de equipo	Nombre de la estación de trabajo/servidor (nombre de host)
Dirección MAC	Dirección MAC (adaptador de red)
Servidor principal	Nombre del ERAS con el que un cliente se está comunicando
Fecha de recepción	Fecha y hora a la que ERAS registra el suceso
Fecha de ocurrencia	Fecha y hora a la que se produce el suceso
Nivel	Nivel de alerta
Suceso	Descripción del suceso
Origen	Dirección IP fuente
Destino	Dirección IP de destino
Protocolo	Protocolo afectado
Regla	Regla del cortafuegos afectado
Aplicación	Aplicación afectada
Usuario	Nombre del usuario que se identificó al producirse el incidente

3.4.6 Ficha Registro de sucesos

Esta ficha muestra la lista de todos los sucesos relacionados del sistema.

Atributo	Descripción
Nombre del cliente	Nombre del cliente que informa del suceso
Nombre de equipo	Nombre de la estación de trabajo o del servidor (nombre de host)
Dirección MAC	Dirección MAC (adaptador de red)
Servidor principal	Nombre del ERAS con el que un cliente se está comunicando
Fecha de recepción	Fecha y hora a la que ERAS registra el suceso
Fecha de ocurrencia	Fecha y hora a la que se produce el suceso
Nivel	Nivel de alerta
Complemento	Nombre del componente del programa que informa del suceso
Suceso	Descripción del suceso
Usuario	Nombre del usuario relacionado con el suceso

3.4.7 Ficha Registro de análisis

Esta ficha enumera los resultados de los análisis del equipo a petición que se iniciaron de forma remota, en equipos cliente locales o como tareas programadas.

Atributo	Descripción
Nombre del cliente	Nombre del cliente en el que se realizó el análisis
Nombre de equipo	Nombre de la estación de trabajo o del servidor (nombre de host)
Dirección MAC	Dirección MAC (adaptador de red)
Servidor principal	Nombre del ERAS con el que un cliente se está comunicando
Fecha de recepción	Fecha y hora a la que ERAS registra el suceso de análisis
Fecha de ocurrencia	Fecha y hora de ejecución del análisis en un cliente
Destinos analizados	Archivos, carpetas y dispositivos analizados
Analizados	Número de archivos comprobados
Infectados	Número de archivos infectados
Limpiados	Número de objetos limpiados (o eliminados)
Estado	Estado del análisis
Usuario	Nombre del usuario que se identificó al producirse el incidente
Tipo	Tipo de usuario
Analizador	Tipo de análisis
Detalles	Estado del envío del registro de clientes

3.4.8 Ficha Tareas

El significado de esta ficha se describe en el capítulo "Tareas". Están disponibles estos atributos:

Atributo	Descripción
Estado	Estado de la tarea (Activa = se está realizando, Finalizada = tarea entregada a los clientes)
Tipo	Tipo de tarea
Nombre	Nombre de tarea
Descripción	Descripción de tarea
Fecha de implementación	Fecha/hora de ejecución de la tarea
Fecha de recepción	Fecha y hora a la que ERAS registra el suceso
Detalles	Estado del envío del registro de tareas
Comentarios	Un comentario corto que describe el cliente (escrito por el administrador)

3.4.9 Ficha Informes

Esta ficha contiene funciones que se pueden usar para archivar la actividad en la red durante ciertos períodos de tiempo. La ficha **Informes** se usa para organizar la información estadística en forma de gráfico o tabla. Para obtener más información, consulte la sección 6, "Informes".

3.4.10 Ficha Instalación remota

Esta ficha proporciona opciones para distintos métodos de instalación remota de ESET Smart Security o ESET NOD32 Antivirus en clientes. Para obtener más información, consulte la sección 4.2, "Instalación remota".

3.5 Configuración de la consola ERA

La ERAC se puede configurar en el menú **Herramientas > Opciones de la consola**...

3.5.1 Ficha Conexión

Esta ficha se usa para configurar la conexión de la ERAC al ERAS. Para obtener más información, consulte la sección 3, "Trabajo con la ERAC".

3.5.2 Columnas – Ficha Mostrar u ocultar

Esta ficha permite especificar los atributos (columnas) que se muestran en fichas individuales. Los cambios se reflejarán en el Modo vista personalizada (ficha **Clientes**). El resto de modos no se puede modificar.

3.5.3 Ficha Colores

Esta ficha permite asociar diferentes colores con sucesos específicos relacionados con el sistema, de forma que los clientes problemáticos se resalten mejor (resaltado condicional). Por ejemplo, los clientes con una base de firmas de virus levemente desactualizada (**Clientes: versión anterior**) se pueden distinguir de los clientes con una base obsoleta (**Clientes: versiones anteriores o N/D**).

3.5.4 Ficha Rutas

Esta ficha permite especificar el directorio en el que la ERAC guardará los informes descargados del ERAS. De forma predeterminada, los informes se guardan en:

%ALLUSERSPROFILE %\Application Data\Eset\Eset Remote Administrator\Console\reports

3.5.5 Ficha Fecha / Hora

Apariencia de las columnas de fecha/hora:

- **Absoluta**
  La consola mostrará la hora de forma absoluta (por ejemplo, 14:30:00).

- **Relativa**
  La consola mostrará el tiempo de forma relativa (por ejemplo, "Hace 2 semanas").

- **Regional**
  La consola mostrará el tiempo de acuerdo con la configuración regional (en función de la configuración de Windows).

- **Recalcular hora &UTC de la hora local (utilizar hora local)**
  Active esta casilla de verificación para volver a calcular la hora local. En caso contrario, se mostrará la hora GMT – UTC.

3.5.6 Ficha Otras opciones

- **Configuración del filtro > Aplicar cambios automáticamente**
  Si se activa, los filtros de las fichas individuales generarán resultados nuevos con cada modificación de la configuración de filtro. Si no es así, el filtrado se realizará sólo después de hacer clic en el botón **Aplicar cambios**.

- **Actualizaciones de administración remota**
  Esta sección le permite activar la comprobación de nuevas versiones de ESET Remote Administrator. Se recomienda mantener el valor predeterminado de **Mensualmente**. Si hay una versión nueva disponible, la ERAC muestra una notificación al iniciar el programa.

- **Otras opciones > Utilizar actualización automática**
  Si se selecciona, los datos de las fichas individuales se actualizan automáticamente en función del intervalo elegido.

- **Otras opciones > Vaciar papeleras de reciclaje de la consola al salir de la aplicación**
  Seleccione esta opción para vaciar automáticamente los elementos de la papelera de reciclaje interna de la ERAC al salir.
  También puede vaciar los elementos manualmente haciendo clic con el botón secundario sobre ellos desde la ficha ***Informes***.

- **Otras opciones > Mostrar líneas de la cuadrícula**
  Seleccione esta opción para separar las celdas individuales en todas las fichas por cuadrícula.

- **Otras opciones > Mostrar preferentemente el cliente como "Servidor/Nombre" en lugar de "Servidor/Equipo/MAC"**
  Incide en el modo de visualización de los clientes en algunas ventanas de diálogo (por ejemplo, Nueva tarea). Esta opción sólo tiene efectos a nivel visual.

- **Otras opciones > Utilizar icono de systray**
  La consola ERA se representará con un icono en el área de notificación de Windows.

- **Otras opciones > Mostrar en la barra de tareas al estar minimizado**
  Si la ventana de la ERAC está minimizada, será accesible desde la barra de tareas de Windows.

- **Otras opciones > Utilizar icono de Systray resaltado al encontrar clientes problemáticos**
  Seleccione esta opción a la vez que el botón **Modificar** para definir los sucesos que desencadenarán un cambio en el color del icono ERAC en el área de notificación.

Si la ERAC en el PC del administrador se va a conectar siempre al ERAS, se recomienda desactivar la opción **Mostrar en la barra de tareas al estar minimizado** y dejar la consola minimizada cuando esté inactiva. Si ocurre un problema, el icono del área de notificación se volverá rojo, lo cual es una señal para que intervenga el administrador. También se recomienda ajustar la opción **Utilizar icono de Systray resaltado al encontrar clientes problemáticos** para especificar qué sucesos desencadenarán un cambio de color en el icono de la ERAC. Sin embargo, la ERAC se desconectará si se activa la compresión de la base de datos en el servidor.

- **Otras opciones > Mostrar todos los grupos en los paneles de filtro**
  Cambia el filtrado del grupo.

- **Otras opciones > Mensajes del tutorial**
  Activa (Activar todo) o desactiva (Desactivar todo) todos los mensajes de información.

3.6 Modos de visualización

La ERAC ofrece a los usuarios dos modos de visualización:

- Modo administrativo
- Modo de sólo lectura

El **modo administrativo** de la ERAC proporciona al usuario el control total sobre todas las características y configuraciones, así como la capacidad de administrar todas las estaciones de trabajo clientes conectadas a la ERAC.

El **modo de sólo lectura** resulta adecuado para ver el estado de las soluciones de clientes de ESET que se conectan al ERAS. No permite la creación de tareas para las estaciones de trabajo, la creación de paquetes de instalación ni la instalación remota. Tampoco se puede acceder al Administrador de licencias, al Administrador de directivas ni al Administrador de notificaciones. **El modo de sólo lectura** sí permite al administrador que modifique la configuración de la ERAC y genere informes.

El modo de visualización se selecciona cada vez que se inicia la consola en el menú desplegable **Acceso**, mientras que la contraseña para conectarse al ERAS se puede establecer para cualquiera de los modos de visualización. Establecer una contraseña resulta especialmente útil si quiere que algunos usuarios tengan acceso total al ERAS, mientras que otros dispongan de un acceso de sólo lectura. Para establecer la contraseña, haga clic en **Herramientas > Opciones del servidor... > Seguridad** y haga clic en el botón **Cambiar...** situado junto a Contraseña para la Consola (acceso de administrador) o (acceso de sólo lectura).

3.7 Editor de configuración de ESET

El editor de configuración de ESET es un componente importante de la ERAC y se usa para distintos fines. Algunos de los más importantes son la creación de los siguientes elementos:

- Configuración predefinida para los paquetes de instalación
- Configuración que se envía como tareas a los clientes
- Archivo de configuración (.xml) general

El editor de configuración forma parte de la ERAC y consta principalmente de los archivos cfgedit.*.

El editor de configuración permite al administrador configurar de forma remota muchos de los parámetros disponibles en cualquier producto de seguridad ESET, especialmente en los productos instalados en estaciones de trabajo clientes. También permite al administrador exportar la configuración a archivos .xml que se podrán utilizar más tarde para varios fines, como crear tareas en la ERAC, importar una configuración local en ESET Smart Security, etc.

La estructura que el editor de configuración utiliza se vale de una plantilla .xml que almacena la configuración en una estructura de tipo árbol. La plantilla se almacena en el archivo *cfgedit.exe*. Por ello, se recomienda actualizar el ERAS y la ERAC de forma periódica.

Advertencia: *el editor de configuración le permite modificar cualquier archivo .xml. No modifique ni sobrescriba el archivo cfgedit.xml original.*

Para que el editor de configuración funcione, deben estar disponibles los archivos siguientes: *eguiEpfw.dll*, *cfgeditLang.dll*, *eguiEpfwLang.dll y eset.chm*.

3.7.1 Capa de configuración

Si se cambia un valor en el editor de configuración, el cambio se muestra con un símbolo azul. Las entradas con icono gris no se han modificado y no se escribirán en la nueva configuración .xml.

Cuando se aplique una configuración en clientes, sólo se aplicarán las modificaciones guardadas en el nuevo archivo de configuración .xml (), todos los demás elementos () permanecerán sin cambios. Con ello se permite la aplicación gradual de distintas configuraciones sin tener que deshacer modificaciones anteriores.

Se muestra un ejemplo en la Figura 3-7. En esta configuración, se inserta el nombre de usuario AV-1234567 y la contraseña y se prohíbe el uso de un servidor proxy.

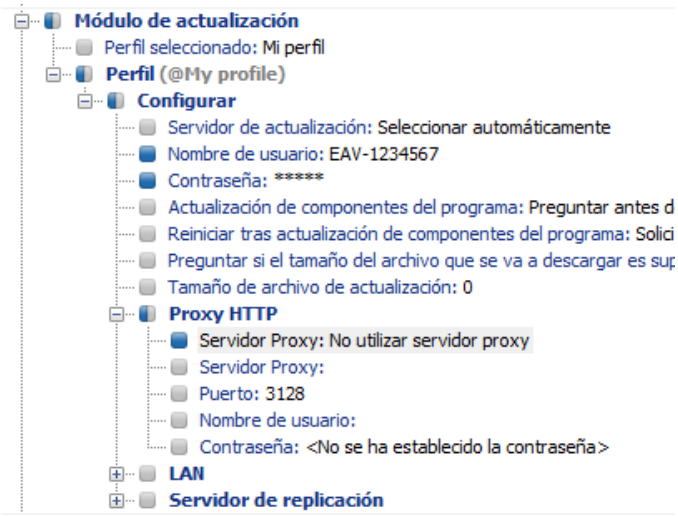


Figura 3-7

La segunda configuración (Figura 3-8) que se envía a los clientes garantizará que conserven las modificaciones anteriores, incluido el nombre de usuario EAV–1234567 y la contraseña, pero también permitirá el uso de un servidor proxy, definiendo la dirección y el puerto correspondientes.

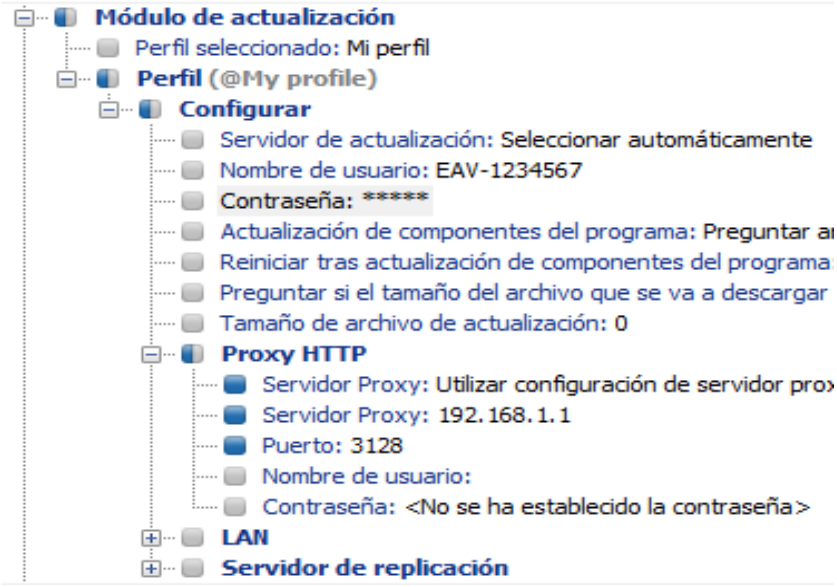


Figura 3-8

3.7.2 Entradas de configuración clave

En esta sección, explicaremos varias entradas de configuración clave para ESET Smart Security y ESET NOD32 Antivirus, disponibles a través del editor de configuración de ESET:

- **ESET Smart Security, ESET NOD32 Antivirus > Kernel de ESET > Configuración > Administración remota**
  Desde aquí puede activar la comunicación entre equipos cliente y el ERAS (**Conectar con servidor de administración remota**). También puede indicar el nombre o la dirección o IP del ERAS (**Dirección del servidor**). La opción **Intervalo entre conexiones al servidor** debe mantenerse con el valor predeterminado de cinco minutos. Para poder realizar pruebas, se puede reducir este valor hasta 0, lo que establecerá una conexión cada diez segundos. Si se establece una contraseña, utilice la contraseña que se especificó en el ERAS. Para obtener más información, consulte la opción **Contraseña para clientes** en la sección 7.1, "Ficha Seguridad". También encontrará información adicional sobre la configuración de la contraseña en esta sección.

- **Kernel de ESET > Configuración > Claves de licencias**
  Los equipos clientes no requieren la administración o adición de claves de licencia. Las claves de licencia sólo se usan para los productos de servidor.

- **Kernel de ESET > Configuración > Threatsense.Net**
  Este apartado define el comportamiento del sistema de alerta temprana ThreatSense.Net, que permite el envío de archivos sospechosos para someterlos al análisis de los laboratorios de ESET. Cuando se implanten las soluciones de ESET en una red amplia, las opciones **Enviar archivos sospechosos** y **Activar envío de información estadística anónima** resultan de especial relevancia. Si se definen como **No enviar** o **No**, respectivamente, el sistema ThreatSense.Net estará totalmente desactivado. Para enviar archivos de forma automática sin requerir la intervención del usuario, seleccione **Enviar sin preguntar** y **Sí**, respectivamente. Si se usa un servidor proxy con conexión a Internet, especifique los parámetros de conexión en **Kernel de ESET > Configuración > Servidor proxy**.
  De forma predeterminada, los productos del cliente remiten los archivos sospechosos al ERAS, quien los remite a su vez a los servidores de ESET. Por ello, es necesario configurar correctamente el servidor proxy en ERAS (**Herramientas > Opciones del servidor > Otras opciones > Modificar configuración avanzada > Servidor ERA > Configuración > Servidor proxy**).

- **Kernel > Configuración > Proteger parámetros de configuración**
  Permite al administrador proteger mediante contraseña los parámetros configurados. Si se establece una contraseña, ésta se requerirá para poder acceder a los parámetros de configuración en las estaciones de trabajo clientes. No obstante, la contraseña no producirá ningún cambio en la configuración realizada desde la ERAC.

- **Kernel > Configuración > Tareas programadas**
  Esta clave contiene las opciones de Tareas programadas, lo que permite al administrador programar los análisis antivirus periódicos, etc.

NOTA: *de forma predeterminada, todas las soluciones de seguridad de ESET contienen distintas tareas predefinidas (incluyendo actualizaciones automáticas periódicas y comprobaciones automáticas de los archivos importantes en el inicio). En la mayoría de los casos, no será necesario modificar o agregar nuevas tareas.*

- **Actualizar**
  Este apartado del editor de configuración le permite definir cómo aplicar los perfiles de actualización. Normalmente, sólo será necesario modificar el perfil predefinido **Mi perfil** y cambiar la configuración de los valores para **Servidor de actualización, Nombre de usuario** y **Contraseña**. Si se configura el servidor de actualización como **Seleccionar automáticamente**, se descargarán todas las actualizaciones de los servidores de actualización de ESET. En este caso, especifique los parámetros para **Nombre de usuario** y **Contraseña** que se suministraron con la compra. Para obtener información sobre las estaciones de trabajo cliente y recibir actualizaciones desde un servidor local (servidor local de actualización), consulte la sección 7.3, "Servidor local de actualización". Para obtener más información acerca del programador de tareas, consulte 9.1, "Programador de Tareas".

NOTA: *en dispositivos portátiles (ordenadores portátiles, por ejemplo), se pueden configurar dos perfiles. Uno para ofrecer actualizaciones desde el servidor local de actualización y otro para descargar las actualizaciones directamente desde los servidores de ESET. Para obtener más información, consulte la sección 10.4, "Actualización combinada para portátiles" al final de este documento.*

4. Instalación de las soluciones cliente de ESET

Este capítulo está dedicado a la instalación de soluciones cliente de ESET para sistemas operativos de Microsoft Windows. Las instalaciones pueden realizarse directamente en estaciones de trabajo o de forma remota, desde el ERAS. Este capítulo también pone de relieve métodos alternativos para la instalación remota.

NOTA: *aunque es factible desde un punto de vista técnico, no recomendamos el uso de la función de la instalación remota para instalar productos de ESET en los servidores (sólo estaciones de trabajo).*

4.1 Instalación directa

Con una instalación directa, el administrador está presente en el equipo en el que se instalará el producto de seguridad de ESET. Este método no requiere mayor preparación y resulta adecuado para redes de equipos pequeñas o para casos en los que no se utilice el ERA.

Esta tarea se puede simplificar mucho con la ayuda de una configuración .xml predefinida. No se requiere mayor modificación, como la definición de un servidor de actualización (nombre de usuario y contraseña, ruta a un servidor local de actualización, etc.), modo silencioso, análisis programado, etc., durante o después de la instalación.

Existen diferencias en la aplicación del formato de configuración .xml entre las versiones 4.x, 3.x y 2.x de las soluciones cliente de ESET:

- Versión 3.x, 4.x: Descargue el archivo de instalación (por ejemplo, ess_nt32_enu.msi) de eset.com. Copie el archivo de configuración .xml (cfg.xml) en el directorio en el que se ubica el archivo de instalación. Cuando se ejecuta, el instalador adopta automáticamente la configuración del archivo de configuración .xml. Si el archivo de configuración .xml tiene un nombre diferente o se ubica en otro lugar, se puede utilizar el parámetro ADMINCFG =“ruta_al_archivo_xml” (por ejemplo, ess_nt32_enu.msi ADMINCFG =“\\servidor\xml\configuración.xml” para aplicar la configuración guardada en una unidad de red).

- Versión 2.x: Descargue el archivo de instalación (por ejemplo, ndntenst.exe) de eset.com. Extraiga el archivo descargado en una carpeta mediante un programa de extracción de archivos, WinRAR por ejemplo. La carpeta contendrá archivos de instalación, incluyendo setup.exe. Copie el archivo de configuración nod32.xml en la carpeta. Ejecute el archivo setup.exe, se aplicará automáticamente la configuración dentro de nod32.xml. Si el archivo de configuración .xml tiene un nombre diferente o tiene otra ubicación, se puede utilizar el parámetro /cfg =“ruta_al_archivo_xml”. (p. ej. setup.exe /cfg =“\\servidor\xml\configuración.xml” para aplicar la configuración guardada en una unidad de red).

4.2 Instalación remota

ERA ofrece distintos métodos de instalación remota. Se puede realizar la distribución de los paquetes de instalación en estaciones de trabajo de destino con los métodos siguientes:

- Instalación impulsada remota
- Instalación remota de secuencia de comandos de inicio de sesión
- Instalación remota por correo electrónico

La instalación remota mediante ERA consta de los siguientes pasos:

- Creación de los paquetes de instalación
- Distribución de los paquetes a las estaciones de trabajo cliente (método de instalación impulsada, secuencia de comandos de inicio de sesión, correo electrónico, solución externa)

El primer paso se inicia mediante la ERAC, pero el paquete de instalación propiamente dicho se encuentra en el ERAS, en el directorio siguiente:

%ALLUSERSPROFILE %\Application Data\Eset\Eset Remote Administrator\Server\packages

Para iniciar los paquetes de instalación mediante la ERAC, haga clic en la ficha **Instalación remota** y haga clic en el botón **Paquetes...**

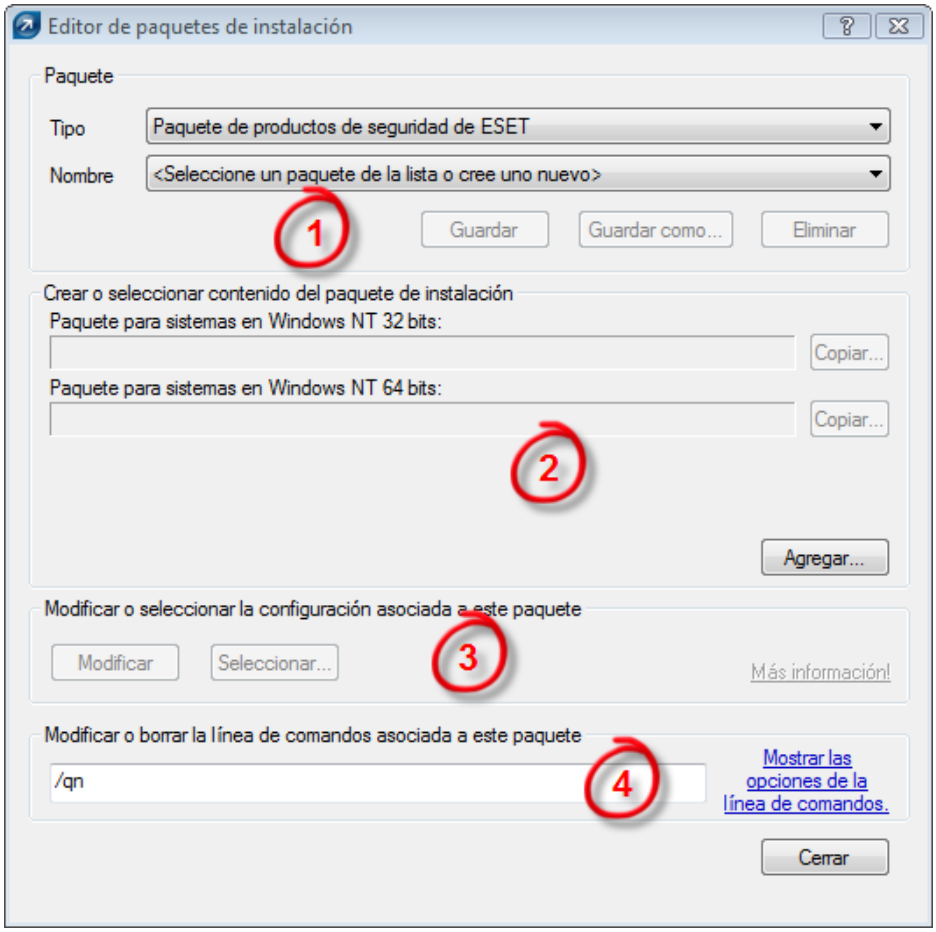


Figura 4-1 Ventana de diálogo del editor de paquetes de instalación

Cada paquete de instalación se define con un Nombre. Vea (1) en la Figura 4-1 anterior. Las secciones restantes de la ventana de diálogo hacen referencia al contenido del paquete, que se aplica tras haber sido entregado correctamente a una estación de trabajo destino. Cada paquete contiene:

- Archivos de instalación de la solución cliente de ESET (2)
- Archivo .xml de configuración para soluciones cliente de ESET (3)
- Parámetros de la línea de comandos asignados al paquete (4)

El menú desplegable **Tipo** de la sección (1) ofrece acceso a las funciones adicionales del ERA. Además de instalarlos, los productos de seguridad de ESET se pueden desinstalar también de forma remota con la opción **Desinstalar productos de seguridad ESET y NOD32 versión 2**. Asimismo, se puede realizar la instalación remota de una aplicación externa seleccionando **Paquete personalizado**.

A cada paquete se le asigna automáticamente un agente de instalador remoto de ESET, que permite una instalación perfecta y una comunicación ininterrumpida entre las estaciones de trabajo destino y el ERAS. El agente de instalador remoto de ESET se denomina einstaller.exe y contiene el nombre del ERAS, además del nombre y el tipo del paquete al que pertenece. Los capítulos siguientes ofrecen una descripción detallada de dicho agente.

Existen varios parámetros que pueden afectar al proceso de instalación. Se pueden usar durante la instalación directa, con el administrador presente en la estación de trabajo, o para la instalación remota. En el caso de instalaciones remotas, los parámetros se seleccionan durante el proceso de configuración de los paquetes de instalación, y estos parámetros seleccionados se aplican automáticamente en clientes de destino. Se pueden indicar parámetros adicionales para ESET Smart Security y ESET NOD32 Antivirus después del nombre del paquete de instalación .msi (p. ej., eav_nt64_ENU.msi /qn):

- **/qn**
  Modo de instalación silenciosa (no se muestran ventanas de diálogo).

- **/qb!**
  El usuario no podrá intervenir en ningún momento, pero el proceso de instalación se muestra mediante una barra de progreso en %.

- **REBOOT =“ReallySuppress”**
  Elimina el reinicio después de la instalación del programa.

- **REBOOT =“Force”**
  Reinicia automáticamente después de la instalación.

- **REBOOTPROMPT =“”**
  Después de la instalación, se muestra una ventana de diálogo que pide al usuario que confirme el reinicio (no se puede usar junto con */qn*).

- **ADMINCFG =“path_to_xml_file”**
  Durante la instalación, los parámetros definidos en los archivos .xml especificados se aplican a los productos de seguridad ESET. No se requiere el parámetro para la instalación remota. Los paquetes de instalación contienen su propia configuración .xml, que se aplica automáticamente.

- **PASSWORD=“contraseña”**
  Debe añadir este parámetro cuando la configuración de ESS/EAV esté protegida mediante contraseña.

Los parámetros para ESET NOD32 Antivirus 2.x deben escribirse después del nombre de archivo *setup.exe*, que se puede extraer junto con otros archivos del paquete de instalación (por ejemplo, *setup.exe /silentmode*):

- **/SILENTMODE**
  Modo de instalación silenciosa (no se muestran ventanas de diálogo).

- **/FORCEOLD**
  Instalará una versión más antigua sobre una versión más reciente instalada.

- **/CFG =“path_to_xml_file”**
  Durante la instalación, los parámetros definidos en los archivos .xml especificados se aplican a las soluciones cliente de ESET. No se requiere el parámetro para la instalación remota. Los paquetes de instalación contienen su propia configuración .xml, que se aplica automáticamente.

- **/REBOOT**
  Reinicia automáticamente después de la instalación.

- **/SHOWRESTART**
  Después de la instalación, se muestra una ventana de diálogo que pide al usuario que confirme el reinicio. Este parámetro sólo se puede usar en combinación con el parámetro *SILENTMODE*.

- **/INSTMFC**
  Instala bibliotecas MFC para el sistema operativo Microsoft Windows 9x, necesarias para la correcta ejecución de ERA. Este parámetro se puede utilizar siempre, incluso si las bibliotecas MFC están disponibles.

En Crear o seleccionar contenido del paquete de instalación (2), el administrador puede crear un paquete de instalación independiente con una configuración predefinida de un paquete de instalación existente y guardado (el botón **Copiar**). Estos paquetes de instalación se pueden ejecutar en estaciones de trabajo cliente donde se va a instalar el programa. El usuario sólo tendrá que ejecutar el paquete para instalar el producto sin conectarse al ERAS durante la instalación.

4.2.1 Requisitos

El requisito básico para una instalación remota es tener configurada correctamente la red TCP/IP. De esa manera, podrá establecerse una comunicación servidor-cliente segura. Al instalar una solución cliente mediante ERA, a la estación de trabajo cliente se le exigen condiciones más estrictas que las exigidas en una instalación directa. Deben cumplirse las condiciones siguientes para la ejecución de una instalación remota:

- Cliente de redes de Microsoft activado
- Servicio de Uso compartido de archivos e impresoras activado
- Puertos para el uso compartido de archivos (445, 135 – 139) accesibles
- Protocolo TCP/IP
- Recurso compartido administrativo ADMIN& activado
- El cliente puede responder a solicitudes PING
- Conectividad del ERAS y de la ERAC (puertos 2221 – 2224 accesibles)

- El nombre de usuario y la contraseña de administrador existen para estaciones de trabajo cliente (el nombre de usuario no puede dejarse en blanco)
- Utilizar uso compartido simple de archivos desactivado
- Servicio del servidor activado
- Servicio Registro remoto activado

Se recomienda encarecidamente comprobar todos los requisitos antes de la instalación, especialmente si existen varias estaciones de trabajo en la red (en la ficha **Instalación remota**, haga clic en **Instalar... > Diagnósticos**).

4.2.2 Configuración del entorno para la instalación remota

Antes de instalar productos de seguridad de ESET en equipos en red, el administrador debe preparar el entorno de forma adecuada para evitar fallos de instalación.

Por ejemplo, con la herramienta integrada Buscar, puede examinar la red en busca de estaciones de trabajo cliente no registradas. Los equipos no registrados son los que no están conectados al ERAS.

Desde la ficha **Instalación remota**, haga clic en **Buscar** para examinar la red. Los equipos no protegidos se muestran a la derecha de la ventana. En los equipos que se encuentran y se muestran en la lista, puede comprobar el estado para las operaciones de **Instalación impulsada, Copiar** y **Exportar**. La opción **Buscar en el servidor** especifica si se examinan los equipos no protegidos desde el ERAS o la ERAC. Se recomienda seleccionar esta opción si se está conectando desde un servidor ERA ubicado en una red diferente.

Cuando haya encontrado estaciones de trabajo adecuadas a la instalación de una solución cliente, utilice la herramienta *Diagnósticos de la instalación remota*.

Acceda a la ficha **Instalación remota** y haga clic en el botón **Instalar...** Haga clic en **Diagnósticos...** para mostrar la ventana **Diagnósticos de la instalación remota**, comprobar los requisitos de instalación e identificar los problemas potenciales.

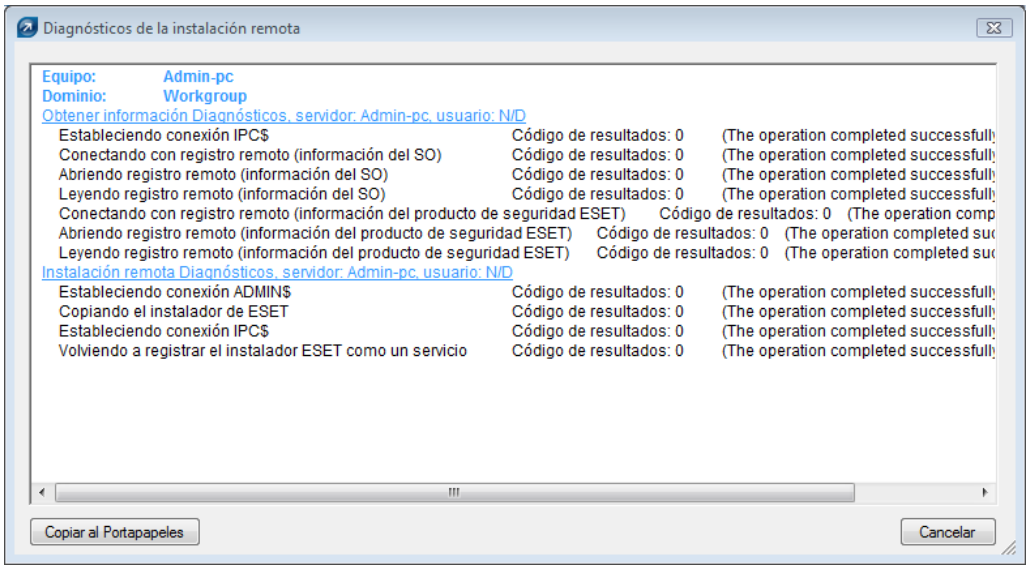


Figura 4-2 La herramienta de diagnósticos puede detectar problemas potenciales antes de la instalación

La primera parte de la sección **Obtener información de los diagnósticos** muestra información sobre el producto de seguridad de ESET instalado en el equipo. En la segunda sección se indica si se cumplen o no todas las condiciones de la instalación para el producto de seguridad de ESET.

4.2.3 Instalación impulsada remota

Este método de instalación remota impulsa instantáneamente las soluciones cliente de ESET en equipos de destino remotos. Los equipos de destino deben estar en línea. A continuación, se muestra una lista de requisitos (para requisitos adicionales, consulte la sección 4.2.1, "Requisitos").

Para iniciar una instalación de impulsión, siga estos pasos:

1) Haga clic en el botón **Instalar...** en la ERAC (ficha **Instalación remota**). En la sección **Sitios de red** situada a la izquierda, desplácese hasta encontrar las estaciones de trabajo en las que desea impulsar el paquete de instalación. Arrástrelas y suéltelas en el panel vacío de la derecha. También puede usar el botón **Agregar cliente...** para agregar el equipo remoto manualmente.

2) En el menú desplegable **Paquete**, seleccione el paquete de instalación que desea entregar a las estaciones de trabajo destino.

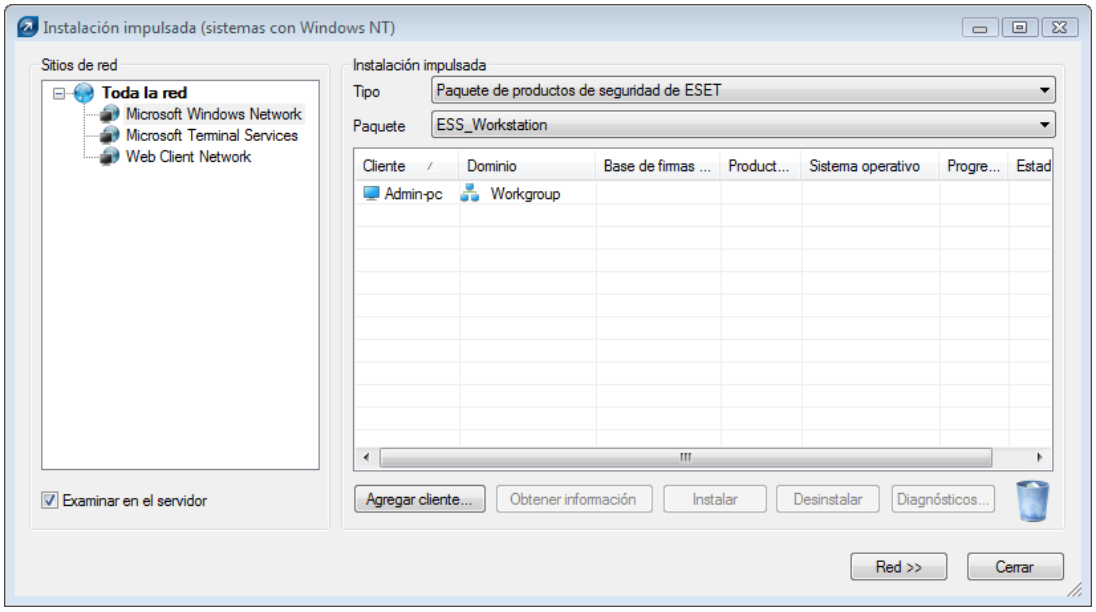


Figura 4-3

3) En el panel de la derecha, seleccione las estaciones de trabajo en las que se requiere la instalación del paquete.

4) Haga clic en **Instalar** (también puede hacer clic en **Obtener información** para ver información sobre los clientes seleccionados).

5) En la mayoría de los casos, se le solicitará que introduzca el nombre de usuario y la contraseña de la cuenta utilizada para acceder a la estación de trabajo destino (debe ser una cuenta con derechos de administrador).

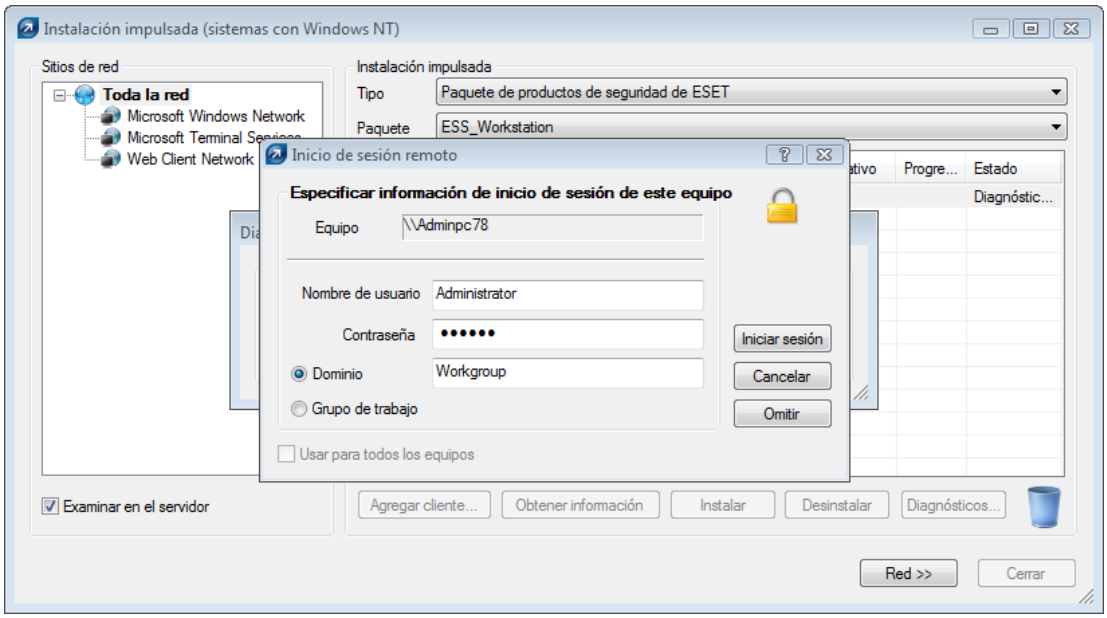


Figura 4-4

Las operaciones siguientes se indican con una barra de progreso y un mensaje de texto. Las operaciones se describen a continuación:

6) ERAS envía el agente einstaller.exe a la estación de trabajo con la ayuda del recurso compartido administrativo admin$.

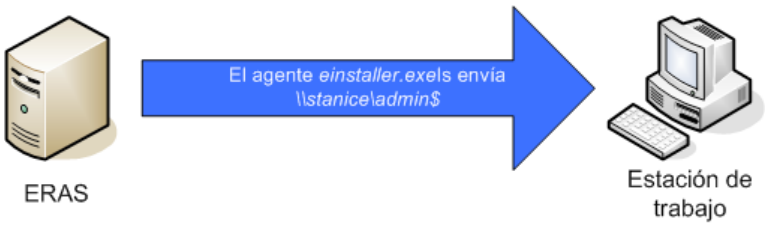
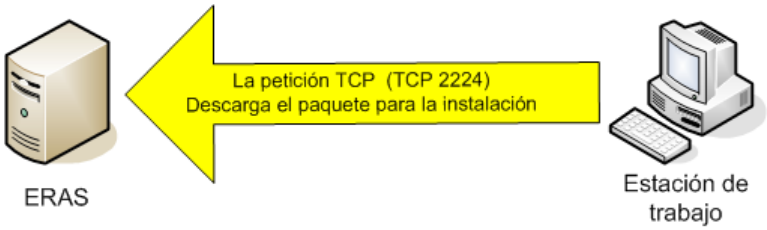


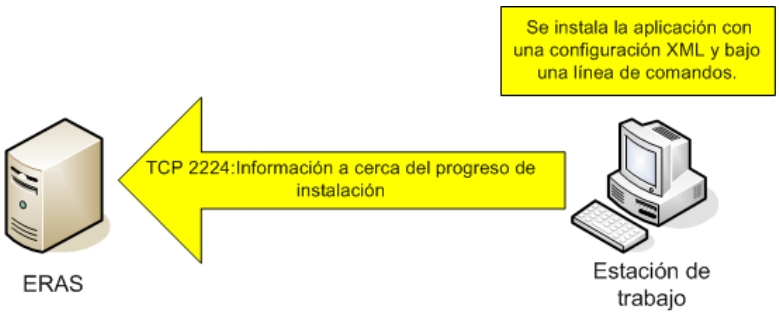
Figura 4-5

7) El agente inicia un servicio en la cuenta del sistema.

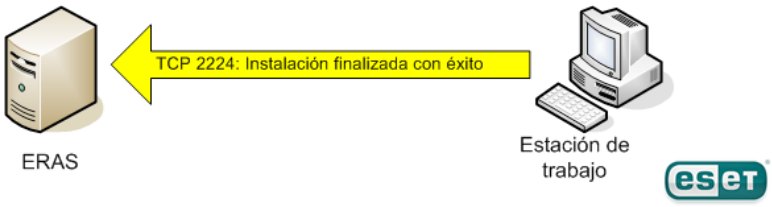
8) El agente establece la comunicación con sus ERAS "principales" y descarga el paquete de instalación correspondiente en el puerto TCP 2224.



9) El agente instala el paquete en la cuenta de administrador definida en el paso 6. También se aplican la configuración .xml correspondiente y los parámetros de la línea de comandos.



10) Inmediatamente después de la finalización de la instalación, el agente envía un mensaje al ERAS. Algunos productos de seguridad de ESET requerirán el reinicio, el equipo lo solicitará en caso necesario.



El menú contextual (clic con el botón secundario) de la ventana de diálogo **Instalación impulsada** ofrece estas opciones:

- **Obtener información**
  Esta función detecta el estado actual del producto de seguridad de ESET en las estaciones de trabajo seleccionadas (requiere el nombre de usuario y la contraseña de administrador). Esta función utiliza el recurso compartido admin$.
- **Desinstalar**
  Eliminación del programa. El agente trata de desinstalar el producto de seguridad de ESET de forma remota. La opción **Desinstalar** no toma en cuenta qué paquete se selecciona en el menú **Paquete**.
- **Diagnóstico**
  Comprueba la disponibilidad de los clientes y servicios que se utilizarán durante la instalación remota. Para obtener más información, consulte la sección 4.2.2, "Configuración del entorno para la instalación remota".
- **Quitar restos del instalador**
  Anula el registro de los agentes (einstaller.exe) del administrador de servicios en las estaciones de trabajo cliente y los elimina del disco duro. Si esta operación se realiza correctamente, se elimina el indicador que impide la instalación repetida del paquete (consulte la sección 4.2.6, "Evitar instalaciones repetidas").
- **Iniciar sesión...**
  Abre una ventana de diálogo para especificar el nombre de usuario y la contraseña de administrador que se muestran automáticamente en los demás casos (paso 5). Esta función fuerza un inicio de sesión en las estaciones de trabajo seleccionadas.
- **Cerrar sesión**
  Finaliza la sesión de inicio para las estaciones de trabajo seleccionadas.
- **Agregar cliente...**
  Agrega estaciones de trabajo cliente individuales a la lista. Inserta la dirección IP o el nombre del cliente. Se pueden añadir clientes adicionales de forma simultánea.

4.2.4 Instalación remota por correo electrónico/inicio de sesión

Los métodos de instalación remota por correo electrónico o inicio de sesión son muy similares. Sólo varían en la forma en la que el agente einstaller.exe se entrega a las estaciones de trabajo cliente. ERA permite que el agente se ejecute a través de secuencia de comandos de inicio de sesión o por correo electrónico. El agente einstaller.exe también se puede utilizar de forma individual y ejecutarse a través de otros métodos (para obtener más información, consulte la sección 4.2.5, "Instalación remota personalizada").

Mientras la secuencia de comandos de inicio de sesión se ejecuta automáticamente cuando el usuario inicia sesión, el método de correo electrónico requiere una intervención por parte del usuario, que deberá iniciar el agente einstaller.exe incluido como archivo adjunto en el correo electrónico. Si se inicia de forma repetida, einstaller.exe no desencadena otra instalación de soluciones cliente de ESET. Para obtener más información, consulte la sección 4.2.6, "Evitar instalaciones repetidas".

La línea de llamada del agente einstaller.exe de la secuencia de comandos de inicio de sesión se puede insertar mediante un editor de texto u otra herramienta. Igualmente, einstaller.exe se puede enviar como archivo adjunto de correo electrónico por cualquier cliente de correo electrónico. Independientemente del método utilizado, asegúrese de utilizar el archivo einstaller.exe correcto.

Para que einstaller.exe se inicie, el usuario actualmente registrado no tiene que ser necesariamente un administrador. El agente adopta el nombre de usuario de administrador/contraseña/dominio de ERAS. Para obtener más información, consulte la parte final de este capítulo.

Introduzca la ruta de acceso a einstaller.exe en la secuencia de comandos de inicio de sesión:

- En la ficha **Instalación remota**, haga clic en **Exportar...** y seleccione el **Tipo** y el nombre del **Paquete** que se va a instalar.
- Haga clic en el botón **...** situado junto a **Carpeta** y seleccione el directorio donde se ubicará y desde el que estará disponible en la red el archivo einstaller.exe.
- En el campo **Compartir**, asegúrese de que la ruta sea correcta y modifíquela si fuera necesario.
- Haga clic en el botón **...** situado junto a **Carpeta de secuencia de comandos** para seleccionar la carpeta donde se ubicará la secuencia de comandos y modifique la máscara en caso de que fuera necesario (**Archivos**).
- En la sección **Archivos**, seleccione el archivo en que se insertará la línea (invocando a einstaller.exe).
- Haga clic en **Exportar a secuencia de comandos de inicio de sesión** para insertar la línea.
- Puede modificar la ubicación de la línea haciendo clic en **Modificar >>** y guardarla haciendo clic en el botón **Guardar**.

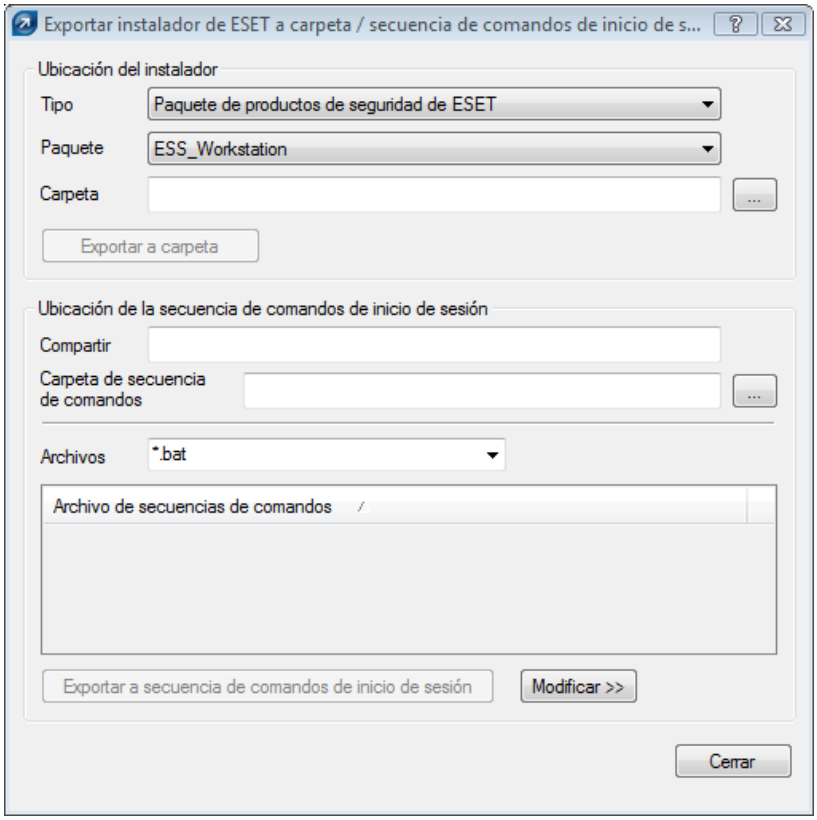


Figura 4-6 Ventana Exportar instalador a carpeta / secuencia de comandos de inicio de sesión

Adjuntar el agente (einstaller.exe) al correo electrónico:

- Haga clic en **Correo electrónico...** en la ficha **Instalación remota** y seleccione **Tipo** y el nombre del **Paquete** que desea instalar.
- Haga clic en **Para...** para seleccionar las direcciones de la libreta de direcciones (también puede añadirlas de forma individual).
- Introduzca un **Asunto** en el campo correspondiente.
- Escriba el mensaje en el **Cuerpo**.
- Compruebe la opción **Enviar comprimido como archivo .zip** si desea enviar el agente comprimido en .zip.
- Haga clic en **Enviar** para enviar el mensaje[4].

[4] Esta función utiliza los parámetros SMTP definidos en el ERAS.

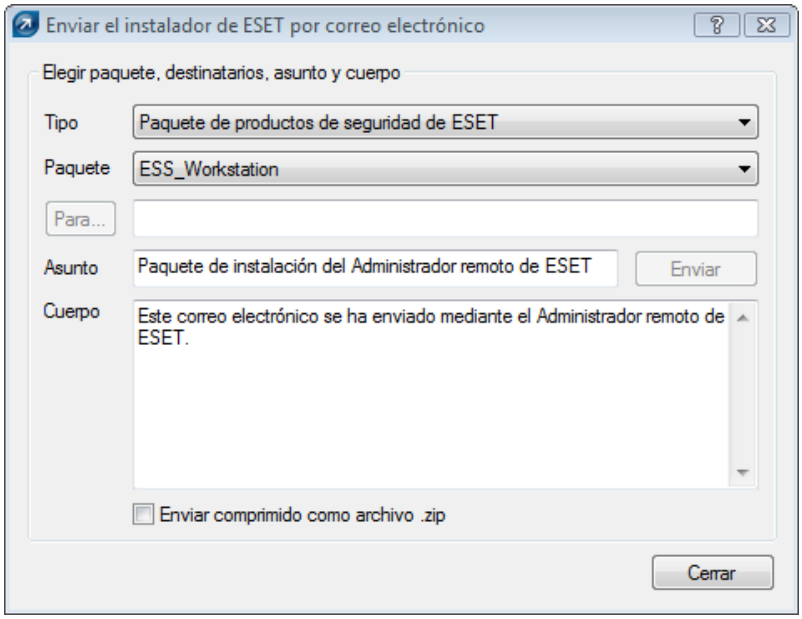


Figura 4-7 Ventana de diálogo Enviar instalador de ESET por correo electrónico

Durante el proceso de instalación remota, se vuelve a establecer la conexión con el ERAS y el agente (einstaller.exe) adopta los parámetros de la configuración **Establecer inicio de sesión predeterminado para correo electrónico** y secuencias de comandos de inicio de sesión en la ficha **Instalación remota**.

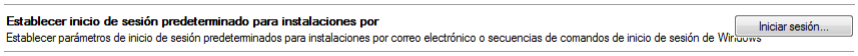


Figura 4,8

Haga clic en **Iniciar sesión...** para especificar el nombre de usuario y la contraseña de la cuenta con la que se va a ejecutar la instalación del paquete. Debe ser una cuenta que disponga de derechos de administrador o, preferiblemente, una cuenta de administrador de dominio.

Los valores insertados en la ventana de diálogo **Iniciar sesión...** no se recuerdan una vez finalizado el servicio (ERAS).

4.2.5 Instalación remota personalizada

No es necesario utilizar herramientas de ERA para instalar soluciones cliente de ESET. En última instancia, el aspecto más importante es entregar y ejecutar el archivo einstaller.exe en las estaciones de trabajo cliente.

Para que einstaller.exe se inicie, el usuario actualmente registrado no tiene que ser necesariamente un administrador. El agente adopta el nombre de usuario de administrador/contraseña/dominio de ERAS. Para obtener más información, consulte la parte final de este capítulo.

El archivo einstaller.exe se puede obtener de la forma siguiente:

- En la ficha **Instalación remota**, haga clic en **Exportar...** y seleccione el **Tipo** y el nombre del **Paquete** que se va a instalar.
- Haga clic en el botón **...** al lado de **Carpeta** y seleccione el directorio en al que einstaller.exe se exportará.
- Haga clic en el botón **Exportar a carpeta**.
- Use el archivo einstaller.exe extraído.

NOTA: *el método de "instalación directa con configuración XML predefinida" se puede usar en las situaciones en las que es posible suministrar derechos de administrador para la instalación. El paquete .msi se inicia utilizando el parámetro /qn (versión 3.x, 4.x) o el parámetro /silentmode (versión 2.x). Estos parámetros ejecutarán la instalación sin mostrar ninguna interfaz de usuario.*

Durante el proceso de instalación remota, se vuelve a establecer la conexión con el ERAS y el agente (einstaller.exe) adopta los parámetros de la configuración **Establecer inicio de sesión predeterminado para correo electrónico** y secuencias de comandos de inicio de sesión en la ficha **Instalación remota**.

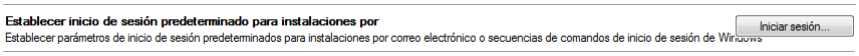


Figura 4-9

Haga clic en **Iniciar sesión...** para especificar el nombre de usuario y la contraseña de la cuenta con la que se va a ejecutar la instalación del paquete. Debe ser una cuenta que disponga de derechos de administrador o, preferiblemente, una cuenta de administrador de dominio.

Si el agente einstaller.exe se inicia manualmente en una estación de trabajo de destino, la instalación remota se desarrolla de forma siguiente:

- El agente einstaller.exe envía una solicitud al ERAS (puerto TCP 2224)
- El ERAS inicia una nueva instalación impulsada (con un agente nuevo) en el paquete correspondiente (enviado a través del recurso compartido *admin$*)[5]. El nuevo agente inicia entonces la descarga del paquete del ERAS a través del protocolo TCP/IP.

La instalación del paquete se inicia, aplicando los parámetros .xml asociados en la cuenta definida en el ERAS (el botón **Iniciar sesión...**)

4.2.6 Evitar instalaciones repetidas

En cuanto el agente completa con éxito el proceso de instalación remota, marca al cliente remoto con un identificador para prohibir las instalaciones repetidas del mismo paquete de instalación. El indicador se escribe en la clave de registro siguiente:

HKEY_LOCAL_MACHINE\Software\ESET\Instalador remoto de ESET

Si el nombre y tipo del paquete definido en el agente einstaller.exe coincide con los datos en el registro, no se realiza ninguna instalación. Este proceso impide la instalación repetida en estaciones de trabajo de destino si se inicia repetidamente el agente einstaller.exe.

NOTA: *el método de instalación impulsada remota ignora esta clave de registro.*

ERAS proporciona un nivel de protección adicional frente a instalaciones repetidas, que se realiza en el momento en el que el instalador establece de nuevo una conexión con el ERAS (TCP 2224). Si se produce un mensaje de error en relación con la estación de trabajo, o en caso de que se complete la instalación correctamente, se deniegan los intentos adicionales de instalación.

El agente graba el error siguiente en el registro del instalador que se encuentra en *%TEMP %\einstaller.log*:

Status 20 001: El servidor "X:2224" ha comunicado al instalador de ESET que debe cerrarse.

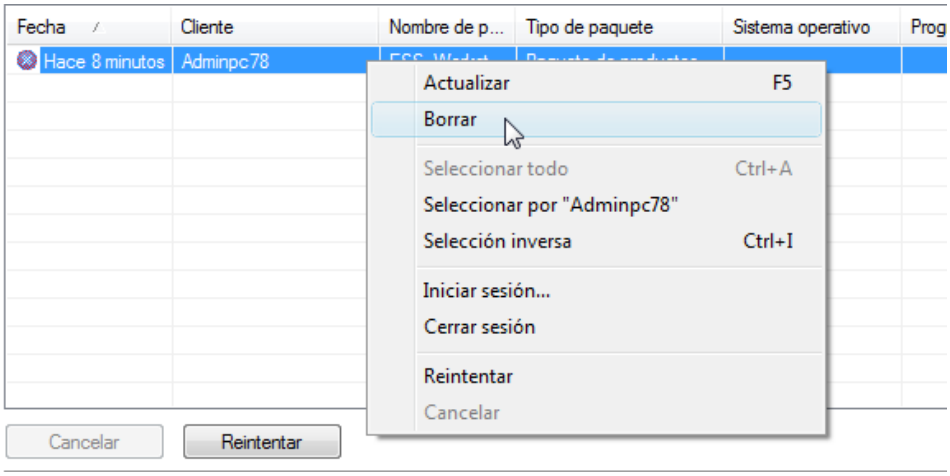


Figura 4-10

[5] El agente espera una respuesta del ERAS (enviando el paquete a través del recurso compartido admin$). En caso de que no se produzca una respuesta, el agente tratará de descargar el paquete de instalación (a través del puerto TCP/IP 2224). En este caso, no se transfieren el nombre de usuario del administrador y la contraseña especificados en Instalación remota > Iniciar sesión.. en el ERAS y el agente trata de instalar el paquete con el usuario actual. En los sistemas operativos Microsoft Windows 9x/Me, no se puede usar el recurso compartido administrativo, por ello, el agente establece automáticamente una conexión TCP/IP directa con el servidor.

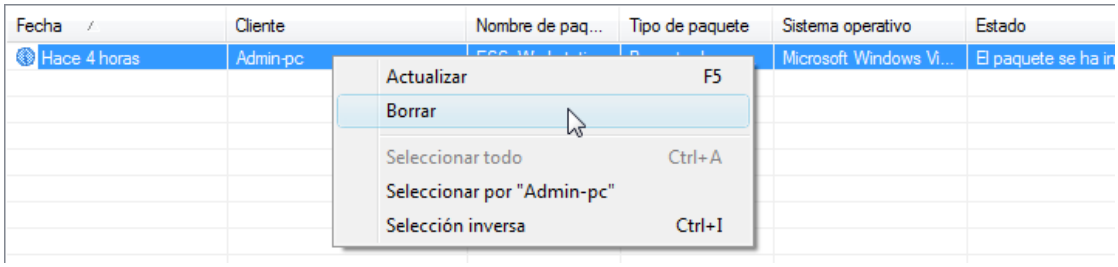


Figura 4.11

Para evitar que el ERAS deniegue la instalación repetida, elimine las entradas relacionadas en la ficha ***Instalación remota***. Para eliminar estas entradas, haga clic con el botón secundario y seleccione la opción ***Borrar*** del menú contextual.

4.3 Instalación en un entorno empresarial

A la hora de implantar programas en grandes redes, es importante usar una herramienta capacitada para realizar instalaciones de programa remotas en cada uno de los equipos de la red.

Instalación a través de Group Policy

En el entorno de Active Directory, esta tarea se puede resolver perfectamente con la instalación de Group Policy. La instalación emplea el instalador MSI, que se distribuye directamente a todos los clientes que se conectan al dominio a través de Group Policy.

Para configurar un controlador de dominio para instalar automáticamente ESET Smart Security o ESET NOD32 Antivirus en cada estación de trabajo después de iniciar sesión, siga estos pasos:

1) Cree una carpeta compartida en el controlador de dominio. Todas las estaciones de trabajo deben contar con permisos de "lectura" para esta carpeta.

2) Copie el paquete de instalación ESET Smart Security o ESET NOD32 Antivirus (.msi) en la carpeta.

3) Inserte un archivo de configuración xml (que se aplicará al programa) en la misma carpeta. El archivo deberá tener el nombre cfg.xml. Para crear un archivo de configuración, se puede utilizar el Editor de configuración ESET. Para obtener más información, consulte el apartado 3.7, "Editor de configuración de ESET".

4) Haga clic en **Inicio > Programas > Herramientas administrativas > Usuarios y equipos de Active Directory**.

5) Haga clic con el botón secundario en el nombre del dominio y seleccione **Propiedades > Group Policy > Modificar > Configuración de usuario**.

6) Haga clic con el botón secundario en **Configuración de software** y seleccione **Nuevo > Paquete**.

7) En la ventana **Abrir**, especifique la ruta UNC para el paquete de instalación compartido, por ejemplo, *nombre_del_equipo**ruta**paquete_de_instalación.msi* y haga clic en **Abrir**. No use la opción **Examinar** para localizar el paquete de instalación porque se mostrará como una ruta de red local en vez de una ruta de red UNC.

8) En la ventana de diálogo siguiente, seleccione la opción **Asignado**. Haga clic en **Aceptar** para cerrar la ventana.

Al seguir los pasos anteriores, el paquete del instalador se instalará en cada equipo que entre en el dominio. Para instalar el paquete en los equipos que están actualmente activos, los usuarios deben cerrar sesión e iniciarla de nuevo.

Si desea dar a los usuarios la posibilidad de aceptar o denegar la instalación del paquete, seleccione **Publicar** en vez de **Asignado** en el paso 8. La próxima vez que el usuario inicie sesión, el paquete se añadirá a **Panel de control > Agregar o quitar programas > Agregar nuevos programas > Agregar programas desde la red**. Los usuarios podrán acceder al paquete para instalaciones futuras desde esta ubicación.

5. Administración de equipos cliente

5.1 Tareas

Las estaciones de trabajo clientes conectadas al ERAS correctamente y visualizadas en la ERAC se pueden configurar y administrar mediante distintos tipos de tareas. Las tareas se pueden aplicar a varios clientes o a uno o varios grupos de clientes. Para aplicar una tarea a una o más estaciones de trabajo cliente, haga clic con el botón secundario en la(s) que corresponda en el panel **Clientes**. A continuación, haga clic en **Nueva tarea** y seleccione el tipo de tarea que desea realizar. Además, el asistente de tareas se puede abrir desde el menú principal de la ERAC haciendo clic en **Acciones > Nueva tarea.**

Las siguientes cuatro secciones desarrollarán los tipos individuales de tareas para estaciones de trabajo clientes. Cada tipo estará acompañado de una situación hipotética.

5.1.1 Tarea de configuración

Las tareas de configuración se utilizan para modificar los ajustes de protección en estaciones de trabajo cliente y se entregan a estas últimas en forma de paquetes de configuración que contienen los parámetros de modificación. Los archivos .xml creados en el Editor de configuración de ESET o exportados desde los clientes también son compatibles con las tareas de configuración. El ejemplo que se muestra a continuación muestra cómo crear una tarea de configuración que modifique el nombre de usuario y la contraseña en equipos de destino. Los modificadores y las opciones que no se utilicen en este ejemplo se incluyen al final de este capítulo.

En primer lugar, designe las estaciones de trabajo a las que se entregará la tarea. Marque esas estaciones de trabajo en el panel **Clientes** de la ERAC.

1) Haga clic con el botón secundario en cualquiera de las estaciones de trabajo marcadas y seleccione **Nueva tarea > Tarea de configuración** desde el menú contextual.

2) Se abrirá la ventana **Configuración para clientes**, que actúa como asistente de tareas de configuración. Puede especificar el origen del archivo de configuración haciendo clic en **Crear**..., **Seleccionar**..., o **Crear de una plantilla**...

3) Haga clic en el botón **Crear** para abrir el Editor de configuración de ESET y especifique la configuración que se va a aplicar. Navegue hasta **ESET Smart Security, ESET NOD32 Antivirus > Módulo de actualización > Perfil > Configurar > Nombre de usuario** y **Contraseña**.

4) Introduzca el nombre de usuario y la contraseña proporcionados por ESET, y haga clic en **Consola**, a la derecha, para volver al asistente de tareas. A continuación, se muestra la ruta de acceso al paquete en el campo **Crear/ Seleccionar configuración**.

5) En el caso de que ya disponga de un archivo de configuración en el que se incluyan las modificaciones deseadas, haga clic en **Seleccionar**, busque el archivo y asígnelo a la tarea de configuración.

6) También puede hacer clic en **Crear de una plantilla**, seleccionar el archivo .xml y realizar los cambios si es necesario.

7) Para ver o modificar el archivo de configuración que acaba de crear o modificar, haga clic en los botones, haga clic en los botones **Ver** o **Modificar**.

8) Haga clic en **Siguiente** para proseguir con la ventana de **Clientes seleccionados**, en la que se mostrarán las estaciones de trabajo a las que se entregará la tarea. En este paso, puede agregar más clientes (o bien, grupos de clientes o todos los clientes). Haga clic en **Agregar especial** para agregar clientes que pertenezcan a los servidores o grupos seleccionados. Haga clic en **Siguiente** para seguir con el siguiente paso.

9) La última ventana de diálogo, **Informe de tareas**, muestra una vista previa de la tarea de configuración. Introduzca un nombre o una descripción para la tarea (opcional). Puede utilizar la opción **Aplicar tarea a partir de las** para establecer que la tarea se ejecute después de una fecha u hora específica. La opción **Eliminar tareas automáticamente mediante su limpieza si se completan correctamente** elimina todas las tareas entregadas correctamente a las estaciones de trabajo de destino.

- Haga clic en **Finalizar** para registrar la tarea que se va a ejecutar.

5.1.2 Tarea de análisis a petición

La opción del menú contextual **Nueva tarea** contiene dos variantes del análisis a petición. La primera opción es **Análisis a petición (limpieza desactivada)**. Este análisis solamente crea un registro, no realiza ninguna acción sobre los archivos infectados. La segunda opción es **Análisis a petición (limpieza desactivada)**.

La ventana **Análisis a petición** contiene la misma configuración predeterminada para ambas variantes, además de la opción **Analizar sin limpiar**. Esta opción determina si el escáner debe o no limpiar los archivos afectados. El ejemplo que aparece a continuación muestra cómo crear una tarea de Análisis a petición.

- El menú desplegable **Sección de configuración** le permite seleccionar el tipo de producto ESET para el cual se está definiendo la tarea de análisis a petición. Seleccione los que estén instalados en las estaciones de trabajo de destino.

- La opción **Excluir esta sección del análisis a petición** desactiva todas las opciones de la ventana para el tipo de producto seleccionado, las cuales no se aplicarán a las estaciones de trabajo que tengan el tipo de producto definido en **Sección de configuración**. Por tanto, todos los clientes que tengan ese producto en particular se eliminarán de la lista de destinatarios. Si el administrador marca a los clientes como receptores y excluye al producto mediante el parámetro mencionado anteriormente, la tarea generará un error y se recibirá una notificación en la que se indica que la tarea no ha podido aplicarse. Para evitarlo, el administrador debe especificar siempre los clientes a los que se asignará la tarea.

- En **Nombre del perfil** puede seleccionar el perfil de análisis que se aplicará con la tarea.

- En la sección **Unidades para analizar**, seleccione los tipos de unidades que desea analizar en los equipos cliente. Si la selección es demasiado general, podrá agregar una ruta de acceso exacta a los objetos que se van a analizar. Para ello, utilice el campo **Ruta** o el botón **Agregar ruta de acceso**. Seleccionar **Borrar historial** para restaurar la lista original de las unidades para analizar.

- Haga clic en **Siguiente** para proseguir con las ventanas de diálogo denominadas **Seleccionar clientes** e **Informe de tareas**, que son idénticas a las ventanas de diálogo del asistente de tareas de configuración (consulte la sección 5.1.1, "Tarea de configuración").

Una vez que la tarea se haya ejecutado en las estaciones de trabajo cliente, los resultados se devuelven al ERAS y se podrán ver en el panel **Registro de análisis**.

5.1.3 Tarea Actualizar ahora

El propósito de esta tarea es forzar las actualizaciones en las estaciones de trabajo de destino (tanto actualizaciones de la base de firmas de virus como actualizaciones de los componentes del programa). Haga clic con el botón secundario en cualquier estación de trabajo del panel **Clientes** y seleccione **Nueva tarea > Actualizar ahora**. Si desea excluir algunos productos de seguridad de ESET de la tarea, selecciónelos en el menú desplegable **Sección de configuración** y seleccione la opción **Excluir esta sección de Actualizar tarea**. Para utilizar un perfil de actualización específico en la tarea Actualizar ahora, active la opción **Seleccionar nombre de perfil** y seleccione el perfil deseado. También puede seleccionar **Nombre de perfil definido por el usuario** e introducir el nombre del perfil. El valor del campo volverá a ser el predeterminado si hace clic en **Borrar historial**. A continuación haga clic en **Siguiente** para continuar con las ventanas de diálogo, **Seleccionar clientes** e **Informe de tareas.** Para obtener una descripción de estos diálogos, consulte la sección 5.1.1, "Tarea de configuración".

5.1.4 Tarea de secuencias de comandos de SysInspector

La tarea Secuencias de comandos de SysInspector le permite ejecutar la secuencia de comandos en el equipo de destino. Haga clic en **Seleccionar** para elegir una secuencia de comandos que se ejecutará en la estación de trabajo destino. Haga clic en **Ver y modificar** para ajustar la secuencia de comandos. Haga clic en **Siguiente** para continuar con las ventanas de diálogo **Seleccionar clientes** e **Informe de tareas**, que son idénticas a las ventanas de diálogo del asistente de tareas de configuración. Una vez que la tarea se haya ejecutado en la estación de trabajo cliente, la información se muestra en la columna **Estado** del panel de **Tareas**.

5.2 Grupos

La ERAC proporciona varias herramientas y características que hacen posible que el usuario administre fácilmente los clientes y eventos. Una de estas características es el Editor de grupos, que resulta útil al aplicar filtros o crear tareas, ya que estas actividades se pueden aplicar simultáneamente a todo un grupo de clientes.

Los clientes individuales se pueden dividir en grupos mediante el editor de grupos de la ERAC. Se puede acceder al editor de grupos desde el menú principal de la ERAC, haciendo clic en **Herramientas > Editor de grupos**, o pulsando CTRL + G.

La ventana del **Editor de grupos** está dividida en dos partes. A la izquierda hay una lista de grupos existentes, mientras que a la derecha hay una lista de clientes. El panel derecho muestra los clientes asignados a un grupo seleccionado en el panel izquierdo. De forma parecida, todas las operaciones que representan los botones de la parte inferior de la ventana se realizan en los grupos o clientes seleccionados en ese momento.

Para crear un grupo nuevo, haga clic en **Crear** y seleccione un nombre para él. Le recomendamos que utilice un nombre que indique dónde están ubicados los equipos (p. ej., Departamento financiero, Asistencia técnica, etc.). El campo **Descripción** se puede usar para dar una descripción más detallada del grupo (p. ej., "Equipos de la oficina C", "Estaciones de trabajo de la oficina central", etc.). Los grupos nuevos que se creen o configuren también se pueden modificar posteriormente.

Haga clic en **Aceptar** para crear el grupo. El nombre y la descripción aparecerán a la izquierda y se activará el botón **Agregar o quitar**. Haga clic en él para agregar clientes que quiera incluir en el grupo (puede hacer doble clic o arrastrarlos y colocarlos de izquierda a derecha). Para encontrar y agregar clientes, escriba el nombre de un cliente, entero o una parte, en el campo **Búsqueda rápida** y se mostrarán todos los clientes que contengan esa cadena de caracteres. Para marcar todos los clientes, haga clic en **Seleccionar todo.** Haga clic en el botón **Actualizar** para comprobar si hay algún cliente nuevo que se haya conectado al servidor recientemente.

Si no le resulta cómodo seleccionar clientes manualmente, puede hacer clic en **Agregar especial**... para ver más opciones.

Seleccione la opción **Agregar clientes cargados en el panel de clientes** para agregar todos los que se muestran en la sección de clientes, o bien elija la opción **Sólo seleccionados**. Para agregar clientes que ya pertenecen a otro servidor u otro grupo, selecciónelos en las listas a derecha e izquierda y haga clic en **Agregar**.

Haga clic en **Aceptar** en la ventana de diálogo **Agregar o quitar** para volver a la ventana principal del editor de grupos. El nuevo grupo debería aparecer con sus clientes correspondientes.

Haga clic en el botón **Agregar o quitar** para agregar o quitar clientes de los grupos, o bien haga clic en el botón **Eliminar** para borrar un grupo entero. Haga clic en el botón **Copiar al Portapapeles** para copiar las listas de clientes y grupos.

La última opción del editor de grupos es utilizar la creación de grupos automáticos (con clientes correspondientes) basada en la estructura definida por Active Directory. Recuerde que esta opción sólo está disponible si el ERAS está instalado en un sistema con Active Directory. Para adoptar la estructura de Active Directory, haga clic en **Sincronizar con Active Directory**. También se puede agregar un cliente a un grupo haciendo clic con el botón secundario en la ficha Clientes y seleccionando **Agregar al grupo...**

Advertencia: *si utiliza la opción de sincronización completa, se eliminarán todos los grupos existentes. En caso contrario, se agregarán los grupos y clientes nuevos y se conservarán los existentes.*

La configuración detallada de la sincronización de Active Directory se puede realizar con el editor de configuración (**ESET Remote Administrator** > **Servidor ERA** > **Configuración** > **Active Directory** > **Crear por grupos/sincronización de Active Directory**). Sólo se sincronizan, de forma predeterminada, los **Grupos de seguridad de los sistemas** y las **Unidades de organización de los sistemas**. Sin embargo, puede agregar más objetos de Active Directory activando la opción deseada.

5.2.1 Filtrado

Si aparecen demasiados clientes en el panel de Clientes, puede utilizar las opciones de filtrado. Para obtener más información, consulte la sección 3.3, "Filtrado de la información".

5.3 Directrices

Las directivas se parecen en muchos rasgos a las tareas de configuración, exceptuando que no se trata de tareas sueltas enviadas a una o más estaciones de trabajo. En vez de eso, proporcionan un mantenimiento continuo de ciertos parámetros de configuración de los productos de seguridad de ESET. Dicho de otro modo, una directiva es una configuración que se le obliga a adoptar a un cliente.

5.3.1 Funcionamiento y principios básicos

Para acceder al Administrador de directivas, seleccione **Herramientas > Administrador de directivas...** El árbol de directivas situado a la izquierda muestra una lista de las directivas presentes en cada servidor individual. La parte derecha está dividida en cuatro secciones: **Parámetros de la directiva, Configuración de la directiva, Acción de la directiva** y **Configuración global de directivas**. Las opciones de estas secciones permiten que un administrador gestione y configure directivas.

Algunas de las funciones principales del administrador de directivas son crear, modificar y eliminar directivas. Los clientes reciben las directivas desde el ERAS. El ERAS puede utilizar múltiples directivas, que heredan sus parámetros entre sí o de otras directivas de un servidor superior.

El sistema de adopción de directivas desde un servidor superior se denomina *herencia*. Las directivas que se crean al heredarse se denominan *directivas combinadas*. La herencia se basa en el principio principal – secundario, esto es, una directiva secundaria hereda parámetros de una directiva principal.

5.3.2 Cómo crear directivas

La instalación predeterminada sólo implementa una directiva, denominada "Directiva del servidor". Este nombre se puede cambiar en el campo **Configuración de directivas > Nombre de la directiva**. La directiva en sí se puede configurar desde el Editor de configuración de ESET. Haga clic en **Modificar** y defina los parámetros para el cliente o el producto de seguridad de ESET. Todos los parámetros están organizados en una estructura exhaustiva y todos los elementos del editor tienen un icono asignado. Los clientes sólo adoptarán parámetros activos (marcados con un icono azul). Todos los parámetros inactivos (sombreados) permanecerán sin cambios en los equipos de destino. Se aplica el mismo principio a todas las directivas heredadas y combinadas. Una directiva secundaria adoptará sólo parámetros activos de una directiva principal.

Los servidores de ERA admiten varias directivas (**Agregar nueva directiva secundaria**). Las siguientes opciones están disponibles para las directivas nuevas: nombre de la directiva, vinculación a una **Directiva principal** y configuración (la configuración puede estar vacía, copiada de otra directiva ya existente o copiada de un archivo de configuración .xml). Las directivas sólo se pueden crear en el servidor al que se está conectado actualmente mediante la ERAC. Para crear una directiva en un servidor inferior tiene que conectarse directamente con este último.

Cada directiva tiene dos atributos básicos: **Anular directivas secundarias** y **Bajar directiva replicable**. Estos atributos definen cómo adoptan los parámetros de configuración activos las directivas secundarias.

Anular directivas secundarias – Fuerza todos los parámetros activos en las directivas heredadas. Si la directiva secundaria difiere, la directiva combinada contendrá todos los parámetros activos de la directiva principal (incluso si está activada la opción **"Anular..."** para la directiva secundaria). Todos los parámetros inactivos de la directiva principal se ajustarán a la directiva secundaria. Si el atributo **Anular directivas secundarias** no está activado, los parámetros de configuración de la directiva secundaria tiene prioridad sobre los de la directiva principal a la hora de configurar la directiva combinada resultante. Este tipo de directivas combinadas se aplicarán a otras directivas, siempre que estén vinculadas en calidad de directivas principales.

Bajar directiva replicable – Activa la replicación en las directivas secundarias, es decir, puede servir como directiva predeterminada para los servidores inferiores y se puede también asignar a clientes conectados a servidores inferiores.

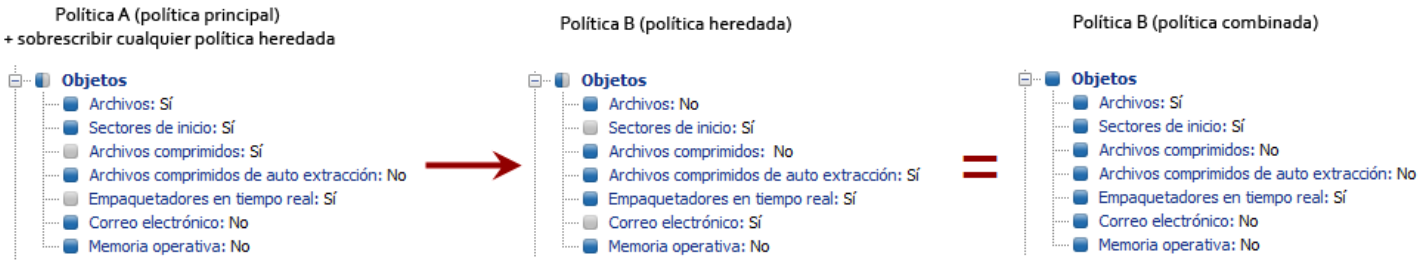


Figura 5-1: Ejemplo de directivas heredadas

5.3.3 Directivas virtuales

Además de las directivas creadas, así como las replicadas desde otros servidores (consulte la sección 7.4, "Ficha Replicación"), el árbol de directivas también contiene una Directiva principal predeterminada y una directiva predeterminada para clientes principales, conocidas como directivas virtuales.

La Directiva principal predeterminada se ubica en un servidor superior en la Configuración global de directivas y se selecciona como **Directiva predeterminada para servidores inferiores**. Si el servidor no está replicado, esta directiva estará vacía (lo explicaremos más adelante).

La Directiva predeterminada para clientes principales se ubica en el servidor en cuestión (no en el servidor superior), en la Configuración global de directivas, y se elige en Directiva predeterminada para clientes principales. Se fuerza automáticamente para los clientes nuevos que se conectan (clientes principales o primarios) desde el ERAS en cuestión, a no ser que ya hayan adoptado otra directiva de las Reglas de la directiva (para obtener más información, consulte el apartado 5.3.6, "Asignación de directivas a clientes"). Las directivas virtuales son vínculos a otras directivas ubicadas en el mismo servidor.

5.3.4 Directivas y estructura del Editor de configuración de ESET

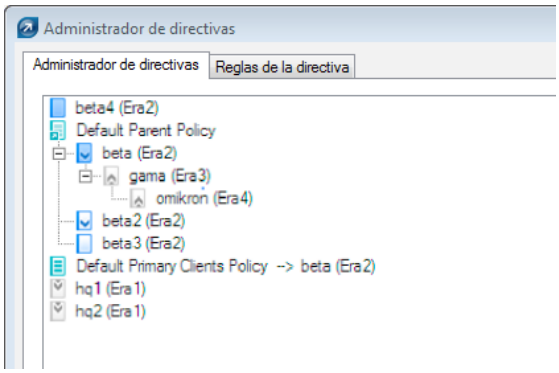


Figura 5-2

Se asigna a todas las directivas del árbol de directivas un icono a la izquierda. El significado de los iconos es el siguiente:

1) Las directivas con iconos azules hacen referencia a las que están presentes en el servidor especificado. Existen tres subgrupos de iconos azules:

Iconos con destinos blancos – Ya existe una directiva creada en ese servidor. Además, no se pueden replicar en sentido descendente, lo que significa que no se asigna a clientes de servidores inferiores y no funciona como directiva principal para los servidores secundarios. Dichas directivas sólo pueden aplicarse dentro del servidor: a clientes conectados al servidor. También puede funcionar como directiva principal para otra del mismo servidor.

Iconos con destinos azules – También se creó una directiva en el servidor, sin embargo, se seleccionó la opción **Anular directivas secundarias** (para obtener más información, consulte el apartado 5.3.2, "Cómo crear directivas").

, Iconos con flechas hacia abajo – Estas directivas están replicadas. La opción **Bajar directiva replicable** está activada. Puede aplicar estas directivas en el servidor en cuestión y en sus servidores secundarios.

2) Las directivas con iconos grises provienen de otros servidores.

 Iconos con flechas hacia arriba – Estas directivas se replican desde servidores secundarios. Sólo pueden verse o eliminarse con la opción **Eliminar apartado de la directiva**. Esta opción no eliminará la directiva en sí misma, sólo la eliminará del árbol de directivas. Por lo tanto, puede volver a aparecer tras la replicación. Si no quiere mostrar directivas de servidores inferiores, utilice la opción **Ocultar directivas de servidores externos no utilizadas en el árbol de directivas**.

 Iconos con flechas hacia abajo – Estas directivas se replican desde servidores superiores. Pueden utilizarse como directivas principales para otras directivas, asignadas a clientes (**Agregar clientes**) o eliminadas (**Eliminar directiva**). Recuerde que la eliminación sólo eliminará la directiva. Volverá a aparecer tras la replicación del servidor superior (a menos que se haya desactivado el atributo **Bajar directiva replicable** del servidor superior).

NOTA: *para desplazar y asignar directivas dentro de la estructura, puede seleccionar la directiva principal o arrastrarla y colocarla con el ratón.*

5.3.5 Visualización de directivas

Se pueden ver las directivas del árbol de directivas directamente en el editor de configuración haciendo clic en **Ver...** o **Ver combinadas...**

Ver combinadas – Muestra la política combinada creada al heredarse (el proceso de herencia se aplica a la configuración de la directiva principal). Esta opción se visualiza de forma predeterminada, debido a que la directiva actual ya es una directiva combinada.

Ver – Muestra la directiva original antes de combinarse con una principal.
En los servidores inferiores, están disponibles las siguientes opciones para directivas heredadas de servidores superiores:

Ver combinadas – Igual que antes

Ver la parte de anulación – Este botón se aplica a directivas con el atributo **Anular directivas secundarias**. Esta opción sólo muestra la parte forzada de la directiva, es decir, la que tiene la prioridad sobre las demás opciones en las directivas secundarias.

Ver la parte no forzada – Tiene el efecto opuesto a Ver la parte de anulación. Sólo muestra elementos activos y no se aplica **Anular...**

5.3.6 Asignación de directivas a clientes

Hay dos reglas principales para asignar directivas a clientes:

1) A los clientes locales (primarios) se les puede asignar cualquier directiva local o cualquier directiva replicada desde los servidores superiores.

2) A los clientes replicados desde servidores inferiores se les puede asignar cualquier directiva local, mediante el atributo **Bajar replicable** o cualquier directiva replicada desde servidores superiores. No se les puede forzar a que adopten directivas de su propio servidor principal (para ello, debe conectarse a él con la ERAC).

Una característica importante es que a todos los clientes se les asigna alguna directiva (no hay ningún cliente sin directivas). Además, no se puede retirar una directiva de un cliente. Sólo se puede sustituir por otra directiva. Si no quiere aplicar ninguna configuración desde una directiva a un cliente, cree una directiva vacía.

5.3.6.1 Directiva predeterminada para clientes principales

Un método para asignar directivas es la aplicación automática de la Directiva predeterminada para clientes principales, una directiva virtual que se puede configurar con la configuración global de directivas. Esta directiva se aplica a los clientes principales o primarios, esto es, a los que se conectan al ERAS directamente. Para obtener más información, consulte el apartado 5.3.3, "Directivas virtuales".

5.3.6.2 Asignación manual

Hay dos maneras de asignar directivas manualmente: Haga clic con el botón secundario en el panel de Clientes y seleccione **Agregar directiva** en el menú contextual, o haga clic en **Agregar clientes > Agregar o quitar** en el Administrador de directivas.

Al hacer clic en **Agregar clientes** en el Administrador de directivas, se abre la ventana de diálogo Agregar o quitar. Los clientes aparecen en una lista a la izquierda, con el formato Servidor/Cliente. Si está seleccionado Bajar directiva replicable, la ventana también mostrará los clientes replicados desde servidores inferiores. Seleccione los clientes para recibir la directiva utilizando el método de arrastrar y colocar, o bien haciendo clic en **>>** para moverlos a Elementos seleccionados. Los clientes recientemente seleccionados muestran un asterisco de color amarillo y todavía se pueden quitar de Elementos seleccionados si se hace clic en **<<** o en el botón **C**. Haga clic en **Aceptar** para confirmar la selección.

NOTA: *después de la confirmación, si vuelve a abrir la ventana de diálogo Agregar o quitar, no podrá quitar los clientes de Elementos seleccionados, solamente podrá sustituir la directiva.*

También puede agregar clientes con la característica **Agregar especial**, que puede añadir todos los clientes a la vez, agregar clientes seleccionados o agregar clientes de servidores o grupos seleccionados.

5.3.6.3 Reglas de la directiva

La herramienta **Reglas de la directiva** permite que un administrador asigne automáticamente directivas a estaciones de trabajo de una manera más exhaustiva. Las reglas se aplican inmediatamente después de que el cliente se conecte con el servidor, tienen prioridad sobre la **Directiva predeterminada para clientes principales** y sobre la asignación manual. La **Directiva predeterminada para clientes principales** sólo es pertinente si el cliente no está incluido en ninguna de las reglas actuales. Del mismo modo, si hay una directiva asignada manualmente que se debe aplicar y entra en conflicto con las reglas de la directiva, la configuración que fuerzan las reglas de la directiva tendrá prioridad.

Las reglas de la directiva tienen una ficha en el Administrador de directivas, donde se pueden crear y administrar. El proceso de creación y aplicación es muy similar al de creación y administración de reglas en los clientes de correo electrónico. Cada regla puede contener uno o más criterios. Cuanto más alta sea su posición en la lista, más importante será (se puede desplazar arriba y abajo).

Para crear una regla nueva, haga clic en el botón **Nueva...** A continuación escriba **Nombre, Descripción, Parámetros del filtro de clientes** y **Directiva** (una directiva que se aplicará a todos los clientes que cumplan con los criterios indicados).

Para configurar los criterios de filtrado, haga clic en el botón **Modificar**.

Los criterios disponibles son:

(NO) DESDE el servidor primario – Si (no) se encuentra en el servidor primario o principal
(NO) ES un cliente nuevo – Si (no) es un cliente nuevo
(NO) TIENE marca "Nuevo" – Se aplica a los clientes con/sin la marca **Cliente nuevo**.
Servidor primario (NO) EN (especificar) – Si el nombre del servidor primario o principal contiene o no contiene
Grupos del administrador remoto EN (especificar) – Si el cliente pertenece al grupo...
Grupos del administrador remoto NO EN (especificar) – Si el cliente no pertenece al grupo...
Dominio/grupo de trabajo (NO) EN (especificar) – Si el cliente pertenece o no al dominio...
Máscara de nombre de equipo (especificar) – Si el nombre del equipo es...
Máscara IP (especificar) – Si el cliente pertenece al grupo definido por la máscara y la dirección IP...
Rango de IP (especificar) – Si el cliente pertenece al grupo definido por el rango de IP...
(NO) HA definido directiva (especificar) – Si el cliente adopta (o no) la política...

Para eliminar una regla de directiva, haga clic en el botón **Eliminar** en la ventana del **Administrador de directivas**. Haga clic en **Ejecutar reglas de la directiva ahora** si desea aplicar las reglas de inmediato.

5.3.7 Eliminación de directivas

Al igual que ocurre con la creación de reglas, sólo puede eliminar las directivas ubicadas en el servidor al que está conectado actualmente. Para eliminar directivas de otros servidores, debe conectarse directamente a ellos con la ERAC.

NOTA: *una directiva podría estar vinculada a otros servidores u otras directivas (como una directiva principal, como una directiva principal para servidores inferiores, como una directiva predeterminada para clientes primarios, etc.). Por lo tanto en algunos casos sería necesario sustituirla en lugar de eliminarla. Para ver las opciones disponibles para eliminar y sustituir, haga clic en el botón Eliminar directiva. Las opciones que se describen a continuación pueden estar o no a su disposición, según la posición que ocupe la directiva en cuestión dentro de la jerarquía de directivas.*

Nueva directiva para clientes principales con la directiva actualmente eliminada – Le permite seleccionar una directiva nueva para clientes principales que sustituya a la directiva que está eliminando. Los clientes principales pueden adoptar la **Directiva predeterminada para clientes principales**, así como otras directivas del mismo servidor (bien asignado manualmente, **Agregar clientes**, o forzado mediante las **Reglas de la directiva**). Para la sustitución puede usar cualquier directiva del servidor en cuestión, o bien una directiva replicada.

Nueva directiva principal para las directivas secundarias de la directiva actualmente eliminada (si existen) – Si una directiva que se va a eliminar servía como directiva principal para otras directivas secundarias, también se debe sustituir. Se puede reemplazar por una directiva de ese servidor, por una directiva replicada desde servidores superiores, o bien por la marca N/D, que significa que no se les asignará ninguna directiva principal que sustituya a las directivas secundarias. Le recomendamos encarecidamente que asigne una directiva sustituta, incluso cuando no haya directivas secundarias. Si otro usuario asignase una directiva secundaria a esa directiva durante el proceso de eliminación, podría surgir un conflicto.

Nueva directiva para clientes replicados con la directiva actualmente modificada o eliminada – Aquí puede seleccionar una directiva nueva para los clientes replicados desde servidores inferiores (aquellos que correspondían a la que está eliminando actualmente). Para la sustitución puede usar cualquier directiva del servidor en cuestión, o bien una directiva replicada.

Nueva directiva predeterminada para servidores inferiores – Si la directiva eliminada funciona como directiva virtual (consulte la **Configuración global de directivas**), debe sustituirse por otra (para obtener más información, consulte el apartado 5.3.3, "Directivas virtuales"). Para la sustitución puede usar cualquier directiva del servidor en cuestión, o bien la marca N/D.

Nueva directiva predeterminada para clientes principales – Si la directiva eliminada funciona de directiva virtual (consulte la **Configuración global de directivas**), debe sustituirse por otra (para obtener más información, consulte el apartado 5.3.3, "Directivas virtuales"). Puede usar una directiva del mismo servidor para la sustitución.

Se abrirá el mismo diálogo si desactiva la opción **Bajar replicable** para una directiva y hace clic en **Aceptar, Aplicar** o si selecciona otra directiva del árbol de directivas. Esto activará los elementos **Nueva directiva para clientes replicados con la directiva actualmente modificada o eliminada** o **Nueva directiva predeterminada para servidores inferiores**.

5.3.8 Configuración especial

Existen dos directivas adicionales que no se encuentran en el Administrador de directivas, sino en **Herramientas > Opciones del servidor > Otras opciones > Modificar configuración avanzada > ESET Remote Administrator > Servidor ERA > Configurar > Directivas**.

Intervalo de ejecución de directrices (minutos):
Esta función se aplica a directivas en el intervalo especificado. Recomendamos la configuración predeterminada.

Desactivar el uso de directivas:
Activar esta opción para cancelar la aplicación de directivas a los servidores. Recomendamos esta opción si existe algún problema con la directiva. Si desea evitar la aplicación de una directiva a algunos clientes, una mejor solución será asignar una directiva vacía.

5.3.9 Situaciones de implantación de directiva

5.3.9.1 Cada servidor es una unidad independiente y las directivas se definen localmente

Para esta situación, supongamos que tenemos una red pequeña, con un servidor principal y dos servidores inferiores. Cada servidor tiene varios clientes. En cada servidor hay creadas al menos una o más directivas. Los servidores inferiores están ubicados en las oficinas de las sucursales de la empresa. Ambos servidores están gestionados por administradores locales. Cada administrador decide para su servidor qué directivas se deben asignar a qué clientes. El administrador principal no interviene en las configuraciones que diseñan los administradores locales, y no asigna directiva alguna a los clientes de los servidores al cargo de éstos. Desde la perspectiva de las directivas de los servidores, esto implica que el Servidor A no tiene una **Directiva predeterminada para servidores inferiores**. También supone que el Servidor B y el Servidor C tienen la marca N/D u otra directiva local (distinta de la **Directiva principal predeterminada**) establecida como directiva principal. (p. ej., los servidores B y C no tienen ninguna directiva principal asignada desde el servidor superior).

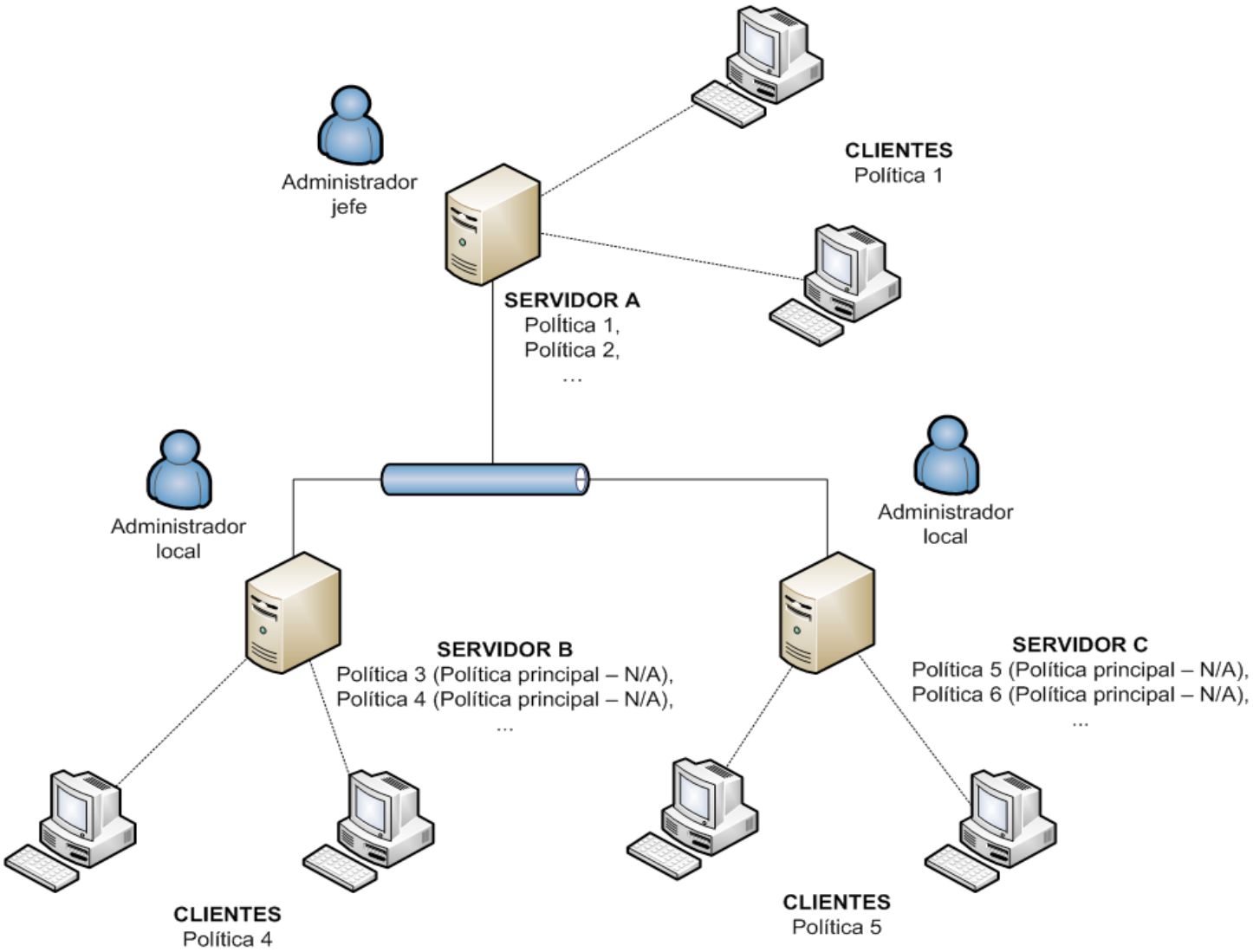


Figura 5-3

5.3.9.2 Cada servidor se administra individualmente. Las directivas se gestionan localmente, pero la Directiva principal predeterminada se hereda del servidor superior

La configuración de la situación anterior también se aplica a ésta. Sin embargo, el servidor A tiene activada la Directiva predeterminada para servidores inferiores y las directivas de los servidores inferiores heredan la configuración de la Directiva principal predeterminada del servidor maestro. En esta situación, los administradores locales tienen un alto grado de autonomía para configurar directivas. Mientras que las Directivas secundarias de los servidores inferiores pueden heredar la Directiva principal predeterminada, los administradores locales aún pueden modificarla según sus propias directivas.

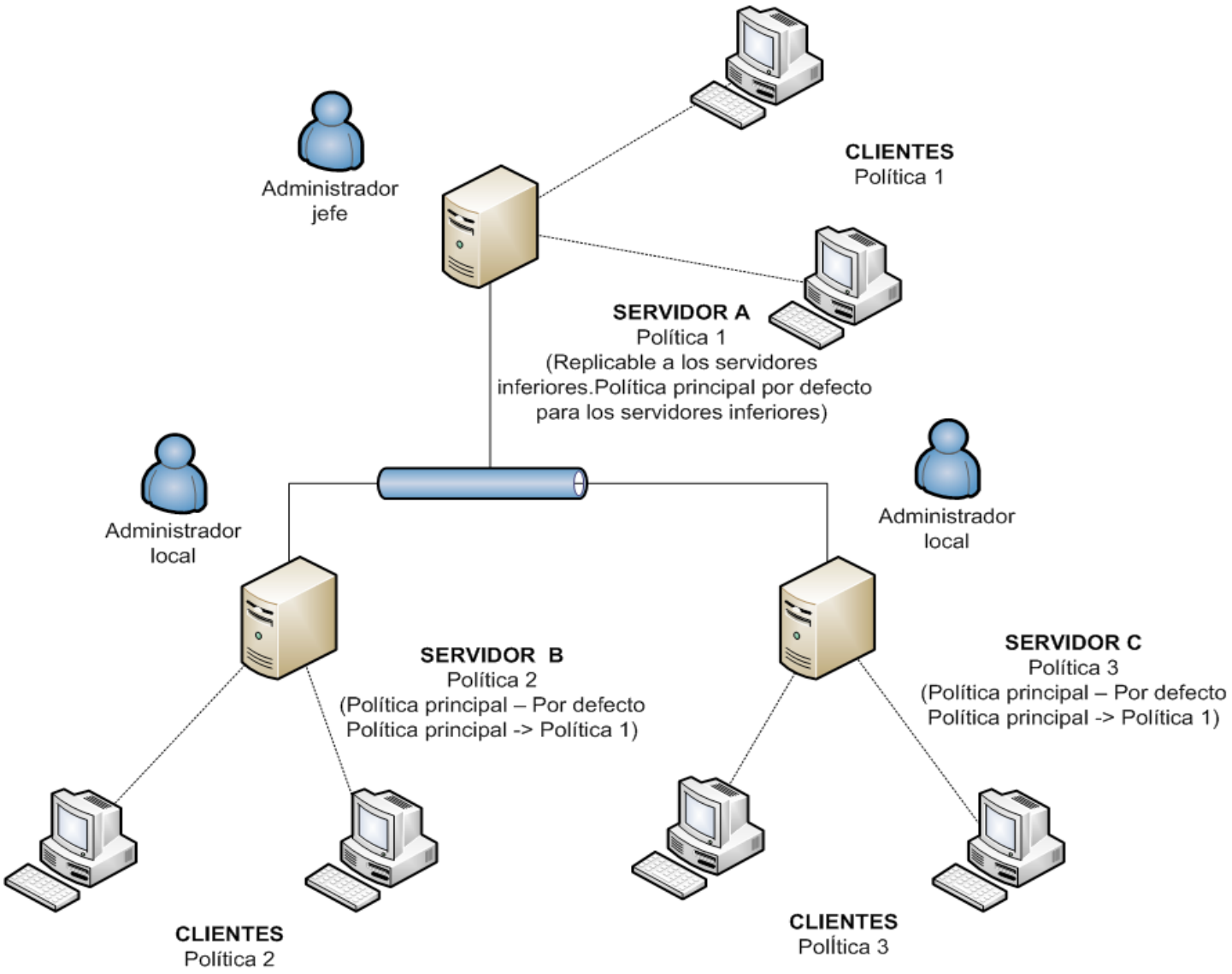


Figura 5-4

5.3.9.3 Heredar directivas de un servidor superior

El modelo de red para esta situación es el mismo de las dos situaciones anteriores. Además, el servidor maestro, junto a la Directiva principal predeterminada, contiene otras directivas, que se pueden replicar en sentido descendente y sirven como directivas principales para los servidores inferiores. Para la Directiva 1 (vea la figura 5-5) está activado el atributo **Anular directivas secundarias**. El administrador local sigue teniendo un alto grado de autonomía, pero el administrador principal define qué directivas se replican en sentido descendente y cuáles de ellas funcionan como directivas principales para las directivas locales. El atributo **Anular...** establece que las configuraciones de las directivas seleccionadas tengan prioridad y anulen las establecidas en los servidores locales.

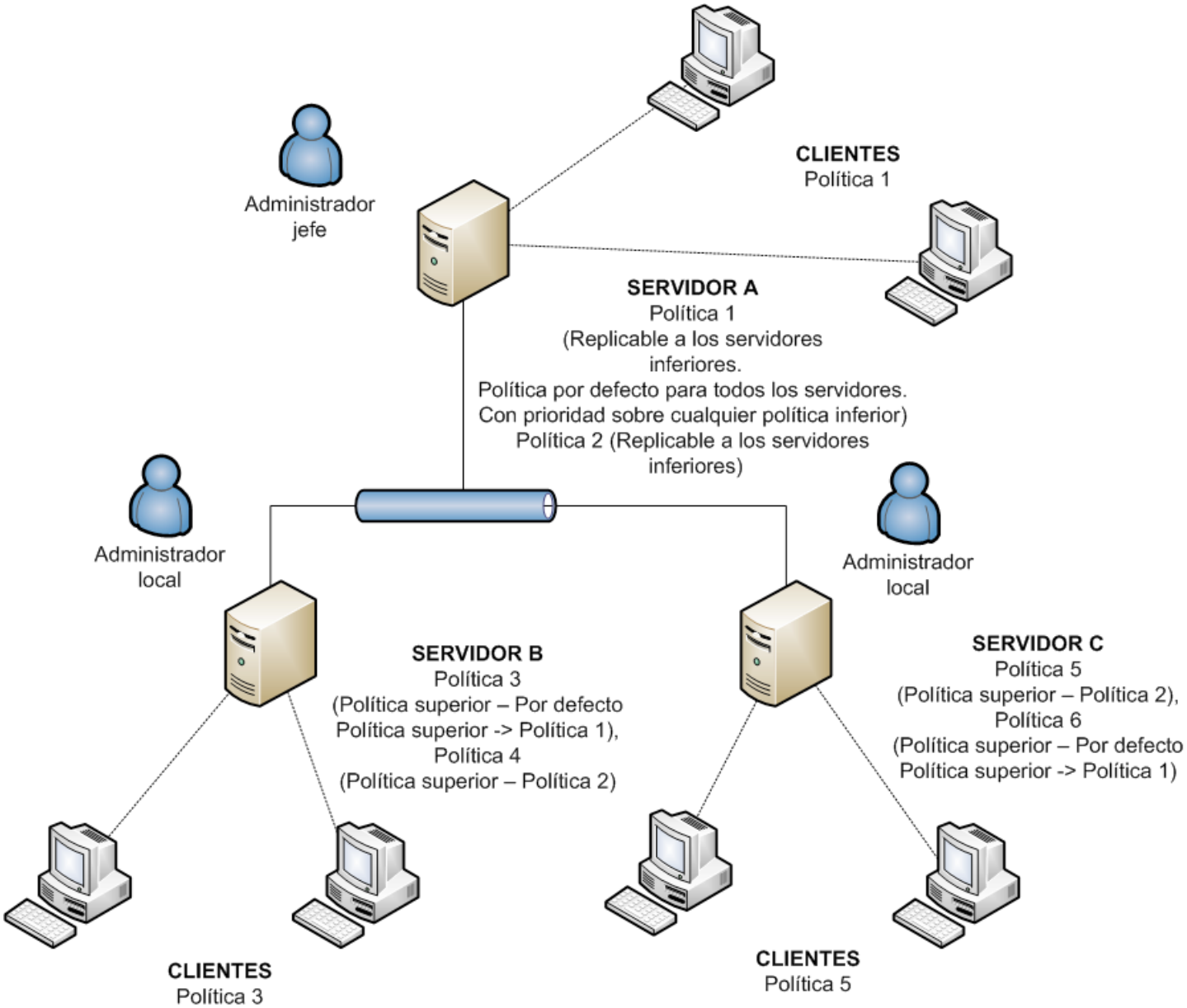


Figura 5-5

5.3.9.4 Asignación de directivas sólo desde el servidor superior

Esta situación representa un sistema de administración de directivas centralizado. Las directivas para los clientes se crean, modifican y asignan exclusivamente en el servidor principal. El administrador local no tiene derechos para modificarlas. Todos los servidores inferiores tienen una directiva básica, que está vacía (llamada Directiva del servidor). Esta directiva también funciona como la Directiva principal predeterminada para clientes principales.

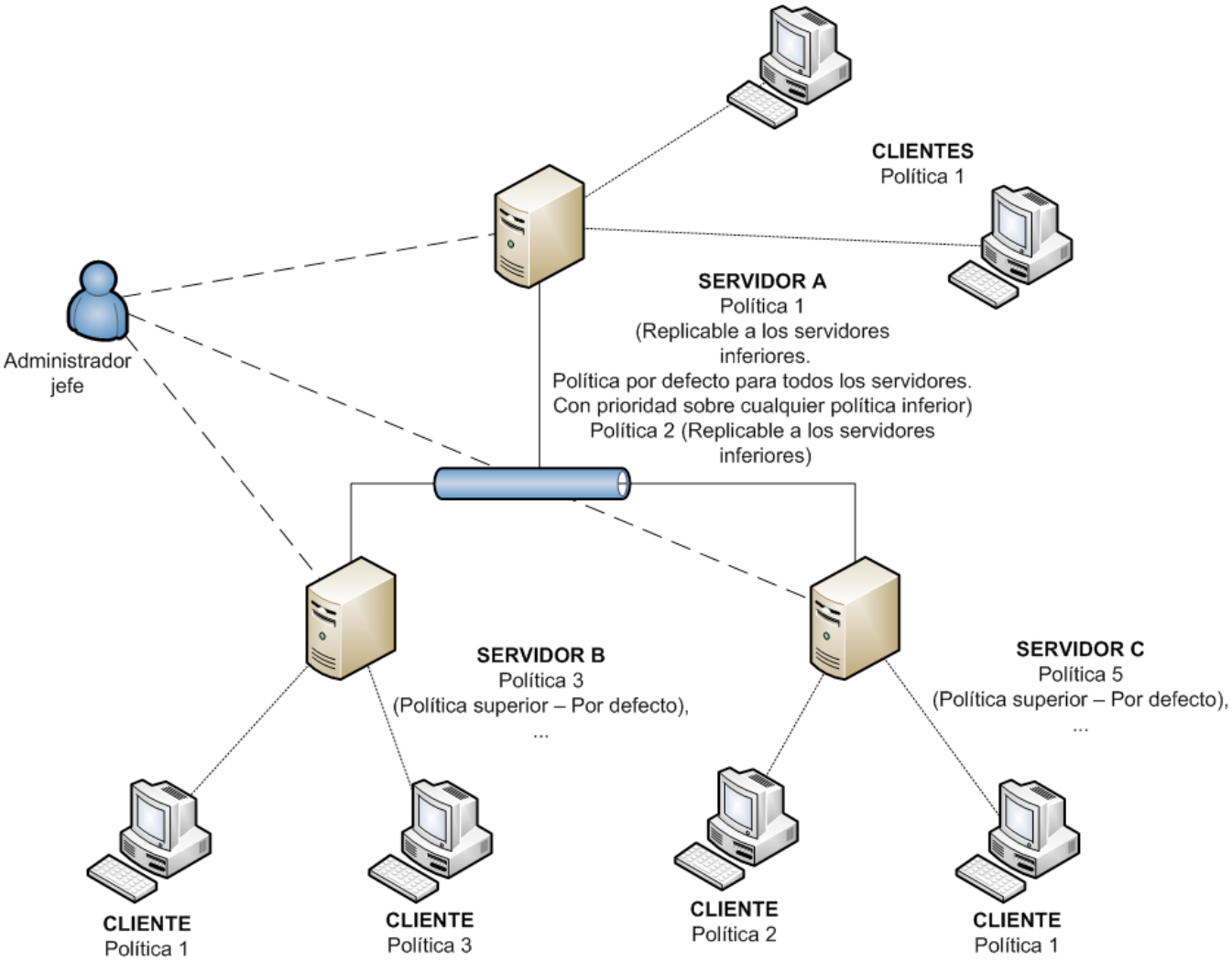


Figura 5-6

5.3.9.5 Uso de las reglas de la directiva

El siguiente ejemplo incluye la asignación automática de directivas, basándose en las reglas de la directiva. Este es un método complementario y debería usarse junto con las situaciones descritas anteriormente, no como una situación independiente.

Si cada servidor está a cargo de un administrador local, cada uno de estos administradores puede crear reglas de directiva individuales para sus clientes. En esta situación es importante que no haya conflictos entre las reglas de las directivas, como sucedería si el servidor superior asignase una directiva a clientes basada en las reglas de la directiva, mientras que el servidor inferior, simultáneamente, asignase directivas independientes basadas en las reglas de directiva locales.

En resumen, un sistema centralizado reduce en gran medida la probabilidad de que surjan conflictos, ya que todo el proceso de administración tiene lugar en el servidor principal.

5.3.9.6 Uso de grupos locales

En algunas situaciones, asignar directivas a grupos de clientes puede complementar a las situaciones anteriores. Los grupos se pueden crear manualmente, o bien mediante la opción **Sincronizar con Active Directory** (consulte el apartado 5.2, "Grupos"). Para ello, puede usar la opción para asignar una directiva suelta (**Agregar clientes > Agregar especial**), o bien distribuir directivas automáticamente mediante las **Reglas de la directiva**.

5.4 Notificaciones

La capacidad de notificar a los administradores de la red y del sistema acerca de eventos importantes es un aspecto esencial de la seguridad e integridad de la red. Una advertencia temprana acerca de un error o de la presencia de código malicioso puede evitar la pérdida de grandes cantidades de tiempo y dinero, que harían falta para solucionar el problema si éste surgiese más tarde. Los tres apartados siguientes describen las opciones de notificación que ofrece el ERA.

5.4.1 Administrador de notificaciones

Para abrir la ventana principal del Administrador de notificaciones, haga clic en **Herramientas > Administración de notificaciones**.

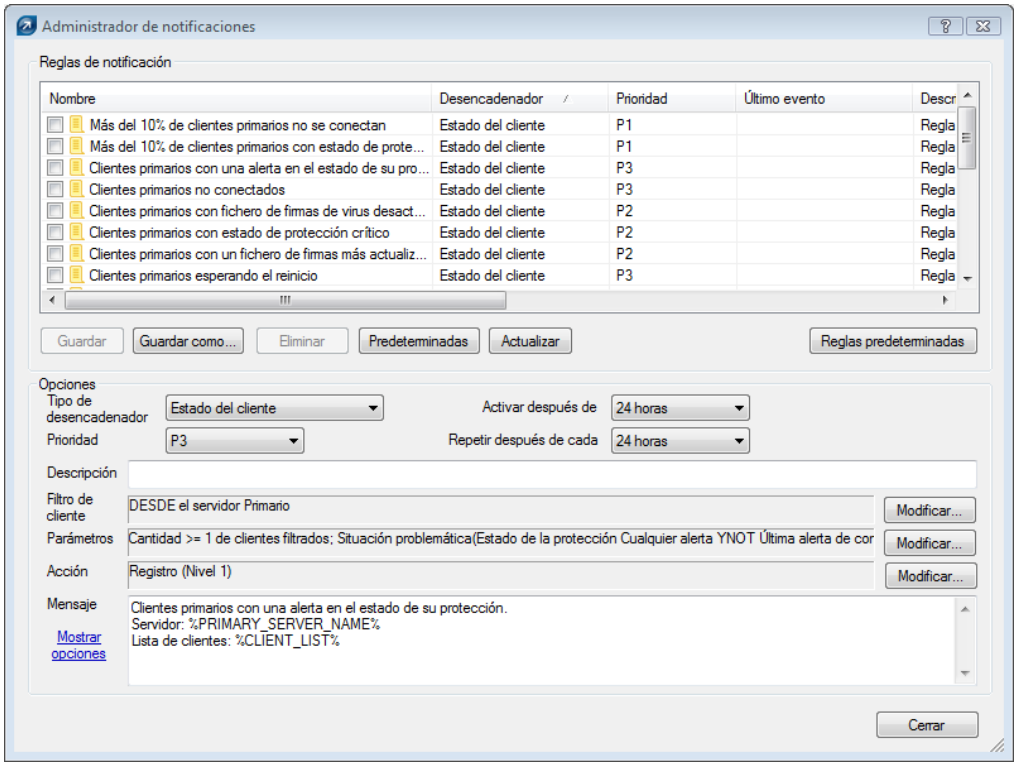


Figura 5-7: Ventana del Administrador de notificaciones

La ventana principal está dividida en dos secciones. La sección Reglas de notificación, en la parte superior de la ventana, contiene una lista de las reglas existentes (ya sean predefinidas o definidas por los usuarios). Para generar mensajes de notificación hay que seleccionar una regla de esta sección. De forma predeterminada, no hay notificaciones activadas. Por lo tanto, recomendamos que compruebe si sus reglas están activas.

Los botones funcionales situados bajo la lista de reglas son **Guardar** (para guardar modificaciones hechas en una regla), **Guardar como...** (para guardar modificaciones hechas en una regla con un nombre nuevo), **Eliminar, Restaurar valores predeterminados** (para restaurar la configuración predeterminada de una regla), y **Actualizar** (para actualizar la lista con reglas predeterminadas).

La sección **Opciones**, situada en la mitad inferior de la ventana, proporciona información sobre la regla que está seleccionada en ese momento. Todos los campos y opciones de esta sección están descritos mediante la regla de ejemplo de la sección 5.4.2, "Creación de reglas".

En cada regla, puede especificar el criterio que activa la regla, llamado desencadenador. Están disponibles estos desencadenadores:

- **Estado del cliente –** La regla se ejecutará si hay problemas en algún cliente
- **Estado del servidor –** La regla se ejecutará si hay problemas en algún servidor
- **Suceso de tarea finalizada –** La regla se ejecutará después de que finalice la tarea especificada
- **Suceso de cliente nuevo –** La regla se ejecutará si se conecta un cliente nuevo al servidor (se incluyen los clientes replicados)
- **Suceso de registro nuevo –** La regla se ejecutará si se encuentra el suceso especificado en algún registro

De acuerdo con el tipo de desencadenador, se pueden activar o desactivar otras opciones de reglas. Por tanto recomendamos crear primero desencadenadores al crear reglas nuevas.

El menú desplegable **Prioridad** permite definir la prioridad de la regla. **P1** es la prioridad más alta, **P5** es la más baja. La prioridad no afecta en modo alguno a la funcionalidad de las reglas. Para asignar una prioridad a los mensajes de notificación, se puede usar la variable %PRIORITY%. En el menú **Prioridad**, hay un campo llamado **Descripción**. Le recomendamos que se escriba una descripción informativa para cada regla, como "regla que advierte sobre las infecciones que se detecten".

En cuanto el sistema detecte el evento desencadenador de un cliente o unos clientes determinados y encuentre la regla que debe ejecutar, se aplicará el filtro de clientes. El filtro se puede asignar a cualquier regla que involucre a clientes. Para acceder a la configuración del filtro, haga clic en **Modificar** en la sección **Filtro de clientes**. En la ventana que se abre, defina los parámetros de filtrado de clientes. Al aplicar una regla, sólo se tomarán en consideración los clientes que satisfagan los criterios del filtro. Los criterios de filtrado son:

- **DESDE el servidor primario –** sólo los clientes del servidor principal (se puede usar la forma negativa NO DESDE)
- **Servidor primario EN –** Incluye al servidor principal en el resultado
- **TIENE marca "Nuevo" –** Clientes destacados con la marca "Nuevo" (también se puede aplicar la forma negativa **NO TIENE**).
- **Grupos del administrador remoto EN –** Clientes pertenecientes al grupo especificado
- **Dominio/grupo de trabajo EN –** Clientes que pertenecen al dominio especificado
- **Máscara de nombre de equipo –** Clientes con el nombre de equipo especificado
- **Máscara IP –** Clientes que tengan la máscara de IP especificada
- **Rango IP –** Clientes dentro del rango de direcciones IP especificado
- **TIENE directiva definida –** Clientes que tengan asignada la directiva especificada (también se puede usar la forma negativa **NO TIENE**).

Tras haber indicado un filtro de clientes para la regla de notificación, haga clic en **Aceptar** y diríjase a los parámetros de las reglas. Los parámetros de clientes definen qué condiciones han de cumplir un cliente o un grupo de clientes para que se ejecute la acción de notificación. Para ver qué parámetros están disponibles, haga clic en el botón **Modificar...** en la sección **Parámetros**.

La disponibilidad de los parámetros depende del tipo de desencadenador seleccionado. A continuación hay una lista completa de parámetros disponibles mediante el tipo de desencadenador.

Estos parámetros están disponibles para los desencadenadores de la regla Estado del cliente:

- **Cantidad –** Porcentaje de clientes que se requiere para activar la regla
- **Estado de la protección: todas las advertencias –** Cualquier alerta que se encuentre en la columna Estado de la protección
- **Estado de protección: advertencias graves –** Cualquier advertencia grave que se encuentre en la columna Estado de la protección
- **Versión de la base de firmas de virus –** Problema con la base de datos de firmas de virus (3 valores posibles)
  - **Anterior –** La base de datos de firmas de virus es la versión anterior a la actual
  - **Anterior o N/D –** La base de datos de firmas de virus es una versión más antigua que la actual (no es la anterior)
  - **Más reciente –** La base de datos de firmas de virus es más reciente que la del servidor
- **Advertencia de última conexión –** La última conexión se estableció antes del período de tiempo especificado
- **Con último suceso de amenaza –** La columna Amenaza contiene una advertencia de amenaza
- **Con último suceso –** La columna Último suceso contiene una entrada
- **Con último suceso de cortafuegos –** La columna Suceso de cortafuegos contiene una entrada de suceso de cortafuegos
- **Con marca "nuevo" –** El cliente tiene la marca "Nuevo"
- **Esperando para reiniciar –** El cliente está esperando para reiniciarse
- **Amenaza encontrada del último análisis –** Número de amenazas especificadas que se encontraron en el cliente durante el último análisis
- **Amenaza no limpiada del último análisis –** Número especificado de amenazas no eliminadas que se encontraron durante el último análisis

Todos los parámetros se pueden negar, pero no pueden utilizarse todas las negaciones. Resulta adecuado negar sólo los parámetros que incluyan dos valores lógicos: verdadero y no verdadero. Por ejemplo, el parámetro **Con marca "nuevo"** sólo cubre a los clientes con la marca "nuevo". La forma negativa del parámetro, por tanto, implica a todos los clientes que no llevan tal marca.

Todas las condiciones mencionadas se pueden combinar e invertir de manera lógica. El menú desplegable de **La regla se aplica** cuando ofrece dos opciones:

- **se cumplen todas las opciones –** La regla sólo se aplicará si se cumplen **todos** los parámetros específicos
- **se cumplen alguna de las opciones –** La regla sólo se aplicará si se cumple al menos **una** condición

Estos parámetros están disponibles para los desencadenadores de Estado del servidor:

- **Servidor actualizado –** El servidor está actualizado
- **Servidor no actualizado –** El servidor no se ha actualizado durante un período mayor al especificado
- **Registros del servidor –** El registro del servidor contiene estos tipos de entradas:
  - **Errores –** Mensajes de error
  - **Errores+Advertencias –** Mensajes de error y advertencia
  - **Filtrar entradas del registro por tipo –** Active esta opción para especificar qué entradas de advertencias y errores se deben visualizar en el registro del servidor. Tenga en cuenta que para que las notificaciones funcionen correctamente, el nivel de detalle del registro (**Herramientas > Opciones del servidor > Registro**) debe estar configurado en el nivel correspondiente. De otro modo, las reglas de notificación no detectarán nunca un desencadenador en el registro del servidor. Están disponibles estas entradas del registro:
    - **ADSI_SYNCHRONIZE –** Sincronización con el grupo Active Directory
    - **CLEANUP –** Tareas de limpieza del servidor
    - **CREATEREPORT –** Generación de informes a petición
    - **DEINIT –** Apagado del servidor
    - **INIT –** Inicio del servidor
    - **INTERNAL –** Mensaje interno del servidor
    - **LICENSE –** Administración de licencias
    - **MAINTENANCE –** Tareas de mantenimiento del servidor
    - **NOTIFICATION –** Administración de notificaciones
    - **PUSHINST –** Instalación impulsada
    - **RENAME –** Cambio de nombre en la estructura interna
    - **REPLICATION –** Replicación del servidor
    - **POLICY –** Administración de directiva
    - **POLICYRULES –** Reglas de directiva
    - **SCHEDREPORT –** Informes generados automáticamente
    - **SERVERMGR –** Administración de subproceso interno del servidor
    - **SESSION –** Conexiones de red del servidor
    - **THREATSENSE –** ThreatSense.NET – Envío de información estadística
    - **UPDATER –** Creación de servidor de actualización local y actualización del servidor

UPDATER es un ejemplo de parámetro útil, ya que envía un mensaje de notificación cuando el administrador de notificaciones encuentra en los registros del servidor un problema relacionado con la creación de un servidor local de actualización y con las actualizaciones.

- **Expiración de la licencia –** La licencia ha caducado, o bien caducará en el número de días indicado. Seleccione la opción **Mostrar advertencia sólo si esta acción va a provocar que el número de clientes de la licencia disminuya por debajo del número real de clientes de la base de datos del servidor** para que se envíe una notificación si la caducidad va a causar que se reduzca el número de clientes por debajo del número de clientes conectados actualmente.
- **Limitar licencia –** Si el porcentaje de clientes libres cae por debajo del valor especificado

Los siguientes parámetros están disponibles para los disparadores de **Suceso de registro nuevo**:

- **Tipo de registro –** Seleccione **Registro de sucesos, Registro de amenazas** o **Registro de cortafuegos**
- **Nivel de registro –** Nivel de las entradas de registro en el registro en cuestión
  - **Nivel 1 – Advertencias graves –** Sólo errores graves (o críticos)
  - **Nivel 2 – Anteriores + Advertencias –** Igual que 1, pero además con las notificaciones de alertas
  - **Nivel 3 – Anteriores + Normal –** Igual que 2, pero además con las notificaciones informativas
  - **Nivel 4 – Anteriores +Diagnóstico –** Igual que 3, pero además con las notificaciones de diagnóstico
- **1.000 repeticiones en 60 minutos –** Escriba el número de repeticiones y seleccione el período de tiempo para indicar la frecuencia que debe alcanzar el suceso para enviar la notificación. La frecuencia predeterminada son 1.000 repeticiones en una hora.
- **Cantidad –** Número de clientes (ya sea en total o como un porcentaje)

Los demás tipos de desencadenador no tienen parámetros específicos.

Si se cumplen los parámetros especificados para una regla, se ejecuta automáticamente la acción definida por el administrador. Para configurar acciones, haga clic en **Modificar...** en la sección **Acción**. El editor de acciones presenta estas opciones:

- **Correo electrónico –** El programa envía el texto de notificación de la regla a la dirección de correo electrónico especificada, escriba un **Asunto** y haga clic en **Para** para abrir la libreta de direcciones.
- **Captura del SNMP –** Genera y envía una notificación SNMP
- **Ejecutar (en el servidor) –** Active esta opción y especifique qué aplicación se ejecutará en el servidor
- **Registrar en archivo (en el servidor) –** Genera entradas de registro en el archivo de registro especificado. Se puede configurar el **Nivel de detalle** de este registro.
- **Registro –** Registra notificaciones en los registros de los servidores. Se puede configurar el **Nivel de detalle** de las mismas.

Para que esta característica funcione correctamente, debe activar el registro en el servidor de ERA (**Herramientas > Opciones del servidor > Registro**).

El formato de la notificación se puede modificar en el cuadro de diálogo **Mensaje**, en la sección inferior de la ventana principal del Administrador de notificaciones. En el texto se pueden usar variables especiales, con esta sintaxis: *%VARIABLE_NAME %*. Para ver la lista de las variables que tiene a su disposición, haga clic en **Mostrar opciones**.

- **Server_Last_Updated –** Fecha de la última actualización
- **Primary_Server_Name –** Nombre del Servidor Primario
- **Rule_Name –** Nombre de la regla
- **Rule_Description –** Descripción de la regla
- **Client_Filter –** Parámetros del filtro de clientes
- **Client_Filter_Short –** Configuración del filtro de clientes (fórmula abreviada)
- **Client_List –** Lista de clientes
- **Triggered –** Fecha de la última notificación enviada (no se incluyen las repeticiones)
- **Triggered Last –** Fecha de la última notificación enviada (no se incluyen las repeticiones)
- **Priority –** Prioridad de la regla de notificación
- **Log_Text_Truncated –** Texto de registro que ha activado la notificación (truncado)
- **Task_Result_List –** Lista de tareas finalizadas
- **Parámetros –** Parámetros de la regla
- **Last_Log_Date –** Fecha del último registro
- **License_Info_Merged –** Información de licencia (resumen)
- **License_Info_Full –** Información de licencia (completa)
- **License_Days_To_Expiry –** Días hasta la fecha de caducidad
- **License_Clients_Left –** Espacios libres en la licencia actual para que más clientes se conecten con el servidor
- **Actual_License_Count –** Número de clientes conectados actualmente al servidor

El parámetro especificado en último lugar es el de hora y fecha. La activación de la regla se puede retrasar hasta un plazo de tiempo que va desde una hora a tres meses. En caso de que desee activar la regla lo antes posible, establezca en el menú desplegable **Activar después de** después de la opción **Lo antes posible**. El Administrador de notificaciones se activa de manera predeterminada cada 10 minutos, así que si selecciona la opción **Lo antes posible**, la tarea debería realizarse en un plazo de 10 minutos o menos. Si se selecciona un período de tiempo específico en este menú, la acción se realizará automáticamente después de que transcurra dicho período (siempre y cuando se cumpla la condición que fija la regla).

El menú Repetir después de cada... le permite especificar un intervalo de tiempo, tras el cual se repetirá la acción. Sin embargo, sigue siendo necesario que se cumpla la condición para activar la regla. En **Servidor > Otras opciones > Modificar configuración avanzada > ESET Remote Administrator > Servidor > Configuración > Notificaciones > Intervalo de procesamiento de notificaciones (minutos)** puede indicar el intervalo de tiempo en el que el servidor comprobará y ejecutará las reglas activas.

El valor predeterminado es de 10 minutos. No le recomendamos que lo reduzca, ya que podría ralentizar notablemente el funcionamiento del servidor.

De forma predeterminada, la ventana del Administrador de notificaciones contiene reglas predefinidas. Para activar una regla, seleccione la casilla de verificación adyacente. A su disposición tiene las reglas de notificación que figuran a continuación. Si están activadas y se cumplen las condiciones de las reglas, generarán entradas de registro.

- **Más del 10 % de clientes primarios no se conectan –** Si hay más de un 10 por ciento de clientes que no se han conectado al servidor durante más de una semana. Esta regla se ejecuta lo antes posible.
- **Más del 10 % de clientes primarios con estado de protección crítico –** Si más del 10 por ciento de clientes generaron una advertencia grave en el estado de protección y no se han conectado durante más de una semana. Esta regla se ejecuta lo antes posible.
- **Clientes primarios con advertencia de estado de protección –** Si hay como mínimo un cliente con una advertencia de estado de protección que no se haya conectado al servidor durante al menos una semana
- **Clientes primarios no conectados –** Si hay como mínimo un cliente que no se haya conectado al servidor durante más de una semana
- **Clientes primarios con base de firmas de virus desactualizada –** Si hay un cliente con una base de datos de firmas de virus que sea una o dos versiones más antigua que la más actual y que no ha estado desconectado del servidor durante más de una semana
- **Clientes primarios con estado de protección crítico –** Si hay un cliente con una advertencia de estado de protección crítico que no ha estado desconectado del servidor durante más de una semana
- **Clientes primarios con una base de firmas de virus más actualizada que el servidor –** Si hay un cliente con una base de firmas de virus más actualizada que la del servidor y que no ha estado desconectado durante más de una semana
- **Clientes primarios esperando el reinicio –** Si hay un cliente esperando el reinicio que no ha estado desconectado durante más de una semana
- **Clientes primarios con una infección no eliminada en un análisis del ordenador –** Si hay un cliente cuyo análisis del equipo no elimine como mínimo una infección y que no ha estado desconectado durante más de una semana. Esta regla se ejecuta lo antes posible.
- **Tarea finalizada –** Si se finalizó una tarea en un cliente. Esta regla se ejecuta lo antes posible.
- **Nuevos clientes primarios –** Si un cliente nuevo se ha conectado al servidor. Esta regla se ejecuta lo antes posible.
- **Nuevos clientes replicados –** si hay un cliente replicado nuevo en la lista de clientes. La regla se ejecuta transcurrida una hora.
- **Posible brote de virus –** Si la frecuencia de las entradas del registro de amenazas supera las 1.000 advertencias graves en una hora en, como mínimo, el 10 % de todos los clientes.
- **Posible ataque de red –** Si la frecuencia de las entradas del registro del cortafuegos personal de ESET supera las 1.000 advertencias graves en una hora en, como mínimo, el 10 % de todos los clientes.
- **Servidor actualizado –** Si el servidor ha sido actualizado
- **Servidor no actualizado –** Si el servidor no se ha actualizado durante más de cinco días. Esta regla se ejecuta lo antes posible.
- **Error en el texto del informe del servidor –** Si el registro del servidor contiene una entrada de error.
- **Expiración de licencia –** Si la licencia actual va a caducar en 20 días o menos y, después de la caducidad, el número máximo de espacios libres para clientes será menor que el número de clientes actual. Esta regla se ejecuta lo antes posible.
- **Límite de la licencia –** Si el número de espacios libres para clientes desciende por debajo del 10 % del total de espacios disponibles.

Si no se indica lo contrario, todas las reglas se ejecutan y se repiten transcurridas 24 horas, aplicándose al servidor principal y a los clientes primarios.

5.4.1.1 Notificaciones mediante captura del SNMP

El SNMP (protocolo simple de administración de red) es un protocolo de administración sencillo y muy empleado apto para la supervisión e identificación de problemas de red. Una de las operaciones de este protocolo es la captura, que envía datos específicos. En ERA, utilizamos la captura para enviar mensajes de notificación.

Para que la herramienta de captura se ejecute de forma eficaz, debe instalarse y configurarse correctamente el protocolo SNMP en el mismo equipo que el ERAS (**Inicio > Panel de control > Agregar o quitar programas > Agregar o quitar componentes de Windows**). Debe configurarse el servicio de SNMP tal y como se describe en este artículo: http://support.microsoft.com/kb/315154. En el ERAS, es necesario activar una regla de notificación de SNMP.

Las notificaciones se pueden ver en el administrador de SNMP, el cual debe estar conectado a un servidor de SNMP en el que se vaya a importar el archivo de configuración eset_ras.mib. El archivo es un componente estándar de una instalación de ERA y suele ubicarse en la carpeta C:\Archivos de programa\ESET\ESET Remote Administrator\Servidor\snmp\.

5.4.2 Creación de reglas

Los siguientes pasos muestran cómo crear una regla que enviará una notificación por correo electrónico al administrador en caso de problema con el estado de protección de alguna estación de trabajo cliente. También se guardará la notificación en un archivo llamado log.txt.

1) Establezca el menú desplegable **Tipo de desencadenador** como **Estado del cliente**

2) Deje las opciones **Prioridad, Activar después de:** y **Repetir después de cada:** en los valores predefinidos. Se asignará automáticamente la prioridad 3 a la regla y se activará tras 24 horas.

3) En el campo **Descripción**, escriba **notificación de estado de protección para clientes HQ**

4) Haga clic en **Modificar...** en la sección **Filtro de clientes** y active sólo la condición que fija la regla de sección **Grupos ERA EN**. En la parte inferior de esta ventana haga clic en el enlace **especificar** y escriba **HQ** en la nueva ventana. Haga clic en **Agregar** y a continuación en **Aceptar** (dos veces) para confirmar. Esto designa que la regla sólo se aplicará a clientes del grupo HQ.

5) Especifique más parámetros para la regla en **Parámetros > Modificar...** Anule todas las selecciones salvo la de **Estado de la protección: todas las advertencias**.

6) Continúe con la sección **Acción** y haga clic en el botón **Modificar...** En la ventana **Acción**, active **Correo electrónico**, especifique los destinatarios (**Para...**) y **Asunto** para el correo electrónico. A continuación seleccione la casilla de verificación **Registrar en archivo** y escriba el nombre y la ruta del archivo de registro que se va a crear. Como opción, puede seleccionar el **Nivel de detalle** del archivo de registro. Haga clic en **Aceptar** para guardar la acción.

7) Finalmente, utilice el área de texto de **Mensaje** para especificar el nivel de detalle que se enviará en el cuerpo del correo electrónico cuando se active la regla. Ejemplo: "El cliente %CLIENT_LIST % informa de un problema de estado de protección".

8) Haga clic en **Guardar como...** para crear un nombre para la regla, por ejemplo, "problemas del estado de protección" y seleccione la regla en la lista de reglas de notificación.

La regla terminada debe parecerse a la de la Figura 5-8:

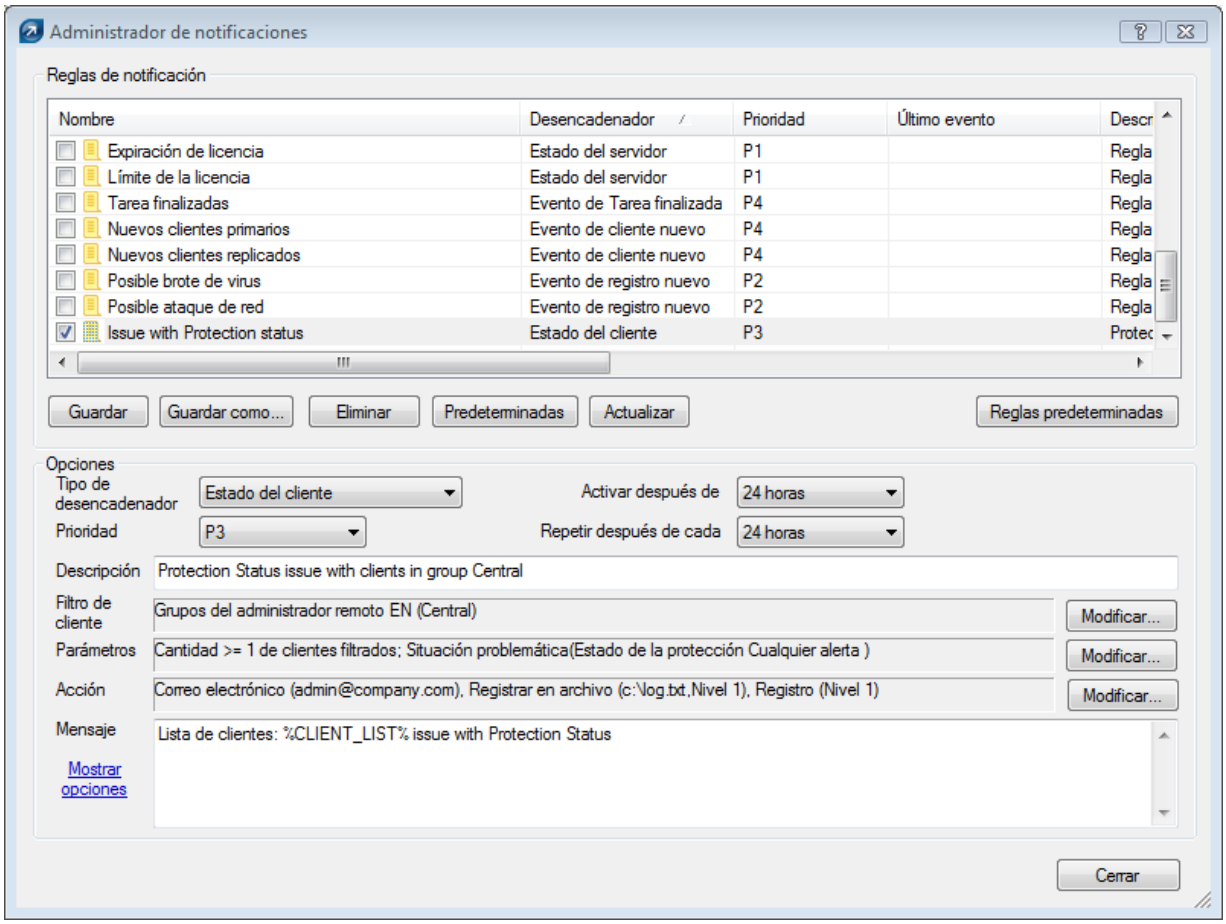


Figura 5-8 Ejemplo de regla de notificación

La regla está actualmente activa. En caso de problema con el estado de protección de un cliente del grupo HQ, se ejecutará la regla. El administrador recibirá una notificación de correo electrónico con un archivo adjunto que contendrá el nombre del cliente problemático. Haga clic en **Cerrar** para salir del Administrador de notificaciones.

5.5 Información detallada de los clientes

ERA le permite extraer de las estaciones de trabajo cliente la información sobre los procesos que se ejecutan, los programas de inicio, etc. Dicha información se puede recuperar con la herramienta integrada ESET SysInspector, que se integra directamente con el ERAS. Junto con otras funciones de utilidad, ESET SysInspector examina en profundidad el sistema operativo y crea los registros del sistema. Para abrirlo, haga clic en **Herramientas > ESET SysInspector** desde el menú principal de la ERAC.

En caso de problemas con un cliente específico, puede solicitar un registro de ESET SysInspector de ese cliente. Para ello, haga clic con el botón secundario en el panel Clientes y seleccione **Solicitar datos – Solicitar información de SysInspector**. Sólo se pueden obtener registros de los productos de generación 4.x y posterior. Las anteriores no son compatibles con esta característica. Haga clic en el enlace **solicitud de registro** para abrir una nueva ventana con las siguientes opciones:

- **Crear instantánea (recordar el registro resultante también en el cliente) –** Guarda una copia del registro en el equipo cliente.

- **Incluir comparación con la última instantánea antes de la hora especificada –** Muestra un registro comparativo. Los registros comparativos se crean al combinar el registro actual con uno anterior si está disponible. ERA elegirá el primer registro anterior a la fecha especificada.

Haga clic en **Aceptar** para obtener los registros seleccionados y guardarlos en el servidor. Para abrir y ver los registros, continúe de la siguiente manera.

Las opciones de ESET SysInspector para estaciones de trabajo cliente individuales pueden encontrarse en la ficha **Propiedades del cliente – SysInspector**. La ventana se divide en tres secciones. La sección superior muestra un texto informativo sobre los registros más recientes del cliente en cuestión. Haga clic en **Actualizar** para cargar la información más reciente.

La sección intermedia de la ventana **Solicitar opciones** es casi idéntica a la ventana que aparece en el proceso descrito anteriormente sobre la solicitud de registros de estaciones de trabajo cliente. El botón **Solicitar** se utiliza para conseguir un registro de ESET SysIspector del cliente.

La sección inferior se compone de estos botones:

- **Ver –** Abre el registro de la sección superior directamente en ESET SysInspector

- **Guardar como... –** Guarda el registro actual en un archivo. La opción **A continuación, ejecute el Visor de SysInspector de ESET para ver el archivo** abre automáticamente el registro tras guardarlo (igual que tras hacer clic en **Ver**).

La generación y visualización de nuevos archivos de registro se puede ralentizar con el cliente local, debido al tamaño del registro y la velocidad de la transferencia de datos. La fecha y la hora asignados a un registro de **Propiedades del cliente > SysInspector** marca la fecha y la hora de envío al servidor.

6. Informes

La ficha Informes (panel **Herramientas > Informes**) se utiliza para convertir la información estadística en gráficos o tablas. Estos se pueden guardar y procesar más tarde con el formato Valor separado por coma (.csv) utilizando las herramientas de ERA para proporcionar gráficos y demás imágenes. De forma predeterminada, ERA guarda el resultado en formato HTML. La mayor parte de los informes relacionados con infecciones se generan a partir del registro de amenazas.

Para buscar y seleccionar estilos gráficos, use el menú desplegable **Estilo** de la sección **Informe**..

ERA proporciona varias plantillas predefinidas para la creación de informes. Para seleccionar un informe, utilice el menú desplegable **Tipo**:

- **Amenazas principales**
  Lista de las amenazas detectadas con mayor frecuencia.

- **Clientes principales con más amenazas**
  Enumera las estaciones de trabajo cliente más "activas" (medido por la cantidad de amenazas detectadas).

- **Progreso de amenazas**
  Progreso de los sucesos de malware (cantidad).

- **Progreso comparativo de amenazas**
  Progreso de sucesos de malware de las amenazas seleccionadas (con filtro) en comparación con la cantidad total de amenazas.

- **Amenazas por análisis**
  Cantidad de alertas de amenazas de los módulos de programa individuales.

- **Amenazas por objeto**
  Número de alertas de amenazas según la ruta por la que intentaron infiltrarse (correos electrónicos, archivos o sectores de inicio).

- **Clientes principales combinados / Amenazas principales**
  Combinación de los tipos anteriores.

- **Amenazas principales combinadas / Progreso de amenazas**
  Combinación de los tipos anteriores.

- **Amenazas principales combinadas / Progreso comparativo de amenazas**
  Combinación de los tipos anteriores.

- **Informe de clientes, Informe de amenazas, Informe de eventos, Informe de análisis, Informe de tareas**
  Informes típicos que se pueden ver en las fichas **Clientes, Registro de amenazas, Registro de eventos, Registro de análisis** o **Tareas**.

- **Informe exhaustivo**
  Resumen de – Clientes principales combinados/Amenazas principales – Amenazas principales combinadas/ Progreso comparativo de amenazas – Progreso de amenazas

En la sección **Filtro** puede utilizar los menús desplegables **Clientes destino** o **Amenaza** para seleccionar qué clientes o virus se incluirán en el informe.

Se pueden configurar otros detalles haciendo clic en el botón **Configuración adicional...** Esta configuración se aplica a la mayoría de los datos del título y de los tipos de diagramas gráficos utilizados. Sin embargo, también puede filtrar los datos según el estado de los atributos seleccionados, así como elegir el formato de informe que va a utilizar (.html, .csv).

La ficha Intervalo le permite definir un intervalo para el que se generará el informe:

- **Actual**
  Sólo se incluirán en el informe los sucesos producidos en un periodo de tiempo concreto. Por ejemplo, si se creó un informe el miércoles y el intervalo se establece como **Semana actual**, a continuación se incluirán los sucesos del domingo, el lunes, el martes y el miércoles.

- **Completado**
  Sólo se incluirán en el informe los sucesos producidos en un periodo concreto y cerrado (es decir, todo el mes de agosto o una semana entera, desde el domingo al siguiente sábado). Si se selecciona la opción **Agregar también el periodo actual**, el informe incluirá los sucesos del último periodo completado hasta el momento de creación.

Ejemplo:

Queremos crear un informe que incluya los sucesos de la última semana, es decir, desde el domingo al siguiente sábado. Queremos que este informe se genere el siguiente miércoles (tras el sábado).

En la ficha **Intervalo**, seleccione **Completado** y **1 semana**. Quitar **Agregar también el periodo actual**. En la ficha **Tareas programadas** establezca la **Frecuencia** como **Semanal** y seleccione **Miércoles**. Se pueden configurar las demás opciones a discreción del administrador.

- **Desde / Hasta**
  Utilice este ajuste para definir un periodo para el que se generará el informe.

La ficha Tareas programadas le permite definir y configurar un informe automático en un periodo o intervalos concretos (utilizando la sección **Frecuencia**).

Uso de la casilla de giro **Ejecutar el** y el seleccionador de fecha de **Inicio** para escribir la hora y la fecha a la que se va a generar el informe. Haga clic en el botón **Seleccionar destino...** de la sección **y almacenar Resultado en** para especificar dónde se va a guardar el informe. Se pueden guardar los informes en el ERAS (de forma predeterminada), enviar por correo electrónico a una dirección concreta o exportarlos a una carpeta. La última opción resulta útil si se envía el informe a una carpeta compartida en la intranet de su empresa, donde la pueden ver otros empleados.

Para enviar por correo electrónico informes generados, necesitará escribir la información del servidor SMTP y la dirección del remitente en **Herramientas > Opciones del servidor > Otras opciones** tal y como se describe en el apartado 7.8.1, "Configuración SMTP".

Para definir un intervalo de fechas fijas para el proceso de generación de informes, utilice las opciones de la sección **Intervalo**. Puede definir la cantidad de informes generados (**Finalizar después del**), o una fecha que el proceso de generación de informes no debe superar (**Finalizar el**).

Para guardar la configuración de los informes definidos en una plantilla, haga clic en los botones **Guardar** o **Guardar como...** Si va a crear una plantilla nueva, haga clic en el botón **Guardar como...** y asígnele un nombre.

En la parte superior de la ventana de la consola, en la sección Plantillas de informe, podrá ver nombres de plantillas ya creadas. Junto a los nombres de plantilla, puede encontrar información sobre tiempo e intervalos y cuándo se generan informes de acuerdo con las plantillas preseleccionadas. Haga clic en el botón **Generar ahora** (asegúrese de que se ha seleccionado la ficha **Opciones**) para generar un informe en cualquier momento sin importar lo programado.

Los informes generados previamente pueden verse en la ficha **Informes generados**. Para obtener más opciones, seleccione los informes individuales (o múltiples) y utilice el menú contextual (clic con el botón secundario).

Las plantillas de la lista **Favoritos** se pueden usar más tarde para generar inmediatamente informes nuevos. Para mover una plantilla a Favoritos, haga clic con el botón secundario en el informe y en **Agregar a favoritos** desde el menú contextual.

7. Configuración del servidor de ESET Remote Administrator (ERAS)

7.1 Ficha Seguridad

Las soluciones de seguridad de generación 3.x, 4.x de ESET (ESET Smart Security, etc.) ofrecen una protección mediante contraseña para la comunicación sin descifrar entre clientes y ERAS (comunicación mediante protocolo TCP, puerto 2222).

Las anteriores versiones (2.x) no cuentan con esta función. Para ofrecer una compatibilidad con las versiones anteriores, debe activarse el modo **Activar acceso sin autentificación para clientes**.

La ficha Seguridad contiene opciones que permiten al administrador usar soluciones de seguridad 2.x, 3.x y 4.x en la misma red, de forma simultánea.

- **Contraseña para la consola (acceso de administrador, acceso de sólo lectura)**
  Permite especificar una contraseña para el administrador y un número limitado de usuarios para protegerse de cambios no autorizados en la configuración de la ERAC.

- **Contraseña para los clientes (productos de seguridad de ESET)**
  Establece una contraseña para el acceso de clientes al ERAS.

- **Contraseña para la replicación**
  Establece una contraseña para los servidores de ERA inferiores si se replican en el ERAS en cuestión.

- **Contraseña del programa de instalación remota de ESET (Agente)**
  Establece una contraseña para que el agente del instalador acceda al ERAS. Es relevante para las instalaciones remotas.

- **Activar acceso sin autentificación para clientes (productos de seguridad de ESET)**
  Permite el acceso al ERAS a los clientes que no disponen de una contraseña válida especificada (si la contraseña actual es distinta de la *Contraseña para clientes*).

- **Activar acceso sin autentificación para replicación**
  Permite el acceso al ERAS a los clientes de servidores ERA inferiores que no cuentan con una contraseña válida para la replicación especificada.

- **Activar acceso sin autentificación para el programa de instalación remota de ESET (Agente)**
  Permite el acceso al ERAS a los clientes de servidores ERA inferiores que no cuentan con una contraseña válida para la replicación especificada.

NOTA: *si se activa la autentificación en ERAS y en todos los clientes [generación 3.x, 4.x], se puede desactivar la opción* ***Activar acceso sin autentificación para clientes***.

7.2 Pestaña Mantenimiento del servidor

Si se configura correctamente en la ficha Mantenimiento del servidor, la base de datos del ERAS se mantendrá y optimizará automáticamente, sin necesidad de establecer configuraciones adicionales. De forma predeterminada, las entradas y los registros con más de seis meses se eliminan, y la tarea *Compactar y reparar* se realiza cada quince días. Se puede acceder a todas las opciones de mantenimiento del servidor desde **Herramientas > Opciones del servidor > Mantenimiento del servidor.**

Entre estas opciones están:

- **Conservar sólo las últimas X amenazas de cada cliente**
  Conserva sólo el número especificado de incidentes de virus de cada cliente.

- **Conservar sólo los últimos X registros de cortafuegos de cada cliente**
  Conserva sólo el número especificado de registros de cortafuegos de cada cliente.

- **Conservar sólo los últimos X sucesos de cada cliente**
  Conserva sólo el número especificado de sucesos del sistema de cada cliente.

- **Conservar sólo los últimos X registros de análisis de cada cliente**
  Conserva sólo el número especificado de registros de análisis de cada cliente.

- **Eliminar clientes no conectados durante los últimos X meses (días)**
  Elimina todos los clientes que no se han conectado al ERAS durante un número de meses (o días) mayor que el especificado.

- **Eliminar registros de amenazas con más de X meses (días)**
  Elimina todos los incidentes de virus anteriores al número de meses (o días) especificado.

- **Eliminar registros de cortafuegos con más de X meses (días)**
  Elimina todos los registros de cortafuegos anteriores al número de meses (o días) especificado.

- **Eliminar registros de sucesos con más de X meses (días)**
  Elimina todos los sucesos del sistema anteriores al número de meses (o días) especificado.

- **Eliminar registros de análisis con más de X meses (días)**
  Elimina todos los registros de análisis anteriores al número de meses (o días) especificado.

7.3 Servidor local de actualización

La función de servidor local de actualización permite al usuario crear un servidor de actualización local. Los equipos cliente no descargarán actualizaciones de firmas de virus de los servidores de ESET en Internet, sino que se conectarán a un servidor local de actualización en su red. La principal ventaja de esta solución es la conservación del ancho de banda de Internet para minimizar el tráfico de red, ya que únicamente se conecta el servidor local de actualización a Internet para las actualizaciones, en lugar de que lo hagan cientos de máquinas cliente. Esta configuración significa que es importante que el servidor local de actualización esté siempre conectado a Internet.

Advertencia: *un servidor local de actualización que ha realizado una actualización de componentes del programa (PCU) y que no se ha reiniciado puede provocar una avería. En este caso, el servidor no podría descargar NINGUNA actualización ni distribuirlas a las estaciones de trabajo cliente. NO DEFINA LA ACTUALIZACIÓN DE COMPONENTES DEL PROGRAMA PARA LOS PRODUCTOS DE SERVIDOR DE ESET. Esto no se aplica al servidor local de actualización creado en el ERAS.*

La función de servidor local de actualización está disponible en dos ubicaciones:

- ESET Remote Administrator (servidor local de actualización que se ejecuta físicamente dentro del ERAS, manejable desde la ERAC)

- ESET Smart Security Business Edition o ESET NOD32 Antivirus Business Edition (siempre que se haya activado Business Edition con una clave de licencia).

El administrador selecciona el método de activación de la función del servidor local de actualización.

En grandes redes, es posible crear varios servidores locales de actualización (por ejemplo, para varios departamentos de la empresa) y definir uno como servidor central (en la sede de la empresa) en cascada, de forma similar a la configuración de un ERAS con varios clientes.

El administrador debe insertar la clave de licencia del producto para un producto adquirido e indicar el nombre de usuario y la contraseña para permitir la función de servidor local de actualización en el ERAS. Si el administrador utiliza una clave de licencia, junto con un nombre de usuario y contraseña para ESET NOD32 Antivirus Business Edition, también se deben sustituir la clave de licencia original, la contraseña y el nombre de usuario para actualizaciones superiores de ESET Smart Security Business Edition.

7.3.1 Funcionamiento del servidor local de actualización

El equipo que aloja el servidor local de actualización deberá estar siempre en funcionamiento y conectado a Internet o a un servidor local de actualización superior para la replicación. Los paquetes del servidor local de actualización se pueden descargar de dos formas:

1. Utilizando el protocolo HTTP (recomendado)
2. Usando una unidad de red compartida (SMB)

Los servidores de actualización de ESET usan el protocolo HTTP con autentificación. Un servidor local de actualización central debería acceder a los servidores de actualización con un nombre de usuario (generalmente, EAV-XXXXXXX) y una contraseña.

El servidor local de actualización, que forma parte de ESET Smart Security/ESET NOD32 Antivirus cuenta con un servidor HTTP integrado (variante 1).

NOTA: *si decide usar el servidor HTTP integrado (sin autentificación), compruebe que no sea accesible desde fuera de su red (es decir, por clientes no incluidos en su licencia). El servidor no debe ser accesible desde Internet.*

De forma predeterminada, el servidor HTTP escucha en el puerto TCP 2221. Compruebe que ninguna otra aplicación esté utilizando este puerto.

También se puede usar cualquier otro tipo de servidor HTTP. ERA también es compatible con métodos de autentificación adicionales (por ejemplo, en Apache Web Server se usa el método .htaccess).

El segundo método (carpeta de red compartida) requiere el uso compartido (permisos de "lectura") de la carpeta que contiene los paquetes de actualización. En este caso, debe indicarse un nombre de usuario y una contraseña de usuario con permisos de "lectura" para la carpeta de actualización en la estación de trabajo cliente.

NOTA: *las soluciones cliente de ESET utilizan la cuenta de usuario SYSTEM y, por lo tanto, tienen permisos de acceso a la red diferentes que un usuario actualmente registrado. La autentificación se requiere incluso si la unidad de red es accesible para "Todos" y si el usuario actual también cuenta con acceso. Asimismo, use las rutas de acceso UNC para definir la ruta de red al servidor local. No se recomienda el uso del formato DISCO:\.*

Si decide usar el método de carpeta de red compartida (variante 2), se recomienda crear un único nombre de usuario (por ejemplo, NODUSER). Esta cuenta se usará en todos los equipos cliente con el único fin de descargar actualizaciones. La cuenta NODUSER deberá contar con permisos de "lectura" en la carpeta de red compartida que contiene los paquetes de actualización.

Para la autentificación a una unidad de red, indique los datos de autentificación de forma completa: GRUPODETRABAJO\Usuario o DOMINIO\Usuario.

Además de la autentificación, también debe definir el origen de las actualizaciones para las soluciones cliente de ESET. El origen de la actualización puede ser una dirección URL a un servidor local (http://nombre_del_servidor_local_de_actualización:puerto) o ruta de acceso UNC a una unidad de red: (\\nombre_del_servidor_local_de_actualización\nombre_de_uso_compartido).

7.3.2 Tipos de actualizaciones

Además de las actualizaciones de la base de firmas de virus (que pueden incluir actualizaciones de kernel de software de ESET), también se cuenta con actualizaciones de componentes del programa. Las actualizaciones de componentes del programa añaden nuevas funciones a los productos de seguridad de ESET y requieren un reinicio.

El servidor local de actualización permite que el administrador desactive la descarga automática de actualizaciones del programa desde servidores de actualización de ESET (o desde un servidor local de actualización superior) y desactive la distribución a los clientes. El administrador podrá ejecutar la distribución más tarde manualmente, si está seguro de que no se producirán conflictos entre la versión nueva y las aplicaciones existentes.

Esta función es especialmente útil si el administrador desea descargar y usar actualizaciones de base de firmas de virus cuando sólo cuenta con una nueva versión de programa disponible. Si se usa una versión anterior del programa junto con la versión más reciente de base de firmas de virus, el programa seguirá ofreciendo la máxima protección disponible. Aún así, se recomienda descargar e instalar la última versión del programa para acceder a las nuevas funciones de programa.

De forma predeterminada, los componentes del programa no se descargan automáticamente y deben configurarse manualmente en el ERAS. Para obtener más información, consulte la sección 7.3.3, "Cómo activar y configurar el servidor local de actualización".

7.3.3 Cómo activar y configurar el servidor local de actualización

Si el servidor local de actualización está directamente integrado en el ERA (un componente de Business Edition), debe conectarse al ERAS a través de la ERAC y seguir estos pasos:

- Desde la ERAC, haga clic en **Herramientas > Opciones del servidor... > Actualizaciones**.
- En el menú desplegable **Servidor de actualización:** elija **Seleccionar automáticamente** (las actualizaciones se descargarán de los servidores de ESET), o indique la ruta de acceso URL/UNC a un servidor local de actualización.

- Establezca el intervalo de actualización para las actualizaciones (se recomienda cada sesenta minutos).
- Si eligió **Seleccionar automáticamente** en el paso anterior, inserte el nombre de usuario (Actualizar nombre de usuario) y contraseña (Actualizar contraseña) que se enviaron después de la compra. Si accede a un servidor superior, indique un nombre de usuario de dominio válido y la contraseña en este servidor.
- Seleccione la opción **Crear servidor local de actualización** e indique una ruta de acceso válida a la carpeta en la que se guardarán los archivos de actualización. De forma predeterminada, es una ruta relativa a la carpeta del servidor local de actualización, siempre que la opción **Proporcionar archivos de actualización mediante el servidor HTTP interno** esté seleccionada y disponible en el puerto HTTP definido en el **Puerto de servidor HTTP** (2221, de forma predeterminada). Defina **Autentificación** en **NINGUNA**[6].

NOTA: *en caso de que surjan problemas con una actualización, seleccione la opción* ***Borrar la caché de actualización*** *para eliminar de la carpeta todos los archivos de actualización temporales.*

- La opción **PCU descargada del servidor local de actualización** permite activar el servidor local de actualización de los componentes del programa. Para configurar la creación de un servidor local de actualización de componentes del programa, acceda a **Otras opciones > Modificar configuración avanzada** y configure los parámetros de **ESET Remote Administrator > Servidor ERA > Configuración > Servidor local de actualización (o bien Servidor local de actualización para NOD32 versión 2)**.
- Seleccione los componentes de idioma para descargar en el apartado **Otras opciones > Modificar configuración avanzada...**, **Servidor ERA> Configuración > Servidor local de actualización > Crear servidor local de actualización para los componentes del programa seleccionados**. Seleccione los componentes para todas las versiones de idioma que se usarán en la red. Tenga en cuenta que descargar una versión de idioma que no está instalada en la red aumentará el tráfico de red de forma innecesaria.

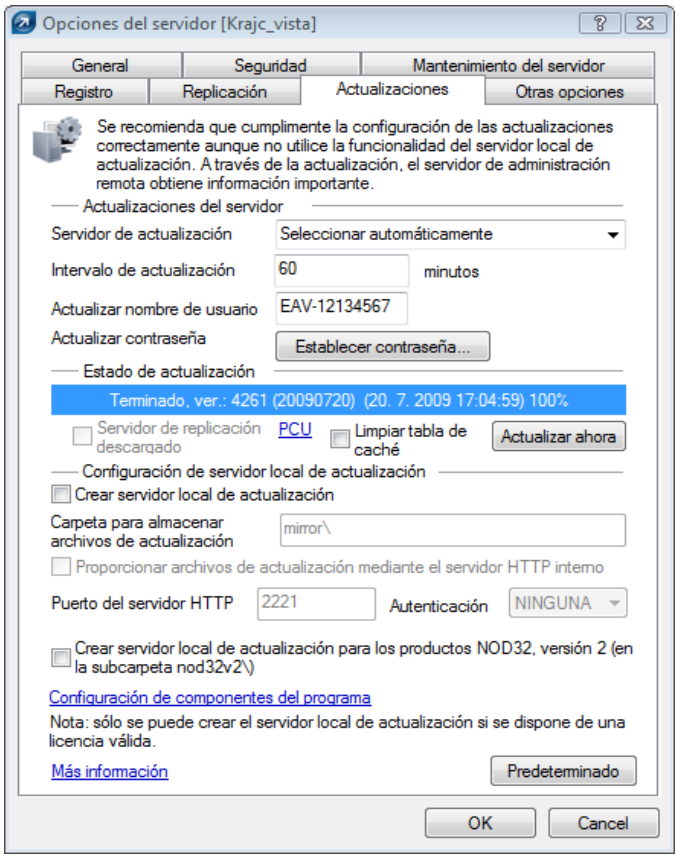


Figura 7-1

La función de servidor local de actualización también está directamente disponible desde la interfaz del programa en ESET Smart Security Business Edition y ESET NOD32 Antivirus Business Edition. Se deja a la discreción del administrador la decisión de decidir en cuál implantar el servidor local de actualización.

[6] Para obtener más información, consulte el apartado sobre autentificación en el servidor ERA.

Para activar y ejecutar el servidor local de actualización en ESET Smart Security Business Edition o ESET NOD32 Antivirus Business Edition, siga estos pasos:

1) Instale ESET Smart Security Business Edition o ESET NOD32 Antivirus Business Edition

2) En la ventana **Configuración avanzada** (**F5**), haga clic en **Varios > Licencias**. Haga clic en el botón **Agregar...**, busque el archivo *.lic y haga clic en **Abrir**. Se instalará la licencia y permitirá la configuración de la función de servidor local de actualización.

3) En la sección **Actualizar** haga clic en el botón **Configuración...** y seleccione la ficha **Servidor local de actualización**.

4) Seleccione la opción **Crear servidor local de actualización** y **Proporcionar archivos de actualización mediante el servidor HTTP interno**.

5) Indique la ruta de acceso al directorio de la carpeta (**Carpeta para almacenar archivos de actualización**) en la que se guardarán los archivos de actualización.

6) El **nombre de usuario** y la **Contraseña** sirven de datos de autentificación para estaciones de trabajo cliente que tratan de obtener acceso a la carpeta Servidor local de actualización. En la mayoría de los casos, no es necesario rellenar estos archivos.

7) Defina Autentificación en **NINGUNA**[7]

8) Seleccione los componentes para descargar[8] (seleccione los componentes para todas las versiones de idioma que se usarán en la red).

NOTA: *para mantener una funcionalidad óptima, recomendamos que active la descarga y el servidor local de actualización de los componentes de programa. Si esta opción está desactivada, sólo se actualiza la base de firmas de virus, no los componentes del programa. Si el servidor local de actualización se usa como parte del ERA, esta opción se puede configurar en la ERAC a través de* ***Herramientas > Opciones del servidor... > ficha Otras opciones > Modificar configuración avanzada... > ESET Remote Administrator > Servidor ERA > Configuración > Servidor de administración remota.*** *Active todas las versiones de idiomas del programa presentes en su red.*

7.3.4 Servidor local de actualización para clientes con NOD32 versión 2.x

ESET Remote Administrator también permite a un administrador crear copias de archivo de actualización para equipos cliente con ESET NOD32 Antivirus 2.x instalado. Para ello, haga clic en **Herramientas > Opciones del servidor > Actualizaciones > Crear servidor local de actualización para los productos NOD32, versión 2**. Esto sólo se aplica a ERA. El servidor local de actualización incluido en la solución cliente de Business Edition (v 3.x, 4.x) no contiene esta opción.

Si dispone de una mezcla de clientes 2.x, 3.x y 4.x en su red, se recomienda utilizar el servidor local de actualización integrado en ERA. Si ambos servidores locales de actualización están activados en el mismo equipo, uno en ERAS para clientes 2.x y otro en un cliente Business Edition, para clientes 3.x, 4.x, se podría provocar un conflicto entre dos servidores HTTP utilizando el mismo puerto TCP.

Las actualizaciones para clientes 2.x se guardan en la carpeta "nod32v2", una subcarpeta de la carpeta principal del servidor local de actualización. Está disponible a través de la dirección URL:

http://Nombre_del_servidor_local_de_actualización:puerto/nod32v2

o ruta de acceso UNC a una unidad de red:

\\Nombre_del_servidor_local_de_actualización\nombre_de_uso_compartido\nod32v2

ERA también puede descargar componentes de programa para clientes 2.x. Para seleccionar los componentes del programa para descargar, acceda a **Herramientas > Opciones del servidor... > ficha Otras opciones >**, haga clic en la sección **Modificar configuración avanzada... > Servidor ERA > Configuración > Servidor local de actualización para NOD32 versión 2**. Para minimizar el volumen de datos descargados, seleccione sólo las versiones de idioma presentes en su red.

---

[7] Para obtener más información acera de la autentificación, consulte el apartado 7.3.1, "Funcionamiento del servidor local de actualización".

[8] Los componentes sólo se muestran si están disponibles en los servidores de actualización de ESET.

7.4 Ficha Replicación

La replicación se utiliza en redes de gran tamaño, donde hay instalados varios servidores de ERA (p. ej., una empresa con varias sucursales). Para obtener más información, consulte la sección 2.3.3, "Instalación".

Las opciones de la ficha Replicación (***Herramientas > Opciones del servidor...***) se dividen en dos secciones:

- Configuración de la replicación "a"
- Configuración de la replicación "desde"

La **Configuración de la replicación "a"** se utiliza para configurar servidores inferiores de ERA. La opción **Activar replicación "a"** debe estar activada y debe haberse introducido la dirección IP o el nombre del ERAS maestro (servidor superior). Por tanto, los datos del servidor inferior se replican al servidor maestro. La configuración de la **replicación "desde"** permite a los servidores de ERA maestros (superiores) aceptar los datos enviados por los servidores de ERA inferiores o transferirlos a sus servidores maestros. La opción **Activar replicación "desde"** debe estar activada y los nombres de los servidores inferiores deben estar definidos (separados por una coma).

Estas dos opciones deben estar activadas para cualquiera de los servidores de ERA ubicados en la mitad de la jerarquía de la replicación (es decir, que tengan tanto servidores inferiores como superiores).

Todas las situaciones anteriores pueden verse en la imagen que se muestra a continuación. Los equipos de color beige representan servidores de ERA individuales. Cada ERAS se representa con su nombre (que debe ser el mismo que %ComputerName %, para evitar confusiones) y con la configuración correspondiente en la ventana de diálogo de la replicación.

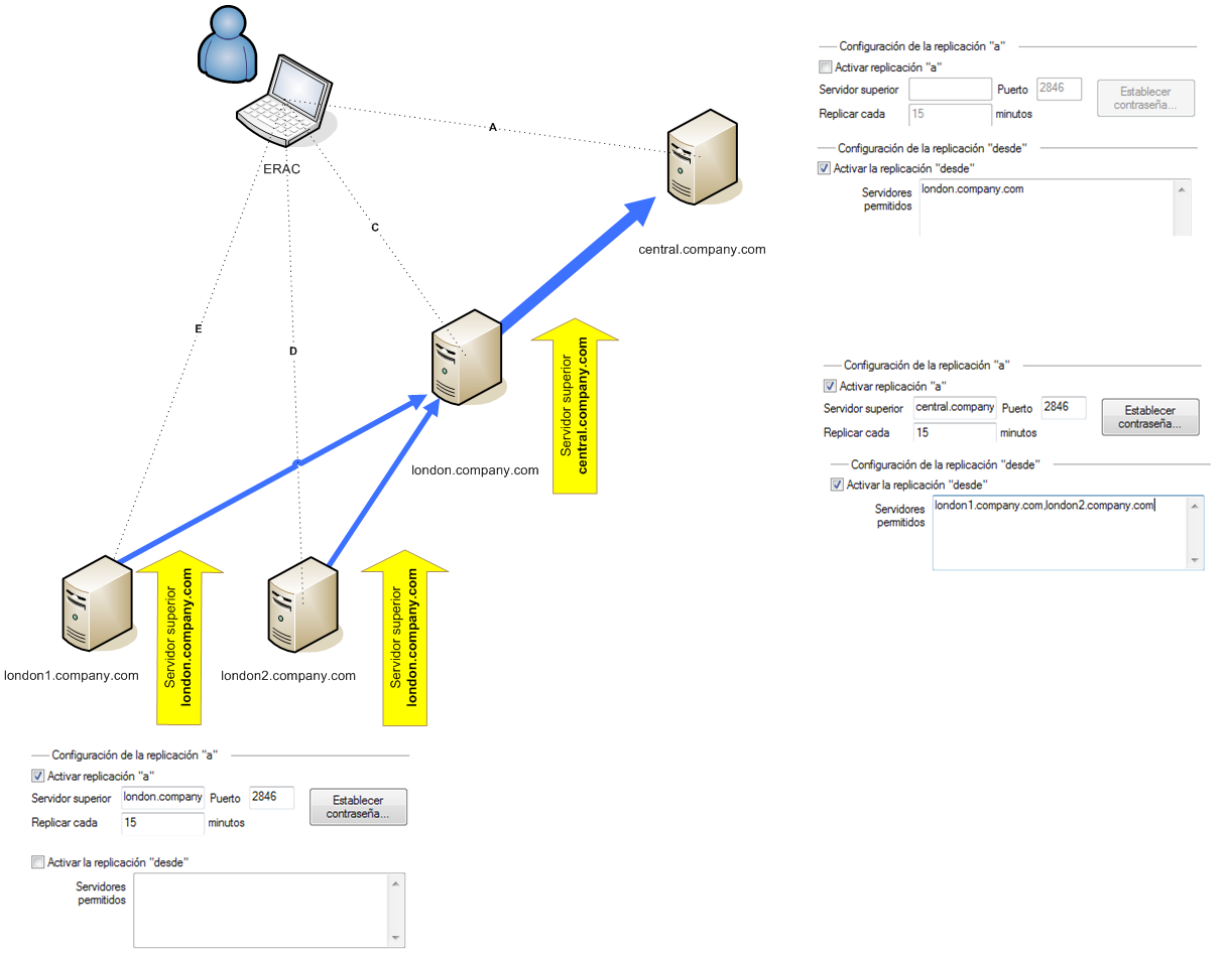


Figura 7-2

El resto de opciones que influyen en el comportamiento de la replicación de los servidores son, entre otras:

- **Replicar registro de amenazas, Replicar registro del cortafuegos, Replicar registro de sucesos, Replicar registro de análisis**
  Si se seleccionan estas opciones, toda la información que se muestra en la ficha **Clientes, Registro de amenazas, Registro de cortafuegos, Registro de sucesos, Registro de análisis,** y **Tareas** se replica en columnas y filas individuales. Es posible que la información que no se haya almacenado directamente en la base de datos sino en archivos individuales (es decir, con formato .txt o .xml) no se replique. Active estas opciones para poder replicar también las entradas de esos archivos.

- **Replicar automáticamente detalles del registro de amenazas, Replicar automáticamente detalles del registro de análisis, Replicar automáticamente detalles de clientes**
  Estas opciones activan la replicación automática de la información complementaria almacenada en archivos individuales. También pueden descargarse a petición haciendo clic en el botón **Solicitar**.

NOTA: *algunos registros se replican automáticamente, mientras que los registros detallados y los registros de configuración del cliente sólo se replican a petición. Esto sucede debido a que ciertos registros contienen grandes cantidades de datos que pueden no ser relevantes. Por ejemplo, un registro de análisis con la opción Registrar todos los archivos activada ocupará gran cantidad de espacio en el disco. Normalmente, dicha información no es necesaria y puede solicitarse manualmente. Los servidores secundarios no envían información automáticamente sobre clientes eliminados. Por tanto, los servidores superiores pueden continuar almacenando información sobre clientes eliminados recibida de los servidores inferiores. Si desea eliminar un cliente de la ficha Clientes en servidores superiores, seleccione la opción Activar la eliminación de clientes replicados en el servidor subyacente situado en* ***Opciones del servidor > Otras opciones > Modificar configuración avanzada > Configurar > Replicación*****.**

Para establecer el nivel de mantenimiento del registro en el ERAS, haga clic en **Herramientas > Opciones del servidor > Otras opciones > Modificar configuración avanzada... > Configurar > Mantenimiento de servidores.**

Si desea replicar solamente clientes con un cambio de estado, seleccione la opción **Herramientas > Opciones del servidor > Replicación > Marcar todos los clientes para la replicación mediante "Replicar ahora"**.

7.5 Ficha Registro

Durante su ejecución, el ERAS crea un registro (**Nombre de archivo de registro**) acerca de su actividad, que se puede configurar (Contenido del registro). Si está seleccionada la opción **Registrar en archivo de texto**, se crearán archivos de registro nuevos (**Alternar si tiene más de X MB**) y se borrarán diariamente (**Eliminar registros alternos con más de X días**).

La opción **Registrar en el registro de la aplicación del SO permite copiar la información en el registro del visor de eventos del sistema (Panel de control de Windows > Herramientas administrativas > Visor de eventos**).

En circunstancias normales, la opción **Registro de depuración de la base de datos** debería estar desactivada.

El resultado en forma de archivo de texto se guarda de forma predeterminada en la siguiente ubicación:
%ALLUSERSPROFILE %\Application data\Eset\Eset Remote Administrator\Server\logs\era.log

Le recomendamos que mantenga el contenido del registro en el Nivel 2 – Anteriores + Errores de sesión. Cambie el nivel de detalle del registro sólo si surgen problemas, o bien si así se lo aconseja el servicio de atención al cliente de ESET.

Haga clic en **Herramientas > Opciones del servidor > Otras opciones > Modificar configuración avanzada... > Configuración > Registro > Compresión de registro de depuración alterno** para configurar el nivel de compresión para registros alternos individuales.

7.6 Administración de licencias

Para que la ERA funcione correctamente, debe cargar un fichero de licencia. Después de la adquisición, las claves de licencia se le entregarán junto con el nombre de usuario y la contraseña en su dirección de correo electrónico. El **Administrador de licencias** sirve para gestionar las licencias.

En ERA 3.x y versiones posteriores, se ha agregado la compatibilidad para múltiples claves de licencia. Esta característica hace que administrar las claves de licencia sea mucho más cómodo.

Se puede acceder a la ventana principal del administrador de licencias desde **Herramientas > Administrador de licencias**.

Para agregar un fichero de licencia nueva:

1. Acceda a **Herramientas > Administrador de licencias** o pulse **CTRL + L** en el teclado.
2. Haga clic en **Examinar** y busque el archivo de fichero de licencia que desee (las claves de licencia tienen la extensión .lic.)
3. Haga clic en **Abrir** para confirmar.
4. Compruebe que la información de la clave de licencia es correcta y seleccione **Cargar en el servidor**
5. Haga clic en **Aceptar** para confirmar.

El botón **Cargar en el servidor** estará activo sólo si se ha seleccionado un fichero de licencia (mediante el botón **Examinar**). La información acerca de la clave de licencia que se muestra actualmente forma parte de la ventana. Esto le permite hacer una comprobación final antes de copiar la clave en el servidor.

La parte central de la ventana muestra información sobre el fichero de licencia que usa actualmente el servidor. Para ver detalles sobre todas las claves de licencia presentes en el servidor, haga clic en el botón **Detalles...**

ERAS puede seleccionar la clave de licencia más adecuada y combinar varias claves en una sola. Si existe más de una clave de licencia cargada, el ERAS tratará siempre de encontrar la clave que tenga más clientes y con la fecha de caducidad más lejana.

La capacidad de combinar varias claves funciona si todas las claves invocadas son propiedad del cliente. La combinación de licencias es un proceso sencillo que da lugar a una clave nueva que contiene a todos los clientes involucrados. La fecha de caducidad de la nueva clave de licencia es igual a la de la clave que tenga la fecha de caducidad más temprana.

La parte inferior de la ventana del administrador de licencias está dedicada a las notificaciones que aparecen cuando surge un problema relacionado con las licencias. Entre las opciones disponibles están:

- **Advertir si la licencia del servidor va a caducar en 20 días** – Muestra una advertencia X días antes de que la licencia caduque
- **Mostrar advertencia sólo si esta acción va a provocar que el número de clientes de la licencia disminuya por debajo del número real de clientes de la base de datos del servidor** – Active esta opción para que se muestre una advertencia sólo si la caducidad de la clave de licencia, o de una parte de la licencia, va a causar un descenso en el número de clientes que lo deje por debajo del número de clientes conectados actualmente o por debajo del número de clientes en la base de datos del ERAS.
- **Advertir si sólo queda un 10 % de clientes libres en las licencias del servidor** – El servidor mostrará una advertencia si el número de espacios libres para clientes car por debajo de un valor indicado (expresado como %)

El ERAS es capaz de combinar varias licencias procedentes de varios clientes. Esta función se activa mediante una clave especial. Si requiere una clave especial, especifíquelo en su pedido o póngase en contacto con el distribuidor de ESET local.

7.7 Ajustes avanzados

Para acceder a los ajustes avanzados de ERA, haga clic en **Herramientas > Opciones del servidor > Otras opciones > Modificar configuración avanzada**.

Los ajustes avanzados incluyen lo siguiente:

- **Uso máx. de espacio en disco (porcentaje)**
  En caso de superarse, es posible que algunas funciones del servidor no estén disponibles. Al conectar con el ERAS, la ERAC muestra una notificación si se supera el límite**.**
- **Codificación de protocolos de comunicación**
  Define el tipo de codificación. Recomendamos la configuración predeterminada.
- **Activar cambio de nombre de dirección MAC (de desconocido a válido)**
  Después de la reinstalación de una solución cliente de ESET que no es compatible con el envío de una dirección MAC (como ESET NOD32 Antivirus 2.x) en una solución cliente que sí lo es (como un cliente 3.x, 4.x), el antiguo registro cliente se convierte a uno nuevo. Recomendamos la configuración predeterminada (Sí).

- **Activar cambio de nombre de dirección MAC (de válido a desconocido)**
  Después de la reinstalación de una solución cliente de ESET que no es compatible con el envío de una dirección MAC (como ESET NOD32 Antivirus 2.x) en una solución cliente que sí lo es (como un cliente 3.x, 4.x), el antiguo registro cliente se convierte a uno nuevo. Recomendamos la configuración predeterminada (No).
- **Activar cambio de nombre de dirección MAC (de válido a otro válido)**
  Permite el cambio de nombre de direcciones MAC válidas. El valor predeterminado no permite el cambio de nombre, lo que significa que la dirección MAC es parte de la identificación única de los clientes. Desactive esta opción si existen varias entradas para un PC. También se recomienda desactivar esta opción si un cliente está identificado como el mismo cliente después de cambiar la dirección MAC.
- **Activar cambio de nombre del equipo**
  Permite el cambio de nombre de los equipos clientes. Si está desactivado, el nombre del equipo formará parte de la identificación única de los clientes.
- **Utilizar también el registro del servidor predeterminado durante la instalación impulsada**
  El ERAS permite al usuario definir el nombre de usuario y la contraseña sólo para la instalación remota por secuencia de comandos de inicio de sesión y correo electrónico. Active esta opción para usar los valores predefinidos también para las instalaciones remotas impulsadas.

7.8 Ficha Otras opciones

7.8.1 Configuración SMTP

- **Configuración SMTP (Servidor. Dirección del remitente, Nombre de usuario, Contraseña)**
  Algunas funciones del ERA requieren una correcta configuración del servidor SMTP. Estas funciones incluyen la instalación por correo electrónico remota y la generación de informes para su envío por correo electrónico.

7.8.2 Puertos

Puertos (Consola, Cliente, Puerto de replicación de este servidor, Instalador remoto de ESET)

Permite personalizar los puertos en los que ERAS escucha las comunicaciones, establecidos por:

- **Consola** (2223, de forma predeterminada)
- **Cliente** (2222, de forma predeterminada)
- El proceso de replicación (**Puerto de replicación** – 2846, de forma predeterminada)
- **Instalador remoto de ESET** (2224, de forma predeterminada)

7.8.3 Nuevos clientes

- **Permitir nuevos clientes**
  Si está desactivado, no se añadirán clientes nuevos en la ficha Clientes (incluso si los clientes nuevos se comunican con los servidores ERA, no serán visibles en la ficha Clientes).
- **Restablecer automáticamente la marca "Nuevo" según los nuevos clientes**
  Si está activada, la marca "Nuevo" se elimina de los clientes que se conectan al ERAS por primera vez. Para obtener más información, consulte la sección 3.4.3, "Ficha Clientes".

7.8.4 ThreatSense. Net

- **Activar reenvío de datos de ThreatSense. Net a servidores de ESET**
  Si se activa, el ERAS reenviará archivos sospechosos e información estadística de los clientes a los servidores de ESET. Tenga en cuenta que no siempre es posible para las estaciones de trabajo cliente enviar esta información directamente, debido a la configuración de la red.

8. Herramienta de mantenimiento de ERA

El objetivo de la herramienta de mantenimiento de ERA es ejecutar tareas específicas para el funcionamiento y mantenimiento del servidor. Está disponible haciendo clic en **Inicio -> Archivos de programa -> ESET Remote Administrator -> Servidor**. Cuando inicia la herramienta de mantenimiento de ERA, se muestra un asistente interactivo para ayudarle a realizar las tareas requeridas.

8.1 Información del servidor de ERA

La herramienta muestra un resumen de información sobre el servidor de ERA instalado. La información que se muestra se puede ver con más detalle, en una ventana independiente, haciendo clic en **Más información**, se puede copiar haciendo clic en **Copiar al Portapapeles** y se puede actualizar, haciendo clic en **Actualizar**. Una vez comprobada la información, acceda al paso siguiente haciendo clic en **Siguiente**.

8.2 Tipo de tarea

La herramienta de mantenimiento contiene la lista de las tareas disponibles. Al final de cada configuración de tarea, puede guardar los ajustes para la tarea actual haciendo clic en **Guardar todos los parámetros en un archivo**. Los ajustes se pueden usar en cualquier momento haciendo clic en **Cargar todos los parámetros de un archivo**. Cada paso individual en la configuración de una tarea cuenta con la opción de **Guardar todos los parámetros en un archivo** o **Cargar todos los parámetros de un archivo**.

8.2.1 Detener el servidor de ERA

Esta tarea detiene el servidor de ESET Remote Administrator.

8.2.2 Inicio del servidor de ERA

Esta tarea inicia el servidor de ESET Remote Administrator.

8.2.3 Transferencia de la base de datos

Esta tarea le permite convertir el formato de la base de datos. La herramienta puede convertir los formatos de estas bases de datos:

- MS Access
- MS SQL Server
- Oracle
- My SQL

El primer paso es seleccionar la base de datos.

Si la base de datos es una base de datos de MS Access, especifique la ruta al archivo .mdb. La ruta especificada durante la instalación del servidor de ERA se utiliza de forma predeterminada.
Todos los demás formatos de base de datos requieren parámetros adicionales para configurarse:

- Cadena de conexión: cadena especial que se usa para identificar la base de datos de origen
- Nombre de usuario: nombre de usuario para acceder a la base de datos
- Contraseña: contraseña para acceder a la base de datos
- Nombre de esquema: nombre de un esquema (disponible sólo para Oracle y MS SQL)

Haga clic en **Cargar configuración actual del servidor** para usar los parámetros actuales del servidor de ERA. Haga clic en **Probar conexión** para probar la conexión de la base de datos. Si no se puede establecer la conexión, compruebe los parámetros en busca de errores. Después de comprobar la base de datos con éxito, continúe haciendo clic en **Siguiente**.

Seleccione la base de datos de destino. Seleccione **Sustituir configuración de conexión del servidor** para conectar el servidor y usar la base de datos nueva después de la conversión. Si no selecciona esta opción, la nueva base de datos se creará sin actualización del servidor en la nueva versión de la base de datos.

Para todos los tipos de base de datos, además de la base de datos de MS Access, seleccione si desea crear las tablas de base de datos automáticamente (**Crear tablas en la base de datos automáticamente**) o insertar las tablas en la base de datos más adelante (**Ver secuencia de comandos > Guardar en archivo**) en el paso siguiente. Para una base

de datos MS SQL, la opción **Crear una base de datos nueva ESETRADB automáticamente** crea automáticamente una nueva base de datos MYSQL llamada ESETRADB. En el paso final, se confirma la conversión de la base de datos.

8.2.4 Copia de seguridad de la base de datos

Esta herramienta le permite crear un archivo de copia de seguridad de la base de datos. Los parámetros de la primera ventana son similares a los de la conversión de la base de datos (véase Transferencia de la base de datos). Aquí se selecciona la base de datos de origen. La base de datos de origen se copiará a un archivo de copia de seguridad en el paso siguiente.

Los parámetros opcionales de la parte inferior de la ventana permiten sobrescribir el archivo existente (**Sobrescribir si existe**) y detener el servidor de ESET Remote Administrator durante el proceso de copia de seguridad (**Detener el servidor durante el procesamiento de la tarea**). Haga clic en **Siguiente** para confirmar la ejecución de la tarea.

8.2.5 Restauración de la base de datos

Esta tarea le permite restaurar la base de datos a partir de un archivo de copia de seguridad Los parámetros de la primera ventana son similares a los de la conversión de la base de datos (véase Transferencia de la base de datos). Aquí se selecciona el tipo de la base de datos.

Para todos los tipos de base de datos, además de la base de datos de MS Access, seleccione si desea crear las tablas de base de datos automáticamente (**Crear tablas en la base de datos automáticamente**) o insertar las tablas en la base de datos más adelante (**Ver secuencia de comandos > Guardar en archivo**) en el paso siguiente. Para una base de datos MS SQL, la opción **Crear una base de datos nueva ESETRADB automáticamente** crea automáticamente una nueva base de datos MYSQL llamada ESETRADB. En el paso final, se confirma la conversión de la base de datos.

Seleccione el archivo desde el que, en el paso siguiente, va a restaurar la base de datos. Los parámetros opcionales situados en la parte inferior de la ventana le permiten importar desde un tipo de base de datos distinto del seleccionado en el paso anterior (**Permitir importar desde un tipo de base de datos diferente**), así como detener el servidor de ESET Remote Administrator durante la restauración de la base de datos (**Detener el servidor durante el procesamiento de la tarea**). Haga clic en **Siguiente** para confirmar la ejecución de la tarea.

8.2.6 Eliminar tablas

Así se eliminarán las tablas que haya actualmente en la base de datos. Como resultado, la base de datos volverá al estado en que se encontraba justo después de la instalación del servidor de ERA. Los parámetros de la primera ventana son similares a los de la conversión de la base de datos (véase Transferencia de la base de datos). Aquí se selecciona el tipo de la base de datos. En el paso siguiente se le solicitará que confirme la acción. Seleccione **Sí, acepto** y a continuación **Siguiente** para confirmar la acción.

8.2.7 Instalación de un fichero de licencia nueva

Para insertar una clave de licencia nueva que vaya a utilizar el servidor, escriba su ubicación.
Sobrescriba la clave existente si es necesario (**Sobrescribir si existe**) y reinicie el servidor si es necesario (**Forzar el inicio del servidor (si no se está ejecutando)**). Haga clic en **Siguiente** para confirmar y completar la acción.

8.2.8 Modificación de la configuración del servidor

Esta tarea inicia el editor de configuración (si está instalado). Al finalizar la tarea se abre la ventana del Editor de configuración, que le permitirá modificar la configuración avanzada del Servidor ERA. También se puede acceder a esta configuración mediante **Herramientas -> Opciones del servidor -> Otras opciones -> Modificar configuración avanzada**.

9. Resolución de problemas

9.1 Preguntas frecuentes

Este capítulo contiene soluciones a las preguntas más frecuentes y problemas relacionados con la instalación y funcionamiento de ERA.

9.1.1 Problemas con la instalación de ESET Remote Administrator en un servidor Windows 2000/2003

Causa:
Una de las posibles causas puede ser el Servidor de terminales activado en el sistema en modo de *ejecución*.

Solución:
Microsoft aconseja pasar el Servidor de terminales a modo "instalación" durante la instalación de programas en un sistema con el servicio de Servidor de terminales activo. Esto se puede hacer a través de **Panel de control > Agregar o quitar programas**, o abriendo una solicitud de comandos y emitiendo el comando *cambiar usuario / instalación*. Tras la instalación, escriba *cambiar usuario / ejecutar* para volver al Servidor de terminales en modo de ejecución. Para obtener instrucciones en distintos pasos sobre este proceso, consulte el siguiente artículo: http://support.microsoft.com/kb/320185.

9.1.2 ¿Qué significa el código de error GLE?

La instalación de ESET Smart Security o ESET NOD32 Antivirus a través de la consola de administración remota puede generar en ocasiones un código de error GLE. Para descubrir el significado de cualquier número de error GLE, siga los siguientes pasos:

1) Abra una solicitud de comando haciendo clic en **Inicio → Ejecutar**. Escriba **cmd** y haga clic en **Aceptar**.
2) En la solicitud de comando, escriba: **net helpmsg error_number**

Ejemplo: "*net helpmsg 55*"

Resultado: El dispositivo o recurso de red especificado ya no está disponible.

9.2 Códigos de error que aparecen con frecuencia

Durante el funcionamiento de ERA, puede encontrarse mensajes de error con códigos de error que indican un problema con alguna función u operación. El apartado 8.2.1 detalla los códigos de error que se encuentran con más frecuencia al realizar instalaciones impulsadas, así como errores que se pueden encontrar en el registro del ERAS.

9.2.1 Mensajes de error en pantalla durante el uso de ESET Remote Administrator para instalar de forma remota ESET Smart Security o ESET NOD32 Antivirus

Código de error SC 6, código de error GLE 53 No se ha podido configurar la conexión IPC con el equipo de destino
Para establecer una conexión IPC, deben cumplirse estos requisitos:
1. Conjunto de TCP/IP instalado en el mismo equipo que el ERAS, así como en el equipo de destino.
2. Debe instalarse el uso compartido de archivos e impresoras para Microsoft Network.
3. Deben estar abiertos los puertos de uso compartido de archivos (135 – 139, 445).
4. El equipo de destino debe responder a solicitudes ping.

Código de error SC 6, código de error GLE 67 No se ha podido instalar el instalador de ESET en el equipo de destino
El recurso administrativo compartido ADMIN$ debe estar accesible en la unidad del sistema del cliente.

Código de error SC 6, código de error GLE 1326 No se ha podido configurar la conexión IPC con el equipo de destino. Es posible que el nombre de usuario o la contraseña especificados no sean correctos
No se han escrito correctamente el nombre de usuario y la contraseña del administrador o simplemente no se han introducido.

Código de error SC 6, código de error GLE 1327 No se ha podido configurar la conexión IPC con el equipo de destino
El campo de contraseña del administrador está en blanco. Una instalación remota impulsada no funciona con un campo de contraseña en blanco.

Código de error SC 11, código de error GLE 5 No se ha podido instalar el instalador de ESET en el equipo de destino
El instalador no puede tener acceso al equipo cliente debido a privilegios de acceso insuficientes (Acceso denegado).

Código de error SC 11, código de error GLE 1726 No se ha podido instalar el instalador de ESET en el equipo de destino
Este código de error aparece después de varios intentos de instalación, si no se cierra la ventana de Instalación impulsada tras el primer intento.

9.2.2 Códigos de error que aparecen con frecuencia en el registro ERA.

0x1203 – UPD_RETVAL_BAD_URL
Error del módulo de actualización – Se ha escrito incorrectamente el nombre del servidor de actualización.

0x1204 – UPD_RETVAL_CANT_DOWNLOAD
Este error puede aparecer:

- al actualizar a través de HTTP
  - el servidor de actualización devuelve un código de error HTTP entre 400–500 exceptuando los 401, 403, 404 y 407
  - si se descargan las actualizaciones desde un servidor CISCO y ha cambiado el formato de respuesta de autentificación de HTML
- al actualizar desde una carpeta compartida:
  - el error de vuelta no entra en las categorías "mala autentificación" o "archivo no encontrado" (por ejemplo, conexión interrumpida, o servidor no existente, etc.)
- ambos métodos de autentificación
  - si no se encuentra ninguno de los servidores del archivo upd.ver (el archivo se ubica en %ALLUSERSPROFILE\Application Data\ESET\ESET Remote Administrator\Server\updfiles)
  - no se ha podido entrar en contacto con el servidor a prueba de fallos (probablemente debido a la eliminación de las entradas de ESET correspondientes en el registro)
- configuración incorrecta del servidor proxy en el ERAS
  - El administrador debe especificar el servidor proxy en el formato

0x2001 – UPD_RETVAL_AUTHORIZATION_FAILED
Se ha producido un error en la autentificación del servidor de actualización: nombre de usuario o contraseña incorrectos.

0x2102 – UPD_RETVAL_BAD_REPLY
Puede encontrarse este error de módulo de actualización si se utiliza un servidor proxy para mediar en una conexión a Internet, en concreto un proxy Webwasher.

0x2104 – UPD_RETVAL_SERVER_ERROR
Error de módulo de actualización que indica un código de error de HTTP superior a 500. Si se utiliza el servidor HTTP de ESET, el error 500 indica un problema con reparto de memoria.

0x2105 – UPD_RETVAL_INTERRUPTED
Puede encontrarse este error de módulo de actualización si se utiliza un servidor proxy para mediar en una conexión a Internet, en concreto un proxy Webwasher.

9.3 ¿Cómo diagnosticar problemas con el ERAS?

Si sospecha que algo anda mal con el ERAS, o que no funciona correctamente, recomendamos que siga estos pasos:

1. Revise el registro de ERAS: haga clic en **Herramientas > Opciones del servidor** desde el menú principal de la ERAC. Desde la ventana de **Opciones del servidor**, haga clic en la ficha **Registro** y a continuación haga clic en **Ver registro**.
2. Si no ve mensajes de error, suba el nivel del **Contenido del registro** en la ventana de **Opciones del servidor** hasta el Nivel 5. Después de localizar el problema, recomendamos que cambie de nuevo al valor predeterminado.
3. También puede solucionar problemas activando el registro de depuración de la base de datos en la misma ficha. Para ello consulte **Registro de depuración**. Recomendamos que sólo active el **Registro de depuración** cuando intente duplicar el problema.
4. Si ve algún código de error distinto a los mencionados en esta documentación, póngase en contacto con el servicio de atención al cliente de ESET. Describa el comportamiento del programa, cómo replicar el problema o cómo evitarlo. Es muy importante incluir la versión del programa de todos los productos de seguridad de ESET involucrados (es decir, el ERAS, la ERAC, ESET Smart Security, ESET NOD32 Antivirus).

10. Ayudas y sugerencias

10.1 Tareas programadas

ESET NOD32 Antivirus y ESET Smart Security contienen un programador de tareas integrado que permite la programación regular de análisis a petición, actualizaciones, etc. Dicho programador muestra todas las tareas especificadas.

Se pueden configurar los siguientes cuatro tipos de tareas con ERA:

- Ejecutar aplicación externa
- Análisis de archivos durante el inicio del sistema
- Análisis del equipo a petición
- Actualizar

En la mayoría de los casos, no es necesario configurar una tarea de **Ejecutar aplicación externa**. La tarea **Análisis de archivos durante el inicio del sistema** es una tarea predeterminada y recomendamos que no se cambien sus parámetros[9]. Desde el punto de vista de un administrador, las tareas **Análisis del equipo a petición** y **Actualizar** son probablemente las más útiles:

- **Análisis del equipo a petición**
  Proporciona un análisis regular del antivirus (normalmente de las unidades locales) en clientes.

- **Actualizar**
  Esta tarea se encarga de actualizar soluciones cliente de ESET. Es una tarea predefinida y se ejecuta de forma predeterminada cada 60 minutos. Normalmente no hay razón para modificar sus parámetros. La única excepción son los portátiles, ya que sus propietarios a menudo se conectan a Internet fuera de las redes locales. En este caso, se puede modificar la tarea de actualización para utilizar dos perfiles de actualización dentro de una única tarea. Esto permitirá a los portátiles actualizarse desde el servidor local de actualización, así como desde los servidores de actualización de ESET.

También se puede encontrar la configuración del Programador de tareas en el Editor de configuración de ESET en **ESET Smart Security / ESET NOD32 Antivirus > Kernel de ESET > Configuración > Tareas programadas > Tareas programadas > Modificar**.

Para obtener más información, consulte el apartado 3.7 , "Editor de configuración de ESET".

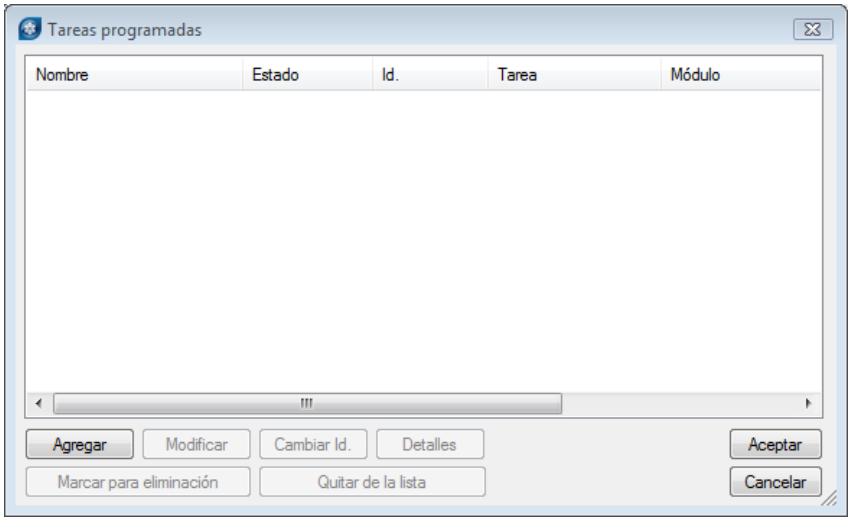


Figura 9-1

La ventana de diálogo puede contener las tareas existentes (haga clic en **Modificar** para modificarlos) o puede estar vacía. Depende de si ha abierto una configuración desde un cliente (por ejemplo, desde un cliente activo y configurado previamente), o ha cerrado un nuevo archivo con la plantilla predeterminada sin tareas.

A cada tarea nueva se le asigna un Id. de atributo. Las tareas predeterminadas tienen Id. decimales (1, 2, 3...) y a las tareas personalizadas se les asignan claves hexadecimales (p. ej. 4AE13D6C), las cuales se generan automáticamente al crear una nueva tarea.

[9] Si no se han realizado cambios tras la instalación, ESET NOD32 y ESET Smart Security contienen dos tareas predefinidas de este tipo. La primera tarea revisa los archivos del sistema en cada inicio de sesión del usuario, y la segunda hace lo mismo tras la correcta actualización de una base de firmas de virus.

Si la casilla de verificación de una tarea está marcada, significa que dicha tarea está activa y que se ejecutará en el cliente en cuestión.

Los botones que aparecen en la ventana Tareas programadas funcionan de la siguiente manera:

- **Agregar –** Agrega una nueva tarea.
- **Modificar –** Modifica las tareas seleccionadas.
- **Cambiar Id. –** Modifica el Id. de las tareas seleccionadas.

- **Detalles –** Información a modo de resumen sobre las tareas seleccionadas
- **Marcar para eliminación –** La aplicación del archivo .xml eliminará las tareas (con el mismo Id.) seleccionadas al hacer clic en este botón desde los clientes de destino.
- **Quitar de la lista –** Elimina las tareas seleccionadas de la lista. Tenga en cuenta que las tareas que se quiten de la lista en la configuración .xml no se eliminarán de las estaciones de trabajo de destino.

Durante la creación de una tarea nueva (botón **Agregar**) o durante la modificación de una existente (**Modificar**), debe especificar cuándo se ejecutará. La tarea puede repetirse tras un cierto periodo de tiempo (todos los días a las 12, todos los viernes, etc.) o se puede desencadenar con un suceso (p. ej. tras realizar correctamente una actualización, la primera vez que el equipo se inicia todos los días, etc.).

El último paso de la tarea **Análisis del equipo a petición** muestra la ventana de configuración especial, donde se puede definir qué configuración se utilizará para el análisis, es decir, qué perfil de análisis y destinos de análisis se usarán.

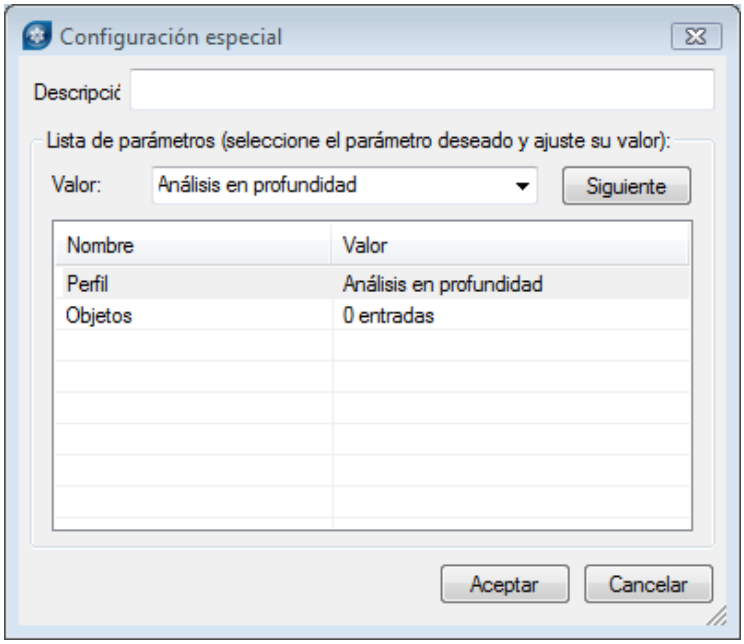


Figura 9-2

El último paso de la tarea **Actualizar** especifica qué perfiles de actualización se ejecutarán dentro de la tarea en concreto. Es una tarea predefinida y se ejecuta cada 60 minutos de forma predeterminada. Normalmente no hay razón para modificar sus parámetros. La única excepción son los portátiles, ya que sus propietarios a menudo se conectan a Internet fuera de las redes de la empresa. El último diálogo le permite especificar dos perfiles de actualización distintos, cubriendo actualizaciones desde un servidor local o desde los servidores de actualización de ESET.

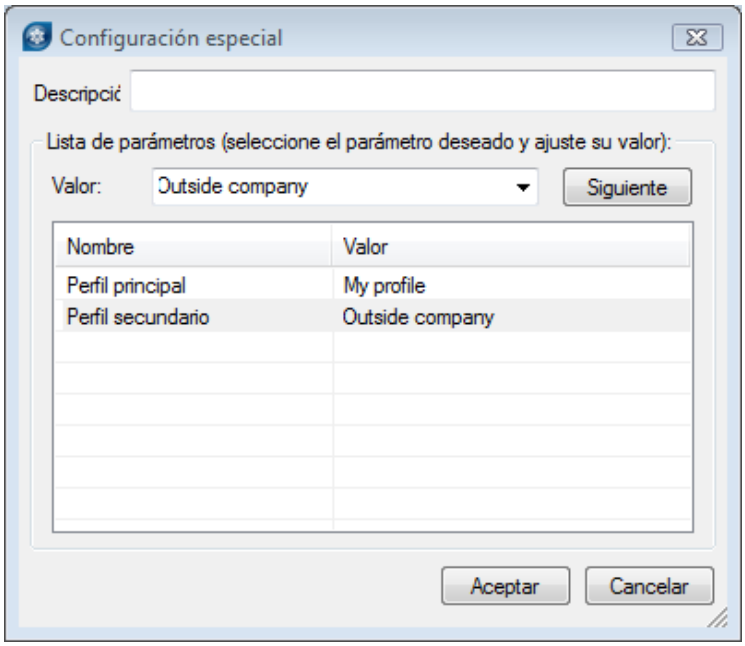


Figura 9-3

10.2 Eliminación de perfiles existentes

De vez en cuando puede encontrarse con perfiles duplicados (perfiles de actualización o análisis) que se crearon por error. Para eliminar esos perfiles de forma remota sin dañar otras opciones del programador de tareas, siga estos pasos:

- Desde la ERAC, haga clic en la ficha **Clientes** y a continuación doble clic en un cliente problemático.
- Desde la ventana de **Propiedades del cliente**, haga clic en la ficha **Configuración**. Seleccione las opciones **A continuación, ejecute el Editor de configuración de ESET para modificar el archivo** y **Utilice la configuración descargada en la nueva tarea de configuración** y, a continuación, haga clic en el botón **Nueva tarea**.
- En el nuevo asistente de tareas, haga clic en **Modificar**.
- En el Editor de configuración, pulse **CTRL + D** para anular la selección (gris) de todas las opciones. Esto ayuda a impedir cambios accidentales, ya que todo cambio nuevo quedará destacado en azul.
- Haga clic con el botón secundario en el perfil que desee eliminar y seleccione **Marcar perfil para eliminación** desde el menú contextual. Se eliminará el perfil tan pronto como se envíe la tarea a los clientes.

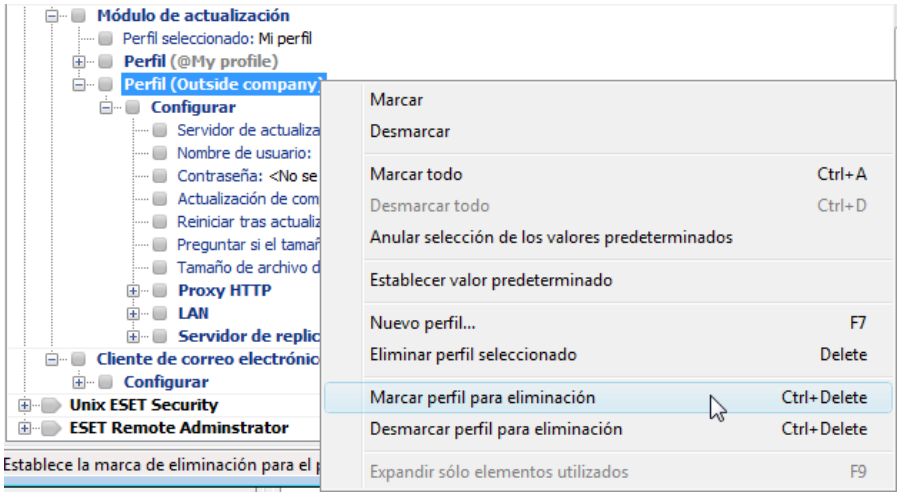


Figura 9-4

- Haga clic en el botón **Consola** del Editor de configuración de ESET y guarde la configuración.
- Compruebe que el cliente que seleccionó se encuentra en la columna **Elementos seleccionados** a la derecha. Haga clic en **Siguiente** y a continuación en **Finalizar**.

10.3 Exportación y otras características de la configuración XML del cliente

Desde la ERAC, seleccione los clientes en la ficha **Clientes**. Haga clic con el botón secundario y seleccione **Configuración...** en el menú contextual. Haga clic en **Guardar como...** para exportar la configuración asignada del cliente en cuestión a un archivo .xml[10]. Después, podrá utilizar el archivo .xml para diversas operaciones:

- En instalaciones remotas, el archivo .xml puede utilizarse como plantilla para una configuración predefinida. De esa manera, no se crea ningún archivo .xml nuevo y se asigna el archivo .xml existente (**Seleccionar...**) a un nuevo paquete de instalación.
- En la configuración de varios clientes, los clientes seleccionados reciben un archivo .xml previamente descargado y adoptan los ajustes que están definidos en el archivo (no se crea una configuración nueva, sólo se asigna mediante el botón **Seleccionar...**).

Ejemplo: *un producto de seguridad de ESET se instala únicamente en una estación de trabajo. Ajuste los valores de configuración directamente a través de la interfaz de usuario del programa. Una vez haya finalizado, exporte la configuración a un archivo .xml. Este archivo .xml podrá utilizarse en instalaciones remotas para otras estaciones de trabajo. En el caso de que se vaya a aplicar el modo "Basado en las directrices", este método puede resultar de gran utilidad en tareas tales como el ajuste de las reglas del cortafuegos.*

10.4 Actualización combinada para portátiles

Si en su red local hay algún dispositivo móvil (es decir, portátiles), le recomendamos que configure una actualización combinada desde dos orígenes: desde los servidores de actualización de ESET y desde el servidor local. En primer lugar, los portátiles establecen conexión con el servidor local y, si la conexión falla (porque se encuentren fuera del lugar de trabajo), descargarán las actualizaciones directamente desde los servidores de ESET. Para permitir esta funcionalidad:

- Cree dos perfiles de actualización, uno para el servidor local (denominado "LAN" en el siguiente ejemplo) y otro para los servidores de actualización de ESET (INET)

- Cree una nueva tarea de actualización o modifique una existente con el Programador (**Herramientas > Programador** del programa principal de ESET Smart Security o ESET NOD32 Antivirus).

La configuración puede realizarse directamente desde los portátiles o de forma remota con el Editor de configuración de ESET. Puede aplicarse durante el proceso de instalación o más tarde como tarea de configuración.

Para crear nuevos perfiles en el Editor de configuración de ESET, haga clic con el botón secundario en el apartado **Actualizar** y seleccione **Nuevo perfil** en el menú contextual.

[10] Los archivos de la configuración .xml también pueden extraerse directamente desde la interfaz del programa ESET Smart Security.

El resultado de las modificaciones debería ser similar al que se muestra a continuación:

Figura 9-5

El perfil LAN descarga actualizaciones desde el servidor local de la compañía (http://servidor:2221), mientras que el perfil INET establece conexión con los servidores de ESET (**Seleccionar automáticamente**). A continuación, defina una tarea de actualización que ejecute cada perfil de actualización sucesivamente. Para ello, navegue hasta **ESET Smart Security, ESET NOD32 Antivirus > Kernel > Configuración > Tareas programadas** en el Editor de configuración de ESET. Haga clic en el botón **Modificar** para que aparezca la ventana **Tareas programadas**.

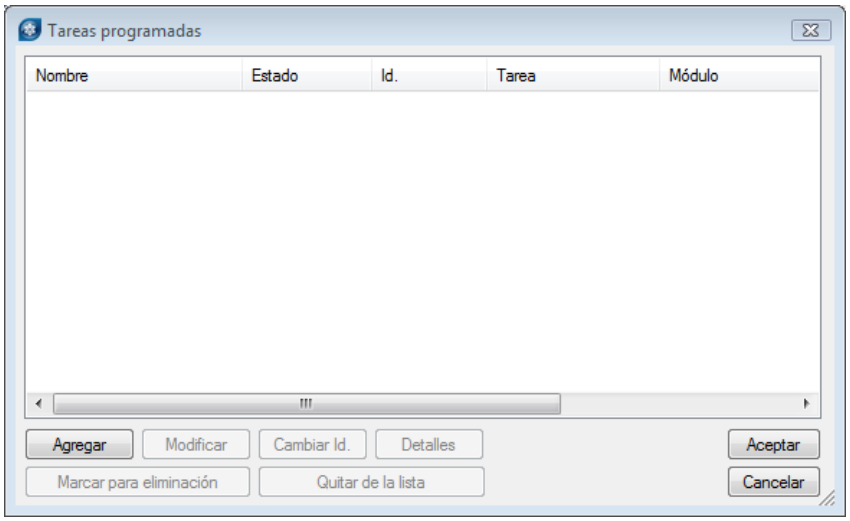


Figura 9-6

Para crear una tarea nueva, haga clic en **Agregar**. Desde el menú desplegable **Tarea programada**, seleccione **Actualizar** y haga clic en **Siguiente**. Introduzca el **Nombre de tarea** (p. ej., "actualización combinada"), seleccione **Repetidamente cada 60 minutos** y proceda a la selección de un perfil principal y otro secundario.

En caso de que las estaciones de trabajo portátiles tuvieran que contactar con el servidor local en primer lugar, el perfil principal debería establecerse como LAN y el secundario como INET. El perfil INET sólo se aplica si la actualización desde LAN falla.

Recomendación: Exporte la configuración .xml actual desde un cliente (para obtener más información, consulte el apartado 9.3) y realice las modificaciones mencionadas anteriormente en el archivo .xml exportado. De esta manera, se evitará toda posible duplicación entre el Programador y los perfiles no operativos.

10.5 Instalación de productos de terceros con ERA

Además de la instalación remota de los productos de ESET, mediante ESET Remote Administrator es posible instalar otros programas. El único requisito es que el paquete de instalación personalizado debe tener el formato .msi.
La instalación remota de paquetes personalizados se puede ejecutar mediante un proceso muy similar al descrito en el apartado 4.2, "Instalación remota".

La principal diferencia reside en el proceso de creación del paquete, que sería el siguiente:

- Desde la ERAC, haga clic en la ficha **Instalación remota**.
- Haga clic en el botón **Paquetes...**
- En el menú desplegable **Tipo de paquete** seleccione **Paquete personalizado**.
- Haga clic en **Agregar...**, haga clic en **Agregar archivo** y seleccione el paquete msi deseado.
- Seleccione el archivo en el menú desplegable **Archivo de entrada del paquete** y haga clic en **Crear**.
- Tras volver a la ventana original, puede especificar los parámetros de la línea de comandos del archivo .msi. Los parámetros serán los mismos que para una instalación local del paquete en cuestión.
- Haga clic en **Guardar como...** para guardar el paquete.
- Haga clic en **Cerrar** para salir del editor de paquetes de instalación.

La distribución a las estaciones de trabajo cliente del paquete personalizado recién creado se realiza de la misma manera que en las instalaciones remotas. Puede consultarla en capítulos anteriores. El paquete puede enviarse a las estaciones de trabajo de destino mediante una instalación remota impulsada, una instalación impulsada por correo electrónico o mediante inicio de sesión. El servicio Windows Installer de Microsoft llevará a cabo el proceso de instalación desde el momento en que se ejecuta el paquete.